# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://csc.gov.co | Checks | 9 pruebas |
| Dominio | csc.gov.co | Hallazgos | 47 totales |
| Fecha | 25 de marzo de 2026 a las 16:24 | Problemas | 16 detectados |

**D**

59/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al dominio arroja una puntuación de 59/100, lo que corresponde a una calificación de grado D. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 4 verificaciones exitosas, 2 advertencias y 2 fallos críticos, además de un error por tiempo de espera. El sitio presenta deficiencias significativas en la configuración de cabeceras de seguridad y una exposición de servicios que aumentan la superficie de ataque. Debido a la presencia de contenido mixto y puertos de transferencia de datos inseguros, se concluye que el sitio es actualmente vulnerable.

## Resumen de Riesgos

| 0 | 5 | 7 | 4 | 31 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 222 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 | CMS detectado: WordPress, PrestaShop |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 20 | FALLO | 4 recursos HTTP en pagina HTTPS |
| Robots.txt y Sitemap | 100 | OK | robots.txt y sitemap.xml presentes |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 21 (FTP) |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 222 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  222 dias restantes (expira: 2026-11-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-10-02T00:00:00.000Z
- 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

- BAJO **Server header expuesto**
  Server: Apache — Revela tecnologia del servidor
- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.2.30 — Revela framework/lenguaje

- 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://csc.gov.co/
- 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

CMS detectado: WordPress, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  No detectado
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, Astro, PHP/8.2.30

## 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

4 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://152.200.185.98:8081/login
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://152.200.185.98:8081/login
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://csc.gov.co/wp-content/uploads/2018/11/solicitud_de_cu...
- MEDIO **href (link/stylesheet)**
  ...y 1 mas del mismo tipo

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (111 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 1 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://csc.gov.co/wp-sitemap.xml
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 21 (FTP)

- 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
- 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] Puerto 21 (FTP) Abierto: El servicio de transferencia de archivos está accesible, lo cual es peligroso porque transmite datos y credenciales sin cifrar.
[HIGH] Ausencia de Content-Security-Policy: No se restringen las fuentes de contenido, lo que facilita ataques de inyección de código y scripts maliciosos (XSS).

[HIGH] Ausencia de X-Frame-Options: La falta de esta cabecera permite que el sitio sea cargado en marcos externos, habilitando ataques de clickjacking.
[HIGH] Falta de Strict-Transport-Security: El servidor no obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradación de protocolo (Man-in-the-Middle).
[MEDIUM] Contenido Mixto Detectado: Se identificaron 4 recursos que cargan mediante HTTP en una página segura, comprometiendo la integridad de la comunicación.
[MEDIUM] Ausencia de X-Content-Type-Options: Permite que el navegador interprete archivos de forma incorrecta, facilitando la ejecución de malware encubierto.
[MEDIUM] Referrer-Policy y Permissions-Policy no configurados: Se carece de control sobre la información de navegación compartida y el acceso a funciones del navegador del usuario.
[LOW] Exposición de Versiones Tecnológicas: Las cabeceras revelan el uso de Apache, PHP 8.2.30 y WordPress 6.9.4, facilitando la búsqueda de exploits específicos.
[LOW] Rutas Sensibles en Robots.txt: El archivo de indexación hace referencia a directorios de administración, revelando áreas críticas a atacantes potenciales.