

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://dgii.gov.do	Checks	9 pruebas
Dominio	dgii.gov.do	Hallazgos	41 totales
Fecha	25 de septiembre de 2026 a las 17:44	Problemas	10 detectados

C

61/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web arroja una puntuación de 61/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos que comprometen la integridad del portal. El sitio presenta deficiencias severas en la implementación de políticas de seguridad mediante cabeceras HTTP y en la gestión de redirecciones seguras. Debido a la ausencia de estos controles fundamentales contra ataques de inyección y suplantación, se concluye que el sitio es actualmente vulnerable.

Resumen de Riesgos

0 CRITICO	5 ALTO	3 MEDIO	2 BAJO	31 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 36 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	100	OK	No se encontraron cookies
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	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 36 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
36 dias restantes (expira: 2026-10-31T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-04-16T00:00:00.000Z
- 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 403 — No redirige a HTTPS
- 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 — 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 — 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 — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Falta de X-Frame-Options: El sitio no protege contra ataques de clickjacking, permitiendo que la interfaz sea embebida en marcos externos no autorizados.

[HIGH] Falta de Strict-Transport-Security: No se obliga al navegador a utilizar exclusivamente conexiones cifradas, facilitando ataques de interceptación de datos.

[HIGH] Fallo en Redirección HTTPS: El servidor no redirige el tráfico HTTP hacia HTTPS, devolviendo un error 403 y dejando el canal de comunicación expuesto.

[MEDIUM] Falta de X-Content-Type-Options: La falta de esta cabecera permite que los navegadores ignoren el tipo de contenido declarado, aumentando el riesgo de ejecución de archivos maliciosos.

[MEDIUM] Falta de Referrer-Policy: No existe un control sobre la información de navegación que se comparte con terceros al seguir enlaces externos.

[MEDIUM] Falta de Permissions-Policy: El portal no restringe el acceso de las APIs del navegador a funciones sensibles como la cámara, el micrófono o la ubicación.

[LOW] Ausencia de robots.txt: No se han definido reglas de acceso para rastreadores, lo que genera errores de acceso 403 y dificulta la auditoría de indexación.

[LOW] Ausencia de sitemap.xml: El servidor bloquea el acceso al mapa del sitio, impidiendo una correcta visibilidad de la estructura jerárquica del portal.