# Documentación del Endpoint de Inicio de Sesión (Login)

## 1. URL del Endpoint

POST /auth/login

## 2. Descripción

Este endpoint permite a los usuarios autenticarse enviando su número de contrato y contraseña. Si las credenciales son válidas, se retorna un token JWT y los datos básicos del usuario.

## 3. Cuerpo de la Solicitud (Body)

Formato: JSON

{  
 "contrato": "Contrato-001",  
 "password": "123456"  
}

## 4. Respuesta Exitosa (200 OK)

{  
 "message": "Login exitoso",  
 "access\_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9...",  
 "user": {  
 "id": 1,  
 "nombre": "Juan",  
 "apellido": "Pérez",  
 "email": "juan@example.com",  
 "rol": "Admin"  
 }  
}

## 5. Posibles Errores

- 401 Unauthorized: Credenciales incorrectas

- 400 Bad Request: Faltan campos requeridos

## 6. Cómo Probar en Postman

Paso 1: Crear una nueva petición en Postman

- Método: POST

- URL: http://localhost:3000/auth/login (ajusta según tu entorno)

Paso 2: Ir a la pestaña "Body" y seleccionar "raw" → "JSON"

Pega este contenido:

{  
 "contrato": "Contrato-001",  
 "password": "123456"  
}

Paso 3: Haz clic en "Send".

Si todo está correcto, deberías ver una respuesta 200 con un token y los datos del usuario.

Paso 4: Para usar el JWT en otros endpoints protegidos, ve a la pestaña "Authorization" de Postman:

- Tipo: Bearer Token

- Token: Pega aquí el valor de "access\_token" recibido.