CARTILHA

Gestão de incidentes de segurança da informação

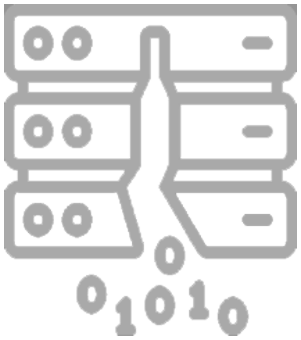
LGPD NA FCAV

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Fundação Vanzolini

De forma geral, a **segurança da informação é a garantia da confiabilidade** da informação, ou seja, de que a confidencialidade, a integridade e a disponibilidade da informação serão todas preservadas. Tendo em vista que ela é fundamental para a proteção dos dados e ativos da FCAV, a Fundação adota medidas físicas (destinadas a proteger fisicamente seus dados e ativos), técnicas (implementadas na infraestrutura e nos sistemas de Tecnologia da Informação [TI]) e organizacionais (relacionadas a políticas, processos e pessoas) para **prevenir e tratar incidentes de segurança** da informação.

A prevenção é feita mediante **fiscalização de processos de trabalho e sistemas** quanto à conformidade com a legislação vigente, os princípios éticos e as regras e restrições estabelecidas pelos documentos normativos internos. Entre as medidas adotadas estão: monitoramento de vulnerabilidades por meio de **ferramentas de supervisão de atividades**; registro, monitoramento e análise de **trilhas de auditoria**; e **controles de acesso**. O tratamento, por sua vez, é o conjunto das providências necessárias para resolver as causas e as consequências de um incidente de segurança da informação identificado.



Fazer gestão de incidentes de segurança da informação envolve **identificação, classificação e resposta ao incidente**, bem como melhoria contínua para prevenir ocorrências semelhantes no futuro. O Programa de Governança em Privacidade e Proteção de Dados da FCAV possui uma norma que prevê todos os processos dessa gestão, para que as **ações de manutenção e retorno à normalidade** sejam eficientes e para que as medidas voltadas à não reincidência sejam implementadas.

Por que é importante

A gestão de incidentes de segurança da informação visa **garantir que todos os incidentes sejam tratados** de forma rápida e eficaz, bem como **proteger as informações e os sistemas** da FCAV contra ameaças, interrupções e danos.

A **conscientização** e a **participação** de todos os colaboradores são cruciais, na medida em que promovem uma **cultura de segurança** voltada à continuidade dos negócios e à proteção de dados e sistemas da Fundação.

Seguir as diretrizes da "Norma de gestão de incidentes de segurança da informação" é essencial para que a FCAV esteja preparada para **enfrentar ameaças e minimizar riscos**.

Como acontece

Para entender como é feita a gestão de incidentes de segurança da informação, é necessário conhecer cinco conceitos:

1. **Segurança da informação:** Refere-se à proteção das informações quanto a **confidencialidade** (apenas pessoas autorizadas podem acessar as informações), **integridade** (todas as informações estão corretas e completas) e **disponibilidade** (as informações podem ser acessadas sempre que necessário). O propósito é proteger os ativos contra ameaças, de modo que as operações sejam mantidas, os danos sejam minimizados e a conformidade com as leis e regulamentações seja assegurada.
2. **Incidente de segurança da informação:** É qualquer evento ou série de eventos que comprometa a confidencialidade, a integridade ou a disponibilidade de informações ou sistemas. Pode ser um acesso não autorizado, uma falha de segurança, uma violação de dado pessoal, um uso inadequado de recurso tecnológico, entre outros.
3. **Ativo:** É qualquer item de valor para a Fundação, que precisa ser protegido. Os principais exemplos são dados, sistemas de TI, infraestrutura, redes e colaboradores. Preservar os ativos da FCAV é fundamental para proteger suas informações e seu funcionamento contínuo.
4. **Ameaça:** É qualquer circunstância ou evento que possa causar impacto negativo nos ativos. Pode ser, por exemplo, um ataque cibernético, uma falha humana, um desastre natural ou uma falha de sistema.
5. **Risco:** É a combinação da probabilidade de um evento indesejado ocorrer e o impacto que ele pode causar. O risco deve ser continuamente monitorado para que sejam implementadas medidas preventivas.

A gestão de incidentes de segurança da informação é realizada por meio de um processo organizado voltado a identificação, comunicação e tratamento de incidentes. A identificação pode ser feita por meio de sistemas automatizados de monitoramento, alertas de segurança controlados pela equipe de TI ou denúncia de qualquer colaborador – por isso é importante que todos estejam atentos a atividades suspeitas ou em desacordo com a Política de Segurança da Informação.

Quando uma ocorrência é identificada, a Equipe de Resposta a Incidentes verifica se ela é de fato um incidente de segurança. Se houver essa confirmação, o **incidente é classificado** com base no **nível do impacto** que ele pode causar nas operações da FCAV (crítico, alto, médio ou baixo), o que determina o prazo máximo para sua resolução.

Para conter o incidente e evitar que ele se espalhe ou cause mais danos, a Equipe de Resposta a Incidentes deve **analisar** seus dados e **propor ações imediatas** para contê-lo e para restaurar os ambientes afetados, ainda que provisoriamente, até a implantação da solução definitiva. São acionadas todas as equipes necessárias, especialmente a de TI, e todas as partes interessadas são comunicadas do incidente e das ações que devem ser tomadas. A prioridade é **recuperar os sistemas afetados o mais rápido possível**, com foco na continuidade das operações da FCAV. Caso o incidente identificado envolva violação de dados pessoais, a atuação requer a participação ativa do Encarregado pelo Tratamento de Dados Pessoais, e a "Norma de gestão de incidentes de violação de dados pessoais" deve ser seguida.

A Equipe de Resposta a Incidentes documenta desde a identificação até a resolução do incidente. Isso inclui descrever como ele foi identificado e as ações de mitigação de seus impactos, assim como registrar as evidências coletadas ao longo do processo. Essa documentação é essencial para análises futuras e implementação de melhorias nas medidas de segurança.

Depois da resolução do incidente, é feita uma análise detalhada, para identificar suas causas e propor melhorias que impeçam sua reincidência. O objetivo final é aprimorar os procedimentos de resposta a incidentes e **fortalecer os controles de segurança**. Além disso, a Equipe de Resposta a Incidentes deve elaborar um plano de ação que defina prazos e responsáveis para a implementação de **medidas preventivas e corretivas**, e os gestores devem avaliar a necessidade de atualizar a planilha de riscos e oportunidades, de acordo com o "Procedimento de levantamento de riscos e oportunidades da FCAV".

O que isso tem a ver comigo

A segurança da informação é uma responsabilidade coletiva, e a gestão de incidentes só é eficaz com a colaboração ativa de todos.

Todos os colaboradores, sem exceção, têm papel fundamental na proteção dos ativos da FCAV. Isso envolve **estar atento** a possíveis incidentes, **reportar qualquer comportamento suspeito**, manter-se informado sobre as boas práticas de segurança da informação e **seguir rigorosamente as políticas de segurança**.

Para reportar, de forma segura e anônima, um incidente ou uma suspeita de incidente, os colaboradores podem usar o Canal de Denúncia da FCAV. Também é possível comunicar o fato enviando e-*mail* para **suportelgpd@vanzolini.org.br**. Cada caso é registrado formalmente para que sejam tomadas as providências cabíveis.

O que acontece se não for respeitado

Se houver falha de segurança da informação, os dados e os ativos da FCAV ficarão expostos e a continuidade de seus negócios poderá ser prejudicada.

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 de dados e ativos. 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 da "Norma de gestão de incidentes de segurança da informação", que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.