SUPERINTENDÊNCIA DE SEGUROS PRIVADOS

MINUTA DE CIRCULAR

Dispõe sobre requisitos de segurança cibernética, a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPC), 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,

R E S O L V E :

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 (EAPC), sociedades de capitalização e resseguradores locais.

CAPÍTULO II

DAS DEFINIÇÕES

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

I - supervisionadas: sociedades seguradoras, entidades abertas de previdência complementar (EAPC), 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, a processos críticos de negócio ou quaisquer outros dados ou informações considerados sensíveis de acordo com as diretrizes estabelecidas pela supervisionada;

V - incidentes relevantes: eventos adversos, decorrentes ou não de atividade maliciosa, que comprometam a confidencialidade, integridade ou disponibilidade de dados relevantes;

VI - serviços relevantes de processamento ou armazenamento de dados: serviços, inclusive de computação em nuvem, que envolvam processamento ou armazenamento de dados relevantes;

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;

IX - órgão de administração máximo: o Conselho de Administração ou, se inexistente, a diretoria; e

X - 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 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 de elaboração do inventário de riscos, os riscos cibernéticos deverão ser considerados na categoria risco operacional, de uso obrigatório.

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 - as diretrizes para:

a) classificação dos dados quanto a sua sensibilidade; e

b) implementação de processos, procedimentos e controles de segurança cibernética.

Parágrafo único. As diretrizes de que trata a alínea “b” do inciso III do **caput** poderão, no que couber, estar contidas na política de gestão de riscos, e deverão:

I - considerar o grau de sensibilidade dos dados envolvidos; e

II - ser desdobradas em normativos internos específicos.

Art. 5º A política de segurança cibernética deverá ser:

I - compatível com o porte da supervisionada, a natureza e a complexidade de suas operações e seu grau de exposição ao risco cibernético;

II - registrada formalmente por escrito;

III - aprovada pelo órgão de administração máximo da supervisionada;

IV - divulgada:

a) aos colaboradores da supervisionada, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções que desempenham; e

b) aos clientes da supervisionada, pelo menos em versão resumida que contenha suas linhas gerais; e

V - revisada, no mínimo, anualmente.

Parágrafo único. No caso de supervisionadas atendidas por SCI/EGR unificado, a política de segurança cibernética deverá ser única, estabelecida e formalizada pela supervisionada indicada na forma da regulação em vigor, a qual será responsável pela aprovação prevista no inciso III do **caput**.

CAPÍTULO V

DA PREVENÇÃO E DO TRATAMENTO DE INCIDENTES

Art. 6º 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. 7º Os processos, procedimentos e controles mencionados no inciso II do art. 6º 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, considerando a relevância das informações envolvidas 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 a sua condição normal de operação;

V - registro do incidente;

VI - compartilhamento de informações sobre o incidente com as demais supervisionadas;

VII - comunicação com clientes e outras partes afetadas; e

VIII - identificação e redução 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. 8º Os processos e procedimentos de que tratam os incisos II a IV do art. 7º 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. 9º A supervisionada deverá comunicar à Susep, no prazo máximo de 5 (cinco) dias úteis, a ocorrência de incidentes relevantes que tenham tido impactos concretos, 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. 10. A supervisionada deverá elaborar um relatório anual sobre prevenção e tratamento de incidentes, abordando, no mínimo:

I - os incidentes detectados, com descrição das respectivas causas, efeitos e respostas adotadas;

II - os resultados dos testes relativos aos cenários previstos no plano de continuidade de negócios, conforme disposto no art. 8º; e

III - as vulnerabilidades identificadas, de forma proativa ou em virtude dos incisos I e II, e as ações implementadas para sua redução.

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

§ 2º O relatório deverá ser aprovado pelo diretor de que trata o art. 16 e 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. 11. Previamente à 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. 12; e

III - no caso de serviços relevantes de processamento e armazenamento de dados:

a) obter aprovação do órgão de administração máximo; e

b) informar à Susep:

1. a denominação da empresa a ser contratada;

2. os serviços relevantes a serem contratados; e

3. os países e as regiões em cada país onde os serviços serão prestados e os dados serão armazenados, processados e gerenciados.

§ 1º As alterações contratuais que modifiquem algum dos itens 1 a 3 da alínea “b” do inciso III devem passar novamente pelo procedimento previsto nas alíneas “a” e “b” do citado inciso.

§ 2º O prazo para prestar as informações referentes à alínea “b” do inciso III é:

I - 20 (vinte) dias corridos antes da formalização de contratos prestados no exterior; e

II - 10 (dez) dias corridos após a formalização de contratos prestados no Brasil.

Art. 12. 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 processamento e armazenamento de dados de mesmo grau de sensibilidade;

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 - possuam, pelo menos no caso de serviços relevantes de processamento e armazenamento de dados, certificação relativa ao tipo de serviço contratado;

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

VII - 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 da integridade e da disponibilidade dos dados recebidos; e

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

§ 1º Para atendimento ao inciso VIII do **caput**, a supervisionada deverá exigir que o prestador de serviços garanta à Susep o acesso 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.

§ 2º Os contratos de prestação de serviços de processamento e armazenamento de dados deverão dispor expressamente sobre as exigências mencionadas neste artigo.

Art. 13. 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. 14. 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. 15. 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. 16. A supervisionada deverá designar um diretor responsável pela implementação do disposto nesta Circular.

Parágrafo único. O diretor de que trata o **caput** não poderá ser o mesmo designado como responsável pelos controles internos.

Art. 17. 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. 10;

III - contratos de terceirização de serviços de processamento e armazenamento de dados, de que trata o § 2º do art. 12; e

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

Art. 18. 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 em até 2 (dois) anos a partir da referida data.

Art. 19. Excepcionalmente, os prazos de adequação para atendimento dos requisitos estabelecidos por esta Circular são:

I - para as supervisionadas enquadradas no segmento S3 no momento de entrada em vigor desta Circular: até 1° de julho de 2022; e

II - para as supervisionadas enquadradas no segmento S4 no momento de entrada em vigor desta Circular: até 3 de outubro de 2022.

Art. 20. Esta Circular entra em vigor em 03 de janeiro de 2022.

Documento assinado eletronicamente por **CESAR DA ROCHA NEVES (MATRÍCULA 1338145)**, **Coordenador-Geral**, em 30/04/2021, às 09:34, conforme horário oficial de Brasília, com fundamento nos art. artigos 369, 405 e 425 da lei nº 13.105/2015 c/c Decreto nº 8.539/2015 e Instruções Susep 78 e 79 de 04/04/2016 .

A autenticidade do documento pode ser conferida no site https://sei.susep.gov.br/sei/controlador_externo.php?acao=documento_conferir&acao_origem=documento_conferir&id_orgao_acesso_externo=0 informando o código verificador **1004659** e o código CRC **768C2EDE**.

Referência: Processo nº 15414.600373/2021-23 SEI nº 1004659