

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://cloud.2.cel.gob.sv
Dominio cloud.2.cel.gob.sv
Fecha 4 de octubre de 2026 a las 19:29

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

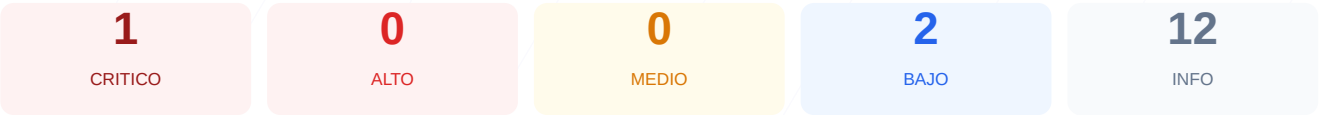
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio cloud.2.cel.gob.sv ha otorgado una puntuación de 73/100, resultando en una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 1 resultó exitoso y 1 se identificó como fallo directo, mientras que el resto presentó errores de conectividad que impidieron una validación completa. La imposibilidad de verificar el cifrado SSL y las cabeceras de seguridad fundamentales sugiere una configuración de servidor deficiente. En consecuencia, el sitio se considera vulnerable debido a que no cumple con los estándares mínimos de comunicación segura y protección de datos.

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 autenticación 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 conexión SSL/TLS, lo que impide el cifrado de la información y expone los datos de los usuarios a interceptaciones.

[CRITICAL] Cabeceras de Seguridad: Ausencia de verificación de políticas de seguridad HTTP, aumentando el riesgo de ataques de inyección y suplantación.

[HIGH] Seguridad de Cookies: No se pudo validar el uso de atributos de seguridad en cookies, lo que podría permitir el robo de sesiones.

[LOW] Ausencia de robots.txt: No se encontró el archivo de directivas para buscadores, lo que dificulta el control sobre el rastreo del sitio.

[LOW] Ausencia de sitemap.xml: El archivo de mapa del sitio no está disponible, afectando la indexación y visibilidad de la estructura web.