DOCUMENTO DE CONSULTA PÚBLICA

N.º 5/2024

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 no âmbito da gestão de fundos de pensões

14 de maio de 2024

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.

Neste contexto, a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) aprovou a Norma Regulamentar n.º 6/2022-R, de 7 de junho, dirigida às empresas de seguros e de resseguros, estabelecendo requisitos e princípios gerais em matéria de segurança e governação das tecnologias da informação e comunicação (TIC) e requisitos específicos em matéria de subcontratação a prestadores de serviços de computação em nuvem.

A gestão dos riscos associados às TIC e à segurança é fundamental para que as entidades supervisionadas pela ASF atinjam os seus objetivos em termos estratégicos, empresariais, operacionais e de reputação. Com efeito, as TIC são cada vez mais complexas e a potencialidade de incidentes relacionados com estas tecnologias, designadamente incidentes de cibersegurança, tem vindo igualmente a aumentar.

Considerando o potencial impacto negativo dos incidentes de cibersegurança e a utilização crescente das TIC no funcionamento operacional das sociedades gestoras de fundos de pensões, a ASF considera essencial que, em alinhamento com o regime estabelecido para as empresas de seguros e de resseguros, seja previsto um regime similar para as sociedades gestoras de fundos de pensões.

Note-se que a criação de um regime para as sociedades gestoras de fundos de pensões que assegure a devida preparação para a gestão de riscos associados às TIC e à respetiva segurança afigura-se fundamental para a preparação e antecipação de determinados requisitos estabelecidos 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[1]

[1] Disponível em

https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32022R2554&from=EN

("Regulamento (UE) 2022/2554"), e respetivos atos delegados, de execução, bem como outros atos jurídicos.

Com efeito, para além de garantir o alinhamento, desde já, com a Norma Regulamentar n.º 6/2022-R, de 7 de junho, o regime previsto na presente norma regulamentar garante a convergência da regulação das matérias relativas à segurança e governação das TIC e subcontratação a prestadores de serviços de computação em nuvem no âmbito da gestão de fundos de pensões com os requisitos previstos no Regulamento mencionado, aplicável a partir de 17 de janeiro de 2025, que visa o alcance de um elevado nível de resiliência operacional digital em relação a todas as entidades reguladas do setor financeiro.

Neste contexto, a ASF elaborou o presente projeto de norma regulamentar que estabelece, para as sociedades gestoras de fundos de pensões, 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 no projeto de norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões, visando promover uma atuação diligente, equitativa e transparente por parte das sociedades gestoras de fundos de pensões, tendo como objetivo uma adequada proteção do consumidor, e devendo ser aplicados de forma proporcional em relação à natureza, dimensão, escala e complexidade dos riscos inerentes às atividades desenvolvidas pelas sociedades gestoras de fundos de pensões.

Sublinha-se que as empresas de seguros que gerem fundos de pensões já se encontram sujeitas aos requisitos aplicáveis à atividade seguradora no âmbito da Norma Regulamentar n.º 6/2022-R, de 7 de junho. Sem prejuízo, a presente norma regulamentar complementa a aplicação das disposições em matéria de subcontratação a prestadores de serviços de computação em nuvem no que concerne à atividade de gestão de fundos de pensões das referidas empresas.

1.2 Regime vigente

Nos artigos 53.º, 108.º, 117.º, 118.º, 120.º, 121.º, 123.º, 150.º, 190.º e 196.º do RJFP 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,

encontram-se regulados os requisitos gerais em matéria de governação das sociedades gestoras de fundos de pensões, bem como os requisitos 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 gestão de fundos de pensões.

Em termos de regulamentação pela ASF, 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 RJFP prevê no n.º 8 do seu artigo 108.º a possibilidade de a ASF, através de norma regulamentar, detalhar os requisitos do sistema de governação.

Por sua vez, o projeto de norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões[2] prevê a regulação, em normativo próprio da ASF, da gestão de riscos de segurança das 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) A Norma Regulamentar n.º 6/2022-R, de 7 de junho, relativa à segurança e governação das tecnologias da informação e comunicação e subcontratação a prestadores de serviços de computação em nuvem[3];

---

[2] Cf. alínea *a)* do n.º 5 do artigo 30.º e artigo 67.º do projeto de norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões, disponível no âmbito da Consulta Pública da ASF n.º 4/2024 em https://www.asf.com.pt/w/consulta-publica-n4-2024.

[3] Disponível em https://files.diariodarepublica.pt/2s/2022/06/125000000/0006400092.pdf

b) O Parecer da EIOPA de 11 de julho de 2019 ["*Opinion on the supervision of the management of operational risks faced by IORPs*"][4].

Complementarmente, enquanto fontes regulatórias da Norma Regulamentar n.º 6/2022-R, de 7 de junho, referida *supra*, devem também aqui ser mencionadas as seguintes orientações da EIOPA:

a) Orientações relativas à subcontratação a prestadores de serviços de computação em nuvem, de 6 de fevereiro de 2020[5];

b) Orientações sobre segurança e governação das tecnologias da informação e comunicação, de 12 de outubro de 2020[6].

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").

Questão 1: *Considera que as disposições do projeto de norma regulamentar são articuláveis com as disposições da demais legislação e regulamentação pertinente para a governação das sociedades gestoras de fundos de pensões e das empresas de seguros que gerem fundos de pensões?*

Questão 2: *Considera que as disposições do projeto de norma regulamentar asseguram a criação de um regime que prepara e antecipa determinados requisitos estabelecidos pelo*

---

[4] Disponível em https://www.eiopa.europa.eu/document/download/adefa03e-2396-48d0-9725-ecca8d879868_en?filename=Opinion%20on%20the%20supervision%20of%20the%20management%20of%20operational%20risks%20faced%20by%20IORPs%20%28EIOPA-BoS-19-247%29

[5] Disponível em https://www.eiopa.europa.eu/publications/guidelines-outsourcing-cloud-service-providers_en

[6] Disponível em https://www.eiopa.europa.eu/publications/guidelines-information-and-communication-technology-security-and-governance_en

Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro, e respetivos atos jurídicos de implementação?

Questão 3: *Concorda que as disposições do projeto de norma regulamentar são aplicáveis de forma proporcional à natureza, dimensão, escala e complexidade dos riscos inerentes à atividade das sociedades gestoras de fundos de pensões e das empresas de seguros que gerem fundos de pensões permitindo que a respetiva capacidade e recursos disponíveis sejam ajustados de forma a garantir uma adequada aplicação dos requisitos estabelecidos?*

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 sociedades gestoras de fundos de pensões, em complemento ao regime estabelecido nos artigos 53.º, 108.º, 117.º, 118.º, 120.º, 121.º, 123.º, 150.º, 190.º e 196.º do RJFP bem como o regime previsto na futura norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões, ao abrigo do disposto no n.º 8 do artigo 108.º do RJFP 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 as sociedades gestoras de fundos de pensões autorizadas a gerir fundos de pensões nos termos da legislação em vigor. Adicionalmente, o referido título prevê ainda que os requisitos previstos no Título III são aplicáveis às empresas de seguros que gerem fundos de pensões no que concerne à atividade de gestão de fundos de pensões, sendo complementares às disposições em matéria de subcontratação a prestadores de serviços de computação em nuvem que lhes são aplicáveis nos termos do disposto na Norma Regulamentar n.º 6/2022-R, de 7 de junho.

O Título I estabelece 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.

Questão 4: *Concorda com o âmbito objetivo da norma regulamentar ou considera que algumas das matérias deveriam ser autonomizadas ou, ainda, que outras matérias deveriam também integrar esta norma regulamentar?*

Questão 5: *Concorda com o âmbito subjetivo da norma regulamentar ou considera que é necessária clarificação adicional quanto à aplicabilidade do projeto de norma regulamentar?*

Questão 6: *Concorda com o conjunto de definições previsto ou entende que a interpretação e aplicabilidade da norma regulamentar seriam facilitadas pelo aditamento de outras definições? Neste último caso, quais?*

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 sociedades gestoras de fundos de pensões, 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 sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões 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 sociedade gestora de fundos de pensões, 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 sociedades gestoras de fundos de pensões no âmbito dos riscos associados às TIC e à segurança.

Questão 7: *Concorda com os requisitos previstos no âmbito das responsabilidades do órgão de administração e com os elementos que devem ser definidos no âmbito da estratégia em matéria de TIC?*

Questão 8: *Concorda com os requisitos estabelecidos no âmbito da gestão dos riscos associados às TIC e à segurança, nomeadamente no que se refere aos procedimentos a adotar?*

Questão 9: *Concorda com o âmbito e a frequência das auditorias periódicas à governação, aos sistemas e aos processos das sociedades gestoras de fundos de pensões?*

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 sociedades gestoras de fundos de pensões 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 deve 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 sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões; *c)* garantia da confidencialidade, integridade e disponibilidade dos sistemas de TIC e dos serviços de TIC; e *d)* monitorização contínua das atividades que afetem a segurança da informação.

Para além disso, é regulamentado o dever de as sociedades gestoras de fundos de pensões 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.

Questão 10: *Concorda com os elementos e restantes requisitos previstos no âmbito da segurança da informação, nomeadamente no que se refere aos procedimentos que as sociedades gestoras devem cumprir para garantir a segurança da informação e dos sistemas de informação?*

2.3.3 O Capítulo III refere-se aos deveres que as sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões, 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.

Questão 11: *Concorda com os elementos, procedimentos mínimos e restantes requisitos previstos no âmbito dos deveres de gestão operacional dos sistemas e serviços de TIC?*

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 sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões disporem de medidas eficazes de comunicação de crises, por forma a que todas as partes interessadas relevantes, internas e externas, bem como os prestadores de serviços relevantes, sejam informados de forma atempada e adequada.

Questão 12: *Concorda com a previsão de requisitos aplicáveis à gestão da continuidade de negócio no âmbito das TIC, em particular no que se refere à sua integração em diferentes vertentes do negócio e aos deveres relativos à comunicação de crises?*

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 sociedades gestoras de fundos de pensões determinarem se um acordo com um prestador de serviços de computação em nuvem corresponde a uma subcontratação na aceção dada pela alínea *g*) do artigo 3.º da futura norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões e de acordo com o disposto no artigo 123.º do RJFP, 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 a informação prévia à ASF, identificam-se as informações que devem ser prestadas no âmbito da subcontratação de funções e atividades fundamentais ou importantes a prestadores de serviços de computação em nuvem.

No âmbito dos requisitos documentais, no Capítulo I estabelece-se que as sociedades gestoras de fundos de pensões 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 fundamentais ou importantes.

Questão 13: *Concorda com os princípios gerais em matéria de governação para a subcontratação de serviços de computação em nuvem?*

Questão 14: *Concorda com os requisitos estabelecidos no âmbito da atualização da política de subcontratação, nomeadamente com os domínios associados a essa atualização?*

Questão 15: *Concorda com o âmbito e a informação previstos no âmbito do reporte de informação prévia à ASF?*

Questão 16: *Concorda com as informações a registar no âmbito dos requisitos documentais previstos no artigo 33.º do projeto de norma regulamentar?*

2.4.2 No Capítulo II desenvolvem-se os requisitos prévios ao acordo de subcontratação, definindo, para o efeito, que as sociedades gestoras de fundos de pensões devem realizar uma análise prévia à subcontratação, na qual importa: *a)* avaliar se o acordo diz respeito a funções e atividades 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 o disposto na alínea *b)* do artigo 60.º da futura norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões.

Para além disso, no referido capítulo densificam-se: *a)* a avaliação das funções e atividades 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.

Questão 17: *Concorda com os elementos para avaliar as funções e atividades fundamentais ou importantes no âmbito da análise prévia à subcontratação?*

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 sociedades gestoras de fundos de pensões 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)* resubcontratação de funções ou atividades 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 62.º da futura norma regulamentar relativa ao sistema de governação das entidades

gestoras de fundos de pensões, 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 sociedades gestoras de fundos de pensões 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 sociedades gestoras de fundos de pensões 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 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 resubcontratação de funções ou atividades fundamentais ou importantes.

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

Questão 18: *Concorda com os requisitos contratuais que o acordo escrito de subcontratação deve identificar e especificar, incluindo os relativos aos direitos de acesso e auditoria e ao controlo do seu cumprimento no âmbito da segurança de informação?*

Questão 19: *Concorda com os elementos a incluir no acordo de subcontratação de serviços de computação nos casos em que se verifica a resubcontratação de funções ou atividades fundamentais ou importantes?*

Questão 20: *Concorda com os procedimentos, a frequência e os restantes requisitos previstos no âmbito do acompanhamento e supervisão de acordos de subcontratação de serviços de computação em nuvem?*

Questão 21: *Concorda com os procedimentos previstos no âmbito dos direitos de rescisão e estratégias de saída?*

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 sociedades gestoras de fundos de pensões, 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 sociedades gestoras de fundos de pensões 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 da adaptação de uma 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) ao setor dos fundos de pensões, mais concretamente da necessidade de alinhamento com o regime estabelecido para as empresas de seguros e de resseguros. A criação de um regime similar para as sociedades gestoras de fundos de pensões decorre da verificação da dependência crescente das TIC no funcionamento operacional das sociedades gestoras, sendo estas tecnologias cada vez mais complexas e os incidentes no contexto da sua utilização mais prováveis.

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 dos fundos de pensões, por forma a que as sociedades gestoras de fundos de pensões atinjam os seus objetivos em termos estratégicos, empresariais, operacionais e de reputação.

Adicionalmente, conforme anteriormente referido, a criação de um regime para as sociedades gestoras de fundos de pensões assegura a devida preparação e antecipação de determinados requisitos estabelecidos pelo Regulamento (UE) 2022/2554 e respetivos atos delegados, de execução, bem como outros atos jurídicos.

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 sociedades gestoras de fundos de pensões e para a estabilidade do setor financeiro. A este nível, dá-se nota de 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, escala e complexidade das atividades desenvolvidas pelas sociedades gestoras de fundos de pensões. 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 sociedades gestoras de fundos de pensões.

3. PEDIDO DE COMENTÁRIOS

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

Mais se informa que o presente processo de consulta pública decorre em paralelo com a Consulta Pública da ASF n.º 4/2024 do projeto de norma regulamentar relativa ao sistema de governação das entidades gestoras de fundos de pensões.

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

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