# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://cartagena.salesianos.edu | Checks | 9 pruebas |
| Dominio | cartagena.salesianos.edu | Hallazgos | 50 totales |
| Fecha | 17 de mayo de 2026 a las 11:56 | Problemas | 17 detectados |

**D**

56/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada al sitio web muestra una puntuación de 56/100, otorgando una calificación de nota D. Durante el proceso se ejecutaron 9 checks pasivos que resultaron en 4 validaciones correctas, 2 advertencias y 3 fallos críticos en la configuración. A pesar de contar con un cifrado SSL robusto, la ausencia total de cabeceras de seguridad y la exposición de servicios antiguos representan un riesgo elevado. Se han detectado fallos en la gestión de contenido mixto y una versión de CMS desactualizada. Por todo ello, se concluye que el sitio es actualmente vulnerable ante ataques de interceptación y explotación de software conocido.

## Resumen de Riesgos

| 0 | 6 | 8 | 3 | 33 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 78 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 |
| Version CMS Expuesta | 20 | FALLO | WordPress 6.9.4 expuesta |
| Seguridad de Cookies | 100 | OK | No se encontraron cookies |
| Contenido Mixto | 20 | FALLO | 5 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 78 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  78 dias restantes (expira: 2026-08-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-07-21T00:00:00.000Z
- 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: nginx — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/8.3.28, PleskLin — 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://cartagena.salesianos.edu/
- 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

- INFO **WordPress**
  Detectado via HTML body
- 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
- BAJO **Meta generator**
  Expone: WordPress 6.9.4
- INFO **Tecnologias detectadas**
  Next.js, PHP/8.3.28, PleskLin

## Version CMS Expuesta — 20/100

Estado: FALLO

WordPress 6.9.4 expuesta

- ALTO **WordPress version**
  Version 6.9.4 expuesta publicamente — Permite a atacantes buscar CVEs conocidos
- INFO **Archivo /readme.html**
  No accesible (correcto)

- INFO **Archivo /README.txt**
  No accesible (correcto)

## 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

5 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qualitasescuelafamilia.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qualitaseducativa.com/
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://qualitaseducativa.com/
- MEDIO **href (link/stylesheet)**
  ...y 2 mas del mismo tipo

## Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (3076 bytes)
- INFO **Reglas robots.txt**
  82 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- INFO **sitemap.xml**
  Presente, ? URLs
- 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] WordPress version: Version 6.9.4 expuesta publicamente que permite a atacantes buscar CVEs conocidos.
[HIGH] Puerto 21 (FTP): El puerto se encuentra abierto permitiendo la transferencia de archivos sin cifrar.
[HIGH] Content-Security-Policy: Falta esta cabecera indispensable para prevenir ataques XSS e inyeccion de contenido.
[HIGH] X-Frame-Options: Falta de proteccion contra ataques de clickjacking.
[HIGH] Strict-Transport-Security: HSTS no configurado, impidiendo que el navegador fuerce conexiones HTTPS.
[MEDIUM] Contenido Mixto: Se identificaron 5 recursos HTTP cargando en una pagina HTTPS, rompiendo la cadena de confianza.
[MEDIUM] X-Content-Type-Options: Falta de cabecera para evitar que el navegador realice MIME-type sniffing.
[MEDIUM] Referrer-Policy: Falta de control sobre la informacion de procedencia enviada a terceros.
[MEDIUM] Permissions-Policy: No se restringen APIs del navegador como camara o microfono mediante cabeceras.
[MEDIUM] Bloqueo total: El archivo robots.txt bloquea todo el sitio con la instruccion Disallow: /, afectando al SEO.
[LOW] Server header expuesto: Revela que el servidor utiliza tecnologia nginx.
[LOW] X-Powered-By expuesto: Revela el uso de PHP/8.3.28 y PleskLin.
[LOW] Meta generator: Expone publicamente el uso de WordPress 6.9.4.