

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://reclutamiento.cel.gob.sv
Dominio reclutamiento.cel.gob.sv
Fecha 4 de octubre de 2026 a las 19:30

Checks 9 pruebas
Hallazgos 15 totales
Problemas 3 detectados

C

73/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio ha arrojado una puntuación de 73/100, obteniendo una calificación de nota C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 1 verificación exitosa, 0 advertencias y 1 fallo crítico detectado. Los errores de conexión impidieron validar parámetros esenciales como el cifrado y las cabeceras de protección. Debido a la imposibilidad de confirmar una capa de transporte segura y la ausencia de archivos de configuración básicos, se concluye que el sitio es actualmente 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	2 puerto(s) abierto(s), todos esperados

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
2 puerto(s) abierto(s), todos esperados

●	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) Abierto (esperado) — Servidor web
●	INFO	Puerto 443 (HTTPS) Abierto (esperado) — 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 autenticacion 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

[CRITICO] Conexion SSL/TLS: No se pudo establecer una conexion segura, lo que indica que el trafico entre el usuario y el servidor podria no estar cifrado.

[CRITICO] Cabeceras de Seguridad: Error al verificar las cabeceras, lo que sugiere una posible exposicion a ataques de inyeccion y suplantacion de identidad.

[CRITICO] Redireccion HTTPS: No se pudo confirmar que el sitio fuerce el uso de protocolos seguros, permitiendo potencialmente conexiones vulnerables.

[BAJO] Archivo robots.txt: El servidor no permite el acceso a las instrucciones de rastreo, dificultando la gestion de motores de busqueda.

[BAJO] Archivo sitemap.xml: Ausencia de mapa del sitio, lo que afecta la organizacion de la informacion y la auditoria de contenidos.