EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://kdk.life	Checks	9 pruebas
Dominio	kdk.life	Hallazgos	44 totales
Fecha	7 de agosto de 2026 a las 12:24	Problemas	8 detectados

B

80/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de ciberseguridad realizada arroja una puntuación de 80/100, lo que corresponde a una calificación de grado B. El análisis se basó en 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 fallidos debido a configuraciones de servidor incompletas. Los resultados indican que el sitio posee una base robusta en cuanto a cifrado de datos y protocolos de transporte seguro. No obstante, la ausencia de cabeceras de seguridad críticas introduce riesgos innecesarios frente a ataques de inyección. En conclusión, el sitio es mayormente seguro para el usuario final, pero se considera vulnerable ante ataques técnicos específicos dirigidos a la estructura del navegador.

Resumen de Riesgos

0	2	3	3	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 48 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
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 48 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  48 dias restantes (expira: 2026-09-24T18:16:52.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-06-26T18:16:53.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Netlify — 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
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://kdk.life/
- 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

- 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 — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

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 Inteligencia Artificial

---RESUMEN EJECUTIVO---
La auditoría de ciberseguridad realizada arroja una puntuación de 80/100, lo que corresponde a una calificación de grado B. El análisis se basó en 9 checks pasivos, de los cuales 7 resultaron satisfactorios y 2 fallidos debido a configuraciones de servidor incompletas. Los resultados indican que el sitio posee una base robusta en cuanto a cifrado de datos y protocolos de transporte seguro. No obstante, la ausencia de cabeceras de seguridad críticas introduce riesgos innecesarios frente a ataques de inyección. En conclusión, el sitio es mayormente seguro para el usuario final, pero se considera vulnerable ante ataques técnicos específicos dirigidos a la estructura del navegador.

---VULNERABILITIES---
[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques de inyección de contenido y scripts maliciosos (XSS).
[HIGH] X-Frame-Options: Al no estar presente, el sitio puede ser cargado dentro de marcos externos, permitiendo ataques de Clickjacking.
[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite que el navegador realice sniffing de tipos MIME, lo que podría derivar en la ejecución de archivos peligrosos.
[MEDIUM] Referrer-Policy: No se define qué información de origen se envía a terceros, lo que puede comprometer la privacidad de la navegación.
[MEDIUM] Permissions-Policy: No existe una restricción sobre las APIs del navegador, dejando expuesto el acceso potencial a funciones como cámara o geolocalización.
[LOW] Server header expuesto: La cabecera revela el uso de Netlify, proporcionando información técnica que ayuda a un atacante a perfilar el servidor.
[LOW] Archivos de indexación faltantes: La inexistencia de robots.txt y sitemap.xml dificulta la gestión del rastreo y la visibilidad de la estructura interna.