CARTILHA

# Gestão de *logs* e trilhas de auditoria

LGPD NA FCAV

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Fundação Vanzolini

A rastreabilidade das ações realizadas em ambientes lógicos é um atributo de extrema importância para garantir a segurança da informação, e sua viabilização depende da gestão de *logs* e trilhas de auditoria.

Com intuito de **assegurar a eficiência da rastreabilidade nos sistemas e ambientes lógicos** da FCAV, seu Programa de Governança em Privacidade e Proteção de Dados possui um procedimento, de responsabilidade da Área de Tecnologia da Informação (TI), com regras para que eles sejam adequadamente monitorados e possuam métodos de registro, coleta, preservação e exclusão de *logs* e trilhas de auditoria.

## Por que é importante

A gestão de *logs* e trilhas de auditoria bem realizada **garante o rastreamento e o registro** de qualquer evento relevante em um ambiente lógico. Dessa maneira, tal gestão é crucial para:

- **prevenção de problemas de segurança**, pois ajuda a identificar e tratar tentativas de acesso não autorizado e fraudes;
- **garantia de conformidade** com políticas internas e normas legais;
- **embasamento de investigações** detalhadas em caso de incidente;
- **proteção de dados sensíveis**, na medida em que garante tratamento seguro das informações.

## Como acontece

Para entender como é feita a gestão de *logs* e trilhas de auditoria, é necessário conhecer seis conceitos:

1. **Ambiente lógico:** É uma rede corporativa ou plataforma digital disponibilizada para uso interno e externo em uma organização.
2. **Auditoria:** É o exame sistemático das atividades realizadas a fim de averiguar sua conformidade com as regras e os procedimentos prévia e expressamente estabelecidos, aferindo-lhe a implementação e a eficácia.
3. **Incidente de segurança com dados pessoais:** É qualquer evento adverso, confirmado ou sob suspeita, relacionado à violação da segurança de dados pessoais, tais como acessos não autorizados, acidentais e ilícitos, que resulte em sua destruição, perda, alteração ou vazamento, ou, ainda, qualquer tratamento de dados inadequado ou ilícito que possa ocasionar risco para os direitos e as liberdades do titular dos dados pessoais.

4. **Incidente de segurança da informação:** É uma ocorrência identificada de estado de sistema, dados, informações, serviço ou rede que indica possível violação à Política de Segurança da Informação ou a normas complementares, falha de controles ou situação previamente desconhecida que possa ser relevante à segurança da informação.
5. ***Log*:** É o registro de evento relevante em um recurso de Tecnologia da Informação e Comunicação (TIC) ou em ambiente lógico da FCAV.
6. **Trilha de auditoria:** É uma técnica que permite o acompanhamento de atividades que afetam determinado conjunto de informações, desde o momento em que se origina até o instante em que é finalizado, mediante identificação de autor, data e horário de cada atividade e dos sistemas acessados.

Todos os **eventos** relevantes nos sistemas da FCAV (por exemplo, acessos, alterações e falhas) são **registrados em *logs***. A Área de TI analisa periodicamente esses registros, utilizando **ferramentas automatizadas para identificar anomalias**. Trilhas de auditoria detalham todas as ações, especificando quem as realizou, quando elas ocorreram e o que foi alterado, entre outras informações, o que permite **acompanhamento completo**.


Os ***logs*** são mantidos de maneira que fiquem **protegidos** contra acessos não autorizados e são **preservados** por período predeterminado com base nas necessidades das demais áreas da FCAV e em critérios jurídicos.

## O que isso tem a ver comigo

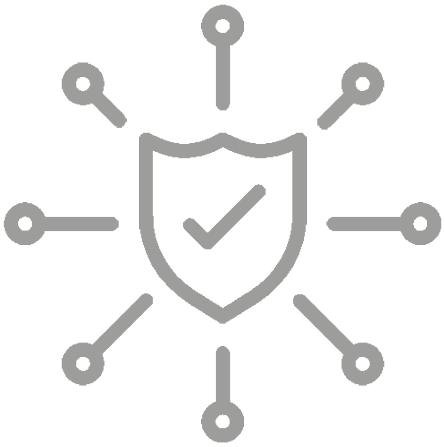
Todos os colaboradores que respeitam os processos e as permissões de acesso definidos pela FCAV favorecem a existência de um ambiente mais seguro para todos.

Cada um é responsável pelas próprias ações nos sistemas e ambientes digitais da Fundação. Sabendo que toda atividade realizada pode contribuir para manter a segurança da informação ou para colocá-la em risco, todos os colaboradores devem se manter atualizados quanto às regras internas e segui-las rigorosamente.

## O que acontece se não for respeitado

Se, em qualquer sistema ou ambiente lógico da FCAV, houver evento que possa levar à violação de regras de segurança, isso poderá resultar em danos à imagem da Fundação e perda de confiança por parte dos envolvidos.

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 da informação. Se o colaborador transgredir as regras da FCAV no contexto do Programa de Governança em Privacidade e Proteção de Dados ou tentar burlar os controles estabelecidos, podem ser aplicadas medidas disciplinares previstas em políticas internas e contratos.



*Este documento foi elaborado para fins informativos e não substitui a íntegra do documento normativo "Procedimento de gestão de* logs *e trilhas de auditoria", que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.*