Direito,
Inovação
& Tecnologia

ANPD Regulamenta Comunicação de Incidentes de Segurança

Resolução CD/ANPD nº 15, de 24 de abril de 2024

www.vlklaw.com.br

26.04.2024

A Autoridade Nacional de Proteção de Dados (ANPD) divulgou hoje (26.04) a Resolução nº 15, que regulamenta a Comunicação de Incidentes de Segurança (CIS) e detalha os procedimentos e responsabilidades dos agentes de tratamento, destacando o uso de linguagem simples nos comunicados à Autoridade. Seguem os principais pontos de atenção:

1) QUEM DEVE COMUNICAR? O controlador, por meio de representante legal ou do Encarregado, nas situações de incidente de segurança da informação confirmado, em que houver risco ou dano relevante aos titulares. Essa comunicação à ANPD, quando feita pelo Encarregado, deverá demonstrar a existência de vínculo contratual, empregatício ou funcional. Se por meio de representante legal, mediante Procuração – a documentação comprobatória deve ser apresentada.

2) O QUE REPRESENTA RISCO OU DANO RELEVANTE? O incidente será assim considerado quando afetar significativamente direitos fundamentais (impedir o uso de um serviço; causar discriminação, violação à integridade física ou à imagem; ou fraude financeira) **E** contiver dados: Sensíveis; De crianças, adolescentes ou idosos; financeiros; de credenciais de acesso ou de confirmação da identidade; protegidos por sigilo legal, judicial ou profissional; **OU** Em larga escala (importante observar a Consulta Pública que está aberta neste momento sobre esse tema). É fundamental que as organizações tenham metodologia fundamentada para calcular o risco que o incidente pode representar, documentando o resultado.

3) QUAL O PRAZO DE COMUNICAÇÃO? 3 dias úteis, contados da data em que se confirmou que o incidente afetou dados pessoais. No caso de comunicação preliminar, as informações complementares deverão ser apresentadas em até 20 dias úteis.

4) O QUE DEVE CONTER O COMUNICADO? Descrição da natureza e categoria dos dados afetados; Número de titulares afetados (especificando os vulneráveis); Medidas técnicas de segurança utilizadas (antes, durante e após o incidente); Riscos do incidente; Data da ocorrência; Dados do Encarregado; Identificação do controlador e do operador; Descrição do incidente e causa principal, entre outros.

5) QUAIS DOCUMENTOS A ANPD PODE SOLICITAR? Além dos documentos comprobatórios acima, a ANPD poderá requisitar: Mapeamento das Atividade de Tratamento de Dados; Relatório de Impacto à Proteção de Dados Pessoais e o Relatório de Tratamento do Incidente.

6) PRECISA DE RELATÓRIO TÉCNICO? Além da documentação interna sobre a apuração da gravidade do incidente (cálculo de risco), a ANPD determina que a elaboração de Relatório Técnico, contendo todas as informações apresentadas no tópico 4 acima. O Relatório deve ser armazenado pelo período mínimo de 5 anos, mesmo que o incidente não seja comunicado à ANPD e aos titulares.

7) ANÁLISE AGREGADA: A ANPD poderá fazer a análise dos incidentes comunicados de forma agregada, ou seja, não específica, com providências padronizadas, conforme os planejamentos da Autoridade para a fiscalização.

8) DETERMINAÇÕES PELA ANPD: Após receber a CIS, a ANPD poderá determinar a ampla divulgação do incidente às expensas do controlador (que não se confunde com a sanção de publicização); e medidas para reverter ou mitigar os efeitos do incidente.

9) MANIFESTAÇÃO DO CONTROLADOR: A ANPD poderá determinar a adoção de medidas imediatas de prevenção, mesmo sem a manifestação do controlador.

10) SANÇÕES: A ANPD poderá instaurar processo administrativo sancionador, caso o controlador não adote as medidas determinadas pela Autoridade.

11) EXTINÇÃO DO PROCESSO DE CIS: O processo será declarado extinto pela ANPD quando: Não houver evidências suficientes da ocorrência do incidente; Se a Autoridade entender que não pode causar risco ou dano relevante; O incidente não envolver dados pessoais; Se tiverem sido tomadas as medidas de mitigação e reversão; OU Se os titulares tiverem sido comunicados e todas as providências necessárias tiverem sido realizadas.

12) OUTRAS OBRIGAÇÕES REGULATÓRIAS: As demais obrigações setoriais precisarão ser cumpridas cumulativamente a essa Resolução da ANPD (Anatel, Banco Central, CVM, SUSEP, entre outros), especialmente em relação à comunicação aos reguladores, conteúdo e prazos, obrigações de medidas de segurança, entre outros.

Autores:

Rony Vainzof
rony@vlklaw.com.br

Caio Lima
caio@vlklaw.com.br

Alexandra Krastins
alexandra.lopes@vlklaw.com.br