



HOPPER TECH

ESTUDIO DIGITAL

CHECKLIST OPERATIVO

Checklist de lanzamiento web

47 controles para revisar SEO, rendimiento, seguridad, privacidad y accesibilidad antes de publicar.

QUE INCLUYE

47 CONTROLES | 5 ÁREAS

Registra conforme, pendiente o no aplica justificado, con evidencia, fecha y responsable. No hay un plazo universal. Esta lista no certifica seguridad ni conformidad WCAG. Antes de publicar se prepara el post-check; sólo después se verifica el sitio público.

USO LIBRE | DESCARGA DIRECTA | SIN REGISTRO

Material educativo. Adapta cada control al contexto y riesgo de tu organización.

Revisión editorial: 2026-09-08



OBJETIVO Y GOBERNANZA

- ☐ 01 El objetivo de negocio y la acción principal están escritos en una frase.
- ☐ 02 Existe una persona responsable de aprobar contenido, diseño y publicación.
- ☐ 03 Dominio, hosting, repositorio y cuentas pertenecen a la organización correcta.
- ☐ 04 Ambientes y proyectos de terceros permanecen separados.
- ☐ 05 Los datos de contacto, razón social y responsables están vigentes.
- ☐ 06 Alcance, exclusiones y criterios de aceptación están documentados.
- ☐ 07 Existe una copia recuperable del código y de los activos críticos.
- ☐ 08 El procedimiento de rollback o recuperación está definido.
- ☐ 09 La versión candidata se vincula con un commit y artefacto exactos; tras publicar se verifica esa relación.

SEO Y DESCUBRIMIENTO

- ☐ 01 Cada página indexable tiene title y description únicos y concisos.
- ☐ 02 El título principal y la jerarquía de encabezados explican el propósito de la página.
- ☐ 03 Canonical usa HTTPS, dominio oficial y ruta normalizada.
- ☐ 04 robots.txt orienta el rastreo, no protege información privada ni garantiza excluir una URL del índice. Lo privado requiere control de acceso. [1]
- ☐ 05 El sitemap incluye las URL canónicas públicas del alcance, sin datos privados. Enviarlos no garantiza indexación. [2]
- ☐ 06 Las fechas del sitemap representan cambios significativos reales, no cada ejecución del build. [2]
- ☐ 07 Open Graph incluye título, descripción, imagen y URL canónica.
- ☐ 08 Los enlaces internos son rastreables, descriptivos y no generan huérfanos.
- ☐ 09 La página 404 responde con estado correcto y conserva navegación útil.
- ☐ 10 Datos estructurados coinciden con el contenido visible.



RENDIMIENTO Y PWA

- ☐ 01 Imágenes tienen dimensiones, compresión adecuada y formato moderno.
- ☐ 02 El recurso visual principal no descarga una variante pesada innecesaria.
- ☐ 03 Las fuentes tienen estrategia de carga y alternativas probadas; no se presupone ausencia de bloqueo por autoalojarlas.
- ☐ 04 JavaScript cliente se limita a interacción que realmente lo necesita.
- ☐ 05 No existen scripts ni conexiones anticipadas de terceros innecesarias.
- ☐ 06 Laboratorio y campo se separan. LCP, INP y CLS reales se registran con muestra, período y alcance URL/origen; sin muestra: sin datos. [3]
- ☐ 07 El diseño no presenta desbordamiento horizontal en anchos críticos.
- ☐ 08 Service worker, manifest e iconos se verifican si existe PWA.
- ☐ 09 El artefacto cumple un presupuesto documentado de archivos y bytes.

SEGURIDAD Y PRIVACIDAD

Revisión técnica proporcional al alcance; una lista marcada no acredita una verificación completa de seguridad. [5]

- ☐ 01 HTTPS y redirecciones conservan ruta y consulta sin downgrade.
- ☐ 02 Headers de seguridad están definidos y probados.
- ☐ 03 CSP permite sólo orígenes necesarios y no incluye comodines amplios.
- ☐ 04 No hay credenciales privadas ni datos personales no autorizados en código, archivos o artefacto.
- ☐ 05 Dependencias tienen origen, integridad y licencias revisadas.
- ☐ 06 El backend o proveedor valida los datos. Cliente, errores y doble envío se prueban con datos ficticios y alcance autorizado.
- ☐ 07 Los envíos de datos personales tienen finalidad, destinatario y autorización documentados; no se amplían durante el diagnóstico.
- ☐ 08 Analítica y marketing esperan consentimiento cuando corresponde.
- ☐ 09 Enlaces externos con pestaña nueva usan protección de opener.
- ☐ 10 MFA y privilegios mínimos protegen cuentas administrativas; se revisa recuperación y MFA resistente a phishing cuando esté disponible. [6]



ACCESIBILIDAD Y CIERRE

Estas comprobaciones no sustituyen la evaluación de todos los criterios WCAG aplicables, páginas y procesos completos. [4]

- ☐ 01 Idioma, viewport y zoom están configurados sin bloquear ampliación.
- ☐ 02 Existe enlace para saltar al contenido y el foco es visible.
- ☐ 03 La jerarquía de encabezados no contiene saltos arbitrarios.
- ☐ 04 Imágenes informativas tienen alternativa y decorativas se ocultan correctamente.
- ☐ 05 Controles y enlaces tienen nombres accesibles y objetivos utilizables.
- ☐ 06 Toda acción principal funciona con teclado.
- ☐ 07 Formularios asocian etiquetas, instrucciones y errores.
- ☐ 08 Estados dinámicos se anuncian y permiten recuperación.
- ☐ 09 Pruebas previas, build y secretos tienen evidencia. Tras un deploy autorizado se ejecuta y registra el post-check, sin darlo por aprobado antes.

FUENTES Y REFERENCIAS

[1] Google - Límites de robots.txt:

<https://developers.google.com/search/docs/crawling-indexing/robots/intro>

[2] Google - Construir sitemaps:

<https://developers.google.com/search/docs/crawling-indexing/sitemaps/build-sitemap>

[3] Google - Campo y laboratorio en PSI:

<https://developers.google.com/speed/docs/insights/v5/about>

[4] W3C - WCAG 2.2 y conformidad: <https://www.w3.org/TR/WCAG22/>

[5] OWASP - Verificación de seguridad ASVS:

<https://owasp.org/www-project-application-security-verification-standard/>

[6] NIST - Autenticación multifactor:

<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/multi-factor-authentication>