

# Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://erp.ceos.digital  
Dominio erp.ceos.digital  
Fecha 12 de mayo de 2026 a las 13:32

Checks 9 pruebas  
Hallazgos 43 totales  
Problemas 3 detectados

# A

## 100/100

puntos de seguridad

### RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre la plataforma arroja una puntuación perfecta de 100/100 con una calificación final de nota A. Se ejecutaron un total de 9 checks pasivos, obteniendo 8 resultados satisfactorios y 0 fallos críticos detectados durante la inspección. A pesar de que no se realizó un pentest activo para evaluar la lógica interna de la aplicación, las defensas perimetrales y de red se encuentran en un estado óptimo. Se concluye que el sitio es seguro y sigue las mejores prácticas de configuración web actuales.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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: 2026-07-31T00:01:39.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-05-02T00:01:40.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 100/100

Estado: OK

Todas las cabeceras de seguridad presentes

- 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...
- **INFO** **X-Frame-Options**  
Presente: DENY
- **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 — Envío 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

- [LOW] Server header expuesto: El servidor revela el uso de Microsoft-IIS/10.0, lo cual facilita a un atacante potencial la búsqueda de vulnerabilidades específicas para esa versión.
- [LOW] X-Powered-By expuesto: La cabecera indica que el sitio utiliza el framework ASP.NET, proporcionando información técnica innecesaria sobre el entorno de ejecución.
- [MEDIUM] Bloqueo total en robots.txt: El archivo bloquea la indexación de todo el contenido mediante la directiva Disallow: /, lo que podría ocultar accidentalmente rutas que deberían ser públicas o ser un indicio de falta de configuración selectiva.
- [LOW] Redirección HTTPS no verificada: Aunque el sitio es seguro, no se pudo confirmar la redirección automática desde el puerto inseguro 80 al 443 durante el escaneo.