# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://dyonyx.vercel.app | Checks | 9 pruebas |
| Dominio | dyonyx.vercel.app | Hallazgos | 45 totales |
| Fecha | 13 de mayo de 2026 a las 21:51 | Problemas | 6 detectados |

**A**

96/100

puntos de seguridad

## RESUMEN EJECUTIVO

La evaluación de seguridad realizada sobre dyonyx.vercel.app arroja una puntuación de 96/100, obteniendo una calificación de nota A. El análisis consistió en nueve checks pasivos, de los cuales ocho resultaron satisfactorios y solo se registró un fallo relacionado con archivos de indexación. Se detectaron exposiciones menores de información técnica y rutas administrativas, aunque las defensas principales como el cifrado y las cabeceras de seguridad están implementadas de forma excelente. A pesar de los hallazgos en archivos de información, el sitio web se considera mayoritariamente seguro frente a ataques externos automatizados. Se recomienda realizar las mitigaciones indicadas para mantener este nivel de protección.

## Resumen de Riesgos

| 0 | 0 | 5 | 1 | 39 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 74 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 | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 100 | OK | 2 puerto(s) abierto(s), todos esperados |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 74 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  74 dias restantes (expira: 2026-07-27T02:04:42.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-04-28T02:04:43.000Z
- 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: Vercel — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self'; script-src 'self' 'unsafe-inline' https://cdn.jsdelivr.net; ...
- INFO **X-Frame-Options**
  Presente: DENY
- INFO **Strict-Transport-Security**
  Presente: max-age=63072000; includeSubDomains; preload
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: camera=(), microphone=(), geolocation=()

## Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 308 redirige a https://dyonyx.vercel.app/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO **HSTS includeSubDomains**
  HSTS cubre subdominios
- INFO **HSTS max-age**
  max-age=63072000 (730 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

- MEDIO **Archivo /readme.html**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Archivo /README.txt**
  Archivo accesible publicamente — Puede revelar version e informacion del CMS
- MEDIO **Ruta /wp-login.php**
  Panel de login accesible publicamente

- MEDIO **Ruta /administrator/**
  Panel de login accesible publicamente
- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- 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

- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

## Puertos Abiertos — 100/100

Estado: OK

2 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)**
  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
- 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 la cabecera Server: Vercel, lo que permite a un atacante identificar la tecnología de infraestructura utilizada.

[MEDIUM] Archivo /readme.html accesible: Este archivo se encuentra disponible públicamente y puede contener detalles sobre la versión del software o instrucciones internas.
[MEDIUM] Archivo /README.txt accesible: La exposición de este archivo facilita el reconocimiento de la estructura del proyecto y posibles metadatos sensibles.
[MEDIUM] Ruta /wp-login.php expuesta: El panel de acceso administrativo es visible, lo que aumenta el riesgo de ataques de fuerza bruta o de diccionario.
[MEDIUM] Ruta /administrator/ expuesta: Existe una interfaz de gestión accesible que amplía la superficie de ataque para usuarios no autorizados.
[MEDIUM] Ruta /user/login expuesta: El punto de entrada de usuarios está disponible de forma pública, permitiendo intentos de enumeración de cuentas.
[FAIL] Ausencia de robots.txt y sitemap.xml: El sitio carece de archivos para la gestión de indexación, lo que dificulta el control sobre qué partes del sitio deben ser rastreadas por motores de búsqueda.