# Documentação da API

## Autenticação

Todos os endpoints (exceto /login) requerem autenticação via token JWT.

**Header necessário:**

Authorization: Bearer <token>

**Endpoints**

### 1. Login

* **Endpoint:** (POST) /api/auth/login
* **Descrição:** Realiza autenticação do usuário e retorna um token JWT.
* **Request Body:**

{

"username": "admin",

"password": "senha123"

}

* **Resposta:**

{

"token": "<jwt\_token>"

"username": "<user>",

"role": "<role>"

}

* **Autenticação:** Não requerida

### 2. Buscar usuários

* **Endpoint:** (GET) /api/users
* **Descrição:** Lista todos os usuários cadastrados.
* **Resposta:**

{

"data": [ {

"id": 123,

"username": "user",

"password": "123456",

"email": "user@dominio.com",

"role": "user"

}]

}

* **Autenticação:** Requer token
* **Autorizacão:** Apenas admin

### 3. Buscar contratos

* **Endpoint:** (GET) /api/contracts
* **Descrição:** Lista contratos registrados, com filtros opcionais por empresa e data.
* **Query Params (opcionais):**
  + empresa: Nome da empresa
  + data: Data de início (formato YYYY-MM-DD)
* **Resposta:**

{

"data": [ {

"id": 1,

"empresa": "Empresa A",

"data\_inicio": "2024-01-01",

"data\_final": "2024-02-01"

} ]

}

* **Autenticação:** Requer token
* **Autorizacão:** Apenas admin

## Melhorias de Segurança Implementadas

* Uso de JWT com exp (expiração)
* Middleware de autenticação com jsonwebtoken
* Verificação de permissão por role
* Armazenamento seguro de JWT\_SECRET via variáveis de ambiente