4 de maio de 2021

TOZZINIFREIRE ADVOGADOS

Consulta Pública Segurança Cibernética:

CP nº 15

INTRO

- Foi colocada em Consulta Pública minuta de Circular SUSEP dispondo sobre requisitos de segurança cibernética;
- Aplicação para: seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais;
- A gestão do risco cibernético, inserida no contexto do Sistema de Controles Internos e da Estrutura de Gestão de Risco, deve estar alinhada a uma política de segurança cibernética, mediante o estabelecimento de procedimentos relativos à prevenção e resposta a incidentes, com critérios mínimos quando da terceirização de serviços de processamento e armazenamento de dados (alinhamento com LGPD e outros supervisores do Sistema Financeiro Nacional);
- Data-limite para sugestões ao texto proposto pela SUSEP: **02/06/2021**;
- Em sendo aprovada, passará a viger a partir de 03/01/2022.

DISPOSIÇÕES GERAIS

OBRIGAÇÕES DA SUPERVISIONADA:

- 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.

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

POLÍTICA DE SEGURANÇA CIBERNÉTICA

DEVE CONTEMPLAR:

- ✓ Os objetivos de segurança cibernética;
- ✓ O compromisso dos órgãos de administração com a segurança cibernética e com a melhoria contínua dos processos, procedimentos e controles a ela relacionados; e
- ✓ As diretrizes para: a) classificação dos dados quanto a sua sensibilidade; e b) implementação de processos, procedimentos e controles de segurança cibernética, que poderão, no que couber, estar contidas na política de gestão de riscos, considerando o grau de sensibilidade dos dados envolvidos;

DEVE SER:

- ✓ Compatível com o porte da supervisionada, a natureza e a complexidade de suas operações e seu grau de exposição ao risco cibernético;
- ✓ Registrada formalmente por escrito;
- ✓ Aprovada pelo órgão de administração máximo da supervisionada (Conselho de Administração ou, se inexistente, diretoria);
- ✓ 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
- ✓ Revisada, no mínimo, anualmente.

No caso de supervisionadas atendidas por SCI/EGR unificado, a política de segurança cibernética deverá ser única.

PREVENÇÃO E TRATAMENTO DE INCIDENTES

A supervisionada deverá possuir, e manter atualizados, processos, procedimentos e controles efetivos para:

- ✓ identificar e reduzir vulnerabilidades de forma proativa; e
- ✓ detectar, responder e recuperar-se de incidentes.

Os processos, procedimentos e controles deverão contemplar, no mínimo:

- ✓ monitoramento contínuo da rede de comunicação, por meio de técnicas que auxiliem na detecção de incidentes;
- ✓ avaliação da natureza, abrangência e do impacto dos incidentes detectados, considerando a relevância das informações envolvidas e seu grau de comprometimento;
- ✓ adoção tempestiva de medidas para a contenção dos efeitos do incidente (comunicação prévia com prestadores de serviços, parceiros e outras partes potencialmente envolvidas de forma coordenada, sempre que possível);
- ✓ restabelecimento dos sistemas ou serviços afetados e retorno a sua condição normal de operação (de forma segura);
- ✓ registro do incidente (implementação de mecanismos de conciliação com o banco de dados de perdas operacionais - BDPO);
- ✓ compartilhamento de informações sobre o incidente com as demais supervisionadas;
- ✓ comunicação com clientes e outras partes afetadas; e
- ✓ identificação e redução das vulnerabilidades exploradas.

Os processos e procedimentos **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: danos a infraestruturas de tecnologia da informação ou sistemas de comunicação considerados críticos; acesso, modificação, exclusão ou divulgação não autorizados de dados relevantes; ou interrupção de serviços relevantes de processamento e armazenamento de dados.

COMUNICAÇÃO À SUSEP:

- ✓ **A supervisionada deverá comunicar à SUSEP, no prazo máximo de 5 dias úteis, a ocorrência de incidentes relevantes** que tenham impactos concretos, detalhando a extensão do dano causado e, se for o caso, as ações em curso para regularização completa da situação, os respectivos responsáveis e prazos.

Incidentes Relevantes: eventos adversos, decorrentes ou não de atividade maliciosa, que comprometam a confidencialidade, integridade ou disponibilidade de dados relevantes.

Dados Relevantes: dados pessoais, conforme LGPD, 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.

RELATÓRIO ANUAL

A supervisionada deverá elaborar um relatório anual sobre prevenção e tratamento de incidentes, abordando, no mínimo:

- ✓ os incidentes detectados, com descrição das respectivas causas, efeitos e respostas adotadas;
- ✓ os resultados dos testes relativos aos cenários previstos no plano de continuidade de negócios,
- ✓ as vulnerabilidades identificadas, de forma proativa ou em virtude do detectado, e as ações implementadas para sua redução, com indicação dos responsáveis e prazos.

O relatório deverá ser aprovado pelo diretor responsável e encaminhado pelo menos:

- ✓ aos órgãos de administração;
- ✓ aos Comitês de Auditoria e de Riscos, se houver;
- ✓ ao diretor responsável pelos controles internos e, se houver, à unidade de gestão de riscos.

As pessoas, órgãos e unidades acima 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.

Atenção: responsabilidade da pessoa física.

DIRETOR RESPONSÁVEL

A supervisionada deverá designar um diretor responsável pela implementação do disposto na norma.

O diretor não poderá ser o mesmo designado como responsável pelos controles internos.

TERCEIRIZAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS

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 (SRO).

Previamente à terceirização de serviços de processamento e armazenamento de dados, a supervisionada deverá:

- ✓ dispor dos recursos, competências e práticas de governança necessários ao adequado monitoramento dos serviços a serem contratados;
- ✓ certificar-se de que os potenciais prestadores de serviços possuem capacidade para cumprir as exigências previstas na norma; e
- ✓ no caso de serviços relevantes de processamento e armazenamento de dados:

I. obter aprovação do órgão de administração máximo (Conselho de Administração ou, se inexistente, Diretoria); e

II. informar à SUSEP no prazo de 20 dias corridos **antes** da formalização de contratos prestados no exterior e de 10 dias corridos **após** a formalização de contratos prestados no Brasil:

a) a denominação da empresa a ser contratada;
b) os serviços relevantes a serem contratados; e
c) os países e as regiões em cada país onde os serviços serão prestados e os dados serão armazenados, processados e gerenciados (alterações contratuais que modificarem esses itens também devem ser submetidas).

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

- ✓ observem as disposições legais e regulamentares em vigor;
- ✓ disponibilizem informações e recursos de gestão que permitam à supervisionada monitorar adequadamente os serviços contratados;
- ✓ 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;
- ✓ 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;
- ✓ possuam, pelo menos no caso de serviços relevantes de processamento e armazenamento de dados, certificação relativa ao tipo de serviço contratado;
- ✓ notifiquem a supervisionada sobre a subcontratação de serviços relevantes;
- ✓ 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 e a confirmação da integridade e da disponibilidade dos dados recebidos; e
- ✓ não causem qualquer tipo de embaraço à atuação da SUSEP (cabe 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 acesso).

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.

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.

A SUPERVISIONADA DEVERÁ GUARDAR as versões atuais e anteriores dos seguintes documentos: I - política de segurança cibernética, II - relatório sobre prevenção e tratamento de incidentes, III - contratos de terceirização de serviços de processamento e armazenamento de dados e IV - demais documentos que comprovem o atendimento ao disposto na norma.

PRAZOS

2 anos para adaptação dos contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da data de início de vigência da norma.

03/01/2022: previsão de entrada em vigor

01/07/2022: Adaptação para S3

03/10/2022: Adaptação para S4

Em sendo aprovada, a norma deverá ser observada em conjunto com a Lei Geral de Proteção de Dados (LGPD), com as normas da ANPD (Autoridade Nacional de Proteção de Dados), além da legislação consumerista (quando aplicável).

CONTATOS:

BÁRBARA BASSANI
bbassani@tozzinifreire.com.br

Seguros e Resseguros

CARLA DO COUTO HELLU BATTILANA
ccouto@tozzinifreire.com.br

Cybersecurity & Data Privacy

MARCELA WAKSMAN EJNISMAN
mejnisman@tozzinifreire.com.br

Cybersecurity & Data Privacy

PATRÍCIA HELENA MARTA MARTINS
pmarta@tozzinifreire.com.br

Cybersecurity & Data Privacy