Veinticuatro mil apps con la puerta abierta

Una firma de seguridad de Hamburgo y el diario Handelsblatt encontraron 24.664 apps hechas con Lovable que entregaban registros de su base de datos sin pedir clave, y por esos datos responde la empresa que publicó la app.

Por Oscar Obando Chaves · Chief AI Officer · Legal AI Engineer · Noviembre 2026 · Documento de distribución libre · Publicado originalmente en LinkedIn

24.664 apps sin pedir clave

24.664 apps hechas con Lovable entregaban registros de su base de datos sin pedir clave, y en 7.403 había correos electrónicos. Lo encontraron Crissy Field, una firma de seguridad de Hamburgo, y el diario Handelsblatt al revisar casi 160.000 proyectos hechos con esa plataforma, donde había pasaportes, datos de pago, mensajes privados y hasta resúmenes de los correos internos de una administradora de inmuebles sobre sus inquilinos.

La IA armó las apps, pero las reglas de acceso de cada base de datos, las que dicen quién puede leer qué, las tenía que poner quien las publicó.

Es la app que hoy una pyme arma en semanas para su tienda, sus reservas o su portal de clientes, y en Ecuador, si esos datos se vulneran, la responsable es la empresa que la publicó.

Fuentes: Crissy Field, informe sobre Lovable, y Handelsblatt (2 y 3 de noviembre de 2026).

Las cifras y lo que había adentro

Los investigadores revisaron 159.041 proyectos hechos con Lovable y publicados entre diciembre de 2025 y septiembre de 2026, de los cuales 34.545 usaban la base de datos Supabase, 24.664 entregaban registros a cualquier visitante sin pedir clave y 7.403 dejaban ver correos de personas.

Adentro había de todo, desde números de pasaporte, datos de pago y códigos de entradas de organizadores de eventos y de restaurantes hasta más de 200.000 mensajes privados de un foro alemán y resúmenes hechos con IA de los correos de una administradora de inmuebles

sobre sus inquilinos y propietarios.

Fuentes: Crissy Field y Handelsblatt (2 y 3 de noviembre de 2026).

Faltaban las reglas de acceso

Cada base de datos necesita reglas que digan quién puede leer qué, y esas reglas las configura quien publica la app, mientras que Lovable le respondió al diario que es un problema conocido de toda la industria.

El informe trae cuatro salvedades que conviene leer junto con las cifras, puesto que entregar datos sin clave no prueba por sí solo una falla, ya que pueden ser datos pensados para mostrarse, y la muestra sale de un archivo público de la web y no representa a todos los proyectos de Lovable. Que los correos estén a la vista tampoco equivale a una tasa confirmada de filtración, y no se sabe si alguien usó esos datos.

Fuentes: Crissy Field, informe sobre Lovable (noviembre de 2026); Handelsblatt (3 de noviembre de 2026); Techzine (4 de noviembre de 2026).

Antes de que atienda a un cliente

Armarla en semanas está muy bien, siempre que alguien revise quién puede leer qué antes de que atienda al primer cliente, y con las recomendaciones del informe de Crissy Field esa revisión tiene tres partes.

1. Quién puede leer qué, con las reglas de acceso de cada tabla puestas antes de cargar datos reales.

2. La app probada como un extraño, sin iniciar sesión, igual que lo hicieron los investigadores.

3. Otros ojos, con permisos, interfaces y cuentas revisados por alguien que no la armó.

Que la app se haya armado en semanas no cambia quién responde, puesto que por los datos de tus clientes responde tu empresa desde el primer día.

Fuentes: recomendaciones del informe de Crissy Field sobre Lovable (noviembre de 2026).

Oscar Obando Chaves es Chief AI Officer y Legal AI Engineer ecuatoriano, con formación en derecho. Ayuda a las empresas a decidir cómo usan la IA y construye con ella sistemas para el negocio y para lo legal. Chief AI Officer y Senior AI Counsel en HEKA Law, ISO 42001 AI Management Leader e ISO 38507 AI Governance Leader. Publica análisis semanal sobre el impacto real de la IA.