

Especificaciones técnicas Jira-clone: BACKEND

1. Introducción

- **Propósito:** Este documento describe los aspectos técnicos para desarrollar el sistema de tickets y kanban, incluyendo la arquitectura, tecnologías y flujos de trabajo.
 - **Alcance:** El sistema permitirá agregar, eliminar, actualizar y leer las tareas y los proyectos creados, así como darles seguimiento en su tablero.
-

2. Requisitos Técnicos

2.1 Requisitos Funcionales

- CRUD de usuarios (con roles y permisos). Siendo solo accesible para el rol Máster.
- CRUD proyectos. Siendo accesible para los roles: Máster y Leader.
- CRUD de las tareas. Siendo accesible para todos los roles.

2.2 Requisitos No Funcionales

- ...
 - ...
 - ...
-

3. Arquitectura del Sistema

- **Tipo:** Arquitectura monolítica.
 - **Componentes principales:**
 - **Backend:** Spring Boot (Java).
 - **Base de datos:** MySQL.
 - **Autenticación:** Implementación de OAuth2 con JWT.
-

4. Detalles Técnicos

4.1 Estructura del Backend (cada API)

- **Controladores:**
 - `ComponentController`: Maneja solicitudes relacionadas con componentes.
 - `AuthController`: Maneja la autenticación.
- **Servicios:**
 - `ComponentService`: Lógica de negocio relacionada con componentes.
 - `AuthService`: Lógica de autenticación y generación de tokens.
- **Repositorios:**
 - `ComponentRepository`: Acceso a la base de datos para los componentes.

4.2 Endpoints de la API

Método	Endpoint	Descripción
POST	<code>/api/components/create</code>	Registrar un nuevo componente.
GET	<code>/api/components/{n_id}</code>	Obtener información de un componente por un <code>n_id</code> .
PUT	<code>/api/components/{n_id}</code>	Actualizar datos del componente.
DELETE	<code>/api/components/{n_id}</code>	Eliminar componente.

Un componente puede ser: un Developer, un Project o una Task.

5. Tecnologías

- **Backend:** Java con Spring Boot.
 - **Base de datos:** MySQL.
 - **Autenticación:** OAuth2 y JWT.
 - **Infraestructura:** Docker para contenedores.
 - **Deploy:** AWS.
-

7. Seguridad

- **Autenticación:** Implementación de OAuth2 con tokens JWT.
 - **Cifrado:** Las contraseñas se cifran con BCrypt.
-

8. Consideraciones Finales

- Este diseño está sujeto a revisión por el equipo técnico.
- Las herramientas para pruebas y monitoreo incluirán Postman, JUnit y SpringTest.