

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://megavenda.ceos.digital
Dominio megavenda.ceos.digital
Fecha 12 de mayo de 2026 a las 13:22

Checks 9 pruebas
Hallazgos 41 totales
Problemas 10 detectados

C

72/100

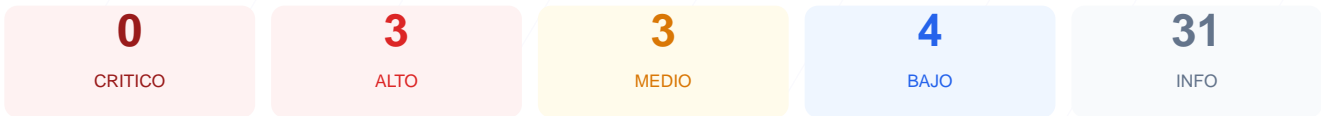
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el sitio web ha arrojado una puntuación de 72/100, lo que equivale a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 2 presentaron fallos críticos en la configuración de seguridad. La plataforma demuestra una gestión correcta del cifrado de datos, pero carece de las defensas modernas necesarias para mitigar ataques web comunes. Debido a la ausencia total de cabeceras de protección y la exposición de tecnologías internas, el sitio se considera vulnerable. Es necesario implementar medidas correctivas inmediatas para elevar los estándares de protección del activo digital.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 79 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
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	20	FALLO	Faltan robots.txt y sitemap.xml
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: 2026-07-31T00:56:24.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-05-02T00:56:25.000Z
- 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: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- **BAJO** **X-Powered-By expuesto**
X-Powered-By: ASP.NET — 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.)

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 — 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

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] Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de ataques de inyección de contenido y Cross-Site Scripting (XSS).
- [HIGH] X-Frame-Options: La falta de esta directiva hace que el sitio sea susceptible a ataques de clickjacking, donde un atacante puede engañar al usuario para realizar acciones no deseadas.
- [HIGH] Strict-Transport-Security: No se fuerza el uso de conexiones seguras mediante HSTS, permitiendo posibles ataques de degradación de protocolo.
- [MEDIUM] X-Content-Type-Options: El sitio es vulnerable a ataques de MIME-sniffing al no impedir que el navegador adivine el tipo de contenido de los archivos.
- [MEDIUM] Referrer-Policy: La falta de control sobre la información de referencia puede filtrar datos sensibles de la navegación a dominios externos.
- [MEDIUM] Permissions-Policy: No se restringen las capacidades del navegador, permitiendo potencialmente el acceso a APIs de hardware como cámara o micrófono.
- [LOW] Server header expuesto: La cabecera revela el uso de Microsoft-IIS/10.0, lo que facilita a los atacantes la búsqueda de exploits específicos para esa versión.
- [LOW] X-Powered-By expuesto: Se expone el uso del framework ASP.NET, proporcionando información valiosa para la fase de reconocimiento de un ataque.
- [LOW] Archivos informativos faltantes: La inexistencia de robots.txt y sitemap.xml dificulta la gestión de indexación y el reconocimiento estructurado del sitio.