EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://nl.gob.mx	Checks	9 pruebas
Dominio	nl.gob.mx	Hallazgos	19 totales
Fecha	8 de agosto de 2026 a las 17:19	Problemas	3 detectados

C

73/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 73/100, lo que corresponde a una nota de C. El análisis se basó exclusivamente en 9 checks pasivos, de los cuales solo uno resultó exitoso, mientras que se registraron advertencias por puertos expuestos y fallos en archivos de configuración. Se detectaron deficiencias importantes en la visibilidad de cabeceras de seguridad y en la gestión de servicios alternativos. Debido a estos hallazgos, se concluye que el sitio es vulnerable y requiere intervenciones técnicas inmediatas para mitigar riesgos de exposición.

Resumen de Riesgos

0	0	1	2	16
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 37 dias
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 — 100/100

Estado: OK

Certificado valido, expira en 37 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  37 dias restantes (expira: 2026-09-14T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-15T00:00:00.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Redireccion HTTPS — 0/100

Estado: ERROR

No se pudo verificar la redireccion HTTPS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://nl.gob.mx/

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)**
  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
- 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

[MEDIUM] Puerto 8080 (HTTP-Alt): Se detectó un servidor web alternativo o proxy abierto, lo cual es peligroso porque suele ser un vector de ataque para servicios administrativos no protegidos.
[LOW] Error en robots.txt: No se pudo acceder al archivo de directivas de rastreo, lo que impide controlar qué partes del sitio deben ser indexadas por buscadores.
[LOW] Error en sitemap.xml: El archivo de mapa del sitio no está disponible, afectando la navegación estructurada y la auditoría de contenidos expuestos.
[HIGH] Error en Cabeceras de Seguridad: La ausencia de verificación de cabeceras indica que el sitio carece de protecciones básicas contra ataques de inyección y XSS.
[HIGH] Error en Redirección HTTPS: No se pudo confirmar la transición automática de tráfico no cifrado a cifrado, permitiendo potenciales conexiones inseguras.
[MEDIUM] Seguridad de Cookies: No se pudo verificar la presencia de atributos de seguridad en las cookies, lo que podría facilitar el secuestro de sesiones.