

L U M B R E



Auditoría de seguridad con IA: el prompt que encuentra lo que tú no ves

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

No sabes de seguridad lo suficiente para auditarla tú: para eso está la IA. La habilidad del AI Software Builder es pedir una auditoría con un guion concreto (no «míralo por si acaso»), leer el informe sin asustarse y priorizar los hallazgos por riesgo real para ordenar las correcciones. Aquí conviertes a la IA en tu revisor de seguridad.

QUÉ APRENDERÁS

- Solicitar y leer un informe de auditoría de seguridad generado por IA y priorizar hallazgos.

No audites con los ojos: audita con un guion

«Revísalo por seguridad» es un prompt débil: la IA responderá «todo está bien». Una auditoría útil exige un **guion de chequeo** y una **salida con formato**. Y sobre todo, saber leer el resultado: no todos los «problemas» valen lo mismo. Tu trabajo es dirigir la revisión y decidir el orden de ataque.

El guion que le pasas

Auditoría con salida accionable

```
Actua como auditor de seguridad. Revisa ESTE codigo y responde SOLO con una
tabla:\n| Hallazgo | Dónde (archivo/linea) | Riesgo (alto/medio/bajo) | Por que
importa | Como arreglarlo |\n\nChequea en concreto:\n- inyeccion SQL (consultas
con concatenacion de entrada)\n- secretos literales en el codigo o expuestos al
frontend\n- endpoints sin comprobar permiso en el servidor\n- datos de usuario
mostrados sin escapar (XSS)\n- contraseñas sin hashing\n- acciones sensibles sin
token CSRF\n- informacion de error que revela detalles internos\n\nPrioriza lo de
RIESGO ALTO primero. No arregles nada aun; solo el informe.
```

Priorizar por riesgo, no por cantidad

Diez hallazgos bajos no valen uno alto. Prioriza por lo que te pueden robar hoy.

Riesgo	Qué significa	Qué haces
Alto	Permite robar datos o entrar sin permiso ahora	se corrige antes de publicar
Medio	Expone algo pero con condiciones	se corrige en la siguiente iteración

Riesgo	Qué significa	Qué haces
Bajo	Buena práctica incumplida sin daño inmediato	se anota para pulir

Cómo leer el informe sin paralizarte

Un buen informe puede listar treinta cosas. No es que tengas un desastre: es que el auditor fue minucioso. Marca los **altos que afectan datos o acceso**, corrígelos, y vuelve a auditar: esa segunda pasada confirma que cerraste lo crítico antes de desplegar.

Umbral de publicación

Regla práctica: antes de publicar, cero hallazgos de riesgo ALTO sobre datos, acceso o secretos. Lo demás se puede iterar.

Prueba

1. El informe de auditoría lista 12 hallazgos: 2 de riesgo alto (acceso sin permiso y una clave expuesta) y 10 bajos de estilo. Tu decisión correcta es:

- ☐ Publicar ya, porque 10 de 12 son solo estilo.
- ☐ Corregir primero los 2 altos (acceso y secreto) y reauditar antes de publicar.
- ☐ Ignorar el informe porque la IA siempre exagera.
- ☐ Corregir los 10 bajos primero porque son más.

2. Pedir a la IA una auditoría con el prompt «révisalo por seguridad» suele bastar para encontrar los riesgos reales.

- ☐ Verdadero
- ☐ Falso

Detecta la falsa auditoría

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

3. Le pides auditoría a una IA y te responde esto. Señala la señal de que NO hizo una revisión útil:



4. Escribe tu propio guion de auditoría (lista de comprobación + formato de tabla) y pásaselo a la IA sobre una pieza de tu proyecto. Ordena los hallazgos por riesgo antes de pedir correcciones.

Un builder no sabe de seguridad todo: sabe pedir, leer y priorizar la revisión.

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/fsi-m11-0a03>

Material educativo generado desde Lumbre · lumbre.lat