ASF
Autoridade de Supervisão
de Seguros e Fundos de Pensões

Não dispensa a consulta da
Norma Regulamentar publicada
em Diário da República

NORMA REGULAMENTAR N.º 6/2022-R, DE 7 DE JUNHO

SEGURANÇA E GOVERNAÇÃO DAS TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO E SUBCONTRATAÇÃO A PRESTADORES DE SERVIÇOS DE COMPUTAÇÃO EM NUVEM

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. As orientações constituem instrumentos jurídicos que se destinam a definir práticas coerentes e eficazes no contexto do Sistema Europeu de Supervisão Financeira e a garantir uma aplicação comum, uniforme e coerente da legislação da União Europeia.

De acordo com o estatuído no n.º 3 do citado artigo 16.º do referido Regulamento, cumpre às autoridades competentes e às instituições financeiras destinatárias das orientações emitidas pela EIOPA envidar os esforços necessários à observância dessas orientações.

Nos termos dos artigos 64.º, 72.º, 74.º, 75.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, e dos artigos 258.º a 260.º, 266.º e 268.º a 271.º do Regulamento Delegado (UE) n.º 2015/35 da Comissão, de 10 de outubro de 2014 ("Regulamento Delegado"), as empresas de seguros e de resseguros devem dispor de requisitos gerais em matéria de governação, bem como de um sistema de gestão de riscos e de controlo interno e de uma função de gestão de riscos, de verificação do cumprimento e de auditoria interna. Adicionalmente, as empresas de seguros e de resseguros devem cumprir o regime previsto nos artigos 31.º e 78.º do RJASR e no artigo 274.º do Regulamento Delegado quando subcontratam funções ou atividades de seguros ou de resseguros.

Por força do disposto na alínea *i)* do n.º 1 do artigo 215.º e na alínea *d)* do n.º 2 do artigo 232.º do RJASR, às sucursais de empresas de seguros e de resseguros de um país terceiro que exerçam a sua atividade em território português são extensíveis os requisitos relativos ao sistema de governação.

No domínio dos grupos seguradores e resseguradores, importa 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 alínea *a)* do n.º 5 do artigo 30.º e o artigo 77.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, preveem a regulação, em normativo próprio da Autoridade de Supervisão de Seguros e Fundos de Pensões (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.

Assim, pela presente norma regulamentar procede-se ao estabelecimento dos requisitos e princípios gerais em matéria de segurança e governação das tecnologias da informação e comunicação (TIC) e ao estabelecimento de requisitos específicos em matéria de subcontratação a prestadores de serviços de computação em nuvem.

As 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, 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.

Considerando a necessidade de preparação para os riscos cibernéticos[1] e de um quadro de cibersegurança sólido por parte das empresas de seguros e de resseguros, a presente norma regulamentar abrange igualmente a cibersegurança no âmbito das medidas de segurança da informação dessas empresas.

[1] Cf. Léxico Cibernético do Conselho de Estabilidade Financeira, de 12 de novembro de 2018, https://www.fsb.org/wp-content/uploads/P121118-1.pdf, que prevê uma definição de «risco cibernético».

As disposições da presente norma regulamentar são aplicáveis de forma proporcional à natureza, dimensão e complexidade dos riscos inerentes à atividade das empresas de seguros e de resseguros.

O projeto da presente norma regulamentar esteve em processo de consulta pública, nos termos do artigo 47.º dos Estatutos da ASF, aprovados pelo Decreto-Lei n.º 1/2015, de 6 de janeiro, tendo sido considerados os contributos recebidos nos termos do Relatório da Consulta Pública n.º 12/2021.

A Autoridade de Supervisão de Seguros e Fundos de Pensões, ao abrigo do disposto no n.º 7 do artigo 64.º do RJASR, bem como na alínea *a)* do n.º 3 do artigo 16.º dos seus Estatutos, aprovados pelo Decreto-Lei n.º 1/2015, de 6 de janeiro, emite a seguinte Norma Regulamentar:

TÍTULO I

Disposições gerais

Artigo 1.º

Objeto

A presente norma regulamentar estabelece os requisitos e princípios gerais que devem presidir ao desenvolvimento de mecanismos de governação e segurança das tecnologias de informação e comunicação (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 regime jurídico de acesso e exercício da atividade seguradora e resseguradora (RJASR), aprovado pela Lei n.º 147/2015, de 9 de setembro, e 258.º a 260.º, 266.º, 268.º a 271.º e 274.º do Regulamento Delegado (UE) n.º 2015/35 da Comissão, de 10 de outubro de 2014 ("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 Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (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.

Artigo 2.º

Âmbito de aplicação

A presente norma regulamentar aplica-se:

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

b) Às sucursais de empresas de seguros e de resseguros de um país terceiro que exerçam a sua atividade em território português;

c) Aos grupos seguradores ou resseguradores, na aceção da alínea *c)* do artigo 252.º do RJASR, quando a Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF) seja o supervisor do grupo;

d) Aos 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.

Artigo 3.º

Definições

Para efeitos da presente norma regulamentar, considera-se:

a) «Ativo de informação», um conjunto de informações, tangíveis ou intangíveis, que devam ser protegidas;

b) «Ativo de TIC», um ativo de programas informáticos ou de equipamentos informáticos que se encontra no ambiente empresarial;

c) «Ciberataque», qualquer tipo de pirataria informática que conduza a uma tentativa prejudicial ou maliciosa de destruir, expor, alterar, incapacitar, roubar ou obter acesso não autorizado ou fazer uma utilização não autorizada de um ativo de informação que tenha como alvo os sistemas de TIC;

d) «Cibersegurança», a preservação da confidencialidade, integridade e disponibilidade de informações ou sistemas de informação através de meios cibernéticos;

e) «Confidencialidade», a característica que inibe a disponibilização ou a divulgação de informação a particulares, entidades, processos ou sistemas não autorizados;

f) «Disponibilidade», a característica de ser acessível e utilizável prontamente a pedido por uma entidade autorizada;

g) «Incidente operacional ou de segurança», um evento único ou uma série de eventos conexos e não previstos que têm, ou poderão vir a ter, um impacto negativo na integridade, disponibilidade e confidencialidade dos serviços e sistemas de TIC;

h) «Integridade», a característica de exatidão e integralidade;

i) «Nuvem comunitária», uma infraestrutura em nuvem disponível para utilização exclusiva por uma comunidade específica de empresas de seguros ou de resseguros, incluindo várias empresas de um único grupo;

j) «Nuvem híbrida», uma infraestrutura em nuvem composta por duas ou mais infraestruturas em nuvem distintas;

k) «Nuvem privada», uma infraestrutura em nuvem disponível para utilização exclusiva por uma única empresa de seguros ou de resseguros;

l) «Nuvem pública», uma infraestrutura em nuvem disponível para utilização em sistema aberto pelo público em geral;

m) «Prestador de serviços», uma entidade terceira que desempenha, no todo ou em parte, um processo, um serviço ou uma atividade ao abrigo de um acordo de subcontratação;

n) «Prestador de serviços de computação em nuvem», um prestador de serviços, tal como definido na alínea anterior, responsável pela prestação de serviços de computação em nuvem ao abrigo de um acordo de subcontratação;

o) «Projetos de TIC», qualquer projeto, ou parte do mesmo, em que os serviços e sistemas de TIC sejam alterados, substituídos ou aplicados;

p) «Proprietário do ativo», a pessoa ou entidade com responsabilidade e autoridade sobre um ativo de informação e de TIC;

q) «Riscos associados às TIC e à segurança», enquanto subcomponente do risco operacional, risco de perdas por violação da confidencialidade, falta de integridade de sistemas e dados, inadequação ou indisponibilidade de sistemas e dados ou incapacidade para

alterar as TIC num período e por um custo razoáveis quando o ambiente ou os requisitos de negócio sofram alterações, incluindo riscos cibernéticos e riscos de segurança da informação resultantes de eventos externos ou de processos internos inadequados ou deficientes, incluindo ciberataques ou uma segurança física inadequada;

r) «Segurança da informação», a preservação da confidencialidade, integridade e disponibilidade de informações ou dos sistemas de informação, podendo ainda envolver outras características, tais como autenticidade, responsabilidade, não rejeição e fiabilidade;

s) «Serviços de computação em nuvem», os serviços fornecidos através de computação em nuvem, ou seja, um modelo que oferece um acesso em rede em qualquer local, prático e a pedido a um conjunto partilhado de recursos informáticos configuráveis, tais como, redes, servidores, sistemas de armazenamento, aplicações e serviços, que podem ser rapidamente disponibilizados e libertados com um esforço mínimo de gestão ou de interação com o fornecedor de serviços;

t) «Serviços de TIC», os serviços fornecidos através de sistemas e prestadores de serviços de TIC a um ou mais utilizadores internos ou externos;

u) «Sistemas de TIC», o conjunto de aplicações, serviços, ativos de tecnologia da informação, ativos de TIC ou outros componentes do tratamento da informação, que inclui o ambiente de operação;

v) «Testes de penetração baseados em ameaças», uma tentativa controlada de comprometer a ciber-resiliência de uma entidade mediante a simulação de táticas, técnicas e procedimentos de autores de ameaças reais, tendo por base informações sobre ameaças específicas e centrando-se nas pessoas, processos e tecnologias de uma entidade, com conhecimento prévio mínimo e impacto reduzido nas atividades;

w) «Vulnerabilidade», uma deficiência, suscetibilidade ou falha de um ativo ou controlo que pode ser explorada por uma ou mais ameaças.

TÍTULO II

Segurança e governação das tecnologias da informação e comunicação

CAPÍTULO I

Requisitos gerais do sistema de governação das tecnologias da informação e comunicação

Artigo 4.º

Responsabilidades do órgão de administração

1 — O órgão de administração é globalmente responsável por estabelecer um sistema eficaz para a gestão dos riscos associados às TIC e à segurança como parte do sistema de gestão global dos riscos da empresa de seguros ou de resseguros, conforme previsto no artigo 6.º

2 — O órgão de administração deve ainda garantir que o sistema de governação, nomeadamente o sistema de gestão de riscos e de controlo interno, gere de forma adequada os riscos associados às TIC e à segurança da própria empresa de seguros ou de resseguros.

3 — Compete, em especial, ao órgão de administração:

a) Assegurar, numa base contínua, um número suficiente de colaboradores com as competências adequadas para apoiar as necessidades operacionais de TIC e os processos de gestão de riscos associados às TIC e à segurança, assim como para garantir a aplicação da estratégia da empresa de seguros ou de resseguros em matéria de TIC;

b) Garantir, aos colaboradores que desempenham funções relacionadas com as TIC, uma formação regular e adequada ao exercício das suas funções, incluindo na área da segurança da informação;

c) Definir e aprovar a estratégia de TIC, formalizada por escrito, como parte integrante da estratégia de negócio global da empresa de seguros ou de resseguros;

d) Supervisionar a comunicação e aplicação da estratégia de TIC referida na alínea anterior;

e) Aprovar a política de segurança da informação prevista no artigo 8.º

4 — O órgão de administração deve garantir que os recursos disponíveis são adequados para o cumprimento dos requisitos previstos no número anterior.

Artigo 5.º

Estratégia em matéria de tecnologias da informação e comunicação

1 — A estratégia das empresas de seguros e de resseguros em matéria de TIC deve definir, no mínimo:

a) A forma como as TIC das empresas devem evoluir de modo a apoiar e aplicar eficazmente a sua estratégia de negócio, incluindo a evolução da estrutura organizacional, os modelos de negócio, o sistema de TIC e as suas principais dependências relativamente aos prestadores de serviços;

b) A evolução da arquitetura das TIC, incluindo a dependência de prestadores de serviços;

c) Objetivos claramente identificados em matéria de segurança da informação, centrados nos sistemas e serviços de TIC, nos colaboradores e nos processos.

2 — As empresas de seguros e de resseguros devem garantir que a estratégia em matéria de TIC é aplicada, adotada e comunicada atempadamente a todos os colaboradores e prestadores de serviços relevantes, sempre que aplicável e relevante.

3 — As empresas de seguros e de resseguros devem estabelecer um processo para monitorizar e medir a eficácia da implementação da estratégia em matéria de TIC e proceder à sua revisão e atualização de forma regular.

Artigo 6.º

Sistema de gestão de riscos

1 — 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.

2 — Nos termos e para efeitos do número anterior, as empresas de seguros e de resseguros devem:

a) Dispor de um levantamento e efetuar uma identificação dos respetivos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, 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 expostas e classificar, em termos de criticidade, os processos e atividades de negócio, as funções de negócio, as tarefas e os ativos, tais como, ativos de informação e ativos de TIC, identificados;

c) Avaliar os requisitos de proteção relativos, pelo menos, à confidencialidade, integridade e disponibilidade dos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, identificados nos termos da alínea anterior;

d) Avaliar os riscos associados às TIC e à segurança, o que deve ser realizado e documentado regularmente, bem como efetuado antes de qualquer alteração significativa na infraestrutura, nos processos ou nos procedimentos que afete os processos e atividades de negócio, as funções de negócio, as tarefas e os ativos, tais como, ativos de informação e ativos de TIC.

3 — Para efeitos do disposto nas alíneas *b)* e *c)* do número anterior:

a) Os métodos utilizados para determinar a criticidade e o nível de proteção exigido, nomeadamente no que se refere aos objetivos no domínio da proteção da integridade, disponibilidade e confidencialidade, devem garantir que os requisitos resultantes em matéria de proteção são coerentes e abrangentes;

b) A medição dos riscos associados às TIC e à segurança deve ser efetuada com base nos critérios definidos em matéria de riscos associados às TIC e à segurança, tendo em conta a criticidade dos respetivos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, a extensão das vulnerabilidades conhecidas e os incidentes anteriores que afetaram as empresas de seguros ou de resseguros;

c) Os proprietários dos ativos, responsáveis pela sua classificação, devem ser identificados.

4 — Com base na avaliação do risco efetuada nos termos da alínea *d)* do n.º 2, as empresas de seguros e de resseguros devem definir e aplicar medidas para gerir os principais riscos identificados associados às TIC e à segurança e de forma a proteger os ativos de informação de acordo com a sua classificação.

5 — O disposto no número anterior deve incluir a definição de medidas para gerir os restantes riscos residuais.

6 — Para efeitos do disposto nos n.os 2 a 6, devem ser estabelecidos 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.

7 — Para além do disposto no número anterior, deve ser elaborado um relatório periódico, aprovado pelo órgão de administração, com os resultados do processo de gestão de riscos associados às TIC e à segurança.

8 — Os resultados do processo de gestão dos riscos associados às TIC e à segurança devem ser incluídos no processo de gestão do risco operacional, como parte integrante da gestão global de riscos das empresas de seguros e de resseguros.

Artigo 7.º

Auditoria

1 — A governação, os sistemas e os processos das empresas de seguros e de resseguros no âmbito dos riscos associados às TIC e à segurança devem ser periodicamente objeto de auditoria, em consonância com o respetivo plano de auditoria, previsto no artigo 271.º do Regulamento Delegado.

2 — A auditoria referida no número anterior deve ser realizada, de forma independente, por auditores com competências, conhecimentos e experiência suficientes no domínio dos riscos associados às TIC e à segurança, com vista a prestar uma garantia independente da sua eficácia, e os seus resultados devem ser reportados ao órgão de administração.

3 — A frequência e o detalhe das auditorias devem ser proporcionais aos riscos associados às TIC e à segurança.

CAPÍTULO II

Segurança da informação

SECÇÃO I

Requisitos aplicáveis à segurança da informação

Artigo 8.º

Política e medidas de segurança da informação

1 — Em complemento ao disposto no artigo 10.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, as empresas de seguros e de resseguros devem dispor de uma política de segurança da informação reduzida a escrito e aprovada pelo órgão de administração, que inclua uma definição dos principais princípios e regras para a proteção da confidencialidade, integridade e disponibilidade da informação das empresas, de forma a apoiar a aplicação da estratégia em matéria de TIC.

2 — A política referida no número anterior deve contemplar de modo claro, pelo menos, os seguintes elementos:

a) Os principais objetivos;

b) A descrição das principais funções e responsabilidades da gestão da segurança da informação;

c) As tarefas a executar e o colaborador ou função responsável pelas mesmas;

d) Os requisitos aplicáveis ao colaborador ou função referidos na alínea anterior, aos processos e à tecnologia relacionada com a segurança da informação;

e) A atribuição a todos os colaboradores da empresa de seguros ou de resseguros da responsabilidade em garantir a segurança da informação da empresa.

3 — A política de segurança da informação é aplicável a todos os colaboradores da empresa de seguros ou de resseguros e, sempre que relevante e aplicável, deve ser comunicada e aplicável, no todo ou em parte, aos prestadores de serviços.

4 — As empresas de seguros e de resseguros devem assegurar, em repositório dedicado para o efeito e de fácil acessibilidade, a divulgação interna da política de segurança da informação a todos os colaboradores.

5 — As empresas de seguros e de resseguros devem estabelecer e implementar procedimentos e medidas de segurança da informação específicos de forma a atenuar os riscos associados às TIC e à segurança a que estão expostas.

6 — Os procedimentos e medidas de segurança da informação referidos no número anterior devem incluir todos os processos previstos na presente norma regulamentar, caso aplicável.

SECÇÃO II

Função de segurança da informação

Artigo 9.º

Tarefas da função de segurança da informação

1 — As empresas de seguros e de resseguros devem estabelecer, no âmbito do respetivo sistema de governação e de acordo com o princípio da proporcionalidade, uma função de segurança da informação, cujas responsabilidades devem ser atribuídas a uma pessoa designada, a qual deve reportar ao órgão de administração.

2 — A função de segurança da informação deve desempenhar as seguintes tarefas:

a) Apoiar o órgão de administração na definição e atualização da política de segurança da informação da empresa de seguros ou de resseguros e controlar a sua execução;

b) Informar e aconselhar o órgão de administração numa base regular e *ad-hoc* relativamente ao estado da segurança da informação e à sua evolução;

c) Acompanhar e rever a aplicação das medidas de segurança da informação;

d) Garantir o cumprimento dos requisitos em matéria de segurança da informação quando haja recurso a prestadores de serviços;

e) Garantir que todos os colaboradores e prestadores de serviços com acesso à informação e aos sistemas são devidamente informados sobre a política de segurança da informação, designadamente através de sessões de formação e de sensibilização no domínio da segurança da informação;

f) Coordenar a análise de incidentes operacionais ou de segurança e informar o órgão de administração dos incidentes pertinentes.

Artigo 10.º

Independência da função de segurança da informação

As empresas de seguros e de resseguros devem assegurar a independência e a objetividade da função de segurança da informação, separando-a devidamente do desenvolvimento e de processos operacionais no âmbito das TIC.

SECÇÃO III

Segurança da informação e dos sistemas de informação

Artigo 11.º

Segurança lógica

1 — As empresas de seguros e de resseguros devem definir, documentar e implementar procedimentos para controlo do acesso lógico ou para a segurança lógica, nomeadamente em matéria de identidade e gestão de acesso, em consonância com os requisitos de proteção previstos no artigo 6.º

2 — Os procedimentos definidos nos termos do número anterior devem abranger controlos para a monitorização de anomalias e devem ser aplicados, executados, monitorizados e revistos periodicamente.

3 — Os procedimentos implementados devem ainda incluir, pelo menos, os seguintes elementos:

a) Necessidade de tomar conhecimento, menor privilégio e segregação de funções, à luz dos quais as empresas de seguros e de resseguros devem:

i) Gerir os direitos de acesso, incluindo o acesso remoto aos ativos de informação e aos seus sistemas de apoio, com base na necessidade de tomar conhecimento;

ii) Conceder aos utilizadores, incluindo utilizadores técnicos, os direitos mínimos de acesso estritamente necessários para a execução das suas funções, conforme o princípio do menor privilégio, de forma a evitar o acesso injustificado aos dados ou para impedir a atribuição de combinações de acesso que possam ser utilizadas para contornar os controlos implementados, conforme o princípio da segregação de funções;

b) Responsabilização dos utilizadores, incluindo utilizadores técnicos, à luz da qual a utilização de contas de utilizador genéricas e partilhadas devem, na medida do possível, ser limitadas, devendo ainda ser assegurada a identificação permanente dos utilizadores e o rastreamento da sua origem como uma tarefa autorizada ou a uma pessoa singular responsável pelas ações executadas nos sistemas de TIC;

c) Direitos de acesso privilegiado, segundo os quais as empresas de seguros e de resseguros devem aplicar controlos rigorosos sobre o acesso privilegiado aos sistemas, limitando estritamente e supervisionando de perto as contas com um elevado nível de acesso aos sistemas, designadamente, as contas de administrador;

d) Acesso remoto, à luz do qual o acesso remoto administrativo aos sistemas críticos de TIC apenas deve ser concedido com base na necessidade de tomar conhecimento e desde que sejam utilizadas soluções de autenticação forte, de forma a assegurar uma comunicação segura e reduzir o risco;

e) Registo das atividades do utilizador, incluindo utilizadores técnicos, de acordo com o qual as atividades dos utilizadores devem ser registadas e monitorizadas de uma forma proporcional ao risco, abrangendo, no mínimo, as atividades dos utilizadores privilegiados;

f) Gestão de acesso, à luz da qual os direitos de acesso devem ser concedidos, revogados e alterados atempadamente, de acordo com rotinas de aprovação predefinidas, sempre que o proprietário do ativo de informação esteja envolvido, devendo ser imediatamente revogados caso o acesso deixe de ser necessário;

g) Avaliação do acesso, à luz da qual os direitos de acesso devem ser revistos periodicamente para assegurar que os utilizadores, incluindo utilizadores técnicos, não possuem privilégios excessivos e que os direitos de acesso são revogados quando já não são necessários;

h) A concessão, a alteração e a revogação dos direitos de acesso, as quais devem ser documentadas de um modo que facilite a sua compreensão e análise;

i) Métodos de autenticação suficientemente sólidos, que devem ser aplicados pelas empresas de seguros e de resseguros para garantir o cumprimento adequado e eficaz das políticas e procedimentos de controlo de acesso.

4 — Nos termos da alínea *e)* do número anterior, os registos de acesso devem ser protegidos para evitar alterações ou eliminações não autorizadas e mantidos durante um período proporcional à criticidade das funções das empresas de seguros e de resseguros, aos processos de apoio e ativos de informação identificados, sem prejuízo dos requisitos de retenção estabelecidos no âmbito da legislação nacional ou europeia, devendo essas empresas utilizar esta informação para facilitar a identificação e investigação de atividades anómalas que tenham sido detetadas durante a prestação de serviços.

5 — Os métodos de autenticação referidos na alínea *i)* do n.º 3 devem ser proporcionais à criticidade dos sistemas de TIC, da informação ou do processo a que se acede, e devem incluir, no mínimo, palavras-passe seguras ou métodos de autenticação mais fortes, tais como a autenticação de dois fatores, com base no risco pertinente.

6 — O acesso eletrónico através de aplicações a dados e sistemas de TIC deve ser limitado ao mínimo necessário para prestar o serviço em causa.

Artigo 12.º

Segurança física

1 — As medidas de segurança física das empresas de seguros e de resseguros, designadamente, de proteção contra falhas de energia, incêndios, água e acesso físico não autorizado, devem ser definidas, documentadas e aplicadas tendo em vista a proteção das suas instalações, dos centros de dados e das áreas sensíveis contra o acesso não autorizado e os riscos ambientais.

2 — O acesso físico aos sistemas de TIC deve ser permitido apenas a pessoas autorizadas.

3 — A autorização a que se refere o número anterior deve ser atribuída de acordo com as tarefas e responsabilidades da pessoa em causa, bem como limitada a pessoas que sejam devidamente habilitadas e supervisionadas.

4 — O acesso físico aos sistemas de TIC deve ser revisto regularmente, a fim de garantir que os direitos de acesso desnecessários são imediatamente revogados.

5 — Consideram-se medidas adequadas de proteção contra os perigos ambientais as medidas que sejam proporcionais à importância dos edifícios e à criticidade das operações ou dos sistemas de TIC localizados nesses edifícios.

Artigo 13.º

Segurança das operações de TIC

1 — As empresas de seguros e de resseguros devem aplicar procedimentos para garantir a confidencialidade, integridade e disponibilidade dos sistemas de TIC e dos serviços de TIC, com vista a minimizar o impacto das questões de segurança na prestação de serviços destes serviços.

2 — Os procedimentos referidos no número anterior devem incluir, de forma adequada, as seguintes medidas:

a) Identificação de potenciais vulnerabilidades, que devem ser avaliadas e corrigidas, assegurando que os sistemas de TIC estão atualizados, incluindo os programas informáticos fornecidos pelas empresas de seguros e de resseguros aos seus utilizadores internos e externos, através da implementação de correções críticas de segurança, como atualizações das definições de antivírus, ou da aplicação de controlos compensatórios;

b) Aplicação de configurações de base seguras para todos os componentes críticos, tais como sistemas operativos, bases de dados, encaminhadores («*routers*») e comutadores;

c) Aplicação de segmentação de rede, sistemas de prevenção de perda de dados e cifragem do tráfego de rede, de acordo com a classificação dos ativos de informação;

d) Aplicação da proteção de terminais, incluindo servidores, estações de trabalho e dispositivos móveis;

e) Garantia da existência de mecanismos de verificação da integridade dos sistemas de TIC;

f) Cifragem dos dados armazenados e em trânsito, de acordo com a classificação dos ativos de informação.

3 — Para efeitos do disposto na alínea *d)* do número anterior, as empresas de seguros e de resseguros devem determinar se um terminal cumpre as normas de segurança definidas pelas próprias antes de lhe ser concedido acesso à rede empresarial.

Artigo 14.º

Monitorização da segurança

1 — As empresas de seguros e de resseguros devem criar e aplicar procedimentos e processos para monitorizar continuamente as atividades que afetem a segurança da informação.

2 — A monitorização a que se refere o número anterior deve abranger, pelo menos:

a) Fatores internos e externos, incluindo as funções administrativas das empresas de seguros e de resseguros e das TIC;

b) Operações efetuadas por prestadores de serviços, outras entidades e utilizadores internos;

c) Potenciais ameaças internas e externas.

3 — No âmbito da monitorização referida no n.º 1, as empresas de seguros e de resseguros devem aplicar recursos adequados e eficazes para detetar, comunicar e dar resposta a atividades anómalas e ameaças, tais como intrusões físicas ou lógicas, violações da confidencialidade, integridade e disponibilidade dos ativos de informação, códigos maliciosos e vulnerabilidades publicamente conhecidas em termos de programas informáticos ou de equipamentos informáticos.

4 — A comunicação decorrente da monitorização da segurança deve ajudar as empresas de seguros e de resseguros a compreender a natureza dos incidentes operacionais ou de segurança, a identificar tendências e a apoiar as suas investigações internas, permitindo tomadas de decisão adequadas.

Artigo 15.º

Revisões, avaliação e testes da segurança da informação

1 — Por forma a garantir a identificação efetiva de vulnerabilidades nos respetivos sistemas e serviços de TIC, as empresas de seguros e de resseguros devem realizar diversas revisões, avaliações e testes de segurança da informação, tais como análises de lacunas em relação às normas de segurança da informação, revisões de conformidade, auditorias internas e externas dos sistemas de informação ou revisões da segurança física.

2 — As empresas de seguros e de resseguros devem estabelecer e aplicar um quadro de testes de segurança da informação que valide a robustez e a eficácia das medidas de segurança da informação, devendo garantir que tal quadro tem em consideração as ameaças e vulnerabilidades identificadas através da monitorização das ameaças e do processo de avaliação dos riscos associados às TIC e à segurança.

3 — Os testes de segurança da informação devem ser realizados regularmente.

4 — O âmbito, a frequência e o método dos testes de segurança da informação, designadamente, testes de penetração, incluindo testes de penetração baseados em ameaças, devem ser proporcionais ao nível de risco identificado.

5 — Sem prejuízo do disposto no número anterior, os testes dos sistemas críticos de TIC e a verificação de vulnerabilidades devem ser realizados anualmente.

6 — Os testes de segurança da informação devem ser efetuados de modo seguro, por pessoas independentes com conhecimentos, competências e experiência suficientes para testar as medidas de segurança da informação.

7 — As empresas de seguros e de resseguros devem garantir que os testes às medidas de segurança são realizados no caso de alterações da infraestrutura, dos processos ou dos procedimentos, bem como caso sejam efetuadas alterações devido a incidentes operacionais ou de segurança de caráter severo ou devido ao lançamento de aplicações críticas novas ou significativamente alteradas.

8 — As empresas de seguros e de resseguros devem monitorizar e avaliar os resultados dos testes de segurança e atualizar as suas medidas de segurança em conformidade, sem demora indevida, no caso dos sistemas críticos de TIC.

Artigo 16.º

Formação e sensibilização no domínio da segurança da informação

1 — As empresas de seguros e de resseguros devem criar programas de formação no domínio da segurança da informação para todos os colaboradores, incluindo o órgão de administração, a fim de assegurar que os mesmos dispõem de formação para desempenhar as suas funções e responsabilidades de forma a reduzir ou evitar o erro humano, o furto, a fraude, a utilização indevida ou a perda.

2 — As empresas de seguros e de resseguros devem garantir que os programas de formação proporcionam formação regular a todos os colaboradores.

3 — Para além do disposto nos números anteriores, as empresas de seguros e de resseguros devem criar e aplicar programas periódicos de sensibilização no domínio da segurança para educar os seus colaboradores, incluindo o órgão de administração, sobre a forma como devem abordar os riscos relacionados com a segurança da informação.

CAPÍTULO III

Gestão operacional dos sistemas e serviços de TIC

Artigo 17.º

Gestão de operações de TIC

1 — No âmbito da gestão de operações de TIC, as empresas de seguros e de resseguros devem:

a) Gerir as suas operações de TIC com base na respetiva estratégia em matéria de TIC;

b) Documentar a forma como operam, monitorizam e controlam os seus sistemas e serviços de TIC, incluindo processos, procedimentos e operações críticos de TIC;

c) Implementar procedimentos de registo e de monitorização de operações críticas de TIC para permitir a deteção, análise e correção de erros;

d) Manter um inventário atualizado dos seus ativos de TIC que seja suficientemente pormenorizado por forma a permitir uma rápida identificação de um ativo de TIC, bem como da sua localização, classificação de segurança e propriedade;

e) Monitorizar e gerir o ciclo de vida dos ativos de TIC, a fim de garantir que estes continuam a cumprir e a servir de suporte aos requisitos de negócio e de gestão dos riscos;

f) Monitorizar se os ativos de TIC são suportados pelos seus fornecedores ou promotores internos e se todas as correções e atualizações pertinentes são aplicadas com base num processo documentado, devendo os riscos decorrentes de ativos de TIC desatualizados ou não apoiados ser avaliados e reduzidos;

g) Aplicar processos de monitorização e de planeamento da capacidade e do desempenho para prevenir, detetar e responder atempadamente a importantes questões de desempenho dos sistemas de TIC e de escassez de capacidade em matéria de TIC;

h) Definir e aplicar procedimentos de segurança e de recuperação de dados e de sistemas de TIC para garantir que estes possam ser recuperados sempre que necessário.

2 — Os ativos de TIC desativados devem ser processados e cedidos de forma segura.

3 — O âmbito e a frequência das cópias de segurança devem ser definidos em consonância com os requisitos de recuperação de negócio e a criticidade dos dados e dos sistemas de TIC, avaliados de acordo com a avaliação dos riscos realizada.

4 — Os procedimentos de segurança e de recuperação devem ser testados regularmente.

5 — As empresas de seguros e de resseguros devem garantir que as cópias de segurança dos sistemas de TIC e dos dados são armazenadas num ou mais locais fora da localização primária, que são seguros e que estão suficientemente afastados da localização primária, de modo que não estejam expostos aos mesmos riscos.

Artigo 18.º

Gestão de problemas e incidentes em matéria de TIC

1 — As empresas de seguros e de resseguros devem estabelecer e implementar 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.

2 — As empresas de seguros e de resseguros devem estabelecer critérios e limites adequados para a classificação de um evento como um incidente operacional ou de segurança, bem como indicadores de alerta prévio que permitam à empresa ser capaz de detetar rapidamente este tipo de incidentes.

3 — Para minimizar o impacto de eventos adversos e permitir uma recuperação atempada, as empresas de seguros e de resseguros devem estabelecer processos e estruturas organizacionais adequados para assegurar uma monitorização, um tratamento e um

acompanhamento coerentes e integrados dos incidentes operacionais e de segurança, com vista a garantir que as causas profundas sejam identificadas e tratadas e sejam tomadas medidas corretivas para evitar a ocorrência repetida de incidentes.

4 — O processo de gestão de problemas e incidentes deve, pelo menos, estabelecer:

a) Os procedimentos para identificar, detetar, registar, categorizar e classificar os incidentes de acordo com uma prioridade definida pela empresa de seguros ou de resseguros e baseada na criticidade do negócio e em contratos de serviço;

b) As funções e responsabilidades para diferentes cenários de incidentes tais como, erros, mau funcionamento e ciberataques;

c) Um procedimento de gestão de problemas para identificar, analisar e resolver a causa subjacente a um ou mais incidentes, no âmbito do qual a empresa de seguros ou de resseguros deve analisar os incidentes operacionais ou de segurança que tenham sido identificados ou que tenham ocorrido dentro ou fora da organização, bem como ter em consideração os principais ensinamentos retirados destas análises e atualizar as medidas de segurança em conformidade;

d) Planos de comunicação interna eficazes, incluindo procedimentos por etapas em caso de incidentes e de notificação de incidentes, bem como as reclamações de clientes relacionadas com a segurança, de modo a garantir que:

i) Os incidentes com um impacto adverso potencialmente elevado nos sistemas e serviços críticos de TIC sejam comunicados à direção de topo relevante;

ii) O órgão de administração seja informado numa base *ad hoc* em caso de incidentes significativos e, pelo menos, informado do impacto, da resposta e dos controlos adicionais a definir em resultado dos incidentes;

e) Procedimentos de resposta a incidentes para atenuar os impactos relacionados com os mesmos e para assegurar que o serviço se torne operacional e seguro em tempo útil;

f) Planos de comunicação externa específicos para processos e funções de negócio críticos, a fim de:

i) Colaborar com as partes interessadas relevantes para responder eficazmente ao incidente e recuperar do mesmo;

ii) Fornecer informações oportunas, incluindo comunicação de incidentes, a partes externas, tais como, clientes, outros participantes no mercado e autoridades de supervisão competentes, conforme adequado e em consonância com a regulamentação aplicável.

Artigo 19.º

Gestão de projetos de TIC

1 — As empresas de seguros e de resseguros devem implementar 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 que sejam adequados para suportar eficazmente a implementação da estratégia em matéria de TIC através de projetos de TIC.

2 — As empresas de seguros e de resseguros devem monitorizar e reduzir adequadamente os riscos decorrentes da carteira de projetos de TIC, tendo igualmente em consideração os riscos que possam resultar de interdependências entre diferentes projetos e de dependências de múltiplos projetos em relação aos mesmos recursos ou conhecimentos especializados.

Artigo 20.º

Aquisição e desenvolvimento de sistemas de TIC

1 — As empresas de seguros e de resseguros devem desenvolver e implementar um processo que regule a aquisição, o desenvolvimento e a manutenção de sistemas de TIC, a fim de garantir a proteção integral da confidencialidade, a integridade e a disponibilidade dos dados a tratar e o cumprimento dos requisitos de proteção definidos.

2 — O processo referido no número anterior deve ser concebido utilizando uma abordagem baseada no risco.

3 — No âmbito da aquisição e desenvolvimento de sistemas de TIC, as empresas de seguros e de resseguros devem:

a) Assegurar que, antes de efetuar aquisições de sistemas ou atividades de desenvolvimento, os requisitos funcionais e não funcionais, incluindo os requisitos de segurança da informação, e os objetivos técnicos são claramente definidos;

b) Assegurar a aplicação de medidas para evitar a alteração não intencional ou a manipulação intencional dos sistemas de TIC durante o seu desenvolvimento;

c) Dispor de uma metodologia para testar e aprovar os sistemas de TIC, os serviços de TIC e as medidas de segurança da informação;

d) Testar, de forma adequada, os sistemas de TIC, os serviços de TIC e as medidas de segurança da informação, a fim de identificar potenciais fragilidades, violações e incidentes em matéria de segurança;

e) Assegurar a segregação dos ambientes de produção em relação aos ambientes de desenvolvimento, aos ambientes de teste e a outros ambientes de não produção;

f) Aplicar medidas para proteger a integridade dos códigos fonte dos sistemas de TIC, quando disponíveis, bem como documentar exaustivamente o desenvolvimento, a implementação, o funcionamento ou a configuração dos sistemas de TIC para reduzir qualquer dependência desnecessária de peritos na matéria.

4 — Os processos de aquisição e desenvolvimento de sistemas de TIC devem igualmente aplicar-se a sistemas de TIC desenvolvidos ou geridos pelos utilizadores finais fora da organização de TIC tais como, aplicações de gestão de negócio ou aplicações informáticas para utilizadores finais, utilizando uma abordagem baseada no risco.

5 — As empresas de seguros e de resseguros devem manter um registo das aplicações referidas no número anterior que suportem funções de negócio ou processos críticos.

Artigo 21.º

Gestão de alterações em matéria de TIC

1 — As empresas de seguros e de resseguros devem estabelecer e implementar 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 — As alterações em matéria de TIC efetuadas durante situações de urgência ou emergência devem ser rastreáveis e notificadas *ex post* ao proprietário do ativo relevante para análise posterior.

3 — As empresas de seguros e de resseguros devem averiguar se as alterações do ambiente operacional existente afetam as medidas de segurança em vigor ou exigem a adoção de medidas adicionais para atenuar os riscos envolvidos.

4 — As alterações referidas no número anterior devem estar em conformidade com o processo formal de gestão de alterações das empresas de seguros e de resseguros.

CAPÍTULO IV

Continuidade das atividades

Artigo 22.º

Gestão da continuidade de negócio

1 — O órgão de administração é responsável por definir e aprovar a política de continuidade das TIC da empresa de seguros ou de resseguros como parte da política global de gestão da continuidade de negócio da empresa.

2 — A política de continuidade das TIC referida no número anterior deve ser devidamente comunicada na empresa de seguros ou de resseguros e ser aplicável a todos os colaboradores relevantes e, se pertinente, aos prestadores de serviços.

Artigo 23.º

Análise de impacto no negócio

1 — Como parte de uma gestão sólida da continuidade de negócio, as empresas de seguros e de resseguros devem realizar uma análise de impacto no negócio para avaliar a sua exposição a perturbações graves no negócio e os seus potenciais impactos, a nível quantitativo e qualitativo, recorrendo a dados internos ou externos e à análise de cenários.

2 — A análise de impacto no negócio deve ter igualmente em consideração a criticidade dos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, que tenham sido identificados e classificados, bem como as suas interdependências, em conformidade com o previsto no artigo 6.º

3 — As empresas de seguros e de resseguros devem assegurar que os seus sistemas e serviços de TIC são concebidos e alinhados com as suas análises de impacto no negócio, por exemplo, através da redundância de determinados componentes críticos para evitar perturbações causadas por eventos que tenham impacto nos componentes em causa.

Artigo 24.º

Planeamento da continuidade de negócio

1 — O plano global de continuidade de negócio ("PCN") das empresas de seguros e de resseguros deve ter em consideração os riscos substanciais que possam ter um impacto negativo nos sistemas e serviços de TIC.

2 — O PCN deve promover objetivos relacionados com a proteção e, se necessário, restabelecimento da confidencialidade, integridade e disponibilidade dos processos e atividades de negócio, funções de negócio, tarefas e ativos das empresas de seguros e de resseguros, tais como, ativos de informação e ativos de TIC.

3 — Para além do disposto no número anterior, a criação de um PCN serve igualmente para garantir que as empresas de seguros e de resseguros conseguem reagir adequadamente a potenciais cenários de falha dentro de um objetivo de tempo de recuperação estabelecido e de um objetivo de ponto de recuperação.

4 — Para efeitos do número anterior, considera-se objetivo de tempo de recuperação estabelecido o intervalo de tempo máximo dentro do qual um sistema ou processo deve ser restaurado após um incidente e objetivo de ponto de recuperação o intervalo de tempo máximo durante o qual é aceitável que os dados se percam em caso de incidente a um nível de serviço predefinido.

5 — As empresas de seguros e de resseguros devem considerar um conjunto de diferentes cenários no seu PCN e avaliar o seu potencial impacto, abrangendo cenários extremos, mas plausíveis, e cenários de ciberataque.

6 — Com base nos cenários referidos no número anterior, as empresas de seguros e de resseguros devem descrever a forma como a continuidade dos sistemas e serviços de TIC, bem como a segurança da informação das empresas, são asseguradas.

7 — Durante a elaboração do PCN, as empresas de seguros e de resseguros devem coordenar-se com as partes interessadas, internas e externas, relevantes, se for caso disso.

Artigo 25.º

Planos de resposta e recuperação

1 — As empresas de seguros e de resseguros devem elaborar planos de resposta e recuperação com base nas análises de impacto no negócio e nos cenários plausíveis, referidos nos artigos anteriores.

2 — Os planos de resposta e recuperação devem visar o cumprimento dos objetivos de recuperação das operações das empresas de seguros e de resseguros e especificar as condições que podem exigir a respetiva ativação e as ações que devem ser tomadas para assegurar a integridade, disponibilidade, continuidade e recuperação, pelo menos, de sistemas de TIC, serviços de TIC e dados críticos das empresas.

3 — Os planos de resposta e recuperação devem ter em consideração as opções de recuperação a curto e, sempre que necessário, a longo prazo, devendo no mínimo:

a) Centrar-se na recuperação das operações de serviços importantes de TIC, funções de negócio, processos de apoio, ativos de informação e respetivas interdependências para evitar efeitos adversos no funcionamento da empresa de seguros ou de resseguros;

b) Ser documentados e disponibilizados às unidades de negócio e de apoio e facilmente acessíveis em caso de emergência, incluindo uma clara definição das funções e responsabilidades;

c) Ser continuamente atualizados em consonância com os ensinamentos retirados dos incidentes, testes, riscos recentemente identificados e ameaças, bem como com as alterações introduzidas nos objetivos de recuperação e prioridades.

4 — Os planos de resposta e recuperação devem ter igualmente em consideração opções alternativas em que a recuperação possa não ser viável a curto prazo devido a custos, riscos, logística ou circunstâncias imprevistas.

5 — Como parte dos planos de resposta e recuperação, as empresas de seguros e de resseguros devem ter em consideração e aplicar medidas de continuidade para atenuar as falhas de prestadores de serviços que sejam de importância fundamental para a continuidade dos serviços de TIC, em conformidade com as disposições previstas na Norma Regulamentar n.º 4/2022-R, de 26 de abril, e no título seguinte da presente norma regulamentar.

Artigo 26.º

Testes ao plano de continuidade de negócio

1 — As empresas de seguros e de resseguros devem testar o seu PCN e garantir que a operação dos seus processos e atividades de negócio críticos, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC, e respetivas interdependências, incluindo os fornecidos por prestadores de serviços, são testados regularmente com base no seu perfil de risco.

2 — O PCN deve ser atualizado regularmente, com base nos resultados dos testes, nas informações sobre ameaças atuais e nos ensinamentos retirados de eventos anteriores, bem como de acordo com quaisquer alterações pertinentes dos objetivos de recuperação, incluindo o objetivo de tempo de recuperação e o objetivo de ponto de recuperação, ou alterações dos processos e atividades de negócio, funções de negócio, tarefas e ativos, tais como, ativos de informação e ativos de TIC.

3 — Os testes ao PCN devem demonstrar que este é capaz de manter a viabilidade das atividades até ao restabelecimento das operações críticas a um nível de serviço predefinido ou de tolerância face ao impacto.

4 — Os resultados dos testes devem ser documentados e quaisquer deficiências identificadas devem ser analisadas, tratadas e comunicadas ao órgão de administração.

Artigo 27.º

Comunicação de crises

No caso de uma interrupção ou emergência, e durante a aplicação dos PCN, as empresas de seguros e de resseguros devem garantir que dispõem de medidas eficazes de comunicação de crises, de modo a que todas as partes interessadas relevantes, internas e externas, entre as quais a ASF, bem como os prestadores de serviços relevantes, sejam informados de forma atempada e adequada.

Artigo 28.º

Subcontratação de serviços e sistemas de TIC

1 — Sem prejuízo do disposto no capítulo VIII da Norma Regulamentar n.º 4/2022-R, de 26 de abril, e no título seguinte da presente norma regulamentar, no caso de subcontratação dos serviços e sistemas de TIC, as empresas de seguros e de resseguros devem assegurar o cumprimento dos requisitos aplicáveis aos serviços de TIC ou aos sistemas de TIC.

2 — No caso de subcontratação de funções fundamentais ou importantes, as empresas de seguros e de resseguros devem garantir que as obrigações contratuais do prestador de serviços, decorrentes, nomeadamente, de contratos, acordos de nível de serviço, disposições de rescisão em contratos relevantes, incluem, pelo menos, o seguinte:

a) Objetivos e medidas adequados e proporcionais relacionados com a segurança da informação, incluindo requisitos mínimos de segurança da informação, especificações do ciclo de vida dos dados da empresa, direitos de acesso e auditoria, bem como quaisquer requisitos relativos à localização dos centros de dados e à cifragem de dados, à segurança da rede e aos processos de monitorização da segurança;

b) Acordos de nível de serviço, a fim de assegurar a continuidade dos serviços e sistemas de TIC e as metas de desempenho em condições normais, bem como as previstas em planos de contingência no caso de interrupção do serviço;

c) Procedimentos de tratamento de incidentes operacionais e de segurança, incluindo procedimentos por etapas e de comunicação de informações.

3 — As empresas de seguros e de resseguros devem monitorizar e assegurar o nível de conformidade dos prestadores de serviços com os seus objetivos de segurança, medidas e metas de desempenho definidos.

TÍTULO III

Subcontratação a prestadores de serviços de computação em nuvem

CAPÍTULO I

Requisitos gerais da governação da subcontratação de serviços de computação em nuvem

Artigo 29.º

Serviços de computação em nuvem e subcontratação

1 — As empresas de seguros e de resseguros devem determinar 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 e no capítulo VIII da Norma Regulamentar n.º 4/2022-R, de 26 de abril.

2 — No âmbito da avaliação referida no número anterior, deve ser tomado em consideração:

a) Se a função ou atividade operacional subcontratada, ou parte da mesma, é realizada de forma recorrente ou contínua;

b) Se a referida função ou atividade operacional, ou parte da mesma, seria normalmente abrangida pelo âmbito das funções ou atividades operacionais que seriam ou poderiam ser exercidas pela empresa de seguros ou de resseguros no exercício das suas atividades regulares, mesmo que essa função ou atividade operacional não tenha sido desempenhada anteriormente.

3 — Sempre que um acordo celebrado com um prestador de serviços abranja várias funções ou atividades operacionais, as empresas de seguros e de resseguros devem ter em conta todos os aspetos do acordo no âmbito da sua avaliação.

4 — Nos casos em que as empresas de seguros e de resseguros subcontratam funções ou atividades operacionais a prestadores de serviços que não sejam prestadores de serviços de computação em nuvem, mas que dependam de forma significativa de infraestruturas em nuvem para prestar os seus serviços, nomeadamente, quando o prestador de serviços de computação em nuvem faz parte de uma cadeia de subcontratação, aplica-se ao acordo de subcontratação o disposto na presente norma regulamentar.

Artigo 30.º

Princípios gerais de governação para a subcontratação de serviços de computação em nuvem

1 — Sem prejuízo do disposto no n.º 3 do artigo 274.º do Regulamento Delegado, o órgão de administração deve assegurar que qualquer decisão de subcontratação de funções operacionais ou atividades fundamentais ou importantes a prestadores de serviços de computação em nuvem é tomada com base numa avaliação de risco exaustiva, incluindo todos os riscos relevantes inerentes ao acordo, como a utilização de TIC, a continuidade de negócio, o cumprimento da legislação e regulamentação aplicável, o risco de concentração, assim como outros riscos operacionais e riscos associados à migração de dados ou à fase de implementação, caso aplicável.

2 — No caso de subcontratação de funções ou atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem, quando relevante, integrar as alterações decorrentes dos seus acordos de subcontratação no seu perfil de risco e na sua autoavaliação do risco e da solvência.

3 — A utilização de serviços de computação em nuvem deve ser consistente com as estratégias estabelecidas pela empresa de seguros ou de resseguros, nomeadamente com a estratégia de TIC, a estratégia de segurança da informação e a estratégia de gestão operacional dos riscos, assim como com as políticas e os processos internos, os quais devem ser atualizados, sempre que necessário.

Artigo 31.º

Atualização da política de subcontratação e respetivos documentos

1 — Quando forem subcontratados prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem atualizar a sua política de subcontratação, nomeadamente através da revisão dos documentos que a contêm, do aditamento de um apêndice separado ou da elaboração de novas políticas específicas, bem como outras políticas internas relevantes relacionadas, tal como, a política de segurança da informação, tendo em conta as especificidades dos serviços de computação em nuvem subcontratados nos seguintes domínios:

a) Atribuições e responsabilidades das funções envolvidas, em particular o órgão de administração e as funções responsáveis pelas TIC, pela segurança da informação, pela verificação do cumprimento, pela gestão dos riscos e pela auditoria interna;

b) Processos e procedimentos de prestação de informação exigidos para a aprovação, execução, acompanhamento, gestão e renovação, caso aplicável, dos acordos de subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes;

c) Supervisão dos serviços de computação em nuvem proporcional à natureza, dimensão e complexidade dos riscos inerentes aos serviços prestados, que deve abranger:

i) A avaliação dos riscos associados aos acordos de subcontratação de serviços de computação em nuvem e o dever de diligência relativamente aos prestadores de serviços de computação em nuvem, incluindo a frequência da avaliação do risco;

ii) Os controlos de acompanhamento e gestão, incluindo a verificação de acordos de níveis de serviço;

iii) As normas e controlos de segurança;

d) Requisitos de informação prévia à ASF e requisitos documentais relativos à subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes, nos termos dos artigos seguintes.

2 — No âmbito da atualização referida no número anterior, no que se refere à subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes:

a) Deve ser feita referência aos requisitos contratuais estabelecidos no n.º 2 do artigo 38.º;

b) Em relação a cada acordo de subcontratação, deve ser definida uma «estratégia de saída» documentada e, sempre que adequado, suficientemente testada, proporcional à natureza, dimensão e complexidade dos riscos inerentes aos serviços prestados.

3 — A estratégia de saída referida na alínea *b)* do número anterior pode envolver uma série de processos de rescisão, incluindo, entre outros, a interrupção, a reintegração ou a transferência dos serviços abrangidos pelo acordo de subcontratação.

Artigo 32.º

Informação prévia à ASF

1 — Os requisitos de informação prévia estabelecidos no n.º 3 do artigo 78.º do RJASR e especificados no artigo 71.º da Norma Regulamentar n.º 4/2022-R, de 26 de abril, são aplicáveis a todas as subcontratações de funções e atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem.

2 — Para além do disposto no número anterior, na informação prévia a enviar à ASF relativa à subcontratação de funções e atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem incluir informação sobre o modelo do serviço de computação em nuvem e o modelo de implementação da nuvem, ou seja, se é nuvem pública, privada, híbrida ou comunitária, bem como a natureza específica dos dados a conservar e os países ou regiões onde esses dados serão armazenados.

3 — Caso uma função ou atividade operacional subcontratada e classificada anteriormente como não fundamental ou não importante venha a tornar-se fundamental ou importante, as empresas de seguros e de resseguros devem informar previamente a ASF nos termos do presente artigo.

Artigo 33.º

Requisitos documentais

1 — No âmbito do seu sistema de governação e, em especial, do sistema de gestão de riscos, 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.

2 — As empresas de seguros e de resseguros devem igualmente conservar, durante um período adequado e em conformidade com a legislação aplicável, um registo dos acordos de subcontratação de serviços de computação em nuvem já cessados.

3 — No caso de subcontratação de funções ou atividades operacionais fundamentais ou importantes, as empresas de seguros e de resseguros devem registar as seguintes informações:

a) As informações a comunicar à autoridade de supervisão referida no artigo anterior;

b) No caso de grupos, as empresas de seguros ou de resseguros e outras empresas abrangidas pela consolidação prudencial que recorram aos serviços de computação em nuvem;

c) A data da avaliação dos riscos mais recente e um breve resumo dos principais resultados;

d) O órgão individual ou decisório nas empresas de seguros e de resseguros que aprovou o acordo de subcontratação de serviços de computação em nuvem;

e) As datas das auditorias mais recentes e das próximas auditorias agendadas, se aplicável;

f) Os nomes dos subcontratantes aos quais sejam subcontratadas partes significativas de uma função ou atividade operacional fundamental ou importante, incluindo o país em que os subcontratantes estão registados, o país em que é realizado o serviço e, caso aplicável, os países ou regiões onde os dados são armazenados;

g) O resultado da avaliação da substituibilidade do prestador de serviços de computação em nuvem, utilizando indicadores para o efeito, tais como fácil, difícil ou impossível;

h) Se a função ou atividade operacional fundamental ou importante subcontratada apoia operações de negócio em que o tempo é um fator crítico;

i) O custo anual orçamentado estimado;

j) Se a empresa de seguros ou de resseguros que procede à subcontratação possui uma estratégia de saída em caso de rescisão por uma das partes ou em caso de interrupção na prestação de serviços pelo prestador de serviços de computação em nuvem.

4 — No caso de subcontratação de funções ou atividades operacionais não fundamentais ou não importantes, as empresas de seguros e de resseguros devem definir as informações a registar com base na natureza, dimensão e complexidade dos riscos inerentes aos serviços prestados pelo prestador de serviços de computação em nuvem.

5 — As empresas de seguros e de resseguros devem disponibilizar à ASF, sempre que solicitado, todas as informações necessárias para permitir uma adequada supervisão, incluindo uma cópia do acordo de subcontratação.

CAPÍTULO II

Requisitos prévios ao acordo de subcontratação

Artigo 34.º

Análise prévia à subcontratação

Antes de celebrar qualquer acordo com prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem:

a) Avaliar se o acordo de subcontratação de serviços de computação em nuvem diz respeito a uma função ou atividade operacional fundamental ou importante, em conformidade com o disposto no artigo seguinte;

b) Identificar e avaliar todos os riscos relevantes do acordo de subcontratação de serviços de computação em nuvem, em conformidade com o disposto no artigo 36.º;

c) Aplicar o dever de diligência, de forma adequada ao potencial prestador de serviços de computação em nuvem, em conformidade com o disposto no artigo 37.º;

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.

Artigo 35.º

Avaliação das funções e atividades operacionais fundamentais ou importantes

1 — Antes de celebrar qualquer acordo de subcontratação com prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem avaliar se o acordo de subcontratação diz respeito a uma função ou atividade operacional que seja fundamental ou importante.

2 — Para efeitos da avaliação referida no número anterior, as empresas de seguros e de resseguros devem ter em conta, sempre que relevante, a possibilidade de as funções ou atividades operacionais contempladas pelo acordo virem a ser fundamentais ou importantes no futuro.

3 — As empresas de seguros e de resseguros devem igualmente reavaliar o caráter fundamental ou a importância da função ou atividade operacional anteriormente subcontratada a prestadores de serviços de computação em nuvem, se a natureza, a dimensão e a complexidade dos riscos inerentes ao acordo se alterarem substancialmente.

4 — Na avaliação a que se refere o presente artigo, as empresas de seguros e de resseguros devem ter em conta, em conjunto com os resultados da avaliação dos riscos, pelo menos, os seguintes elementos:

a) O potencial impacto de qualquer perturbação significativa da função ou atividade operacional subcontratada ou da incapacidade do prestador de serviços de computação em nuvem para prestar os serviços nos níveis de serviço acordados sobre:

i) O cumprimento contínuo das suas obrigações regulamentares;

ii) A resiliência e a viabilidade financeira a curto e longo prazo;

iii) A continuidade da atividade e a resiliência operacional;

iv) O risco operacional, incluindo a conduta, as TIC e o risco legal;

v) O risco reputacional;

b) O potencial impacto do acordo de subcontratação de serviços de computação em nuvem na respetiva capacidade para:

i) Identificar, monitorizar e gerir todos os riscos relevantes;

ii) Cumprir todos os requisitos legais e regulamentares;

iii) Realizar auditorias específicas sobre a função ou atividade operacional subcontratada;

c) A exposição agregada da empresa ou do grupo ao mesmo prestador de serviços de computação em nuvem e o potencial impacto dos acordos de subcontratação cumulativos na mesma área de atividade;

d) A dimensão e a complexidade de qualquer área de atividade afetada pelo acordo de subcontratação de serviços de computação em nuvem;

e) A capacidade para transferir o acordo de subcontratação proposto para outro prestador de serviços de computação em nuvem, se necessário ou desejável, ou reintegrar os serviços;

f) A proteção de dados pessoais e não pessoais e o potencial impacto, para a empresa, tomadores de seguros ou outros titulares de dados, de uma violação da confidencialidade ou da incapacidade de assegurar a disponibilidade e a integridade dos dados, conforme previsto, nomeadamente, no Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

5 — Para efeitos do disposto na alínea *f)* do número anterior, as empresas de seguros e de resseguros devem ter especialmente em conta os dados sujeitos a sigilo comercial ou sensíveis, como os dados de saúde dos tomadores de seguros.

Artigo 36.º

Avaliação dos riscos dos acordos de subcontratação de serviços de computação em nuvem

1 — As empresas de seguros e de resseguros devem adotar uma abordagem proporcional à natureza, dimensão e complexidade dos riscos inerentes aos serviços subcontratados a prestadores de serviços de computação em nuvem, a qual deve incluir a avaliação do potencial impacto dos acordos de subcontratação de serviços de computação em nuvem, em particular, nos seus riscos operacionais e reputacionais.

2 — Quando subcontratem funções ou atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem:

a) Ter em conta os benefícios e custos esperados do acordo de subcontratação de serviços de computação em nuvem proposto, incluindo a ponderação de quaisquer riscos significativos que possam ser reduzidos ou mais bem geridos face a quaisquer riscos significativos que possam resultar do acordo de subcontratação proposto;

b) Avaliar, sempre que aplicável e adequado, os riscos, incluindo os riscos jurídicos, das TIC, de conformidade e de reputação, assim como as limitações de supervisão relacionadas com:

i) O serviço de computação em nuvem selecionado e os modelos de implementação da nuvem propostos, designadamente pública, privada, híbrida ou comunitária;

ii) A migração ou a implementação;

iii) As atividades e os dados e sistemas associados que se pondere incluir no acordo de subcontratação, ou que já foram subcontratados, assim como a sua sensibilidade e as medidas de segurança necessárias;

iv) A situação de estabilidade política e de segurança dos países, pertencentes e não pertencentes à União Europeia, em que os serviços subcontratados são ou podem ser prestados e em que os dados são, ou são suscetíveis de virem a ser, armazenados;

v) A subcontratação em cadeia, incluindo os riscos adicionais que possam surgir se o subcontratante em cadeia estiver localizado num país terceiro ou num país diferente do prestador de serviços de computação em nuvem e o risco de que cadeias de subcontratação longas e complexas reduzam a capacidade da empresa para supervisionar as suas funções ou atividades operacionais fundamentais ou importantes e a capacidade da ASF para o exercício das suas funções de supervisão de forma eficaz;

vi) O risco global de concentração quando várias empresas de seguros e de resseguros celebram acordos de subcontratação com um mesmo prestador de serviços de computação em nuvem, incluindo os casos em que é celebrado um acordo com um prestador de serviços que não é facilmente substituível ou em que são celebrados vários acordos de subcontratação com um único prestador de serviços de computação em nuvem.

3 — Para efeitos do disposto na subalínea *iv)* da alínea *b)* do número anterior, devem ter-se em conta os seguintes elementos:

a) A legislação em vigor, incluindo em matéria de proteção de dados;

b) As normas de execução da lei em vigor;

c) A legislação em matéria de insolvência que seria aplicável em caso de incumprimento por um prestador de serviços e eventuais restrições relacionadas com a recuperação urgente dos dados das empresas de seguros e de resseguros.

4 — Para efeitos do disposto na subalínea *vi)* da alínea *b)* do n.º 2 as empresas de seguros e de resseguros ou os grupos devem ter em conta todos os seus acordos de subcontratação celebrados com o prestador de serviços de computação em nuvem em causa.

5 — A avaliação dos riscos a que se refere o presente artigo deve ser efetuada antes da celebração de um acordo de subcontratação de serviços de computação em nuvem.

6 — Se as empresas de seguros e de resseguros tomarem conhecimento de deficiências graves ou de alterações significativas nos serviços prestados ou na situação do prestador de serviços de computação em nuvem, a avaliação dos riscos deve ser imediatamente revista ou novamente realizada.

7 — Em caso de reformulação de um acordo de subcontratação de serviços de computação em nuvem para modificar o seu conteúdo e o seu âmbito de aplicação, incluindo o alargamento do âmbito de aplicação ou a inclusão de funções operacionais fundamentais ou importantes que não estavam anteriormente incluídas, deve ser efetuada uma reavaliação dos riscos.

Artigo 37.º

Dever de diligência em relação ao prestador de serviços de computação em nuvem

1 — Durante o seu processo de seleção e avaliação, as empresas de seguros e de resseguros devem certificar-se de que o prestador de serviços de computação em nuvem é adequado à luz dos critérios definidos nos termos da sua política de subcontratação.

2 — O dever de diligência em relação ao prestador de serviços de computação em nuvem deve ser cumprido antes de subcontratar qualquer função ou atividade operacional.

3 — Caso celebrem um segundo acordo com um prestador de serviços de computação em nuvem que já tenha sido avaliado, as empresas de seguros ou de resseguros devem

determinar, em função do risco associado, se é necessário proceder a uma segunda avaliação em cumprimento do dever de diligência.

4 — Se as empresas de seguros ou de resseguros tomarem conhecimento de deficiências graves ou de alterações significativas nos serviços prestados ou na situação do prestador de serviços de computação em nuvem, a situação deve ser imediatamente revista à luz dos procedimentos do dever de diligência que, sendo necessário, devem ser novamente realizados.

5 — No caso de subcontratação de serviços de computação em nuvem relacionados com funções operacionais fundamentais ou importantes, o cumprimento do dever de diligência deve incluir uma avaliação da adequação do prestador de serviços de computação em nuvem, designadamente, das suas competências, infraestruturas, situação financeira, estatuto empresarial e legal.

6 — Sempre que relevante, as empresas de seguros e de resseguros podem utilizar, como prova do cumprimento do dever de diligência, certificações baseadas em normas internacionais, relatórios de auditoria de entidades reconhecidas ou relatórios de auditoria interna.

CAPÍTULO III

Acordo de subcontratação de serviços de computação em nuvem

Artigo 38.º

Requisitos contratuais

1 — 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.

2 — Sem prejuízo dos requisitos previstos no n.º 4 do artigo 274.º do Regulamento Delegado, quando forem subcontratadas funções ou atividades operacionais fundamentais ou importantes a um prestador de serviços de computação em nuvem, o acordo escrito de subcontratação deve estabelecer:

a) Uma descrição clara da função subcontratada, incluindo o tipo de serviço de suporte;

b) A data de início e a data de termo, caso aplicável, do acordo e os períodos de pré-aviso aplicáveis ao prestador de serviços de computação em nuvem e à empresa de seguros ou de resseguros;

c) O órgão jurisdicional competente e a lei aplicável ao acordo;

d) As obrigações financeiras das partes;

e) Se é permitida a subcontratação em cadeia de uma função ou atividade operacional fundamental ou importante, ou de partes significativas da mesma, e, em caso afirmativo, as condições a que está sujeita a subcontratação em cadeia, nos termos do disposto no artigo 41.º;

f) As regiões ou os países em que os dados serão armazenados e tratados e as condições a cumprir, incluindo a obrigação de notificar a empresa de seguros ou de resseguros caso o prestador de serviços pretenda alterar a localização dos centros de dados;

g) Disposições relativas à acessibilidade, disponibilidade, integridade, confidencialidade, privacidade e segurança dos dados, tendo em conta o disposto no artigo 40.º;

h) O direito de a empresa de seguros ou de resseguros acompanhar regularmente o desempenho do prestador de serviços de computação em nuvem;

i) Os níveis de serviço acordados, que devem incluir objetivos de desempenho quantitativos e qualitativos concretos, a fim de permitir o acompanhamento em tempo útil e a adoção sem demora de medidas corretivas adequadas, caso os níveis de serviço acordados não sejam cumpridos;

j) As obrigações de reporte do prestador de serviços de computação em nuvem à empresa de seguros ou de resseguros, incluindo, sempre que aplicável, as obrigações de apresentação de relatórios relevantes para a função de segurança da empresa e para as suas principais funções, tais como relatórios da função de auditoria interna do prestador de serviços de computação em nuvem;

k) Se o prestador de serviços de computação em nuvem deve subscrever um seguro contra determinados riscos e, se for caso disso, o nível de cobertura exigido;

l) Os requisitos de execução e ensaio dos planos de contingência;

m) A obrigação de o prestador de serviços de computação em nuvem conceder à empresa de seguros ou de resseguros, à ASF e a qualquer outra pessoa por estas designada:

i) Pleno acesso a todas as instalações comerciais relevantes, tais como sedes e centros de operações, incluindo todos os dispositivos, sistemas, redes, informações e dados utilizados no desempenho da função subcontratada, em especial, as informações financeiras conexas, os colaboradores e os auditores externos do prestador de serviços de computação em nuvem;

ii) Direitos ilimitados de inspeção e auditoria relacionados com o acordo de subcontratação de serviços de computação em nuvem, com vista a permitir o acompanhamento do acordo de subcontratação e assegurar a conformidade com todos os requisitos regulamentares e contratuais aplicáveis;

n) Disposições que assegurem que os dados detidos pela empresa possam ser imediatamente recuperados em caso de insolvência, resolução ou interrupção das atividades do prestador de serviços de computação em nuvem.

Artigo 39.º

Direitos de acesso e de auditoria

1 — A fim de cumprir as suas obrigações regulamentares, o acordo de subcontratação de serviços de computação em nuvem não pode limitar o exercício efetivo dos direitos de acesso e de auditoria pelas empresas de seguros e de resseguros, nem as opções de controlo sobre os serviços de computação em nuvem.

2 — As empresas de seguros e de resseguros devem exercer os seus direitos de acesso e de auditoria, determinar a frequência das auditorias e os domínios e serviços a auditar, segundo uma abordagem baseada no risco, em conformidade com o disposto na Norma Regulamentar n.º 4/2022-R, de 26 de abril.

3 — Ao determinar a frequência e o âmbito dos seus direitos de acesso ou de auditoria, as empresas de seguros e de resseguros devem ter em consideração se a subcontratação de serviços de computação em nuvem está relacionada com uma função ou atividade operacional fundamental ou importante, a natureza e dimensão do risco, e o impacto que os acordos de subcontratação de serviços de computação em nuvem representam na empresa.

4 — Se o exercício dos seus direitos de acesso ou de auditoria ou a utilização de determinados métodos de auditoria criarem riscos para o ambiente do prestador de serviços de computação em nuvem ou de outro cliente do prestador de serviços relacionados, nomeadamente, com o impacto nos níveis de serviço, disponibilidade de dados, questões de confidencialidade, as empresas de seguros e de resseguros e o prestador de serviços de computação em nuvem devem acordar formas alternativas de fornecer àquelas um nível de garantia e de serviço semelhantes, designadamente , através da inclusão de controlos específicos, testados através de um relatório ou certificação específicos elaborados pelo prestador de serviços de computação em nuvem.

5 — Sem prejuízo da sua responsabilidade relativamente às atividades desempenhadas pelos seus prestadores de serviços de computação em nuvem, com vista a fazer uso dos recursos de auditoria com maior eficiência e a reduzir os encargos administrativos para o prestador de serviços e os seus clientes, as empresas de seguros e de resseguros podem utilizar:

a) Certificações de terceiros e relatórios de auditoria interna ou de terceiros disponibilizados pelo prestador de serviços de computação em nuvem;

b) Auditorias comuns realizadas conjuntamente com outros clientes do mesmo fornecedor de serviços de computação em nuvem ou realizadas por terceiros por si designados.

6 — No que respeita à subcontratação de funções ou atividades operacionais fundamentais ou importantes, as empresas de seguros e de resseguros só devem utilizar o método referido na alínea *a)* do número anterior se:

a) Assegurarem que o âmbito da certificação ou do relatório de auditoria abrange os sistemas, designadamente, processos, aplicações, infraestruturas, centros de dados e os controlos identificados pela empresa e permite avaliar o cumprimento dos requisitos regulamentares aplicáveis;

b) Efetuarem uma avaliação exaustiva e regular do conteúdo das novas certificações ou dos relatórios de auditoria e verificarem que os relatórios ou as certificações não são obsoletos;

c) Assegurarem que os sistemas e controlos fundamentais são incluídos em futuras versões da certificação ou do relatório de auditoria;

d) Tiverem confirmado a aptidão da entidade de certificação ou de auditoria, designadamente, no que se refere à rotatividade das empresas de certificação ou de auditoria, qualificações, conhecimentos especializados, repetição ou verificação das provas no ficheiro de auditoria subjacente;

e) Tiverem a certeza de que as certificações são emitidas e as auditorias são realizadas de acordo com as normas relevantes e incluem um teste da eficácia operacional dos controlos essenciais existentes;

f) Tiverem o direito contratual de solicitar a extensão do âmbito das certificações ou dos relatórios de auditoria a outros sistemas e controlos relevantes, devendo o número e a frequência desses pedidos de alteração do âmbito ser razoáveis e legítimos do ponto de vista da gestão dos riscos;

g) Mantiverem o direito contratual de realizar auditorias individuais no local, por sua livre iniciativa, no que diz respeito à subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes, o qual deve ser exercido em caso de necessidades específicas em que não seja possível interagir de outra forma com o prestador de serviços de computação em nuvem.

7 — No que respeita à subcontratação de funções fundamentais ou importantes a fornecedores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem avaliar se as certificações e os relatórios de terceiros mencionados na alínea *a*) do n.º 5 são adequados e suficientes para cumprir as suas obrigações regulamentares, não devendo, contudo, de acordo com uma abordagem baseada no risco, recorrer exclusivamente a esses relatórios e certificações ao longo do tempo.

8 — Antes de uma visita planeada ao local, a parte que exerce o seu direito de acesso, seja a empresa de seguros ou de resseguros ou um auditor, ou um terceiro mandatado por aquela empresa, deve notificar a outra parte com uma antecedência razoável, exceto se tal não for possível devido a uma situação de emergência ou de crise.

9 — Na notificação prévia referida no número anterior, devem ser indicados a localização e o objetivo da visita, assim como a identificação das pessoas que participarão na mesma.

10 — Tendo em conta que as soluções de computação em nuvem têm um elevado nível de complexidade técnica, as empresas de seguros e de resseguros devem verificar se as

pessoas que realizam a auditoria, sejam os seus auditores internos, o grupo de auditores que atua em seu nome, ou os auditores do prestador de serviços de computação em nuvem, ou, caso aplicável, as pessoas que fiscalizam a certificação de terceiros ou os relatórios de auditoria do prestador de serviços, possuem as competências e os conhecimentos adequados para realizar as auditorias ou as avaliações relevantes.

Artigo 40.º

Segurança dos dados e sistemas

1 — As empresas de seguros e de resseguros devem garantir que os prestadores de serviços de computação em nuvem cumprem a legislação europeia e nacional aplicável, assim como as normas de segurança adequadas em matéria de TIC.

2 — Quando forem subcontratadas funções ou atividades operacionais fundamentais ou importantes a prestadores de serviços de computação em nuvem, as empresas de seguros e de resseguros devem ainda estabelecer, no acordo de subcontratação, requisitos específicos de segurança da informação e controlar regularmente o cumprimento desses requisitos.

3 — Para efeitos do disposto no número anterior, utilizando uma abordagem baseada no risco e tendo em conta, quer as suas responsabilidades, quer as responsabilidades do prestador de serviços de computação em nuvem, as empresas de seguros e de resseguros devem:

a) Definir e distinguir de forma clara as competências e responsabilidades que cabem ao prestador de serviços e à empresa relativamente às funções ou atividades operacionais abrangidas pelo acordo de subcontratação;

b) Sem prejuízo dos deveres previstos no Regulamento (UE) n.º 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, definir e decidir um nível adequado de proteção de dados confidenciais, de continuidade das atividades subcontratadas e da integridade e rastreabilidade dos dados e sistemas no contexto da subcontratação de serviços de computação em nuvem pretendida;

c) Considerar medidas específicas, se necessário, no que respeita a dados em trânsito, dados em memória e dados armazenados, como a utilização de tecnologias de encriptação, em conjugação com uma arquitetura de gestão de chaves adequada;

d) Considerar os mecanismos de integração dos serviços de computação em nuvem com os sistemas da empresa, como as interfaces de programação de aplicações e um processo eficiente de gestão de acesso e de utilizador;

e) Assegurar contratualmente que a disponibilidade e a capacidade de tráfego da rede previstas cumprem requisitos de continuidade rigorosos, quando aplicáveis e exequíveis;

f) Definir e estabelecer requisitos de continuidade apropriados que garantam níveis de desempenho adequados em cada nível da cadeia tecnológica, quando aplicáveis;

g) Utilizar um processo de gestão de incidentes consistente e bem documentado, incluindo as respetivas responsabilidades, designadamente, através da definição de um modelo de cooperação em caso de ocorrência ou de suspeitas de incidentes;

h) Adotar uma abordagem baseada no risco para o país ou região de armazenamento e de tratamento de dados, bem como considerações em matéria de segurança da informação;

i) Controlar o cumprimento dos requisitos relativos à eficácia e eficiência dos mecanismos de controlo implementados pelo prestador de serviços de computação em nuvem que permitem atenuar os riscos inerentes aos serviços prestados.

Artigo 41.º

Subcontratação em cadeia de funções ou atividades operacionais fundamentais ou importantes

Se a subcontratação em cadeia de funções operacionais fundamentais ou importantes, ou de parte das mesmas, for autorizada, o acordo de subcontratação de serviços de computação em nuvem deve:

a) Especificar os tipos de atividades que são excluídas da possível subcontratação em cadeia;

b) Indicar as condições a respeitar em caso de subcontratação em cadeia, designadamente o cumprimento integral e nos mesmos termos das obrigações impostas ao prestador de serviços de computação em nuvem pelo subcontratante em cadeia, bem como os direitos de acesso e de auditoria e a garantia de segurança dos dados e sistemas;

c) Indicar que o prestador de serviços de computação em nuvem é obrigado a supervisionar os serviços que subcontratou em cadeia e assume a plena responsabilidade pelos mesmos;

d) Incluir a obrigação de o prestador de serviços de computação em nuvem informar a empresa de seguros ou de resseguros de qualquer alteração prevista nos subcontratantes em cadeia ou nos serviços subcontratados em cadeia, suscetível de afetar a respetiva capacidade de cumprir as suas responsabilidades no âmbito do acordo de subcontratação de serviços de computação em nuvem, mediante um prazo de notificação que permita que a empresa realize, pelo menos, uma avaliação dos riscos que as alterações propostas representam antes de estas serem implementadas;

e) Quando um prestador de serviços de computação em nuvem planear introduzir alterações num subcontratante em cadeia ou em serviços subcontratados em cadeia, suscetíveis de afetar negativamente a avaliação dos riscos dos serviços acordados, assegurar que a empresa de seguros ou de resseguros tem o direito de se opor a tais alterações ou de rescindir e abandonar o contrato.

Artigo 42.º

Acompanhamento e supervisão de acordos de subcontratação de serviços de computação em nuvem

1 — As empresas de seguros e de resseguros devem acompanhar permanentemente as atividades dos seus prestadores de serviços de computação em nuvem, assim como as medidas de segurança e o cumprimento do nível de serviço acordado, de acordo com uma abordagem baseada no risco, prestando especial atenção à subcontratação de funções operacionais fundamentais ou importantes.

2 — Para efeitos do disposto no número anterior, as empresas de seguros e de resseguros devem criar mecanismos de acompanhamento e supervisão, que devem ter em conta, sempre que possível e adequado, a existência de subcontratação em cadeia de funções operacionais fundamentais ou importantes ou de uma parte das mesmas.

3 — O órgão de administração deve ser regularmente informado sobre os riscos identificados na subcontratação de funções ou atividades operacionais fundamentais ou importantes.

4 — A fim de assegurar o acompanhamento e a supervisão adequados dos seus acordos de subcontratação de serviços de computação em nuvem, as empresas de seguros e de resseguros devem mobilizar recursos suficientes com competências e conhecimentos adequados para monitorizar os serviços de computação em nuvem subcontratados.

5 — As pessoas responsáveis pelas atividades referidas no número anterior devem possuir os meios informáticos e tecnológicos necessários, assim como os devidos conhecimentos sobre a área de atividade.

Artigo 43.º

Direitos de rescisão e estratégias de saída

1 — Quando forem subcontratados serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes, as empresas de seguros e de resseguros devem dispor, ao abrigo do acordo de subcontratação em causa, de uma estratégia de saída claramente definida, que garanta a possibilidade de pôr termo ao acordo, se necessário.

2 — De modo a assegurar a possibilidade de rescindir o acordo de subcontratação sem prejudicar a continuidade e a qualidade dos serviços prestados aos tomadores de seguros, as empresas de seguros e de resseguros devem:

a) Elaborar e implementar planos de saída abrangentes, baseados em serviços, documentados e suficientemente testados, nomeadamente, através da realização de uma análise dos potenciais custos, impactos, recursos e implicações em termos de calendarização das várias opções de saída viáveis;

b) Identificar soluções alternativas e elaborar planos de transição adequados e viáveis que lhes permitam eliminar as atividades e dados subcontratados ao prestador de serviços de computação em nuvem e transferi-los para prestadores de serviços alternativos ou para a própria empresa;

c) Assegurar que o prestador de serviços de computação em nuvem presta apoio adequado durante o processo de transferência de dados, sistemas ou aplicações subcontratados para outro prestador de serviços ou para a própria empresa;

d) Acordar com o prestador de serviços de computação em nuvem que este, depois de transferir os dados novamente para a empresa, procede ao respetivo apagamento integral, de forma segura, em todas as regiões.

3 — As soluções a que se refere a alínea *b)* do número anterior devem ser definidas tendo em conta os desafios que possam surgir devido à localização dos dados, bem como mediante a adoção das medidas necessárias para garantir a continuidade da atividade durante a fase de transição.

4 — Na elaboração das estratégias de saída, as empresas de seguros e de resseguros devem:

a) Definir os objetivos da estratégia de saída;

b) Definir os fatores que devem desencadear a saída, designadamente, indicadores-chave de risco alertando para um nível de serviço inaceitável;

c) Realizar uma análise do impacto das atividades que seja proporcional às atividades subcontratadas, a fim de identificar os recursos humanos e materiais que seriam necessários para implementar o plano de saída e o tempo necessário para executá-lo;

d) Atribuir funções e responsabilidades para gerir os planos de saída e o processo de transição;

e) Definir critérios de sucesso para a transição.

Artigo 44.º

Supervisão dos acordos de subcontratação de serviços de computação em nuvem pela ASF

1 — A ASF analisa os impactos decorrentes dos acordos de subcontratação de serviços de computação em nuvem celebrados pelas empresas de seguros e de resseguros, no âmbito dos seus processos de supervisão.

2 — A análise dos impactos a que se refere o número anterior incide, em particular, nos acordos relacionados com a subcontratação de funções ou atividades operacionais fundamentais ou importantes.

3 — Ao supervisionar os acordos de subcontratação de serviços de computação em nuvem celebrados pelas empresas de seguros e de resseguros, a ASF tem em consideração os seguintes riscos:

a) Os riscos relacionados com as TIC;

b) Outros riscos operacionais, incluindo os riscos jurídicos e de conformidade, os riscos associados à subcontratação e gestão por terceiros;

c) Os riscos reputacionais;

d) Os riscos de concentração, incluindo a nível nacional ou setorial.

4 — Na sua avaliação, a ASF inclui os seguintes aspetos, de acordo com uma abordagem baseada no risco:

a) A adequação e eficácia dos processos operacionais e de governação da empresa de seguros ou de resseguros relacionados com a aprovação, execução, acompanhamento, gestão e renovação dos acordos de subcontratação de serviços de computação em nuvem;

b) Se a empresa de seguros ou de resseguros dispõe de recursos suficientes, com competências e conhecimentos adequados, para acompanhar os serviços de computação em nuvem subcontratados;

c) Se a empresa de seguros ou de resseguros identifica e gere todos os riscos referidos no presente título.

5 — Nos casos em que assuma funções de supervisor de grupo, a ASF assegura que os impactos da subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes são refletidos na avaliação do risco de supervisão do grupo, tendo em conta os requisitos previstos nos n.os 3 e 4, assim como a governação e as características operacionais individuais do grupo.

6 — Se a subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes envolver mais do que uma empresa de seguros ou de resseguros em diferentes Estados membros, e for gerida de forma

centralizada pela empresa-mãe ou por uma filial do grupo, nomeadamente uma empresa de serviços por conta da empresa ou do grupo, tal como o prestador de serviços TIC do grupo, o supervisor do grupo ou as autoridades competentes para supervisionar as empresas envolvidas na referida subcontratação devem discutir, no seio do colégio de supervisores, quando relevante, o respetivo impacto no perfil de risco do grupo.

7 — Sempre que sejam identificadas preocupações que permitam concluir que uma empresa de seguros ou de resseguros já não dispõe de mecanismos de governação sólidos ou não cumpre os requisitos regulamentares aplicáveis, a ASF adota medidas adequadas, nomeadamente exigindo à empresa que, num prazo razoável, melhore o seu mecanismo de governação, limite ou restrinja o âmbito das funções subcontratadas ou cesse um ou mais acordos de subcontratação.

8 — Atendendo à necessidade de assegurar a continuidade da atividade da empresa de seguros ou de resseguros, a cessação de contratos referida no número anterior pode ser especialmente necessária caso não seja possível assegurar a supervisão e aplicação dos requisitos regulamentares através de outras medidas.

TÍTULO IV

Disposições finais e transitórias

Artigo 45.º

Regime transitório

1 — Até 31 de dezembro de 2022, as empresas de seguros e de resseguros devem rever e alterar em conformidade com o disposto no título III da presente norma regulamentar as atuais disposições dos respetivos acordos de subcontratação de funções ou atividades operacionais fundamentais ou importantes.

2 — Se a revisão dos acordos de subcontratação de funções fundamentais ou importantes não estiver concluída até 31 de dezembro de 2022, as empresas de seguros e de resseguros devem informar a ASF, dando nota das medidas implementadas para concluir essa revisão ou a eventual estratégia de saída desses acordos.

3 — A ASF pode conceder uma prorrogação do prazo para a conclusão da revisão dos acordos de subcontratação de funções fundamentais ou importantes, sempre que adequado, mediante a apresentação de um pedido das empresas de seguros ou de resseguros devidamente fundamentado.

4 — Os requisitos de documentação previstos no artigo 33.º relativamente aos acordos de subcontratação de serviços de computação em nuvem relacionados com funções ou atividades operacionais fundamentais ou importantes devem ser implementados até 31 de dezembro de 2022.

Artigo 46.º

Início de vigência

A presente norma regulamentar entra em vigor 30 dias após a data da sua publicação.

Em 7 de junho de 2022. — O CONSELHO DE ADMINISTRAÇÃO: *Margarida Corrêa de Aguiar*, presidente — *Filipe Aleman Serrano*, vice-presidente.