RELATÓRIO DA CONSULTA PÚBLICA

N.º 6/2024

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

26 de setembro de 2024

A — INTRODUÇÃO E 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 *h)* do n.º 2 do artigo 25.º da Norma Regulamentar n.º 6/2024-R, de 20 de agosto]. 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, e da Norma Regulamentar n.º 6/2024-R, de 20 de agosto, relativas, respetivamente, ao sistema de governação das empresas de seguros e de resseguros e das entidades gestoras de fundos de pensões, que o órgão de administração destas entidades deve assegurar a

existência de processos para identificar, analisar e comunicar eventos de risco operacional. Acrescenta ainda a parte final do n.º 2 do artigo 30.º da Norma Regulamentar n.º 6/2024-R, de 20 de agosto, que os referidos processos devem incluir o reporte à ASF de incidentes operacionais significativos, de acordo com a legislação e regulamentação aplicável neste âmbito.

Por sua vez, a Norma Regulamentar n.º 6/2022-R, de 7 de junho, e a Norma Regulamentar n.º 7/2024-R, de 20 de agosto, 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, determinam, no seu artigo 27.º que no caso de uma interrupção ou emergência, e durante a aplicação dos Planos de Continuidade de Negócio, as empresas de seguros e de resseguros e as sociedades gestoras de fundos de pensões "*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, 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 – 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 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 de norma regulamentar foi submetido a um processo de consulta pública, que decorreu entre os dias 7 de junho e 1 de julho de 2024, tendo sido recebidas duas respostas, publicadas em anexo, em virtude de os respondentes não se terem oposto à publicação dos respetivos contributos, conforme previsto no Ponto 3. do Documento de Consulta Pública n.º 6/2024.

A ASF agradece o envolvimento dos interessados no processo de consulta pública.

B — SÍNTESE DAS QUESTÕES SUSCITADAS E DOS FUNDAMENTOS PARA A DECISÃO DA ASF QUANTO AO RESPETIVO ACOLHIMENTO

De acordo com a metodologia aplicável às consultas públicas da ASF, propôs-se a utilização de uma tabela de comentários destinada a facilitar a formulação de comentários sobre as matérias vertidas no projeto sob consulta, nos termos previstos no Ponto 3. do Documento de Consulta Pública.

Assim, apresenta-se em anexo a referida tabela com a consolidação de todos os comentários suscitados nas respostas à consulta pública, bem como os fundamentos para o seu acolhimento / acolhimento parcial / não acolhimento na versão final da Norma Regulamentar n.º 9/2024-R, de 26 de setembro.

Por último, aproveitou-se o presente ensejo normativo para proceder a alguns ajustamentos formais, tendo em conta o Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de carácter severo, bem como tendo em consideração a recente aprovação das Normas Regulamentares n.os 6/2024-R e 7/2024-R, de 20 de agosto.

Pessoa/Entidade: **APS – Associação Portuguesa de Seguradores**
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

Indicações:

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
Questão 1 "Concorda com o âmbito subjetivo do projeto de norma regulamentar?"	Sim, embora com dúvidas em relação à inclusão do exercício da atividade através de sucursal ou em regime de livre prestação de serviços (LPS) no território de outros Estados membros da União Europeia. Tal inclusão poderá conduzir à sobreposição de comunicações de incidentes, caso as sucursais ou LPS tenham obrigações semelhantes nos territórios de outros Estados membros.	A ASF tomou devida nota do presente comentário. Atendendo à natureza prudencial da matéria relativa à gestão de riscos associados às TIC, bem como à provável utilização dos mesmos serviços de TIC que são prestados à sede, afigura-se adequada a inclusão no presente dever de comunicação

		à ASF do exercício da atividade seguradora e de mediação através de sucursal ou em regime de livre prestação de serviços (LPS) no território de outros Estados membros da União Europeia.
Artigo 2.º, n.º 1, alínea *c)*	A norma reconhece as especificidades das micro e pequenas empresas ao estabelecer exceções proporcionais aos seus recursos e perfil de risco. Sugere-se a avaliação da possibilidade de segmentar as entidades com base em critérios mais abrangentes, como porte, tipologia, faturação e histórico de incidentes cibernéticos, permitindo uma modulação mais precisa dos requisitos da norma. Com efeito, embora alinhado com o DORA, este enfatiza a necessidade de uma abordagem proporcional, considerando os requisitos atrás mencionados para cada entidade.	**Não acolhido.** Em primeiro lugar, nota-se que o quadro regulatório vigente em matéria de gestão de riscos, em particular do risco operacional, se aplica, de forma transversal, a todas as empresas de seguros e de resseguros e entidades gestoras de fundos de pensões. Por outro lado, conforme referido no documento de consulta pública e no preâmbulo da norma regulamentar, esta tem também como objetivo a devida preparação e a antecipação dos requisitos estabelecidos neste âmbito pelo Regulamento DORA e respetivos atos delegados e de execução, de forma gradual, mitigada e mais simplificada, alertando, assim, as entidades por si supervisionadas para a necessidade de cumprimento dos referidos requisitos a partir de 17 de janeiro de 2025. Assim, não se afigura que a presente proposta acautele este objetivo.

		A este propósito, procedeu-se ao ajustamento da redação da alínea *c)* do n.º 1 do artigo 2.º da norma regulamentar, de forma a promover um alinhamento mais adequado com o Regulamento DORA.
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?"	De uma forma genérica concorda-se com o elenco de definições constante da norma regulamentar, ainda que não exaustivo, parecendo-nos adequado ao propósito da mesma, merecendo, contudo, as seguintes notas. O artigo 78.º da Lei 147/2015 define como funções ou atividades operacionais fundamentais ou importantes (*critical or important functions or activities*) aquelas de que resulte: a) Um prejuízo significativo para a qualidade do sistema de governação; b) Um aumento indevido do risco operacional; c) Um prejuízo para a capacidade da ASF de verificar se a empresa de seguros ou de resseguros cumpre as suas obrigações; d) Um prejuízo para a continuidade ou qualidade dos serviços prestados aos tomadores de seguros, segurados e beneficiários. Por sua vez o artigo 71.º da NR 4/2022, de 16/4, prevê como funções e atividades operacionais fundamentais ou importantes as que impossibilitem a empresa de: a) Cumprir, em permanência, as condições de acesso à atividade seguradora ou resseguradora; b) Cumprir, em permanência, o quadro regulatório aplicável em caso de incumprimento por parte do prestador de serviços; c) Assegurar a estabilidade, continuidade e qualidade dos serviços prestados aos tomadores de seguros, segurados e beneficiários. Entendemos que deve haver harmonização do conceito. Apresentamos ainda as seguintes sugestões: - Definição "Duração de um incidente" - detalhar as diferentes etapas. O conceito de início de incidente é claro, no entanto, o final do mesmo, na forma como está	**Acolhido parcialmente.** Em primeiro lugar, cumpre notar que o disposto no artigo 78.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, não corresponde a uma definição de funções ou atividades operacionais fundamentais ou importantes, mas antes a um conjunto de condições que devem ser asseguradas para que possa ser efetuada a subcontratação das referidas funções ou atividade. O n.º 1 do artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, por sua vez, prevê um conjunto de elementos definidores de uma função ou atividade fundamental ou importante. Sem prejuízo, para efeitos de aplicação da presente norma regulamentar, deve atender-se ao disposto na alínea *c)* do artigo 3.º, que teve por base o disposto no

	descrito, pode levar a diferentes interpretações. Após a ocorrência do incidente, ocorre a sua contenção, depois a mitigação e finalmente a resolução efetiva (eliminação da causa raiz). É importante clarificar a que se refere exatamente "o momento em que o incidente é resolvido", dado que as organizações podem optar apenas pela mitigação e aceitação do risco remanescente ao invés da eliminação total da causa raiz. - Definição "Incidente relacionado com as TIC" - apresenta o conceito de autenticidade dos dados e é importante definir mais aprofundadamente. Os conceitos, confidencialidade, disponibilidade e integridade são amplamente conhecidos no contexto da cibersegurança, no entanto o de autenticidade pode já fazer parte destes. Assim, sugeria-se que fosse reavaliado a sua inclusão ou em alternativa ser clarificado para evitar interpretações heterogéneas. - A designação de "serviço crítico" pode gerar confusão com a designação da função crítica ou importante. Sugere-se a revisão da terminologia. Especialmente relevante para efeitos de divulgação no SFCR em que se pretende a indicação das funções críticas ou importantes e não dos serviços críticos numa perspetiva de TIC. - Definição "serviço de TIC" mereceria uma explicitação mais concretizada do que a constante do Regulamento DORA, *v.g.* quanto ao sentido e alcance de "*equipamentos informáticos enquanto serviço e serviços de equipamento informático*".	Regulamento DORA, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos naquele regulamento, razão pela qual não se optou por remeter, na norma regulamentar, para o n.º 1 do artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril. Nota-se que o regime previsto no Regulamento DORA é aplicável aos vários subsetores do setor financeiro, não sendo possível, nessa medida, prever definições que sejam totalmente condizentes com a legislação setorial. Relativamente à definição de "Duração de um incidente", não se afigura, contudo, necessário proceder à alteração da definição, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. No entanto, esclarece-se, tendo em conta os n.os 1 e 2 do artigo 17.º, a alínea *c)* do n.º 2 do artigo 18.º e o n.º 1 do artigo 19.º do Regulamento DORA, que um incidente pode ser considerado resolvido quando: os sistemas afetados retornaram à normalidade operacional; as atividades de

		negócio foram restauradas de forma segura; o incidente não requer mais gestão ativa; os riscos associados foram mitigados para um nível aceitável, de acordo com a tolerância ao risco da organização. É importante notar que o Regulamento DORA não exige explicitamente a eliminação total da causa principal de um incidente para o considerar resolvido. A decisão de mitigar e aceitar um risco remanescente, ao invés de eliminar completamente a causa principal do incidente, pode ser aceitável, desde que esteja alinhada com as políticas de gestão de risco da entidade e com as exigências regulatórias aplicáveis. No que respeita à definição de "Incidente relacionado com as TIC", não se afigura adequado proceder à alteração da definição, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. No que se refere às definições de "serviço crítico" e de "função crítica ou

		importante", considera-se que a norma regulamentar já distingue as duas definições de forma adequada: trata-se de um serviço digital que apoia/dá suporte a uma função crítica ou importante. Quanto à definição de "Serviço de TIC", não se afigura adequado proceder à alteração da definição, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Sem prejuízo, nota-se que "*equipamentos informáticos enquanto serviço*" refere-se ao modelo de negócio em que recursos de *hardware* são fornecidos e geridos por um terceiro prestador de serviço, sendo acedidos pelos clientes através da Internet. Já os "*serviços de equipamento informático*" abrangem uma gama mais ampla de serviços relacionados com *hardware*, incluindo manutenção, suporte e gestão de equipamentos. Um exemplo de "*equipamentos informáticos enquanto serviço*" seria um serviço de *Infrastructure as a Service* (*IaaS*) fornecido por

		um prestador de serviço de computação em nuvem. Nota-se ainda, neste contexto, a lista de tipos de serviços de TIC prevista no anexo III do relatório final do *Draft Implementing Technical Standards on the standard templates for the purposes of the register of information in relation to all contractual arrangements on the use of ICT services provided by ICT third-party service providers under Article 28(9) of Regulation (EU) 2022/2554*.
Artigo 3.º, alínea *c)*	A definição é convoluta. As referências independentes a "perturbação", e depois a "interrupção anomalia ou falha" não acrescentam valor. O significado do termo "Solidez" não é evidente, e parece ser dispensável. Sugere-se a seguinte redação alternativa: "Função crítica ou importante, uma função cuja perturbação comprometeria significativamente o desempenho financeiro de uma entidade, a continuidade dos serviços ou atividades, ou o contínuo cumprimento das condições e obrigações decorrentes da respetiva autorização, ou das restantes obrigações legais ou regulamentares de uma entidade mencionada no n.º 1 do artigo anterior."	**Acolhido parcialmente.** Procedeu-se à eliminação do termo "solidez", considerando-se as demais referências adequadas ao conceito em causa, tendo igualmente em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA.
Artigo 3.º, alínea *d)*	Sugere-se, sem perda de significado e com ganho de generalidade, remover a referência a segurança da rede e sistemas. Sugere-se a seguinte redação alternativa: "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 têm um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados, ou nos serviços prestados pelas entidades;"	**Não acolhido.** Entende-se que a eliminação proposta altera o significado do conceito, uma vez que, dessa forma, deixaria de limitar-se a incidentes relacionados com as TIC e passaria a abranger também incidentes não

		suportados por sistemas de rede e de informação.
Artigo 3.º, alínea *e)*	A definição de incidente cibernético severo, embora abrangente e adequada, poderia ser complementada com exemplos concretos de cenários que se enquadram na categoria, facilitando a interpretação e aplicação da norma pelas entidades.	**Não acolhido.** Não se afigura adequada a exemplificação proposta, porquanto será o resultado da avaliação inerente à classificação dos incidentes que vai determinar, em cada caso concreto, se o incidente é severo ou não. Deverão ter-se em consideração os critérios previstos no artigo 4.º da norma regulamentar.
Artigo 3.º, alínea *f)*	Sugere-se a seguinte redação alternativa, mais alinhada com a ISO 31000: «Risco associado às TIC», qualquer circunstância razoavelmente identificável relacionada com a utilização de sistemas de rede e de informação que, caso se materialize, conduza a incerteza quanto à execução de processos de negócio, prestação de serviços, ou quanto às características de confidencialidade, integridade ou disponibilidade dos ativos de informação da entidade.	**Não acolhido.** Não se afigura adequado proceder à alteração da definição, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Por outro lado, a presente norma regulamentar pretende ser agnóstica de um ponto de vista tecnológico e metodológico.
Questão 3 "Concorda e considera adequado o conjunto de critérios de classificação previsto no projeto de norma regulamentar ou	Atendendo a que o Projeto de Norma Regulamentar tem como um dos objetivos 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 – consideramos suficiente o conjunto dos critérios de classificação previstos e concordamos genericamente	**Não acolhido.** Relativamente à alínea *a)* do n.º 1 do artigo 4.º, cf. resposta ao comentário seguinte.

entende que facilitaria a sua aplicabilidade o aditamento de outros elementos? No último caso, quais?"	com os critérios. Contudo, sem prejuízo dos comentários na especialidade, infra, salientamos: **Artigo 4.º/1/a)** - Discordância em relação à alínea a) do n.º 1 do artigo 4.º, conforme comentários na Tabela de Comentários (na mesma Tabela de Comentários, apresentam-se diversas sugestões a este artigo). **Artigo 4.º/1/b) ii)** - Consideramos que o critério "A duração do incidente é superior a 24 horas" deve ser retirado e mantidos apenas os critérios de impacto. A duração, por si só, não se traduz necessariamente em impacto e, adicionar este critério, pode sobrecarregar operacionalmente as equipas que têm a responsabilidade de resolver o incidente com mais uma atividade. Assumindo que o impacto é avaliado caso o incidente esteja relacionado com serviços críticos, importa definir quais serão os serviços críticos. Neste ponto consideramos que deverão ser os mesmos constantes no Plano de Continuidade de Negócios, em concreto BIA. Adicionalmente, perspetivando-se uma revisão desta Norma Regulamentar, por ora em projeto, após a entrada em vigor do Regulamento DORA (em 17/01/2025), tendo em vista evitar sobreposições e identificar os mecanismos de reporte que poderão ser utilizados no âmbito daquele quadro regulatório (cfr., neste sentido, o enquadramento do documento de Consulta Pública – p. 5), julgamos ser avisado adotar uma abordagem relativamente parcimoniosa na presente Norma Regulamentar, sob pena de num futuro não muito longínquo as empresas de seguros terem de reequacionar e reformular os desenvolvimentos ao sistema de gestão de riscos empreendidos para dar resposta às obrigações de reporte agora fixadas (com o inerente acréscimo de custos ao já avultado dispêndio de recursos que a implementação da norma regulamentar reclama). Sugere-se, ainda, adicionar as dimensões de avaliação de especialista e de risco sistémico, alinhando com o artigo 3.º e artigo 4.º da Instrução n.º 21/2019 do Banco de Portugal.	No que respeita à subalínea *ii)* da alínea *b)* do n.º 1 do artigo 4.º da norma regulamentar, nota-se que o critério da duração do incidente configura um dos critérios previstos no Regulamento DORA [cf. alínea *b)* do n.º 1 do seu artigo 18.º], pela que a sua eliminação resultaria numa limitação a uma adequada preparação para o cumprimento dos requisitos estabelecidos neste âmbito. Por outro lado, importa ter em conta que que a avaliação dos critérios previstos na alínea *b)* do n.º 1 do artigo 4.º da norma regulamentar deve ser efetuada de forma holística e de forma conjugada entre si (isto é, o facto de um incidente ter uma duração superior 24h não determina, só por si, a sua classificação como severo). Refira-se ainda que cabe a cada entidade avaliar e definir os respetivos serviços críticos e quais os serviços críticos que devem integrar os seus planos de continuidade, tendo por referência as funções críticas ou importantes que suportam. No que concerne às preocupações manifestadas quanto à abordagem adotada na norma regulamentar, nota-se, conforme

		referido no documento de consulta pública, que a ASF procurou precisamente estabelecer, de forma mais simplificada, os requisitos relativos à comunicação de incidentes relacionados com as TIC previstos no Regulamento DORA, tendo em vista assegurar a adequada preparação e desenvolvimento dos sistemas de gestão de riscos das entidades e a implementação de melhorias para efeitos da aplicação daquele regulamento a partir de 17 de janeiro de 2025. Por fim, quanto à sugestão de aditamento das dimensões de avaliação de especialista e de risco sistémico, nota-se que esta última ideia já se encontra subjacente aos limiares dos critérios de classificação estabelecidos. Por outro lado, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência, o quadro regulatório que lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário).

Artigo 4.º, n.º 1, alínea *a)*	Relativamente à redação da alínea a) do n.º 1 do artigo 4.º, os contributos que as Associadas transmitiram foram no sentido de aperfeiçoar a densificação da alínea, concretamente: • "O critério previsto nesta alínea abrange qualquer acesso, não estando o critério limitado aos acessos que afetem serviços críticos da entidade. Parece-nos que um acesso que não afete serviços críticos não reúne características que conduzam à sua classificação como incidente severo. Face ao exposto, sugerimos que a redação da alínea a), do número 1, do Artigo 4º, deveria ser a seguinte: "Existe um acesso doloso, não autorizado e efetivo às redes e sistemas de informação afetando serviços críticos da entidade" • "Na redação proposta, este critério define, só por si, um incidente severo. Observamos, no entanto, que o texto não qualifica o acesso obtido, nem tão pouco a cardinalidade ou qualidade dos sistemas acedidos. Sugerimos uma redação alternativa, que mantendo o foco no acesso doloso não autorizado, introduz qualificadores de relevância: «a) Existe um acesso doloso, não autorizado e efetivo às redes ou sistemas de informação da entidade, que tenha condições para configurar um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados, ou nos serviços prestados pelas entidades; ou »"	**Acolhido parcialmente.** Nota-se que o critério previsto na alínea *a)* do n.º 1 do artigo 4.º da norma regulamentar configura um dos critérios previstos no Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo [cf. alínea *b)* do n.º 5 do artigo 9.º]. Contudo, de facto, tendo em conta o considerando 10, a alínea *c)* do artigo 6.º e o proémio do n.º 1 do artigo 8.º do referido regulamento, foi aditada, na alínea *a)* do n.º 1 do artigo 4.º da norma regulamentar, a referência a um acesso bem-sucedido, mal-intencionado e não autorizado às redes e sistemas de informação da entidade de apoio a funções críticas ou importantes.
Artigo 4.º, n.º 1, alínea *b)*	Um sistema cuja perturbação conduza a impactos que verifiquem qualquer uma das condições i)-v) é, por definição, crítico, pelo que a condição apresentada é	**Não acolhido.**

	grandemente redundante. Sugere-se a redação alternativa: «b) verificam-se duas ou mais das seguintes situações:» Adicionalmente, a condição iii) verificar-se-á sempre que uma das restantes seja verdadeira, pelo que se sugere eliminar o ponto iii) e adotar a seguinte redação alternativa: «b) verifica-se uma ou mais das seguintes situações:»	Não se afigura adequado proceder à alteração proposta, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Note-se que os limiares de materialidade para permitir a deteção dos incidentes de carácter severo relacionados com as TIC devem centrar-se, nomeadamente, no impacto nos respetivos serviços críticos (cf. considerando 9 e artigo 8.º do Regulamento Delegado referido na resposta ao comentário anterior).
Artigo 4.º, n.º 1, alínea b), subalínea *i)*	Sugere-se alinhar com o critério para incidente significativo do artigo 3.º n.º 1 da Instrução n.º 21/2019 do Banco de Portugal, com a seguinte redação alternativa: «i) O número de clientes afetados pelo incidente é superior a 25% do total de clientes que utilizam o serviço afetado ou é superior a cinquenta mil clientes;»	**Não acolhido.** Não se afigura adequado proceder à alteração proposta, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Por outro lado, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que

		lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário). Ademais, afigura-se que a presente sugestão não iria acautelar o objetivo de adequado desenvolvimento dos sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC, podendo implicar a sua reformulação no futuro próximo.
Artigo 4.º, n.º 1, alínea b), subalínea *iii)*	Esta condição verificar-se-á sempre que uma das restantes seja verdadeira. Sugerimos remover a condição e alterar 1b) para: «b) verifica-se uma ou mais das seguintes situações:»	**Não acolhido.** Não se afigura adequado proceder à alteração proposta, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA.
Artigo 4.º, n.º 1, alínea b), subalínea *iv)*	Sugere-se alinhar com as magnitudes do critério para incidente significativo do artigo 3.º n.º 1 da Instrução n.º 21/2019 do Banco de Portugal, com a seguinte redação alternativa: «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 cinco milhões de euros, ou XXX% dos capitais próprios, excluindo eventuais montantes recuperáveis; »	**Não acolhido.** Realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será aplicável em matéria de resiliência

		operacional digital (o qual – note-se – será igualmente ao setor bancário). Por outro lado, afigura-se que a presente sugestão não iria acautelar o objetivo de adequado desenvolvimento dos sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC, podendo implicar a sua reformulação no futuro próximo.
Artigo 4.º, n.º 3, alínea *a)*	Considera-se que o critério carece de densificação e concretização. Basta uma única notícia? Em qualquer meio de comunicação social? Mesmo que regional?	Estas questões encontram-se esclarecidas no formulário relativo ao relatório intercalar, no campo "Contextualização do impacto reputacional".
Artigo 4.º, n.º 3, alínea *b)*	Considera-se que o critério carece de densificação e concretização, designadamente quando se refere "(…) múltiplas reclamações (…)". Quantas?	Cf. resposta ao comentário anterior.
Artigo 4.º, n.º 3, alínea *c)*	Sugere-se mover este ponto para 1.b), com a redação: «vi) A entidade, em resultado do incidente, não consegue dar cumprimento ou é suscetível de não dar cumprimento a exigências legais ou regulatórias;	**Não acolhido.** Nota-se que o critério previsto na alínea *c)* do n.º 3 do artigo 4.º da norma regulamentar configura um dos critérios previstos no Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que

		especificam os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo em relação ao critério do impacto em termos de reputação [cf. alínea *d)* do n.º 1 do artigo 2.º], configurando a sua alteração sistemática uma limitação a uma adequada preparação para o cumprimento dos requisitos estabelecidos neste âmbito.
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?"	O conjunto de elementos previstos no artigo 5.º do Projeto de Norma Regulamentar estão, *grosso modo*, harmonizados com o Regulamento DORA e, nessa medida, parecem-nos ser adequados ao propósito normativo do Projeto de NR. Sempre diremos que a granularidade dos elementos de informação previstos nos formulários preparados à luz do artigo 7.º do Projeto de NR, com vista a densificar o respetivo artigo 5.º/1 nos parece (sem prejuízo de a consideramos abstratamente adequada e pertinente) demasiado ambiciosa, mormente quanto aos relatórios inicial e intercalar. Nesta sequência, em resposta à questão 7, gizamos uma proposta de melhores esforços no sentido de as entidades reportantes prestarem toda a informação de que disponham, sem que a falta de algum elemento dos reportes prejudique a respetiva submissão na plataforma dedicada ao efeito. Colocamos ainda uma dúvida, relativamente ao caso de serem funções inerentes ao cargo de CISO (previsto em normativo interno), no sentido de saber se é necessária uma designação formal específica para este efeito? E se é necessária a	A ASF tomou devida nota dos presentes comentários. Em relação aos formulários, cf. resposta ao comentário sobre a questão 7. Em relação às questões de governação interna suscitadas, nota-se que a (des)necessidade de designação formal se insere no âmbito dos procedimentos internos e liberdade organizativa conferida às entidades supervisionadas em matéria de governação. Refira-se, contudo, que apenas se encontram sujeitas a registo junto da ASF as funções identificadas na Norma

	sua comunicação à ASF para além do respetivo registo e da informação no formulário de comunicação de incidente?	Regulamentar n.º 9/2023-R, de 3 de outubro, relativa ao registo prévio para o exercício de funções reguladas. No caso da presente norma regulamentar, remete-se para o cumprimento do disposto no n.º 5 do artigo 5.º.
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?"	Não detetamos óbice a que a designação do responsável pela comunicação de incidentes de caráter severo relacionados com TIC seja formalizada através de uma deliberação do órgão de administração. Aliás, ainda que não seja regulamentarmente exigido o mesmo formalismo, em princípio a designação do responsável pela segurança da informação previsto pelo artigo 9.º da Norma Regulamentar n.º 6/2022-R, de 7 de junho (pelouro igualmente relevante no domínio das TIC), também será deliberada, ou pelo menos ratificada, pelo órgão de administração, uma vez que implica alterações ao sistema de governação da empresa de seguros. De resto, o próprio artigo 5.º/6 do Projeto de Norma Regulamentar possibilita que a mesma pessoa cumule as funções de responsável pela comunicação de incidentes de caráter severo relacionados com as TIC e de responsável pela função de segurança da informação. A questão que suscita maiores dúvidas é a possibilidade de subcontratação de um terceiro prestador de serviços para assegurar a comunicação de incidentes de caráter severo relacionados com TIC, conforme permitido pelo artigo 5.º/5 do Projeto de Norma Regulamentar. Com efeito, suscita-se em primeiro lugar a questão de saber se essa atividade deve ser considerada, para efeitos do artigo 78.º do Regime Jurídico de Acesso e Exercício da Atividade Seguradora e Resseguradora (RJASR), e aprovado pela Lei n.º 147/2015, de 9 de setembro, e do artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, fundamental ou importante.	Em primeiro lugar, cumpre notar que o artigo 5.º da norma regulamentar estabelece o dever de designação, pelo órgão de administração, de um responsável pela comunicação de incidentes de carácter severo relacionados com as TIC, tendo como finalidade assegurar a identificação do ponto de contacto junto do qual a ASF possa obter informações relacionadas com o incidente que lhe foi comunicado, no contexto das suas atribuições enquanto autoridade de supervisão. Por forma a mitigar os eventuais encargos administrativos para as entidades decorrentes dessa designação, permite-se o cometimento desta tarefa ao responsável pela função de segurança da informação ou a respetiva subcontratação a um terceiro prestador de serviços. Tal não significa, na primeira situação, a qualificação da responsabilidade pela

	Considerando que o prestador subcontratado para os identificados efeitos deverá, sob pena de incumprimento legal e regulamentar da empresa de seguros, permitir que esta cumpra, em permanência, o quadro regulatório aplicável [cfr. alínea b) do n.º 1 do artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril], será do nosso ponto de vista relevante que a ASF esclareça se considera que a subcontratação sub judice deve ser qualificada como fundamental ou importante e, como tal, ser notificada à Autoridade de Supervisão. Não se olvide que se trata de uma atividade que teria de ser assegurada internamente pela empresa de seguros, dando-se, então, por preenchido o conceito de subcontratação do artigo 5.º/1/x) do RJASR. Por outro lado, há que esclarecer se a função de responsável pela comunicação de incidentes de caráter severo relacionados com as TIC poderá ser objeto de subcontratação ou se apenas poderão ser subcontratadas as atividades (materiais, procedimentais ou processuais) relacionadas com a comunicação dos incidentes, caso em que a superintendência deverá continuar sob a égide da empresa de seguros (isto é, do colaborador do segurador que exerça a função de responsável pela comunicação de incidentes). Esta questão resulta, em nosso entender, relevante uma vez que não se exige no instrumento regulamentar sob consulta pública que o responsável pela comunicação de incidentes de carácter severo relacionados com as TIC deva imperativamente ser um colaborador dos quadros do segurador. Acresce que o artigo 5.º/6 do Projeto de Norma Regulamentar prevê a possibilidade de o responsável pela comunicação de incidentes de caráter severo relacionados com as TIC ser a pessoa responsável pela função de segurança da informação (que deverá ser colaborador dos quadros da empresa de seguros, porquanto a Norma Regulamentar n.º 6/2022-R, de 7 de junho não prevê idêntica faculdade de subcontratação), não determinando uma obrigatoriedade.	comunicação deste tipo de incidentes como uma função como é efetuado no artigo 9.º da Norma Regulamentar n.º 6/2022-R, de 7 de junho em relação à função de segurança de informação (trata-se de uma tarefa que pode ser executada pelo responsável daquela função). No segundo caso, tal significa que a tarefa de comunicação do incidente pode ser executada por um terceiro prestador de serviços, mantendo, no entanto, a entidade financeira a responsabilidade por assegurar que o dever de comunicação do incidente à autoridade de supervisão é cumprido. A informação prévia à ASF de funções e atividades operacionais fundamentais ou importantes ao abrigo do n.º 3 do artigo 78.º do RJASR, tendo, designadamente, em conta a alínea *b)* o n.º 1 do artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, corresponde a uma avaliação que cabe a cada entidade efetuar (isto é, aferir se, em caso de incumprimento por parte do prestador de serviços, a entidade é capaz de cumprir o quadro regulatório aplicável). Sem prejuízo do acima exposto, por razões de consistência sistemática, procedeu-se à

		troca da ordem dos n.os 5 e 6 do artigo 5.º da norma regulamentar.
Artigo 5.º "Comunicação de incidentes de carácter severo relacionados com as TIC"	A definição de canais específicos para comunicação de incidentes à ASF é importante, mas a obrigatoriedade de utilização exclusiva desses canais pode onerar as entidades. Sugere-se a avaliação da possibilidade de integração com plataformas já existentes ou a conclusão da prevista criação de um portal único e centralizado, otimizando a comunicação e reduzindo custos. Independentemente dos canais, os mesmos têm de ser seguros e confiáveis para a comunicação de incidentes, a fim de proteger informações sensíveis durante a transmissão, sendo certo que não podem comprometer os requisitos de segurança previstos no RGPD, ou seja, a existência de medidas técnicas e organizativas adequadas. Está previsto existir articulação do teor do reporte à CNPD e à ASF no caso do incidente envolver dados pessoais? Ou serão as entidades que internamente têm de estabelecer esse processo de harmonização?	**Não acolhido.** Não se afigura adequada a utilização de plataformas já existentes, por razões de segurança dos sistemas de informação da ASF. Por outro lado, nota-se que o mecanismo de comunicação adotado (cf. n.º 1 do artigo 7.º da norma regulamentar) simplifica o processo e cumpre requisitos de segurança e de confidencialidade. Os formulários serão acessíveis a partir de hiperligações para os mesmos, previamente disponibilizadas às entidades abrangidas pela norma regulamentar e para as quais apenas estas terão credenciais de acesso. Esclarece-se ainda que cabe às entidades supervisionadas o reporte à Comissão Nacional de Proteção de Dados (CNPD) no caso de violação de dados pessoais decorrentes de um incidente de carácter severo relacionado com as TIC.
Artigo 5.º, n.º 7	No âmbito do Regulamento Geral sobre a Proteção de Dados está prevista a obrigação de notificação à Comissão Nacional de Proteção de Dados ("CNPD") dos incidentes que envolvam a violação de dados pessoais, sempre que essa violação seja suscetível de implicar um risco para os direitos e liberdades das	Cf. resposta ao comentário anterior.

	pessoas singulares. No caso de estarmos perante um incidente de carácter severo relacionado com as TIC que envolva dados pessoais, existe a obrigatoriedade de duplo reporte?	
Questão 6 "Concorda e considera adequados os prazos de comunicação à ASF da notificação inicial, do relatório intercalar e do relatório final?"	O regime de prazos consagrado no artigo 6.º do Projeto de Norma Regulamentar contende, a nosso ver, com o regime geral de contagem de prazos previstos no artigo 87.º do Código do Procedimento Administrativo (CPA), que fixa na sua alínea c) a regra de os prazos serem contados em dias úteis. De resto, a referida alínea claramente dispõe que os prazos se suspendem aos sábados, domingos e feriados. Ainda que compreendamos e acompanhemos a urgência dos reportes em questão, não podemos deixar de realçar que, caso ocorra algum incidente de caráter severo relacionado com as TIC em dia não útil, não se afigura proporcional nem praticável (mormente em seguradores com estruturas reduzidas) alocar recursos às comunicações destinadas à ASF. A nosso ver, os esforços iniciais deverão centrar-se, antes de tudo o resto, na contenção e mitigação dos efeitos dos incidentes, especialmente se os mesmos ocorrerem em dias não úteis, em que a dimensão das equipas e inerente capacidade de resposta serão necessariamente mais reduzidas. Assim, consideramos adequado que os prazos previstos no Projeto de Norma Regulamentar sejam contados em dias úteis. Caso contrário, vislumbramos que possa existir risco de incumprimento dos prazos por escassez ou indisponibilidade das equipas mobilizadas para fazer face à resolução dos incidentes em dias não úteis (problema que poderá revestir maior acuidade nos casos em que a comunicação de incidentes tenha sido subcontratada a um terceiro prestador de serviços – conforme admite o artigo 5.º/5 do Projeto de Norma Regulamentar –, especialmente pela circunstância deste depender de informação prestada pela entidade afetada pelo incidente, ocupada, antes de tudo o mais, com a resolução do incidente).	**Acolhido parcialmente.** A ASF reconhece as preocupações manifestadas no presente comentário e a exigência dos prazos de reporte previstos, não podendo, contudo, deixar de salientar a relevância da comunicação de incidentes de carácter severo relacionados com as TIC ao supervisor com a brevidade possível. Ademais, importa acautelar uma adequada preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA e respetivos atos de execução, evitando, assim, a reformulação de sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC no futuro próximo. Neste contexto, procedeu-se à alteração do artigo 6.º da norma regulamentar, tendo em conta o relatório final do *Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents*.

	Relativamente aos prazos concretos apresentados no projeto, sem prejuízo das sugestões apresentadas no artigo 6.º do Projeto, considera-se desde logo que: - O prazo de 4 ou 24 horas para apresentar a **notificação inicial** do incidente é de muito difícil concretização (veja-se a eventualidade de o incidente ocorrer fora do período normal de trabalho). Sugere-se, p.e., que o prazo de notificação inicial seja efetuado logo que possível, até um máximo de 72 horas após a sua deteção ou classificação como severo. - O prazo do **relatório intercalar** (72 horas após a classificação como incidente severo) é demasiado exigente, considerando que as equipas responsáveis podem ainda estar a resolver o incidente e, serem envolvidas nesse momento na elaboração de um relatório, pode contribuir para uma resolução menos eficaz do incidente. Aliás, o prazo de 72 horas para envio do relatório intercalar não contribui diretamente para a efetiva resolução do incidente. - O prazo de um mês (em dias de calendário) para apresentação à ASF do **relatório final** poderá ser insuficiente para total resolução do incidente ou para apuramento de todos os impactos decorrentes do mesmo.	
Artigo 6.º, n.º 2	Sugerimos uma redação alternativa que alinha com os prazos para o relatório intermédio com o artigo 7.º n.º 3 da Instrução n.º 21/2019 do Banco de Portugal, que incorpora a necessidade de comunicação quando existir alteração relevante ao estado do incidente, e prevê a recolha de informação e elaboração do relatório: «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 máximo de 10 dias úteis desde o momento em que o incidente é classificado como severo, ou assim que, após a entidade recuperar as suas atividades e voltar a operar normalmente, estejam reunidas as condições para reporte.» Sugerimos esta redação alternativa que alinha com os prazos para o relatório final com artigo 7.º n.º 4 da Instrução n.º 21/2019 do	**Não acolhido.** Cf. resposta ao comentário anterior. Ademais, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será

	Banco de Portugal, incorpora a necessidade de comunicação atempada, e prevê a recolha de informação e elaboração do relatório. «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 máximo de 30 dias úteis desde o momento em que o incidente é classificado como severo ou assim que, após o incidente ter sido dado como resolvido de forma permanente, estejam reunidas as condições para reporte, incluindo a análise de causas subjacentes e os valores reais de impacto.»	aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário).
Questão 7 "Concorda e considerado adequado o conteúdo dos formulários respeitantes à notificação inicial e aos relatórios intercalar e final?"	Origem do incidente" – sugere-se alterar b) para "Outra Entidade Financeira" "Tipo de incidente" e "Ameaças e técnicas utilizadas pelo agente de ameaça" – sugere-se alinhar com a taxonomia do CNCS (https://www.cncs.gov.pt/pt/certpt/taxonomia/), que implementa o previsto na taxonomia do grupo de cooperação NIS (https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf), ou adotar o bloco "Information on the incident" do formulário de reporte do Banco de Portugal/BCE. "Componentes da infraestrutura que apoiam processos de negócio" e "Sistemas afetados pelo incidente na infraestrutura " – consideramos que esta alínea é demasiadamente intrusiva, frequentemente não é relevante e representa um esforço desnecessário na criação do relatório. Sugere-se que seja passada para opcional, ou, idealmente, removida. "Principal causa do incidente" – a taxonomia de classificação de causas é demasiadamente opinada e detalhada. Sugiro seja adotada a estrutura descrita no ponto 5.1 do documento do grupo de cooperação NIS (URL acima), que seja limitada ao segundo nível, ou que seja adotada a secção "Vulnerabilities/weaknesses exposed" do formulário de reporte do Banco de Portugal/BCE.	**Acolhido parcialmente.** Procedeu-se à alteração relativa ao campo "Origem do incidente". Relativamente aos campos "Tipo de incidente" e "Ameaças e técnicas utilizadas pelo agente de ameaça", não se afigura adequado o alinhamento com a taxonomia do Centro Nacional Cibersegurança, pois importa acautelar uma adequada preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA, evitando, assim, a reformulação de sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC no futuro próximo. Por outro lado, importa notar que o artigo 20.º do Regulamento DORA determina a necessidade de consulta da

	Sugerimos que, à imagem do que existe já com o Banco de Portugal, seja considerada a criação de um ponto único de reporte para o setor segurador, que terá a responsabilidade de encaminhar os reportes de incidente para o CNCS Para além dos contributos suprarreferidos, entendemos que o conteúdo dos formulários respeitantes à notificação inicial e aos relatórios intercalar e final parece-nos adequado e pertinente para a compreensão do incidente ocorrido. No entanto, em nosso entender, a plataforma na qual serão submetidos os reportes (cfr. art. 7.º/1 do Projeto de Norma Regulamentar) não deverá condicionar o upload dos ficheiros ao completo e integral preenchimento de todos os campos, mesmo os classificados como "obrigatórios", uma vez que a entidade reportante poderá não estar munida da totalidade da informação solicitada no momento da submissão do reporte (ainda que a mesma deva ser estimada com base na informação disponível – cfr. n.º 2 do artigo 4.º do Projeto de Norma Regulamentar), tendo ainda de assegurar o cumprimento do respetivo prazo. Caso a ASF assim não entenda, propomos que a única submissão de reporte subordinada ao integral preenchimento do formulário seja a do relatório final, atenta a natureza precária, transitória e tendencialmente dinâmica dos restantes.	Agência da União Europeia para a Cibersegurança (ENISA) na elaboração do conteúdo das notificações de incidentes de caráter severo relacionados com as TIC, devendo ser a taxonomia dessa Autoridade a ser tida em conta (cf. relatório final do *Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents*). No que respeita ao campo "Componentes da infraestrutura que apoiam processos de negócio", não se afigura que o preenchimento pelas entidades seja demasiado oneroso, dada a natureza da resposta (escolha múltipla). No que concerne ao campo "Sistemas afetados pelo incidente na infraestrutura ", aditou-se a opção de resposta "Sem informação disponível". Quanto ao campo "Principal causa do incidente", procedeu-se à redução do número de subcategorias e ao agrupamento

		de opções semelhantes, mas alerta-se para a aplicação de uma estrutura de resposta mais detalhada a partir da data de aplicação do Regulamento DORA. Em relação à sugestão de criação de um ponto único de reporte para o setor segurador, que teria a responsabilidade de encaminhar os reportes de incidente para o Centro Nacional de Cibersegurança, nota-se que o quadro regulatório vigente neste âmbito não impõe uma obrigação de comunicação de incidentes à aquela Autoridade. Por último, esclarece-se que não será possível o *upload* de ficheiros, devendo proceder-se ao preenchimento dos formulários. Por outro lado, relativamente à categorização dos campos como obrigatórios e facultativos, nota-se que a referida categorização está também relacionada com o cumprimento ou não de determinado critério de classificação. Além disso, a maior parte das questões contidas nos formulários são de resposta fechada, exceto no relatório final, momento em que

		é expectável que a entidade disponha de mais informação sobre o incidente.
Artigo 7.º "Meio de comunicação"	Determina o n.º 1 do artigo 7.º do Projeto de NR que a informação prevista no artigo 5.º, n.º 1 seja enviada à ASF através de uma plataforma dedicada para o efeito. Em função da experiência adquirida por uma empresa de seguros vítima de ciberataques, à qual a ASF bloqueou o acesso a todos os portais, partilhamos a nossa apreensão com este meio (exclusivo) de reporte (que, à partida, deverá exigir coordenadas de acesso próprias para cada segurador). Com efeito, a menos que exista um firme compromisso da ASF com a permanente disponibilidade de acessos à plataforma de reporte, inclusive a seguradores afetados por incidentes de caráter severo, por forma a não inviabilizar o pontual cumprimento das novas obrigações estabelecidas por esta nova norma regulamentar, sugerimos que seja disponibilizado um endereço de e-mail para o qual possa ser remetida a informação devida.	**Acolhido parcialmente.** Realça-se que o mecanismo de comunicação adotado (cf. n.º 1 do artigo 7.º da norma regulamentar) simplifica o processo e cumpre requisitos de segurança e de confidencialidade. Os formulários serão acessíveis a partir de hiperligações para os mesmos, previamente disponibilizadas às entidades abrangidas pela norma regulamentar e para as quais apenas estas terão credenciais de acesso. Sem prejuízo, foi aditado um novo número (novo n.º 2) ao artigo 7.º, possibilitando a comunicação do incidente por outra via segura, em caso de impossibilidade de cumprimento pontual da obrigação de comunicação ou de indisponibilidade dos formulários fornecidos para o efeito.
Artigo 8.º "Início de vigência"	Considerando que as entidades abrangidas pelo presente projeto de norma estão em fase de preparação para a implementação dos requisitos do Regulamento DORA, sugere-se que a norma entre em vigor 1 mês após a sua publicação, permitindo uma melhor preparação das diversas entidades à mesma.	**Não acolhido.** Conforme referido no documento de consulta pública e no preâmbulo da norma regulamentar, esta tem também como objetivo a devida preparação e a antecipação dos requisitos estabelecidos neste âmbito pelo Regulamento DORA, e

		respetivos atos delegados e de execução, de forma mitigada e gradual 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. Neste sentido, não se afigura que a presente proposta acautele este objetivo. Nota-se, por outro lado, que a avaliação e gestão dos riscos relacionados com as TIC e notificação de incidentes desta natureza já deverá, naturalmente, estar a ser contemplada pelas empresas de seguros e de resseguros, atendendo ao quadro legal, regulamentar e de *soft law* vigente em matéria de gestão de riscos operacionais e à especial acuidade que a mesma apresenta no contexto atual de crescente digitalização e utilização de serviços de TIC de terceiros.
Outros contributos	• Suscitamos desde já uma eventual articulação da ASF com outras autoridades relevantes, como o Centro Nacional de Cibersegurança, dado que consideramos fundamental para otimizar a resposta a incidentes cibernéticos de grande escala e garantir uma abordagem abrangente da segurança cibernética. O estabelecimento de protocolos de comunicação e colaboração entre as entidades pode fortalecer a capacidade de resposta a eventos cibernéticos complexos e de impacto sistémico.	A ASF partilha do entendimento exposto no presente comentário, não se afigurando, contudo, adequada a sua previsão na presente norma regulamentar.

	• Dada a natureza global das TIC, é essencial que a norma inclua diretrizes para a cooperação com organismos internacionais, o que não acontece no projeto apresentado, facilitando a troca de informações e a coordenação em resposta a incidentes transfronteiriços.	

Pessoa/Entidade: **APFIPP – Associação Portuguesa de Fundos de Investimento, Pensões e Patrimónios**
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

Indicações:

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
Artigo 2.º "Âmbito de aplicação"	O Projecto de Norma em apreciação reconhece, no âmbito da alínea c), do n.º 1, do respectivo artigo 2.º, as especificidades das micro e pequenas empresas ao estabelecer excepções proporcionais aos seus recursos e perfil de risco. Não obstante, sugere-se a avaliação da possibilidade de segmentar as Entidades com base em critérios mais abrangentes, como porte, tipologia, facturação e histórico de incidentes cibernéticos, permitindo uma modulação mais precisa dos requisitos patentes neste diploma.	**Não acolhido.** Em primeiro lugar, nota-se que o quadro regulatório vigente em matéria de gestão de riscos, em particular do risco operacional, se aplica, de forma transversal, a todas as empresas de seguros e de resseguros e entidades gestoras de fundos de pensões.

		Por outro lado, conforme referido no documento de consulta pública e no preâmbulo da norma regulamentar, esta tem também como objetivo a devida preparação e a antecipação dos requisitos estabelecidos neste âmbito pelo Regulamento DORA, e respetivos atos delegados e de execução, de forma gradual, mitigada e mais simplificada, alertando, assim, as entidades por si supervisionadas para a necessidade de cumprimentos dos referidos requisitos a partir de 17 de janeiro de 2025. Assim, não se afigura que a presente proposta acautele este objetivo. A este propósito, procedeu-se ao ajustamento da redação da alínea *c)* do n.º 1 do artigo 2.º da norma regulamentar, de forma a promover um alinhamento mais adequado com o Regulamento DORA.
Questão 2 "Concorda e considera adequado o conjunto de definições previsto no projeto de norma regulamentar ou entende que facilitaria a sua	Remete-se para os comentários apresentados, neste Anexo, no que diz respeito ao artigo 3.º do Projecto de Norma em análise.	Cf. resposta ao comentário seguinte.

aplicabilidade o aditamento de outras definições? No último caso, quais?"		
Artigo 3.º "Definições"	O artigo em referência incorpora um conjunto de definições, que a ASF considerou relevantes para a aplicação da Norma em apreciação. No que concerne às diversas alíneas que fazem parte desta disposição, coloca-se à consideração do Supervisor os seguintes comentários/sugestões: • Alínea c) – No que diz respeito ao conceito de "*Função crítica ou importante*", patente nesta alínea, as Associadas da APFIPP consideram que a definição proposta é, salvo melhor opinião, convoluta, entendendo que a inclusão da expressão "*interrupção, anomalia ou falha*" não será necessária, havendo, também, dúvidas sobre o verdadeiro alcance da utilização do termo "solidez". Com o objectivo de tornar o texto mais claro, sugerem-se as seguintes alterações: *"«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***~~***, a*** *continuidade dos* ~~***seus***~~ *serviços* ~~***e das suas***~~ ***ou*** *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* ***de uma entidade mencionada no n.º 1 do artigo anterior****;"* (sublinhado, rasurado e realce nossos);	**Acolhido parcialmente.** Procedeu-se à eliminação do termo "solidez" da definição de "função crítica ou importante", considerando-se as demais referências adequadas ao conceito em causa, tendo igualmente em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. No que respeita à definição de "Incidente relacionado com as TIC", entende-se que a eliminação proposta altera o significado do conceito, uma vez que, dessa forma, deixaria de limitar-se a incidentes relacionados com as TIC e passaria a abranger também incidentes não suportados por sistemas de rede e de informação. No que se refere à definição de "Incidente de carácter severo relacionado com as TIC", não se afigura adequada a exemplificação proposta, porquanto será

	• Alínea d) – Em relação à definição de "*Incidente relacionado com as TIC*", entende-se que existe margem de simplificação do texto proposto, sem perda do seu significado, através da eliminação da referência à "*segurança dos sistemas de rede e informação*", conforme ajustamento assinalado infra: *"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;"* (rasurado e realce nossos); • Alínea e) – Sugere-se que a definição de "*Incidente de carácter severo relacionado com as TIC*", patente na alínea em referência, que remete para os critérios previstos no artigo 4.º do Projecto de Norma, seja complementada com exemplos concretos de cenários que se enquadrem nesta categoria de incidentes, facilitando a interpretação e aplicação do diploma pelas Entidades supervisionadas; • Alínea f) – Com o intuito de alinhar a definição de "*Risco associado às TIC*" com o previsto na ISO 31000, propõem-se os seguintes ajustamentos na alínea em apreço: *"«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***~~	o resultado da avaliação inerente à classificação dos incidentes que vai determinar, em cada caso concreto, se o incidente é severo ou não. Deverão ter-se em consideração os critérios previstos no artigo 4.º da norma regulamentar. Por último, quanto à definição de "Risco associado às TIC", não se afigura adequado proceder à alteração da definição, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Por outro lado, a presente norma regulamentar pretende ser agnóstica de um ponto de vista tecnológico e metodológico.

	~~***funcionamento e da*** ***conduza a incerteza quanto à*** *execução de processos* ***de negócio,*** ~~***ou da***~~ *prestação de serviços,* ***ou quanto às características de confidencialidade, integridade ou disponibilidade dos ativos de informação da entidade*** ~~***causando efeitos adversos no ambiente digital ou físico***~~*;"* (sublinhado, rasurado e realce nossos).	
Questão 3 "Concorda e considera adequado o conjunto de critérios de classificação previsto no projeto de norma regulamentar ou entente que facilitaria a sua aplicabilidade o aditamento de outros elementos? No último caso, quais?"	Relativamente à classificação de incidentes relacionados com as TIC, para além dos comentários apresentados, neste Anexo, no que diz respeito ao artigo 4.º do Projecto de Norma em análise, sugere-se adicionar ao normativo proposto as dimensões de avaliação de especialista e de risco sistémico, que se encontram previstas nos artigos 3.º e 4.º da Instrução do Banco de Portugal n.º 21/2019, a qual versa, também, sobre o "Reporte de Incidentes de Cibersegurança", àquele Supervisor, no contexto das Entidades pelo mesmo supervisionadas. As regras estabelecidas na citada Instrução vão, salvo melhor opinião, no sentido de dar visibilidade sobre incidentes que, não cumprindo outros critérios de reporte, são considerados relevantes pelos especialistas internos ou representam um risco transversal à Indústria, por vulnerabilidades comuns, interdependências ou outros, propondo-se, assim, a inclusão de tais princípios na Norma em apreço, com o intuito de uma maior aproximação entre estes enquadramentos.	**Não acolhido.** Quanto à sugestão de aditamento das dimensões de avaliação de especialista e de risco sistémico, nota-se que esta última ideia já se encontra subjacente aos limiares dos critérios de classificação estabelecidos. Por outro lado, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário).
Artigo 4.º	O n.º 1 do artigo 4.º do Projecto de Norma elenca um conjunto de critérios que devem ser considerados pelas Entidades que se encontram no âmbito de aplicação	**Acolhido parcialmente.**

"Classificação de incidentes relacionados com as TIC"	do diploma, no que respeita à classificação como severo de qualquer incidente relacionado com as TIC. Em relação aos critérios propostos, para o efeito, nas várias alíneas do citado n.º 1, apresentam-se os seguintes comentários/sugestões: • Alínea a) – O critério proposto, nesta norma, pela ASF, parece definir, por si só, o que se entende por incidente severo, observando-se, no entanto, que no texto não é qualificado o acesso obtido, nem a cardinalidade ou qualidade dos sistemas acedidos. Nestas circunstâncias, coloca-se à consideração do Supervisor as seguintes modificações que, salvo melhor opinião, mantendo o foco no acesso doloso não autorizado, introduzem qualificadores de relevância: *"a) Existe um acesso doloso, não autorizado e efetivo às redes e* ***/ou*** *sistemas de informação da entidade* ***, que tenha condições para configurar um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados, ou nos serviços prestados pelas entidades****; ou"* (sublinhado e realce nossos). • Alínea b) – Esta disposição prevê que um incidente relacionado com as TIC seja classificado de severo, pelas Entidades abrangidas pela Norma, se: *"O incidente afeta serviços críticos da entidade e, cumulativamente, verificam-se duas ou mais das seguintes situações:(…)".* Verifica-se que o texto proposto coloca como primeira condição que o sistema/serviços afectados sejam críticos, sendo um requisito que, salvo melhor opinião, constitui uma redundância, atendendo às diversas condições previstas	Nota-se que o critério previsto na alínea *a)* do n.º 1 do artigo 4.º da norma regulamentar configura um dos critérios previstos no Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo [cf. alínea *b)* do n.º 5 do artigo 9.º]. Contudo, de facto, tendo em conta o considerando 10, a alínea *c)* do artigo 6.º e o proémio do n.º 1 do artigo 8.º do referido regulamento, foi aditada, na alínea *a)* do n.º 1 do artigo 4.º da norma regulamentar, a referência a um acesso bem-sucedido, mal-intencionado e não autorizado às redes e sistemas de informação da entidade de apoio a funções críticas ou importantes.

	nas subalíneas i) a v) (com eventual exclusão da subalínea ii)), dado que se estas se aplicarem, o sistema/serviços terão obrigatoriamente que ser críticos. Face ao exposto, sugere-se que a redacção do proémio da alínea b) em referência seja revista em conformidade, propondo-se, para o efeito, o ajustamento seguidamente indicado: *"~~**b) O incidente afeta serviços críticos da entidade e, cumulativamente, v**~~ **V**erificam-se duas ou mais das seguintes situações:"* (sublinhado, rasurado e realce nossos). No que toca às várias subalíneas, da alínea b), do n.º 1 do artigo 4.º do Projecto de Norma apresentam-se os seguintes contributos adicionais: ▪ Subalínea i) – Em relação ao critério proposto, sugere-se que o mesmo seja alinhado com o previsto no n.º 1 do artigo 3.º da mencionada Instrução do Banco de Portugal n.º 21/2019, no que diz respeito a incidentes considerados significativos. Em concreto, propõe-se a seguinte alteração: *"i) O número de clientes afetados pelo incidente é superior a ~~**10**~~**25**% do total de clientes que utilizam o serviço afetado ou é superior a ~~**cem**~~ **cinquenta** mil clientes;"* (sublinhado, rasurado e realce nossos); ▪ Subalínea iii) – Salvo melhor entendimento, a condição prevista na disposição em referência (i.e.: "*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 das exigências regulatórias*")	No entanto, não se afigura adequado proceder à alteração proposta em relação à alínea *b)* do n.º 1 do artigo 4.º, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Note-se que os limiares de materialidade para permitir a deteção dos incidentes de carácter severo relacionados com as TIC devem centrar-se, nomeadamente, no impacto nos respetivos serviços críticos (cf. considerando 9 e artigo 8.º do Regulamento Delegado referido na resposta ao comentário anterior). Não se afigura adequado proceder à alteração proposta em relação à subalínea *i)* da alínea *b)* do n.º 1 do artigo 4.º, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Por outro lado, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança, um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e

	verificar-se-á sempre que uma das restantes subalíneas seja verdadeira, sugerindo-se, desse modo, a respectiva supressão. No caso da ASF acolher favoravelmente esta proposta de eliminação, defende-se que o proémio da alínea b), do n.º 1, do artigo 4.º do Projecto de Norma seja, em simultâneo, modificado da seguinte forma: *"**~~b) O incidente afeta serviços críticos da entidade e, cumulativamente, v~~** **V**erifica**~~m~~** se **~~duas~~** **uma** ou mais das seguintes situações:"* (sublinhado, rasurado e realce nossos); ▪ Subalínea iv) – Uma das situações, propostas pela ASF, que poderá, entre outros factores, conduzir à classificação de um incidente como severo, baseia-se no respectivo impacto económico, conforme reproduzido infra: *"(…) 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;"* (realce nosso). No que concerne ao critério transcrito, as Associadas da APFIPP entendem que o mesmo deverá ser revisto, no sentido de uma maior aproximação ao previsto na Instrução do Banco de Portugal n.º 21/2019, em matéria de incidentes considerados significativos (*vide* o n.º 1 do respectivo artigo 3.º), fixando-se, por exemplo, uma percentagem por referência ao capital próprio ou ao volume de negócios, num montante nunca inferior a cinco milhões de euros.	resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário). Ademais, afigura-se que a presente sugestão não iria acautelar o objetivo de adequado desenvolvimento dos sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC, podendo implicar a sua reformulação no futuro próximo. Não se afigura adequado proceder à alteração proposta em relação à subalínea *iii)* da alínea *b)* do n.º 1 do artigo 4.º, tendo em conta o objetivo de preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA. Relativamente à alteração proposta para subalínea *iv)* da alínea *b)* do n.º 1 do artigo 4.º, realça-se que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança,

	Com efeito, recorda-se que o Projecto de Diploma em análise tem por objecto regulamentar a comunicação de incidentes de carácter severo, considerando-se, salvo melhor opinião, que o valor proposto pela ASF é reduzido, para ser enquadrável nesta classificação, defendendo-se, desse modo, que o mesmo seja incrementado. Em complemento dos comentários apresentados supra, propõe-se, também, que a alínea c) do n.º 3 do artigo 4.º, que refere que "*A entidade, em resultado do incidente, não consegue dar cumprimento ou é suscetível de não dar cumprimento a exigências regulatórias*", passe a constar da subalínea vi), da alínea b) do n.º 1 deste artigo, com a consequente remuneração das restantes alíneas do mencionado n.º 3.	um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário). Por outro lado, afigura-se que a presente sugestão não iria acautelar o objetivo de adequado desenvolvimento dos sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC, podendo implicar a sua reformulação no futuro próximo. Nota-se que o critério previsto na alínea *c)* do n.º 3 do artigo 4.º da norma regulamentar configura um dos critérios previstos no Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024, que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam os critérios de classificação dos incidentes

		relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo em relação ao critério do impacto em termos de reputação [cf. alínea *d)* do n.º 1 do artigo 2.º], configurando a sua alteração sistemática uma limitação a uma adequada preparação para o cumprimento dos requisitos estabelecidos neste âmbito.
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?"	De uma forma geral, as Associadas da APFIPP concordam e consideram adequado o conjunto de elementos que devem ser comunicados à ASF aquando da existência de um incidente de carácter severo relacionado com as TIC, remetendo-se, no entanto, para as sugestões apresentadas infra, nomeadamente no âmbito dos comentários ao artigo 5.º do Projecto de Norma e da resposta à Questão 7. Não obstante, importa sublinhar que as Associadas da APFIPP reconhecem a importância da definição de canais específicos para comunicação de incidentes à ASF, mas entendem que a obrigatoriedade de utilização exclusiva desses canais pode onerar em demasia as Entidades Gestoras. Nesse contexto, sugere-se que seja avaliada a possibilidade de uma integração com plataformas já existentes ou a conclusão da prevista criação de um portal único e centralizado, optimizando a comunicação e reduzindo custos. Por outro lado, independentemente dos canais utilizados, é imperioso que os mesmos sejam seguros e confiáveis para a comunicação de incidentes, a fim de proteger informações sensíveis durante a transmissão, sendo certo que não podem comprometer os requisitos de segurança	**Não acolhido.** A ASF tomou devida nota dos presentes comentários. Em relação aos formulários, cf. resposta ao comentário sobre a questão 7. Não se afigura adequada a utilização de plataformas já existentes, por razões de segurança dos sistemas de informação da ASF. Por outro lado, nota-se que mecanismo de comunicação adotado (cf. n.º 1 do artigo 7.º da norma regulamentar)

	previstos no "Regulamento Geral sobre a Protecção de Dados" (RGPD), ou seja, a existência de medidas técnicas e organizativas adequadas. Em matéria de protecção de dados, questiona-se, também, se está prevista a existência de uma articulação do teor do reporte à Comissão Nacional de Protecção de Dados (doravante "CNPD") e à ASF, no caso do incidente envolver dados pessoais ou se serão as Entidades supervisionadas que terão de estabelecer esse processo de harmonização.	simplifica o processo e cumpre requisitos de segurança e de confidencialidade. Os formulários serão acessíveis a partir de hiperligações para os mesmos, previamente disponibilizadas às entidades abrangidas pela norma regulamentar e para as quais apenas estas terão credenciais de acesso. Esclarece-se ainda que cabe às entidades supervisionadas o reporte à CNPD no caso de violação de dados pessoais decorrentes de um incidente de carácter severo relacionado com as TIC.
Artigo 5.º "Comunicação de incidentes de carácter severo relacionados com as TIC"	De acordo com o artigo em referência, as Entidades abrangidas pelo Projecto de Norma em apreço, devem comunicar à ASF, nos prazos definidos no artigo 6.º, incidentes de carácter severo relacionados com as TIC, devendo apresentar ao Supervisor, para o efeito, a seguinte informação: i) Notificação inicial; ii) Relatório intercalar; e iii) Relatório final. A este respeito, coloca-se à consideração da ASF a sugestão de, no contexto de Grupo, quando se verifique um incidente que afecte mais do que uma ou todas as Entidades desse Grupo, as informações referidas no parágrafo anterior possam, no caso de Entidades sujeitas à Supervisão da ASF e que se encontrem no escopo do Projecto de Norma, ser submetidas através de um reporte único, em contraposição ao reporte por Entidade. No tocante ao artigo 5.º do Projecto de Norma, realça-se, igualmente, o facto do seu n.º 7 prever que o responsável pela comunicação de incidentes de carácter severo relacionados com as TIC, designado pelo Órgão de Administração das Entidades Gestoras, deve, juntamente com a notificação inicial, "*tomar conhecimento da informação*	**Acolhido.** Foi aditado um novo número (n.º 8) ao artigo 5.º da norma regulamentar, admitindo a possibilidade de reporte único e agregado, quando um incidente afete mais do que uma entidade ou todas as entidades do mesmo grupo, desde que as entidades em causa se encontrem sujeitas à presente norma regulamentar, a origem do incidente seja a mesma e o incidente seja classificado como severo em todas as entidades.

	relativa ao tratamento de dados pessoais constante do formulário referente a essa comunicação". Em linha com as dúvidas suscitadas, anteriormente, neste Anexo, na resposta à Questão 4, importa reiterar que, no âmbito do RGPD, está prevista a exigência de notificação à CNPD dos incidentes que envolvam a violação de dados pessoais, sempre que essa violação seja susceptível de implicar um risco para os direitos e liberdades das pessoas singulares. Nestas circunstâncias, no caso de estarmos perante um incidente de carácter severo relacionado com as TIC que envolva dados pessoais, existirá a obrigatoriedade de um duplo reporte?	Cf. resposta ao comentário anterior em relação à CNPD.
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?"	As Associadas da APFIPP concordam com a designação, nos termos do n.º 6 do artigo 5.º do Projecto de Norma, de um responsável pela comunicação de incidentes de carácter severo relacionados com as TIC.	A ASF tomou devida nota dos presentes comentários.
Questão 6 "Concorda e considera adequados os prazos de comunicação à ASF da notificação inicial, do relatório intercalar e do relatório final?"	Remete-se para os comentários apresentados, neste Anexo, no que diz respeito ao artigo 6.º do Projecto de Norma em análise.	Cf. resposta ao comentário seguinte.
Artigo 6.º "Prazos"	Conforme referido anteriormente, no comentário ao artigo 5.º, a disposição em referência fixa os prazos a observar no que toca ao envio, à ASF, no âmbito da ocorrência de incidentes de carácter severo relacionados com as TIC, dos seguintes	**Acolhido parcialmente.**

	elementos: i) Notificação inicial; ii) Relatório intercalar; e iii) Relatório final, estando os mesmos previstos, respectivamente, nos n.ºs 1, 2 e 3, sobre os quais se apresentam as seguintes sugestões: • N.º 1 - Em relação à notificação inicial, as Associadas da APFIPP consideram que os prazos, de quatro (4) ou 24 horas, estabelecidos, para submissão da mesma ao Supervisor, poderão ser insuficientes, nomeadamente na eventualidade do incidente ocorrer fora do período normal de trabalho. Nessa medida, sugere-se que a notificação inicial seja efectuada logo que possível, até um máximo de 72 horas após a detecção ou classificação do incidente como severo. Propõem-se, assim, nesse sentido, as seguintes alterações: *"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***~~ ***72*** *horas desde o momento em que o incidente é* ***detetado ou*** *classificado como severo* ~~***ou, no máximo, no prazo de 24 horas desde o momento em que o incidente é detetado***~~*."* (sublinhado, rasurado e realce nossos); • N.º 2 - No que concerne ao relatório intercalar, que, segundo o disposto no n.º 2 do artigo 6.º do Projecto de Norma, deverá 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 actividades e voltar a operar normalmente, regista-se que, no âmbito do RGPD, qualquer violação de dados pessoais deverá ser notificada à Autoridade de Controlo, sem demora injustificada e, sempre que possível, no prazo, também, de 72 horas.	A ASF reconhece as preocupações manifestadas no presente comentário e a exigência dos prazos de reporte previstos, não podendo, contudo, deixar de salientar a relevância da comunicação de incidentes de carácter severo relacionados com as TIC ao supervisor com a brevidade possível. Ademais, importa acautelar uma adequada preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA e respetivos atos de execução, evitando, assim, a reformulação de sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC no futuro próximo. Neste contexto, procedeu-se à alteração do artigo 6.º da norma regulamentar, tendo em conta o relatório final do *Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents*. Realça-se, por fim, que subjaz à Instrução n.º 21/2019 do Banco de Portugal, sobre o reporte de incidentes de cibersegurança,

	Não obstante, solicita-se que, neste âmbito, seja analisada a hipótese de se ter em linha de conta o disposto na Instrução do Banco de Portugal n.º 21/2019, no sentido de, ser possível, um maior alinhamento entre os regimes impostos por ambos os Reguladores ou, pelo menos, que tal aproximação se verifique quando não estejam em causa dados pessoais. De facto, muito embora o sector dos Fundos de Pensões esteja exposto a riscos diferentes do sector Bancário e os impactos causados, por qualquer situação adversa, possam ser de natureza e/ou magnitude distintas, solicita-se que, em relação ao relatório intercalar, o Projecto de Norma passe a prever, à semelhança do consagrado no n.º 3 do artigo 7.º da citada Instrução do Banco de Portugal, um prazo máximo de 10 dia úteis, a contar desde que o incidente é classificado como severo, para envio do relatório intercalar, ou que o mesmo seja submetido assim que, após a entidade recuperar as suas actividades e voltar a operar normalmente, estejam reunidas as condições para o reporte. Face ao exposto, sugere-se que o n.º 2 do artigo 6.º do Projecto de Norma seja ajustado do seguinte modo: *"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***~~ ***de 10 dias úteis*** *desde o momento em que o incidente é classificado como severo****,*** *ou assim que****, após*** *a entidade recuperar as suas atividades e voltar a operar normalmente****, estejam reunidas as condições para reporte****."* (sublinhado, rasurado e realce nossos); • N.º 3 - Por último, relativamente ao relatório final, entendem as Associadas da APFIPP que o prazo de um mês, a contar desde "*o momento em que o incidente é classificado como severo ou no dia seguinte ao incidente ter sido dado como resolvido de forma*	um quadro regulatório específico do setor bancário (não aplicável à atividade seguradora e resseguradora), devendo a ASF adotar, ao invés, *in casu*, como referência o quadro regulatório que lhe será aplicável em matéria de resiliência operacional digital (o qual – note-se – será igualmente ao setor bancário).

	permanente" poderá, também, revelar-se insuficiente para a total resolução do incidente ou para o apuramento de todos os impactos decorrentes do mesmo, sugerindo-se, igualmente, neste ponto, um maior alinhamento com o previsto na Instrução do Banco de Portugal n.º 21/2019. Em concreto, propõe-se que esta disposição passe a adoptar o seguinte texto: *"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* ***máximo*** *de* ~~***um mês***~~ ***30 dias úteis*** *desde o momento em que o incidente é classificado como severo ou* ***assim que, após o*** ~~***no dia seguinte ao***~~ *incidente ter sido dado como resolvido de forma permanente****, estejam reunidas as condições para reporte, incluindo a análise de causas subjacentes e os valores reais de impacto****."* (sublinhado, rasurado e realce nossos). Sem prejuízo das sugestões e comentários apresentados supra, atendendo à possibilidade de existirem incidentes complexos e que exigem uma investigação, análise e tratamento aprofundados, sugere-se que seja ponderada a hipótese de, em situações excepcionais, mediante justificação apresentada previamente pela Entidade à ASF, os prazos de comunicação serem dilatados. Reitera-se, neste âmbito, que os prazos de comunicação de incidentes devem ser adequados e ter em devida consideração o tempo necessário para a avaliação e contenção do incidente pelas Entidades afectadas, pelo que, a previsão de prazos muito curtos e desajustados poderá conduzir a notificações incompletas e imprecisas, que terão de ser corrigidas posteriormente.	
Questão 7 "Concorda e considera adequado o conteúdo dos formulários respeitantes à	No que diz respeito ao conteúdo dos formulários, a remeter à ASF, aquando da ocorrência de um incidente severo relacionado com as TIC, submetem-se à apreciação do Supervisor os seguintes comentários/sugestões:	**Acolhido parcialmente.** Procedeu-se à alteração relativa ao campo "Origem do incidente".

notificação inicial e aos relatórios intercalar e final?"	• Notificação inicial: Na parte relativa à "*Descrição do incidente*", o formulário em apreço apresenta um Campo referente à "*Origem do incidente*", ao qual são associadas as seguintes observações: *"Escolha múltipla:* *a) Terceiro prestador de serviços;* *b) Entidade financeira;* *c)Não aplicável"* Na alínea b) transcrita supra, onde consta "*Entidade financeira*", sugere-se que passe a constar "*Outra Entidade Financeira*"; • Relatório intercalar: Relativamente aos Campos "*Tipo de Incidente*" e "*Ameaças e técnicas utilizadas pelo agente de ameaça*", incluídos na parte relativa à "*Descrição do Incidente*" do formulário em referência, sugere-se que os mesmos sejam alinhados com a taxonomia do CNCS - Centro Nacional de Cibersegurança (que se encontra disponível para consulta em: *https://www.cncs.gov.pt/pt/certpt/taxonomia/*), a qual implementa o previsto na taxonomia do *NIS Cooperation Group* (disponível em: https://ec.europa.eu/information_society/newsroom/image/document/2018-30/cybersecurity_incident_taxonomy_00CD828C-F851-AFC4-0B1B416696B5F710_53646.pdf). Em alternativa, propõe-se a adopção do Bloco "*Information on the incident*" do formulário ao Banco de Portugal/BCE. Ainda no que concerne ao conteúdo do relatório intercalar e à parte da "*Descrição do Incidente*", solicita-se, também, que os Campos referentes às "*Componentes da infraestrutura que apoiam processos de negócio*" e aos "*Sistemas afetados pelo incidente na*	Relativamente aos campos "Tipo de incidente" e "Ameaças e técnicas utilizadas pelo agente de ameaça", não se afigura adequado o alinhamento com a taxonomia do Centro Nacional Cibersegurança, pois importa acautelar uma adequada preparação para o cumprimento dos requisitos estabelecidos no Regulamento DORA, evitando, assim, a reformulação de sistemas de gestão de riscos a empreender para dar resposta à obrigação de comunicação de incidentes de carácter severo relacionados com as TIC no futuro próximo. Por outro lado, importa notar que o artigo 20.º do Regulamento DORA determina a necessidade de consulta da Agência da União Europeia para a Cibersegurança (ENISA) na elaboração do conteúdo das notificações de incidentes de caráter severo relacionados com as TIC, devendo ser a taxonomia dessa Autoridade a ser tida em conta (cf. relatório final do *Draft Regulatory Technical Standards on the content of the notification and reports for major incidents and significant cyber threats and determining the time limits for reporting major incidents*).

	infraestrutura" sejam suprimidos ou que o respectivo preenchimento seja opcional, dado que a informação em causa não é, de acordo com a opinião de Associadas da APFIPP, frequentemente considerada relevante, representando um esforço adicional desnecessário na elaboração do relatório. • Relatório final: Em relação ao conteúdo do relatório final, considera-se que o Campo "*Principal causa do incidente*" incorpora um juízo de valor e um elevado nível de detalhe, sugerindo-se, ao invés, a adopção da secção "*Vulnerabilities/weeknesses exposed*" do formulário de reporte do Banco de Portugal/BCE, assegurando, assim, uma maior uniformização entre os modelos de reporte. No caso de tal alteração não ser aceite, propõe-se, em alternativa, a utilização da estrutura que é descrita no ponto 5.1 do documento do NIS Cooperation Group, anteriormente citado (respectivo URL acima indicado) ou, mantendo-se o desenho previsto no Projecto de Norma, sugere-se que a taxonomia seja limitada ao segundo nível, ou seja, que a classificação seja efectuada ao nível dos números e das alíneas (i.e.: 1. – a) a c); 2. – a) a i); 3. – a) a g); 4. – a) a f); e 5. – a) a c)), sendo eliminadas as diversas subalíneas (associadas a 2.a) e a 2.c)). Por último, sugere-se que, à semelhança do que sucede com o Banco de Portugal (*vide* o disposto no primeiro parágrafo da segunda página da Instrução do Banco de Portugal n.º 21/2019, correspondente ao sexto parágrafo da respectiva introdução[1]), seja considerada, pela ASF, a possibilidade de criação de um ponto único de reporte, para o sector dos Fundos de Pensões, que tenha a responsabilidade de encaminhar os reportes de incidentes para o CNCS.	No que respeita ao campo "Componentes da infraestrutura que apoiam processos de negócio", não se afigura que o preenchimento pelas entidades seja demasiado oneroso, dada a natureza da resposta (escolha múltipla). No que concerne ao campo "Sistemas afetados pelo incidente na infraestrutura", aditou-se a opção de resposta "Sem informação disponível". Quanto ao campo "Principal causa do incidente", procedeu-se à redução do número de subcategorias e ao agrupamento de opções semelhantes, mas alerta-se para a aplicação de uma estrutura de resposta mais detalhada a partir da data de aplicação do Regulamento DORA. Em relação à sugestão de criação de um ponto único de reporte para o setor

[1] O parágrafo indicado refere o seguinte: "*(…) Na sequência do enquadramento supramencionado, entende-se necessário harmonizar os processos de reporte e agilizar a comunicação das entidades através de um ponto único de contacto que reencaminhará, se necessário e sem demora, a informação ao BCE e ao CNCS, consoante o âmbito e a natureza do incidente (…)*".

		segurador, que teria a responsabilidade de encaminhar os reportes de incidente para o Centro Nacional de Cibersegurança, nota-se que o quadro regulatório vigente neste âmbito não impõe uma obrigação de comunicação de incidentes à aquela Autoridade.
Artigo 8.º "Início de vigência"	Segundo o Documento de Consulta Pública que acompanha o Projecto de Norma, o diploma em apreciação, tem como objectivo, entre outros: "*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)*", propósito que é, igualmente, evidenciado no próprio Projecto de Norma, no âmbito do respectivo proémio. Muito embora se compreenda e corrobore a importância das Entidades Supervisionadas prepararem, com a devida antecedência, a implementação de quaisquer alterações jurídico-regulamentares, quer elas sejam de natureza nacional, quer de carácter comunitário, como é o caso da Regulamentação DORA, defende-se que as regras com origem europeia sejam aplicáveis a partir das datas previstas nos diplomas europeus, por forma a assegurar o desejável *level playing field* entre os diversos Estados-Membros, bem como entre os vários sectores abrangidos. Assim, e dado que o artigo 8.º do Projecto em análise, estipula que a Norma entra "*em vigor no dia imediato ao da sua aplicação*", solicita-se que o mencionado *level playing field* seja devidamente assegurado, por forma a que o sector dos Fundos de Pensões não seja prejudicado relativamente ao tempo de adaptação conferido, no plano comunitário, à implementação do DORA, colocando-o em desvantagem face aos seus concorrentes nacionais e europeus.	**Não acolhido.** Conforme referido no documento de consulta pública e no preâmbulo da norma regulamentar, esta tem também como objetivo a devida preparação e a antecipação dos requisitos estabelecidos neste âmbito pelo Regulamento DORA, e respetivos atos delegados e de execução, de forma mitigada e gradual 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. Neste sentido, não se afigura que a presente proposta acautele este objetivo. Nota-se, por outro lado, que a avaliação e gestão dos riscos relacionados com as TIC e notificação de incidentes desta

		natureza já deverá, naturalmente, estar a ser contemplada 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 apresenta no contexto atual de crescente digitalização e utilização de serviços de TIC de terceiros.