Circular estabelece diretrizes para políticas de segurança e contempla monitoramento de serviços terceirizados

A Superintendência de Seguros Privados (SUSEP) publicou, no dia 3 de agosto de 2021, a Circular SUSEP nº 638/2021, que contém os requisitos de segurança cibernética que devem ser observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais.

A norma insere a segurança cibernética no âmbito do Sistema de Controles Internos (SCI) e da Estrutura de Gestão de Riscos (EGR), estabelecendo a adoção de boas práticas nacionais e internacionais de segurança cibernética como o padrão de segurança para vários dos aspectos das atividades das entidades supervisionadas pela SUSEP. O objetivo é minimizar as vulnerabilidades dos sistemas empregados por meio do estabelecimento de padrões de segurança cibernética sem, contudo, desestimular a inovação.

Formulação de política de segurança cibernética

Um dos pontos principais do novo normativo diz respeito a necessidade de se formular e implementar uma política de segurança cibernética complementar à política de gestão de riscos. Ela deve contemplar, no mínimo, os seus objetivos, o compromisso dos órgãos de administração com a segurança cibernética e com a melhoria dos processos, procedimentos e controles a ela relacionados. Além disso, deve conter os parâmetros e as diretrizes para a classificação de dados, a implementação de procedimentos de segurança cibernética e a terceirização de serviços correlatos.

A norma disciplina a prevenção e o tratamento dos incidentes cibernéticos, exigindo que as supervisionadas possuam e mantenham atualizados os processos, procedimentos e controles efetivos para identificar e reduzir as vulnerabilidades de forma proativa, ou seja, capazes não apenas de detectar, mas de responder aos incidentes e atuar na recuperação das suas consequências. Tais processos e procedimentos precisam constar do plano de continuidade de negócios de cada uma das entidades supervisionadas pela SUSEP.

Os incidentes relevantes identificados pelas supervisionadas serão objeto de um relatório anual sobre a prevenção e o tratamento de incidentes, devendo descrevê-los e apresentar o resultado da apuração de suas causas, efeitos e as respostas adotadas pelas supervisionadas. O relatório precisa ser encaminhado aos órgãos de administração da supervisionada, Comitês de Auditoria e de Riscos, diretor responsável pelos controles internos e à unidade de gestão de riscos de cada supervisionada, e deverá:

- Conter dados estatísticos sobre os incidentes detectados, acompanhado do apontamento de ações para o seu tratamento;

- Indicar a responsabilidade sobre os incidentes e prazos para a tomada de ações pertinentes aos mesmos.

Segurança cibernética em serviços terceirizados

A SUSEP cuidou de regulamentar os requisitos de segurança cibernética também para a hipótese em que supervisionada terceiriza os serviços de processamento e armazenamento de dados. Nesses casos, a supervisionada terá que dispor de recursos, competências e práticas de governança aptos ao monitoramento regular dos serviços que serão contratados de terceiros, bem como certificar-se da capacidade técnica dos mesmos para a prestação do serviço. A terceirização precisa ser comunicada à SUSEP pela entidade supervisionada em até 30 dias após a formalização dos contratos.

O dever de informar à SUSEP não se encerra no momento da contratação, mas se mantém durante toda a execução do contrato de prestação de serviços, de maneira que a supervisionada fica obrigada a informar a autoridade a respeito de qualquer alteração do objeto da contratação, bem como da forma e localidade em que os serviços serão prestados.

A Circular SUSEP nº 638/2021 faculta às supervisionadas que optarem pela terceirização do processamento e armazenamento de dados competência para monitorar a prestação dos serviços pelos terceiros contratados. Nesse sentido, atribui às supervisionadas o dever de exigir dos prestadores de serviços:

- A observância das disposições legais e regulamentares incidentes sobre as suas atividades;

- A disponibilização de informações e ferramentas de gestão que permitam o exercício regular do monitoramento dos serviços contratados;

- A adoção de processos, procedimentos e controles de segurança não inferiores aos seus próprios, com igual gradação de sensibilidade aptos a garantir que os dados da supervisionada e de seus clientes estejam devidamente segregados dos dados dos demais clientes do prestador de serviços.

A Circular não exime as entidades supervisionadas de responsabilidade pela garantia da confidencialidade, integridade e disponibilidade dos dados em poder do prestador de serviços, bem como pelo cumprimento da legislação e regulamentação aplicáveis à proteção de dados.

Prazos para adequação à Circular SUSEP nº 638/202

O normativo entra em vigor no dia 1º de setembro de 2021 e prevê os seguintes prazos de adequação:

- Os contratos de terceirização de serviços de processamento e armazenamento de dados firmados antes da data de início da vigência da Circular terão até o dia 1º de setembro de 2024 para adequarem-se às suas disposições;

- As supervisionadas dos segmentos S1 ou S2 terão até o dia 30 de junho de 2022 para adequarem-se, o que inclui a formulação e implementação da política de segurança cibernética;

- As supervisionadas dos segmentos S3 e S4 terão até o dia 1º de setembro de 2022 para adequarem-se, o que inclui a formulação e implementação da política de segurança cibernética.

Fonte: Mattos Filho, em 18.08.2021