

# Anonimização e pseudonimização

**LGPD**  
NA FCAV



Fundação Vanzolini



A anonimização e a pseudonimização são duas técnicas distintas que permitem o **uso de dados sem que se identifiquem as pessoas** a quem eles se referem, ou seja, duas técnicas de desidentificação. A diferença entre elas reside no fato de que, em uma, a expectativa é que a reidentificação não possa ser obtida e, na outra, há previsão de recuperar o vínculo identificador. Ambas são importantes no cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) porque protegem a privacidade dos titulares de dados pessoais.



Reforçando o compromisso da FCAV com a **segurança da informação**, seu Programa de Governança em Privacidade e Proteção de Dados possui uma norma sobre anonimização e pseudonimização, de responsabilidade da Área de Tecnologia da Informação (TI), que estabelece as diretrizes sobre sua utilização, quando aplicável.

## Por que é importante

O objetivo da “Norma de anonimização e pseudonimização” é **proteger os dados** nos ambientes de desenvolvimento, integração, qualidade e produção da FCAV. Quando estão anonimizados ou pseudonimizados, há **maior garantia contra o uso indevido dos dados pessoais**, o que amplia a confiança e a transparência de seu tratamento.

Essas técnicas, quando aplicáveis, são indicadas para **evitar violações, reduzindo o impacto de incidentes de segurança**. Elas são, portanto, essenciais para **cumprir a LGPD e evitar riscos legais**, pois protegem os titulares dos dados pessoais, além de contribuírem para **resguardar a reputação** da FCAV.

## Como acontece

A anonimização transforma dados pessoais em dados que não podem mais ser associados a uma pessoa específica, de maneira presumidamente definitiva. Pode-se dizer que seja uma medida de proteção mais eficaz, e ela é usada, por exemplo, em relatórios estatísticos e pesquisas de mercado. Para fins de aplicação da LGPD, dados anonimizados não são considerados dados pessoais.

A pseudonimização, por sua vez, mascara dados pessoais, ou seja, os substitui por identificadores que, usados em conjunto com informações adicionais, podem ser novamente vinculados à pessoa a quem se referem, identificando-a. A reidentificação depende dessas informações adicionais, que são guardadas sob controle rigoroso, separadas dos dados pseudonimizados. Essa técnica é aplicada em sistemas de teste e processamento seguro de dados, entre outras situações.

Na FCAV, **métodos de anonimização e pseudonimização são adotados** de acordo com as necessidades específicas de cada caso, podendo fazer parte de estratégias de:

- privacy by design** (“privacidade desde a concepção”), para oferecer proteção adicional aos titulares dos dados pessoais;
- minimização de riscos no compartilhamento de dados** com operadores (quem executa o tratamento) ou outros controladores (quem decide como e por que tratar dados pessoais);
- redução da possibilidade de violações acidentais** quando colaboradores têm acesso a dados pessoais;
- minimização do volume de dados pessoais tratados**, para reduzir os riscos de violação.

A escolha pela aplicação de anonimização ou de pseudonimização considera **aspectos da governança de dados**, por exemplo:

- |                                                                                                              |                                                                                                                      |
|--------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------|
| <input checked="" type="checkbox"/> o <b>objetivo da desidentificação</b> dos dados pessoais;                | <input checked="" type="checkbox"/> a <b>finalidade</b> do uso dos dados pessoais;                                   |
| <input checked="" type="checkbox"/> a <b>natureza dos dados pessoais</b> a serem desidentificados;           | <input checked="" type="checkbox"/> os <b>riscos de reidentificação</b> ;                                            |
| <input checked="" type="checkbox"/> a <b>necessidade de reversibilidade</b> do processo de desidentificação; | <input checked="" type="checkbox"/> o <b>custo</b> e a <b>complexidade dos métodos</b> possíveis de serem aplicados. |
| <input checked="" type="checkbox"/> a <b>conformidade</b> com leis e demais regulamentos aplicáveis;         |                                                                                                                      |



Os **gestores das áreas** corporativas e de negócios podem solicitar apoio do **Encarregado** pelo Tratamento de Dados Pessoais (a pessoa indicada pela FCAV para fazer a interface entre ela e os titulares dos dados ou a Autoridade Nacional de Proteção de Dados – ANPD) para **identificar ou avaliar a necessidade de anonimização ou pseudonimização de dados tratados** em projetos ou serviços sob sua responsabilidade. Eles devem consultar antecipadamente o Encarregado quando for preciso divulgar ou compartilhar dados anonimizados ou pseudonimizados, para confirmar se isso pode ser feito.

A **Área de TI avalia e define os métodos** que podem ser utilizados para anonimização e pseudonimização de dados pessoais tratados pela FCAV.

Os gestores de área, o Encarregado pelo Tratamento de Dados Pessoais e a Área de TI são responsáveis por avaliar a possibilidade de reidentificação e os riscos de reversão dos processos de anonimização e pseudonimização sempre que aplicados, considerando não apenas o uso de meios próprios da FCAV, mas também a atuação de terceiros que, com meios e esforços razoáveis, possam reidentificar um conjunto de dados anonimizados ou pseudonimizados.

## O que isso tem a ver comigo

Todos os colaboradores são responsáveis por garantir a privacidade e a segurança dos dados pessoais tratados na FCAV. Para desempenhar seu papel na proteção dos dados, cada colaborador deve **apoiar seu gestor na identificação e na avaliação da necessidade de anonimização ou pseudonimização** em projetos ou serviços, bem como manter-se atento a possível tratamento de dados desnecessários em seus processos de trabalho e comunicar a situação ao gestor assim que identificá-la, de modo a **evitar a coleta e o uso excessivo de dados pessoais**. Todos devem respeitar as diretrizes estabelecidas para os processos e consultar o Encarregado pelo Tratamento de Dados Pessoais sobre a necessidade de anonimização ou pseudonimização, antes de compartilhar dados.



## O que acontece se não for respeitado

Se, em qualquer processo da FCAV, houver falha que possa levar a violação ou tratamento indevido de dados pessoais, a Fundação ficará sujeita a multas e sanções previstas na LGPD, e sua imagem poderá ser prejudicada pela perda de confiança por parte dos contratantes e dos titulares dos dados.

Por isso é imprescindível que a FCAV adote medidas de proteção de dados pessoais e que todos os colaboradores desempenhem suas atividades em consonância com as diretrizes, as orientações e as normas estabelecidas. Se o colaborador transgredir as regras 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 anonimização e pseudonimização”, que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.*