RELATÓRIO ANUAL DE RISCOS OPERACIONAIS E DE SEGURANÇA

(EBA/GL/2019/04, N.º3 E N.º 4 DO ART. 70.º DO RJSPME)

MANUAL DE INSTRUÇÕES

BANCO DE PORTUGAL
EUROSISTEMA

DSP • Departamento de Supervisão Prudencial

DATA DE CRIAÇÃO: 02-04-2020

DATA DA ÚLTIMA ATUALIZAÇÃO: 11-02-2021

Índice

1| Introdução

A Autoridade Bancária Europeia (EBA) emitiu, a 28 de novembro de 2019, as "Orientações relativas à gestão dos riscos associados às tecnologias de informação e comunicação (TIC) e à segurança" (EBA/GL/2019/04, doravante "Orientações").

As Orientações destinam-se a prestadores de serviços de pagamento (PSP) e definem um conjunto de requisitos para uma gestão adequada dos riscos associados às TIC e à segurança, incluindo riscos de subcontratação externa e de ocorrência de incidentes de cibersegurança.

Concretamente, as Orientações estabelecem no número 1.3.5. das Orientações (parágrafo 24), que remete para o disposto no n.º 2 do artigo 95.º da DSP2[1] (o qual foi transposto para a ordem jurídica nacional pelo n.º 3 do Artigo 70.º do RJSPME[2]), um dever de reporte anual ao Banco de Portugal, aplicável aos PSP, dos riscos operacionais e de segurança associados aos serviços de pagamento por si prestados.

A Instrução n.º 4/2021 visou implementar (i) as Orientações e (ii) o reporte de riscos operacionais e de segurança decorrente da DSP2, relativamente aos PSP.

Para facilitar o cumprimento deste requisito de reporte, o Banco de Portugal disponibiliza no Portal *BPnet*, na Área de Supervisão Prudencial, em "Reportes Ad-hoc", um modelo de relatório anual de avaliação dos riscos operacionais e de segurança. Todos os campos assinalados com um "*" deverão ser preenchidos pelas entidades visadas. O relatório final deverá ser remetido ao Banco de Portugal até ao último dia de julho de cada ano, com referência a junho, devendo os PSP proceder ao seu envio através do Portal BP*net*, na Área de Supervisão Prudencial, em "Reportes Ad-hoc". Ressalva-se que o Banco de Portugal poderá solicitar informação adicional às entidades visadas.

O presente documento sistematiza as regras de preenchimento do modelo de relatório anual de avaliação de riscos operacionais e de segurança.

[1] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro (Diretiva de Serviços de Pagamento revista, ou DSP2).
[2] Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei n.º 91/2018, de 12 de Novembro transpondo a Diretiva (UE) 2015/2366.

2| Modelo de reporte

O modelo de relatório visa recolher informação relevante sobre a avaliação geral dos riscos operacionais e de segurança, incluindo riscos de cibersegurança e os principais riscos associados aos serviços de pagamentos prestados (i.e., Top 5).

Em seguida, apresentam-se em detalhe as instruções de preenchimento.

2.1. Informação geral

A entidade visada deverá prestar a seguinte informação básica, de preenchimento obrigatório:

- **Contacto (Nome, Telefone, Email).**
- **Confirmação que a informação remetida no relatório é fidedigna e completa:** e*ste campo deve ser preenchido assinalando uma das seguintes opções disponíveis: Confirmo/Não confirmo.*
- **Data da última avaliação aos riscos operacionais e de segurança dos serviços de pagamento prestados:** *Data da última avaliação na caixa de texto, com o formato (dd/mm/aaaa).*

2.2. Avaliação

Esta secção requer que os PSP descrevam sucintamente a sua avaliação anual de riscos, em cumprimento do n.º 1.3.5 das Orientações EBA/GL/2019/04. Recorda-se que este ponto remete para o disposto no n.º 2 do artigo 95.º da DSP2, disposição igualmente prevista no RJSPME, nomeadamente no âmbito do disposto no n.º 3 do artigo 70.º, a qual estabelece o dever de reporte ao Banco de Portugal, por parte dos PSP, de 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 dos riscos e dos mecanismos de controlo implementados em resposta a esses

riscos. Nesse sentido, as respostas devem refletir, pelo menos, os requisitos estipulados nos pontos 17 a 23 das EBA/GL72019/04:

1. **Explicação, de forma detalhada, dos riscos operacionais e de segurança relacionados com os principais serviços prestados." (campo de preenchimento obrigatório).** *A resposta deve apresentar um grau de detalhe suficiente que permita ao supervisor analisar a avaliação dos riscos operacionais e de segurança, embora sem exceder as 3000 palavras. Se necessário, poderá ser anexada uma matriz de risco devidamente fundamentada.*
2. **Descrição, para cada risco supramencionado, das medidas de mitigação e os mecanismos de controlo existentes.** *Este campo deve ser preenchido, tendo em conta os requisitos definidos na EBA/GL/2019/04, em particular, deverá ser apresentado:*
    - *i) Descrição sucinta da metodologia utilizada para medir a eficácia e adequação das medidas de mitigação e controlo;*
    - *ii) Descrição sucinta de adequação e eficácia das medidas de mitigação e mecanismos de controlo.*

    Caso seja apresentada matriz de risco e/ou plano de ação para reduzir o risco residual, devem ser indicados os responsáveis pela implementação das medidas e mecanismos de controlo bem como respetivas datas de implementação. Este campo deve ser preenchido com um grau de detalhe suficiente que permita ao supervisor analisar a avaliação de riscos operacionais e de segurança, sem exceder as 3000 palavras.

3. **Informação detalhada sobre o grau de cumprimento atual do SWIFT Customer Security Controls Framework.** *Este campo deve conter, pelo menos, a seguinte informação:*
    - *i) Percentagem de cumprimento dos controlos obrigatórios e dos controlos recomendados definidos na SWIFT Customer Security Controls Framework;*
    - *ii) Data da última avaliação de conformidade com o programa;*
    - *iii) Principais pontos de atenção e medidas de melhoria em curso e/ou planeadas.*

4. **Indicação do número de incidentes operacionais e de segurança com serviços de pagamento desde o início do ano corrente, discriminando quantos destes incidentes constituem incidentes de cibersegurança. Indicação do número de incidentes operacionais e de segurança que são classificados como "de caráter severo" ao abrigo das Instruções do Banco de Portugal n.º 1/2019 e n.º 21/2019.** *Este campo deve ser preenchido com base no registo interno de incidentes operacionais e de segurança, o qual poderá ser anexado.*

2.3. Principais riscos (Top 5)

Devem ser listados os 5 principais riscos TIC e de segurança associados aos serviços de pagamento prestados:

- **Identificação dos principais riscos operacionais e de segurança.** *A resposta a esta questão deve ter em conta, pelo menos, os requisitos nos pontos 17 a 21 das EBA/GL/2019/04.*
- **Descrição do risco.** *A resposta a esta questão deve terem conta, pelo menos, os requisitos nos pontos 17 a 21 das EBA/GL/2019/04.*
- **Áreas de negócio, processos críticos e ativos de informação afetados.** *A resposta a esta questão deve terem conta, pelo menos, os requisitos no ponto 17 das EBA/GL/2019/04.*

De seguida, solicita-se que seja apresentada informação *específica* para cada um dos riscos identificados, designadamente:

A. Risco Inerente:

Probabilidade. *Indicação da probabilidade do risco se materializar, tendo em conta a metodologia interna adotada (Lista: baixa, média, alta).*

Impacto potencial. *Descrição do potencial impacto do risco materializado, tendo em conta a metodologia interna adotada (Lista: baixo, médio, alto).*

Classificação de risco. *Indicação do nível de risco atribuído, tendo em conta a metodologia interna adotada (Lista: elevado, médio, reduzido).*

B. Controlos de risco:

- **Controlos existentes.** *Descrição sobre as medidas de mitigação e controlo existentes.*

  Classificação do controlo. *Informação sobre o nível de adequação das medidas de mitigação e controlos para cada risco identificado (Lista: adequado, suficiente, insuficiente ou não adequado).*

C. Risco Residual

Classificação. *Atendendo aos controlos listados na coluna I, informação sobre a classificação de risco residual (Lista: elevado, médio, reduzido).*

D. Informação adicional

- **Responsável.** *Nome e o cargo da pessoa responsável por gerir o risco.*
- **Recorrência.** *Número de ocorrências, acompanhado de explicação sumária das mesmas, indicando se ocorreram antes ou depois da implementação dos controlos.*
- **Metodologia de classificação de risco.** *Descrição sucinta da metodologia interna de classificação de risco.*
- **Informação adicional.** *Informação adicional considerada relevante sobre o risco.*

3| Validação

O formato do modelo de relatório foi propositadamente bloqueado para não serem alterados, eliminados ou adicionados novos campos de informação. O modelo de reporte inclui também um separador de "Validação" que deverá ser consultado para garantir o preenchimento de todos os campos de carácter obrigatório antes da submissão no Portal BP*net*.