# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://www.usco.edu.co/es/ingreso/ | Checks | 9 pruebas |
| Dominio | www.usco.edu.co | Hallazgos | 56 totales |
| Fecha | 9 de mayo de 2026 a las 06:46 | Problemas | 17 detectados |

C

74/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web obtuvo una puntuación exacta de 74/100, lo que equivale a una nota de C. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 1 presentó advertencias y 3 fueron fallidos. Aunque el sitio cuenta con un cifrado de conexión robusto, se han detectado deficiencias críticas en la gestión de sesiones y en las cabeceras de protección del navegador. En su estado actual, el sitio se considera vulnerable ante ataques de interceptación de sesiones e inyección de código.

## Resumen de Riesgos

| 0 | 7 | 8 | 2 | 39 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 312 dias |
| Cabeceras de Seguridad | 50 | FALLO | Solo 3/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 100 | OK | HTTP redirige a HTTPS y HSTS esta habilitado |
| 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 | 17 | FALLO | JSESSIONID: falta HttpOnly; JSESSIONID: falta Se... |
| Contenido Mixto | 60 | AVISO | 1 recurso(s) HTTP en pagina HTTPS |
| 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 312 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  312 dias restantes (expira: 2027-03-16T20:27:14.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-12T20:27:15.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 50/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Content-Security-Policy, Referrer-Policy, Permissions-Policy

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000 ; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 302 redirige a https://www.usco.edu.co/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000 ; includeSubDomains
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 dias)
- 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

## 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)
- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version expuesta

## Seguridad de Cookies — 17/100

Estado: FALLO

JSESSIONID: falta HttpOnly; JSESSIONID: falta Secure; JSESSIONID: falta SameSite; f5avraaaaaaaaaaaaaaa_session_: falta SameSite; TS01e5638e: falta HttpOnly; TS01e5638e: falta Secure; TS01e5638e: falta SameSite; TS01e5638e026: falta HttpOnly; TS01e5638e026: falta Secure; TS01e5638e026: falta SameSite

- INFO **Cookies detectadas**
  4 cookie(s) encontrada(s)
- ALTO **Cookie: JSESSIONID — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: JSESSIONID — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: JSESSIONID — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: f5avraaaaaaaaaaaaaaa_session_ — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: f5avraaaaaaaaaaaaaaa_session_ — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: f5avraaaaaaaaaaaaaaa_session_ — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01e5638e — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01e5638e — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01e5638e — SameSite**
  Falta SameSite — Vulnerable a CSRF
- ALTO **Cookie: TS01e5638e026 — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: TS01e5638e026 — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: TS01e5638e026 — SameSite**
  Falta SameSite — Vulnerable a CSRF

## Contenido Mixto — 60/100

Estado: AVISO

1 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.urnadecristal.gov.co/

## Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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] Content-Security-Policy: Falta esta cabecera, lo que facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido malicioso.
[HIGH] Cookies sin flag HttpOnly: Las cookies JSESSIONID y TS01e5638e son accesibles vía scripts, permitiendo el robo de sesiones en caso de un ataque XSS.
[HIGH] Cookies sin flag Secure: Varias cookies de sesión se envían a través de conexiones no cifradas, permitiendo su captura por terceros en la red.
[MEDIUM] Cookies sin flag SameSite: La ausencia de este atributo en los identificadores de sesión hace que el sitio sea susceptible a ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Ruta /administrator/ expuesta: El panel de administración es accesible de forma pública, aumentando el riesgo de ataques de fuerza bruta o acceso no autorizado.
[MEDIUM] Contenido Mixto: Se detectó un recurso vinculado mediante HTTP (http://www.urnadecristal.gov.co/), lo que degrada la seguridad de la conexión HTTPS.
[MEDIUM] Ausencia de Referrer-Policy y Permissions-Policy: Falta de control sobre la información de procedencia enviada y sobre el acceso a funciones del navegador como cámara o micro.
[LOW] Ausencia de archivos de indexación: No se encontraron los archivos robots.txt ni sitemap.xml, lo que afecta la visibilidad y el control de rastreo por motores de búsqueda.