

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nextcode.cl/	Checks	9 pruebas
Dominio	nextcode.cl	Hallazgos	43 totales
Fecha	8 de octubre de 2026 a las 15:51	Problemas	6 detectados

B

84/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad del dominio ha resultado en una puntuación exacta de 84/100 con una calificación final de grado B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 3 advertencias por configuraciones incompletas y 1 fallo en la disponibilidad de archivos de estructura. Aunque la base de cifrado es sólida, la ausencia de políticas de transporte estricto y la exposición de puertos no estándar representan riesgos potenciales. Se concluye que el sitio es generalmente seguro, pero se encuentra en un estado vulnerable ante ataques de interceptación de tráfico y reconocimiento de infraestructura.

Resumen de Riesgos

0 CRITICO	2 ALTO	1 MEDIO	3 BAJO	37 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 53 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 53 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
53 dias restantes (expira: 2026-11-30T15:48:53.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-01T14:49:09.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO Server header expuesto
Server: cloudflare — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: default-src 'none'; script-src 'nonce-DftzO7g6Pjq3nDKP8x9oUL' 'unsafe-eval' http...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: same-origin
- INFO

Permissions-Policy
Presente: accelerometer=(),camera=(),clipboard-read=(),clipboard-write=(),geolocation=(),g...

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://nextcode.cl/
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

Deteccion CMS — 100/100

Estado: OK

No se detecto un CMS conocido

- INFO

WordPress
No detectado
- INFO

Joomla
No detectado
- INFO

Drupal
No detectado
- INFO

Magento
No detectado
- INFO

Shopify
No detectado
- INFO

PrestaShop
No detectado
- INFO

Wix
No detectado
- INFO

Squarespace
No detectado
- INFO

Tecnologias detectadas
Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO

Archivo /readme.html
No accesible (correcto)
- INFO

Archivo /README.txt
No accesible (correcto)
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

INFO

Cookies detectadas

El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 100/100

Estado: OK

No se detecto contenido mixto

INFO

Contenido mixto

Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO

robots.txt

No encontrado (HTTP 403)
- BAJO

sitemap.xml

No encontrado (HTTP 403)
- BAJO

security.txt

No encontrado — Recomendado para política de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

- INFO

Puerto 21 (FTP)

Cerrado — Transferencia de archivos sin cifrar
- INFO

Puerto 22 (SSH)

Cerrado — Acceso remoto seguro
- INFO

Puerto 23 (Telnet)

Cerrado — Acceso remoto sin cifrar
- INFO

Puerto 25 (SMTP)

Cerrado — Envio de correo
- INFO

Puerto 80 (HTTP)

Abierto (esperado) — Servidor web
- INFO

Puerto 443 (HTTPS)

Abierto (esperado) — Servidor web seguro
- INFO

Puerto 3306 (MySQL)

Cerrado — Base de datos MySQL expuesta
- INFO

Puerto 3389 (RDP)

Cerrado — Escritorio remoto Windows
- INFO

Puerto 5432 (PostgreSQL)

Cerrado — Base de datos PostgreSQL expuesta
- INFO

Puerto 6379 (Redis)

Cerrado — Cache Redis sin autentificacion por defecto
- MEDIO

Puerto 8080 (HTTP-Alt)

ABIERTO — Servidor web alternativo / proxy
- INFO

Puerto 27017 (MongoDB)

Cerrado — Base de datos MongoDB expuesta

Analisis de Inteligencia Artificial

---RESUMEN EJECUTIVO---

El análisis de seguridad del dominio ha resultado en una puntuación exacta de 84/100 con una calificación final de grado B. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 5 resultados satisfactorios, 3 advertencias por configuraciones incompletas y 1 fallo en la disponibilidad de archivos de estructura. Aunque la base de cifrado es sólida, la ausencia de políticas de transporte estricto y la exposición de puertos no estándar representan riesgos potenciales. Se concluye que el sitio es generalmente seguro, pero se encuentra en un estado vulnerable ante ataques de interceptación de tráfico y reconocimiento de infraestructura.

---VULNERABILITIES---

[HIGH] Falta de Strict-Transport-Security: No se ha configurado la cabecera HSTS, lo que permite que las conexiones puedan ser degradadas a protocolos no seguros mediante ataques de intermediario.

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: La exposición de este puerto alternativo aumenta la superficie de ataque, pudiendo revelar servicios internos o interfaces de gestión no protegidas.

[LOW] Cabecera Server expuesta: El servidor revela el uso de tecnología Cloudflare, proporcionando información técnica valiosa para que un atacante dirija exploits específicos contra la infraestructura.

[LOW] Ausencia de robots.txt y sitemap.xml: El servidor devuelve un error 403 al intentar acceder a estos archivos, lo que indica una configuración de permisos deficiente o la falta de estos elementos esenciales para la auditoría y navegación legítima.