SUSEP edita novas regras de segurança cibernética para entidades supervisionadas

19.08.2021 4 minutos de leitura

Autores

Felipe Palhares

Áreas relacionadas

Proteção de Dados e Cybersecurity

Assuntos

Informativos | Proteção de Dados e Cybersecurity | Seguros | Segurança Cibernética

No dia 3 de agosto de 2021, foi publicada no Diário Oficial da União a Circular SUSEP nº 638/2021 ("Circular"), que dispõe sobre requisitos de segurança cibernética a serem observados por sociedades seguradoras, entidades abertas de previdência complementar, sociedades de capitalização e resseguradores locais.

As novas regras, que estão em linha com regulamentação similar disciplinada pelo Banco Central do Brasil para instituições financeiras e instituições de pagamento, podem exigir diversos ajustes em práticas, políticas, processos e contratos mantidos pelas entidades supervisionadas.

Em relação aos ajustes nas práticas da organização, a Circular estabelece a adoção de boas práticas de segurança cibernética, que incluem a adoção de criptografia, de defesas contra softwares maliciosos, de segurança física e lógica para proteção de equipamentos e redes, de controle de acesso a sistemas e informações, e de manutenção de cópias de segurança e logs de atividades dos usuários. Também passa a ser obrigatória a promoção de ações contínuas para a capacitação dos colaboradores a respeita da cultura de segurança cibernética, aspecto fundamental para que os controles estabelecidos pelas sociedades sejam eficientes e conhecidos por todos.

Do ponto de vista de políticas, torna-se obrigatória a elaboração de uma política de segurança cibernética, que deve ser compatível com o porte da entidade supervisionada, a natureza e complexidade de suas operações e o seu grau de exposição ao risco cibernético, contemplando requisitos mínimos previstos na Circular. Em especial, a política de segurança cibernética deve estipular parâmetros para a classificação de dados e incidentes, bem como a implementação de controles de segurança de acordo com a respectiva classificação e diretrizes para a terceirização de serviços de processamento e armazenamento de dados.

A Circular também determina a necessidade de serem estabelecidos e atualizados processos e controles para a identificação e redução de vulnerabilidades, assim como para a detecção, resposta e recuperação de incidentes. Dentre os aspectos que precisam ser contemplados nos respectivos processos e controles estão o monitoramento contínuo da rede de comunicação, a adoção de medidas para a contenção e registro dos incidentes e o compartilhamento de informações sobre incidentes relevantes com as demais supervisionadas, em formado a ser acordado de forma mútua e que garanta o sigilo das informações confidenciais.

Outras obrigações que passam a ser exigidas das supervisionadas incluem a comunicação à SUSEP, no prazo máximo de 5 dias úteis a partir do conhecimento do evento, da ocorrência de incidentes relevantes, com

detalhes sobre os danos causados e ações de resposta promovidas, bem como a elaboração de relatório anual sobre prevenção e tratamento de incidentes, que deverá ser encaminhado aos órgãos de administração e, quando houver, aos comitês de auditoria e riscos e ao diretor responsável pelos controles internos.

As mudanças promovidas pela Circulam também atingem os contratos firmados pelas supervisionadas para a terceirização de serviços de processamento e armazenamento de dados. Quando se tratar de serviços relevantes, conceituados como aqueles que envolvam acesso ou manipulação de dados relevantes (dados pessoais, relativos a clientes ou a processos críticos de negócio, ou informações consideradas como sensíveis) ou suportem atividades consideradas como essenciais para a continuidade do negócio, a supervisionada deverá informar à SUSEP, em até 30 dias após a contratação, os serviços contratados, a denominação da empresa contratada e de eventuais subcontratadas, e, sempre que possível, os países ou regiões em cada país onde os serviços poderão ser prestados e os dados armazenados.

Também para a contratação de serviços relevantes será obrigação da supervisionada garantir que a contratada possua processos, procedimentos e controles de segurança cibernética não inferiores aos adotados pela supervisionada. Essa verificação pode ser feita por meio de exigência de certificação concedida por instituição independente ou por meio de realização de diligências prévias. Salvo nas hipóteses de contratos de adesão, os acordos contratuais firmados pelas supervisionadas com os prestadores de serviço devem conter menção expressa às exigências previstas na Circular.

Supervisionadas enquadradas nos segmentos S1 ou S2 possuem até o dia 30 de junho de 2022 para se adequarem às novas regras, enquanto as entidades enquadradas nos segmentos S3 e S4 têm até o dia 1º de setembro de 2022 para se adequar. Eventuais contratos que já estejam em vigor antes da vigência da Circular poderão ser ajustados até o dia 1º de setembro de 2024.

A nossa equipe de Proteção de Dados, Tecnologia e Negócios Digitais está à disposição para auxiliar na adequação aos termos da Circular nº 638/2021, seja na estruturação das respectivas políticas e processos, na condução de *due diligence* em fornecedores ou na revisão e negociação dos respectivos contratos.

Crédito da imagem: Shutterstock

› PROFISSIONAIS

Profissionais que aliam visão jurídica e visão de mercado

Felipe Palhares