

Escanear Vulnerabilidades

Informe de Seguridad Web

URL https://Licenciab.mtc.gob.pe
Dominio licenciab.mtc.gob.pe
Fecha 2 de mayo de 2026 a las 05:38

Checks 9 pruebas
Hallazgos 44 totales
Problemas 10 detectados

C

64/100

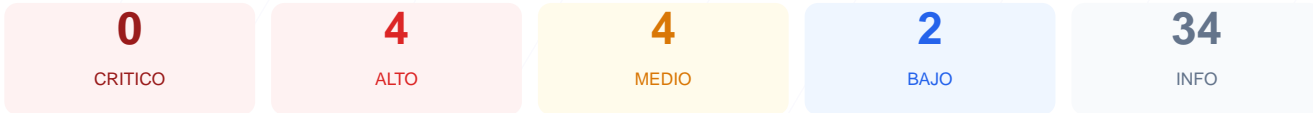
puntos de seguridad



RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio licenciab.mtc.gob.pe arroja una puntuación de 64/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 presentaron fallos críticos de seguridad. Aunque la infraestructura posee un certificado SSL válido, la carencia de cabeceras de protección y errores en la gestión de protocolos de cifrado elevan el riesgo técnico. En conclusión, el sitio se considera vulnerable debido a configuraciones de servidor incompletas que exponen a los usuarios a ataques de intermediación e inyección de código.

Resumen de Riesgos



Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 336 dias
Cabeceras de Seguridad	25	FALLO	Solo 2/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	FALLO	No hay redireccion HTTP a 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	60	AVISO	Falta sitemap.xml
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 8080 (HT...

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 336 dias

- INFO **Certificado valido**
El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
336 dias restantes (expira: 2027-04-02T23:59:59.000Z)
- INFO **Fecha de emision**
Emitido desde: 2026-03-02T00:00:00.000Z
- INFO **Puerto 443**
Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 25/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, X-Content-Type-Options, Permissions-Policy

- BAJO **Server header expuesto**
Server: cloudflare — Revela tecnologia del servidor

- **ALTO** **Content-Security-Policy**
Falta — Previene XSS y ataques de inyección de contenido
- **INFO** **X-Frame-Options**
Presente: SAMEORIGIN
- **ALTO** **Strict-Transport-Security**
Falta — Fuerza conexiones HTTPS (HSTS)
- **MEDIO** **X-Content-Type-Options**
Falta — Evita MIME-type sniffing
- **INFO** **Referrer-Policy**
Presente: same-origin
- **MEDIO** **Permissions-Policy**
Falta — Restringe APIs del navegador (camara, micro, etc.)

Redirección HTTPS — 0/100

Estado: **FALLO**

No hay redirección HTTP a HTTPS

- **ALTO** **HTTP !' HTTPS redirección**
HTTP 403 — No redirige a HTTPS
- **ALTO** **HSTS (Strict-Transport-Security)**
HSTS no configurado — El navegador no fuerza HTTPS
- **INFO** **Respuesta HTTPS**
HTTPS responde con status 403

Detección CMS — 100/100

Estado: **OK**

No se detectó 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 detectó versión de CMS expuesta

- **INFO** **Archivo /readme.html**
No accesible (correcto)
- **INFO** **Archivo /README.txt**
No accesible (correcto)
- **INFO** **Version CMS**
No se detecta ninguna versión 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- **INFO** **robots.txt**
Presente (1738 bytes)
- **INFO** **Reglas robots.txt**
9 Disallow, 1 Allow
- **MEDIO** **Bloqueo total**
robots.txt bloquea todo el sitio con Disallow: /
- **BAJO** **sitemap.xml**
No encontrado (HTTP 403)
- **BAJO** **security.txt**
No encontrado — Recomendado para politica de divulgacion

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

[HIGH] Content-Security-Policy: La ausencia de esta cabecera facilita ataques de Cross-Site Scripting (XSS) y la inyección de contenido no autorizado en el navegador del usuario.

[HIGH] HTTP a HTTPS redirección: El servidor no redirige automáticamente las conexiones inseguras a seguras, lo que permite la interceptación de datos en tránsito.

[HIGH] Strict-Transport-Security: La falta de configuración HSTS impide que el navegador obligue siempre una conexión cifrada, dejando el sitio vulnerable a ataques de degradación de SSL.

[MEDIUM] X-Content-Type-Options: La omisión de esta cabecera permite el MIME-sniffing, lo que puede llevar al navegador a interpretar archivos de forma incorrecta y ejecutar scripts maliciosos.

[MEDIUM] Permissions-Policy: No se definen restricciones sobre el uso de APIs del navegador, permitiendo potencialmente el acceso no autorizado a funciones como la cámara o el micrófono.

[MEDIUM] Puerto 8080 (HTTP-Alt): La presencia de un puerto de servidor web alternativo abierto incrementa la superficie de ataque y puede exponer servicios internos no protegidos.

[MEDIUM] Bloqueo en robots.txt: El archivo de rastreo prohíbe el acceso total al sitio, lo cual es una práctica irregular que puede ocultar problemas de configuración o denegación de servicios.

[LOW] Server header expuesto: El servidor revela el uso de tecnología Cloudflare, entregando información técnica que puede ser utilizada para dirigir ataques específicos.

[LOW] sitemap.xml: La ausencia de un mapa del sitio dificulta la verificación de la estructura web y la auditoría de rutas de contenido.