

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://cloud.2el.gob.sv
Dominio cloud.2el.gob.sv
Fecha 4 de octubre de 2026 a las 19:28

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

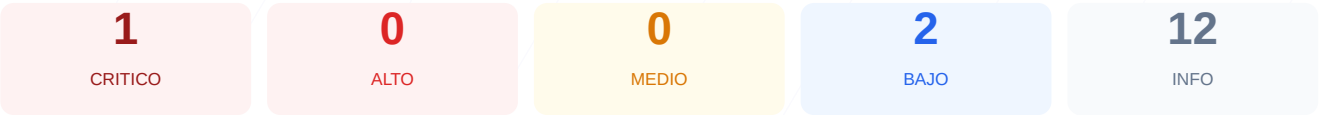
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio evaluado arrojó una puntuación de 73/100, lo que equivale a una nota de grado C. Durante la auditoría se ejecutaron un total de 9 checks pasivos, de los cuales 1 resultó satisfactorio, se registraron 0 advertencias y se identificó 1 fallo directo. Los resultados muestran múltiples errores técnicos que impidieron verificar elementos críticos como el cifrado SSL y las cabeceras de seguridad. Debido a la incapacidad de confirmar protecciones básicas y la presencia de fallos de configuración, el sitio se clasifica actualmente como vulnerable.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	0	ERROR	No se pudo verificar SSL/TLS
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
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO Conexion SSL
No se pudo establecer conexion SSL/TLS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
Error al acceder
- BAJO sitemap.xml
Error al acceder

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 autentificación 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

- [CRITICAL] Conexion SSL: No se pudo establecer una conexion SSL/TLS, lo que impide garantizar la integridad y privacidad de los datos transmitidos.
- [HIGH] Cabeceras de Seguridad: No se pudieron verificar las cabeceras, lo que sugiere una posible ausencia de directivas contra ataques XSS e inyecciones.
- [HIGH] Redireccion HTTPS: Error al verificar la redireccion automatica, lo que podria exponer a los usuarios a conexiones no cifradas.
- [MEDIUM] Seguridad de Cookies: Imposibilidad de verificar los atributos de seguridad en las cookies, aumentando el riesgo de robo de sesiones.
- [LOW] robots.txt y sitemap.xml: Error al acceder a estos archivos, lo cual afecta la correcta indexacion y el control de acceso para rastreadores.