

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://eldorado.sd.cloud.invgate.net/portal	Checks	9 pruebas
Dominio	eldorado.sd.cloud.invgate.net	Hallazgos	51 totales
Fecha	28 de julio de 2026 a las 16:33	Problemas	4 detectados

A

93/100

puntos de seguridad



RESUMEN EJECUTIVO

El analisis de seguridad realizado al sitio eldorado.sd.cloud.invgate.net arroja una puntuacion de 93/100 con una nota de A. De los 9 checks pasivos ejecutados, 7 finalizaron con exito, registrandose 1 advertencia relacionada con cabeceras de seguridad y 1 fallo por ausencia de archivos de configuracion. La infraestructura presenta un cifrado robusto y una gestion de sesiones adecuada, minimizando los riesgos de interceptacion de datos. Se concluye que el sitio es seguro, aunque requiere ajustes tecnicos especificos para alcanzar un estado de proteccion optimo.

Resumen de Riesgos

0 CRITICO	0 ALTO	1 MEDIO	3 BAJO	47 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 136 dias
Cabeceras de Seguridad	85	AVISO	5/6 presentes. Faltan: Permissions-Policy
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	2 cookies, todas con flags correctos
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 136 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
136 dias restantes (expira: 2026-12-11T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2025-11-13T00:00:00.000Z
- INFO Puerto 443
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 85/100

Estado: AVISO

5/6 presentes. Faltan: Permissions-Policy

- BAJO Server header expuesto
Server: Apache — Revela tecnologia del servidor

- INFO

Content-Security-Policy
Presente: base-uri 'self'; default-src 'self'; child-src https://www.youtube.com http://ww...
- INFO

X-Frame-Options
Presente: SAMEORIGIN
- INFO

Strict-Transport-Security
Presente: max-age=63072000; includeSubDomains; preload
- INFO

X-Content-Type-Options
Presente: nosniff
- INFO

Referrer-Policy
Presente: strict-origin-when-cross-origin
- 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://eldorado.sd.cloud.invgate.net:443/
- INFO

HSTS (Strict-Transport-Security)
HSTS activo: max-age=63072000; includeSubDomains; preload
- BAJO

HSTS includeSubDomains
HSTS cubre subdominios
- INFO

HSTS max-age
max-age=63072000 (730 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
- INFO

Tecnologias detectadas
React, Next.js

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
2 cookies, todas con flags correctos

INFO

Cookies detectadas
2 cookie(s) encontrada(s)

INFO

Cookie: IGSMSESSID — HttpOnly
HttpOnly activo — No accesible via JavaScript

INFO

Cookie: IGSMSESSID — Secure
Flag Secure activo — Solo se envia por HTTPS

INFO

Cookie: IGSMSESSID — SameSite
SameSite=lax

INFO

Cookie: IGSMSESSID — HttpOnly
HttpOnly activo — No accesible via JavaScript

INFO

Cookie: IGSMSESSID — Secure
Flag Secure activo — Solo se envia por HTTPS

INFO

Cookie: IGSMSESSID — SameSite
SameSite=lax

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 Seguridad

VULNERABILIDADES DETECTADAS

[MEDIUM] Permissions-Policy: La ausencia de esta cabecera impide al administrador restringir el acceso a funcionalidades sensibles del navegador, como la camara o el microfono, aumentando el riesgo de ataques de inyeccion.

[LOW] Server header expuesto: El servidor responde con la cabecera Server: Apache, lo cual revela informacion tecnica que permite a un atacante identificar posibles vectores de ataque especificos para esa version.

[LOW] robots.txt: El archivo no fue localizado (Error 404), lo que puede resultar en una indexacion descontrolada de rutas internas por parte de motores de busqueda.

[LOW] sitemap.xml: La falta de este archivo dificulta la auditoria de la estructura completa del sitio y la visibilidad de todos sus endpoints publicos.