

L U M B R E



Registro y login con IA: la parte que no debes pedir a ciegas

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

Pedirle a la IA «hazme un login» es la forma más rápida de obtener un login inseguro. La autenticación es la puerta de tu casa: si está mal, todo lo de dentro vale poco. Aquí aprendes a especificar registro y acceso con los requisitos que no se negocian —contraseña cifrada, sin contraseñas en texto plano, protección contra fuerza bruta— y a revisar que la IA los cumplió.

QUÉ APRENDERÁS

- Especificar el flujo de autenticación con requisitos de seguridad y revisar los puntos críticos.

La puerta no se le puede encargar a la suerte



Identidad no es un botón de login: es quién entra, qué toca y qué pasa cuando se va. De toda tu app, esta es la parte donde la IA no puede improvisar.

Autenticarse es demostrar quién eres. Es la parte de tu app donde un error no es un bug: es una **brecha**. La IA la construye en segundos, pero si solo le pediste «login», usará el primer patrón que se le ocurra, no necesariamente el seguro. Aquí tú pones los requisitos y conviertes la seguridad en criterio de aceptación.

Los no-negociables al especificar el acceso

Estos cinco convertidos en criterios son la diferencia entre un login y una puerta abierta.

Requisito	Por qué importa	Cómo se lo pides a la IA
Contraseña cifrada (hash), nunca en texto plano	Si te roban la base, nadie recupera contraseñas	«guarda la contraseña con hashing, jamás en claro»
Longitud mínima y reglas	Contraseñas cortas se rompen fácil	«mínimo 8 caracteres, con mensaje claro»
No revelar cuál campo falló	Ayuda al atacante a adivinar cuentas	«mensaje genérico: credenciales incorrectas»
Limitar intentos	Frena la fuerza bruta	«bloquea tras N intentos seguidos»
La contraseña viaja por HTTPS	Evita que se lea en tránsito	«todo el flujo por HTTPS»

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

1. El viaje de una contraseña



Para reforzar tokens y claves

Prompt con requisitos

Seguridad como criterio de aceptación

Crea registro y login seguros para mi app. Requisitos OBLIGATORIOS (confirma cada uno al terminar):\n- la contraseña se guarda con hashing (bcrypt o similar), NUNCA en texto plano\n- minimo 8 caracteres al registrarse, con mensaje de error claro\n- al fallar el login, mensaje generico "correo o contrasena incorrectos" sin decir cual fallo\n- tras 5 intentos fallados seguidos, bloquea temporalmente ese correo\n- todo por HTTPS\n\nNo inventes un cifrado propio. Usa una libreria madura de hashing.

Prueba

2. La IA terminó tu login y, al revisar, ves que la base de datos guarda la contraseña tal como la escribe el usuario. ¿Qué requisito se incumplió?

- ☐ El mensaje de error genérico.
- ☐ El almacenamiento cifrado (hash): jamás en texto plano.
- ☐ El bloqueo por intentos.
- ☐ La longitud mínima.

3. Un mensaje de error que dice «el correo existe pero la contraseña no» es una buena práctica de seguridad.

- ☐ Verdadero
- ☐ Falso

Detecta el login inseguro

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

4. Revisas el resumen de lo que hizo una IA para el login. Señala la decisión peligrosa:



5. Escribe los requisitos de seguridad de tu login como lista de criterios (cifrado, longitud, mensaje genérico, intentos, HTTPS). Pídele a la IA que los confirme uno a uno al entregar.

En autenticación, «funciona» no es suficiente: tiene que ser seguro por diseño.

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/fsi-m10-0a01>

Material educativo generado desde Lumbre · lumbre.lat