BANCO DE PORTUGAL
EUROSISTEMA

Relatório da Consulta Pública n.º 2 /2019

PROJETO DE INSTRUÇÃO RELATIVO AO REPORTE DE INCIDENTES DE CIBERSEGURANÇA

Nota introdutória

O Banco de Portugal (BdP) colocou à consulta pública, entre os dias 8 de julho e 19 de agosto de 2019, um projeto de Instrução que pretende regulamentar o reporte de incidentes de cibersegurança nas instituições de crédito supervisionadas pelo Banco de Portugal e nas instituições de crédito classificadas como Significativas (SIs) à luz do Regulamento (UE) n.º 468/2014 do Banco Central Europeu (BCE), de 16 de abril de 2014, que define o quadro de cooperação no âmbito do Mecanismo Único de Supervisão (MUS).

O projeto de Instrução visa i) estabelecer o dever de reporte de incidentes de cibersegurança em instituições supervisionadas pelo BdP e BCE ii) harmonizar os diferentes modelos, taxonomias e terminologias existentes nesta matéria; e iii) centralizar a comunicação de incidentes num ponto único de contacto, nomeadamente no portal BP*net*, em que o Banco de Portugal reencaminhará esta informação ao BCE e ao Centro Nacional de Cibersegurança (quando aplicável).

No decurso do período de consulta pública, foram recebidas respostas de 4 entidades, num total de 35 comentários, destacando-se, dos contributos recebidos, os seguintes aspetos relevantes:

- Clarificação da definição de "incidente de cibersegurança" e do seu alcance, tendo em conta os diferentes reportes de incidentes existentes;
- Clarificação sobre a aplicação do conceito de "incidente de cibersegurança" a casos concretos;
- Clarificação de alguns dos termos utilizados nas especificações do Artigo 4.º sobre os critérios e indicadores de materialidade, em particular, dos termos "área de negócio crítica para a confiança dos consumidores", "consequência negativa", "comunicação formal" e "especialista";
- Clarificação de algumas questões operacionais relacionadas com o envio dos reportes, nomeadamente sobre os canais alternativos de envio em caso de incapacidade operacional e sobre a relevância ou interpretação de campos específicos (p. ex., "classificação do incidente");
- Aditamento de um período de "*vacatio legis*" de 30 dias úteis após a publicação da Instrução, tendo em vista a necessidade de as instituições adequarem os seus procedimentos internos para responder aos requisitos da presente Instrução.

Seguidamente, são apresentados em maior detalhe os comentários recebidos com a respetiva análise e eventuais alterações à proposta original de Instrução. Para maior facilidade de exposição e/ou quando tal se justifique por outros motivos ponderosos, os comentários recebidos são apresentados e analisados de forma agregada.

Como nota final, o Banco de Portugal agradece o carácter positivo e construtivo dos comentários recebidos, que revelam um interesse crescente na temática do risco de segurança das tecnologias de informação e comunicação.

Análise dos contributos recebidos na consulta pública

Preceitos do projeto de Instrução	Entidades consultadas	Respostas recebidas	Análise do Banco de Portugal	Decisão
Artigo 1.º n.º 1	CGD, APB	«Especificar neste Artigo (ou num outro Artigo da Instrução) qual o conceito de "incidente de cibersegurança" a ser considerado pelas instituições.» «A delimitação do objeto e âmbito desta obrigação de reporte deve de forma clara afastar situações de duplicação com a que está instituída pela Instrução do Banco de Portugal nº 1/2019 e ser coerente com os restantes preceitos da presente instrução, nomeadamente com o preconizado no nº 9 do art 7º.»	O Banco de Portugal informa que o preâmbulo do projeto de Instrução inclui uma definição de incidente de cibersegurança. No entanto, atendendo às preocupações expressas sobre a necessidade de maior clareza no conceito de "incidente de cibersegurança", o Banco de Portugal introduziu uma disposição no n.º 2 do Artigo 1.º contendo uma definição de incidente de cibersegurança. Cabe ressalvar que poderão existir determinados incidentes que impliquem uma duplicação de reportes, na medida em que a Instrução n.º1/2019 do Banco de Portugal se mantém em vigor após a entrada em vigor do presente Projeto de Instrução. Importa, no entanto, sublinhar que a Instrução n.º1/2019 do Banco de Portugal se destina apenas a Prestadores de Serviços de Pagamento registados e autorizados pelo Banco de Portugal e abrange, unicamente, incidentes operacionais ou de segurança em serviços relacionados com pagamentos.	Acolhido.

Artigo 2.º n.º 1	CGD, APB	«Clarificar que, nomeadamente no caso das instituições de crédito significativas sob supervisão do BCE, a aplicação dos critérios de classificação de um ciberincidente como significativo/severo deve efetuar-se em base consolidada (ao nível de Grupo).» «Os incidentes de segurança ocorridos em operações sedeadas no estrangeiro terão que ser comunicados pela casa-mãe em Portugal, em virtude daquelas operações consolidarem em Portugal? Ou significa que para o cálculo das variáveis que contribuem para uma eventual comunicação do incidente são somados os valores em causa, em cada uma das operações, nos casos de incidentes que afetem as várias operações internacionais?»	O n.º1 do Artigo 2.º estabelece que um incidente de cibersegurança deve ser comunicado, em base consolidada, quando afete entidades incluídas no perímetro de supervisão, independentemente do local onde prestam atividade. Em consequência - e sem prejuízo do *infra* referido - os incidentes de segurança ocorridos em entidades sedeadas no estrangeiro terão que ser comunicados pela casa-mãe em Portugal, caso aquelas entidades consolidem em Portugal. A única exceção prevista são as sucursais de instituições de crédito com sede no estrangeiro que, segundo o n.º 2 do Artigo 2.º, devem comunicar ao Banco de Portugal, em base individual, a ocorrência de incidentes de cibersegurança significativos ou severos que afetem, ou possam vir a afetar, a atividade exercida em território nacional. No caso das instituições de crédito (ICs) significativas (SIs) e, em particular, das filiais e sucursais de ICs com sede no estrangeiro, o Banco de Portugal reconhece que o texto atual do projeto de Instrução poderá implicar uma duplicação de tarefas e/ou suscitar o envio de reportes segundo um critério mais abrangente do que aquele que foi definido pelo BCE. No entanto, na presente Instrução, considerou-se — em conformidade com a	Não acolhido.

			posição da autoridade competente a nível nacional no âmbito da aplicação da Diretiva SRI — que os critérios devem ser aplicados a nível individual.	
Artigo 2.º n.º 1	APB, BPI	«2 horas é um prazo demasiado curto para se analisar/investigar a existência real de um incidente de segurança. Sugere-se que, onde se lê "no prazo de até 2 horas após a deteção do incidente", se passe a ler "no prazo de até 2 horas após o incidente ser considerado relevante, tendo por base os critérios definidos".»	O Banco de Portugal manteve a proposta original do projeto de Instrução, tendo em conta o reporte de incidentes de cibersegurança das SIs ao BCE que estabelece um prazo de reporte inicial de 2 horas após a deteção do incidente classificado como significativo ou severo.	Não acolhido.
Artigo 2.º n.º 2	APB	«Na eventualidade de ocorrência de um incidente que se enquadre no âmbito da presente Instrução e que obrigue a um reporte, as sucursais de instituições de crédito com sede no estrangeiro estarão sujeitas a uma dupla obrigação de reporte, isto é, via casa-mãe ao supervisor do respetivo país e um outro reporte, referente à atividade da Sucursal, ao Banco de Portugal (autoridade competente do Estado-Membro de acolhimento)? »	O Banco de Portugal considera fundamental que os incidentes que afetem a atividade em Portugal sejam reportados diretamente ao Banco de Portugal, optando por manter a proposta original do projeto de Instrução. Vide resposta ao Artigo 2.º nº1.	Não acolhido.
Artigo 3.º n.º 1	CGD, APB	«Alterar o sétimo critério para "Comunicação formal a autoridades competentes a nível nacional ou na União Europeia".»	O Banco de Portugal concorda com o comentário, tendo substituído o termo "União Europeia" pelo termo "internacional" de forma a abranger o envolvimento de autoridades fora da União Europeia.	Acolhido parcialmente.

Artigo 3.º n.º 1	CGD, APB	«Clarificar o nono critério "Avaliação de especialista", desejavelmente através do que se entende por especialista para efeito da presente proposta de Instrução.»	O Banco de Portugal reconhece a importância de incluir maior detalhe sobre este ponto no n.º 10 do Artigo 4.º., tendo especificado que a avaliação de especialista pressupõe a aplicação de eventuais critérios internos, previamente estabelecidos pela entidade, para avaliar os riscos da ocorrência de um incidente.	Acolhido.
Artigo 4.º n.º 1	BPI	«Necessidade de clarificação e melhor determinação do que se deve entender por "consequência negativa".»	O Banco de Portugal informa que "consequência negativa" refere-se à probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação.	Não acolhido.

Artigo 4.º n.º 4 ii)	BPI	«O que deve ser entendido por "área de negócio crítica para a confiança dos consumidores"?»	O Banco de Portugal esclarece que esta alínea tem como objetivo abranger os incidentes com potencial impacto significativo na reputação das entidades junto dos consumidores (independentemente de os incidentes terem tido ou não cobertura mediática), incluindo incidentes que comprometam sistemas com dados pessoais ou financeiros de utilizadores ou que afetem sistemas críticos para a manutenção da confiança no setor, como, por exemplo, sistemas de pagamentos. Por razões de clareza, o Banco de Portugal decidiu, ainda assim, reformular este ponto.	Acolhido.
Artigo 4.º n.º 5 ii)	BPI	«O critério previsto na subalínea ii) do n.º 5 do art.º 4 deve ser melhor delimitado.»	O Banco de Portugal manteve a proposta original por considerar que o grau de detalhe da subalínea ii) é suficiente, devendo ser reportados os incidentes que possam implicar a ativação de seguros ou outros instrumentos similares na cobertura de perdas.	Não acolhido.

Artigo 4.º n.º 6	Finantia	«Os bancos com pequena dimensão, como são normalmente os Bancos de Investimento, e em que o Banco Finantia se enquadra, têm um número reduzido de Colaboradores. Por essa razão, há uma maior multidisciplinaridade e o seu modelo de gestão assenta numa forte participação das Direções ao nível das decisões operacionais, correspondendo no nosso caso a um administrador delegado. Assim sendo, de acordo com a proposta do ponto 6 do Artº 4, ao se envolver o responsável de qualquer função, para o acompanhamento e tomada de decisão, o incidente tem obrigatoriamente de ser classificado como significativo. Nestes casos não deveria haver alguns considerandos específicos para esta realidade?»	O reporte de um incidente de cibersegurança a um administrador delegado deve ser considerado um encaminhamento para instância interna superior ao tratar-se de "um cargo relevante de direção de topo", sempre e quando este "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)".	Acolhido.

Artigo 4.º n.º 6	APB	«Em geral, o Diretor de Segurança da Informação (Chief Security Officer) deve estar a par de todos os incidentes de cibersegurança. Não significa, por si só, que o incidente deva ser classificado como significativo, até porque poderá não ter qualquer impacto para o negócio. Sugere-se a alteração de "titulares de cargos de gestão e/ou direção" para a seguinte redação: "titulares de cargos de gestão de topo."»	O Banco de Portugal esclarece que a redação atual estabelece que devem ser classificados como significativos os incidentes que impliquem que um cargo de direção de topo, como a Direção de Segurança de Informação, "acompanhe [o incidente], numa base continuada, durante o período da sua ocorrência e resolução, fora do âmbito de qualquer procedimento periódico de notificação". Assim, estariam excluídas as situações mencionadas, já que correspondem a reportes periódicos e/ou atos de mera tomada de conhecimento por parte da direção de topo. Porém, o Banco de Portugal decidiu substituir o termo "cargos de gestão e/ou direção" pelo termo "cargos de direção de topo" que consta no Artigo 2.º-A, alínea p) do RGICSF, com vista a incluir de forma explícita os cargos diretamente responsáveis perante o órgão de administração, bem como quaisquer funções responsáveis pela gestão corrente de risco.	Acolhido parcialmente.

Artigo 4.º n.º 8	CGD, APB	«Clarificar que não deve ser considerada uma comunicação formal de um incidente, a simples partilha de informação no âmbito das redes de CSIRT (ex: comunicação de URL's maliciosos, emails/campanhas de phishing, spam).» «A obrigação de reporte decorrente da Lei n.º 46/2018 beneficia da ajuda do CERT.pt, entidade que coordena a resposta a incidentes de cibersegurança no espaço nacional. Pretende-se com a presente Instrução assegurar a comunicação às duas entidades? Ou, como é referido no artigo 1º da Instrução, os Bancos reportam apenas ao BdP e este reportará em nome destes ao CNCS (nesse caso, como é contactado o CERT.PT)?»	A atual redação do projeto de Instrução refere que devem ser considerados "significativos" todos os incidentes que impliquem uma "comunicação formal" a autoridades competentes, pelo que estariam excluídos meros exercícios de partilha de informação e conhecimento no âmbito das redes de CSIRT. De forma a clarificar este entendimento, o Banco de Portugal decidiu, ainda assim, substituir o termo "comunicação formal" por "notificação formal" e eliminar a referência ao CNCS, já que o reporte realizado no Portal BP*net* é reencaminhado de forma automática e imediata ao CNCS (quando aplicável).	Acolhido.

Artigo 4.º n.º 9	APB	«Papel e envolvimento de entidades que prestam serviços comuns aos Bancos.»	O Banco de Portugal informa que as instituições de crédito devem reportar incidentes significativos com origem em terceiros sempre que estes resultem em eventos de segurança de informação com probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação da instituição (p. ex., assinalando no modelo de reporte o vetor de entrada "rede de terceiros" ou "outro").	Não acolhido.
Artigo 5.º n.º 3	APB	«Deverá existir terceira via, por exemplo contacto telefónico ou entrega física.»	O Banco de Portugal informa que a probabilidade de ocorrência destas situações é manifestamente diminuta e sublinha que o reporte, em formato Excel, pode ser descarregado pelas entidades, a qualquer momento, no Portal BP*net,* para antecipar futuras situações de incapacidade operacional temporária.	Não acolhido.

Artigo 8.º n.º 1	APB, CGD	«Instituir um período de transição razoável (ex. 60 dias após publicação da Instrução) para adequação de processos e procedimentos pelas instituições.»	O Banco de Portugal sublinha que o disposto no presente projeto de Instrução não prevê o desenvolvimento de soluções informáticas específicas para efeitos de reporte, visto que o reporte será efetuado via Portal BP*net,* disponibilizado pelo Banco de Portugal. Adicionalmente, o Banco de Portugal considera que existe um elevado grau de maturidade das entidades na utilização do Portal BP*net* para efeitos de reporte de informação. Não obstante, o Banco de Portugal concorda em instituir um período de "*vacatio legis*" de 30 dias úteis após a publicação da Instrução, por forma a garantir que as entidades abrangidas dispõem de um intervalo de tempo razoável para adequar quaisquer procedimentos internos.	Acolhido parcialmente.
Clarificação	Finantia	«No âmbito do projeto de instrução, o reporte de incidentes de cibersegurança de origem interna e não intencionais, também deve ser reportado ao BdP?»	A definição proposta abrange todos os tipos de incidentes de cibersegurança, incluindo aqueles imprevistos com origem interna.	Vide resposta ao n.º1 do Artigo 1.º.

Clarificação	Finantia	«Um incidente interno, como a avaria por ex.de um Servidor, Switch de rede, UPS ou mesmo um problema Aplicacional, que provoque a indisponibilidade do acesso à informação, por tempo determinado, é considerado incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	São considerados incidentes de cibersegurança as ocorrências que constituam um evento de segurança de informação com probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação. Nesse sentido, as eventuais falhas operacionais ou avarias em sistemas, redes e aplicações previstas no Plano de Continuidade de Negócio, em princípio não constituirão, por si só, incidentes de cibersegurança, desde que não constituam eventos de segurança de informação com impacto significativo.	Vide resposta ao n.º1 do Artigo 1.º.
Clarificação	Finantia	«O envio inadvertido de um e-mail para um destinatário diferente do pretendido, que não contém dados pessoais, mas sim confidenciais, é considerado incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	O envio inadvertido de uma mensagem de correio eletrónico com informação confidencial poderá infringir as políticas de informação e uso dos sistemas, aplicações ou redes, pelo que pode ser considerado um incidente de cibersegurança significativo ou severo caso preencha um dos critérios definidos no n.º1 do Artigo 3.º.	Vide resposta ao n.º1 do Artigo 1.º.

Clarificação	Finantia	«O extravio de informação pessoal ou confidencial em formato físico é considerado incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	A recolha de informação pessoal ou confidencial pode ser considerada um incidente de cibersegurança nos seguintes casos: i) *scan*, *sniffing* ou *phishing*, ii) intrusões resultantes da exploração de vulnerabilidade ou compromisso de conta, iii) violações da política de segurança da informação em sistemas, aplicações ou redes, como por exemplo nos casos de acessos indevidos ou modificações não autorizadas.	Vide resposta ao n.º1 do Artigo 1.º.
Clarificação	Finantia	«A queda de um link de rede para uma Agência, que provoque a indisponibilidade dos colaboradores aí sediados, à informação por um período determinado de tempo, é considerada incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	São considerados incidentes de cibersegurança as ocorrências que constituam um evento de segurança de informação com probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação. Nesse sentido, as eventuais falhas operacionais ou avarias em sistemas, redes e aplicações previstas no Plano de Continuidade de Negócio, em princípio não constituirão, por si só, incidentes de cibersegurança, desde que não tenham efeito adverso na segurança da informação.	Vide resposta ao n.º1 do Artigo 1.º.

Clarificação	Finantia	«A queda de um link de rede para um Parceiro (ex. SIBS), que provoque a indisponibilidade de acesso aos seus recursos, por um período determinado de tempo, é considerada incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	Em linha com o comentário anterior, o Banco de Portugal esclarece que a indisponibilidade de acesso a serviços prestados por terceiros só deve ser considerado incidente de cibersegurança se a indisponibilidade resultar de um evento de segurança de informação que comprometa as operações de negócio e/ou ameace a segurança da informação da entidade (por exemplo incidentes de cibersegurança em terceiros que possibilitem a exploração de vulnerabilidades nos sistemas da entidade).	Vide resposta ao n.º1 do Artigo 1.º.
Clarificação	Finantia	«Qualquer incidente que envolva dados pessoais e que tenha de ser comunicado no âmbito do RGPD à CNPD, é considerado incidente de cibersegurança e como tal deve ser reportado consoante a sua gravidade?»	O presente projeto de Instrução estabelece que devem ser reportados os eventos de segurança de informação que possam ter um impacto material na reputação da entidade. Estão incluídos os incidentes de cibersegurança que comprometam dados pessoais dos utilizadores e que resultem no incumprimento do Regulamento Geral de Proteção de Dados (RGPD).	Vide resposta ao n.º1 do Artigo 1.º.

Anexo - Modelo de reporte (em Excel)	Finantia	«No anexo do Projeto de Instrução não se encontra nenhum atributo para preencher a classificação do incidente (significativo ou severo). O Excel atribui automaticamente a classificação com base no conteúdo preenchido?»	O Banco de Portugal ponderou as vantagens da introdução de um campo de informação no relatório inicial que permita assinalar os incidentes classificados como severos. No entanto, concluiu-se que todos os incidentes severos são, por definição, significativos, devendo ser comunicados ao Banco de Portugal. De acordo com o atual modelo de reporte, as entidades afetadas devem indicar no campo de descrição geral se o incidente cumpre com os critérios para a atribuição da classificação de "severo". Adicionalmente, o n.º 10 do Art. 4.º estabelece que o incidente possa ser classificado como severo por parte de um especialista do Banco de Portugal.	Não acolhido.
Anexo - Modelo de reporte (em Excel)	APB	«No Modelo de Reporte, na secção em Português, está indicado "APS" como Advanced Persistent Threat, contudo o acrónimo certo é "APT".»	O Banco de Portugal toma boa nota do comentário recebido e corrigirá o acrónimo para a sua forma correta no modelo de reporte em formato Excel.	Acolhido.

Anexo - Modelo de reporte (em Excel)	APB	«No campo “incidente descoberto por”, acrescentar “SOC”.»	O Banco de Portugal informa que, nestes casos, a instituição deve assinalar o campo “Se outro, pf especificar” e indicar “SOC”, mas considera que não é necessário proceder a alterações no modelo de reporte, já que a opção de redação aberta pretende e permite acomodar qualquer opção não contemplada nas restantes.	Não acolhido.
Anexo - Modelo de reporte (em Excel)	APB	«Nos campos “Quem lidera a investigação ao incidente” e “Quem lidera as ações de remediação”, importa clarificar o que se entende por “Grupo”.»	O Banco de Portugal informa que as “sociedades em relação de grupo” estão definidas na alínea jj) do Artigo 2.º-A do RGICSF como sociedades coligadas entre si, nos termos em que o Código das Sociedades Comerciais caracteriza este tipo de relação, independentemente de as respetivas sedes se situarem em Portugal ou no estrangeiro.	Não acolhido.