EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://mail.regioncallao.gob.pe	Checks	9 pruebas
Dominio	mail.regioncallao.gob.pe	Hallazgos	45 totales
Fecha	14 de junio de 2026 a las 03:21	Problemas	9 detectados

C

72/100

puntos de seguridad

RESUMEN EJECUTIVO

El análisis de ciberseguridad realizado sobre el portal institucional arroja una puntuación de 72/100, lo que equivale a una calificación de grado C. Se ejecutaron un total de 9 verificaciones pasivas, de las cuales 5 resultaron satisfactorias, 2 generaron advertencias y 1 se identificó como fallo crítico de configuración. El sitio web demuestra una implementación robusta en su cifrado de transporte, pero presenta deficiencias significativas en las políticas de seguridad del servidor y en la protección de las sesiones de usuario. En su estado actual, el sitio se considera vulnerable a ataques de inyección de contenido y secuestro de sesiones debido a la ausencia de cabeceras de protección modernas.

Resumen de Riesgos

0	3	5	1	36
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 214 dias
Cabeceras de Seguridad	15	FALLO	Solo 1/6 presentes. Faltan: Content-Security-Pol...
Redireccion HTTPS	0	ERROR	No se pudo verificar la redireccion 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	50	AVISO	ZM_TEST: falta HttpOnly; ZM_TEST: falta SameSite...
Contenido Mixto	100	OK	No se detecto contenido mixto
Robots.txt y Sitemap	60	AVISO	Falta sitemap.xml
Puertos Abiertos	100	OK	2 puerto(s) abierto(s), todos esperados

SSL/TLS — 100/100

Estado: OK

Certificado valido, expira en 214 dias

- INFO **Certificado valido**
  El certificado SSL es valido y de confianza
- INFO **Dias hasta expiracion**
  214 dias restantes (expira: 2027-01-13T18:24:07.000Z)
- INFO **Fecha de emision**
  Emitido desde: 2025-12-12T18:24:08.000Z
- INFO **Puerto 443**
  Conexion HTTPS establecida correctamente en puerto 443

Cabeceras de Seguridad — 15/100

Estado: FALLO

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

- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido

- INFO **X-Frame-Options**
  Presente: SAMEORIGIN
- 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.)

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 — 50/100

Estado: AVISO

ZM_TEST: falta HttpOnly; ZM_TEST: falta SameSite; ZM_LOGIN_CSRF: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- ALTO **Cookie: ZM_TEST — HttpOnly**
  Falta HttpOnly — Cookie accesible via document.cookie (riesgo XSS)
- INFO **Cookie: ZM_TEST — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: ZM_TEST — SameSite**
  Falta SameSite — Vulnerable a CSRF
- INFO **Cookie: ZM_LOGIN_CSRF — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: ZM_LOGIN_CSRF — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- MEDIO **Cookie: ZM_LOGIN_CSRF — 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 — 60/100

Estado: AVISO

Falta sitemap.xml

- INFO **robots.txt**
  Presente (25 bytes)
- INFO **Reglas robots.txt**
  0 Disallow, 1 Allow
- BAJO **sitemap.xml**
  No encontrado (HTTP 404)
- BAJO **security.txt**
  No encontrado — Recomendado para politica de divulgacion

Puertos Abiertos — 100/100

Estado: OK

2 puerto(s) abierto(s), todos esperados

- 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
- 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] Content-Security-Policy: La ausencia de esta cabecera permite ataques de Cross-Site Scripting (XSS) y la inyección de scripts maliciosos en el navegador del usuario.
[HIGH] Strict-Transport-Security: No se detectó la cabecera HSTS, lo que deja a los usuarios expuestos a ataques de degradación de protocolo y robo de información en redes no seguras.
[HIGH] Cookie ZM_TEST (HttpOnly): Esta cookie carece del atributo HttpOnly, permitiendo que scripts maliciosos accedan a ella mediante el DOM del navegador, facilitando el robo de identidad.
[MEDIUM] X-Content-Type-Options: El servidor no previene el MIME-sniffing, lo que podría permitir que archivos cargados sean interpretados de forma malintencionada por el navegador.

[MEDIUM] Referrer-Policy: La falta de esta política provoca que el sitio no controle qué información de navegación se envía a terceros al seguir enlaces externos.
[MEDIUM] Permissions-Policy: No se han definido restricciones sobre el uso de APIs del navegador, como la cámara o geolocalización, dentro del contexto del sitio.
[MEDIUM] Cookie ZM_TEST (SameSite): La ausencia de este atributo incrementa el riesgo de ataques de Falsificación de Petición en Sitios Cruzados (CSRF).
[MEDIUM] Cookie ZM_LOGIN_CSRF (SameSite): Al no tener definido el atributo SameSite, esta cookie técnica es vulnerable a manipulaciones externas que podrían comprometer la sesión.
[LOW] sitemap.xml: No se encontró el mapa del sitio, lo cual dificulta el análisis preventivo de la estructura web y la indexación correcta.