EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://micrositios.avalpaycenter.com/instituto-centro-sistemas-ma	Checks	9 pruebas
Dominio	micrositios.avalpaycenter.com	Hallazgos	48 totales
Fecha	15 de mayo de 2026 a las 02:40	Problemas	4 detectados

A

96/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web micrositios.avalpaycenter.com arrojó una puntuación sobresaliente de 96/100, lo que equivale a una calificación de nota A. Durante el proceso se ejecutaron 9 checks pasivos, obteniendo 6 resultados satisfactorios, 2 advertencias y 0 fallos críticos. El sitio demuestra un manejo excelente de los protocolos de cifrado y la implementación de cabeceras de seguridad fundamentales. En conclusión, el sitio se considera seguro, presentando únicamente riesgos menores de configuración técnica que no comprometen la integridad inmediata de la plataforma.

Resumen de Riesgos

0	1	1	2	44
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 246 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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 246 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  246 dias restantes (expira: 2027-01-15T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-15T00:00:00.000Z
- 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: Apache — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: base-uri 'self';form-action 'self';media-src 'self';object-src 'none';worker-src...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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=(), fullscreen=(), usb=(), accelerometer=(...

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**
  Next.js

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=strict

- INFO **Cookie: micrositios-avalpaycenter-com — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: micrositios-avalpaycenter-com — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: micrositios-avalpaycenter-com — SameSite**
  SameSite=strict

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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (26 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- 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] Cookie: XSRF-TOKEN: Falta el atributo HttpOnly, lo que permite que la cookie sea accesible mediante scripts del cliente (document.cookie) y aumenta el riesgo de robo de tokens en ataques XSS.
[MEDIUM] Bloqueo total: El archivo robots.txt utiliza la directiva Disallow: / que bloquea el acceso de rastreadores a todo el sitio, afectando la visibilidad y auditoría externa.
[LOW] Server header expuesto: El encabezado Server revela el uso de Apache, lo cual otorga información sobre la tecnología subyacente que un atacante podría usar para buscar vulnerabilidades específicas.
[LOW] sitemap.xml: El archivo de mapa del sitio no fue encontrado (HTTP 404), dificultando la indexación estructurada.
[LOW] Redireccion HTTPS: No se pudo verificar la redirección automática de tráfico inseguro hacia la versión cifrada del sitio.