EscanearVulnerabilidades

Informe de Seguridad Web

URL	https://sgd.regioncallao.gob.pe/sisdoc/login.do	Checks	9 pruebas
Dominio	sgd.regioncallao.gob.pe	Hallazgos	47 totales
Fecha	14 de junio de 2026 a las 03:18	Problemas	9 detectados

B

77/100

puntos de seguridad

RESUMEN EJECUTIVO

La auditoría de seguridad realizada al sitio web ha arrojado una puntuación de 77/100, lo que equivale a una nota B. Durante el proceso se ejecutaron 9 checks pasivos, resultando en 5 verificaciones exitosas, 1 advertencia y 2 fallos críticos en la configuración. Aunque el cifrado de datos es sólido, existen carencias importantes en las políticas de seguridad del navegador y en la protección de sesiones. En su estado actual, el sitio se considera vulnerable a ataques de inyección y suplantación de identidad debido a la falta de cabeceras defensivas esenciales.

Resumen de Riesgos

0	2	3	4	38
CRITICO	ALTO	MEDIO	BAJO	INFO

Resumen de Checks

SSL/TLS	100	OK	Certificado valido, expira en 214 dias
Cabeceras de Seguridad	30	FALLO	Solo 2/6 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	83	AVISO	JSESSIONID: falta SameSite
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	1 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 — 30/100

Estado: FALLO

Solo 2/6 presentes. Faltan: Content-Security-Policy, Strict-Transport-Security, Referrer-Policy, Permissions-Policy

- BAJO **Server header expuesto**
  Server: Payara Server 5.2020.2 #badassfish — Revela tecnologia del servidor

- BAJO **X-Powered-By expuesto**
  X-Powered-By: Servlet/4.0 JSP/2.3 (Payara Server 5.2020.2 #badassfish Java/Oracle Corporation/1.8) — Revela framework/lenguaje
- ALTO **Content-Security-Policy**
  Falta — Previene XSS y ataques de inyeccion de contenido
- INFO **X-Frame-Options**
  Presente: DENY
- 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.)

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**
  Servlet/4.0 JSP/2.3 (Payara Server 5.2020.2 #badassfish Java/Oracle Corporation/1.8)

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

JSESSIONID: falta SameSite

- INFO **Cookies detectadas**
  2 cookie(s) encontrada(s)
- INFO **Cookie: key — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: key — Secure**
  Flag Secure activo — Solo se envia por HTTPS

- INFO **Cookie: key — SameSite**
  SameSite=strict
- INFO **Cookie: JSESSIONID — HttpOnly**
  HttpOnly activo — No accesible via JavaScript
- INFO **Cookie: JSESSIONID — Secure**
  Flag Secure activo — Solo se envia por HTTPS
- MEDIO **Cookie: JSESSIONID — 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 — 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

1 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)**
  Cerrado — 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] Falta de Content-Security-Policy: La ausencia de esta cabecera permite la ejecución de scripts maliciosos y ataques de inyección de contenido (XSS).

[HIGH] Falta de Strict-Transport-Security: El sitio no obliga al uso de conexiones seguras mediante HSTS, permitiendo ataques de interceptación de tráfico.
[MEDIUM] Cookie JSESSIONID sin atributo SameSite: La falta de esta instrucción en la cookie de sesión facilita ataques de falsificación de peticiones en sitios cruzados (CSRF).
[MEDIUM] Falta de Referrer-Policy: No se controla la información de procedencia enviada a otros dominios, lo que puede filtrar URLs internas sensibles.
[MEDIUM] Falta de Permissions-Policy: El servidor no restringe el acceso de la aplicación a funciones del hardware del usuario como cámara o micrófono.
[LOW] Cabecera Server expuesta: Se revela el uso de Payara Server 5.2020.2, entregando información valiosa a atacantes sobre la infraestructura técnica.
[LOW] Cabecera X-Powered-By expuesta: Indica el uso de Java y Servlet/JSP, facilitando la búsqueda de exploits específicos para esas versiones.
[LOW] Ausencia de robots.txt y sitemap.xml: La falta de estos archivos dificulta la correcta indexación y gestión del rastreo por parte de buscadores.