4 de agosto de 2021

TOZZINIFREIRE ADVOGADOS

# Segurança Cibernética CIRCULAR SUSEP Nº 638

INTRO

Em 03/08/2021, foi publicada a Circular SUSEP nº 638, dispondo sobre requisitos de segurança cibernética, inserida no contexto geral do Sistema de Controles Internos (SCI) e da Estrutura de Gestão de Riscos (EGR).

Aplicação para: seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

Muitos dispositivos da norma foram simplificados se comparados ao regramento inicialmente proposto quando da Consulta Pública (por exemplo, no que se refere às regras de comunicação prévia de terceirização, bem como à supressão de um diretor específico e diferente daquele nomeado para controles internos). Por outro lado, foram mantidas exigências e foram inseridos controles específicos relacionados aos prestadores de serviços de processamento e armazenamento de dados.

## 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 (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.

- 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.

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

**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.**

## 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 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;
- ✓ adoção tempestiva de medidas para a contenção dos efeitos do incidente;
- ✓ restabelecimento dos sistemas ou serviços afetados e retorno à sua condição normal de operação;
- ✓ registro do incidente;
- ✓ 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;
- ✓ comunicação com as partes afetadas pelo incidente, sobretudo clientes; e
- ✓ identificação e tratamento 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 (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.

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.

## RELATÓRIO ANUAL

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

- ✓ descrição dos incidentes relevantes detectados, com detalhamento das respectivas causas, efeitos e respostas adotadas;
- ✓ dados estatísticos referentes à totalidade dos incidentes detectados, contemplando sua quantidade e principais causas e efeitos;
- ✓ resultados dos testes relativos aos cenários previstos no plano de continuidade de negócios; e
- ✓ descrição das principais vulnerabilidades identificadas e das ações adotadas para seu tratamento.

O relatório deverá ser encaminhado pelo menos: aos órgãos de administração; aos Comitês de Auditoria e de Riscos, se houver; e ao diretor responsável pelos controles internos e, se houver, à unidade de gestão de riscos.

As pessoas, órgãos e unidades 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.

## TERCEIRIZAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS

Quando da 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, informar à SUSEP, em até 30 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; e
c) sempre que possível, os países e as regiões em cada país onde os serviços mencionados poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados.

OBS.: As alterações contratuais que modifiquem alguma das alíneas "a" a "c" também deverão ser informadas à SUSEP em até 30 dias após sua formalização.

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 o mesmo grau de sensibilidade, podendo ser observados controles mitigatórios (mediante exigência de certificação concedida por instituição independente; ou realização de diligências prévias, exceto na hipótese de dispensa da política de segurança cibernética para serviços entendidos como não relevantes);**
- ✓ 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;
- ✓ 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 prevista na alínea "a", e a confirmação, por parte da supervisionada, da integridade e da disponibilidade dos dados recebidos; e
- ✓ não causem qualquer tipo de embaraço à atuação da SUSEP, 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.

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 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.

Referidas regras aplicam-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.

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

**01/09/2021:** Entrada em vigor da Circular

**30/06/2022:** Prazo de adequação para as supervisionadas S1 e S2

**01/09/2022:** Prazo de adequação para as supervisionadas S3 e S4

**01/09/2024:** Prazo de adequação para os contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da data de início de vigência da norma.

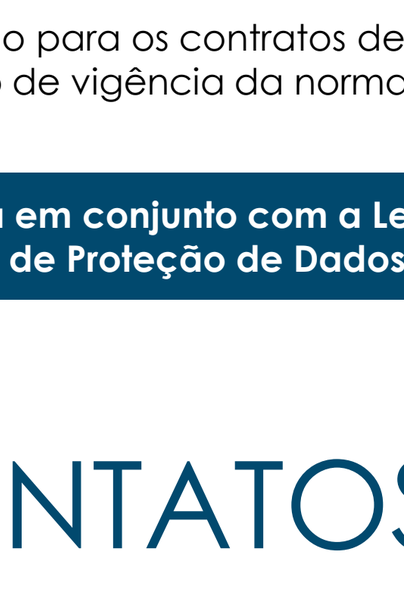
**A norma deverá ser observada em conjunto com a Lei Geral de Proteção de Dados (LGPD) e com as normas da ANPD (Autoridade Nacional de Proteção de Dados), além da legislação consumerista (quando aplicável).**

## CONTATOS:


**BÁRBARA BASSANI**
bbassani@tozzinifreire.com.br

Seguros e Resseguros

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

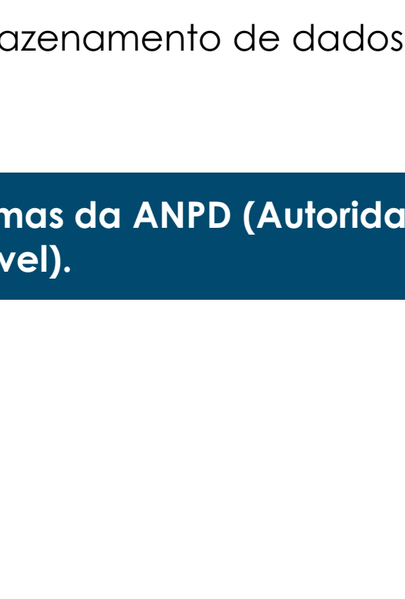


Cybersecurity & Data Privacy

**MARCELA WAKSMAN EJNISMAN**
mejnisman@tozzinifreire.com.br

Cybersecurity & Data Privacy

**PATRÍCIA HELENA MARTA MARTINS**
pmarta@tozzinifreire.com.br



Cybersecurity & Data Privacy