# EscanearVulnerabilidades

Informe de Seguridad Web

| | | | |
|---|---|---|---|
| URL | https://hatysa.inocar.mil.ec | Checks | 9 pruebas |
| Dominio | hatysa.inocar.mil.ec | Hallazgos | 16 totales |
| Fecha | 10 de septiembre de 2026 a las 02:59 | Problemas | 5 detectados |

**D**

47/100

puntos de seguridad

## RESUMEN EJECUTIVO

Este informe técnico evalúa la postura de seguridad del sitio analizado, el cual ha obtenido una puntuación de 47/100 con una nota final de D. El análisis se basó en 9 checks pasivos ejecutados, detectando un fallo crítico en la infraestructura de cifrado y una advertencia de exposición de servicios. La ausencia de protocolos de seguridad básicos y la falta de redirección segura indican que la plataforma no cumple con los estándares mínimos de protección actuales. Se concluye que el sitio es vulnerable, exponiendo la comunicación entre el servidor y los usuarios a posibles interceptaciones.

## Resumen de Riesgos

| 1 | 1 | 1 | 2 | 11 |
|---|---|---|---|---|
| CRITICO | ALTO | MEDIO | BAJO | INFO |

## Resumen de Checks

| | | | |
|---|---|---|---|
| SSL/TLS | 0 | ERROR | No se pudo verificar SSL/TLS |
| Cabeceras de Seguridad | 0 | ERROR | No se pudieron verificar las cabeceras |
| Redireccion HTTPS | 0 | ERROR | No se pudo verificar la redireccion HTTPS |
| Deteccion CMS | 0 | ERROR | No se pudo analizar el CMS |
| Version CMS Expuesta | 0 | ERROR | No se pudo verificar la version del CMS |
| Seguridad de Cookies | 0 | ERROR | No se pudieron verificar las cookies |
| Contenido Mixto | 0 | ERROR | No se pudo verificar contenido mixto |
| Robots.txt y Sitemap | 20 | FALLO | Faltan robots.txt y sitemap.xml |
| Puertos Abiertos | 60 | AVISO | 1 puerto(s) potencialmente riesgoso(s): 8080 (HT... |

## SSL/TLS — 0/100

Estado: ERROR

No se pudo verificar SSL/TLS

- CRITICO **Conexion SSL**
  No se pudo establecer conexion SSL/TLS

## Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- ALTO **HTTP !' HTTPS redireccion**
  HTTP 200 — No redirige a HTTPS

## Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  Error al acceder

- BAJO **sitemap.xml**
  Error al acceder

## 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)**
  Cerrado — 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**

[CRITICAL] Conexion SSL: No fue posible establecer una conexion SSL/TLS verificable, lo que significa que la transmision de datos no cuenta con una capa de cifrado valida.
[HIGH] Redireccion HTTPS: El servidor responde mediante HTTP 200 sin redirigir automaticamente a una version segura, permitiendo que la informacion viaje en texto plano por la red.
[MEDIUM] Puerto 8080 ABIERTO: Se detecto un servidor web alternativo o proxy en el puerto 8080, lo cual amplia la superficie de ataque y puede exponer servicios administrativos no protegidos.
[LOW] Ausencia de archivos de control: No se detectaron los archivos robots.txt ni sitemap.xml, lo que dificulta la gestion del rastreo por motores de busqueda y la organizacion del sitio.
[HIGH] Cabeceras de seguridad faltantes: No se pudieron verificar las cabeceras de proteccion contra ataques de inyeccion, clickjacking y ejecucion de scripts maliciosos.