# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://google.es | Checks | 9 pruebas |
| Dominio | google.es | Hallazgos | 53 totales |
| Fecha | 15 de julio de 2026 a las 07:27 | Problemas | 9 detectados |

C

67/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el dominio google.es ha arrojado una puntuación de 67/100, lo que equivale a una nota de C. De los 9 checks pasivos ejecutados, 6 resultaron satisfactorios, 1 presentó advertencias y 2 finalizaron con errores críticos. El análisis revela deficiencias importantes en la configuración de cabeceras de seguridad y en los protocolos de redirección de tráfico. Debido a la ausencia de políticas de seguridad modernas y la gestión mejorable de sesiones, se concluye que el sitio es actualmente vulnerable a ataques de intermediario e inyección.

## Resumen de Riesgos

| 0 | 5 | 3 | 1 | 44 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 68 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 | 89 | AVISO | SOCS: falta HttpOnly |
| Contenido Mixto | 100 | OK | No se detecto contenido mixto |
| 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 68 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  68 dias restantes (expira: 2026-09-21T08:41:15.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-29T08:41:16.000Z
- 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, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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 301 — 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**
  Next.js

## 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 — 89/100

Estado: AVISO

SOCS: falta HttpOnly

- INFO **Cookies detectadas**
  3 cookie(s) encontrada(s)
- ALTO **Cookie: SOCS — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: SOCS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: SOCS — SameSite**
  SameSite=lax
- INFO **Cookie: AEC — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: AEC — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: AEC — SameSite**
  SameSite=lax
- INFO **Cookie: __Secure-ENID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: __Secure-ENID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: __Secure-ENID — SameSite**
  SameSite=lax

## 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (6607 bytes)
- INFO **Reglas robots.txt**
  177 Disallow, 67 Allow
- INFO **Sitemap en robots.txt**
  https://www.google.com/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

## 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] Content-Security-Policy: Falta esta cabecera esencial que previene ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Strict-Transport-Security: La ausencia de HSTS impide que el navegador fuerce conexiones seguras, facilitando ataques de degradación de SSL.
[HIGH] Redirección HTTPS: El servidor no redirige automáticamente el tráfico HTTP a HTTPS, permitiendo la transmisión de datos en canales no cifrados.
[HIGH] Cookie SOCS sin flag HttpOnly: El atributo de seguridad falta en esta cookie, permitiendo que sea accesible mediante scripts y aumentando el riesgo de robo de sesión.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite el MIME-type sniffing, lo que puede llevar a la ejecución de archivos maliciosos disfrazados.
[MEDIUM] Referrer-Policy: No existe una política definida, lo que provoca la exposición involuntaria de información de navegación a terceros dominios.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, dejando expuestas funciones sensibles como la cámara o el micrófono ante posibles scripts.
[LOW] Server header expuesto: La cabecera revela el valor "gws", proporcionando a atacantes potenciales pistas sobre la tecnología del servidor.