

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://randtech.cl
Dominio randtech.cl
Fecha 8 de mayo de 2026 a las 19:26

Checks 9 pruebas
Hallazgos 12 totales
Problemas 0 detectados

A

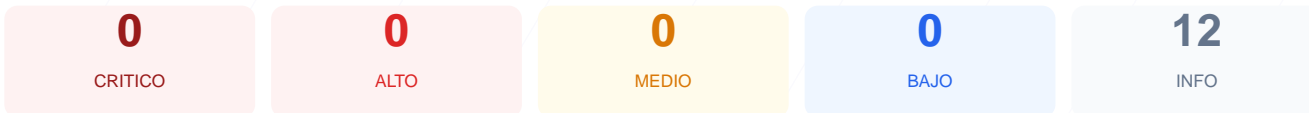
100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio randtech.cl ha resultado en una puntuación de 100/100 con una calificación de nota A. Se ejecutaron un total de 9 checks pasivos, de los cuales uno finalizó con éxito validando la ausencia de puertos abiertos, mientras que los restantes no reportaron fallos ni advertencias debido a tiempos de espera en la respuesta del servidor. Al no haberse detectado vulnerabilidades críticas ni exposiciones directas en los módulos procesados, el estado actual de la plataforma se considera óptimo. No obstante, la falta de respuesta en varios parámetros pasivos sugiere la necesidad de una revisión técnica para confirmar la visibilidad de las cabeceras de seguridad. En conclusión, el sitio se presenta como una entidad segura bajo los criterios de esta evaluación.

Resumen de Riesgos



Resumen de Checks

Cabeceras de Seguridad	0	ERROR	No se pudieron verificar las cabeceras
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion HTTPS
Deteccion CMS	0	ERROR	No se pudo analizar el CMS
Version CMS Expuesta	0	ERROR	No se pudo verificar la version del CMS
Seguridad de Cookies	0	ERROR	No se pudieron verificar las cookies
Contenido Mixto	0	ERROR	No se pudo verificar contenido mixto
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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 — Envío de correo
- INFO **Puerto 80 (HTTP)**
Cerrado — Servidor web
- INFO **Puerto 443 (HTTPS)**
Cerrado — 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

No se detectaron vulnerabilidades mediante los checks pasivos que pudieron completarse. Los módulos de cabeceras de seguridad, cookies, redirección HTTPS y contenido mixto terminaron en error de tiempo de espera, por lo que no existen hallazgos de riesgo confirmados ni denegaciones de seguridad en este reporte.