EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://www.minsa.gob.pa/	Checks	9 pruebas
Dominio	www.minsa.gob.pa	Hallazgos	59 totales
Fecha	27 de abril de 2026 a las 13:39	Problemas	22 detectados

B

75/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoria de seguridad realizada sobre el dominio minsa.gob.pa arroja una puntuacion de 75/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, de los cuales 5 resultaron satisfactorios, 2 generaron advertencias y 2 fallaron criticamente. Aunque el sitio posee un certificado SSL valido, la ausencia de cabeceras de seguridad fundamentales y la presencia masiva de contenido mixto debilitan su postura defensiva. Se concluye que el sitio es funcionalmente estable pero vulnerable a ataques de intermediario (MitM) y reconocimiento de infraestructura debido a configuraciones incompletas.

Resumen de Riesgos

0	2	16	4	37
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 46 dias
Cabeceras de Seguridad	55	FALLO	Solo 3/6 presentes. Faltan: Strict-Transport-Sec...
Redireccion HTTPS	70	AVISO	HTTP redirige a HTTPS pero falta HSTS
Deteccion CMS	100	OK	CMS detectado: WordPress, Drupal, PrestaShop
Version CMS Expuesta	100	OK	No se detecto version de CMS expuesta
Seguridad de Cookies	100	OK	No se encontraron cookies
Contenido Mixto	20	FALLO	155 recursos HTTP en pagina HTTPS
Robots.txt y Sitemap	100	OK	robots.txt y sitemap.xml presentes
Puertos Abiertos	60	AVISO	1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 46 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  46 dias restantes (expira: 2026-06-12T23:03:58.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-03-14T23:03:59.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 55/100

Estado: FALLO

Solo 3/6 presentes. Faltan: Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: nginx/1.16.1 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: PHP/7.2.34 — Revela framework/lenguaje
- INFO **Content-Security-Policy**
  Presente: upgrade-insecure-requests
- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- ALTO **Strict-Transport-Security**
  Falta — Fuerza conexiones HTTPS (HSTS)
- INFO **X-Content-Type-Options**
  Presente: nosniff
- MEDIO **Referrer-Policy**
  Falta — Controla la informacion de referer enviada
- MEDIO **Permissions-Policy**
  Falta — Restringe APIs del navegador (camara, micro, etc.)

Redireccion HTTPS — 70/100

Estado: AVISO

HTTP redirige a HTTPS pero falta HSTS

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://www.minsa.gob.pa/
- ALTO **HSTS (Strict-Transport-Security)**
  HSTS no configurado — El navegador no fuerza HTTPS
- INFO **Respuesta HTTPS**
  HTTPS responde con status 200

Deteccion CMS — 100/100

Estado: OK

CMS detectado: WordPress, Drupal, PrestaShop

- INFO **WordPress**
  Detectado via HTML body
- INFO **Joomla**
  No detectado
- INFO **Drupal**
  Detectado via HTML body
- INFO **Magento**
  No detectado
- INFO **Shopify**
  No detectado
- INFO **PrestaShop**
  Detectado via HTML body
- INFO **Wix**
  No detectado
- INFO **Squarespace**
  No detectado
- BAJO **Meta generator**
  Expone: Drupal 7 (http://drupal.org)
- INFO **Tecnologias detectadas**
  Next.js, PHP/7.2.34

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)

- MEDIO **Ruta /user/login**
  Panel de login accesible publicamente
- INFO **Version CMS**
  No se detecta ninguna version 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 — 20/100

Estado: FALLO

155 recursos HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://minsa.b-cdn.net/sites/all/modules/contrib/jquery_upda...
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://minsa.b-cdn.net/misc/jquery-extend-3.4.0.js?v=1.8.3
- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://minsa.b-cdn.net/misc/jquery-html-prefilter-3.5.0-back...
- MEDIO **src (script/img/iframe)**
  ...y 82 mas del mismo tipo
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://minsa.b-cdn.net/sites/all/themes/minsa/css/ie-lte-8.c...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://minsa.b-cdn.net/sites/all/themes/minsa/css/ie-lte-7.c...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.presidencia.gob.pa
- MEDIO **href (link/stylesheet)**
  ...y 32 mas del mismo tipo
- MEDIO **Recurso HTTP (CSS url())**
  http://minsa.b-cdn.net/modules/system/system.base.css?t9u3bc
- MEDIO **Recurso HTTP (CSS url())**
  http://minsa.b-cdn.net/modules/system/system.menus.css?t9u3b...
- MEDIO **Recurso HTTP (CSS url())**
  http://minsa.b-cdn.net/modules/system/system.messages.css?t9...
- MEDIO **CSS url()**
  ...y 32 mas del mismo tipo

Robots.txt y Sitemap — 100/100

Estado: OK

robots.txt y sitemap.xml presentes

- INFO **robots.txt**
  Presente (2189 bytes)
- INFO **Reglas robots.txt**
  36 Disallow, 32 Allow
- BAJO **Ruta sensible en robots.txt**
  Referencia a "admin" — Puede revelar rutas sensibles a atacantes
- INFO **sitemap.xml**
  Presente, 6 URLs
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 60/100

Estado: AVISO

1 puerto(s) potencialmente riesgoso(s): 22 (SSH)

- INFO **Puerto 21 (FTP)**
  Cerrado — Transferencia de archivos sin cifrar
- MEDIO **Puerto 22 (SSH)**
  ABIERTO — 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

[HIGH] Strict-Transport-Security: Falta la cabecera HSTS, lo que impide que el navegador fuerce conexiones HTTPS de forma automatica, permitiendo ataques de degradacion.
[HIGH] Contenido Mixto: Se detectaron 155 recursos (scripts, imagenes y estilos) cargados mediante protocolos no seguros (HTTP) dentro de la pagina HTTPS, rompiendo la cadena de confianza.
[MEDIUM] Puerto 22 (SSH) ABIERTO: La exposicion de este puerto de administracion remota incrementa el riesgo de intentos de acceso no autorizados por fuerza bruta.
[MEDIUM] Referrer-Policy: La ausencia de esta cabecera podria exponer informacion sensible sobre el origen de la navegacion a dominios externos.
[MEDIUM] Permissions-Policy: No se han definido restricciones para APIs del navegador, dejando activos permisos potenciales para el uso de hardware o sensores por parte de terceros.
[MEDIUM] Ruta /user/login: El panel de acceso administrativo es publicamente visible, lo que facilita el mapeo de la superficie de ataque por parte de actores maliciosos.
[LOW] Server header expuesto: El servidor revela el uso de nginx/1.16.1, informacion tecnica que permite a un atacante buscar vulnerabilidades especificas para esa version.
[LOW] X-Powered-By expuesto: Se divulga el uso de PHP/7.2.34, permitiendo identificar el lenguaje de programacion y sus debilidades conocidas.
[LOW] Meta generator: El codigo fuente expone el uso de Drupal 7, revelando la tecnologia base del portal.
[LOW] Ruta sensible en robots.txt: El archivo hace referencia a directorios de administracion, ayudando involuntariamente al atacante a navegar por rutas internas.