

Gestão de incidentes de violação de dados pessoais

LGPD
NA FCAV



Fundação Vanzolini



A FCAV trabalha continuamente para **proteger os ativos e as informações** próprios e de seus contratantes, inclusive os dados pessoais tratados. Por essa razão, seu Programa de Governança em Privacidade e Proteção de Dados possui uma norma que especifica processos para a gestão de incidentes de violação de dados pessoais.



Por que é importante

A gestão de incidentes de violação de dados pessoais tem como objetivo estabelecer diretrizes claras para **a identificação, o registro, a análise e a resposta a qualquer incidente** dessa natureza e, com a “Norma de gestão de incidentes de violação de dados pessoais”, a FCAV atende a exigências da Lei Geral de Proteção de Dados Pessoais (LGPD). Contudo, para que essa gestão seja efetiva, é essencial que todos os colaboradores envolvidos no tratamento de dados pessoais sigam as determinações dessa norma.

Como acontece

Para entender como é feita a gestão de incidentes de violação de dados pessoais, é necessário conhecer quatro conceitos:

- 1. Dado pessoal:** É qualquer informação que permita identificar uma pessoa física, por exemplo, nome, número de CPF e endereço de *e-mail*.
- 2. Dado pessoal sensível:** É qualquer dado de uma pessoa física sobre sua origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou organização religiosa, filosófica ou política, saúde ou vida sexual, além de dado genético ou biométrico.
- 3. Incidente de segurança com dados pessoais:** É qualquer evento que envolva a violação da segurança dos dados pessoais.
- 4. Violação de dados pessoais:** É qualquer comprometimento da segurança dos dados pessoais, por exemplo, acesso não autorizado, perda, destruição, alteração ou divulgação.

A gestão de incidentes de violação de dados pessoais é feita em etapas preestabelecidas, que se iniciam no monitoramento para identificação de violações. A identificação pode ser feita por meio de sistemas automatizados de monitoramento, alertas de segurança ou denúncia de qualquer colaborador – por isso é importante que todos permaneçam atentos e reportem imediatamente qualquer suspeita ou evidência de violação de dados.

Em casos que envolvem a atuação de terceiros que tratam dados pessoais em nome da FCAV, o incidente deve ser registrado oficialmente por meio de um formulário específico.

Quando uma violação é informada, a **Equipe de Resposta a Incidentes** e o **Encarregado** pelo Tratamento de Dados Pessoais **analisam o incidente** para confirmar se houve realmente uma violação de dados pessoais. Se os dados estiverem anonimizados (ou seja, se não for possível saber a qual pessoa física eles se referem), o incidente é tratado como problema de segurança da informação.



Se for confirmada a **violação de dados pessoais**, a Equipe de Resposta a Incidentes e a Área de Tecnologia da Informação (TI) atuam para **recuperar** os dados, **isolar a causa** da violação e coletar evidências para a **investigação** do caso, entre outras ações de mitigação dos danos.

É feita uma análise de riscos para **avaliar o impacto** que o incidente pode causar, considerando-se a quantidade de pessoas afetadas, a natureza do dado violado (dados pessoais sensíveis exigem atenção redobrada) e o tipo de dano futuro associado (por exemplo, perda de confidencialidade, fraude, roubo de identidade e prejuízo financeiro). Os riscos são classificados conforme sua gravidade, e isso determina as ações a serem realizadas na sequência.



Quando o incidente oferece **risco significativo** aos direitos dos titulares dos dados pessoais, o Encarregado pelo Tratamento de Dados Pessoais deve **notificar** a Autoridade Nacional de Proteção de Dados (**ANPD**), informando detalhes sobre o tipo de dado violado, o número de titulares afetados e as medidas corretivas tomadas. Se os dados pessoais tiverem sido comprometidos, o Encarregado deve **informar** também os seus **titulares** sobre a violação, explicando os riscos e oferecendo orientações sobre como mitigar possíveis consequências.

Para evitar que o problema se repita, são implementadas medidas corretivas, como **aprimoramentos em sistemas de segurança**, **reforço nas orientações** sobre proteção de dados, **revisão de processos de trabalho** e treinamentos para colaboradores. É elaborado um relatório, que documenta tudo o que foi feito desde a identificação até a solução do incidente.

O que isso tem a ver comigo

A proteção dos dados pessoais tratados na FCAV é uma responsabilidade coletiva.

Todos os colaboradores precisam ficar atentos e, ao perceber qualquer incidente ou suspeita de violação, reportá-lo imediatamente ao gestor de sua área. Também é possível enviar e-mail para suportelgpd@vanzolini.org.br ou fazer uma comunicação anônima por meio do Canal de Denúncia da FCAV.

Quando solicitado, o colaborador também pode **apoiar** no preenchimento do formulário específico para **registro de violação** de dados pessoais e na **investigação** de incidente.

O que acontece se não for respeitado

Se houver violação de dados pessoais, seus titulares ficarão expostos; se incidentes de violação de dados pessoais não forem tratados em conformidade com a legislação sobre o tema, a FCAV ficará sujeita a sanções.

Por isso é imprescindível que todos os colaboradores desempenhem suas atividades em consonância com as diretrizes, as orientações e as normas estabelecidas pela Fundação, a fim de mitigar riscos à segurança e à proteção de dados pessoais. Se o colaborador transgredir as regras da FCAV no contexto do Programa de Governança em Privacidade e Proteção de Dados, podem ser aplicadas medidas disciplinares previstas em políticas internas e contratos.



Este documento foi elaborado para fins informativos e não substitui a íntegra da “Norma de gestão de incidentes de violação de dados pessoais”, que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.