

Escanear Vulnerabilidades

Informe de Seguridad Web

URL	https://www.cps.org.bo/	Checks	9 pruebas
Dominio	www.cps.org.bo	Hallazgos	18 totales
Fecha	10 de abril de 2026 a las 04:29	Problemas	3 detectados

F

37/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad técnica realizado al sitio web ha arrojado una puntuación de 37/100, lo que equivale a una nota F. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales solo 1 resultó exitoso, detectándose 2 fallos críticos y diversos errores de conectividad que impidieron validar parámetros esenciales. La ausencia de un certificado SSL válido y la incapacidad de verificar las cabeceras de seguridad exponen la plataforma a riesgos de interceptación de datos. Basándose en estos resultados, se concluye que el sitio es vulnerable y no cumple con los requisitos mínimos de seguridad para la navegación de usuarios.

Resumen de Riesgos

1 CRITICO	0 ALTO	0 MEDIO	2 BAJO	15 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	0	FALLO	Certificado SSL no valido
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: FALLO

Certificado SSL no valido

- CRITICO Certificado valido
El certificado SSL NO es valido
- INFO Dias hasta expiracion
172 dias restantes (expira: 2026-09-28T18:45:02.000Z)
- INFO Fecha de emision
Emitido desde: 2026-03-13T18:45:02.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO robots.txt
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] Certificado SSL no válido: El certificado SSL es inválido, lo que impide el cifrado de la comunicación y permite ataques de intermediario (Man-in-the-Middle).

[LOW] Ausencia de robots.txt: No se pudo acceder al archivo de directivas para buscadores, lo que puede causar una exposición no deseada de directorios.

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

[MEDIUM] Fallo en verificación de cabeceras: No se detectaron cabeceras de seguridad HTTP, dejando el sitio desprotegido contra ataques de inyección y clickjacking.

[MEDIUM] Error de redirección HTTPS: No se pudo confirmar que el sitio fuerce el uso de conexiones seguras, permitiendo el acceso por protocolos no cifrados.