GUÍA PDF · STUDIO SANTOLE

Checklist de seguridad para tu web

15 puntos que todo sitio debería revisar antes de salir a producción. Sin letra chica.

familia Santole
Marketing · Programación · Ciberseguridad
studiosantole.com · familiasantole@gmail.com

Los 15 puntos

Repásalos con la web ya montada y antes de abrirla al público. Si fallan más de dos o tres, el riesgo es más alto de lo necesario para lo poco que cuesta corregirlo.

- [ ] 01 **HTTPS en todo el dominio, sin excepciones**

  Certificado válido y renovación automática. Redirección 301 de http a https y de www a no-www (o al revés, pero una sola versión canónica).

- [ ] 02 **Sin contenido mixto**

  Ninguna imagen, script u hoja de estilos cargando por http dentro de una página https. La consola del navegador te lo dice en dos minutos.

- [ ] 03 **Cabeceras de seguridad configuradas**

  Content-Security-Policy, X-Content-Type-Options, Referrer-Policy y Strict-Transport-Security. Son cuatro líneas en el servidor y cierran familias enteras de ataque.

- [ ] 04 **Paneles y rutas de administración protegidos**

  Nada de /wp-admin o /admin accesible al mundo con usuario admin y contraseña débil. Restringe por IP, cambia la ruta por defecto y activa 2FA.

- [ ] 05 **Validación en servidor, no solo en el navegador**

  Todo formulario y todo endpoint valida y sanea lo que recibe en el servidor. La validación del navegador es comodidad para el usuario, no seguridad.

- [ ] 06 **Protección antispam y rate limiting en formularios**

  Un formulario de contacto sin límite de envíos es un buzón de spam y un vector de abuso. Limita por IP y añade honeypot o captcha discreto.

- [ ] 07 **Nada de secretos en el código del cliente**

  Claves de API, tokens y credenciales viven en variables de entorno del servidor. Si está en el bundle de JavaScript, es público.

- [ ] 08 **Dependencias actualizadas y auditadas**

  Ejecuta la auditoría de tu gestor de paquetes antes de publicar y repítela cada mes. La mayoría de ataques automatizados explotan fallos ya parcheados.

- [ ] 09 **Copias de seguridad probadas**

  Backup automático de ficheros y base de datos, guardado fuera del mismo servidor, y una restauración de prueba hecha al menos una vez. Un backup sin restaurar no es un backup.

- [ ] 10 **Permisos y accesos revisados**

  Mínimo privilegio: cada persona e integración con lo justo. Retira accesos de exempleados, colaboradores puntuales e integraciones antiguas.

- [ ] **11** **Errores que no cuentan de más**

  En producción, nada de trazas, rutas del servidor ni versiones de software en los mensajes de error. Registra el detalle en el log, no en pantalla.

- [ ] **12** **Ficheros expuestos por descuido**

  Comprueba que no son accesibles .env, .git, backups .zip, phpinfo ni ficheros de configuración. Es el primer sitio donde mira un escáner automático.

- [ ] **13** **Cookies, RGPD y aviso legal en regla**

  Banner que bloquea de verdad hasta el consentimiento, política de privacidad, aviso legal y base legal para cada dato que recoges.

- [ ] **14** **Monitorización y avisos activos**

  Alguien tiene que enterarse de que la web se ha caído o de que el certificado expira antes que el cliente. Monitorización de uptime y aviso por correo.

- [ ] **15** **Un plan por escrito para cuando pase algo**

  Quién decide desconectar, a quién se avisa, dónde está el backup y si hay obligación de notificar (RGPD, 72 horas). Pensarlo antes ahorra las horas que valen.

> **¿Te has quedado con dudas en algún punto?** En Studio Santole hacemos auditorías de seguridad y hardening de webs y APIs partiendo exactamente de esta checklist, adaptada a cada caso. Escríbenos a familiasantole@gmail.com o desde studiosantole.com/#contacto y te damos una segunda opinión sobre vuestra situación actual.