EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.policianacional.gob.do/	Checks	9 pruebas
Dominio	www.policianacional.gob.do	Hallazgos	47 totales
Fecha	27 de mayo de 2026 a las 18:11	Problemas	19 detectados

D

51/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web policianacional.gob.do arroja una puntuación de 51/100, lo que equivale a una calificación de grado D. Durante el análisis se ejecutaron 9 checks pasivos, obteniendo 3 resultados satisfactorios, 2 advertencias y 4 fallos críticos en la configuración. Se han detectado deficiencias severas en la implementación de cabeceras de seguridad y una exposición peligrosa de servicios de infraestructura interna. Debido a la presencia de puertos críticos abiertos y la falta de políticas de protección de datos, el sitio web se considera actualmente vulnerable ante ataques externos.

Resumen de Riesgos

3	8	6	2	28
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	70	AVISO	Certificado expira en 25 dias
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_3294842: falta Secure; visid_incap_3...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 70/100

Estado: AVISO

Certificado expira en 25 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- MEDIO **Dias hasta expiracion**
  25 dias restantes (expira: 2026-06-21T07:04:19.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-23T07:04:56.000Z
- 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.policianacional.gob.do/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 403

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

- INFO **Archivo /readme.html**
  No accesible (correcto)
- INFO **Archivo /README.txt**
  No accesible (correcto)
- INFO **Version CMS**
  No se detecta ninguna version expuesta

Seguridad de Cookies — 17/100

Estado: FALLO

visid_incap_3294842: falta Secure; visid_incap_3294842: falta SameSite; incap_ses_690_3294842: falta HttpOnly; incap_ses_690_3294842: falta Secure; incap_ses_690_3294842: falta SameSite

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

- INFO **Cookie: visid_incap_3294842 — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- ALTO **Cookie: visid_incap_3294842 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: visid_incap_3294842 — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: incap_ses_690_3294842 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: incap_ses_690_3294842 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: incap_ses_690_3294842 — 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

- BAJO **robots.txt**
  No encontrado (HTTP 403)
- BAJO **sitemap.xml**
  No encontrado (HTTP 403)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO **Puerto 21 (FTP)**
  ABIERTO — 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
- CRITICO **Puerto 3306 (MySQL)**
  ABIERTO — Base de datos MySQL expuesta
- CRITICO **Puerto 3389 (RDP)**
  ABIERTO — Escritorio remoto Windows
- INFO **Puerto 5432 (PostgreSQL)**
  Cerrado — Base de datos PostgreSQL expuesta
- CRITICO **Puerto 6379 (Redis)**
  ABIERTO — Cache Redis sin autenticacion por defecto
- MEDIO **Puerto 8080 (HTTP-Alt)**
  ABIERTO — Servidor web alternativo / proxy
- INFO **Puerto 27017 (MongoDB)**
  Cerrado — Base de datos MongoDB expuesta

Analisis de Seguridad

VULNERABILIDADES DETECTADAS

[CRITICAL] Puerto 3306 (MySQL) ABIERTO: La base de datos principal está expuesta directamente a internet, permitiendo intentos de intrusión y ataques de fuerza bruta.
[CRITICAL] Puerto 3389 (RDP) ABIERTO: El protocolo de Escritorio Remoto de Windows es visible públicamente, lo que facilita ataques de toma de control del servidor.
[CRITICAL] Puerto 6379 (Redis) ABIERTO: El servicio de caché Redis se encuentra expuesto, pudiendo permitir la extracción de datos sensibles en memoria sin autenticación.
[HIGH] Cabeceras de Seguridad Faltantes: Ausencia total (0/6) de políticas como CSP, X-Frame-Options y HSTS, dejando el sitio vulnerable a ataques de XSS, Clickjacking y degradación de protocolo.
[HIGH] Puerto 21 (FTP) ABIERTO: Uso de un protocolo de transferencia de archivos no cifrado que permite la interceptación de credenciales en texto plano.
[HIGH] Seguridad de Cookies Deficiente: Las cookies de sesión carecen de los flags Secure y HttpOnly, lo que permite su robo mediante scripts maliciosos o intercepción de tráfico.
[HIGH] HSTS no configurado: El servidor no instruye a los navegadores para usar exclusivamente conexiones HTTPS, permitiendo posibles ataques de tipo Man-in-the-Middle.
[MEDIUM] Puerto 8080 (HTTP-Alt) ABIERTO: Un servidor web alternativo o proxy está expuesto, aumentando innecesariamente la superficie de ataque.
[MEDIUM] Vulnerabilidad CSRF en Cookies: La falta del atributo SameSite en las cookies de la plataforma permite que un atacante realice acciones no autorizadas en nombre del usuario.
[LOW] Fallo en robots.txt y sitemap.xml: El acceso a estos archivos devuelve un error 403, impidiendo una indexación correcta y controlada por parte de los buscadores.
[WARN] Expiración de Certificado SSL: El certificado de cifrado actual caduca en 25 días, lo que requiere una renovación inmediata para evitar alertas de seguridad a los usuarios.