Documentación del Requisito Funcional: Eliminación de Cuenta Tonguetrek

Código del Requisito	RF-04
Nombre del Requisito	Recuperación de Cuenta de Cliente
Características	- Flujo multi-paso para verificar la identidad del usuario sin estar logueado. - Validación de identidad basada en la combinación de una respuesta a una pregunta de seguridad y la fecha de expedición del documento. - Control de intentos fallidos específico para el proceso de recuperación. - Bloqueo de cuenta automático si se excede el límite de intentos. - Generación de un Token de Reseteo (JWT) de un solo propósito y corta duración (5 minutos). - Notificaciones de seguridad por correo en etapas clave del proceso.
Descripción Detallada	El sistema proveerá un mecanismo seguro para que los clientes que han olvidado su contraseña puedan recuperar el acceso. El proceso requiere que el usuario primero solicite sus preguntas de seguridad, luego responda correctamente a una de ellas y proporcione su fecha de expedición de documento. El sistema protege este flujo contra ataques de fuerza bruta limitando los intentos. Una validación exitosa genera un token temporal que autoriza de forma segura el restablecimiento final de la contraseña, notificando al usuario en cada paso.
Prioridad	Crítica
Tipo	Funcional / Seguridad

Información del Caso de Uso (CU-05)

Código del Caso de Uso	CU-04
Nombre del Caso de Uso	Recuperación de Cuenta de Cliente
Descripción	Describe el proceso completo que sigue un cliente para restablecer su contraseña olvidada, validando su identidad a través de un sistema seguro de preguntas/respuestas y datos personales.
Actores	Primario: Cliente Secundarios: Sistema, Base de Datos, Servicio de Correo
Precondiciones	- El cliente debe estar previamente registrado en el sistema. - El cliente debe haber completado su perfil de seguridad (establecido sus preguntas y respuestas). - El cliente no recuerda su contraseña y no está logueado.
Secuencia Normal	1. El cliente, desde la pantalla de login, accede a la opción "Recuperar Contraseña". 2. Ingresa su número de documento. 3. El sistema busca al usuario y le presenta en pantalla sus tres preguntas de seguridad. 4. El cliente elige una pregunta, escribe la respuesta correcta y también ingresa su fecha de expedición de documento. 5. El cliente pulsa "Validar". 6. El sistema recibe el paquete de datos (documento, respuesta, fecha de expedición). 7. El sistema verifica que la fecha de expedición sea correcta y que la respuesta coincida con la respuesta encriptada correspondiente a esa pregunta en la base de datos. 8. Al ser la validación exitosa, el sistema

	reinicia el contador de intentos de preguntas, envía un correo de notificación y genera un Token de Reseteo de 5 minutos. 9. El sistema devuelve este resetToken al cliente. 10. El cliente envía el resetToken junto con su nueva contraseña. 11. El sistema valida el resetToken, encripta la nueva contraseña y la actualiza en la tabla clientes, asegurando que la cuenta quede en estado 'activo'. 12. El sistema envía un correo final confirmando el cambio de contraseña.
Postcondición	El cliente ha restablecido su contraseña, su cuenta está activa y puede iniciar sesión con sus nuevas credenciales.
Excepciones	E1 - Usuario no encontrado: Si el documento no corresponde a ningún cliente. E2 - Perfil no configurado: Si el cliente no ha guardado sus preguntas de seguridad. E3 - Validación incorrecta: Si la respuesta o la fecha de expedición son incorrectas, el sistema muestra un error e incrementa el contador de intentos_preguntas_fallidos. E4 - Límite de intentos alcanzado: Tras 3 fallos en la validación, la cuenta se bloquea (estado = 'bloqueado_preguntas') y se notifica al usuario. E5 - Token de Reseteo inválido o expirado: Si el cliente intenta usar un token incorrecto o después de los 5 minutos, el sistema rechazará la petición de cambio de contraseña.

Historia de Usuario (HU-04)

- **ID:** HU-04

- **Título:** Recuperación de cuenta por contraseña olvidada
- **Como** cliente registrado que ha olvidado su contraseña,
- **Quiero** un método seguro para verificar mi identidad usando mis preguntas secretas y poder establecer una nueva contraseña,
- **Para** recuperar el acceso a mi cuenta sin comprometer su seguridad.

Criterios de Aceptación

1. El sistema debe permitir a un usuario solicitar sus preguntas de seguridad proporcionando su número de documento.
2. El sistema debe devolver únicamente las preguntas, nunca las respuestas almacenadas.
3. El sistema debe permitir al usuario enviar sus respuestas junto con su fecha de expedición de documento para validación.
4. La validación debe ser exitosa solo si todas las respuestas y la fecha de expedición son correctas.
5. El sistema debe comparar las respuestas enviadas por el usuario con los hashes bcrypt almacenados en la base de datos.
6. El sistema debe contar los intentos de validación fallidos y bloquear la cuenta (estado = 'bloqueado_preguntas') después de 3 intentos.
7. Tras una validación exitosa, el sistema debe generar un Token de Reseteo (JWT) de corta duración (5 minutos) y de un solo propósito (purpose: 'password-reset').
8. El sistema debe enviar una notificación por correo al usuario cuando la validación de respuestas sea exitosa.
9. El sistema debe permitir al usuario establecer una nueva contraseña únicamente si presenta un Token de Reseteo válido y no expirado.
10. Al restablecer la contraseña, el sistema debe guardar la nueva versión encriptada en la base de datos y enviar un correo final de confirmación.

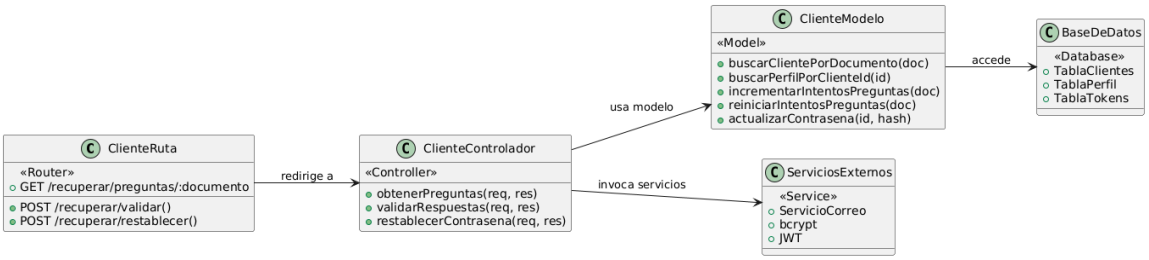

Diagrama Entidad-Relación (ER) para RF-02 (Autenticación)

Propósito: Este diagrama modela la estructura de las tablas de la base de datos que son relevantes para el flujo de autenticación y cómo se relacionan entre sí.

Tu descripción textual es **perfecta** y muy clara. Aquí te la incluyo, seguida del código PlantUML que la representa visualmente.

Descripción Textual (La tuya, que está excelente):

Para este requisito funcional, las dos entidades (tablas) más importantes 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:** id (Clave Primaria), correo, contrasena, estado, intentos_fallidos.
    2. **TOKENS:**
        - **Propósito:** Entidad que registra cada sesión de usuario, permitiendo un control detallado.
        - **Atributos relevantes:** id (Clave Primaria), documento (para enlazar con el cliente), token, estado, tipo.
- **Relación:**
    - Existe una relación de **Uno a Muchos (1:N)** entre CLIENTES y TOKENS.
    - **Explicación:** Un (1) cliente puede tener muchos (N) tokens, pero cada (1) token pertenece a un único cliente.

Diagrama de Actividad - Recuperación de Cuenta (CU-04)

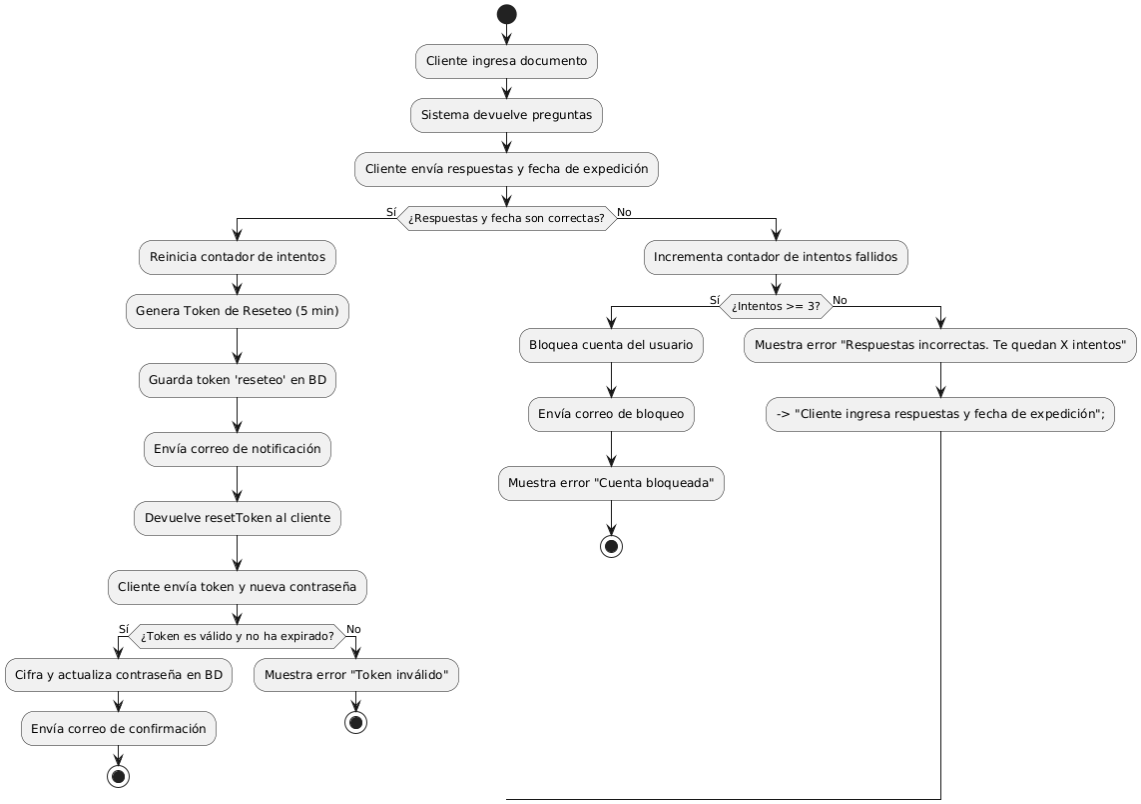

Diagrama de Secuencia - Recuperación de Cuenta (CU-04)

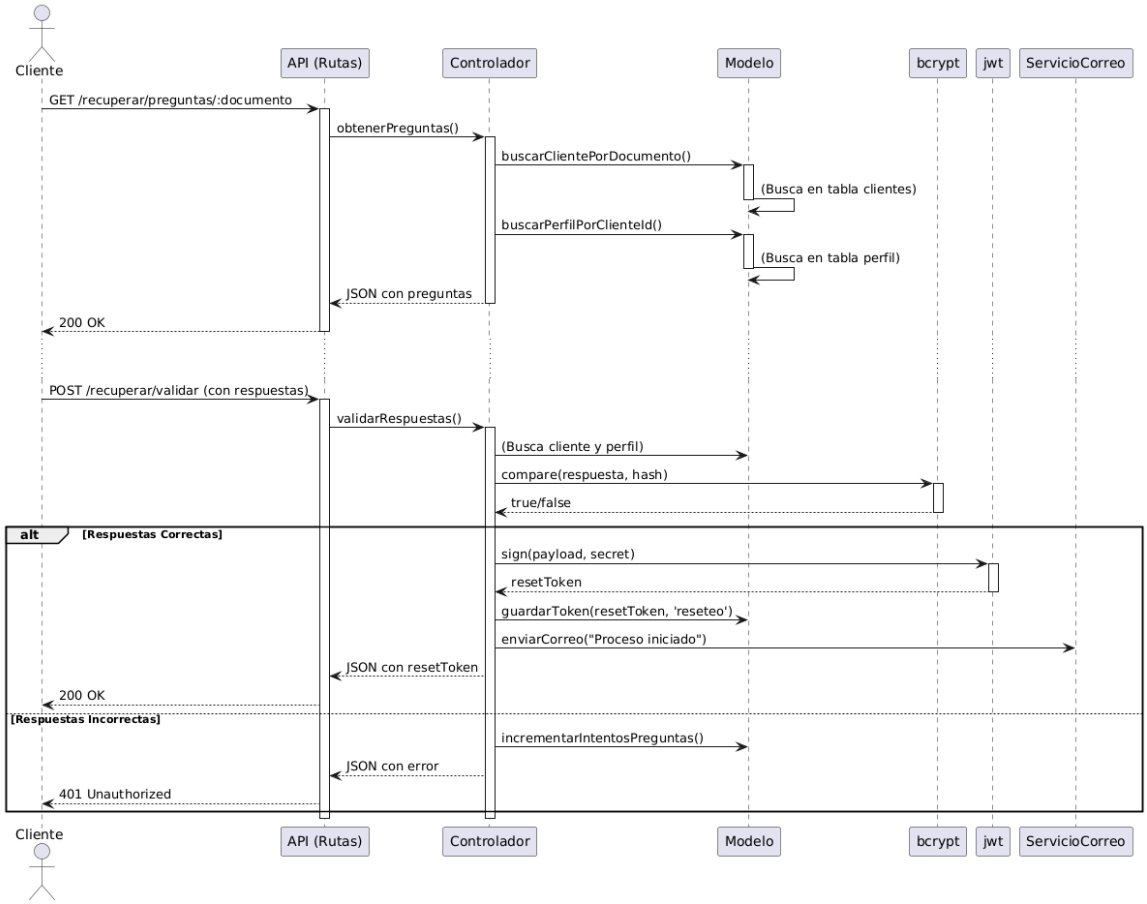

Diagrama de Estado - Proceso de Recuperación de Cuenta

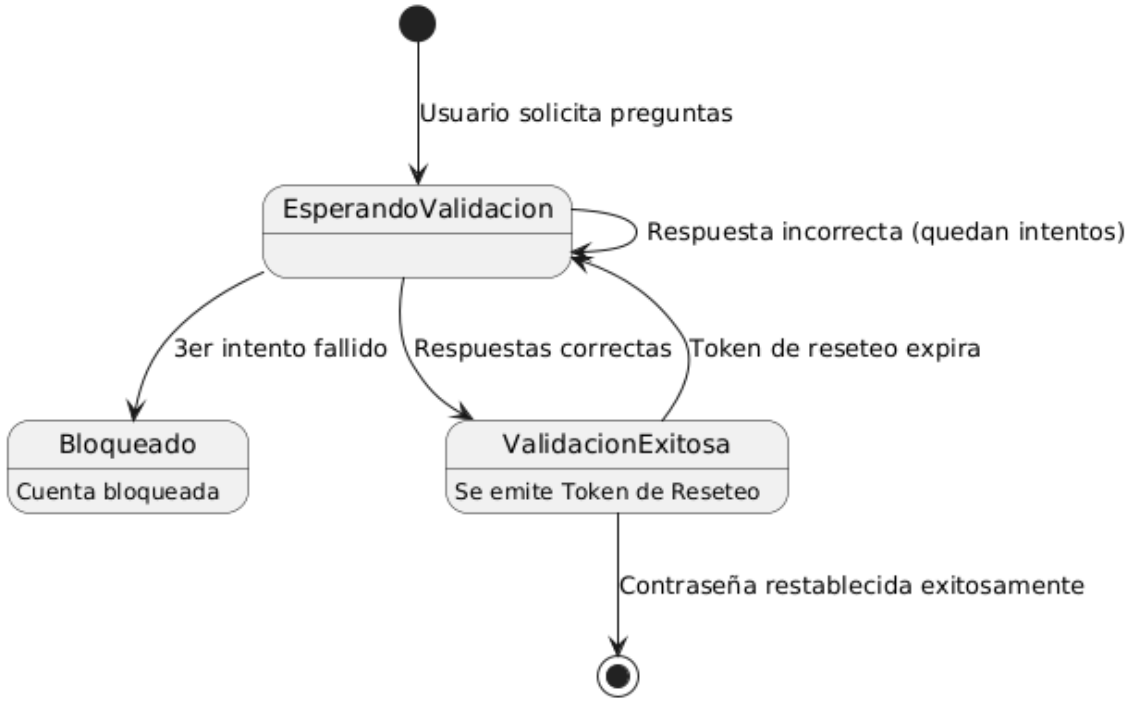

Diagrama de Componentes - Arquitectura General

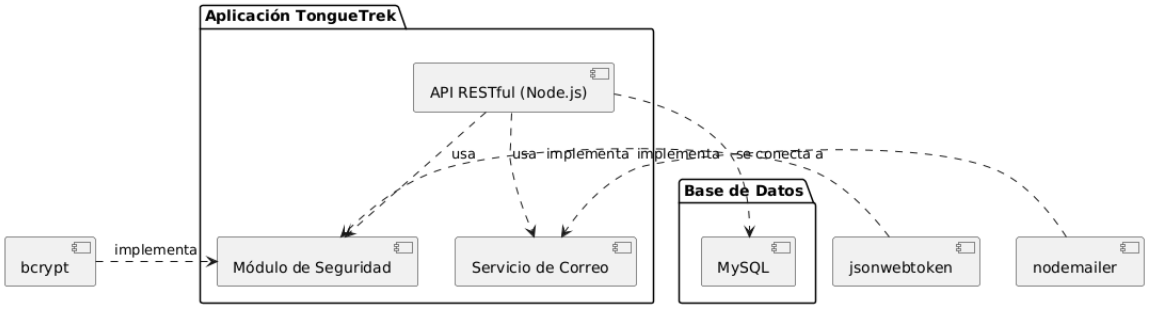

Diagrama de Despliegue - TongueTrek API

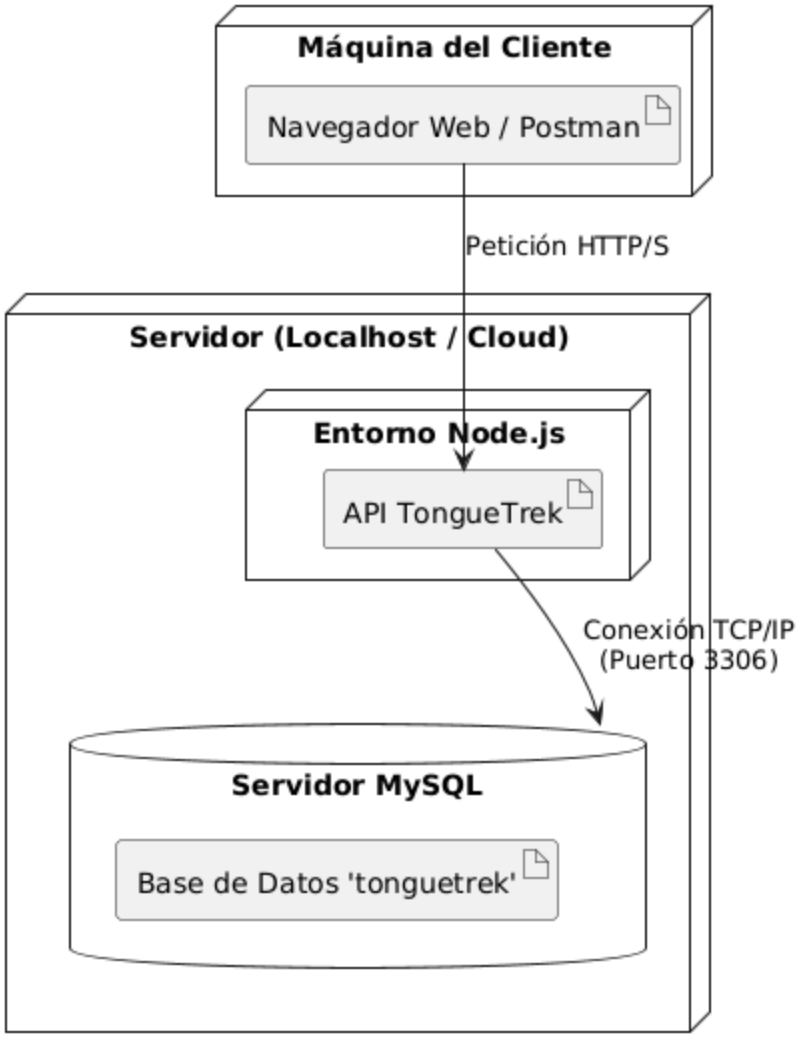

Diagrama de Objetos - Validación de Respuestas Exitosa