EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://buzonciudadano.stps.gob.mx/Buzon.aspx	Checks	9 pruebas
Dominio	buzonciudadano.stps.gob.mx	Hallazgos	53 totales
Fecha	7 de agosto de 2026 a las 03:28	Problemas	17 detectados

C

65/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado al sitio web buzonciudadano.stps.gob.mx arroja una puntuación de 65/100, lo que corresponde a una calificación de grado C. Durante la evaluación se ejecutaron 9 checks pasivos, obteniendo 4 resultados satisfactorios, 2 advertencias por configuraciones mejorables y 3 fallos críticos en la infraestructura de seguridad. Si bien la capa de transporte se encuentra cifrada, la ausencia de políticas de seguridad modernas y la exposición de cookies sensibles comprometen la integridad de la sesión del usuario. En conclusión, el sitio web se considera vulnerable ante ataques de inyección y suplantación de identidad debido a configuraciones deficientes en el servidor.

Resumen de Riesgos

0	5	8	4	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 185 dias
Cabeceras de Seguridad	20	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	100	OK	HTTP redirige a HTTPS y HSTS esta habilitado
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	33	FALLO	ApplicationGatewayAffinityCORS: falta HttpOnly; ...
Contenido Mixto	60	AVISO	2 recurso(s) HTTP en pagina HTTPS
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 185 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  185 dias restantes (expira: 2027-02-07T19:28:40.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-06T19:28:40.000Z
- 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: Microsoft-IIS/10.0 — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: ASP.NET — Revela framework/lenguaje
- 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=0
- 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 — 100/100

Estado: OK

HTTP redirige a HTTPS y HSTS esta habilitado

- INFO **HTTP !' HTTPS redireccion**
  HTTP 301 redirige a https://buzonciudadano.stps.gob.mx/
- INFO **HSTS (Strict-Transport-Security)**
  HSTS activo: max-age=0
- BAJO **HSTS includeSubDomains**
  HSTS no cubre subdominios
- MEDIO **HSTS max-age**
  max-age=0 (0 dias) — Recomendado minimo 180 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
- INFO **Tecnologias detectadas**
  ASP.NET

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 — 33/100

Estado: FALLO

ApplicationGatewayAffinityCORS: falta HttpOnly; ApplicationGatewayAffinity: falta HttpOnly; ApplicationGatewayAffinity: falta Secure; ApplicationGatewayAffinity: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: ApplicationGatewayAffinityCORS — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ApplicationGatewayAffinityCORS — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- INFO **Cookie: ApplicationGatewayAffinityCORS — SameSite**
  SameSite=none
- ALTO **Cookie: ApplicationGatewayAffinity — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- ALTO **Cookie: ApplicationGatewayAffinity — Secure**
  Falta flag Secure — Cookie se envia en conexiones HTTP
- MEDIO **Cookie: ApplicationGatewayAffinity — SameSite**
  Falta SameSite — Vulnerable a CSRF

Contenido Mixto — 60/100

Estado: AVISO

2 recurso(s) HTTP en pagina HTTPS

- MEDIO **Recurso HTTP (src (script/img/iframe))**
  http://framework-gb.cdn.gob.mx/assets/scripts/jquery-ui-date...
- MEDIO **Recurso HTTP (href (link/stylesheet))**
  http://www.stps.gob.mx/gobmx/avisosprivacidad/AvisoPrivacida...

Robots.txt y Sitemap — 20/100

Estado: FALLO

Faltan robots.txt y sitemap.xml

- BAJO **robots.txt**
  No encontrado (HTTP 404)
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- 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 permite la ejecución de scripts no autorizados y ataques de Cross-Site Scripting (XSS).
[HIGH] X-Frame-Options: Al no estar presente, el sitio es susceptible a ataques de clickjacking donde un atacante puede engañar al usuario para realizar acciones no deseadas.
[HIGH] Cookies sin flag HttpOnly: Las cookies ApplicationGatewayAffinity y ApplicationGatewayAffinityCORS son accesibles vía scripts, facilitando el robo de sesiones.
[HIGH] Cookies sin flag Secure: La cookie ApplicationGatewayAffinity puede enviarse a través de canales no cifrados, exponiendo datos de navegación.
[MEDIUM] Contenido Mixto: Se detectó la carga de scripts y hojas de estilo mediante HTTP en una página protegida por HTTPS, rompiendo la cadena de confianza.
[MEDIUM] Puerto 8080 Abierto: La exposición del puerto HTTP-Alt incrementa la superficie de ataque al ofrecer un servicio web alternativo potencialmente menos protegido.
[MEDIUM] X-Content-Type-Options: La falta de esta cabecera permite que el navegador intente adivinar el tipo de contenido, lo que puede derivar en la ejecución de archivos maliciosos.
[MEDIUM] HSTS con duración nula: El valor max-age=0 desactiva la protección de transporte estricto, permitiendo ataques de degradación de protocolo.
[MEDIUM] Cookies sin atributo SameSite: La ausencia de este flag en la cookie de afinidad hace al sitio vulnerable a ataques de falsificación de solicitud en sitios cruzados (CSRF).
[MEDIUM] Referrer-Policy y Permissions-Policy: No se limitan los datos de navegación compartidos ni el acceso a funciones del dispositivo como cámara o micrófono.
[LOW] Cabeceras de tecnología expuestas: Las cabeceras Server y X-Powered-By revelan el uso de Microsoft-IIS/10.0 y ASP.NET, facilitando el reconocimiento a atacantes.
[LOW] Archivos de indexación faltantes: La ausencia de robots.txt y sitemap.xml dificulta la gestión adecuada del rastreo y seguridad de directorios.