

Escanear Vulnerabilidades

Informe de Seguridad Web

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

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

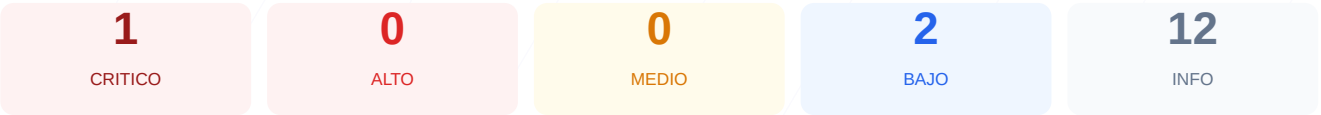
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web cloud.cel.gob.sv arroja una puntuación de 73/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo un resultado satisfactorio, un fallo directo y varios errores críticos de comunicación con el servidor. La imposibilidad de validar componentes fundamentales como el cifrado y las cabeceras de seguridad indica una configuración de servidor deficiente. Por lo tanto, se concluye que el sitio es actualmente vulnerable y presenta riesgos elevados para la integridad de los 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 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

[CRITICAL] Conexión SSL/TLS: No se pudo establecer una conexión segura, lo que impide el cifrado de la información entre el usuario y el servidor.

[CRITICAL] Cabeceras de Seguridad: Ausencia de verificación de headers esenciales, dejando la plataforma expuesta a ataques de interceptación y suplantación.

[CRITICAL] Redirección HTTPS: El servidor no fuerza el uso de protocolos seguros, permitiendo conexiones vulnerables a través de HTTP.

[CRITICAL] Seguridad de Cookies: No se pudo validar la presencia de atributos de seguridad en las cookies, facilitando el posible robo de sesiones.

[LOW] Robots.txt y Sitemap: El acceso a estos archivos falló o son inexistentes, dificultando la auditoría de rutas y la gestión de indexación.

[LOW] Contenido Mixto: Riesgo de carga de elementos no seguros dentro de la aplicación debido a la falta de una política de transporte estricta.