Flash

Banking and Finance

Reporte de Incidentes de Cibersegurança

Introdução

Foi divulgada a 25 de Novembro, pelo Banco de Portugal, a Instrução n.º 21/2019, que regulamenta 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).

Esta instrução entrará em vigor a 9 de Janeiro de 2020, e visa harmonizar as eventuais sobreposições de deveres de reporte ao BCE e ao Centro nacional de cibersegurança e agilizar a comunicação das entidades através de um ponto único de contacto, o Banco de Portugal, que reencaminhará, se necessário e sem demora, a informação ao BCE e ao Centro Nacional de cibersegurança, consoante o âmbito e a natureza do incidente, não prejudicando, porém, os eventuais deveres de comunicação à Comissão Nacional de Proteção de Dados.

As instituições visadas devem comunicar, em base consolidada, no prazo de até 2 horas após a deteção do incidente, todos os incidentes de cibersegurança significativos ou severos ocorridos ou que produzam efeitos nas entidades incluídas no perímetro de supervisão, independentemente do local onde estas últimas prestam a sua atividade, 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 (Nota: todos os campos são de preenchimento obrigatório).

I. Cibersegurança

No âmbito da Instrução, são considerados incidentes de cibersegurança todos os eventos de segurança de informação com probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação, designadamente eventos que:

- impliquem um efeito adverso na segurança dos sistemas, aplicações ou redes;
- comprometam a informação que estes sistemas, aplicações e redes processam, armazenam ou partilham;
- infrinjam as políticas de segurança de informação e uso dos sistemas, aplicações ou redes das entidades.

II. Incidentes Significativos ou Severos

As entidades devem classificar como significativos ou severos os incidentes que preencham pelo menos um dos seguintes critérios de materialidade:

Critérios	Significativo	Severo
Utilizadores afetados (todos os clientes que tenham sofrido ou possam vir a sofrer qualquer consequência negativa resultante da ocorrência do incidente de cibersegurança)	> 50 000 utilizadores **ou** > 25 % da base de clientes	–
Impacto económico (perdas globais, diretas ou indiretas, associadas à ocorrência do incidente, que tenham ocorrido ou que apresentem elevada probabilidade de vir a ocorrer)	> 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 (tendo em conta, nomeadamente, se o incidente teve cobertura mediátca, afetou sistemas críticos para a confiança dos utilizadores, resultou em perdas de confidencialidade e integridade de dados sensíveis, tem caráter recorrente, ou se pode vir a dar lugar à aplicação de sanções)	✓	–
Ativação de mecanismos de gestão de crises (nomeadamente, planos de continuidade de negócio ou de recuperação de desastres, seguros ou outros instrumentos similares de cobertura de perdas relacionadas com o Incidente ou mecanismos ou procedimentos internos de resposta a crises, como planos de contingência, equipas ou comités de crise, comités de cibersegurança, entre outros)	✓	–
Encaminhamento para instâncias internas superiores	✓	–
Incumprimentos legais ou regulamentares (nomeadamente, não cumprimento de prazos regulatórios, incluindo prazos de reporte de informação financeira; incapacidade de cumprir obrigações legais e contratuais perante os clientes ou consumidores do; incumprimento de regulação em matéria de prevenção do branqueamento de capitais e do terrorismo ou potencial risco jurídico associado a uma elevada probabilidade de ocorrerem litígios)	✓	–
Notificação formal a autoridades competentes a nível nacional ou internacional	✓	–
Risco sistémico (nomeadamente, se existir possibilidade de efeito contágio a outras entidades; colocar em causa a estabilidade do setor financeiro, outra entidade for alvo do mesmo incidente de cibersegurança ou o incidente expuser vulnerabilidades relevantes para o setor)	✓	✓
Avaliação de especialista	✓	✓

III. Reporte em Inicial, Intercalar e Final

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

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

iii. Por último, as entidades devem submeter um reporte final no prazo de até 30 dias úteis após o reporte inicial. O reporte final deve refletir a informação recolhida na investigação interna das causas do incidente, bem como potenciais medidas mitigadoras adotadas ou previstas para resolver o incidente e evitar a sua recorrência no futuro. Este reporte deve incluir i) valores reais sobre o impacto do incidente, substituindo eventuais estimativas em reportes anteriores e ii) uma descrição, clara e rigorosa, das medidas mitigadoras adotadas ou previstas.

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

Aconselha-se a consulta da Instrução, que se encontra neste link, que se ocupa de esclarecer possíveis dúvidas e definir os critérios que utiliza.

www.csassociados.pt
André Fernandes Bento
Tomás Ludovice