

EscanearVulnerabilidades

Informe de Seguridad Web

URL https://presidencia.gob.pa
Dominio presidencia.gob.pa
Fecha 7 de octubre de 2026 a las 01:36

Checks 9 pruebas
Hallazgos 45 totales
Problemas 15 detectados

D

56/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el dominio institucional arroja una puntuación de 56/100, lo que resulta en una calificación técnica de nota D. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo como resultado 4 verificaciones satisfactorias, 2 advertencias por configuraciones debilitadas y 3 fallos críticos en parámetros esenciales. Los hallazgos principales revelan una ausencia total de cabeceras de seguridad y una gestión de cookies que no cumple con los estándares mínimos de protección. Por lo tanto, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación de datos, suplantación de identidad y secuestro de sesiones. No se realizó un pentest activo, por lo que el riesgo real podría ser superior al detectado en esta fase preliminar.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	50	AVISO	Certificado expira en 5 días
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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_29617: falta Secure; visid_incap_296...
Contenido Mixto	100	OK	No se detecto 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 — 50/100

Estado: AVISO

Certificado expira en 5 días

- INFO Certificado valido
El certificado SSL es valido y de confianza
- ALTO Días hasta expiracion
5 días restantes (expira: 2026-10-11T19:22:44.000Z)
- INFO Fecha de emision
Emitido desde: 2025-09-09T19:22:45.000Z
- 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 — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO

HTTP !' HTTPS redireccion
HTTP 301 redirige a https://www.presidencia.gob.pa/
- 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
- INFO

Version CMS
No se detecta ninguna version expuesta

Seguridad de Cookies — 17/100

Estado: FALLO

visid_incap_29617: falta Secure; visid_incap_29617: falta SameSite; incap_ses_612_29617: falta HttpOnly; incap_ses_612_29617: falta Secure; incap_ses_612_29617: falta SameSite

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)

- INFO

Cookie: visid_incap_29617 — HttpOnly

HttpOnly activo — No accesible via JavaScript
- ALTO

Cookie: visid_incap_29617 — Secure

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

Cookie: visid_incap_29617 — SameSite

Falta SameSite — Vulnerable a CSRF
- ALTO

Cookie: incap_ses_612_29617 — HttpOnly

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

Cookie: incap_ses_612_29617 — Secure

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

Cookie: incap_ses_612_29617 — 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- 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] Certificado SSL/TLS con expiración inminente: El certificado expira en solo 5 días (2026-10-11), lo que provocará errores de conexión y pérdida de confianza del usuario.

[HIGH] Ausencia total de Cabeceras de Seguridad: El servidor no entrega ninguna de las 6 cabeceras básicas (CSP, X-Frame-Options, HSTS, etc.), facilitando ataques de XSS e inyección.

[HIGH] Inexistencia de Strict-Transport-Security (HSTS): No se fuerza el uso de HTTPS a nivel de navegador, permitiendo ataques de degradación de protocolo y robo de información.

[HIGH] Cookies de sesión sin flag HttpOnly: La cookie incap_ses_612_29617 es accesible mediante scripts, lo que permite el robo de sesiones a través de vulnerabilidades XSS.

[HIGH] Cookies de sesión sin flag Secure: Las cookies visid_incap y incap_ses se transmiten por canales no cifrados, exponiendo las credenciales de navegación en redes inseguras.

[MEDIUM] Falta de configuración SameSite en cookies: La ausencia de este atributo en todas las cookies detectadas hace que el sitio sea vulnerable a ataques de falsificación de peticiones (CSRF).

[MEDIUM] Exposición de archivos técnicos de infraestructura: Los archivos /readme.html y /README.txt son accesibles públicamente, pudiendo revelar información sensible sobre la plataforma.

[MEDIUM] Ausencia de X-Content-Type-Options: El servidor no previene el sniffing de tipos MIME, lo que podría permitir la ejecución de archivos maliciosos camuflados.

[MEDIUM] Falta de políticas de control (Referrer y Permissions): No se restringe la información de navegación compartida ni el acceso a periféricos del usuario desde el navegador.

[LOW] Inexistencia de archivos de control de rastreo: La falta de robots.txt y sitemap.xml indica una carencia en los estándares de organización y visibilidad web controlada.