A Superintendência de Seguros Privados (Susep) publicou, em 22 de maio de 2026, a Instrução Normativa (IN) nº 7/2026, que estabelece diretrizes e procedimentos internos para o tratamento de **incidentes de segurança com dados pessoais** no âmbito da Autarquia. A norma se insere no contexto de conformidade da Susep com a Lei Geral de Proteção de Dados Pessoais (LGPD) e dialoga com a Resolução CD/ANPD nº 15/2024. que regulamenta a comunicação de incidentes à Agência Nacional de Proteção de Dados (ANPD).

Essa medida é relevante porque a Susep, como controladora de dados pessoais de segurados, corretores, agentes de mercado e demais partes interessadas, deve manter uma estrutura de governança. Essa estrutura deve ser capaz de responder com agilidade a eventos que comprometam a confidencialidade, integridade ou disponibilidade dessas informações. Nesse contexto, a IN nº 7/2026 formaliza obrigações já existentes na legislação de proteção de dados.

O que a Instrução Normativa define como incidente de segurança

A IN adota a mesma lógica conceitual da LGPD ao definir **incidente de segurança envolvendo dados pessoais.** Esse é um evento adverso confirmado que resulta, ou pode resultar, em comprometimento da confidencialidade, integridade ou disponibilidade de dados pessoais. A norma também reitera definições importantes como dados pessoais sensíveis, encarregado de proteção de dados e agente de tratamento, alinhando o vocabulário interno à legislação federal.

É importante observar que a Instrução não se aplica às supervisionadas (seguradoras, resseguradores e demais entidades reguladas pela Susep). Ela se destina à própria autarquia, como órgão público que trata dados pessoais em suas atividades de supervisão e regulação.

A norma aplicável às supervisionadas é a Circular SUSEP nº 638/2021. Essa circular dispõe sobre requisitos de segurança cibernética a serem observados pelas sociedades seguradoras, entidades abertas de previdência complementar (EAPCs), sociedades de capitalização e resseguradores locais. O descumprimento dessas diretrizes pode sujeitar as entidades a sanções administrativas impostas pela Susep e, até mesmo, no âmbito da ANPD, se o descumprimento estiver relacionado a previsões da LGPD.

Competências e atribuições internas

A IN nº 7/2026 distribui competências entre três agentes internos. O encarregado pelo tratamento de dados pessoais atua como canal de comunicação com a ANPD e com os titulares afetados, além de apoiar a avaliação do impacto dos incidentes. A unidade responsável pela segurança da informação concentra as funções de monitoramento, identificação, análise e contenção técnica, por meio da Equipe de Tratamento e Resposta a Incidentes (ETIR). Por fim, as unidades gestoras dos sistemas e dados afetados colaboram na avaliação de impacto e na recuperação dos ambientes comprometidos.

Etapas do tratamento de incidentes

A norma prevê sete etapas obrigatórias no processo de tratamento: notificação do incidente, identificação e análise, classificação, contenção, erradicação, recuperação e comunicação à ANPD e aos titulares de dados, quando aplicável. Essa sequência reflete o ciclo consagrado de resposta a **incidentes de segurança da informação**, adaptado à proteção de dados pessoais.

O fluxo de tratamento será formalmente instituído pela Administração e disponibilizado na intranet institucional da Susep, em ferramenta de modelagem de processos. A Instrução Normativa prevê atualização semestral desse fluxo pela unidade de segurança da informação, dispensando alteração da norma para ajustes procedimentais. Dessa forma, a Susep confere flexibilidade operacional ao processo sem comprometer a base normativa.

Diálogo com o ecossistema regulatório de proteção de dados

A IN nº 7/2026 deve ser lida em conjunto com outras normas. A Resolução CD/ANPD nº 15/2024 estabelece que o controlador deve comunicar à ANPD a ocorrência de **incidente de segurança com dados pessoais** no prazo de três dias úteis, a contar do conhecimento de que o incidente afetou dados pessoais, quando o evento puder acarretar risco ou dano relevante aos titulares. Essa obrigação se aplica à Susep enquanto controladora de dados.

Por outro lado, a Circular Susep nº 638/2021 já exigia das seguradoras e demais entidades reguladas a comunicação de incidentes relevantes à autarquia no prazo de cinco dias úteis. A IN nº 7/2026, portanto, complementa esse cenário ao organizar a resposta da própria Susep quando seus sistemas e dados são afetados, mas os prazos não se confundem, na medida em que um é aplicável à própria Susep e o outro às supervisionadas.

Relevância para as supervisionadas pela Susep

Embora a Instrução Normativa seja de caráter interno, ela sinaliza ao mercado a importância que a Susep atribui à governança de dados pessoais. As supervisionadas pela Susep, em razão de uma série de outras regras, como o envio de informações periódicas (FIP) e do Sistema de Registro de Operações (SRO), por exemplo, compartilham dados com a autarquia ou dependem de sistemas integrados dentro das credenciadoras ou do Open Insurance. Portanto, devem estar atentas ao fato de que a Susep, ao estruturar seus próprios procedimentos de resposta, tende a exigir padrões equivalentes de suas supervisionadas. O sistema de peticionamento eletrônico (SEI) e as respostas na aba de documentos ao mercado também contêm dados pessoais.

Além disso, a formalização do papel do encarregado de dados e da equipe de resposta a incidentes dentro da Susep reforça a expectativa de que as entidades reguladas mantenham estruturas internas equivalentes, conforme já previsto na Circular nº 638/2021 e na Resolução Susep nº 45/2024, que trata da Política de Segurança da Informação da autarquia.

Próximos passos para as supervisionadas Susep

As empresas que integram o mercado supervisionado pela Susep devem revisar seus próprios planos de resposta a **incidentes de segurança**, especialmente para assegurar a compatibilidade com o fluxo de comunicação agora formalizado pela autarquia. É recomendável mapear os dados pessoais compartilhados com a Susep, avaliar os protocolos de comunicação com a equipe de resposta a incidentes da autarquia e manter atualizados os registros de incidentes e as evidências de conformidade, tendo em vista o dever de prestação de contas da própria Susep previsto na LGPD.

Isso tudo em um contexto no qual o regime sancionador da Susep passa por mudanças introduzidas pela Lei Complementar nº 213/2025, com o aumento substancial das multas que podem ser aplicadas pela Autarquia. As multas podem chegar até R$ 35 milhões, o dobro do valor do contrato; o dobro do prejuízo causado aos consumidores em decorrência do ilícito; ou o triplo do valor da vantagem econômica obtida ou da perda evitada em decorrência do ilícito.

Leia aqui na íntegra.

Fonte: TozziniFreire, em 29.05.2026