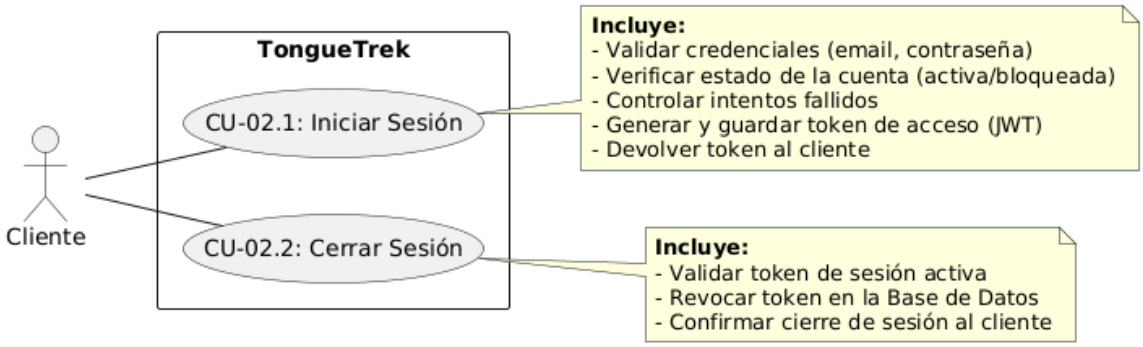
Caso de Uso - Autenticación y Sesión del Cliente Tonguetrek

Campo	Descripción
Código del Requisito	RF-02
Nombre del Requisito	Autenticación y Sesión de Cliente
Características	• Formulario de inicio de sesión que solicita correo y contraseña. • Verificación segura de la contraseña contra el hash almacenado. • Control de intentos fallidos y bloqueo automático de la cuenta. • Generación de Tokens de Acceso (JWT) para gestionar la sesión. • Invalidación de tokens al cerrar sesión.
Descripción Detallada	El sistema permitirá a un cliente registrado autenticarse proporcionando su correo y contraseña. El sistema verificará las credenciales de forma segura. Si son correctas, generará un token de acceso (JWT), lo registrará en la base de datos y se lo devolverá al cliente para autorizar peticiones futuras. El sistema controlará los intentos fallidos, bloqueando la cuenta si se excede el límite. Finalmente, permitirá al usuario cerrar su sesión, revocando el token de acceso para que no pueda ser reutilizado.
Prioridad	Crítica
Tipo	Funcional / Seguridad
Código del Caso de Uso	CU-02
Nombre del Caso de Uso	Autenticación y Gestión de Sesión de Cliente
Descripción	Describe cómo un cliente ya registrado inicia sesión para obtener acceso a la plataforma, cómo el sistema lo protege de

	intentos maliciosos, y cómo puede cerrar su sesión de forma segura.
Actores	Primario: Cliente Secundarios: Sistema, Base de datos
Precondiciones	• El cliente debe estar previamente registrado en el sistema. • El estado de la cuenta del cliente debe ser 'activo'.
Secuencia Normal	Flujo de Login: 1. El cliente accede a la página de inicio de sesión. 2. El sistema muestra el formulario (correo y contraseña). 3. El cliente ingresa sus credenciales y pulsa "Iniciar Sesión". 4. El sistema valida que las credenciales son correctas y la cuenta está activa. 5. El sistema reinicia el contador de intentos fallidos del cliente a 0. 6. El sistema genera un Token JWT de acceso y lo guarda en la tabla tokens. 7. El sistema devuelve el token al cliente. Flujo de Logout: 1. El cliente autenticado solicita cerrar su sesión. 2. El sistema recibe la petición con el token de acceso. 3. El sistema busca el token en la base de datos y actualiza su estado a 'revocado'. 4. El sistema envía un mensaje de confirmación de cierre de sesión.
Postcondición	• Login: El cliente está autenticado y posee un token activo para realizar peticiones a rutas protegidas. • Logout: El token de sesión del cliente queda invalidado y ya no puede ser utilizado.

Excepciones	E1 - Credenciales incorrectas: El sistema muestra "Credenciales incorrectas" e incrementa el contador de intentos fallidos. E2 - Cuenta ya bloqueada: El sistema muestra "Cuenta bloqueada. Contacte a soporte" y no permite el acceso. E3 - Límite de intentos alcanzado: Tras el 3er intento fallido, el sistema bloquea la cuenta y muestra el mensaje correspondiente. E4 - Token inválido/revocado: Si se intenta acceder a una ruta protegida (como logout) con un token inválido, el sistema devuelve un error de autorización.

Diagrama de Casos de Uso - Autenticación y Sesión (CU-02)



Autor: Mauricio Villegas

Historia de Usuario – Autenticación y Gestión de Sesión

ID: HU-02

Título: Inicio de Sesión y Gestión de Sesión de Cliente

Como cliente registrado, **Quiero** iniciar sesión en TongueTrek con mis credenciales y poder cerrar mi sesión de forma segura, **Para** poder acceder a mi perfil, proteger la privacidad de mi cuenta y asegurar que nadie más pueda usar mi sesión activa.

Criterios de Aceptación

1. El sistema debe proveer una interfaz (endpoint) para que el cliente pueda enviar su correo y contraseña.
2. El sistema debe validar las credenciales comparando la contraseña enviada con el hash seguro almacenado en la base de datos.
3. Al iniciar sesión exitosamente, el sistema debe generar un Token de Acceso (JWT) y devolverlo al cliente.
4. El sistema debe registrar cada intento de inicio de sesión fallido, incrementando un contador en la base de datos.
5. El sistema debe bloquear permanentemente la cuenta de un usuario (estado = 'bloqueado') después de 3 intentos fallidos consecutivos.
6. El sistema debe rechazar cualquier intento de inicio de sesión de una cuenta que ya se encuentre bloqueada.
7. Un cliente autenticado debe poder solicitar el cierre de su sesión activa.
8. Al cerrar sesión, el sistema debe invalidar el token de acceso correspondiente en la base de datos (estado = 'revocado'), impidiendo su uso futuro.
9. El sistema debe rechazar el acceso a rutas protegidas si se utiliza un token que ha sido revocado.

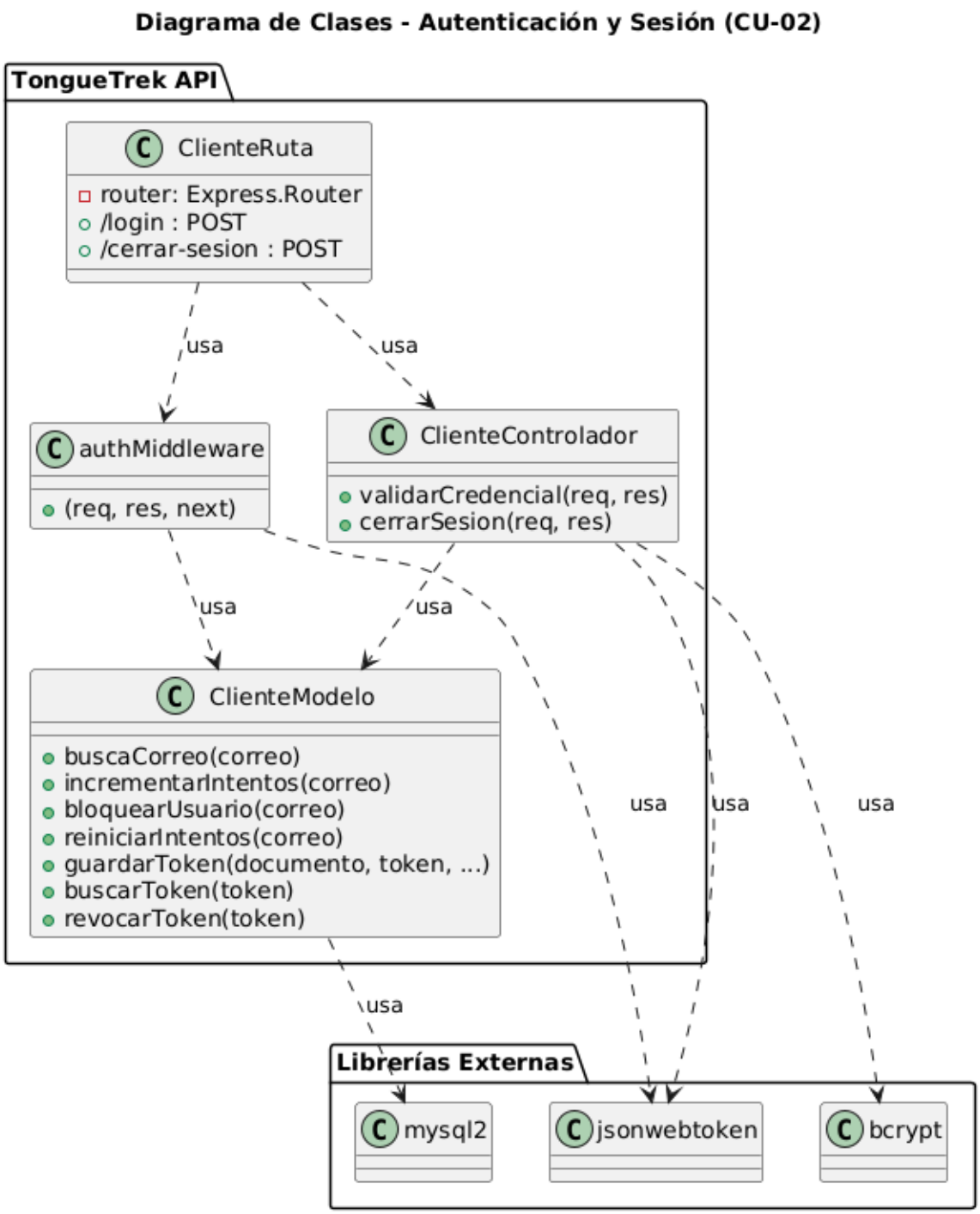


Diagrama Entidad-Relación (ER) para RF-02

Para este requisito funcional, las dos entidades (tablas) más importantes de nuestra base de datos que interactúan son **clientes** y **tokens**.

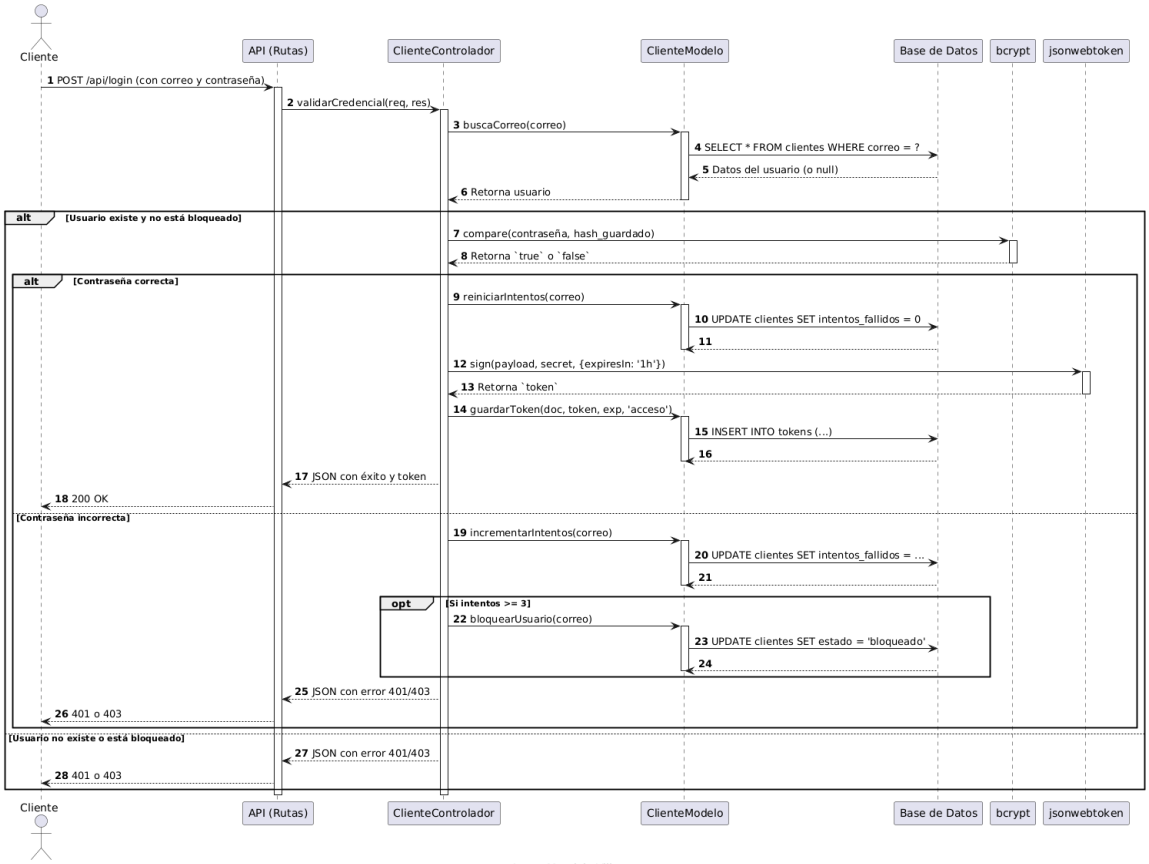
Entidades y Atributos Clave:

1. **CLIENTES:**
    - **Propósito:** Entidad principal que almacena la identidad y el estado de seguridad del usuario.
    - **Atributos relevantes para este caso de uso:**
        - id (Clave Primaria)
        - correo (para la búsqueda en el login)
        - contrasena (para la validación)
        - estado (para verificar si la cuenta está 'activa' o 'bloqueada')
        - intentos_fallidos (el contador para el bloqueo)
2. **TOKENS:**
    - **Propósito:** Entidad que registra cada sesión de usuario, permitiendo un control detallado.
    - **Atributos relevantes para este caso de uso:**
        - id (Clave Primaria)
        - documento (para enlazar con el cliente)
        - token (el JWT generado)
        - estado (para saber si el token está 'activo' o 'revocado')
        - tipo (para diferenciar si es de 'acceso' o 'reseteo')

Relación:

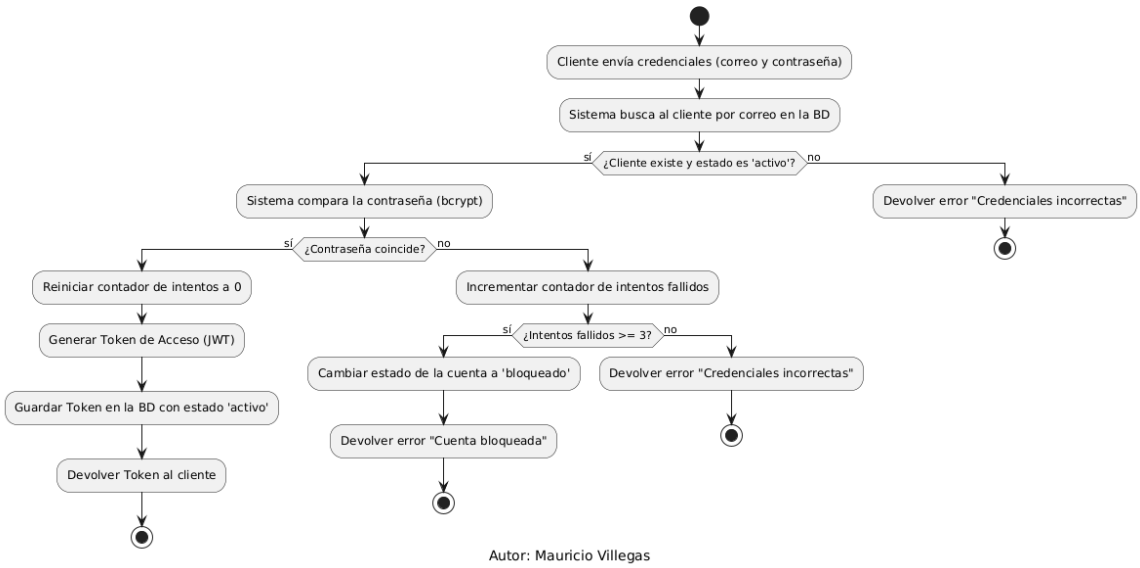
- Existe una relación de **Uno a Muchos (1:N)** entre CLIENTES y TOKENS.
- **Explicación:** Un (1) cliente puede tener muchos (N) tokens a lo largo del tiempo (por ejemplo, si inicia sesión desde su celular y desde su computador, tendrá dos tokens activos). Sin embargo, cada (1) token en la tabla tokens pertenece a un único y solo un cliente.

Diagrama de Secuencia - Inicio de Sesión (CU-02)



Autor: Mauricio Villegas

Diagrama de Actividad - Autenticación de Cliente (CU-02)



Autor: Mauricio Villegas

Diagrama de Estado - Cuenta de Cliente

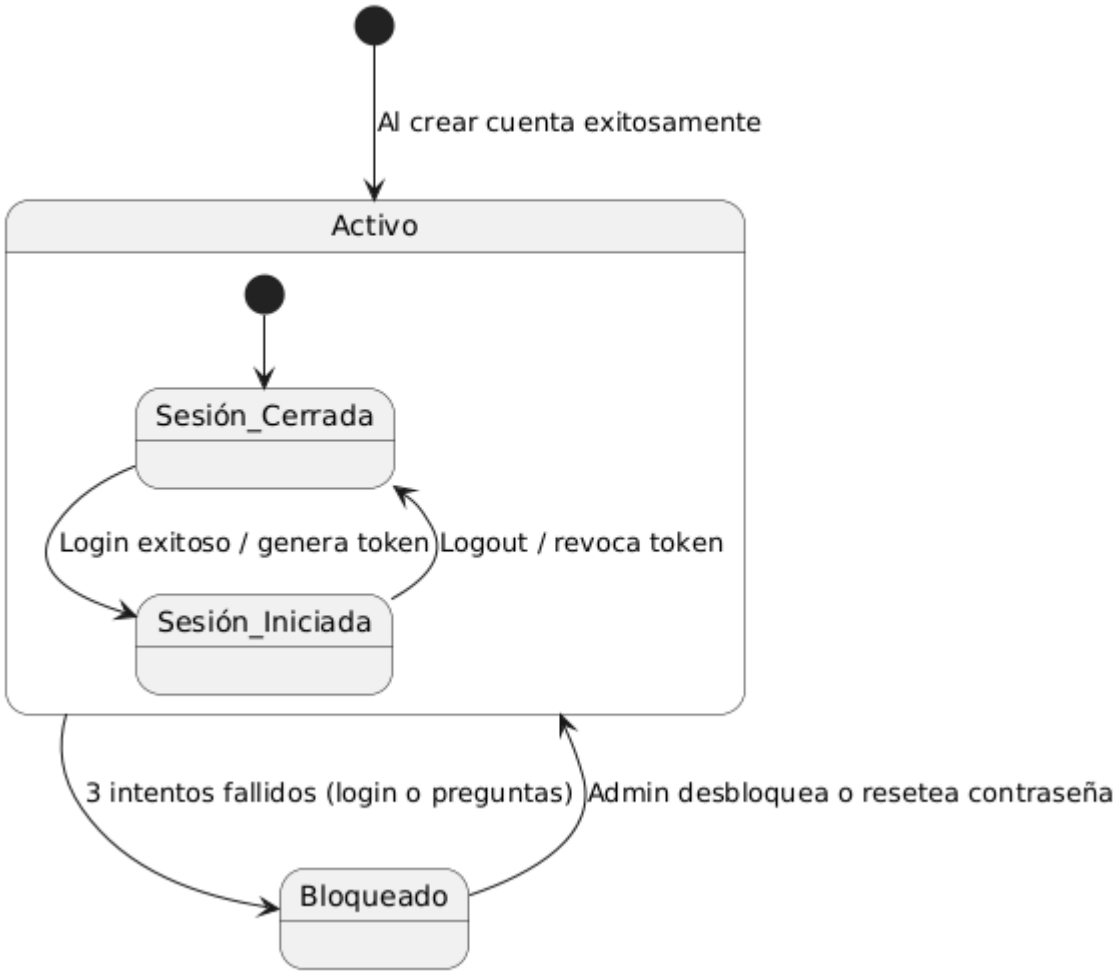
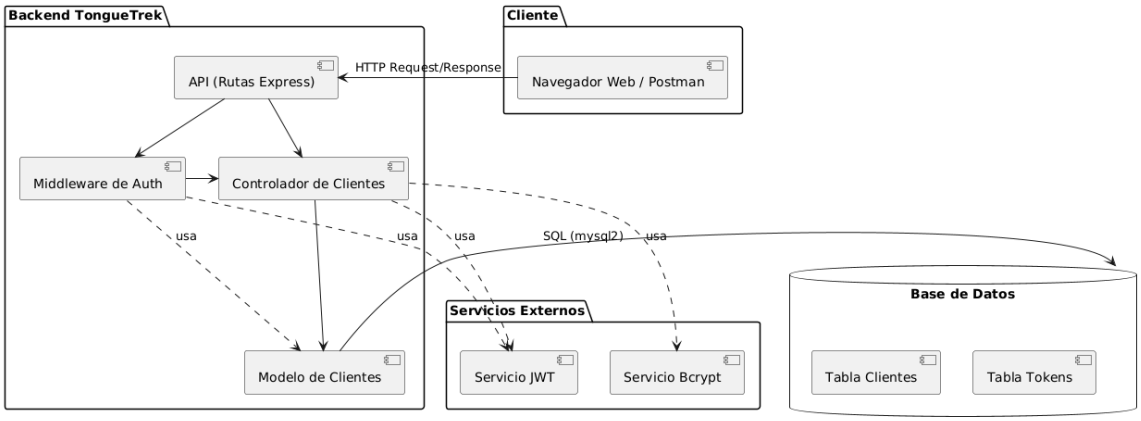
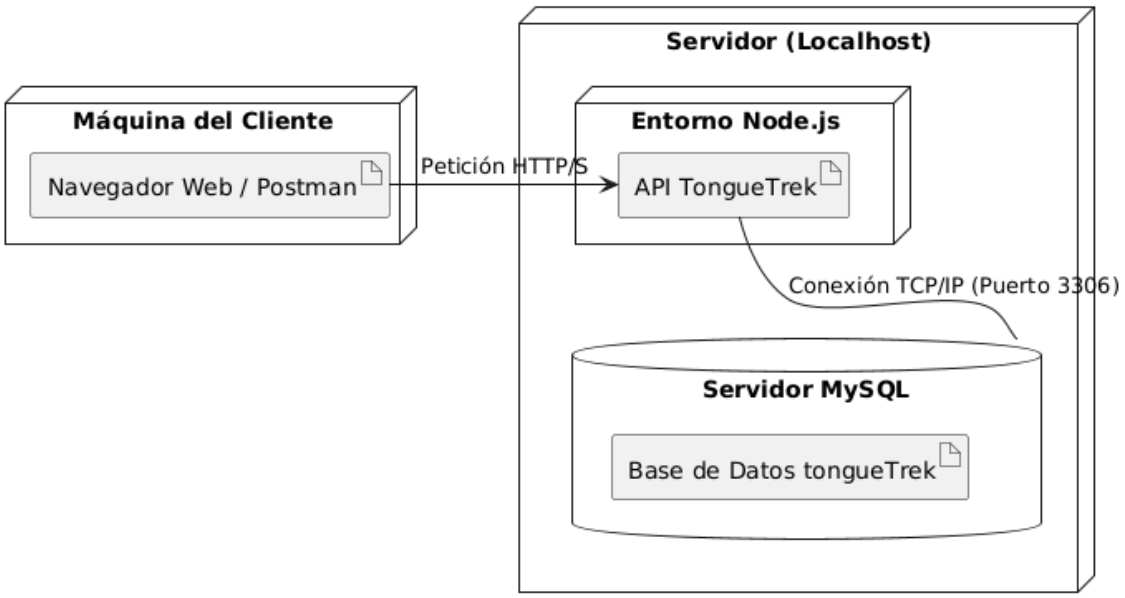


Diagrama de Componentes - Autenticación y Sesión (CU-02)



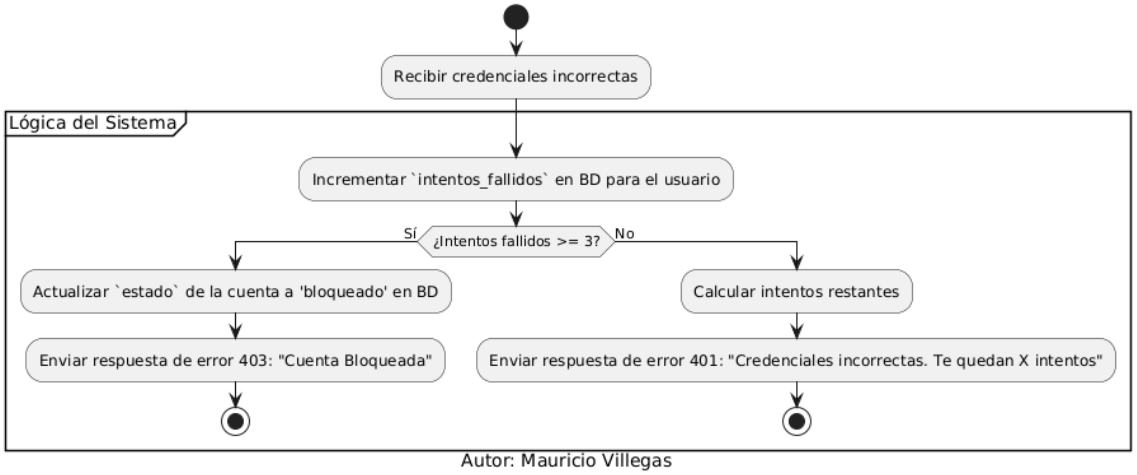
Autor: Mauricio Villegas

Diagrama de Despliegue - Autenticación y Sesión (CU-02)



Autor: Mauricio Villegas

Diagrama de Flujo - Manejo de Login Fallido (CU-02)



Autor: Mauricio Villegas