

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://dashboard.cel.gob.sv  
Dominio dashboard.cel.gob.sv  
Fecha 4 de octubre de 2026 a las 20:25

Checks 9 pruebas  
Hallazgos 15 totales  
Problemas 3 detectados

C

73/100

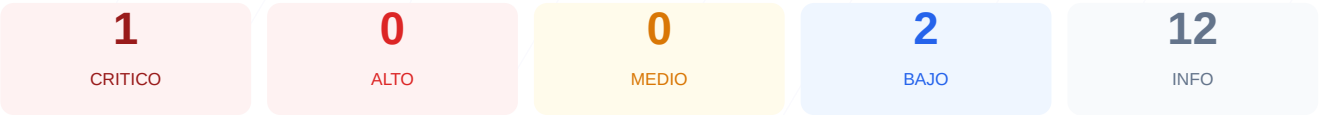
puntos de seguridad



## RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio dashboard.cel.gob.sv muestra una puntuación de 73/100, lo que equivale a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo uno resultó exitoso, detectándose fallos críticos en la infraestructura de cifrado y configuración de seguridad. Los resultados indican que el sistema no pudo validar la conexión SSL/TLS ni la presencia de cabeceras de protección esenciales. En conclusión, el sitio web se considera actualmente vulnerable debido a errores fundamentales en su configuración de red y seguridad.

## 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 | <b>Puerto 21 (FTP)</b><br>Cerrado — Transferencia de archivos sin cifrar          |
| ● | INFO | <b>Puerto 22 (SSH)</b><br>Cerrado — Acceso remoto seguro                          |
| ● | INFO | <b>Puerto 23 (Telnet)</b><br>Cerrado — Acceso remoto sin cifrar                   |
| ● | INFO | <b>Puerto 25 (SMTP)</b><br>Cerrado — Envío de correo                              |
| ● | INFO | <b>Puerto 80 (HTTP)</b><br>Cerrado — Servidor web                                 |
| ● | INFO | <b>Puerto 443 (HTTPS)</b><br>Cerrado — Servidor web seguro                        |
| ● | INFO | <b>Puerto 3306 (MySQL)</b><br>Cerrado — Base de datos MySQL expuesta              |
| ● | INFO | <b>Puerto 3389 (RDP)</b><br>Cerrado — Escritorio remoto Windows                   |
| ● | INFO | <b>Puerto 5432 (PostgreSQL)</b><br>Cerrado — Base de datos PostgreSQL expuesta    |
| ● | INFO | <b>Puerto 6379 (Redis)</b><br>Cerrado — Cache Redis sin autenticación por defecto |
| ● | INFO | <b>Puerto 8080 (HTTP-Alt)</b><br>Cerrado — Servidor web alternativo / proxy       |
| ● | INFO | <b>Puerto 27017 (MongoDB)</b><br>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 y permite la interceptación de datos por terceros.

[CRITICAL] Cabeceras de Seguridad: Ausencia total de políticas HTTP como HSTS o CSP, lo que facilita ataques de inyección, clickjacking y robo de información sensible.

[CRITICAL] Redirección HTTPS: El servidor no garantiza el tráfico cifrado de forma obligatoria, permitiendo accesos inseguros a través del protocolo HTTP.

[CRITICAL] Seguridad de Cookies: Imposibilidad de verificar atributos de protección en cookies de sesión, lo que aumenta el riesgo de secuestro de cuentas.

[MEDIUM] Detección de CMS y Versión: El sistema no permite identificar las tecnologías subyacentes, lo cual, aunque añade oscuridad, impide verificar si existen parches de seguridad pendientes.

[LOW] Archivos robots.txt y sitemap.xml: Los archivos no están accesibles o no existen, dificultando la gestión del rastreo y la visibilidad de la estructura del sitio.