

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://ide.inocar.mil.ec	Checks	9 pruebas
Dominio	ide.inocar.mil.ec	Hallazgos	38 totales
Fecha	10 de septiembre de 2026 a las 14:58	Problemas	8 detectados

C

72/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio ide.inocar.mil.ec ha arrojado una puntuación de 72/100, lo que corresponde a una calificación de C. Durante la evaluación se ejecutaron 9 checks pasivos, resultando en 6 verificaciones satisfactorias y 2 fallos críticos en la configuración del servidor. Aunque la conexión está cifrada, la carencia total de políticas de seguridad en las cabeceras expone a los usuarios a riesgos evitables. En su estado actual, el sitio presenta vulnerabilidades que comprometen la integridad de la sesión del visitante, por lo cual no puede considerarse plenamente seguro.

Resumen de Riesgos

0 CRITICO	3 ALTO	3 MEDIO	2 BAJO	30 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 66 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 66 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
66 dias restantes (expira: 2026-11-15T15:32:36.000Z)
- INFO Fecha de emision
Emitido desde: 2025-10-15T15:32:36.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 0/100

Estado: FALLO

Solo 0/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, Strict-Transport-Security, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- ALTO Content-Security-Policy
Falta — Previene XSS y ataques de inyeccion de contenido

- ALTO

X-Frame-Options
Falta — Protege contra clickjacking
- ALTO

Strict-Transport-Security
Falta — Fuerza conexiones HTTPS (HSTS)
- 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.)

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 política de divulgacion

Puertos Abiertos — 100/100

Estado: OK

1 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 — Envío de correo
- INFO

Puerto 80 (HTTP)
Cerrado — 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] Content-Security-Policy: La ausencia de esta cabecera facilita la ejecución de ataques Cross-Site Scripting (XSS) y la inyección de contenido malicioso.

[HIGH] X-Frame-Options: El sitio no protege contra clickjacking, permitiendo que atacantes embeban la página en marcos externos para engañar al usuario.

[HIGH] Strict-Transport-Security: No se obliga al navegador a utilizar exclusivamente conexiones HTTPS, lo que permite ataques de degradación de protocolo.

[MEDIUM] X-Content-Type-Options: La falta de esta directiva permite el MIME-type sniffing, aumentando el riesgo de que archivos cargados se ejecuten como scripts.

[MEDIUM] Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que podría filtrar rutas internas de la infraestructura.

[MEDIUM] Permissions-Policy: El servidor no restringe el acceso a APIs sensibles del navegador como la cámara, el micrófono o la ubicación.

[LOW] Redirección HTTPS: Se detectó un error en la verificación de la redirección automática, lo que podría permitir accesos por canales no cifrados.

[LOW] Archivos de indexación faltantes: No se encontraron los archivos robots.txt ni sitemap.xml, necesarios para una gestión controlada del rastreo por motores de búsqueda.