ASCENDA

RECURSO DESCARGABLE

Checklist de seguridad web — 20 puntos

La lista que usamos internamente antes de dar cualquier sitio por lanzado. Imprímela, repásala punto por punto, y márcala antes de decir "listo, ya está en línea".

> Si tu sitio es una landing estática sin backend, el bloque de "Autenticación y acceso a datos" todavía no aplica — pero repasa igual el resto. En cuanto sumes un formulario con base de datos, un login o un webhook público, la lista completa entra en juego.

SECRETOS Y CLAVES

- [ ] Oculta claves API — nunca hardcodeadas en el frontend ni en el repo
- [ ] Elimina secretos de Git — revisa el historial, rota cualquier clave que se haya filtrado
- [ ] Clave pública vs. privada de la BD — solo la key "anon/public" va en el cliente (ej. Supabase/Firebase); la "service_role"/secreta nunca sale del backend

AUTENTICACIÓN Y ACCESO A DATOS

- [ ] Row-Level Security (RLS) activo en la base de datos, no solo checks en el frontend
- [ ] Cifrado de datos sensibles (HTTPS en tránsito, cifrado en reposo cuando aplique)
- [ ] Autenticación forzada server-side en cada endpoint/ruta protegida, no solo ocultar el botón
- [ ] Acceso a registros restringido por dueño/tenant — un usuario no debe poder pedir el ID de otro
- [ ] Bloquea la manipulación de campos (mass assignment) — el cliente no debe poder setear role/precio/admin vía payload
- [ ] Cookies con flags HttpOnly, Secure, SameSite
- [ ] Contraseñas hasheadas (bcrypt/argon2), nunca en texto plano ni cifradas reversibles
- [ ] Límite de intentos de login (rate-limit / bloqueo tras varios fallos)

ENTRADAS Y CONTENIDO

- [ ] Consultas parametrizadas siempre (nunca concatenar SQL)
- [ ] Valida toda entrada en el servidor, no confíes solo en la validación del frontend
- [ ] Escapa contenido generado por el usuario antes de renderizarlo (previene XSS)
- [ ] Restringe subida de archivos (tipo, tamaño, sin ejecutables, servidos sin permiso de ejecución)

RED Y ABUSO

- [ ] Protección anti-bots en formularios públicos (captcha/rate-limit)
- [ ] Rate-limit / cuotas en cualquier API pública
- [ ] Cabeceras de seguridad: CSP, X-Frame-Options, X-Content-Type-Options, Strict-Transport-Security, Referrer-Policy
- [ ] Fuerza HTTPS en todo (redirect + HSTS)