Segurança

Para garantir a segurança das aplicações desenvolvidas na plataforma, nossa esteira de desenvolvimento segue as melhores práticas de segurança.

Entendemos que acompanhar as melhores práticas de mercado possibilita a melhoria contínua do nosso produto e atende a exigência do mercado que busca soluções confiáveis e eficientes, por isso investimos sempre em melhoria continua.

Alguns exemplos de medidas implantadas:

- Controles de acesso.
- Criptografia.
- Proteção contra injeção de código.
- Isolamento de ambientes entre clientes.
- Entre outros.

Conteúdo complementar

- Permissão de Segurança
- Log de Auditoria
- Multi aplicações
- Autenticação via Active Directory
- Autenticação via SSO (Single Sign-On)
- Autenticação mútua (certificado digital)
- Autenticação via SAML
- Invalidação de tokens

Controles de acesso

O sistema de autenticação e controle de acesso do Cronapp são baseados em tokens e possui recursos de autenticação utilizando os *endpoints* "`<domínio>/auth`", que permite informar o login e senha de um usuário para obter o seu token de acesso, e "`<domínio>/auth/refresh`", que permite atualizar o token após finalizar o seu tempo de expiração.

Essas funcionalidades podem ser utilizadas em aplicações web e mobile sempre que for necessário utilizar requisições REST para acessar determinados recursos de forma externa. Para mais informações de uso, acesse o tópico "Recursos privados" da documentação Disponibilizando Web Service REST ou o tópico "Acesso aos recursos privados" da documentação Swagger - OpenAPI.