EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://23go.coop23dejulio.fin.ec/	Checks	9 pruebas
Dominio	23go.coop23dejulio.fin.ec	Hallazgos	40 totales
Fecha	7 de julio de 2026 a las 21:06	Problemas	1 detectados

A

100/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado a la plataforma arroja una puntuación de 100/100 con una calificación de grado A. Se ejecutaron 9 checks pasivos, obteniendo 8 resultados satisfactorios y ninguna advertencia de seguridad crítica. El portal presenta una configuración de cifrado SSL y cabeceras de protección de primer nivel, lo cual es fundamental para la integridad de los datos. No se detectaron fallos que comprometan la disponibilidad o confidencialidad inmediata de la información. En conclusión, basándose exclusivamente en los parámetros analizados, el sitio se considera altamente seguro.

Resumen de Riesgos

0	0	0	1	39
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 57 dias
Cabeceras de Seguridad	100	OK	Todas las cabeceras de seguridad presentes
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	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	100	OK	1 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 57 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  57 dias restantes (expira: 2026-09-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-08-27T00:00:00.000Z
- 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: nginx — Revela tecnologia del servidor

- INFO **Content-Security-Policy**
  Presente: default-src 'self' data: blob:; script-src 'self' 'unsafe-inline' https:; style-...
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000; includeSubDomains
- INFO **X-Content-Type-Options**
  Presente: nosniff
- INFO **Referrer-Policy**
  Presente: strict-origin-when-cross-origin
- INFO **Permissions-Policy**
  Presente: geolocation=(), microphone=(), camera=(), fullscreen=(self)

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 — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (113 bytes)
- INFO **Reglas robots.txt**
  2 Disallow, 1 Allow
- INFO **Sitemap en robots.txt**
  https://23go.coop23dejulio.fin.ec/sitemap.xml
- INFO **security.txt**
  Presente en /.well-known/security.txt — Buena practica

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 — Envio 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

[BAJA] Server header expuesto: El servidor revela la tecnología Server: nginx, lo que permite a un atacante potencial conocer el software base y buscar vulnerabilidades específicas para esa versión.
[BAJA] Redirección HTTPS no verificada: El sistema de escaneo reportó un error al intentar validar la redirección automática de tráfico HTTP a HTTPS, lo que podría implicar un riesgo menor si no se fuerza la conexión cifrada.