CARTILHA

Controles criptográficos

LGPD NA FCAV

LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS

Fundação Vanzolini

Criptografia é um **método automatizado** que utiliza algoritmos e chaves criptográficas para codificar e decifrar informações, restringindo os dados para pessoas não autorizadas, ou seja, um método que **transforma informações legíveis em códigos abstratos** que só poderão ser decifrados por quem tiver a chave correta. Por exemplo, a mensagem "Segurança é essencial", ao ser criptografada, pode se transformar em "K&@13P#L", e apenas quem tiver a chave correta poderá traduzir a sequência nova de volta à mensagem original.

O uso de ferramentas de criptografia **protege dados e informações**, assegurando que permaneçam **confidenciais, íntegros e acessíveis apenas a pessoas autorizadas**. Reforçando o compromisso da FCAV com a segurança da informação, seu Programa de Governança em Privacidade e Proteção de Dados possui uma norma sobre controles criptográficos, de responsabilidade da Área de Tecnologia da Informação (TI), que estabelece critérios para a implantação e a utilização de tais ferramentas, de maneira que seu emprego seja efetivo e adequado.

Por que é importante

Dados pessoais, contratos, estratégias de negócio e outros tipos de informação são ativos valiosos para a FCAV, e a "Norma de controles criptográficos" auxilia em sua proteção, impedindo que informações confidenciais caiam em mãos erradas. Dessa forma, a norma **evita ocorrências com vazamento de dado** que possam causar prejuízos financeiros e reputacionais.

Além disso, ela **cumpre exigências legais e regulatórias** de proteção de dados, como a Lei Geral de Proteção de Dados Pessoais (LGPD), garantindo conformidade às atividades da Fundação.

Como acontece

A FCAV utiliza ferramentas de criptografia provenientes de **fornecedores reconhecidos e homologados** pela Área de TI.

Todos os seus sistemas são **monitorados continuamente** para garantir que essas ferramentas estejam sempre atualizadas e em perfeito funcionamento. Em todos os procedimentos de TI – desde o acesso remoto

via VPN (*Virtual Private Network*) até a transmissão de documentos com informações sigilosas ou confidenciais – são aplicados **métodos de criptografia robustos**, como SSL/TLS (*Secure Sockets Layer/Transport Layer Security*) e **chaves assimétricas** (*public key infrastructure*).

A gestão das chaves criptográficas inclui processos rigorosos e detalhados, para que elas sejam geradas, trafegadas, armazenadas, distribuídas e destruídas de maneira segura.

Caso seja detectado qualquer **recebimento ou envio de conteúdo criptografado em desconformidade**, isso é tratado como incidente de segurança da informação: a Área de TI solicita formalmente ao gestor responsável os esclarecimentos necessários e reporta o fato à **Equipe de Resposta a Incidentes**.

O que isso tem a ver comigo

Cada colaborador é parte essencial da segurança da informação e deve **conhecer e seguir as regras estabelecidas**, para proteger a FCAV e os dados de todos os envolvidos.

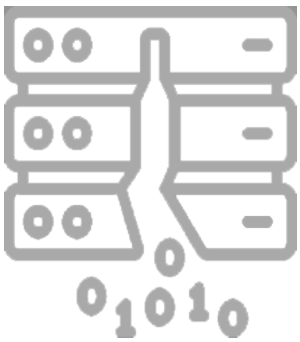
Sempre que for necessário enviar informações confidenciais, a equipe de suporte da Área de TI deve ser consultada sobre a melhor ferramenta a ser usada, o que deve ser feito pelo *e-mail* suporteti@vanzolini.org.br.

Para evitar riscos, **apenas ferramentas de criptografia aprovadas** pela Área de TI podem ser empregadas, e ninguém pode instalar nem utilizar ferramentas não autorizadas.

O que acontece se não for respeitado

O uso indevido de criptografia pode colocar em risco informações da FCAV e seus contratantes. Se, de alguma maneira, dados pessoais ou outros ativos forem expostos a acessos não autorizados, a Fundação ficará sujeita a multas e poderá haver danos à sua imagem.

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. O descumprimento das diretrizes pode resultar em investigação interna e aplicação das sanções legais cabíveis.



Este documento foi elaborado para fins informativos e não substitui a íntegra da "Norma de controles criptográficos", que estabelece diretrizes específicas para gestores e colaboradores diretamente envolvidos.