BANCO DE PORTUGAL
EUROSISTEMA

Carta Circular n.º CC/2020/00000029

Assunto: Orientações relativas à gestão dos riscos associados às TIC e à segurança

A 28 de novembro de 2019, a Autoridade Bancária Europeia (EBA, na sigla inglesa) publicou as "Orientações relativas à gestão dos riscos associados às TIC e à segurança" (EBA/GL/2019/04) (doravante "Orientações")[1].

Estas Orientações revogam e incorporam 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). Dadas as matérias em causa, as Orientações complementam as "Orientações relativas à avaliação do risco das TIC no âmbito do processo de revisão e avaliação pelo supervisor (SREP)" (EBA/GL/2017/05), que foram integradas pelo Banco de Portugal na sua avaliação do risco das tecnologias de informação e comunicação (TIC) no âmbito do SREP.

As Orientações são dirigidas aos prestadores de serviços de pagamento, instituições de crédito e empresas de investimento. Em termos gerais, especificam as medidas de gestão dos riscos que as instituições devem adotar para gerir os seus riscos associados às TIC e à segurança para todas as atividades, e, em particular, as medidas que os prestadores de serviços de pagamento devem tomar para gerir os riscos operacionais e de segurança relacionados com os serviços de pagamento por si prestados. As orientações incluem também requisitos destinados a mitigar os riscos de segurança associados a sistemas em regime de subcontratação e/ou expostos a incidentes de cibersegurança.

Dada a sua importância para o reforço da resiliência operacional do setor financeiro, o Banco de Portugal comunicou à EBA a sua intenção de cumprir com estas Orientações a partir de 30 de junho de 2020, o que implicará que os requisitos subjacentes sejam tomados em consideração no exercício da atividade de supervisão a partir dessa data.

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, vem transmitir a sua expectativa de que, em conformidade com o seu âmbito de aplicação, os requisitos previstos nas Orientações sejam observados a partir de 30 de junho de 2020, por: prestadores de serviços de pagamento, na aceção do artigo 4.º, n.º 11, da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015 (DSP2), e instituições de crédito e empresas de investimento, na aceção do artigo 4.º, n.º 1, ponto 3, do Regulamento (UE) n.º 575/2013, do Parlamento Europeu e do Conselho, de 26 de junho de 2013 (CRR).

Os requisitos previstos nas Orientações serão oportunamente objeto de regulamentação pelo Banco de Portugal.

[1] https://eba.europa.eu/eba-publishes-guidelines-ict-and-security-risk-management

Enviada a:
Instituições de Crédito; Instituições de Pagamento; Instituições de Moeda Eletrónica e Empresas de Investimento.