ASF
Autoridade de Supervisão
de Seguros e Fundos de Pensões

DOCUMENTO DE CONSULTA PÚBLICA

N.º 12/2021

Projeto de norma regulamentar relativa à segurança e governação das tecnologias da informação e comunicação e à subcontratação a prestadores de serviços de computação em nuvem

17 de dezembro de 2021

1. ENQUADRAMENTO

1.1 Objetivo e âmbito geral

Nos termos do artigo 16.º do Regulamento (UE) n.º 1094/2010, do Parlamento Europeu e do Conselho, de 24 de novembro, a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma ("EIOPA") publicou, em 6 de fevereiro de 2020, Orientações relativas à subcontratação a prestadores de serviços de computação em nuvem e, em 12 de outubro de 2020, Orientações sobre segurança e governação das tecnologias da informação e comunicação.

Com efeito, as tecnologias da informação e comunicação (TIC) são cada vez mais complexas e a frequência de incidentes relacionados com TIC (incluindo incidentes de cibersegurança) está igualmente a aumentar, bem como o impacto negativo de tais incidentes no funcionamento operacional das empresas de seguros e de resseguros. Por este motivo, a gestão dos riscos associados às TIC e à segurança é fundamental para que as empresas de seguros e de resseguros atinjam os seus objetivos em termos estratégicos, empresariais, operacionais e de reputação.

Adicionalmente, no setor segurador verifica-se uma utilização crescente das TIC na prestação de serviços de seguros e no funcionamento operacional das empresas de seguros e de resseguros, tornando as atividades vulneráveis a incidentes de segurança, incluindo ciberataques, pelo que importa garantir que essas empresas se encontram devidamente preparadas para gerir os riscos associados às TIC e à respetiva segurança.

Neste contexto, a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) elaborou o presente projeto de norma regulamentar que estabelece, para as empresas de seguros e de resseguros, requisitos e princípios gerais em matéria de segurança e governação das TIC e requisitos específicos em matéria de subcontratação a prestadores de serviços de computação em nuvem.

Os referidos requisitos acrescem aos requisitos gerais em matéria de governação estabelecidos na Norma Regulamentar n.º [sistema de governação das empresas de seguros e de resseguros], devendo ser aplicados de forma proporcional em relação à natureza, dimensão e complexidade dos riscos inerentes às atividades desenvolvidas pelas empresas de seguros e de resseguros.

1.2 Regime vigente

Nos artigos 31.º, 64.º, 72.º, 74.º, 75.º, 78.º e 149.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, encontram-se regulados os requisitos gerais em matéria de governação das empresas de seguros e de resseguros com sede em Portugal, bem como os relativos ao sistema de gestão de riscos e de controlo

interno, às funções de gestão de riscos, de verificação do cumprimento e de auditoria interna, e ainda à subcontratação de funções ou atividades de seguros ou de resseguros.

O referido regime é extensível às sucursais de empresas de seguros ou de resseguros de um país terceiro que exerçam a sua atividade em território português, por força do disposto na alínea *i)* do n.º 1 do artigo 215.º e da alínea *d)* do n.º 2 do artigo 232.º do RJASR, e aplicável, com as necessárias adaptações, ao nível dos grupos seguradores e resseguradores, nos termos do n.º 1 do artigo 283.º do RJASR.

O disposto nos artigos 258.º a 260.º, 266.º, 268.º a 271.º e 274.º do Regulamento Delegado n.º 2015/35 (UE), da Comissão, de 10 de outubro de 2014 ("Regulamento Delegado"), 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) é aplicável a empresas de seguros e de resseguros com sede em Portugal.

Em termos de regulamentação pela ASF com relevância no domínio do presente projeto de norma regulamentar, importa ainda referir a aplicação da Circular n.º 5/2021, de 7 de outubro, que divulga as Recomendações sobre Gestão da Continuidade de Negócio (revistas) aprovadas pelo Conselho Nacional de Supervisores Financeiros (CNSF).

1.3 Normas habilitantes

O RJASR prevê no n.º 7 do seu artigo 64.º a possibilidade de a ASF, através de norma regulamentar, detalhar os requisitos do sistema de governação.

Por força do disposto na alínea *d)* do n.º 2 do artigo 232.º do RJASR, às sucursais de empresas de seguros ou de resseguros de um país terceiro que exerçam a sua atividade em território português são extensíveis os requisitos relativos ao sistema de governação previstos nos artigos 63.º a 80.º do RJASR.

No domínio dos grupos seguradores e resseguradores, cabe considerar que nos termos do n.º 1 do artigo 283.º do RJASR são aplicáveis, com as necessárias adaptações, ao nível do grupo, os requisitos estabelecidos nos artigos 63.º a 80.º do RJASR.

Por sua vez, a Norma Regulamentar n.º [sistema de governação das empresas de seguros e de resseguros][1] prevê a regulação, em normativo próprio da ASF, da gestão de riscos de segurança das

[1] Cf. alínea *a)* do n.º 5 do artigo 29.º e artigo 75.º do projeto de norma regulamentar relativa ao sistema de governação das empresas de seguros e de resseguros, disponível no âmbito da Consulta Pública da ASF n.º 11/2021.

tecnologias da informação e comunicação e do regime aplicável à subcontratação a prestadores de serviços de computação em nuvem.

1.4 Fontes da iniciativa regulamentar

Em particular, serviram como principais fontes regulatórias à elaboração do projeto de norma regulamentar:

a) As Orientações da Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA), relativas à subcontratação a prestadores de serviços de computação em nuvem, de 6 de fevereiro de 2020[2];

b) As Orientações da EIOPA sobre segurança e governação das tecnologias da informação e comunicação, de 12 de outubro de 2020[3].

[2] Disponível em

https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/guidelines_on_outsourcing_to_cloud_service_providers_cor_pt.pdf

[3] Disponível em

https://www.eiopa.europa.eu/sites/default/files/publications/eiopa_guidelines/eiopa-gls-ict-security-and-governance-pt.pdf

2. PROJETO DE NORMA REGULAMENTAR E AVALIAÇÃO DE IMPACTO

A) Descrição do conteúdo da norma regulamentar

2.1. O projeto de norma regulamentar está organizado em quatro títulos: Título I ("Disposições Gerais"); Título II ("Segurança e governação das tecnologias da informação e comunicação"); Título III ("Subcontratação a prestadores de serviços de computação em nuvem") e Título IV ("Disposições finais e transitórias").

2.2. O Título I define o âmbito objetivo desta iniciativa regulatória, na qual se estabelecem os requisitos e princípios gerais que devem presidir ao desenvolvimento de mecanismos de governação e segurança das TIC e à subcontratação a prestadores de serviços de computação em nuvem pelas empresas de seguros e de resseguros em base individual e ao nível do grupo, em complemento ao regime estabelecido nos artigos 31.º, 64.º, 72.º, 74.º, 75.º, 78.º, 149.º e 283.º do RJASR e 258.º a 260.º, 266.º, 268.º a 271.º e 274.º do Regulamento Delegado, ao abrigo do disposto no n.º 7 do artigo 64.º do RJASR e tendo em consideração o teor das orientações da EIOPA sobre segurança e governação das tecnologias da informação e comunicação e as orientações da EIOPA relativas à subcontratação a prestadores de serviços de computação em nuvem.

Além disso, o Título I delimita o âmbito subjetivo de aplicação do projeto de norma regulamentar, prevendo que esta tem como destinatários: *a)* as empresas de seguros e de resseguros com sede em Portugal; *b)* as sucursais de empresas de seguros e de resseguros de um país terceiro que exerçam a sua atividade em território português; *c)* os grupos seguradores ou resseguradores, quando a ASF seja o supervisor do grupo; e *d)* os subgrupos cuja empresa-mãe de seguros ou de resseguros de topo, a sociedade gestora de participações no setor dos seguros de topo ou a companhia financeira mista de topo a nível nacional se encontre submetida a supervisão de grupo pela ASF, nos termos do artigo 256.º do RJASR.

O referido título prevê ainda um conjunto de definições consideradas relevantes para a aplicação do projeto de norma regulamentar, tendo primordialmente em conta as Orientações da EIOPA relativas à segurança e governação das tecnologias da informação e comunicação e à subcontratação a prestadores de serviços de computação em nuvem.

2.3. O Título II do projeto de norma regulamentar tem por base as Orientações da EIOPA sobre segurança e governação das tecnologias da informação e comunicação e desenvolve requisitos e

princípios gerais em matéria de segurança e governação das TIC. Está organizado em quatro capítulos: Capítulo I ("Requisitos gerais do sistema de governação das tecnologias da informação e comunicação"); Capítulo II ("Segurança da informação"); Capítulo III ("Gestão operacional dos sistemas e serviços de TIC") e Capítulo IV ("Continuidade das atividades").

2.3.1 No Capítulo I são definidos os requisitos gerais em matéria de governação das TIC, designadamente as responsabilidades do órgão de administração, a estratégia em matéria de TIC, a integração dos riscos associados às TIC, a segurança no sistema de gestão de riscos e a realização de auditorias periódicas.

No que se refere às responsabilidades do órgão de administração, releva, em especial, o dever de garantir que o sistema de governação gere de forma adequada os riscos associados às TIC e à segurança, nomeadamente assegurando: *a)* um número suficiente de colaboradores com as competências adequadas em matéria de TIC; *b)* uma formação regular e adequada para os colaboradores que desempenham funções relacionadas com as TIC, incluindo na área da segurança da informação; *c)* a definição, aprovação e supervisão da comunicação e aplicação da estratégia de TIC; e *d)* a aprovação da política de segurança da informação.

No referido capítulo prevê-se que a estratégia em matéria de TIC deve definir, no mínimo: *a)* a forma como as TIC devem evoluir de modo a apoiar e aplicar eficazmente a sua estratégia de negócio, *b)* a evolução da arquitetura das TIC, incluindo a dependência de prestadores de serviços; e *c)* os objetivos em matéria de segurança da informação, centrados nos sistemas e serviços de TIC, nos colaboradores e nos processos.

Para assegurar que a gestão dos riscos associados às TIC e à segurança deve ser parte integrante do sistema de gestão de riscos global das empresas de seguros e de resseguros, no Capítulo I indica-se que relativamente aos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, as empresas de seguros e de resseguros devem: *a)* dispor de um levantamento e efetuar uma identificação dos mesmos, de forma a traduzir a importância de cada um e as suas interdependências relativamente aos riscos associados às TIC e à segurança; *b)* identificar e medir todos os riscos pertinentes, associados às TIC e à segurança, a que estão expostos, e classificá-los, em termos de criticidade; *c)* avaliar os requisitos de proteção relativos, pelo menos, à confidencialidade, integridade e disponibilidade; e *d)* avaliar os riscos associados às TIC e à segurança, regularmente e de forma documentada.

Com base na avaliação do risco efetuada, as empresas de seguros e de resseguros devem definir e aplicar medidas para gerir os principais riscos identificados de forma a proteger os ativos de informação de acordo com a sua classificação.

No Capítulo I prevê-se, ainda, o estabelecimento de limites de tolerância aos riscos associados às TIC e à segurança, de acordo com a estratégia de risco da empresa de seguros ou de resseguros, e a elaboração de um relatório periódico, aprovado pelo órgão de administração, com os resultados do processo de gestão de riscos associados às TIC e à segurança.

Por último, devem ser realizadas auditorias periódicas à governação, aos sistemas e aos processos das empresas de seguros e de resseguros no âmbito dos riscos associados às TIC e à segurança.

2.3.2 O Capítulo II refere-se à segurança da informação e está organizado em três secções: Secção I ("Requisitos aplicáveis à segurança da informação"); Secção II ("Função de segurança da informação") e Secção III ("Segurança da informação e dos sistemas de informação").

Na Secção I estabelece-se que as empresas de seguros e de resseguros devem dispor de uma política de segurança da informação, indicando os principais elementos que devem ser, no mínimo, contemplados, e densifica o modo como a política dever ser comunicada e a quem deve ser aplicada.

Na Secção II regulamenta-se a função de segurança da informação, a sua independência e densificam-se as tarefas da função.

Por último, na Secção III identificam-se os procedimentos que as empresas de seguros e de resseguros devem definir, documentar e implementar de forma a garantir a segurança da informação e dos sistemas de informação.

Neste âmbito, estão incluídos requisitos sobre procedimentos para: *a)* controlo do acesso lógico ou para a segurança lógica, nomeadamente em matéria de identidade e gestão de acesso; *b)* definição, documentação e aplicação das medidas de segurança física das empresas de seguros e de resseguros; *c)* garantia da confidencialidade, integridade e disponibilidade dos sistemas de TIC e dos serviços de TIC; e *d)* monitorização continua das atividades que afetem a segurança da informação.

Para além disso, é regulamentado o dever de as empresas de seguros e de resseguros realizarem diversas revisões, avaliações e testes de segurança da informação e de criarem programas de formação no domínio da segurança da informação para todos os colaboradores, incluindo o órgão de administração.

2.3.3 O Capítulo III refere-se aos deveres que as empresas de seguros e de resseguros devem cumprir relativamente à gestão operacional de TIC. Neste âmbito, são desenvolvidos os requisitos aplicáveis: *a)* às operações de TIC e aos ativos de TIC; *b)* à gestão de problemas e incidentes em matéria de TIC; *c)* à gestão de projetos de TIC; *d)* à aquisição e desenvolvimento de sistemas de TIC; e *e)* à gestão de alterações em matéria de TIC.

No contexto da gestão de operações de TIC, antevê-se a necessidade de testagem regular dos procedimentos de segurança e de recuperação.

No que se refere à gestão de problemas e incidentes em matéria de TIC, o projeto de norma regulamentar prevê que deve ser implementado um processo de gestão de problemas e de incidentes que permita monitorizar e registar os incidentes operacionais ou de segurança e que permita a continuidade operacional ou a recuperação das funções e processos críticos sempre que ocorram perturbações, densificando os elementos que, no mínimo, devem encontrar-se estabelecidos.

No que respeita à gestão de projetos de TIC, antecipa-se a necessidade de as empresas de seguros e de resseguros implementarem uma metodologia de projetos de TIC que inclua considerações sobre requisitos de segurança independentes e seja dotada de um processo de governação e de uma liderança de execução de projetos adequados.

Em matéria de aquisição e desenvolvimento de sistemas de TIC, também é indicado que deve ser implementado, pelas empresas de seguros e de resseguros, um processo que regule a aquisição, o desenvolvimento e a manutenção de sistemas de TIC. Neste âmbito, o presente capítulo estabelece os procedimentos que, no mínimo, devem ser realizados aquando da aquisição e desenvolvimento de sistemas de TIC.

Quanto à gestão de alterações em matéria de TIC, regista-se a necessidade de estabelecimento e implementação de um processo de gestão de alterações em matéria de TIC para assegurar que todas as alterações introduzidas nos sistemas de TIC sejam registadas, avaliadas, testadas, aprovadas, autorizadas e aplicadas de forma controlada.

2.3.4 No Capítulo IV regulamentam-se os requisitos aplicáveis à gestão da continuidade de negócio no âmbito das TIC.

Neste âmbito, o projeto de norma regulamentar define que o órgão de administração é responsável por definir e aprovar a política de continuidade das TIC como parte da política global de gestão da continuidade de negócio da empresa e que esta deve ser comunicada e aplicável a todos os colaboradores relevantes e, se pertinente, aos prestadores de serviços.

O presente capítulo densifica também a integração das TIC no âmbito: *a)* da análise de impacto no negócio para avaliar a exposição das empresas de seguros e de resseguros a perturbações graves no negócio e os seus potenciais impactos; *b)* do planeamento da continuidade de negócio, que deve ter em consideração os riscos substanciais que possam ter um impacto negativo nos sistemas e serviços de TIC, e promover objetivos relacionados com a proteção dos processos e atividades; *c)* dos planos de resposta e recuperação com base nas análises de impacto no negócio e nos cenários plausíveis; e *d)* da testagem regular ao plano de continuidade de negócio.

Além disso, prevê-se a necessidade de as empresas de seguros e de resseguros disporem de medidas eficazes de comunicação de crises, de modo a que todas as partes interessadas relevantes, internas e externas, bem como os prestadores de serviços relevantes, sejam informados de forma atempada e adequada.

2.4. O Título III do projeto de norma regulamentar tem por base as Orientações da EIOPA relativas à subcontratação a prestadores de serviços de computação em nuvem e desenvolve os requisitos específicos em matéria de subcontratação a prestadores de serviços de computação em nuvem, estando organizado em três capítulos: Capítulo I ("Requisitos gerais da governação da subcontratação de serviços em nuvem"); Capítulo II ("Requisitos prévios ao acordo de subcontratação") e Capítulo III ("Acordo de subcontratação de serviços de computação em nuvem").

2.4.1 No Capítulo I regulamenta-se o dever de as empresas de seguros e de resseguros determinarem se um acordo com um prestador de serviços de computação em nuvem corresponde a uma subcontratação na aceção dada pela alínea *x)* do artigo 5.º do RJASR e de acordo com o disposto no artigo 78.º do RJASR, elencando os elementos a serem considerados para o efeito.

Ademais, estabelecem-se princípios gerais de governação para a subcontratação de serviços em nuvem, garantindo uma consistência com o sistema de governação das TIC e definem-se os requisitos aplicáveis às seguintes matérias: *a)* atualização da política de subcontratação e respetivos documentos; *b)* informação prévia à ASF; e *c)* requisitos documentais.

Em matéria de atualização, prevê-se que a política de subcontratação deve ser atualizada quando forem subcontratados prestadores de serviços de computação em nuvem, tendo em consideração as especificidades dos referidos serviços em determinados domínios.

No que se refere informação prévia à ASF, identificam-se as informações que devem ser prestadas no âmbito da subcontratação de funções e atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem.

No âmbito dos requisitos documentais, no Capítulo I estabelece-se que as empresas de seguros e de resseguros devem manter um registo dedicado de informações, permanentemente atualizado, sobre os seus acordos de subcontratação de serviços de computação em nuvem e densifica as informações que devem ser registadas, no caso de subcontratação de funções ou atividades operacionais fundamentais ou importantes.

2.4.2 No Capítulo II desenvolvem-se os requisitos prévios ao acordo de subcontratação, definindo, para o efeito, que as empresas de seguros e de resseguros devem realizar uma análise prévia à subcontratação, na qual importa: *a)* avaliar se o acordo diz respeito a funções e atividades operacionais fundamentais ou importantes; *b)* identificar e avaliar todos os riscos relevantes do acordo de subcontratação de serviços de computação em nuvem; *c)* aplicar o dever de diligência em relação ao potencial prestador de serviços de computação em nuvem; e *d)* identificar e avaliar os conflitos de interesses que a subcontratação possa implicar, em conformidade com os requisitos estabelecidos na alínea *b)* do n.º 3 do artigo 274.º do Regulamento Delegado.

Para além disso, no referido capítulo densificam-se: *a)* a avaliação das funções e atividades operacionais fundamentais ou importantes; *b)* a avaliação dos riscos dos acordos de subcontratação de serviços de computação em nuvem; e *c)* o dever de diligência em relação ao prestador de serviços de computação em nuvem.

2.4.3 No Capítulo III regulamentam-se os acordos de subcontratação de serviços de computação em nuvem, estabelecendo-se que os direitos e obrigações das empresas de seguros e de resseguros e do prestador de serviços de computação em nuvem devem ser claramente identificados e especificados num acordo escrito.

Para tal, são densificados os requisitos aplicáveis no âmbito dos acordos de subcontratação de serviços de computação em nuvem, nomeadamente em matéria de: *a)* requisitos contratuais; *b)* direitos de acesso e de auditoria; *c)* segurança dos dados e sistemas; *d)* subcontratação em cadeia de funções ou atividades operacionais fundamentais ou importantes; *e)* acompanhamento e supervisão de acordos de subcontratação de serviços de computação em nuvem; e *f)* direitos de rescisão e estratégias de saída.

No que se refere aos requisitos contratuais, e sem prejuízo da aplicação do disposto no artigo 274.º do Regulamento Delegado, desenvolvem-se os requisitos que o acordo escrito de subcontratação deve estabelecer.

No domínio do acordo de subcontratação de serviços de computação em nuvem, regulamenta-se que as empresas de seguros e de resseguros devem garantir que o acordo não limita o exercício efetivo dos direitos de acesso e de auditoria, nem as opções de controlo sobre os serviços em nuvem, densificando a forma como este direito pode ser exercido.

Prevê-se que as empresas de seguros e de resseguros devam garantir que os prestadores de serviços cumprem a legislação europeia e nacional aplicável, assim como as normas de segurança adequadas em matéria de TIC. Na eventualidade de os serviços se referirem a funções ou atividades operacionais fundamentais ou importantes, prevê-se que o acordo de subcontratação deve estabelecer requisitos específicos de segurança da informação e controlar regularmente o seu cumprimento. Ademais, elencam-se os elementos a considerar para efeitos da definição dos requisitos específicos.

O presente capítulo identifica, ainda, os elementos que devem ser incluídos no acordo de subcontratação de serviços de computação, quando se verifica a subcontratação em cadeia de funções ou atividades operacionais fundamentais ou importantes.

Caso sejam subcontratados serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes, define-se que as empresas de seguros e de resseguros devem dispor, ao abrigo do acordo de subcontratação em causa, de uma estratégia de saída. Neste quadro, estabelecem-se os procedimentos que as empresas devem adotar de modo a assegurar a possibilidade de rescindir o acordo de subcontratação sem prejudicar a continuidade e a qualidade dos serviços prestados.

2.5. Por último, como consequência do regime previsto no projeto de norma regulamentar, procede-se, no Título IV (“Disposições finais e transitórias”), à identificação do período de entrada em vigor e respetivos períodos transitórios para a aplicação de determinadas matérias.

B) Avaliação do impacto da norma regulamentar

Na ponderação do impacto desta intervenção normativa importa reconhecer que o respetivo cumprimento acarreta eventuais custos adicionais para as empresas de seguros e de resseguros, associados à implementação dos requisitos relativos à segurança e governação das tecnologias da

informação e comunicação, bem como à subcontratação a prestadores de serviços de computação em nuvem.

Em particular, antevê-se a necessidade de desenvolvimento do sistema de governação das empresas de seguros e de resseguros em razão da consagração de matérias inovatórias no projeto de norma regulamentar, nomeadamente as referentes: *a)* à definição de um plano estratégico e de um sistema para a gestão de riscos associados às TIC; *b)* à previsão regulamentar da função de segurança da informação e das operações de TIC; *c)* à elaboração de um relatório periódico com os resultados do processo de gestão de riscos associados às TIC e à segurança; *d)* à formação e sensibilização no domínio da segurança da informação; *e)* à revisão dos acordos de subcontratação de funções fundamentais ou importantes; e *f)* à implementação dos requisitos de documentação no âmbito do sistema de governação e, em especial, do sistema de gestão de riscos.

Ademais, antecipa-se a necessidade de elaboração de uma política de segurança da informação e a revisão das políticas que integram o sistema de governação, bem como de revisão dos sistemas de gestão de riscos e de controlo interno e das responsabilidades cometidas ao órgão de administração e à função de auditoria interna, em função do regime previsto no projeto de norma regulamentar.

Por outro lado, importa ter em conta que o novo regime previsto no presente projeto de norma regulamentar resulta essencialmente de iniciativa supranacional (mormente, das Orientações da EIOPA relativas à subcontratação a prestadores de serviços de computação em nuvem e das Orientações da EIOPA sobre segurança e governação das tecnologias da informação e comunicação).

Além disso, verifica-se uma dependência crescente das TIC na prestação de serviços de seguros e no funcionamento operacional das empresas de seguros e de resseguros, sendo estas tecnologias cada vez mais complexas e os incidentes no contexto da sua utilização mais frequentes. Por estas razões, o presente projeto de norma regulamentar visa assegurar a redução da vulnerabilidade a incidentes de segurança, incluindo ciberataques, bem como a otimização da gestão de riscos associados às TIC e à segurança no setor segurador, por forma a que as empresas de seguros e de resseguros atinjam os seus objetivos em termos estratégicos, empresariais, operacionais e de reputação.

Consequentemente, a ASF considera que o novo regime previsto no presente projeto de norma regulamentar reputa-se como essencial para a promoção da gestão sã e prudente das empresas de seguros e resseguros. A este nível, dá-se nota que o novo regime regulamentar importará também a adaptação das práticas de supervisão da ASF.

Ainda assim, cumpre sublinhar que os requisitos definidos no projeto de norma regulamentar devem ser aplicados de forma proporcional em relação à natureza, dimensão e complexidade das atividades desenvolvidas pelas empresas de seguros e de resseguros. O presente projeto de norma regulamentar, juntamente com o quadro regulatório nacional e europeu vigente, serve de enquadramento para essa implementação, estruturando-a e realçando objetivos fundamentais que não podem ser descurados pelas empresas de seguros e de resseguros.

3. PEDIDO DE COMENTÁRIOS

Solicita-se aos interessados que submetam os seus comentários sobre o projeto de norma regulamentar, por escrito, até ao dia 31 de janeiro de 2022, para o seguinte endereço de correio eletrónico: consultaspublicas@asf.com.pt, nos termos da tabela anexa.

Atendendo a razões de transparência, a ASF propõe-se publicar os contributos recebidos ao abrigo desta consulta pública. Assim, caso o respondente se oponha à referida publicação deve referi-lo expressamente no contributo que enviar.

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

ASF
Autoridade de Supervisão
de Seguros e Fundos de Pensões

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

TABELA DE COMENTÁRIOS

Projeto de norma regulamentar relativa à segurança e governação das tecnologias da informação e comunicação e à subcontratação a prestadores de serviços de computação em nuvem

Indicações:

Na coluna "Artigo", indicar o artigo (incluindo o número e a alínea, caso aplicável) do projeto de norma regulamentar relativa à segurança e governação das tecnologias da informação e comunicação e à subcontratação a prestadores de serviços de computação em nuvem;

Na coluna "Comentário", indicar o comentário ao artigo do projeto de norma regulamentar relativa à segurança e governação das tecnologias da informação e comunicação e à subcontratação a prestadores de serviços de computação em nuvem, incluindo qualquer proposta de redação alternativa;

Cada comentário/proposta de redação alternativa deve reportar-se a um artigo/número/alínea específicos;

Em cada 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 comentário/proposta de redação alternativa ou observação e será preenchida pela ASF.

Artigo	Comentário	Resolução