

L U M B R E



Contraseñas, hashing y secretos: lo que jamás va en el código

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

Hay información que no debe quedar escrita donde cualquiera la pueda ver: contraseñas, claves de API, datos de acceso a la base de datos. Aquí aprendes la diferencia entre cifrar (recuperable) y hashear (irreversible), qué son los «secretos» y por qué van en variables de entorno, y cómo detectar cuando la IA metió una clave en el código o en el repositorio.

QUÉ APRENDERÁS

- Distinguir cifrado de hashing, manejar variables de entorno y nunca exponer claves.

Dos formas de ocultar que no son lo mismo

Cifrar es cerrar con llave: quien la tiene reabre y lee el original. Sirve para datos que necesitas volver a usar. **Hashear** es triturar: se convierte en una huella irreversible; no se «deshashea». Sirve para contraseñas, porque solo necesitas comprobar, no recuperar. Confundirlas es un error de seguridad clásico de la IA.

ACTIVIDAD INTERACTIVA DISPONIBLE EN LUMBRE

1. Cifrado vs hashing



Los «secretos»: lo que nunca va en el código

Un secreto escrito en el código viaja al repositorio, al desplegar y a cualquiera que lea el archivo.

Secreto	Ejemplo	Dónde va
Clave de API	API_KEY del clima o de pagos	variable de entorno en el servidor
Credencial de base de datos	DB_PASSWORD	variable de entorno
Contraseña de usuario	la que escribe al registrarse	solo como hash en la base de datos
Token de firma	SECRET_TOKEN de la sesión	variable de entorno

Cómo detectar la IA que expone un secreto

El literal es la filtración

```
MAL (clave pegada en el código, va al repositorio):\n  const API_KEY = "abc123-CLAVE-REAL";\n  fetch(API+"/pagos?key="+ API_KEY);\n\nBIEN (se lee del entorno del servidor, nunca se imprime):\n  const API_KEY = process.env.API_KEY;  // llega del entorno\n  // y la llamada se hace desde el backend, no desde el navegador\n\nREGLA: ningún secreto aparece literal en el código ni en el frontend; solo referencias a variables de entorno.
```

Prueba

2. ¿Por qué las contraseñas se guardan con hashing y no cifradas?

- ☐ Porque el hash es más rápido de calcular siempre.
- ☐ Porque no necesitas recuperar la contraseña, solo verificarla; el hash irreversible protege ante un robo de datos.
- ☐ Porque el cifrado está prohibido.
- ☐ Porque el hash permite leer la contraseña.

3. Guardar una API key directamente en el código fuente es aceptable mientras el proyecto sea privado.

- ☐ Verdadero
- ☐ Falso

Detecta el secreto expuesto

ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

4. Revisas lo que entregó una IA. Señala el punto que filtra un secreto:



5. Haz una lista de los secretos de tu proyecto (claves, credenciales) y de dónde debe vivir cada uno (variable de entorno). Pide a la IA que no deje ninguno literal en el código.

Si un secreto se puede ver en el repositorio, da por hecho que ya lo vio alguien.

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/fsi-m11-0a02>

Material educativo generado desde Lumbre · lumbre.lat