Lista de tareas: seguridad antes de publicar

Módulo 11 · iA desde cero · 360MKT

Claves y secretos

- [ ] Ninguna clave, token o contraseña está escrita en el código
- [ ] El archivo `.env` está en `.gitignore`
- [ ] He buscado en el historial de Git que nunca se subió una clave
- [ ] Las claves de producción son distintas de las de pruebas
- [ ] Si una clave se filtró alguna vez, la he cambiado

Usuarios y permisos

- [ ] Las contraseñas se guardan cifradas con un algoritmo de hash, nunca en claro
- [ ] Un usuario no puede ver ni modificar los datos de otro (probado con dos cuentas)
- [ ] Las páginas de administración exigen sesión y rol
- [ ] Los permisos se comprueban en el servidor, no solo en la pantalla
- [ ] Hay límite de intentos de inicio de sesión

Datos de entrada

- [ ] Todo lo que escribe el usuario se valida en el servidor
- [ ] Las consultas a la base de datos usan parámetros, no texto concatenado
- [ ] Lo que escribe un usuario se muestra escapado
- [ ] La subida de archivos limita tipo y tamaño
- [ ] Los formularios públicos tienen protección contra envíos automáticos

Base de datos

- [ ] No es accesible desde internet
- [ ] Si uso Supabase o similar, las reglas de acceso por fila están activadas en todas las tablas
- [ ] La clave de administración de la base de datos no está en el navegador

Servidor y despliegue

- [ ] Todo va por `https`
- [ ] Los mensajes de error no muestran detalles internos al usuario
- [ ] El modo de depuración está desactivado en producción
- [ ] Dependencias actualizadas y sin vulnerabilidades conocidas
- [ ] Sistema, Docker y panel de despliegue actualizados

Pagos

- [ ] Los datos de tarjeta nunca pasan por mi servidor
- [ ] El importe se calcula en el servidor
- [ ] Verifico la firma de los avisos de la pasarela

Revisión

- [ ] He pedido a Claude una revisión de seguridad del proyecto completo
- [ ] He entendido y resuelto cada punto, o he anotado por qué no aplica
- [ ] Si manejo datos sensibles o pagos, lo ha revisado un profesional

Si algo sale mal

- [ ] Sé cómo restaurar la última copia de seguridad
- [ ] Sé cómo cambiar todas las claves
- [ ] Sé a quién debo avisar si se filtran datos personales