DIÁRIO OFICIAL DA UNIÃO

Publicado em: 03/08/2021 | Edição: 145 | Seção: 1 | Página: 23

Órgão: Ministério da Economia/Superintendência de Seguros Privados

CIRCULAR SUSEP Nº 638, DE 27 DE JULHO DE 2021

Dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

A SUPERINTENDENTE DA SUPERINTENDÊNCIA DE SEGUROS PRIVADOS - SUSEP, no uso das atribuições que lhe conferem a alínea "b" do art. 36 do Decreto-Lei nº 73, de 21 de novembro de 1966; o parágrafo único do art. 3º da Lei Complementar nº 126, de 15 de janeiro de 2007; o § 2º do art. 3º do Decreto-Lei nº 261, de 28 de fevereiro de 1967, com a redação dada pela Lei Complementar nº 137 de 26 de agosto de 2010; e o art. 74 da Lei Complementar nº 109, de 29 de maio de 2001, e considerando o que consta do Processo Susep nº 15414.600373/2021-23, resolve:

CAPÍTULO I

DO OBJETO E DO ÂMBITO DE APLICAÇÃO

Art. 1º Dispor sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

CAPÍTULO II

DAS DEFINIÇÕES

Art. 2º Para efeitos desta Circular, consideram-se:

I - supervisionadas: sociedades seguradoras, EAPCs, sociedades de capitalização e resseguradores locais;

II - segurança cibernética: conjunto de estratégias, políticas e padrões voltados à mitigação do risco cibernético;

III - risco cibernético: possibilidade de ocorrência de perdas resultantes do comprometimento da confidencialidade, integridade ou disponibilidade de dados e informações em suporte digital, em decorrência da sua manipulação indevida ou de danos a equipamentos e sistemas utilizados para seu armazenamento, processamento ou transmissão;

IV - dados relevantes: dados pessoais, conforme definido na legislação em vigor, dados relativos a clientes ou a processos críticos de negócio, bem como quaisquer outros dados ou informações considerados sensíveis de acordo com as diretrizes estabelecidas pela supervisionada;

V - serviços relevantes de processamento ou armazenamento de dados: serviços de processamento ou armazenamento de dados, inclusive de computação em nuvem, que:

a) envolvam acesso ou manipulação de dados relevantes; ou

b) suportem atividades que a supervisionada considere essenciais para a continuidade de seu negócio;

VI - incidentes relevantes: eventos adversos, decorrentes ou não de atividade maliciosa, que, conforme parâmetros definidos pela supervisionada, comprometam substancialmente:

a) a confidencialidade, integridade ou disponibilidade de dados relevantes; ou

b) serviços relevantes de processamento ou armazenamento de dados;

VII - computação em nuvem: serviço que permite acesso por demanda, e independentemente da localização, a um conjunto compartilhado de recursos configuráveis de computação, provisionados com esforços mínimos de gestão ou de interação com o prestador de serviços;

VIII - órgãos de administração: Conselho de Administração e diretoria; e

IX - colaboradores: administradores, funcionários, prestadores de serviços terceirizados e demais parceiros relevantes da supervisionada.

CAPÍTULO III

DAS DISPOSIÇÕES GERAIS

Art. 3º A segurança cibernética inserir-se-á no contexto geral do Sistema de Controles Internos (SCI) e da Estrutura de Gestão de Riscos (EGR), conforme disposto na regulamentação que os define, devendo a supervisionada, complementarmente:

I - observar, na adoção de tratamentos e controles para os riscos cibernéticos, as boas práticas nacionais e internacionais de segurança cibernética, pelo menos no que se refere a:

a) segurança física de equipamentos e instalações;

b) controle de acesso a sistemas e informações;

c) criptografia;

d) proteção contra softwares maliciosos;

e) manutenção de cópias de segurança de dados e informações;

f) manutenção de registros (logs) de atividades dos usuários, exceções e falhas;

g) técnicas de proteção de redes e de segurança das comunicações; e

h) desenvolvimento e aquisição de sistemas; e

II - promover ações voltadas à disseminação da cultura de segurança cibernética, incluindo programa de capacitação contínua de colaboradores, com base na sensibilidade das informações por eles manipuladas.

Parágrafo único. Para fins da regulamentação mencionada no caput:

I - os riscos cibernéticos deverão ser considerados na categoria risco operacional, de uso obrigatório; e

II - a política de segurança cibernética, de que trata o capítulo IV, deverá ser considerada uma política complementar à política de gestão de riscos, aplicando-se a ela os requisitos definidos para tais políticas complementares.

CAPÍTULO IV

DA POLÍTICA DE SEGURANÇA CIBERNÉTICA

Art. 4º A supervisionada deverá possuir uma política de segurança cibernética que contemple, no mínimo:

I - os objetivos de segurança cibernética;

II - o compromisso dos órgãos de administração com a segurança cibernética e com a melhoria contínua dos processos, procedimentos e controles a ela relacionados; e

III - os parâmetros e diretrizes para:

a) classificação de dados, incidentes e serviços quanto a sua relevância, considerando o disposto no art. 2º, incisos IV a VI;

b) implementação de processos, procedimentos e controles de segurança cibernética, com base na classificação mencionada na alínea "a"; e

c) terceirização de serviços de processamento e armazenamento de dados, em especial os relevantes, incluindo requisitos mínimos e alçadas relativas à aprovação e alteração de contratos.

Parágrafo único. A política de segurança cibernética deverá ser compatível com o porte da supervisionada, a natureza e a complexidade de suas operações e seu grau de exposição ao risco cibernético.

CAPÍTULO V

DA PREVENÇÃO E DO TRATAMENTO DE INCIDENTES

Art. 5º A supervisionada deverá possuir, e manter atualizados, processos, procedimentos e controles efetivos para:

I - identificar e reduzir vulnerabilidades de forma proativa; e

II - detectar, responder e recuperar-se de incidentes.

Art. 6º Os processos, procedimentos e controles mencionados no inciso II do art. 5º deverão contemplar, no mínimo:

I - monitoramento contínuo da rede de comunicação, por meio de técnicas que auxiliem na detecção de incidentes;

II - avaliação da natureza, abrangência e impacto dos incidentes detectados, de acordo com graus de criticidade previamente estabelecidos, considerando a relevância dos dados, sistemas ou serviços envolvidos e seu grau de comprometimento;

III - adoção tempestiva de medidas para a contenção dos efeitos do incidente;

IV - restabelecimento dos sistemas ou serviços afetados e retorno à sua condição normal de operação;

V - registro do incidente;

VI - compartilhamento de informações sobre incidentes relevantes com as demais supervisionadas, em formato mutuamente acordado, observada a garantia de sigilo das informações confidenciais e segredos comerciais;

VII - comunicação com as partes afetadas pelo incidente, sobretudo clientes; e

VIII - identificação e tratamento das vulnerabilidades exploradas.

§ 1º As medidas de contenção mencionadas no inciso III do caput deverão incluir, sempre que pertinente, comunicação prévia com prestadores de serviços, parceiros e outras partes potencialmente envolvidas, com vistas à adoção de uma resposta coordenada.

§ 2º A supervisionada deverá certificar-se de que o restabelecimento mencionado no inciso IV do caput seja conduzido de forma segura, sem dar margem a vulnerabilidades que possam agravar os impactos do incidente em andamento ou aumentar substancialmente o risco de novos incidentes.

§ 3º A supervisionada deverá implementar mecanismos de conciliação entre o registro de incidentes mencionado no inciso V do caput e o banco de dados de perdas operacionais (BDPO), se existente, pelo menos para os incidentes que resultem em perda operacional.

Art. 7º Os processos e procedimentos de que tratam os incisos II a IV do art. 6º deverão ser previstos no plano de continuidade de negócios, pelo menos para cenários de ataques e outros eventos que, na avaliação da supervisionada, possam ocasionar:

I - danos a infraestruturas de tecnologia da informação ou sistemas de comunicação considerados críticos;

II - acesso, modificação, exclusão ou divulgação não autorizados de dados relevantes; ou

III - interrupção de serviços relevantes de processamento e armazenamento de dados.

Art. 8º A supervisionada deverá comunicar à Susep, no prazo máximo de 5 (cinco) dias úteis a partir do conhecimento do evento, a ocorrência de incidentes relevantes, detalhando a extensão do dano causado e, se for o caso, as ações em curso para regularização completa da situação e os respectivos responsáveis e prazos.

Art. 9º A supervisionada deverá elaborar um relatório anual sobre prevenção e tratamento de incidentes, contendo, no mínimo:

I - descrição dos incidentes relevantes detectados, com detalhamento das respectivas causas, efeitos e respostas adotadas;

II - dados estatísticos referentes à totalidade dos incidentes detectados, contemplando sua quantidade e principais causas e efeitos;

III - resultados dos testes relativos aos cenários previstos no plano de continuidade de negócios, conforme disposto no art. 7º; e

IV - descrição das principais vulnerabilidades identificadas e das ações adotadas para seu tratamento.

§ 1º Para as ações mencionadas no inciso IV do caput, que ainda estejam em curso, o relatório deverá conter indicação dos respectivos responsáveis e prazos.

§ 2º O relatório deverá ser encaminhado pelo menos:

I - aos órgãos de administração;

II - aos Comitês de Auditoria e de Riscos, se houver; e

III - ao diretor responsável pelos controles internos e, se houver, à unidade de gestão de riscos.

§ 3º As pessoas, órgãos e unidades mencionadas no § 2º deverão considerar o conteúdo do relatório no desempenho de suas respectivas atribuições, especialmente no que se refere à avaliação da efetividade dos processos, procedimentos e controles de segurança cibernética.

CAPÍTULO VI

DA TERCEIRIZAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS

Art. 10. Quando da terceirização de serviços de processamento e armazenamento de dados, a supervisionada deverá:

I - dispor dos recursos, competências e práticas de governança necessários ao adequado monitoramento dos serviços a serem contratados;

II - certificar-se de que os potenciais prestadores de serviços possuem capacidade para cumprir as exigências previstas no art. 11; e

III - no caso de serviços relevantes de processamento e armazenamento de dados, informar à Susep, em até 30 (trinta) dias após a formalização dos contratos:

a) os serviços relevantes a serem contratados;

b) a denominação da empresa contratada, e, se houver, das subcontratadas responsáveis pelos serviços mencionados na alínea "a"; e

c) sempre que possível, os países e as regiões em cada país onde os serviços mencionados na alínea "a" poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados.

Parágrafo único. As alterações contratuais que modifiquem alguma das alíneas "a" a "c" do inciso III do caput deverão ser informadas à Susep em até 30 (trinta) dias após sua formalização.

Art. 11. A supervisionada deverá exigir que os prestadores de serviços de processamento e armazenamento de dados:

I - observem as disposições legais e regulamentares em vigor;

II - disponibilizem informações e recursos de gestão que permitam à supervisionada monitorar adequadamente os serviços contratados;

III - possuam processos, procedimentos e controles de segurança cibernética não inferiores aos que a própria supervisionada adota para o mesmo grau de sensibilidade, podendo ser observados controles mitigatórios;

IV - garantam, por meio de controles físicos e/ou lógicos, que os dados da supervisionada e de seus clientes sejam devidamente segregados dos dados dos demais clientes do prestador de serviços;

V - notifiquem a supervisionada sobre a subcontratação de serviços relevantes;

VI - providenciem, em caso de extinção do contrato:

a) a transferência dos dados objeto do contrato ao novo prestador de serviços ou à supervisionada, conforme o caso; e

b) a exclusão dos dados objeto do contrato, após a transferência prevista na alínea "a" e a confirmação, por parte da supervisionada, da integridade e da disponibilidade dos dados recebidos; e

VII - não causem qualquer tipo de embaraço à atuação da Susep.

§ 1º Nos casos de serviços relevantes de processamento e armazenamento de dados, a supervisionada, a fim de garantir o disposto no inciso III do caput, deverá recorrer a pelo menos um dos seguintes procedimentos:

I - exigência de certificação, relativa ao serviço a ser contratado, concedida por instituição independente; ou

II - realização de diligências prévias (due diligence).

§ 2º A política de segurança cibernética poderá estabelecer exceções ao disposto no inciso III do caput, para serviços de processamento e armazenamento de dados que não sejam classificados como relevantes, definindo expressamente os requisitos mínimos de segurança cibernética a serem observados.

§ 3º Para atendimento ao inciso VII do caput, a supervisionada deverá exigir que o prestador de serviços garanta à Susep, quando solicitado, o acesso de consulta aos dados objeto do contrato, às informações referentes aos serviços prestados e aos contratos e acordos firmados para a sua execução, cabendo à supervisionada certificar-se de que a legislação e a regulamentação dos países e das regiões em cada país onde os serviços poderão ser prestados não impõem restrições para o referido acesso.

§ 4º Os contratos de prestação de serviços de processamento e armazenamento de dados, exceto quando de adesão, deverão dispor expressamente sobre as exigências mencionadas neste artigo.

Art. 12. A terceirização de serviços de processamento e armazenamento de dados não exime a supervisionada de sua responsabilidade pelo cumprimento da legislação e da regulamentação em vigor e pela garantia da confidencialidade, integridade e disponibilidade dos dados em poder do prestador de serviços.

Art. 13. A supervisionada deverá definir e documentar estratégias para substituição de prestadores de serviços ou para execução própria dos serviços terceirizados, a serem adotadas na hipótese de descontinuidade da prestação de serviços relevantes de processamento e armazenamento de dados.

Art. 14. O disposto neste Capítulo aplica-se a toda e qualquer terceirização de serviços de processamento e armazenamento de dados, inclusive de computação em nuvem, com exceção apenas do serviço de registro das operações da supervisionada em sistema de registro previamente homologado pela Susep e administrado por entidade registradora devidamente credenciada nos termos da regulamentação específica.

CAPÍTULO VII

DAS DISPOSIÇÕES TRANSITÓRIAS E FINAIS

Art. 15. A supervisionada deverá conservar, nos termos da regulamentação vigente, as versões atuais e anteriores dos seguintes documentos:

I - política de segurança cibernética, de que trata o Capítulo IV;

II - relatório sobre prevenção e tratamento de incidentes, de que trata o art. 9º;

III - contratos de terceirização de serviços relevantes de processamento e armazenamento de dados, de que trata o § 4º do art. 11; e

IV - demais documentos que comprovem o atendimento ao disposto nesta Circular.

Art. 16. Os contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da data de início de vigência desta Circular deverão ser adequados até 1º de setembro de 2024.

Art. 17. As supervisionadas terão os seguintes prazos para adequação ao disposto nesta Circular:

I - para as supervisionadas enquadradas nos segmentos S1 ou S2: até 30 de junho de 2022; e

II - para as supervisionadas enquadradas nos segmentos S3 ou S4: até 1º de setembro de 2022.

Art. 18. Esta Circular entra em vigor em 1º de setembro de 2021.

SOLANGE PAIVA VIEIRA