

L U M B R E



Recuperar la contraseña sin abrir una puerta

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

«¿Olvidaste tu contraseña?» parece un detalle amable; es otro frente expuesto al atacante. Una recuperación mal diseñada regala acceso o información. Aquí aprendes a pedirle a la IA un flujo seguro: enlace de un solo uso que caduca, sin revelar cuentas, sin respuestas de seguridad absurdas, y a entender por qué lo obvio suele ser lo peligroso.

QUÉ APRENDERÁS

- Diseñar una recuperación segura (tokens de un solo uso, expiración, sin pistas débiles).

La puerta de atrás del inicio de sesión

La recuperación existe porque la gente olvida. Pero es, literalmente, un camino para entrar **sin** la contraseña. Si ese camino es demasiado cómodo, el atacante lo usará contra ti. Diseñarlo bien no es complicar al usuario: es que solo el dueño real de la cuenta pueda recorrerlo.

Cómo debe funcionar (y por qué)

ACTIVIDAD INTERACTIVA DISPONIBLE EN
LUMBRE

1. El flujo seguro de recuperación



Las reglas que evitan la puerta abierta

Cada regla cierra un hueco concreto; no son burocracia, son defensa.

Regla	Qué ataque previene
Mensaje neutro («si el correo existe...») sin confirmar si la cuenta existe	Enumeración de cuentas registradas
Token aleatorio, largo y de un solo uso	Adivinar o reutilizar un enlace
Expiración corta (minutos)	Enlaces robados que siguen válidos
Invalidar el token tras usarlo y al cambiar la contraseña	Reutilización del mismo enlace
Nada de «preguntas de seguridad» (nombre de tu mascota)	Respuestas fáciles de investigar en redes

Prompt de recuperación

Cerrar cada hueco, uno por uno

Implementa la recuperacion de contraseña con estas reglas (confirma cada una):\n- al pedir recuperacion, responde SIEMPRE el mismo mensaje, exista o no el correo (no reveles cuentas)\n- genera un token aleatorio largo, guardado hasheado, con expiracion de 15 minutos y de un solo uso\n- envia un enlace con ese token al correo del usuario\n- al usarse el token y cambiar la clave, invalida el token\n- NO uses preguntas de seguridad tipo "nombre de tu mascota"\n\nExplica como invalido el token tras usarlo.

Prueba

2. Cuando alguien escribe un correo en «recuperar contraseña», la app responde «ese correo no está registrado». ¿Qué problema abre esa respuesta?

- ☐ Ninguno: es más útil para el usuario.
- ☐ Permite a un atacante descubrir qué correos tienen cuenta (enumeración).
- ☐ Acelera la recuperación.
- ☐ Hace el sistema más seguro.

3. Un enlace de recuperación que nunca caduca es más cómodo y aceptable para producción.

- ☐ Verdadero
- ☐ Falso

Detecta la recuperación insegura

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN LUMBRE

4. Revisas el flujo de recuperación de una IA. Señala la decisión que abre una puerta:



5. Escribe tu flujo de recuperación como reglas con su ataque asociado (mensaje neutro, token que caduca, un solo uso). Pídele a la IA que confirme cada regla al entregar.

La comodidad de una recuperación insegura la paga el usuario al que le roban la cuenta.

Referencia curricular

Materia:	Desarrollo de Software con IA
-----------------	-------------------------------

Versión interactiva completa (con actividades, videos y autoevaluación):



<https://empresa.lumbre.lat/object/fsi-m10-0a02>

Material educativo generado desde Lumbre · lumbre.lat