# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://Psincro.es | Checks | 9 pruebas |
| Dominio | psincro.es | Hallazgos | 48 totales |
| Fecha | 7 de mayo de 2026 a las 21:34 | Problemas | 5 detectados |

**A**

96/100

puntos de seguridad

## RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado ha otorgado una puntuación de 96/100, obteniendo una nota A. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 8 resultaron correctos y únicamente uno generó una advertencia por la apertura de un puerto no estándar. La infraestructura analizada demuestra una implementación sólida de protocolos de cifrado y una correcta configuración de cabeceras de seguridad. Concluyo que el sitio es seguro y presenta una postura defensiva superior a la media, aunque existen puntos de mejora en la exposición de servicios secundarios y archivos de configuración.

## Resumen de Riesgos

| 0 | 0 | 2 | 3 | 43 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 88 dias |
| Cabeceras de Seguridad | 100 | OK | Todas las cabeceras de seguridad presentes |
| Redireccion HTTPS | 100 | OK | HTTP redirige a HTTPS y HSTS esta habilitado |
| 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 | 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: 2026-08-03T18:00:16.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-05-05T18:00:17.000Z
- 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: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://www.google.com htt...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=15552000; 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=()

## Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://psincro.es/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=15552000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=15552000 (180 dias)
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

## 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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2664 bytes)
- INFO **Reglas robots.txt**
  18 Disallow, 4 Allow
- MEDIO **Bloqueo total**
  robots.txt bloquea todo el sitio con Disallow: /
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- BAJO **Ruta sensible en robots.txt**
  Referencia a "backup" — Puede revelar rutas sensibles a atacantes
- INFO **Sitemap en robots.txt**
  https://psincro.es/sitemap.xml
- 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 autenticacion 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**

[MEDIUM] Puerto 8080 (HTTP-Alt) abierto: Este puerto alternativo está activo y podría estar exponiendo servicios de gestión o proxies que no deberían ser accesibles públicamente.
[MEDIUM] Bloqueo total en robots.txt: La directiva Disallow: / impide el rastreo legítimo y, aunque no es una falla técnica per se, indica una configuración de visibilidad que requiere supervisión.
[LOW] Rutas sensibles expuestas en robots.txt: El archivo menciona explícitamente las rutas admin y backup, lo cual facilita a un atacante la identificación de directorios críticos durante la fase de reconocimiento.
[LOW] Server header expuesto: El servidor responde con la cabecera Server: cloudflare, revelando información sobre la infraestructura tecnológica que podría ser utilizada para personalizar intentos de ataque.