

Informe de revisión pre-lanzamiento



Los 3 hallazgos más importantes — revisión inicial gratuita

SubeSeguro

subeseguro.com · Veta Studios

APP REVISADA

kiosco-digital.vercel.app
(ejemplo)

STACK DETECTADO

Next.js · Supabase · Vercel

FECHA

15 de julio de 2026

Resumen en una frase

Tu app funciona bien y se nota el trabajo — pero hoy **cualquier persona podría leer y borrar tu base de datos completa**. Son tres arreglos concretos y ninguno te tomará más de una tarde.

1 · La llave maestra de tu base de datos está visible

CRÍTICO

QUÉ ENCONTRAMOS

En el código que tu app envía al navegador viene incluida la clave `service_role` de Supabase. Esa clave es la «llave maestra»: quien la tenga puede leer, modificar o borrar TODA tu base de datos, saltándose cualquier regla de seguridad.

QUÉ RIESGO TIENE

Cualquiera que abra las herramientas de desarrollador del navegador (F12) puede copiarla en menos de un minuto. Con ella podría descargar los datos de tus clientes o borrar todo. Este es el error más común y más grave en apps hechas con IA.

CÓMO SE ARREGLA

1. En el panel de Supabase: Settings → API → «Reset service_role key» (la actual ya está comprometida).
2. En tu código, usa solo la clave `anon` en el navegador; la `service_role` va únicamente en el servidor, como variable de entorno.
3. En el informe completo te dejamos el paso a paso exacto para tu código.

2 · Tu tabla de clientes no tiene reglas de acceso

CRÍTICO

QUÉ ENCONTRAMOS

La tabla `clientes` de Supabase tiene Row Level Security (RLS) desactivado. En simple: la puerta está sin llave — cualquier visitante puede pedirle a la base de datos la lista completa de tus clientes, con nombres, correos y teléfonos.

QUÉ RIESGO TIENE

Filtración de datos personales de tus clientes. Además del daño de confianza, en varios países esto puede significar multas por protección de datos.

CÓMO SE ARREGLA

1. En Supabase: Table Editor → tabla `clientes` → activar «Enable RLS».
2. Crear una política para que cada usuario vea solo sus propios datos (te dejamos la política lista para copiar en el informe completo).
3. Repetir la revisión en el resto de tus tablas — encontramos 4 más en la misma situación.

3 · Tu login acepta intentos ilimitados ALTO

QUÉ ENCONTRAMOS

El formulario de inicio de sesión no tiene límite de intentos ni protección contra robots. Probamos (con cuidado) y aceptó decenas de intentos seguidos sin frenar ninguno.

QUÉ RIESGO TIENE

Un programa automático puede probar miles de contraseñas hasta entrar a las cuentas de tus usuarios. También puede inflar tu cuenta de Supabase/Vercel con tráfico basura.

CÓMO SE ARREGLA

1. Activar la protección contra bots de Supabase Auth (Captcha integrado, gratis).
2. Agregar límite de intentos por IP en el servidor — son 15 líneas de código que te incluimos en el informe completo.

Lo que también miramos

HTTPS y dominio: bien configurados. Velocidad de carga: buena en escritorio, mejorable en celular (las imágenes pesan 4 MB). Experiencia de usuario: el botón principal se pierde en pantallas chicas. Encontramos 6 hallazgos adicionales de prioridad media y baja — están en el informe completo.

¿Quieres el detalle completo?

El informe completo (US\$29) trae los 9 hallazgos con su arreglo paso a paso y el checklist de lanzamiento. Y si prefieres no tocar nada, te lo dejamos listo nosotros (desde US\$149).

Este es un informe de ejemplo con una app ficticia. Revisión de mejores prácticas — no constituye un pentest certificado.
SubeSeguro · un servicio de Veta Studios · Hecho en Chile para toda Latinoamérica