

# Escanear Vulnerabilidades

Informe de Seguridad Web

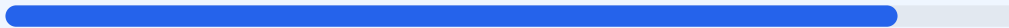
URL <https://catalogo.zynktechsolutions.com/>  
Dominio [catalogo.zynktechsolutions.com](https://catalogo.zynktechsolutions.com/)  
Fecha 16 de mayo de 2026 a las 23:42

Checks 9 pruebas  
Hallazgos 45 totales  
Problemas 6 detectados

# B

## 88/100

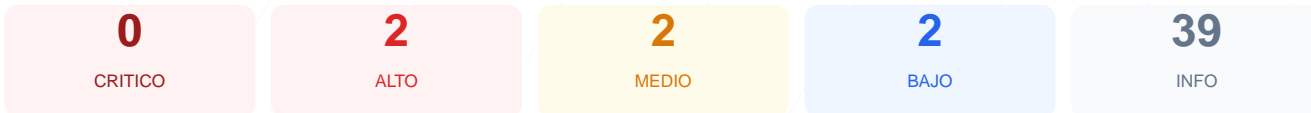
puntos de seguridad



### RESUMEN EJECUTIVO

El análisis de seguridad realizado sobre el dominio evaluado arroja una puntuación de 88/100, lo que corresponde a una nota B según los estándares de auditoría. Se ejecutaron un total de 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 generaron advertencias de seguridad, sin registrarse fallos críticos. Aunque la infraestructura base presenta un nivel de cifrado óptimo, se detectaron omisiones en las cabeceras de seguridad y puertos abiertos innecesarios. Se concluye que el sitio es generalmente seguro, pero se considera vulnerable a ataques de reconocimiento y de degradación de protocolo debido a configuraciones pendientes.

### Resumen de Riesgos



### Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 59 dias
Cabeceras de Seguridad	80	AVISO	5/6 presentes. Faltan: Strict-Transport-Security
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
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 59 dias

- INFO **Certificado valido**  
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**  
59 dias restantes (expira: 2026-07-15T05:13:57.000Z)
- INFO **Fecha de emision**  
Emitido desde: 2026-04-16T05:13:58.000Z
- INFO **Puerto 443**  
Conexion HTTPS establecida correctamente en puerto 443

### Cabeceras de Seguridad — 80/100

Estado: AVISO

5/6 presentes. Faltan: Strict-Transport-Security

- BAJO **Server header expuesto**  
Server: cloudflare — Revela tecnologia del servidor

- INFO **Content-Security-Policy**  
Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://static.cloudflarei...
- INFO **X-Frame-Options**  
Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**  
Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**  
Presente: nosniiff
- INFO **Referrer-Policy**  
Presente: same-origin
- INFO **Permissions-Policy**  
Presente: accelerometer=(),browsing-topics=(),camera=(),clipboard-read=(),clipboard-write=...

## Redireccion HTTPS — 70/100

---

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**  
HTTP 301 redirige a https://catalogo.zynktechsolutions.com/
- ALTO **HSTS (Strict-Transport-Security)**  
HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**  
HTTPS responde con status 403

## 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 (1982 bytes)
- INFO **Reglas robots.txt**  
15 Disallow, 2 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
- INFO **Sitemap en robots.txt**  
<https://catalogo.zynktechsolutions.com/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

[ALTA] HSTS (Strict-Transport-Security): No se encuentra configurado, lo que impide que el navegador fuerce conexiones cifradas y permite posibles ataques de intermediario (MitM).

[MEDIA] Puerto 8080 (HTTP-Alt) abierto: La presencia de este puerto activo sugiere la existencia de un servidor web alternativo o proxy que aumenta la superficie de ataque.

[MEDIA] Bloqueo total y rutas sensibles en robots.txt: El archivo bloquea la indexación de todo el sitio y revela la ruta "admin", lo que facilita a un atacante identificar paneles de gestión.

[BAJA] Server header expuesto: El servidor responde con la cabecera "cloudflare", revelando información sobre la tecnología de infraestructura y facilitando el reconocimiento.

[INFO] Respuesta HTTPS 403: El servidor responde con un código de estado prohibido al acceder por HTTPS, lo que indica restricciones de acceso que deben ser verificadas.