AUTORIDADE DE SUPERVISÃO
DE SEGUROS E FUNDOS DE PENSÕES

DOCUMENTO DE CONSULTA PÚBLICA

N.º 6/2024

Projeto de norma regulamentar relativa à comunicação de incidentes de carácter severo relacionados com as TIC

5 de junho de 2024

1. ENQUADRAMENTO

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.

Assim, a ASF elaborou o projeto de norma regulamentar que ora se submete a consulta pública.

2. PROJETO DE NORMA REGULAMENTAR E AVALIAÇÃO DE IMPACTO

A) Descrição do conteúdo da norma regulamentar

2.1. O projeto de norma regulamentar tem por objeto regular a comunicação de incidentes de carácter severo relacionados com as TIC pelas entidades sujeitas à supervisão da ASF (cf. artigo 1.º), através do estabelecimento dos elementos de informação, do formato, do 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.

2.2. No n.º 1 do artigo 2.º do projeto de norma regulamentar delimita-se o respetivo âmbito subjetivo de aplicação, prevendo-se como destinatários:

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

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

c) Os 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.

Conforme já referido, esta exclusão está relacionada com razões de proporcionalidade, tendo-se atendido, nomeadamente, ao facto de as entidades em causa já se encontrarem atualmente sujeitas ao quadro regulatório em matéria de reporte de incidentes de cibersegurança aplicável ao setor bancário.

Clarifica-se ainda que a aplicação da presente norma regulamentar às entidades referidas nas alíneas *a)* e *c) supra* 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 (cf. n.º 2 do artigo 2.º do projeto de norma regulamentar).

Conforme acima referido, o presente projeto de norma regulamentar tem também como objetivo a preparação e a antecipação, de forma mitigada e gradual, dos requisitos estabelecidos pelo Regulamento DORA, e respetivos atos delegados e de execução, em matéria de comunicação de incidentes de carácter severo relacionados com as TIC.

Foi tido, como referência, o tipo de entidades financeiras abrangidas pelo Regulamento DORA que são supervisionadas pela ASF [cf. alíneas *n)* a *p)* do n.º 1 e alínea *e)* do n.º 3 do artigo 2.º], desconsiderando-se, contudo, as isenções relativas às empresas de seguros e de resseguros a que se refere o artigo 4.º da Diretiva Solvência II e às entidades gestoras responsáveis pela gestão de planos

de pensões profissionais que, no seu conjunto, tenham menos de 15 participantes [cf. alíneas *b)* e *c)* do n.º 3 do artigo 2.º], porquanto a ASF entende adequada a aplicação do presente regime a estas entidades, bem como às entidades gestoras de fundos de pensões relativamente à atividade de gestão de fundos de pensões abertos de adesão individual, em linha com a opção regulatória tomada quanto à transposição e correspondente aplicação, na ordem jurídica nacional, dos regimes previstos nas Diretivas Solvência II e IORP II.

Questão 1: *Concorda com o âmbito subjetivo do projeto de norma regulamentar?*

2.3. O artigo 3.º prevê um conjunto de definições consideradas relevantes para a aplicação do projeto de norma regulamentar.

Para além de terem sido consideradas algumas definições previstas no Regulamento DORA (cf. n.os 2, 5, 8, 10, 21 e 22 do seu artigo 3.º), para facilitar a aplicabilidade do projeto de norma regulamentar, atendeu-se igualmente ao disposto no projeto de normas técnicas de regulamentação relativo aos critérios de classificação de incidentes relacionados com as TIC elaborado pelas Autoridades Europeias de Supervisão (AES) ao abrigo daquele regulamento[1].

Questão 2: *Concorda e considera adequado o conjunto de definições previsto no projeto de norma regulamentar ou entende que facilitaria a sua aplicabilidade o aditamento de outras definições? No último caso, quais?*

2.4. No artigo 4.º do projeto de norma regulamentar, preveem-se os critérios de classificação de incidentes relacionados com as TIC, tendo em conta os critérios definidos no n.º 1 do artigo 18.º do Regulamento DORA e especificados no projeto de normas técnicas de regulamentação acima referido, bem como os limiares de materialidade aí estabelecidos.

Assim, para efeitos da classificação como severo de um incidente relacionado com as TIC – que determinará, por sua vez, a respetiva comunicação à ASF – as entidades deverão avaliar, desde logo,

se existe um acesso doloso, não autorizado e efetivo às respetivas redes e sistemas de informação [cf. alínea *a)* do n.º 1 do artigo 4.º do projeto de norma regulamentar].

Caso não exista, as entidades deverão avaliar se o incidente afeta serviços críticos da mesma e se, cumulativamente, se verificam duas ou mais das seguintes situações [cf. alínea *b)* do n.º 1 do artigo 4.º do projeto de norma regulamentar]:

a) 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;

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

c) 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;

d) 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;

e) O incidente tem impacto reputacional, nos termos previstos nos n.os 3 e 4 do artigo 4.º do projeto de norma regulamentar.

Quando não seja possível calcular com precisão os critérios referidos nas alíneas *a)*, *b)* e *d)*, as entidades devem ter em conta estimativas com base na informação disponível (cf. n.º 2 do artigo 4.º do projeto de norma regulamentar).

Note-se que, tendo o presente projeto de norma regulamentar como objetivo a antecipação dos requisitos estabelecidos pelo Regulamento DORA – neste caso, também do projeto de normas técnicas de regulamentação relativo aos critérios de classificação de incidentes relacionados com as TIC –, procurou-se estabelecer e especificar, de forma mais simplificada, os critérios de classificação e limiares de materialidade ali previstos (exceto no que se refere à distribuição geográfica, não contemplado nesta iniciativa regulatória), considerando-se, neste âmbito, os elementos que a ASF reputa como essenciais e prioritários para um adequado processo de preparação para a aplicação dos

[1] A versão mais atualizada deste projeto de normas técnicas de regulamentação correspondente à adotada pela Comissão Europeia, por meio de ato delegado, a 13 de março de 2024, disponível em https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en.

requisitos em apreço. Adicionalmente, optou-se por não incluir no projeto de norma regulamentar a comunicação de ciberameaças significativas.

Questão 3: *Concorda e considera adequado o conjunto de critérios de classificação previsto no projeto de norma regulamentar ou entende que facilitaria a sua aplicabilidade o aditamento de outros elementos? No último caso, quais?*

2.5. No artigo 5.º do projeto de norma regulamentar, estabelecem-se os elementos que as entidades devem comunicar à ASF em caso de incidente de carácter severo relacionado com as TIC. Em conformidade com o n.º 4 do artigo 19.º do Regulamento DORA, as entidades devem apresentar à ASF uma notificação inicial, um relatório intercalar e um relatório final (cf. n.º 1 do artigo 5.º).

Para o efeito, as entidades devem prestar informação completa e rigorosa, ou valores estimados quando tal não seja possível aquando da notificação inicial ou do relatório intercalar, bem como atualizar, sempre que possível, a informação prestada na notificação inicial ou no relatório intercalar quando apresentarem, respetivamente, o relatório intercalar ou o relatório final (cf. n.os 2 e 3 do artigo 5.º do projeto de norma regulamentar).

Quando, após reavaliação, concluam que o incidente comunicado nunca cumpriu os critérios de classificação acima referidos, as entidades devem apenas enviar à ASF um relatório final com a informação relacionada com a reclassificação do incidente como não severo (cf. n.º 4 do artigo 5.º do projeto de norma regulamentar).

Sem prejuízo da manutenção da respetiva responsabilidade, confere-se às entidades a possibilidade de subcontratar a comunicação de incidentes, em conformidade com o regime aplicável em matéria de subcontratação (cf. n.º 5 do artigo 5.º do projeto de norma regulamentar).

O órgão de administração das entidades abrangidas pelo projeto de norma regulamentar deve designar um responsável pela comunicação de incidentes de carácter severo relacionados com as TIC. No caso das empresas de seguros e de resseguros e das sociedades gestoras de fundos de pensões,

esta tarefa pode ser cometida ao responsável pela função de segurança da informação[2] (cf. n.º 6 do artigo 5.º do projeto de norma regulamentar).

Este responsável deve ainda, juntamente com a notificação inicial, tomar conhecimento da informação relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação (cf. n.º 7 do artigo 5.º do projeto de norma regulamentar).

Questão 4: *Concorda e considera adequado o conjunto de elementos a comunicar à ASF em caso de incidente de carácter severo relacionado com as TIC?*

Questão 5: *Concorda e considera adequado o cometimento da comunicação de incidentes de carácter severo relacionados com as TIC a um responsável designado pelo órgão de administração?*

2.6. O artigo 6.º do projeto de norma regulamentar estabelece os prazos de apresentação dos elementos que devem ser comunicados à ASF em caso de incidente de carácter severo relacionado com as TIC.

Assim, a notificação inicial 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 (cf. n.º 1 do artigo 6.º do projeto de norma regulamentar).

Seguidamente, o relatório intercalar 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 (cf. n.º 2 do artigo 6.º do projeto de norma regulamentar).

Por fim, o relatório final 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 (cf. n.º 3 do artigo 6.º do projeto de norma regulamentar).

De igual modo, procurou-se também neste âmbito antecipar, de forma mais simplificada, os requisitos previstos no n.º 4 do artigo 19.º do Regulamento DORA e o disposto no projeto de normas

[2] Prevista no artigo 9.º da Norma Regulamentar n.º 6/2022-R, de 7 de junho, e no artigo 9.º do projeto de norma regulamentar relativa à segurança e governação das tecnologias da informação e comunicação (TIC) e à subcontratação a prestadores de serviços de computação em nuvem no âmbito da gestão de fundos de pensões (cf. Consulta Pública n.º 5/2024 da ASF, disponível em https://www.asf.com.pt/w/consulta-publica-n5-2024).

técnicas de regulamentação elaborado pelas AES ao abrigo daquele regulamento, no qual se determinam os prazos para a notificação inicial e para os relatórios intercalar e final[3].

Questão 6: *Concorda e considera adequados os prazos de comunicação à ASF da notificação inicial, do relatório intercalar e do relatório final?*

2.7. Por sua vez, o artigo 7.º do projeto de norma regulamentar estabelece o meio de comunicação da notificação inicial, do relatório intercalar e do relatório final em caso de incidentes de carácter severo relacionados com as TIC.

Estes elementos de informação devem, assim, ser enviados à ASF através do preenchimento de formulários próprios, que irão constar, por razões de segurança da informação, de uma plataforma informática dedicada para o efeito, a qual se encontra em preparação na ASF (cf. n.º 1 do artigo 7.º do projeto de norma regulamentar).

Na elaboração destes formulários, a ASF teve em conta o projeto de norma técnicas de execução que estabelece os formulários, os modelos e os procedimentos normalizados para a notificação de incidentes de carácter severo relacionados com as TIC elaborado pelas AES ao abrigo do Regulamento DORA[4]. Neste âmbito, tendo por referência os critérios de classificação previstos no projeto de norma regulamentar, foram considerados os campos de informação que a ASF entende como fundamentais para a cabal compreensão do incidente de carácter severo relacionado com as TIC e para a adequada preparação das entidades para o reporte desta informação a partir da data de produção de efeitos do Regulamento DORA.

---

[3] Submetido a consulta pública entre 8 de dezembro de 2023 e 4 de março de 2024 e acessível em https://www.eiopa.europa.eu/consultations/dora-public-consultation-second-batch-policy-products_en. Não se tratando da versão final deste ato jurídico, ressalvam-se eventuais alterações aos requisitos aí previstos decorrentes do procedimento de consulta pública.

[4] Submetido igualmente a consulta pública entre 8 de dezembro de 2023 e 4 de março de 2024 e acessível em https://www.eiopa.europa.eu/consultations/dora-public-consultation-second-batch-policy-products_en. Não se tratando da versão final deste ato jurídico, ressalvam-se eventuais alterações aos requisitos aí previstos decorrentes do procedimento de consulta pública.

Em linha com a nova metodologia adotada na regulamentação do reporte (cf. Normas Regulamentares n.os 4/2023-R e 5/2023-R, de 11 de julho), estabelece-se a disponibilização dos referidos formulários e das respetivas alterações em local dedicado no sítio da ASF na Internet, após aprovação pelo Conselho de Administração desta Autoridade (cf. n.º 1 do artigo 7.º do projeto de norma regulamentar).

Questão 7: *Concorda e considerado adequado o conteúdo dos formulários respeitantes à notificação inicial e aos relatórios intercalar e final?*

2.8. Por último, o artigo 8.º do projeto de norma regulamentar determina o respetivo início de vigência.

B) Avaliação do impacto da norma regulamentar

Na ponderação do impacto desta intervenção normativa importa reconhecer que o respetivo cumprimento acarreta custos adicionais para as entidades abrangidas pelo projeto de norma regulamentar, associados à implementação dos requisitos relativos à comunicação à ASF de incidentes de carácter severo relacionados com as TIC.

Assim, antevê-se a necessidade de desenvolvimento do sistema de gestão de riscos, em particular, dos riscos operacionais, que deve incluir a gestão de incidentes relacionados com as TIC, nomeadamente no que se refere à deteção, rastreamento, classificação, gestão, resposta e reporte de informação sobre estes incidentes pelas entidades supervisionadas.

Não obstante, importa ter em conta que a avaliação e gestão dos riscos relacionados com as TIC e notificação de incidentes desta natureza já deve ser contemplada pelas empresas de seguros e de resseguros e pelas sociedades gestoras de fundos de pensões, atendendo ao quadro legal, regulamentar e de *soft law* vigente em matéria de gestão de riscos operacionais e à especial acuidade que a mesma merece no contexto atual de crescente digitalização e utilização de serviços de TIC de terceiros, realidade que também afeta os mediadores de seguros, de resseguros e de seguros a título acessório.

Por outro lado, a ASF pretende alertar as entidades por si supervisionadas para os requisitos relativos à comunicação de incidentes relacionados com as TIC previstos no Regulamento DORA, e

respetivos atos delegados e de execução, que lhes serão aplicáveis a partir de 17 de janeiro de 2025. Com efeito, a presente iniciativa regulamentar visa preparar as entidades abrangidas para a conformidade com os referidos requisitos, antecipando a respetiva aplicação de forma gradual, mitigada e mais simplificada, o que irá permitir desenvolver, testar e identificar melhorias no processo de gestão de incidentes de carácter severo relacionados com as TIC, em especial quanto à respetiva classificação e reporte à autoridade de supervisão.

Adicionalmente, cumpre notar que, na previsão do presente regime, foram considerados critérios de proporcionalidade, uma vez que, conforme acima referido, quer no que respeita aos critérios de classificação, quer no que concerne aos prazos e ao conteúdo dos formulários para apresentação da notificação inicial e dos relatórios intercalar e final, a ASF procurou atender aos requisitos que se revelam essenciais e prioritários para esta fase preparatória de implementação do Regulamento DORA (e respetivos atos delegados e de execução) e para a cabal compreensão dos incidentes de carácter severo relacionado com as TIC que eventualmente ocorram neste período.

Neste sentido, a ASF considera que o regime previsto no presente projeto de norma regulamentar se afigura pertinente e útil para a promoção da gestão de incidentes relacionados com as TIC e, nessa medida, para a adequada implementação do Regulamento DORA e respetivos atos delegados e de execução, assim como para que esta Autoridade possa exercer cabalmente as atribuições e competências que lhe estão legalmente cometidas e que serão reforçadas a partir da data de produção de efeitos daqueles diplomas, designadamente ao nível da supervisão da resiliência operacional digital das entidades supervisionadas.

3. PEDIDO DE COMENTÁRIOS

Solicita-se aos interessados que submetam os seus comentários sobre o projeto de norma regulamentar, relativos às matérias versadas nas questões concretamente colocadas, ou sobre quaisquer outras matérias, por escrito, até ao dia 1 de julho de 2024, para o endereço de correio eletrónico consultaspublicas@asf.com.pt, nos termos da tabela anexa.

Atendendo a razões de transparência, a ASF propõe-se publicar no seu sítio na Internet os contributos recebidos ao abrigo desta consulta pública. Assim, caso o respondente se oponha à referida publicação, integral ou parcial, deve referi-lo expressamente no contributo que enviar, indicando quais os excertos do seu contributo cuja publicação não autoriza.

Por razões de equidade, os contributos recebidos após o final do prazo da consulta pública não serão considerados.

Os dados pessoais recebidos neste âmbito serão tratados exclusivamente para a presente finalidade e em conformidade com o RGPD.

Pessoa/Entidade: _____
Assinalar caso se oponha à publicação dos contributos: ☐

TABELA DE COMENTÁRIOS **Projeto de norma regulamentar relativa à comunicação de incidentes de carácter severo relacionados com as TIC**		
<u>Indicações:</u> **Na coluna "Questão/Artigo", indicar a questão referida no documento de consulta pública ou o artigo (incluindo o número e a alínea, caso aplicável) do projeto de norma regulamentar relativa à comunicação de incidentes de carácter severo relacionados com as TIC;** **Na coluna "Resposta/Comentário", indicar a resposta à questão referida no documento de consulta pública ou o comentário à disposição do projeto de norma regulamentar relativa à comunicação de incidentes de carácter severo relacionados com as TIC, incluindo qualquer proposta de redação alternativa;** **Cada resposta/comentário/proposta de redação alternativa deve reportar-se a uma questão ou artigo/número/alínea específicos;** **Em cada resposta/comentário/proposta de redação alternativa deve ser apresentada uma justificação para o seu acolhimento, podendo ainda ser acrescentadas outras observações.** **A coluna "Resolução" corresponde à resolução de cada resposta/comentário/proposta de redação alternativa ou observação e será preenchida pela ASF.**		
Questão/Artigo	**Resposta/Comentário**	**Resolução**