

Resumen

Entrega: 5 de octubre de 2026 · v1.2

Contexto: Webapp B2B lanzada en pocas semanas (vibe coding): dashboard, login de clientes y chat con IA. Pidieron revisar el gasto en IA; el informe incluye también privacidad y base de datos porque ahí está el riesgo antes de una multa o una reclamación.

GASTO MENSUAL

412 €

GASTO ANUAL (×12)

4944 €

AHORRO POSIBLE (ESTIMACIÓN)

71 €–125 €/mes

Equivalente anual: 852 €–1500 € (estimación).

NIVEL DE CONTROL

● Bajo

La app ya factura clientes pero la base de datos permite ver datos ajenos, el chat IA trata datos personales sin aviso y hay herramientas duplicadas sin uso.

ACCIONES PARA ESTA SEMANA

1. Cerrar el acceso cruzado entre cuentas de clientes

0 €

Prioridad legal: hasta que no esté corregido y probado, no conviene captar más clientes con datos sensibles.

2. Regularizar el chat con IA (aviso + contrato con proveedor)

0 €

Dejar claro qué se envía a OpenAI y actualizar la página de privacidad antes de seguir promocionando el asistente.

3. Cancelar GitHub Copilot (duplicado con Cursor)

28 €

Ahorro directo en licencias; el equipo ya trabaja solo en Cursor.

Dónde se va el dinero

Herramientas incluidas en el análisis del periodo.

Herramienta	Tipo	Coste/mes	Uso	Veredicto
OpenAI (asistente en la web)	Consumo (tokens/API)	124 €	Chat en producto; en la revisión se vio que recibe email y nombre del usuario	VIGILAR
Supabase (base de datos)	Otros	48 €	Datos de clientes y ficheros; reglas de acceso incompletas (ver hallazgos)	VIGILAR
Cursor	Licencias (seats)	40 €	Desarrollo diario del producto	MANTENER
Vercel (hosting)	Otros	34 €	Web en producción	MANTENER
Anthropic (pruebas internas)	Consumo (tokens/API)	72 €	Experimentos puntuales; solapa con Cursor	REDUCIR
GitHub Copilot	Licencias (seats)	28 €	Sin uso en 30 días	CANCELAR
Make (automatizaciones)	Agentes	66 €	Onboarding y emails; corre de noche sin necesidad	REDUCIR

REPARTO POR TIPO

Licencias (seats)		68 € (17 %)
Consumo (tokens/API)		196 € (48 %)
Agentes		66 € (16 %)
Otros		82 € (20 %)

Riesgos, privacidad y fugas de gasto

Primero lo que puede multar o parar el negocio; después el ahorro mensual en herramientas.

Los clientes pueden ver datos que no son suyos

Exposición orientativa 15.000 €–80.000 €

Qué pasa

La web en producción no separa bien las cuentas: un usuario entra y ve proyectos y nombres de otra empresa. Es un fallo grave de base de datos, muy habitual cuando la app se montó rápido con plantillas.

Por qué importa (€ y legal)

No es un ahorro mensual: es exposición a reclamaciones, parar ventas, notificar a la Agencia Española de Protección de Datos si confirman filtración y sanciones RGPD (en pymes el daño reputacional y legal suele superar con creces el ahorro en licencias de IA).

Qué hacer

Corregir reglas de acceso en la base de datos, probar con dos cuentas de prueba y guardar captura de que ya no ocurre.

El chat con IA trata datos personales sin dejarlo claro

Exposición orientativa 5000 €–35.000 €

Qué pasa

El asistente manda email y nombre a OpenAI. En privacidad no se explica y no consta contrato de encargo (DPA) con el proveedor.

Por qué importa (€ y legal)

Riesgo de incumplimiento del RGPD (información y base legal) y de que un cliente o empleado presente reclamación antes de que lo arregléis.

Qué hacer

Texto claro en el chat y en privacidad, minimizar lo que se envía al modelo y formalizar el DPA con OpenAI.

Datos personales en logs demasiado tiempo

Exposición orientativa 3000 €–25.000 €

Qué pasa

Los registros del servidor guardan emails y rutas con nombres de clientes sin plazo de borrado definido.

Por qué importa (€ y legal)

Si esos logs se filtran o los pide un auditor, el mismo problema que una brecha de la app; multas por conservación excesiva.

Qué hacer

Dejar de loguear datos sensibles, fijar retención (p. ej. 30 días) y anotarlo en el registro de actividades de tratamiento.

Copilot pagado sin nadie usándolo

Ahorro 28 €/mes

Qué pasa

Dos licencias activas en factura; el equipo desarrolla en Cursor.

Cuánto cuesta

28 € al mes tirados.

Qué hacer

Cancelar en GitHub y revisar licencias cada trimestre.

Plan de acción

ESTA SEMANA

- Corregir acceso a datos entre clientes y documentar la prueba.
- Actualizar privacidad y aviso del chat IA; iniciar DPA con OpenAI.
- Cancelar Copilot y acortar retención de logs.

ESTE MES

- Registro de actividades de tratamiento (RGPD) al día con lo que realmente hace la app.
- Revisar copias de seguridad de la base de datos (cifrado y quién puede exportar).
- Tope de gasto en OpenAI y recortar API Anthropic si sobra.

SIGUIENTE NIVEL

Revisión de 45 min para priorizar legal + gasto en IA en equipos que han lanzado la app muy rápido.

Reservar revisión · 590 €

AVISOS

- Las cifras de exposición legal son órdenes de magnitud orientativas, no predicciones de multa.
- Este documento no es asesoramiento jurídico; para sanciones y notificaciones consultad abogado y DPO.
- Ejemplo ilustrativo con Hatchpad ficticio; Strix es herramienta de terceros citada solo como referencia de formato.

Anexo: Muestra de auditoría (formato Strix)

Fragmento de informe técnico generado con un agente open source de pruebas de seguridad, reescrito para dirección y finanzas. En un encargo real cruzamos esto con vuestras facturas de IA.

Referencia técnica: github.com/usestrix/strix · Apache-2.0 · usestrix/strix

ALCANCE

Revisión de seguridad y privacidad — Hatchpad (web en producción)

App publicada en internet (login de clientes, base de datos en la nube). Revisión sin acceso a vuestro panel de admin: pruebas como las haría un tercero.

Flujo inspirado en Strix (agente open source, Apache-2.0)

CRÍTICO

Un cliente puede ver datos de otro

Con una cuenta normal se accede a ficheros y nombres de empresas que no son la suya. Típico cuando la base de datos se dejó abierta durante el desarrollo rápido.

Qué hacer: Separar datos por cliente en la base de datos y probarlo con dos cuentas de prueba antes de seguir vendiendo.

Si no actuáis: Reclamación de afectados, parada de servicio y sanción RGPD: exposición alta para una pyme (decenas de miles de € en el peor escenario).

ALTO

Datos personales en registros sin plazo de borrado

Emails y nombres quedan guardados en logs del servidor más de lo necesario; no hay política clara de cuánto tiempo se conservan.

Qué hacer: Dejar de registrar datos sensibles, acortar retención y documentarlo en el registro de actividades (RGPD).

Si no actuáis: Incumplimiento de minimización y conservación (art. 5 RGPD); multa y obligación de notificar a la autoridad si hay filtración.

ALTO

Chat con IA sin aviso al usuario

El asistente del producto envía nombre y email del usuario a OpenAI sin explicarlo en privacidad ni contrato de encargo con el proveedor.

Qué hacer: Actualizar la política de privacidad, informar en el chat y firmar DPA con el proveedor de IA.

Si no actuáis: Tratamiento sin base legal clara; reclamaciones y bloqueo de marketing hasta regularizar.

MEDIO

Copias de seguridad de la base sin cifrar

Las copias automáticas existen, pero no consta cifrado ni quién puede descargarlas.

Qué hacer: Activar cifrado en el proveedor de base de datos y limitar quién puede exportar datos.

Si no actuáis: Si una copia se filtra, misma gravedad que una brecha de la app en vivo.

Ejemplo ilustrativo para el informe de auditamia. Hatchpad es ficticio; el formato imita informes de agentes como Strix (usestrix/strix), traducido a lenguaje de negocio.