Guia de Requisitos e Melhores Práticas para Fornecedores

Este guia apresenta informações essenciais sobre APIs, segurança no desenvolvimento de sistemas e melhores práticas que fornecedores interessados em colaborar com a Dock devem observar para garantir uma parceria sólida e segura.

O que são APIs?
API (Interface de Programação de Aplicações) é um conjunto de regras que permite que sistemas diferentes se comuniquem e compartilhem dados. APIs são fundamentais para a integração entre plataformas, facilitando a automação de processos e a troca de informações com segurança.

Principais Características de uma API

- Escalabilidade e Flexibilidade

APIs devem ser projetadas para se adaptarem às necessidades do negócio, suportando diferentes volumes de tráfego e complexidades de serviço.

- Tipos de Dados e Interações

• APIs podem lidar com dados sensíveis, como informações pessoais ou transações financeiras, o que exige altos padrões de segurança.
• Suas funções incluem leitura de dados (saldo, histórico) e operações sensíveis (transferências, alterações de perfil).

- Segurança Incorporada

• A comunicação via API deve ser protegida por autenticação robusta e criptografia de dados para evitar acessos não autorizados.
• O uso de tokens, como JWT (JSON Web Tokens), é uma prática comum para proteger sessões e autenticar usuários.

Benefícios das APIs para Fornecedores

• Integração eficiente com os sistemas da Dock.
• Redução de custos e aumento da automação em processos operacionais.
• Melhoria da experiência do usuário por meio de serviços conectados e seguros.

Desenvolvimento Seguro
Princípios de Desenvolvimento Seguro
O desenvolvimento seguro visa proteger sistemas e aplicações contra vulnerabilidades durante todo o ciclo de vida, desde a concepção até a operação. Isso inclui práticas que minimizem riscos e garantam a conformidade com padrões de segurança.

- Políticas de Segurança

• Gerenciamento de Senhas:
• Exija senhas complexas com no mínimo 8 caracteres, incluindo letras maiúsculas, minúsculas, números e símbolos.
• Bloqueie senhas comuns ou previsíveis usando listas de exclusão.
• Reset Seguro:
• Redefinições de senha devem exigir autenticação multifatorial (MFA).

- Controle de Acesso
  - Utilize autenticação baseada em tokens seguros, como OAuth 2.0 com PKCE.
  - Implemente controle de permissões baseado em funções (RBAC) para limitar o acesso de usuários a apenas o necessário.

- Validação e Sanitização
  - Valide todas as entradas de dados para evitar ataques como injeções de código (SQL Injection, XSS).
  - Aplique listas de permissão (whitelisting) para definir valores aceitáveis de entrada.

- Testes de Segurança
  - Realize auditorias frequentes, incluindo testes de penetração e análise de vulnerabilidades.
  - Simule ataques em ambiente controlado para avaliar a robustez do sistema.

- Gestão de Logs e Erros
  - Registre atividades de sistemas e APIs de forma segura, sem expor informações sensíveis.
  - Evite mensagens de erro detalhadas que possam revelar informações internas.

Requisitos de Segurança para Fornecedores

- Criptografia de Dados
  - Proteja todos os dados em trânsito com TLS 1.2 ou superior.
  - Armazene dados sensíveis de forma criptografada.

- Proteção contra Ataques
  - Configure limites de taxa (rate limiting) para evitar abusos.
  - Utilize Web Application Firewalls (WAFs) para bloquear ataques direcionados.

- Resiliência Operacional
  - Mantenha backups atualizados e planos de recuperação de desastres.
  - Garanta que sistemas essenciais tenham alta disponibilidade e redundância.

Melhores Práticas e Recomendações

- Auditorias Regulares: Fornecedores devem realizar revisões periódicas de segurança.
- Monitoramento Contínuo: Implemente soluções de monitoramento para identificar e responder a anomalias.
- Atualizações e Patches: Mantenha bibliotecas, frameworks e sistemas atualizados para corrigir vulnerabilidades.

- Treinamento de Equipe: Certifique-se de que os desenvolvedores estejam capacitados em práticas de segurança.