PROJETO DE NORMA REGULAMENTAR N.º […]/2024-R, DE […] DE […]

COMUNICAÇÃO DE INCIDENTES DE CARÁCTER SEVERO RELACIONADOS COM AS TIC

De acordo, respetivamente, com os artigos 63.º e seguintes do regime jurídico de acesso e exercício da atividade seguradora e resseguradora (RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, e 103.º e seguintes do regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões (RJFP), aprovado pela Lei n.º 27/2020, de 23 de julho, as empresas de seguros e de resseguros e as sociedades gestoras de fundos de pensões devem dispor de um sistema de governação eficaz, que garanta uma gestão sã e prudente das suas atividades.

No âmbito do sistema de governação, as referidas entidades devem implementar sistemas de gestão de riscos e de controlo interno eficazes, cujos requisitos se encontram previstos, respetivamente, nos artigos 72.º e 74.º do RJASR e nos artigos 118.º e 120.º do RJFP.

De entre os riscos que o sistema de gestão de riscos deve abranger – e onde a eficácia e eficiência do controlo interno se revela fundamental –, figura o risco operacional, que se refere ao risco de perdas resultantes da inadequação ou falha dos procedimentos internos, das pessoas ou sistemas, ou de eventos externos às entidades em apreço [cf. alínea *d)* do artigo 7.º do RJASR e alínea *b)* do n.º 4 do artigo 9.º da Norma Regulamentar n.º 8/2009-R, de 4 de junho, que estabelece os princípios gerais e regras relativos aos mecanismos de governação no âmbito dos fundos de pensões]. É nesta sede que se inserem os riscos de segurança das tecnologias de informação e comunicação (TIC).

Com efeito, a utilização crescente das TIC na prestação de serviços financeiros e no funcionamento operacional das entidades financeiras torna as respetivas atividades vulneráveis a incidentes operacionais e de segurança, incluindo ciberataques. Estas vulnerabilidades podem revelar-se sistémicas, dadas as interligações existentes entre as entidades financeiras e as interdependências dos seus sistemas de TIC, nomeadamente em relação a infraestruturas de terceiros e serviços prestados por terceiros.

Por outro lado, em virtude da rápida evolução e do potencial impacto dos riscos relacionados com as TIC, importa que as entidades financeiras prestem particular atenção à avaliação e gestão destes riscos.

No que respeita à gestão do risco operacional, prevê o n.º 2 do artigo 30.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, relativa ao sistema de governação das empresas de seguros e de resseguros, que o órgão de administração destas entidades deve assegurar a existência de processos para identificar, analisar e comunicar eventos de risco operacional.

Por sua vez, a Norma Regulamentar n.º 6/2022-R, de 7 de junho, que, tendo em consideração as Orientações da Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA) neste âmbito, estabelece os requisitos e princípios gerais que devem presidir ao desenvolvimento de mecanismos de governação e segurança das TIC, determina, no seu artigo 27.º: "*No caso de uma interrupção ou emergência, e durante a aplicação dos [Planos de Continuidade de Negócio], as empresas de seguros e de resseguros devem garantir que dispõem de medidas eficazes de comunicação de crises, de modo a que todas as partes interessadas relevantes, internas e externas, entre as quais a ASF, bem como os prestadores de serviços relevantes, sejam informados de forma atempada e adequada.*".

O estabelecimento de "*circuitos de transmissão de informação claros que garantem a transmissão rápida de informações a todas as pessoas que dela necessitam, de forma que lhes permita reconhecer a importância das respetivas responsabilidades*" configura, aliás, um requisito essencial em matéria de governação que as empresas de seguros e de resseguros devem cumprir [cf. alínea *k)* do n.º 1 do artigo 258.º do Regulamento Delegado (UE) 2015/35 da Comissão, de 10 de outubro de 2014, que completa a Diretiva 2009/138/CE, do Parlamento Europeu e do Conselho, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II)].

No que concerne às sociedades gestoras de fundos de pensões, para além dos requisitos relativos ao sistema de gestão de riscos previstos na Norma Regulamentar n.º 8/2009-R, de 4 de junho, a gestão do risco operacional (nomeadamente, através da definição de planos de contingência) é densificada na Circular n.º 1/2011, de 17 de março (que complementou aquela norma regulamentar). Ainda que estes normativos estejam em processo de revisão, os conteúdos dos mesmos integrarão a futura regulamentação do sistema de governação das sociedades gestoras de fundos de pensões.

Mais recentemente, no quadro da Diretiva (UE) 2016/2341, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2016, relativa às atividades e à supervisão das instituições de realização de planos de pensões profissionais (vulgarmente designada "IORP II"), transposta para a ordem jurídica nacional pela Lei n.º 27/2020, de 23 de julho, que aprovou o RJFP, a EIOPA emitiu o Parecer de 10 de julho de 2019 "*Opinion on the supervision of the management of operational risks faced by IORPs*".

Neste parecer, refere-se que as instituições de realização de planos de pensões profissionais (IORP) devem dispor de uma política relativa ao reporte de incidentes operacionais significativos às autoridades competentes. Mais se refere – em particular quanto aos riscos cibernéticos – a importância e necessidade de integrar estes riscos nos sistemas de gestão de riscos das IORP, através da respetiva identificação, mensuração, monitorização, gestão e reporte. É ainda referido que as autoridades competentes devem recolher informação sobre os riscos cibernéticos sistémicos e em evolução que possam afetar as IORP.

Cumpre também assinalar as Recomendações do Conselho Nacional de Supervisores Financeiros (CNSF) sobre Gestão da Continuidade de Negócio (revistas), divulgadas através da Circular n.º 5/2021, de 7 de outubro, nas quais se recomenda às instituições financeiras por estas abrangidas que disponham, para os casos de crise, de uma política de comunicação com todos os interessados, incluindo autoridades de supervisão.

No que respeita à comunicação com estas entidades, entende-se que "*é fundamental que as instituições financeiras reportem todos os custos e perdas decorrentes de disrupções e incidentes operacionais, assim como lhes prestem informação, com elevados níveis de tempestividade e exatidão, acerca da ocorrência de qualquer desastre, incidente ou interrupção de funcionamento, emergência grave, falha nas TIC, potencial ou efetiva violação das informações dos clientes e/ou de atividade ilegal. A comunicação imediata às autoridades de supervisão de um incidente grave relacionado com a suspensão ou atraso de operações informáticas, incidentes financeiros relacionados com a manipulação de dados ou programas informáticos, e de falhas no sistema de processamento de informação, permite acautelar um eventual risco sistémico.*" (cf. Recomendação 9 sobre a "Política de comunicação").

Relativamente aos mediadores de seguros, de resseguros e de seguros a título acessório, embora o regime jurídico da distribuição de seguros e de resseguros (RJDS), aprovado pela Lei n.º 7/2019, de 16 de janeiro, e demais regulamentação aplicável, não lhes imponha um quadro de gestão de

gestão de riscos semelhante ao previsto para as empresas de seguros e de resseguros e para as sociedades gestoras de fundos de pensões, verifica-se que também estas entidades estão expostas a riscos relacionados com as TIC, fruto da crescente digitalização da sua atividade e da utilização de serviços de TIC prestados por terceiros, encontrando-se, nesta medida, abrangidas pelo Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro (DORA), que entrou em vigor a 16 de janeiro de 2023.

É neste contexto que se justifica a comunicação à Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) de incidentes de carácter severo relacionados com as TIC e das medidas tomadas em resposta aos mesmos, estabelecendo a presente norma regulamentar os elementos de informação, o formato, o meio e os prazos dessa comunicação, ao abrigo do dever de prestação de informação que impende sobre as entidades por si supervisionadas e atendendo às respetivas responsabilidades de supervisão.

Adicionalmente, a previsão do presente regime tem como objetivo a devida preparação e a antecipação, de forma mitigada e gradual, dos requisitos estabelecidos neste âmbito pelo Regulamento DORA, e respetivos atos delegados e de execução (cuja elaboração e aprovação se encontra em curso a nível europeu).

Neste sentido, o presente normativo aplica-se às empresas de seguros e de resseguros com sede em Portugal, às sociedades gestoras de fundos de pensões autorizadas em Portugal e aos mediadores de seguros, de resseguros e de seguros a título acessório residentes ou com sede em Portugal, que não sejam microempresas ou pequenas ou médias empresas de acordo com os critérios previstos no Decreto-Lei n.º 372/2007, de 6 de novembro. Excecionam-se, contudo, deste âmbito os mediadores de seguros que também sejam instituições de crédito, por razões de proporcionalidade, nomeadamente porquanto estas entidades já se encontram atualmente sujeitas ao quadro regulatório em matéria de reporte de incidentes de cibersegurança aplicável ao setor bancário.

Com a aplicação dos requisitos previstos no Regulamento DORA e nos respetivos atos delegados e de execução a partir de 17 de janeiro de 2025, afigurar-se-á necessária a revisão desta norma

regulamentar, tendo em vista não apenas evitar sobreposições, mas também identificar os mecanismos de reporte que poderão ser utilizados no âmbito daquele quadro regulatório.

Note-se, por último, que a obrigação de comunicação à ASF ora prevista difere da obrigação de reporte de incidentes cibernéticos prevista nas Normas Regulamentares n.os 4/2023-R e 5/2023-R, de 11 de julho, nomeadamente quanto ao respetivo âmbito, momento da comunicação, natureza e finalidade da informação a prestar. Sem prejuízo, a comunicação de um incidente ao abrigo da presente norma regulamentar não preclude o cumprimento da obrigação de reporte prevista naquelas normas regulamentares, caso se trate de um incidente cibernético.

O projeto da presente norma regulamentar esteve em processo de consulta pública, nos termos do artigo 47.º dos Estatutos da ASF, aprovados pelo Decreto-Lei n.º 1/2015, de 6 de janeiro, tendo […].

Assim, a Autoridade de Supervisão de Seguros e Fundos de Pensões, ao abrigo do disposto no n.º 4 do artigo 81.º do regime jurídico de acesso e exercício da atividade seguradora e resseguradora (RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, no n.º 4 do artigo 150.º do regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões (RJFP), aprovado pela Lei n.º 27/2020, de 23 de julho, na alínea *a)* do n.º 1 e no n.º 2 do artigo 34.º, no artigo 36.º e no artigo 39.º do regime jurídico da distribuição de seguros e de resseguros (RJDS), aprovado pela Lei n.º 7/2019, de 16 de janeiro, bem como na alínea *a)* do n.º 3 do artigo 16.º dos seus Estatutos, emite a seguinte norma regulamentar:

Artigo 1.º

Objeto

A presente norma regulamentar tem por objeto regular a comunicação de incidentes de carácter severo relacionados com as tecnologias de informação e comunicação (TIC) pelas entidades sujeitas à supervisão da Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) previstas no artigo seguinte.

Artigo 2.º

Âmbito de aplicação

1 — A presente norma regulamentar aplica-se:

a) Às empresas de seguros e de resseguros com sede em Portugal;

b) Às sociedades gestoras de fundos de pensões autorizadas em Portugal;

c) Aos mediadores de seguros, de resseguros e de seguros a título acessório residentes ou com sede em Portugal, que não sejam microempresas ou pequenas ou médias empresas de acordo com os critérios previstos no Decreto-Lei n.º 372/2007, de 6 de novembro, com exceção dos mediadores de seguros que também sejam instituições de crédito.

2 — A aplicação da presente norma regulamentar às entidades referidas nas alíneas *a)* e *c)* do número anterior inclui o exercício da respetiva atividade através de sucursal ou em regime de livre prestação de serviços no território de outros Estados membros da União Europeia.

Artigo 3.º

Definições

Para efeitos da presente norma regulamentar, entende-se por:

a) «Cliente», o tomador de seguros, segurado, beneficiário ou terceiro lesado, no âmbito da atividade seguradora e de distribuição de seguros, bem como o associado, contribuinte, participante ou beneficiário, no âmbito da atividade de gestão de fundos de pensões e de distribuição no âmbito de fundos de pensões;

b) «Duração de um incidente», o tempo decorrido entre o momento em que o incidente ocorre, ou é detetado caso não seja possível identificar o momento da ocorrência, e o momento em que o incidente é resolvido;

c) «Função crítica ou importante», uma função cuja perturbação comprometeria significativamente o desempenho financeiro de uma entidade mencionada no n.º 1 do artigo anterior ou a solidez ou continuidade dos seus serviços e das suas atividades, ou a interrupção, anomalia ou falha dessa função comprometeria significativamente o contínuo cumprimento das

condições e obrigações decorrentes da respetiva autorização, ou das suas restantes obrigações legais ou regulamentares;

d) «Incidente relacionado com as TIC», uma ocorrência ou uma série de ocorrências conexas não previstas pelas entidades mencionadas no n.º 1 do artigo anterior que compromete a segurança dos sistemas de rede e de informação e têm um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou nos serviços prestados pelas entidades;

e) «Incidente de carácter severo relacionado com as TIC», um incidente relacionado com as TIC que cumpre os critérios previstos no artigo seguinte;

f) «Risco associado às TIC», qualquer circunstância razoavelmente identificável relacionada com a utilização de sistemas de rede e de informação que, caso se materialize, pode comprometer a segurança dos sistemas de rede e de informação, de qualquer instrumento ou processo dependente de tecnologia, do funcionamento e da execução de processos ou da prestação de serviços, causando efeitos adversos no ambiente digital ou físico;

g) «Serviço crítico», o serviço de TIC ou um sistema de rede e de informação que suporta funções críticas ou importantes das entidades mencionadas no artigo anterior;

h) «Serviço de TIC», o serviço digital e de dados prestado por meio de sistemas de TIC a um ou mais utilizadores internos ou externos, de forma contínua, incluindo equipamentos informáticos enquanto serviço e serviços de equipamento informático, o que inclui a prestação de apoio técnico através de atualizações de programas informáticos ou microprogramas pelo fornecedor de equipamentos informáticos, com exclusão dos serviços telefónicos analógicos tradicionais;

i) «Sistema de rede e de informação», um sistema de rede e de informação na aceção do ponto 1 do artigo 6.º da Diretiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022;

j) «Tempo de indisponibilidade do serviço», o tempo decorrido entre o momento em que o serviço se encontra, totalmente ou parcialmente, indisponível e o momento em que o serviço é restaurado ao nível prestado antes do incidente.

Artigo 4.º

Classificação de incidentes relacionados com as TIC

1 — As entidades previstas no n.º 1 do artigo 2.º classificam um incidente relacionado com as TIC como severo de acordo com os seguintes critérios:

a) Existe um acesso doloso, não autorizado e efetivo às redes e sistemas de informação da entidade; ou

b) O incidente afeta serviços críticos da entidade e, cumulativamente, verificam-se duas ou mais das seguintes situações:

i) O número de clientes afetados pelo incidente é superior a 10% do total de clientes que utilizam o serviço afetado ou é superior a cem mil clientes;

ii) A duração do incidente é superior a 24 horas ou o tempo de indisponibilidade do serviço crítico é superior a duas horas;

iii) O incidente afeta a disponibilidade, autenticidade, integridade ou confidencialidade dos dados, com impacto ou potencial impacto negativo na implementação dos objetivos de negócio ou no cumprimento de exigências regulatórias;

iv) O incidente tem impacto económico, nomeadamente quando os custos e as perdas diretos e indiretos incorridos pela entidade devido ao incidente excedam ou são suscetíveis de exceder os cem mil euros, excluindo eventuais montantes recuperáveis;

v) O incidente tem impacto reputacional, nos termos previstos nos n.os 3 e 4.

2 — Para efeitos das subalíneas *i), ii)* e *iv)* da alínea *b)* do número anterior, quando não seja possível calcular com precisão os critérios aí referidos, as entidades devem ter em conta estimativas com base na informação disponível.

3 — Para efeitos da subalínea *v)* da alínea *b)* do n.º 1, considera-se que o incidente tem impacto reputacional quando pelo menos uma das seguintes situações se verifica:

a) O incidente é noticiado nos meios de comunicação social;

b) O incidente deu origem a múltiplas reclamações de diferentes clientes relativamente a serviços prestados a clientes ou a relações comerciais críticas;

c) A entidade, em resultado do incidente, não consegue dar cumprimento ou é suscetível de não dar cumprimento a exigências regulatórias;

d) A entidade, em resultado do incidente, é ou poderá ser suscetível a uma perda de clientes com um impacto material na sua atividade.

4 — Na avaliação do impacto de um incidente em termos reputacionais, as entidades devem tomar em consideração o nível de visibilidade que o incidente adquiriu ou é suscetível de adquirir relativamente a cada um dos critérios referidos no número anterior.

Artigo 5.º

Comunicação de incidentes de carácter severo relacionados com as TIC

1 — As entidades previstas no n.º 1 do artigo 2.º comunicam à ASF, nos prazos definidos no artigo seguinte, incidentes de carácter severo relacionado com as TIC, através da apresentação dos seguintes elementos:

a) Notificação inicial;

b) Relatório intercalar;

c) Relatório final.

2 — As entidades previstas no n.º 1 do artigo 2.º devem assegurar que a informação prestada é completa e rigorosa e, quando tal não seja possível nos casos das alíneas *a)* e *b)* do número anterior, que são apresentados valores estimados com base na informação disponível.

3 — Quando apresentarem o relatório intercalar ou final, as entidades previstas no n.º 1 do artigo 2.º devem atualizar, sempre que possível, a informação prestada anteriormente.

4 — Quando, após reavaliação, concluam que o incidente comunicado nunca cumpriu os critérios de classificação previstos no artigo anterior, as entidades previstas no n.º 1 do artigo 2.º devem apenas enviar à ASF um relatório final com a informação relacionada com a reclassificação do incidente como não severo.

5 — Sem prejuízo da manutenção da responsabilidade das entidades previstas no n.º 1 do artigo 2.º, a comunicação de incidentes nos termos do presente artigo pode ser subcontratada a um

terceiro prestador de serviços, em conformidade com o regime aplicável em matéria de subcontratação.

6 — Deve ser designado pelo órgão de administração das entidades previstas no n.º 1 do artigo 2.º um responsável pela comunicação de incidentes de carácter severo relacionados com as TIC, que, no caso das entidades referidas nas alíneas *a)* e *b)* daquela disposição, pode ser o responsável pela função de segurança da informação.

7 — O responsável a que se refere o número anterior deve, juntamente com a comunicação prevista na alínea *a)* do n.º 1, tomar conhecimento da informação relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação.

Artigo 6.º

Prazos

1 — A notificação inicial a que se refere a alínea *a)* do n.º 1 do artigo anterior deve ser apresentada à ASF no prazo de quatro horas desde o momento em que o incidente é classificado como severo ou, no máximo, no prazo de 24 horas desde o momento em que o incidente é detetado.

2 — O relatório intercalar a que se refere a alínea *b)* do n.º 1 do artigo anterior deve ser apresentado à ASF no prazo de 72 horas desde o momento em que o incidente é classificado como severo ou assim que a entidade recuperar as suas atividades e voltar a operar normalmente.

3 — O relatório final a que se refere a alínea *c)* do n.º 1 do artigo anterior deve ser apresentado à ASF no prazo de um mês desde o momento em que o incidente é classificado como severo ou no dia seguinte ao incidente ter sido dado como resolvido de forma permanente.

Artigo 7.º

Meio de comunicação

1 — Os elementos de informação referidos no n.º 1 do artigo 5.º são enviados à ASF através do preenchimento de formulários próprios, constantes da seguinte plataforma dedicada para o efeito: [*em preparação*].

2 — Os formulários referidos no número anterior, bem como as alterações aos mesmos, são disponibilizados no sítio da ASF na Internet, após aprovação pelo Conselho de Administração desta Autoridade.

Artigo 8.º

Início de vigência

A presente norma regulamentar entra em vigor no dia imediato ao da sua publicação.

Em

O CONSELHO DE ADMINISTRAÇÃO