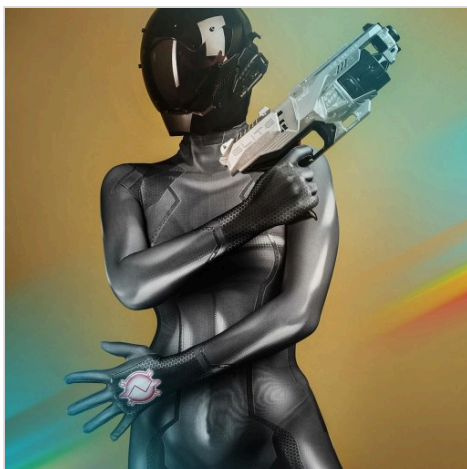


L U M B R E



Seguridad, roles, logs y respaldo

Materia: IA Aplicada, Vibe Coding y Negocios Digitales

07/10/2026

Antes de empezar

Lo que un cliente te preguntará antes de firmar. Claves API escondidas, permisos por rol, un registro que no guarda datos de más y un respaldo que sí se puede restaurar.

QUÉ APRENDERÁS

- Entender los cuatro cimientos operativos de un producto: proteger accesos, separar permisos por rol, registrar lo que pasa y poder recuperar los datos.

Cuatro preguntas que separan amateurs de profesionales



Imagen libre de Wikimedia Commons (CC BY-SA 4.0, autor: El Pantera)

VIDEO

Qué es un MVP y cómo desarrollarlo

La diferencia entre un prototipo y un producto que se puede vender. Este marco acompaña los doce exámenes de producción del curso.



Escanea para verlo en Lumbre

<https://www.youtube.com/watch?v=j93sHYwcdLI>

Cuando un negocio te va a confiar su operación, hace cuatro preguntas, con o sin palabras técnicas. **Seguridad:** ¿están protegidas las llaves de acceso (las API key)? **Roles:** ¿cada quien ve solo lo que debe? **Logs:** ¿hay registro de lo que pasó para revisar después? **Respaldo:** si algo se borra o se corrompe, ¿se puede recuperar?

Ninguna de las cuatro hace tu producto más 'inteligente', pero la ausencia de cualquiera te puede costar el cliente y un problema legal.

No son funciones: son seguros que evitan el desastre. Un respaldo sin probar no es respaldo.

Cimiento	Qué protege	El error típico del prototipo
Seguridad	Que nadie use tu cuenta de IA gratis ni robe accesos	La API key pegada en el código o expuesta en el navegador
Roles	Que un usuario no vea datos de otro	Un solo usuario "administrador" para todos
Logs	Poder reconstruir qué pasó	No registrar nada, o registrar datos sensibles de más
Respaldo	No perder los datos del cliente	Nunca probar que el respaldo sí se puede restaurar

Una API key expuesta es una fuga

Si tu clave de IA está en el código que se envía al navegador, cualquiera la copia y gasta **con tu tarjeta** o accede **con tus permisos**. La clave vive en el servidor, nunca en el cliente. Y si se filtró, se **rota** (se genera una nueva), no se "esconde un poquito".

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

1. Un desarrollador describe cómo dejó su prototipo. Un detalle es un error de seguridad serio. Márcalo.



2. ¿Cuál práctica hace que un respaldo merezca llamarse así?

- ☐ Copiar la base de datos una vez al año y guardarla en un USB en tu cajón.
- ☐ Hacer copias periódicas Y probar de vez en cuando que puedes restaurar una.
- ☐ Confiar en que el hosting nunca se caerá.
- ☐ Guardar todo en una sola cuenta de correo.

ACTIVIDAD
INTERACTIVA
DISPONIBLE EN
LUMBRE

3. Tu producto guarda en los logs "todo por si acaso", incluyendo el contenido completo de los mensajes y datos personales. ¿Qué tan sano es eso?



4. Ordena el flujo de defensa ante una API key que se filtró.

Confirmar la filtración y dónde quedó expuesta. _____

Rotar: generar una nueva clave y revocar la vieja en el proveedor.

Actualizar el servidor para que use la nueva clave. _____

Revisar el uso reciente para detectar consumo anómalo. _____

Corregir la causa para que no vuelva a exponerse. _____

5. De los cuatro cimientos (seguridad, roles, logs, respaldo), ¿cuál tiene hoy tu mejor prototipo y cuál le falta por completo? Una línea de evidencia para cada uno.

Si no sabes si tu respaldo se restaura, no tienes respaldo todavía.

Siguiente paso: Proyecto — auditarás un prototipo con los 12 exámenes y escribirás su plan realista para volverse producto.

Referencia curricular

Materia:	IA Aplicada, Vibe Coding y Negocios Digitales
-----------------	---

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



<https://empresa.lumbre.lat/object/iav-c15-r01-0a02>

Material educativo generado desde Lumbre · lumbre.lat