# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://cikadron.co.in | Checks | 9 pruebas |
| Dominio | cikadron.co.in | Hallazgos | 45 totales |
| Fecha | 23 de abril de 2026 a las 15:51 | Problemas | 12 detectados |

C

63/100

puntos de seguridad

## RESUMEN EJECUTIVO

La auditoría de seguridad realizada sobre el sitio web arroja una puntuación de 63/100, lo que corresponde a una calificación de grado C. El análisis se basó en 9 checks pasivos, obteniendo 5 resultados satisfactorios, 1 advertencia y 3 fallos críticos en la configuración. Se detectó una carencia importante de cabeceras de seguridad esenciales y una gestión deficiente de los protocolos de conexión cifrada. A pesar de contar con un certificado SSL válido, la falta de redirección automática y la exposición de rutas administrativas aumentan el riesgo operativo. En conclusión, el sitio se considera vulnerable ante ataques de interceptación y manipulación de contenido debido a configuraciones de servidor incompletas.

## Resumen de Riesgos

| 0 | 3 | 8 | 1 | 33 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 100 | OK | Certificado valido, expira en 31 dias |
| Cabeceras de Seguridad | 30 | FALLO | Solo 2/6 presentes. Faltan: Content-Security-Pol... |
| Redireccion HTTPS | 0 | FALLO | No hay redireccion HTTP a 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 | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 22 (SSH) |

## SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 31 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  31 dias restantes (expira: 2026-05-24T11:19:09.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-02-23T11:19:10.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

## Cabeceras de Seguridad — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.26.2 — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000
- MEDIO **X-Content-Type-Options**
  Falta — Evita MIME-type sniffing
- INFO **Referrer-Policy**
  Presente: no-referrer
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

## Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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 — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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**

[HIGH] Redirección HTTP a HTTPS: El sitio permite conexiones mediante HTTP sin redirigir al protocolo seguro, lo que expone los datos de los usuarios a ataques de interceptación.

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de Cross-Site Scripting (XSS) e inyecciones de contenido malicioso.
[HIGH] X-Frame-Options: No se detectó esta cabecera, lo que hace al sitio susceptible a ataques de clickjacking al permitir que sea cargado dentro de frames externos.
[MEDIUM] X-Content-Type-Options: La falta de esta política permite que los navegadores realicen sniffing de tipos MIME, pudiendo ejecutar archivos con extensiones incorrectas.
[MEDIUM] Permissions-Policy: No se restringen las APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o el micrófono.
[MEDIUM] Rutas Administrativas Expuestas: Los directorios /wp-login.php, /administrator/ y /user/login son accesibles al público, facilitando intentos de acceso no autorizado.
[MEDIUM] Archivos Informativos Expuestos: Los archivos /readme.html y /README.txt están accesibles, lo cual puede revelar detalles técnicos sensibles sobre el sistema.
[MEDIUM] Puerto 22 (SSH) Abierto: El servicio de acceso remoto está expuesto públicamente, incrementando el riesgo de ataques de fuerza bruta contra el servidor.
[LOW] Exposición de Cabecera Server: El servidor revela el software y versión exacta (nginx/1.26.2), permitiendo a atacantes buscar vulnerabilidades específicas para esa versión.