

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://gabinete.gob.pa	Checks	9 pruebas
Dominio	gabinete.gob.pa	Hallazgos	51 totales
Fecha	7 de octubre de 2026 a las 01:35	Problemas	19 detectados

D

55/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 55/100, lo que corresponde a una calificación de grado D. Durante la evaluación se ejecutaron un total de 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 generó una advertencia y 3 fallaron críticamente. La ausencia total de cabeceras de seguridad y la falta de redirección forzada hacia protocolos seguros representan un riesgo elevado. Debido a estas deficiencias en la configuración del servidor y la gestión de sesiones, se concluye que el sitio es vulnerable. Es imperativo realizar ajustes técnicos inmediatos para elevar los estándares de protección y mitigar riesgos de interceptación de datos.

Resumen de Riesgos

0 CRITICO	8 ALTO	10 MEDIO	1 BAJO	32 INFO
--------------	-----------	-------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 68 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a HTTPS
Deteccion CMS	100	OK	No se detecto un CMS conocido
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	17	FALLO	visid_incap_520351: falta Secure; visid_incap_52...
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 68 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
68 dias restantes (expira: 2026-12-13T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-05-29T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO

X-Frame-Options

Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security

Falta — Fuerza conexiones HTTPS (HSTS)
- MEDIO

X-Content-Type-Options

Falta — Evita MIME-type sniffing
- MEDIO

Referrer-Policy

Falta — Controla la informacion de referer enviada
- MEDIO

Permissions-Policy

Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion

HTTP 200 — No redirige a HTTPS
- 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

No se detecto un CMS conocido

- INFO

WordPress

No detectado
- INFO

Joomla

No detectado
- INFO

Drupal

No detectado
- INFO

Magento

No detectado
- INFO

Shopify

No detectado
- INFO

PrestaShop

No detectado
- INFO

Wix

No detectado
- INFO

Squarespace

No detectado

Version CMS Expuesta — 100/100

Estado: OK

No se detecto version de CMS expuesta

- MEDIO

Archivo /readme.html

Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Archivo /README.txt

Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO

Ruta /wp-login.php

Panel de login accesible publicamente
- MEDIO

Ruta /administrator/

Panel de login accesible publicamente
- MEDIO

Ruta /user/login

Panel de login accesible publicamente
- INFO

Version CMS

No se detecta ninguna version expuesta

Seguridad de Cookies — 17/100

Estado: FALLO

visid_incap_520351: falta Secure; visid_incap_520351: falta SameSite; incap_ses_1018_520351: falta HttpOnly; incap_ses_1018_520351: falta Secure; incap_ses_1018_520351: falta SameSite

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)
- INFO

Cookie: visid_incap_520351 — HttpOnly
HttpOnly activo — No accesible via JavaScript
- ALTO

Cookie: visid_incap_520351 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: visid_incap_520351 — SameSite
Falta SameSite — Vulnerable a CSRF
- ALTO

Cookie: incap_ses_1018_520351 — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: incap_ses_1018_520351 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: incap_ses_1018_520351 — SameSite
Falta SameSite — Vulnerable a CSRF

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 (24 bytes)
- INFO

Reglas robots.txt
1 Disallow, 0 Allow
- BAJO

sitemap.xml
No encontrado (HTTP 404)
- INFO

security.txt
Presente en /.well-known/security.txt — Buena practica

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] Ausencia de Cabeceras de Seguridad: No se detectó ninguna de las 6 cabeceras principales, lo que facilita ataques de XSS, clickjacking e inyección de contenido.

[HIGH] Falta de Redirección HTTPS y HSTS: El sitio permite conexiones HTTP sin cifrar y no fuerza el uso de transporte seguro, exponiendo el tráfico a interceptaciones.

[HIGH] Cookies sin flag HttpOnly: La cookie incap_ses_1018_520351 es accesible mediante scripts, aumentando el riesgo de robo de sesión por ataques XSS.

[HIGH] Cookies sin flag Secure: Varias cookies de sesión se envían a través de conexiones no cifradas, lo que permite su captura en ataques de intermediario.

[MEDIUM] Cookies sin atributo SameSite: La falta de este atributo en las cookies visid_incap e incap_ses hace que el sitio sea susceptible a ataques de falsificación de solicitudes (CSRF).

[MEDIUM] Archivos Informativos Expuestos: Los archivos /readme.html y /README.txt son accesibles públicamente, pudiendo revelar información técnica sobre la infraestructura.

[MEDIUM] Paneles de Administración Expuestos: Se detectaron rutas de login como /wp-login.php, /administrator/ y /user/login abiertas al público, facilitando intentos de acceso no autorizado.

[LOW] Ausencia de Sitemap.xml: No se encontró el archivo de mapa del sitio, lo cual dificulta la indexación correcta y el análisis de la estructura por herramientas legítimas.