EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://aisem.gob.bo	Checks	9 pruebas
Dominio	aisem.gob.bo	Hallazgos	48 totales
Fecha	23 de junio de 2026 a las 14:28	Problemas	10 detectados

B

85/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el portal institucional arroja una puntuación de 85/100, lo que equivale a una nota de B. Durante la auditoría se ejecutaron 9 comprobaciones pasivas, de las cuales 6 resultaron satisfactorias, 2 generaron advertencias y una fue clasificada como fallo. El sitio demuestra una implementación sólida en cuanto al cifrado de datos, pero presenta deficiencias en la configuración de políticas de seguridad del servidor y exposición de metadatos. Concluyo que el sitio es generalmente seguro, aunque vulnerable a ataques de reconocimiento y de intermediario debido a la falta de mecanismos de transporte estricto.

Resumen de Riesgos

0	2	3	5	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 227 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 227 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  227 dias restantes (expira: 2027-02-05T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-06T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.18.0 (Ubuntu) — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://aisem.gob.bo/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: Drupal, PrestaShop

- INFO **WordPress**
  No detectado
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- 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: Drupal 10 (https://www.drupal.org)
- INFO **Tecnologias detectadas**
  Next.js

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente

- INFO **Version CMS**
  No se detecta ninguna version expuesta

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 — 100/100

Estado: OK

No se detecto contenido mixto

- INFO **Contenido mixto**
  Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (2027 bytes)
- INFO **Reglas robots.txt**
  34 Disallow, 18 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "config" — Puede revelar rutas sensibles a atacantes
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 — Envio 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 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] HSTS (Strict-Transport-Security): La ausencia de esta cabecera impide que el servidor obligue al navegador a usar siempre conexiones HTTPS, permitiendo posibles ataques de degradación de protocolo.
[MEDIUM] Referrer-Policy: Al no estar configurada, el sitio no controla qué información de procedencia se comparte con dominios externos al navegar por enlaces.
[MEDIUM] Permissions-Policy: La falta de esta cabecera permite que el navegador acceda potencialmente a funciones del hardware o APIs sensibles sin restricciones definidas por el servidor.
[MEDIUM] Ruta /user/login: El panel de acceso administrativo es accesible de forma pública, lo que facilita intentos de intrusión mediante ataques de fuerza bruta.
[LOW] Server header expuesto: El servidor revela la versión exacta nginx/1.18.0 (Ubuntu), proporcionando información valiosa para que un atacante busque exploits específicos.
[LOW] Meta generator expuesto: La etiqueta meta revela el uso de Drupal 10, permitiendo identificar la tecnología base del sitio y sus posibles vectores conocidos.
[LOW] Rutas sensibles en robots.txt: Se referencian directorios como admin y config, lo que orienta a posibles atacantes sobre la estructura interna del sistema.
[LOW] sitemap.xml: No se encontró el archivo de mapa del sitio, lo que dificulta la indexación correcta y la auditoría de contenidos públicos.