

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://buk.cl	Checks	9 pruebas
Dominio	buk.cl	Hallazgos	53 totales
Fecha	11 de septiembre de 2026 a las 09:15	Problemas	3 detectados

A

97/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web buk.cl arroja una puntuación de 97/100, lo que otorga una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, de los cuales 8 resultaron satisfactorios y 1 presentó advertencias menores, sin registrarse fallos críticos. El análisis destaca un excelente manejo del cifrado SSL/TLS y la correcta redirección de protocolos seguros. En conclusión, el sitio se considera altamente seguro, requiriendo únicamente ajustes menores en la configuración de cabeceras para alcanzar la excelencia técnica.

Resumen de Riesgos

0 CRITICO	0 ALTO	1 MEDIO	2 BAJO	50 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 98 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	2 cookies, todas con flags correctos
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 98 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
98 dias restantes (expira: 2026-12-17T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-06-03T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

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

- INFO **Content-Security-Policy**
Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
Presente: nosniff
- INFO **Referrer-Policy**
Presente: no-referrer-when-downgrade
- MEDIO **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
HTTP 301 redirige a https://buk.cl/
- INFO **HSTS (Strict-Transport-Security)**
HSTS activo: max-age=31536000; includeSubDomains
- BAJO **HSTS includeSubDomains**
HSTS cubre subdominios
- INFO **HSTS max-age**
max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
HTTPS responde con status 200

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
- BAJO **Meta generator**
Expone: HubSpot
- 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

2 cookies, todas con flags correctos

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- INFO

Cookie: __cf_bm — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: __cf_bm — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: __cf_bm — SameSite
SameSite=none
- INFO

Cookie: _cfuvid — HttpOnly
HttpOnly activo — No accesible via JavaScript
- INFO

Cookie: _cfuvid — Secure
Flag Secure activo — Solo se envia por HTTPS
- INFO

Cookie: _cfuvid — SameSite
SameSite=none

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO

robots.txt
Presente (843 bytes)
- INFO

Reglas robots.txt
14 Disallow, 7 Allow
- INFO

Sitemap en robots.txt
https://www.buk.cl/sitemap.xml
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
●	INFO	Puerto 8080 (HTTP-Alt) Cerrado — Servidor web alternativo / proxy
●	INFO	Puerto 27017 (MongoDB) Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[MEDIUM] Permissions-Policy: Falta esta cabecera de seguridad que permite restringir el acceso a APIs del navegador como la cámara, el micrófono o la geolocalización, lo cual es vital para la privacidad del usuario.

[LOW] Server header expuesto: El servidor revela el uso de Cloudflare, lo que permite a un atacante identificar la tecnología de intermediación utilizada en la infraestructura.

[LOW] Meta generator: El código fuente expone el uso de HubSpot, facilitando a terceros la identificación de la plataforma de gestión de contenidos empleada.