Checkliste: SEO & Sicherheit

1. Comprovar els encapçalaments de seguretat

[ ] X-Content-Type-Options present?
Estableix l'encapçalament: X-Content-Type-Options: nosniff

[ ] X-Frame-Options configurat?
Recomanat: SAMEORIGIN

[ ] Content-Security-Policy establerta?
Com a mínim: default-src 'self'; permet altres fonts explícitament

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

[ ] HSTS configurat?
Utilitza l'encapçalament: Strict-Transport-Security amb max-age i includeSubDomains

2. Assegurar contingut i recursos

[ ] Tots els recursos es carreguen amb HTTPS?
No incrustis contingut HTTP en pàgines HTTPS

[ ] Contingut extern amb Subresource Integrity?
Utilitza l'atribut integrity per JS/CSS externs

[ ] Hi ha enllaços HTTP interns o externs?
Substitueix-los per https:// sempre que sigui possible

[ ] Scripts de fonts fiables?
Només carrega scripts necessaris i verificats

[ ] CSP limita les fonts?
Defineix fonts de confiança mitjançant Content-Security-Policy

3. Formularis i enviament de dades segurs

[ ] Formularis només disponibles amb HTTPS?
La pàgina i l'acció del formulari han d'utilitzar HTTPS

[ ] Hi ha advertiments del navegador?
Evita contingut mixt o formularis insegurs

[ ] No s'envien dades sensibles al referrer?
Configura una Referrer-Policy adequada

[ ] Google reCAPTCHA està correctament inserit?
Carrega'l amb HTTPS i compleix amb les regles CSP

[ ] Serveis externs de formularis utilitzen HTTPS?
Només utilitza proveïdors segurs amb HTTPS

4. Estructura d'enllaços segura

[ ] Enllaços amb target='_blank' estan protegits?
Utilitza sempre rel='noopener noreferrer'

[ ] Redireccions de HTTP a HTTPS configurades?
Configura redireccions 301 per a totes les peticions HTTP

[ ] Etiquetes canòniques utilitzen HTTPS?
Les URLs canòniques han de ser sempre HTTPS

[ ] El sitemap utilitza URLs HTTPS?
Inclou només enllaços HTTPS al sitemap XML

[ ] Enllaços amb target='_blank' protegits?
Evita el reverse tabnabbing amb rel='noopener' o 'noreferrer'