

L U M B R E



El costo silencioso: dependencias, parches y vulnerabilidades

Materia: Desarrollo de Software con IA

07/10/2026

Antes de empezar

Tu aplicación es 20 % código que dirigiste y 80 % código prestado: librerías, paquetes, frameworks. Todo ese edificio de terceros recibe parches —unos te salvan la vida, otros te rompen la app— y a veces el mantenimiento se abandona y sus grietas pasan a ser tuyas. Entender la cadena de deuda invisible es lo que te deja decidir con la IA cuándo actualizar, cuándo congelar y cuándo desconfiar de un paquete nuevo.

QUÉ APRENDERÁS

- Entender qué es una dependencia, por qué se actualiza y cómo gestionar el riesgo.

Vas sobre un edificio que no cuidas tú



Publicar no termina el proyecto: empieza su vida. Logs, backups, dependencias y parches: la rutina mensual que separa un producto de una fotografía.

Casi todo lo que usa tu app viene de terceros: el framework, el lector de fechas, el cliente de base de datos, hasta el utilitario que formatea correos. Esas **dependencias** son gratis de usar y ajenas de mantener... hasta que algo pasa. Un parche de

seguridad que no aplicas es una puerta abierta que sí es tuya; una actualización que aplicas sin probar puede romper lo que funcionaba.

ACTIVIDAD INTERACTIVA
DISPONIBLE EN LUMBRE

1. El ciclo de vida (y muerte) de una dependencia



Las cuatro reglas de la convivencia

La paradoja: los paquetes te ahorran semanas de trabajo y te hipotecan minutos de atención para siempre. Barato no es gratis.

Regla	Qué significa	Cómo se la pides a la IA
Versiones ancladas	tu app fija exactamente qué versión de cada paquete usa; sin anclar, el día que el mundo actualice, tu app cambia sin tu permiso	«asegúrate de que package/requirements queda fijado a versiones exactas»
Mantén la lista corta	cada paquete es una deuda: si lo puedes hacer en 30 líneas, no lo traigas de terceros	«cuestiona cada dependencia: ¿qué gana y qué nos ata?»
Actualiza en rama con pruebas	los parches entran por tu puerta, con suite verde, no por sorpresa un martes	«abre rama de actualización, corre la suite y muéstrame qué rompió»
Escucha los avisos	un scanner de vulnerabilidades te dice HOY lo que alguien descubrirá en tu app mañana	«integra un chequeo de vulnerabilidades en dependencias, con reporte semanal»

El prompt del inventario de deudas

Inventario con acción: la foto y el mapa

Hazme el inventario de dependencias de mi app y clasificalas:\n1. criticas (framework, base de datos, autenticacion, pagos)\n2. utiles (fechas, validadores, imagenes)\n3. cuestionables (lo que ocupa 30 lineas y podria no ser de terceros)\n\nPara cada una: version anclada, que tan activa esta su mantencion\n(ultima publicacion, issues abiertos, quien la mantiene) y si hay vulnerabilidades reportadas.\n\nTermina con un plan de ACCION, no una lista: que actualizo esta semana, que congelo,\nque reemplazo, que elimino. Prioriza lo que toca autenticacion o datos de usuarios.

Prueba

2. Tu framework publica un parche de seguridad y tu app lo usa. ¿Qué decisión es la sana?

- ☐ Ignorarlo: el viejo funciona bien.
- ☐ Actualizar ya, directo a producción, porque es seguridad.
- ☐ Actualizar en una rama, correr la suite completa y, si está verde, publicar.
- ☐ Esperar un mes a ver si nadie reporta ataques.

3. Cuántas más dependencias usas, más rápido construyes... y menos control tienes sobre los cambios que llegan.

- ☐ Verdadero
- ☐ Falso

Detecta la adopción ingenua

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

4. La IA sugirió instalar un paquete para formatear teléfonos. Revisa su tarjeta de identidad. Señala la señal que debe preocuparte:



5. Pide a la IA el inventario del prompt con tu proyecto real y decide: ¿qué paquete sale, cuál queda anclado y quién revisará los avisos cada mes? Escribe las tres respuestas en tu documento maestro.

La deuda invisible solo es peligrosa mientras es invisible.

Referencia curricular

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

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



<https://empresa.lumbre.lat/object/fsi-m18-0a01>

Material educativo generado desde Lumbre · lumbre.lat