

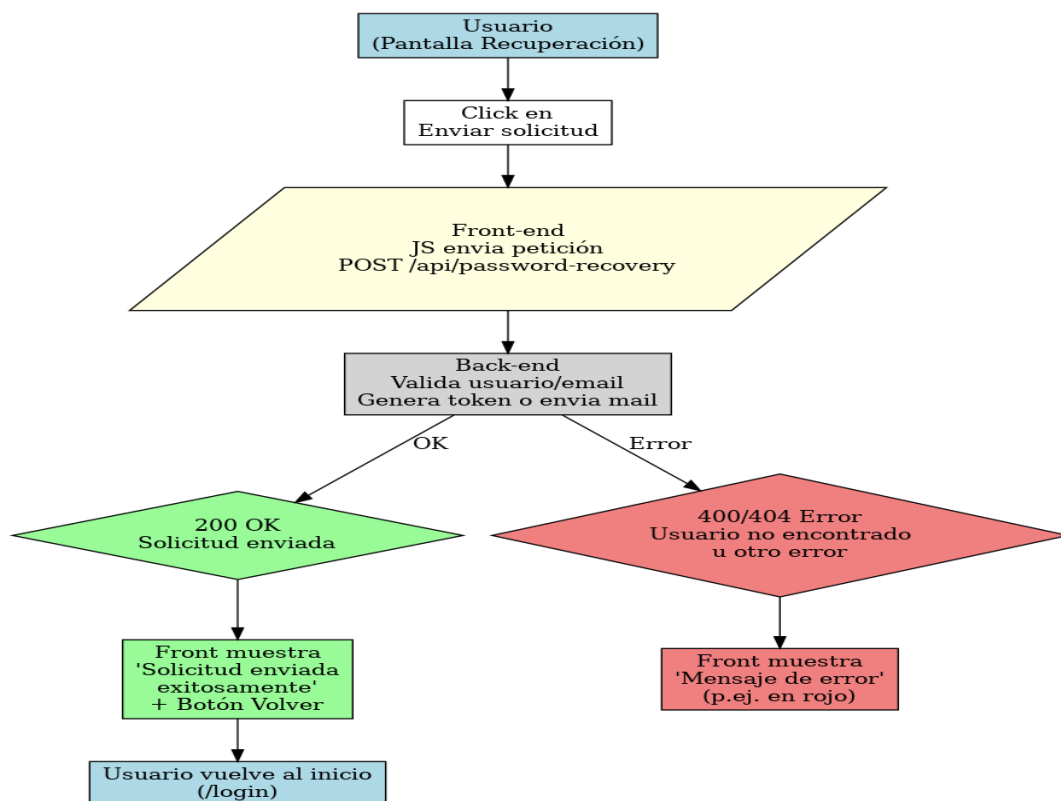
Documento Técnico – Flujo de Recuperación de Contraseña

1. Descripción General

La funcionalidad de recuperación de contraseña permite que un usuario que olvidó sus credenciales pueda solicitar asistencia para restablecerlas. El front-end gestiona la interfaz y la interacción con el usuario, mientras que el back-end se encarga de validar la información, generar la solicitud y devolver una respuesta apropiada.

2. Flujo del Proceso

1. Pantalla inicial: El usuario accede a la página de Recuperación de Contraseña. 2. Acción de envío: El usuario presiona Enviar solicitud, el front dispara un POST hacia el back-end. 3. Procesamiento en el back-end: Se valida usuario/email, se genera token o se envía notificación. 4. Respuesta del back-end: 200 OK (éxito), 400/404 (error usuario), 500 (error interno). 5. Manejo en el front-end: Mostrar mensajes de éxito o error según la respuesta. 6. Finalización: El usuario vuelve al inicio (/login).



3. Requerimientos para el Back-end

- Endpoint: Definir la URL oficial (ejemplo: /api/password-recovery). - Datos de entrada: Confirmar si se usará email, usuario o DNI. - Validaciones: Usuario existente, intentos múltiples, etc. - Respuesta estándar: {status: ok, message: 'Solicitud registrada'} o {status: error, message:

'Usuario no encontrado'}. - Seguridad: Token temporal, expiración, encriptación. - Correo: Definir si se enviará automáticamente o será atendido por un administrador.

4. Consideraciones de Seguridad

- Evitar exponer si un usuario existe o no. - Implementar límites de solicitudes (rate limiting). - Manejar los tokens de forma segura (firmados, con expiración).