INSTITUTO FEDERAL
Catarinense

Recomendação de Uso de API

Diretoria
de Tecnologia
da Informação

1. Introdução

A recomendação de uso de APIs visa estabelecer diretrizes claras e medidas de segurança robustas para garantir a proteção adequada dos dados e informações transmitidas e processadas por meio de APIs.

Esta recomendação se aplica a todas as APIs desenvolvidas e mantidas pelo Instituto Federal Catarinense e foi construída com base no Guia de Requisitos Mínimos de Privacidade e Segurança da Informação para APIs do Governo Federal.

2. Dos termos e definições

- **API**: Contrato de serviço entre duas aplicações distintas e/ou bibliotecas de terceiros integradas ao código
- **API Interna:** São as APIs desenvolvidas e disponibilizadas nos sistemas internos hospedados e/ou mantidos pelo Instituto Federal Catarinense, as APIs externas serão relacionadas em catálogo interno, disponibilizado para o time técnico de Tecnologia da Informação do Instituto Federal Catarinense. São destinadas para uso exclusivo para solução de problemas ou desenvolvimento de sistemas que atendam o IFC no âmbito Institucional.
- **API Externa:** São as APIs desenvolvidas e disponibilizadas por parceiros terceiros do IFC, cabendo aos mesmos a manutenção, hospedagem e disponibilização em ambiente seguro
- **HTTPS**: Protocolo seguro de comunicação entre APIs por meio de rede de dados
- **Parceiro Externo**: empresa, pessoa ou parceiro não vinculado ao quadro de servidores efetivos do Instituto Federal Catarinense

3. Objetivo

O objetivo desta recomendação é:

- Garantir a confidencialidade, integridade e disponibilidade dos dados e informações transmitidas e processadas por meio de APIs desenvolvidas e mantidas pelo Instituto Federal Catarinense.
- Estabelecer padrões de segurança consistentes para o desenvolvimento, implementação e uso de APIs no âmbito do Instituto Federal Catarinense.
- Proteger as informações institucionais, disponibilizadas via API, contra ameaças cibernéticas, violações de segurança e uso indevido dos dados.

4. Princípios

Esta recomendação é baseada nos seguintes princípios:

- **Transparência:** As ações de segurança e privacidade relacionadas às APIs devem ser transparentes a todos os envolvidos;
- **Responsabilidade:** Todos os indivíduos envolvidos no desenvolvimento, implementação e uso de APIs têm responsabilidade pela proteção dos dados, implementando, de forma proativa, soluções para mitigar riscos de segurança;
- **Compliance:** As APIs devem cumprir as regulamentações de privacidade, principalmente aquelas contidas na Lei Geral de Proteção dos Dados(LGPD).

5. Requisitos de Segurança

As APIs devem atender aos seguintes requisitos mínimos de segurança:

- Criptografia dos dados
    - Utilizar protocolos de criptografia dos dados, como o HTTPS, por exemplo, durante o processo de transferência das informações.
- Autenticação e autorização adequadas para garantir que apenas usuários autorizados tenham acesso aos dados.
    - Utilização de chaves e tokens de acesso para garantir a confiabilidade no acesso das informações
- Princípio do menor privilégio.
    - Os usuários devem possuir somente as permissões necessárias para realização das suas tarefas.
- Implementação de mecanismos de proteção contra ameaças.
    - Prevenção de ações como injeção de SQL, ataques de cross-site scripting (XSS) e ataques de força bruta.
- Registro e monitoramento de atividades para detectar e responder a eventos de segurança.
    - Mecanismo de logs de acesso e de requisições feitas à API.

6. Responsabilidades

- Equipe de Desenvolvimento:
    - Responsável por implementar medidas de segurança durante o desenvolvimento das APIs.

        - Criar e disponibilizar a documentação da API desenvolvida.
    - Equipe de Infraestrutura:
        - Responsável por garantir a operação segura das APIs, incluindo monitoramento e resposta a incidentes de segurança.
    - Usuários das APIs:
        - Devem cumprir as políticas de segurança estabelecidas e relatar quaisquer preocupações e/ou eventos de segurança à equipe responsável.
        - APIs internas podem ser disponibilizadas a parceiros externos desde que os mesmos estejam aderentes às conformidades legais da Lei Geral de Proteção de Dados, Marco Civil da Internet e por meio de assinatura de termos de cooperação e responsabilidade.
        - Zelar pelo uso consciente dos recursos computacionais das APIs internas.

7. Conformidade e Auditoria

Serão realizadas auditorias regulares para garantir a conformidade com esta recomendação e os requisitos de segurança estabelecidos.

- Os sistemas que utilizarem as APIs internas deverão estar em conformidade com a Lei Geral de Proteção de Dados, Marco Civil da Internet e alinhados aos objetivos estratégicos definidos no Plano de Desenvolvimento Institucional e Plano de Diretor de Tecnologia da Informação.

- As solicitações de uso de APIs devem passar por avaliação de comitê interno composto pelo Diretor de Tecnologia da Informação, Coordenador de Sistemas de Informação, Coordenador de Infraestrutura e Tecnologia de Informação, Encarregado de Dados e Gestor de Segurança da Informação.

8. Revisão da Recomendação

Esta recomendação será revisada periodicamente para garantir sua eficácia contínua e sua conformidade com as melhores práticas de segurança da informação e regulamentações aplicáveis.

9. Disposições Finais

Esta recomendação entra em vigor imediatamente após a sua aprovação e será de cumprimento obrigatório para todas as partes envolvidas no desenvolvimento, implementação e uso de APIs.