EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://siproa.energia.gob.mx/login	Checks	9 pruebas
Dominio	siproa.energia.gob.mx	Hallazgos	51 totales
Fecha	24 de julio de 2026 a las 09:10	Problemas	9 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio siproa.energia.gob.mx arroja una puntuación de 65/100, lo que corresponde a una nota C. El análisis se basó en 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fueron identificados como fallos críticos. Se detectó una carencia importante de cabeceras de seguridad y una gestión deficiente en la redirección de tráfico cifrado. Debido a la ausencia de protecciones modernas contra ataques de inyección y secuestro de clics, el sitio se considera vulnerable.

Resumen de Riesgos

0	4	3	2	42
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 81 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 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	83	AVISO	XSRF-TOKEN: falta HttpOnly
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 81 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  81 dias restantes (expira: 2026-10-13T00:03:33.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-09-11T00:03:33.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 20/100

Estado: FALLO

Solo 1/6 presentes. Faltan: Content-Security-Policy, X-Frame-Options, X-Content-Type-Options, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Apache/2.4.67 (Debian) — Revela tecnologia del servidor

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- ALTO **X-Frame-Options**
  Falta — Protege contra clickjacking
- INFO **Strict-Transport-Security**
  Presente: max-age=31536000, max-age=31536000
- 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 503 — No redirige a HTTPS
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=31536000, max-age=31536000
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- INFO **HSTS max-age**
  max-age=31536000 (365 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

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 — 83/100

Estado: AVISO

XSRF-TOKEN: falta HttpOnly

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: XSRF-TOKEN — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: XSRF-TOKEN — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: XSRF-TOKEN — SameSite**
  SameSite=lax
- INFO **Cookie: siproa_session — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: siproa_session — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: siproa_session — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (24 bytes)
- INFO **Reglas robots.txt**
  1 Disallow, 0 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

No se detectaron puertos abiertos

- 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)**
  Cerrado — 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

[HIGH] Redirección HTTP a HTTPS fallida: El servidor devuelve un error 503 y no fuerza el tráfico hacia una conexión segura, permitiendo comunicaciones no cifradas.
[HIGH] Content-Security-Policy faltante: La ausencia de esta política permite la ejecución de scripts maliciosos y ataques de inyección de contenido.
[HIGH] X-Frame-Options faltante: El sitio no previene ser cargado dentro de marcos externos, lo que lo hace susceptible a ataques de clickjacking.
[HIGH] Cookie XSRF-TOKEN sin HttpOnly: La cookie de seguridad carece del atributo que impide su lectura mediante scripts, facilitando el robo de sesiones mediante XSS.
[MEDIUM] X-Content-Type-Options faltante: No se evita que el navegador intente interpretar el tipo de contenido, lo que puede derivar en la ejecución de archivos inesperados.
[MEDIUM] Referrer-Policy faltante: No existe control sobre la información de navegación que se envía a otros sitios web externos.
[MEDIUM] Permissions-Policy faltante: El servidor no restringe el acceso de la aplicación a funciones sensibles del navegador como cámara, micrófono o ubicación.
[LOW] Cabecera Server expuesta: Se revela la versión específica del software del servidor (Apache/2.4.67 Debian), lo que ayuda a atacantes a buscar exploits conocidos.
[LOW] Sitemap.xml no encontrado: La falta de un mapa del sitio dificulta la correcta indexación y supervisión de la estructura de directorios del portal.