

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://elespejogotico.blogspot.com
Dominio elespejogotico.blogspot.com
Fecha 9 de mayo de 2026 a las 19:20

Checks 9 pruebas
Hallazgos 47 totales
Problemas 12 detectados

C

60/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada sobre el sitio web arroja una puntuación de 60/100, lo que resulta en una nota de calificación C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos en la configuración de seguridad. Se han detectado deficiencias severas en la implementación de cabeceras de protección y en la gestión del tráfico cifrado. Debido a la falta de redirecciones automáticas a HTTPS y la presencia masiva de contenido mixto, el sitio se considera vulnerable a ataques de interceptación y manipulación de datos.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 65 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 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	20	FALLO	127 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 65 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
65 dias restantes (expira: 2026-07-13T08:36:19.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-04-20T08:36:20.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
Server: GSE — Revela tecnologia del servidor

- **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)
- **INFO** **X-Content-Type-Options**
Presente: nosniiff
- **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
- **INFO** **Tecnologias detectadas**
Astro

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 — 20/100

Estado: FALLO

127 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://elespejogotico.blogspot.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://elespejogotico.blogspot.com/2007/11/poesia-gotica-poe...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
http://elespejogotico.blogspot.com/2009/07/clark-ashton-smit...
- MEDIO **href (link/stylesheet)**
...y 124 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
Presente (169 bytes)
- INFO **Reglas robots.txt**
3 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
https://elespejogotico.blogspot.com/sitemap.xml
- BAJO **security.txt**
No encontrado — Recomendado para política 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 autentificacion 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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques de Cross-Site Scripting (XSS) e inyección de contenido malicioso.

[HIGH] X-Frame-Options: Al no estar configurada, el sitio es susceptible a ataques de clickjacking, permitiendo que atacantes carguen la web en marcos invisibles.

[HIGH] Strict-Transport-Security: La falta de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de protocolo (SSL Stripping).

[HIGH] Redirección HTTP a HTTPS: El servidor no redirige automáticamente a los usuarios hacia la versión segura, exponiendo el tráfico a escuchas no autorizadas.

[MEDIUM] Contenido Mixto: Se identificaron 127 recursos cargados mediante HTTP dentro de la página HTTPS, lo que anula la integridad del cifrado SSL.

[MEDIUM] Referrer-Policy: No se define cómo se comparte la información de procedencia con otros dominios, lo que podría filtrar datos de navegación privada.

[MEDIUM] Permissions-Policy: La falta de esta política permite el acceso potencial de scripts a APIs del navegador como la cámara, el micrófono o la geolocalización.

[LOW] Server header expuesto: El encabezado revela el uso de tecnología GSE, proporcionando información técnica específica que ayuda a un atacante en la fase de reconocimiento.