

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://comfacor.com.co/	Checks	9 pruebas
Dominio	comfacor.com.co	Hallazgos	42 totales
Fecha	29 de septiembre de 2026 a las 22:16	Problemas	10 detectados

C

62/100

puntos de seguridad



RESUMEN EJECUTIVO

La auditoria de seguridad realizada al sitio comfacor.com.co ha resultado en una puntuacion de 62/100, lo que equivale a una nota C. El analisis se baso en 9 checks pasivos, de los cuales 5 fueron exitosos, se emitio 1 advertencia y se identificaron 3 fallos criticos en la configuracion. Se han detectado debilidades importantes en la implementacion de cabeceras de seguridad y en la gestion de protocolos de cifrado. Debido a estos hallazgos y a la falta de redirecciones seguras, el sitio se considera vulnerable a ataques de interceptacion de datos y ejecucion de scripts maliciosos.

Resumen de Riesgos

0 CRITICO	4 ALTO	3 MEDIO	3 BAJO	32 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 88 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 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	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 88 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
88 dias restantes (expira: 2026-12-27T06:18:10.000Z)
- INFO Fecha de emision
Emitido desde: 2026-09-28T05:19:43.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO Server header expuesto
Server: cloudflare — 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
- INFO

Referrer-Policy
Presente: same-origin
- 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 403 — No redirige a HTTPS
- ALTO

HSTS (Strict-Transport-Security)
HSTS no configurado — El navegador no fuerza HTTPS
- INFO

Respuesta HTTPS
HTTPS responde con status 403

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)
- 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 — 100/100

Estado: OK

No se detecto contenido mixto

● INFO **Contenido mixto**
Todos los recursos se cargan por HTTPS

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

● BAJO **robots.txt**
No encontrado (HTTP 403)

● BAJO **sitemap.xml**
No encontrado (HTTP 403)

● BAJO **security.txt**
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 8080 (HTTP-Alt)

● 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

● MEDIO **Puerto 8080 (HTTP-Alt)**
ABIERTO — 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 facilita ataques de Cross-Site Scripting (XSS) y la inyeccion de contenido no autorizado en el navegador del usuario.

[HIGH] Strict-Transport-Security: Al no estar configurado HSTS, el sitio no obliga al navegador a usar conexiones HTTPS, permitiendo ataques de degradacion de protocolo.

[HIGH] Redireccion HTTP a HTTPS: El sistema responde con un error 403 y no redirige automaticamente el trafico inseguro hacia el protocolo cifrado, exponiendo la navegacion.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador intente adivinar el tipo de contenido (MIME-sniffing), lo que puede derivar en la ejecucion de archivos maliciosos disfrazados.

[MEDIUM] Permissions-Policy: No se han definido restricciones para el uso de APIs sensibles como la camara o el microfono, aumentando el riesgo de abuso de funciones del navegador.

[MEDIUM] Puerto 8080 (HTTP-Alt): Este puerto se encuentra abierto y suele utilizarse para servicios secundarios o de administracion, lo que incrementa la superficie de ataque.

[LOW] Server header expuesto: Se revela el uso de Cloudflare como servidor, informacion que ayuda a posibles atacantes a perfilar la infraestructura tecnologica.

[LOW] Ausencia de robots.txt y sitemap.xml: No se encontraron estos archivos de gestion, devolviendo un error 403, lo cual afecta la transparencia de la estructura del sitio ante auditorias externas.