

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://cms.ceos.digital  
Dominio cms.ceos.digital  
Fecha 12 de mayo de 2026 a las 13:43

Checks 9 pruebas  
Hallazgos 43 totales  
Problemas 4 detectados

# A

## 96/100

puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web arroja una puntuación de 96/100 y una nota final de A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 7 resultaron satisfactorios, se registro 1 advertencia y 0 fallos críticos. Los resultados demuestran una configuración de seguridad sólida y un manejo adecuado del cifrado de datos. Se concluye que el sitio es seguro para su uso operativo, aunque requiere ajustes menores en las cabeceras de respuesta para alcanzar un nivel de protección óptimo.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: X-Frame-Options
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

### SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 79 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
79 dias restantes (expira: 2026-07-31T01:02:14.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-05-02T01:02:15.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: X-Frame-Options

- BAJO **Server header expuesto**  
Server: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**  
X-Powered-By: ASP.NET — Revela framework/lenguaje
- **INFO** **Content-Security-Policy**  
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' 'unsa...
- **ALTO** **X-Frame-Options**  
Falta — Protege contra clickjacking
- **INFO** **Strict-Transport-Security**  
Presente: max-age=31536000; includeSubDomains; preload
- **INFO** **X-Content-Type-Options**  
Presente: nosniff
- **INFO** **Referrer-Policy**  
Presente: strict-origin-when-cross-origin
- **INFO** **Permissions-Policy**  
Presente: geolocation=(), microphone=(), camera=(), payment=()

## 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**  
Astro, ASP.NET

## 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**  
Presente (193 bytes)
- INFO **Reglas robots.txt**  
1 Disallow, 1 Allow
- MEDIO **Bloqueo total**  
robots.txt bloquea todo el sitio con Disallow: /
- INFO **Sitemap en robots.txt**  
https://www.seusite.com/sitemap.xml
- BAJO **security.txt**  
No encontrado — Recomendado para politica de divulgacion

## Puertos Abiertos — 100/100

Estado: OK

1 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)**  
Cerrado — 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] X-Frame-Options: Esta cabecera de seguridad no se encuentra presente, lo que permite que el sitio sea cargado dentro de un iframe y facilita ataques de Clickjacking.

[MEDIUM] Bloqueo total en robots.txt: El archivo robots.txt utiliza la directiva Disallow: / para todo el sitio, lo cual puede interferir con la visibilidad o indicar una configuracion de desarrollo expuesta.

[LOW] Server header expuesto: El servidor responde con la cabecera Microsoft-IIS/10.0, revelando informacion tecnica que permite a un atacante identificar posibles exploits especificos para esa version.

[LOW] X-Powered-By expuesto: Se detecto la cabecera X-Powered-By: ASP.NET, lo que revela el framework de desarrollo utilizado y facilita la etapa de reconocimiento de una intrusion.