Checkliste: SEO & Sicherheit

1. Revisar los encabezados de seguridad

[ ] ¿X-Content-Type-Options está presente?
Establecer encabezado: X-Content-Type-Options: nosniff

[ ] ¿X-Frame-Options está configurado?
Recomendado: SAMEORIGIN

[ ] ¿Existe Content-Security-Policy?
Mínimo: default-src 'self'; permitir otras fuentes explícitamente

[ ] ¿Referrer-Policy activada?
Recomendado: strict-origin-when-cross-origin

[ ] ¿HSTS configurado?
Usar encabezado: Strict-Transport-Security con max-age e includeSubDomains

2. Asegurar contenido y recursos

[ ] ¿Todos los recursos se cargan vía HTTPS?
No insertar contenido HTTP en páginas HTTPS

[ ] ¿Contenido externo con Subresource Integrity?
Usar el atributo integrity para JS/CSS externos

[ ] ¿Enlaces HTTP internos o externos?
Sustituir por https:// siempre que sea posible

[ ] ¿Scripts de fuentes confiables?
Solo cargar scripts necesarios y verificados

[ ] ¿CSP limita las fuentes?
Definir fuentes confiables mediante Content-Security-Policy

3. Formularios y envío de datos seguros

[ ] ¿Los formularios solo están disponibles por HTTPS?
La página y el formulario deben usar HTTPS

[ ] ¿Hay advertencias del navegador?
Evitar contenido mixto o formularios inseguros

[ ] ¿No se envían datos sensibles en el referrer?
Establecer una Referrer-Policy adecuada

[ ] ¿Google reCAPTCHA está correctamente insertado?
Cargar vía HTTPS y cumplir con las reglas CSP

[ ] ¿Los servicios de formularios externos usan HTTPS?
Solo utilizar proveedores seguros con HTTPS

4. Estructura de enlaces segura

[ ] ¿Enlaces externos con target='_blank' están protegidos?
Usar siempre rel='noopener noreferrer'

[ ] ¿Redirecciones HTTP a HTTPS configuradas?
Configurar redirecciones 301 para todas las solicitudes HTTP

[ ] ¿Etiquetas canónicas usan HTTPS?
Las URLs canónicas deben ser siempre HTTPS

[ ] ¿Sitemap con URLs HTTPS?
Incluir solo enlaces HTTPS en el sitemap XML

[ ] ¿Enlaces con target='_blank' protegidos?
Evitar ataques reverse tabnabbing con rel='noopener' o 'noreferrer'