EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://soluciones.linea.pe/plataformas/bo	Checks	9 pruebas
Dominio	soluciones.linea.pe	Hallazgos	43 totales
Fecha	27 de marzo de 2026 a las 21:48	Problemas	11 detectados

C

61/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de seguridad realizado a la plataforma arroja una puntuación de 61/100, lo que equivale a una calificación de grado C. Se ejecutaron 9 checks pasivos, de los cuales 6 resultaron satisfactorios y 3 presentaron fallos críticos relacionados con la configuración del servidor. Aunque el cifrado SSL es correcto y el entorno no expone vulnerabilidades de CMS conocidos, la ausencia total de cabeceras de seguridad y la falta de redirección HTTPS representan riesgos significativos. Debido a estas omisiones técnicas en la protección del tráfico y la integridad del navegador, el sitio se considera vulnerable ante ataques de interceptación y suplantación. Es imperativo aplicar las correcciones recomendadas para fortalecer la postura defensiva del portal.

Resumen de Riesgos

0	5	3	3	32
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 312 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	100	OK	No se encontraron cookies
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	20	FALLO	Faltan robots.txt y sitemap.xml
Puertos Abiertos	100	OK	No se detectaron puertos abiertos

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 312 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  312 dias restantes (expira: 2027-02-02T23:59:59.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2026-01-30T00:00:00.000Z
- 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

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Next.js, 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
- 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 200 — No redirige a HTTPS
- 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

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**
  React, Next.js, Next.js, 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 — 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 — 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 — 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 ausente: El servidor permite conexiones inseguras a través del puerto 80 sin redirigir al protocolo seguro.
[HIGH] HSTS (Strict-Transport-Security) faltante: No se obliga al navegador a usar conexiones cifradas, facilitando ataques de degradación de SSL.
[HIGH] Content-Security-Policy (CSP) faltante: La ausencia de esta política permite la ejecución de scripts no autorizados y ataques de inyección de contenido (XSS).
[HIGH] X-Frame-Options faltante: El sitio puede ser embebido en marcos externos, lo que lo hace vulnerable a ataques de clickjacking.
[MEDIUM] X-Content-Type-Options faltante: El navegador podría interpretar archivos como tipos MIME diferentes a los declarados, permitiendo la ejecución de código malicioso.
[MEDIUM] Referrer-Policy faltante: No se controla qué información de procedencia se envía a otros sitios, lo que puede derivar en fugas de datos sensibles en las URLs.
[MEDIUM] Permissions-Policy faltante: No se restringe el acceso a funciones del navegador como la cámara, el micrófono o la geolocalización desde el contexto de la web.

[LOW] X-Powered-By expuesto: El encabezado revela el uso de Next.js y ASP.NET, facilitando a un atacante la búsqueda de exploits específicos para estas tecnologías.
[LOW] Archivos robots.txt y sitemap.xml no encontrados: La ausencia de estos archivos dificulta la auditoría de indexación y el control de rastreo por motores de búsqueda.