BANCO DE PORTUGAL
EUROSISTEMA

Projeto de instrução sobre a gestão e reporte, pelos prestadores de serviços de pagamento, dos riscos operacionais e de segurança

Assunto: Gestão e reporte, pelos prestadores de serviços de pagamento, dos riscos operacionais e de segurança

Em 2017, a Autoridade Bancária Europeia (EBA) publicou as "Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366" (EBA/GL/2017/17), estabelecendo um conjunto de requisitos de segurança nas Tecnologias de Informação e Comunicação (TIC) dos prestadores de serviços de pagamento (PSP).

Adicionalmente, também em 2017, a EBA publicou as "Orientações relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP)" (EBA/GL/2017/05) com o objetivo de garantir a convergência das práticas de supervisão na avaliação do risco das TIC, tal como especificado de forma detalhada nas "Orientações da EBA relativas aos procedimentos e metodologias comuns a seguir no âmbito do SREP" (EBA/GL/2014/13).

Em fevereiro de 2019, a EBA publicou as "Orientações sobre Subcontratação Externa" (EBA/GL/2019/02) que estabelecem procedimentos e requisitos para uma gestão eficaz da subcontratação externa das TIC, tendo para este efeito o Banco de Portugal emitido a Carta Circular n.º CC/2019/00000065[1].

Mais recentemente, a 28 de novembro de 2019, a EBA publicou as "Orientações relativas à gestão dos riscos associados às TIC e à segurança" (EBA/GL/2019/04, doravante "Orientações"), dirigidas a instituições de crédito, empresas de investimento e PSP[2]. Estas Orientações incorporam e revogam as anteriores "Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE) 2015/2366" (EBA/GL/2017/17). Em concreto, as Orientações especificam as medidas e procedimentos que as instituições financeiras devem adotar, no âmbito do risco operacional e governo interno, para gerir os seus riscos associados às TIC e à segurança (no qual se incluem, entre outros, por um lado o risco de cibersegurança e, por outro os riscos operacionais e de segurança relacionados com os serviços de pagamento).

Neste âmbito, as Orientações preveem, através de remissão para o disposto no n.º 2 do artigo 95.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)[3], que os PSP devem comunicar ao Banco de Portugal uma avaliação exaustiva e atualizada dos riscos operacionais e de segurança relacionados com os serviços de pagamento por si prestados, bem como da adequação das medidas de mitigação e controlo dos riscos que foram implementadas em resposta a esses riscos. Esta comunicação anual visa recolher informação relevante sobre os riscos operacionais e de segurança dos serviços de pagamento, assegurando que as entidades visadas controlam estes riscos, bem como a sua exposição a incidentes operacionais e de segurança severos.

[1] https://www.bportugal.pt/cartacircular/cc201900000065.
[2] https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management.
[3] Transposto para o ordenamento jurídico português pelo n.º 3 do artigo 70.º do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro.

O Banco de Portugal comunicou à EBA a sua intenção de cumprir com as referidas Orientações a partir de 30 de junho de 2020, e neste contexto publicou a Carta Circular n.º CC/2020/00000029, de 6 de maio, divulgando às instituições visadas a sua intenção e respetiva data de cumprimento com as Orientações.

A presente Instrução tem como objeto implementar os requisitos constantes das Orientações, incluindo o dever de reporte da avaliação anual dos riscos operacionais e de segurança dos serviços de pagamento prestados.

Cabe notar que a Instrução se dirige exclusivamente aos PSP, pelo que não se aplica às Empresas de Investimento, às sucursais em Portugal de instituições de crédito autorizadas noutros Estados-Membros da União Europeia (UE), às sucursais de instituições de moeda eletrónica com sede na UE e às sucursais de instituições de pagamento com sede na UE.

O Banco de Portugal sublinha a importância destas Orientações para o reforço da resiliência operacional do setor financeiro.

Em primeiro lugar, as Orientações introduzem uma maior especificação das expetativas de supervisão do risco associados às TIC e à segurança e robustecem desse modo os atuais requisitos prudenciais, em particular no questionário de autoavaliação do risco TIC das instituições de crédito cujos resultados são tidos em conta no SREP, designadamente na análise de riscos para o capital, na categoria de sistemas de informação e no contexto do risco operacional.

Em segundo lugar, as Orientações descrevem com maior clareza as responsabilidades da direção de topo e da segunda e terceira linha de defesa na gestão da estratégia TIC e modelo de governo.

Em terceiro lugar, as Orientações fortalecem a recente estratégia do Banco de Portugal para o reforço da resiliência operacional em matéria de cibersegurança, complementando a Instrução n.º 1/2019[4] e a Instrução n.º 21/2019[5], que instituem deveres de reporte de incidentes operacionais e de segurança, e incidentes de cibersegurança, em Portugal.

Finalmente, as Orientações introduzem a possibilidade de as instituições realizarem testes de intrusão, com maior ou menor âmbito, intensidade e periodicidade, como forma de testar eventuais vulnerabilidades em sistemas e de aferir a eficácia e capacidade de resposta dos mecanismos de defesa.

A presente Instrução foi objeto de consulta pública nos termos e para os efeitos previstos nos artigos 100.º, n.º 3, alínea c) e artigo 101.º, ambos do Código do Procedimento Administrativo.

Neste contexto, o Banco de Portugal, no uso da competência que lhe é atribuída pelos artigos 14.º e 17.º da sua Lei Orgânica, aprovada pela Lei n.º 5/98, de 31 de janeiro, bem como pelos artigos 115.º-T e 116.º, al. f), do Regime Geral das Instituições de Crédito e Sociedades Financeiras e pelos artigos 70.º, n.º 3, 60.º, n.º 3 e 157.º, n.º 1 do RJSPME, aprova a seguinte Instrução:

[4] https://www.bportugal.pt/instrucao/12019
[5] https://www.bportugal.pt/instrucao/212019

Artigo 1.º
Destinatários

São destinatários da presente Instrução os prestadores de serviços de pagamento (doravante "PSP"), na aceção do artigo 11.º, n.º 1 do RJSPME, com sede em Portugal, ainda que operando em outros países por intermédio do exercício do direito de estabelecimento ou da livre prestação de serviços.

Artigo 2.º
Requisitos operacionais e de segurança

Os PSP observam os requisitos previstos nas Orientações relativas à gestão dos riscos associados às TIC e à segurança da Autoridade Bancária Europeia (EBA/GL/2019/04), na gestão dos riscos operacionais e de segurança relacionados com os serviços de pagamento por si prestados.

Artigo 3.º
Relatório anual de avaliação dos riscos operacionais e de segurança

1 – Os PSP elaboram, com referência a 30 de junho de cada ano, um relatório anual de avaliação dos riscos operacionais e de segurança dos serviços de pagamento prestados, de acordo com o modelo anexo à presente Instrução.

2 – O relatório referido no número anterior é reportado ao Banco de Portugal até 31 de julho do mesmo ano.

3 – O relatório anual de avaliação dos riscos visa recolher informação relevante sobre os riscos operacionais e de segurança dos serviços de pagamento, assegurando que os PSP controlam estes riscos e não estão expostos a um elevado número de incidentes operacionais e de segurança severos, bem como incidentes de cibersegurança significativos ou severos.

4 – Mediante autorização prévia solicitada ao Banco de Portugal, os destinatários da presente Instrução poderão delegar o reporte da informação noutra entidade do mesmo grupo, sem prejuízo de permanecerem responsáveis pela correção e atualização da informação reportada.

5 – Os PSP devem preencher o modelo de relatório que consta em "Reportes Ad-hoc via correspondência" na Área Temática de "Supervisão Prudencial" do Portal BP*net* (www.bportugal.net), cumprindo as instruções aí constantes e submetê-lo através desse portal.

Artigo 4.º
Entrada em vigor e disposição final

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

2 – O primeiro relatório anual de avaliação dos riscos operacionais e de segurança, referente a 30 de junho de 2021, deverá ser remetido ao Banco de Portugal até 31 de julho de 2021.