

PROMPTS DE AUDITORÍA DE SEGURIDAD IA

Vibe Coding & Base de Datos

Copiar y pegar en tus asistentes de IA (Antigravity, Claude Code, V0, Supabase AI)



1. Prompt para Auditar Seguridad con IA en Antigravity / Vibe Coding (Claude Code, V0, Lovable)

Copia y pega este prompt en tu entorno de desarrollo para revisar vulnerabilidades de claves y permisos antes de cada despliegue:

"Analiza mi proyecto y audita la seguridad de las API Keys y entorno de desarrollo. Comprueba:

- Si hay API Keys o secretos expuestos en el código o en el historial de commits.
- Si el archivo .env está en .gitignore.
- Si las claves se cargan de forma segura desde variables de entorno.
- Si hay permisos excesivos en las keys activas.

Dame un informe claro con los riesgos encontrados (gravedad Alta/Media/Baja) y cómo solucionarlos paso a paso."

■ **RECOMENDACIÓN:** Ejecuta esta auditoría antes de cada despliegue importante a producción.

2. Prompt para Auditar Seguridad con IA en Supabase / Backend

Copia y pega este prompt en el agente de IA de Supabase o gestor de base de datos para revisar la seguridad del backend:

"Analiza mi proyecto y realiza una auditoría de seguridad completa sobre la configuración de Supabase. Comprueba:

- Si las credenciales de conexión (anon key y service role key) están protegidas y no expuestas en el repositorio.
- Si las políticas de Row-Level Security (RLS) están activas y correctamente definidas para cada tabla sensible.
- Si las reglas de autenticación y autorización en Supabase Auth limitan el acceso según roles y permisos adecuados.
- Si los endpoints de la API pública están restringidos y no permiten operaciones inseguras (insert, update, delete sin control).
- Si los buckets de almacenamiento (Storage) tienen configuraciones de privacidad correctas y no exponen archivos públicos.
- Si las variables de entorno están correctamente cargadas desde .env y el archivo está incluido en .gitignore.
- Si existen claves o tokens con permisos excesivos o sin rotación periódica.

Dame un informe claro con los riesgos encontrados y cómo solucionarlos paso a paso, incluyendo ejemplos de configuración segura y comandos SQL o de Supabase CLI cuando sea necesario."

■ **RECOMENDACIÓN:** Ejecuta esta auditoría periódicamente o tras realizar cambios en el esquema de base de datos.