

EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://edutk.imss.gob.mx/enrol/index.php?id=147	Checks	9 pruebas
Dominio	edutk.imss.gob.mx	Hallazgos	47 totales
Fecha	7 de agosto de 2026 a las 16:48	Problemas	20 detectados

D

45/100

puntos de seguridad



RESUMEN EJECUTIVO

El análisis de seguridad realizado al sitio web arroja una puntuación de 45/100, lo que corresponde a una nota D. Durante el procedimiento se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 0 advertencias y 5 fallos críticos. La infraestructura presenta deficiencias severas en la configuración de cabeceras de protección, gestión de sesiones y exposición de servicios internos. Se concluye que el sitio es actualmente vulnerable y presenta un riesgo significativo para la integridad de los datos de los usuarios.

Resumen de Riesgos

3 CRITICO	9 ALTO	6 MEDIO	2 BAJO	27 INFO
--------------	-----------	------------	-----------	------------

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 179 dias
Cabeceras de Seguridad	0	FALLO	Solo 0/6 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	17	FALLO	visid_incap_2259261: falta Secure; visid_incap_2...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	20	FALLO	5 puertos riesgosos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 179 dias

- INFO Certificado valido
El certificado SSL es valido y de confianza
- INFO Dias hasta expiracion
179 dias restantes (expira: 2027-02-02T23:59:59.000Z)
- INFO Fecha de emision
Emitido desde: 2026-02-03T00:00:00.000Z
- 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.)

Redireccion HTTPS — 0/100

Estado: FALLO

No hay redireccion HTTP a HTTPS

- ALTO

HTTP !' HTTPS redireccion
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

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 — 17/100

Estado: FALLO

visid_incap_2259261: falta Secure; visid_incap_2259261: falta SameSite; incap_ses_690_2259261: falta HttpOnly; incap_ses_690_2259261: falta Secure; incap_ses_690_2259261: falta SameSite

- INFO

Cookies detectadas
2 cookie(s) encontrada(s)

- INFO

Cookie: visid_incap_2259261 — HttpOnly
HttpOnly activo — No accesible via JavaScript
- ALTO

Cookie: visid_incap_2259261 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: visid_incap_2259261 — SameSite
Falta SameSite — Vulnerable a CSRF
- ALTO

Cookie: incap_ses_690_2259261 — HttpOnly
Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO

Cookie: incap_ses_690_2259261 — Secure
Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO

Cookie: incap_ses_690_2259261 — SameSite
Falta SameSite — Vulnerable a CSRF

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 403)
- BAJO

sitemap.xml
No encontrado (HTTP 403)
- BAJO

security.txt
No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 20/100

Estado: FALLO

5 puertos riesgosos abiertos

- ALTO

Puerto 21 (FTP)
ABIERTO — 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
- CRITICO

Puerto 3306 (MySQL)
ABIERTO — Base de datos MySQL expuesta
- CRITICO

Puerto 3389 (RDP)
ABIERTO — Escritorio remoto Windows
- INFO

Puerto 5432 (PostgreSQL)
Cerrado — Base de datos PostgreSQL expuesta
- CRITICO

Puerto 6379 (Redis)
ABIERTO — 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

- [CRITICAL] Puerto 3306 (MySQL): Base de datos expuesta directamente a Internet, lo que permite intentos de acceso no autorizado y ataques de fuerza bruta.
- [CRITICAL] Puerto 3389 (RDP): El servicio de escritorio remoto de Windows se encuentra abierto, facilitando posibles intrusiones al servidor.
- [CRITICAL] Puerto 6379 (Redis): Servicio de caché accesible sin autenticación por defecto, exponiendo datos temporales almacenados en memoria.
- [HIGH] Cabeceras de Seguridad Faltantes: La ausencia total de cabeceras como CSP y X-Frame-Options facilita ataques de XSS y clickjacking.
- [HIGH] Redirección HTTPS Inexistente: El servidor no fuerza el tráfico cifrado, permitiendo la interceptación de datos en tránsito.
- [HIGH] Puerto 21 (FTP): El uso de este puerto implica la transferencia de archivos y credenciales sin cifrado, siendo vulnerable a escucha activa.
- [HIGH] Configuración de Cookies Insegura: Las cookies carecen de los atributos Secure, HttpOnly y SameSite, permitiendo el robo de sesiones mediante scripts.
- [MEDIUM] Puerto 8080 (HTTP-Alt): Puerto de servidor web alternativo abierto que suele albergar paneles de administración desprotegidos.
- [LOW] Archivos de Estructura Faltantes: La ausencia de robots.txt y sitemap.xml expone el sitio a un reconocimiento no controlado por parte de terceros.