EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.contraloria.gob.bo/	Checks	9 pruebas
Dominio	www.contraloria.gob.bo	Hallazgos	47 totales
Fecha	9 de abril de 2026 a las 19:42	Problemas	7 detectados

B

83/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al portal institucional ha arrojado una puntuación de 83/100, lo que equivale a una calificación de grado B. De los 9 controles pasivos ejecutados, 6 resultaron satisfactorios, 2 generaron advertencias y 1 fue clasificado como fallo de seguridad. Se han identificado riesgos relacionados con la exposición de versiones específicas del software y la ausencia de políticas de seguridad en las cabeceras HTTP. Aunque la base del cifrado y transporte de datos es robusta, la visibilidad de información técnica facilita las fases de reconocimiento para un atacante. En conclusión, el sitio es mayormente seguro, pero se considera vulnerable ante ataques dirigidos debido a fallos de configuración en el servidor y el CMS.

Resumen de Riesgos

0	2	2	3	40
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 303 dias
Cabeceras de Seguridad	75	AVISO	5/6 presentes. Faltan: Content-Security-Policy
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
Deteccion CMS	100	OK	CMS detectado: WordPress, PrestaShop
Version CMS Expuesta	20	FALLO	WordPress 6.7.1 expuesta, WordPress 2 expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	60	AVISO	1 recurso(s) HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 303 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  303 dias restantes (expira: 2027-02-06T15:52:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-05T15:52:34.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 75/100

Estado: AVISO

5/6 presentes. Faltan: Content-Security-Policy

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN, SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), fullscreen=(self)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.contraloria.gob.bo/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.7.1

Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.7.1 expuesta, WordPress 2 expuesta

- ALTO **WordPress version**
  Version 6.7.1 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS

- INFO **Archivo /README.txt**
  No accesible (correcto)

Seguridad de Cookies — 100/100

Estado: OK

No se encontraron cookies

- INFO **Cookies detectadas**
  El sitio no establece cookies en la respuesta inicial

Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://gmpg.org/xfn/11

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (87 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, ? URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — Envio 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

[HIGH] Content-Security-Policy: Falta esta cabecera, lo cual es peligroso porque permite la ejecución de ataques de inyección de código y XSS al no restringir las fuentes de contenido.
[HIGH] WordPress version: La versión 6.7.1 está expuesta públicamente, permitiendo a atacantes identificar y explotar CVEs conocidos para esta versión específica.
[MEDIUM] Archivo /readme.html: Este archivo es accesible de forma pública, lo que revela información técnica y detalles de la instalación del CMS que deben ser privados.
[MEDIUM] Recurso HTTP en página HTTPS: Se detectó contenido mixto a través del enlace http://gmpg.org/xfn/11, lo que debilita la integridad de la conexión cifrada.
[LOW] Server header expuesto: El servidor responde con Apache, revelando la tecnología subyacente y facilitando la búsqueda de exploits específicos para ese software.
[LOW] Meta generator: El código fuente expone la etiqueta WordPress 6.7.1, confirmando la tecnología y versión exacta utilizada.
[LOW] Ruta sensible en robots.txt: Se hace referencia al directorio admin, proporcionando pistas innecesarias sobre la ubicación de rutas administrativas a posibles atacantes.