



MEMORANDUM DINAPI/DAII N° 069/2026

A : José Ramírez, Director Interino.
Dirección de Informática

DE : C.P. Sergio Penayo, Director Interino.
Dirección de Auditoría Interna Institucional

REF. : Remitir INFORME FINAL DAII/AI N° 01/2026 Auditoría Informática a la
Aplicación Web Institucional Joajú.

FECHA : 08/06/2026.



Me dirijo a Usted, en el marco de los trabajos de Auditoría Informática a la Aplicación Web Institucional Joajú, en cumplimiento del Plan de Trabajo Anual (PTA) Versión 01 de esta Dirección de Auditoría Interna Institucional aprobado por Resolución DINAPI N° 482/2025 donde se establece la realización de una Auditoría Informática dentro del Primer Semestre del presente Ejercicio Fiscal.

En tal sentido, se remite en formato físico el INFORME FINAL DAII/AI N° 01/2026, se aclara que el presente informe contiene los hallazgos con sus respectivos descargos levantados en la Plataforma del SIAGPE, como así también el análisis realizado sobre los mismos, determinando el levantamiento o no de las observaciones.

En vista de los hallazgos ratificados por la Auditoría Informática, se establece un **plazo de 5 (cinco) días hábiles** a partir del día siguiente de la recepción del Informe Final, a los efectos de elaborar un Plan de Mejoramiento Funcional, con las acciones de mejora a tomar, periodo de ejecución, evidencias de cumplimiento y responsables.

Dicho Plan de Mejoramiento Funcional, deberá ser remitido en formato físico a esta Dirección de Auditoría Interna Institucional para su evaluación antes de la carga en el SIAGPE.

Sin otro particular, me despido de usted muy atentamente.


Lic. Adrian Steven Gray Murray
Jefe Interino Dpto. de Infraestructura Tecnológica
Dirección de Informática
Dirección Nacional de Propiedad Intelectual

08/06/26
12:45 h.s.



MEMORANDUM DINAPI/DAII N° 070/2026

PARA : Abg. CLAUDIA LORENA FRANCO Q., Directora Nacional
Dirección Nacional de Propiedad Intelectual

DE : C.P. Sergio Daniel Penayo, Director Interino
Dirección de Auditoría Interna Institucional

REF. : Remitir para conocimiento el INFORME FINAL DAII/AI N° 01/2026
Auditoría Informática a la Aplicación Web Institucional Joajú.

FECHA : 08/06/2026



Me place saludarle, y por este medio remitir para su conocimiento, el INFORME FINAL DAII/AI N° 01/2026 AUDITORIA INFORMATICA A LA APLICACIÓN WEB INSTITUCIONAL JOAJÚ.

Dicha Auditoría Informática se ha realizado, en cumplimiento del Plan de Trabajo Anual (PTA) Versión 1 de esta Dirección de Auditoría Interna Institucional aprobado por Resolución DINAPI N° 482/2025.

El presente INFORME FINAL, contiene los hallazgos con sus respectivos descargos levantados en la Plataforma del SIAGPE, como así también el análisis realizado con las recomendaciones del Auditor Informático sobre los mismos.

Se concluye que de los 5 (cinco) hallazgos encontrados, los mismos corresponden a vulnerabilidades con carácter medias y bajas que no revisten de gravedad, de las cuales 4 (cuatro) ya fueron mitigadas por la Dirección de Informática, quedando 1 (un) hallazgo a ser subsanado por medio de un Plan de Mejoramiento Funcional a ser elaborado por dicha Dirección.

Sin otro particular, me despido de usted con mi consideración más distinguida.

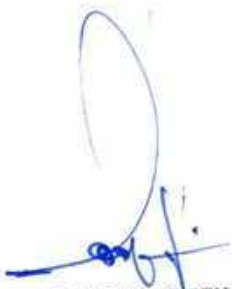
Se adjunta al presente MEMORANDUM INFORME FINAL DAII/AI N° 01/2026
conteniendo 58 páginas.

DIRECCIÓN NACIONAL DE PROPIEDAD INTELECTUAL	
Secretaría General - Mesa de Entrada	
Expediente N°:	1804
Fecha:	08-06-2026 Hora: 12:53
Fojas:	01.- Obs. ad: Cuadrante 60 V-fijos
Recibido por:	Diego Lopez



INFORME FINAL
DAII/AI N° 01/2026
***“AUDITORÍA AL SISTEMA
WEB INSTITUCIONAL
JOAJÚ”***

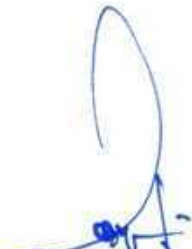
AÑO 2026


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual



INDICE

CONTENIDO	N° PÁGINA
I. IDENTIFICACIÓN DE LA ENTIDAD	3
II. ANTECEDENTES DE LA AUDITORÍA	4
III. OBJETIVOS DE LA AUDITORÍA	4
IV. ALCANCE DE LA AUDITORÍA	5
V. PROCEDIMIENTOS DE AUDITORÍA	5 - 9
VI. RIESGO E IMPORTANCIA RELATIVA	9
VII. TIPOS DE INFORMES	9
VIII. DESARROLLO DE LA AUDITORIA	9-14
IX. CONCLUSION FINAL	14
X. RECOMENDACIÓN FINAL	14
XI. PLAN DE MEJORAMIENTO	14
XII. ANEXO 1 - Minuta de Reunión 01	16 - 18
XIII. ANEXO 2 - Minuta de Reunión 02	19 - 20
XIV. ANEXO 3 - Escaneo Joajú	21 - 56
XV. ANEXO 4 - Evidencias Técnicas	57 - 58


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977


Página web: www.dinapi.gov.py

Página 2 de 58

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

INFORME FINAL DAI/AI N° 01/2026

AUDITORÍA INFORMÁTICA – SISTEMA WEB JOAJÚ

I. IDENTIFICACIÓN DE LA INSTITUCIÓN

La DINAPI es una institución autónoma y autárquica, creada por la Ley N°4798/2012 como órgano de ejecución de la política nacional de Propiedad Intelectual. Se relaciona con el Poder Ejecutivo, a través del Ministerio de Industria y Comercio.

Con su creación en el año 2012 la DINAPI pasó a asumir las funciones de dos antiguas direcciones dependientes del Ministerio de Industria y Comercio: la Dirección General de Propiedad Intelectual y la Dirección Nacional de Derecho de Autor.

Por mandato legal, la DINAPI aplica en el área administrativa las normas destinadas a la protección de los derechos de propiedad intelectual, de acuerdo con lo dispuesto en la Constitución Nacional, las leyes, los tratados y los convenios internacionales del ámbito ratificados por el Paraguay.

MISIÓN

Proteger, promover y defender los derechos de Propiedad Intelectual, propiciando la creatividad e innovación para el desarrollo sostenible del Paraguay.

VISIÓN

Proteger, promover y defender los derechos de Propiedad Intelectual, propiciando la creatividad e innovación para el desarrollo sostenible del Paraguay.

FUNCIONES DE LA INSTITUCIÓN

- ✓ Administrar y disponer el otorgamiento y protección de los derechos de propiedad intelectual, como ser: Derechos de Autor y Derechos Conexos, Marcas, Dibujos y Modelos Industriales, Patentes de Invención y de Modelos de Utilidad, Transferencia de Tecnología, Indicaciones Geográficas y otras que pudieran legislarse o reglamentarse.
- ✓ Promover y fomentar la creación intelectual, tanto en su forma literaria, artística o científica, como en su ámbito de aplicación industrial, y la difusión de los conocimientos tecnológicos dentro de los sectores culturales y productivos.
- ✓ Administrar eficazmente los Activos de Propiedad Intelectual para propiciar la protección y uso consentido, en beneficio de nuestro país, de nuestros recursos genéticos autóctonos.
- ✓ Fomentar la creación y desarrollo de empresas culturales.
- ✓ Propiciar el reconocimiento y la utilización de los conocimientos tradicionales indígenas, a favor de los pueblos originarios.
- ✓ Fomentar la innovación, la investigación y el acceso a la ciencia, favoreciendo la transferencia de tecnología.
- ✓ Representar a los intereses nacionales, en tratados y convenios de cooperación con entidades y países en materia de Propiedad Intelectual.
- ✓ Formular las políticas nacionales en todas aquellas materias relacionadas con la protección de la propiedad intelectual, en coordinación con los ministerios y demás órganos competentes para cada caso.



- ✓ Promover iniciativas y desarrollar actividades conducentes al mejor conocimiento y protección de la Propiedad Intelectual, en el orden nacional.
- ✓ Dictar las reglamentaciones técnicas para la ejecución de cualquier actividad de su competencia en todo el territorio nacional, de acuerdo con la legislación pertinente.
- ✓ Celebrar convenios y contratos, para el cumplimiento de sus fines, con organismos nacionales públicos o privados, Gobernaciones y/o Municipios; así como con organismos internacionales, previa autorización de las instancias pertinentes.
- ✓ Registrar, habilitar y fiscalizar a personas jurídicas, públicas o privadas encargadas de la gestión colectiva de derecho de autor, así como de la titularidad de marcas de certificación o marcas colectivas, indicaciones geográficas y en general a todas aquellas que se creen para la representación y gestión de Derechos de la Propiedad Intelectual.
- ✓ Propiciar la participación del sector industrial y universitario en el desarrollo y aplicación de tecnologías que incrementen su calidad, competitividad y productividad; así como realizar investigaciones sobre el avance y aplicación de la tecnología industrial, nacional e internacional y su incidencia en el cumplimiento de tales objetivos, pudiendo proponer a su vez políticas para fomentar su desarrollo.
- ✓ Coordinar las tareas de negociación nacional e internacional que correspondan al ámbito de competencia, conjuntamente con el Ministerio de Relaciones Exteriores y de otras reparticiones públicas afectadas.
- ✓ Establecer y percibir las tasas que por diversos conceptos se deban abonar, de conformidad con las normas vigentes y la presente Ley.
- ✓ Establecer y percibir aranceles por servicios prestados.
- ✓ Establecer las exoneraciones y reducciones de tasas y aranceles establecidas en la presente Ley en los siguientes casos:
 - Situación de insolvencia económica.
 - Promoción de la Política Nacional de apoyo a micro y pequeñas empresas.
 - Políticas de Desarrollo sectorial de la economía establecidas por el Poder Ejecutivo.

II. ANTECEDENTES DE LA AUDITORÍA

Por **Resolución DINAPI N° 482/2025 “POR LA CUAL SE APRUEBA EL PLAN DE TRABAJO ANUAL PARA EL EJERCICIO FISCAL 2026 DE LA DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL, DE LA DIRECCIÓN NACIONAL DE PROPIEDAD INTELECTUAL – DINAPI”**.

III. OBJETIVOS DE LA AUDITORÍA

• OBJETIVO GENERAL

Evaluar de manera integral el nivel de seguridad de la aplicación web JO'AJU (www.joaju.dinapi.gov.py), mediante la identificación y análisis de vulnerabilidades críticas alineadas al estándar internacional OWASP Top 10, con el fin de determinar el nivel de exposición al riesgo y proponer medidas de mitigación que garanticen la confidencialidad, integridad y disponibilidad de la información gestionada por la aplicación.

• OBJETIVOS ESPECÍFICOS

1. Identificar y analizar vulnerabilidades presentes en la aplicación web JO'AJU, incluyendo inyecciones, fallas de autenticación, exposición de datos sensibles, control de acceso roto, XSS, deserialización insegura y uso de componentes vulnerables, siguiendo los lineamientos del OWASP Top 10.
2. Verificar la efectividad de los controles de seguridad implementados en la aplicación, tales como autenticación, gestión de sesiones, cifrado de datos, permisos de acceso y registro de eventos críticos.
3. Realizar pruebas automatizadas y manuales, mediante la herramienta OWASP ZAP y validaciones manuales según la OWASP Testing Guide, para asegurar la cobertura completa de los riesgos identificados.
4. Evaluar el nivel de riesgo de los hallazgos considerando su impacto potencial en la confidencialidad, integridad y disponibilidad de la información, así como la probabilidad de explotación de las vulnerabilidades detectadas.
5. Proponer medidas de mitigación y recomendaciones para corregir las vulnerabilidades identificadas, fortaleciendo la seguridad de la aplicación y alineándola con buenas prácticas.

IV. ALCANCE DE LA AUDITORÍA

El trabajo de Auditoría se realizará en base a los procedimientos considerados en el Manual de Auditoría Gubernamental y el Encargo de Auditoría con el fin de cumplir lo estipulado en la **Resolución DINAPI N° 482/2025 "POR LA CUAL SE APRUEBA EL PLAN DE TRABAJO ANUAL PARA EL EJERCICIO FISCAL 2026 DE LA DIRECCIÓN DE AUDITORÍA INTERNA INSTITUCIONAL, DE LA DIRECCIÓN NACIONAL DE PROPIEDAD INTELECTUAL – DINAPI"**.

V. PROCEDIMIENTOS DE AUDITORÍA

1. Definición del Alcance (Scope):

La delimitación operativa de la auditoría técnica sobre la Aplicación Web Institucional Joajú se estableció formalmente mediante la concertación de los siguientes parámetros metodológicos y administrativos entre las áreas intervinientes:

- **Ambiente y Objetivos Evaluados:** El alcance técnico se circunscribió al análisis de la plataforma Joajú bajo el dominio institucional <https://joaju.dinapi.gov.py>, incluyendo las llamadas e interacciones síncronas hacia servicios externos automatizados por el entorno durante la ejecución de las pruebas.
- **Marco de Referencia Metodológico:** Se determinó la aplicación del estándar internacional **OWASP Top 10** como el marco conceptual y regulatorio para la identificación, evaluación y categorización de las vulnerabilidades y riesgos en la capa de la aplicación web.
- **Ventana Operativa y Mitigación de Impacto:** A efectos de preservar la disponibilidad del servicio y evitar afectaciones a la experiencia de usuario, se dispuso la ejecución de las actividades en días hábiles y horarios específicos con baja concurrencia o nula atención al público.
- **Reglas de Compromiso y Permisibilidad Técnica:** Se acordó la asignación de un equipo informático exclusivo para el escaneo, gestionando la inclusión de su dirección

IP en una lista de excepciones temporales dentro de los mecanismos de seguridad perimetral (Firewall y WAF).

Evidencia: El fundamento administrativo y la aprobación de los términos del alcance técnico se encuentran debidamente refrendados en el documento institucional **MINUTA DE REUNIÓN N° 01** de fecha 08/04/2026, el cual se encuentra incorporado en el **Anexo 1** del presente informe.

Dicho documento consolida los aspectos tratados en la reunión realizada en las oficinas de la Dirección de Informática de la DINAPI, la designación de la contraparte técnica como enlace operativo y las firmas en conformidad de los actores intervinientes de ambas dependencias.

2. Recolección de Información Técnica:

Se procedió a realizar una inspección manual y estructurada de la aplicación web a través de su interfaz pública (página de inicio y secciones indexadas). Este procedimiento tuvo como objetivo mapear de forma interactiva los puntos de entrada, analizar el comportamiento de las respuestas del servidor frente a la navegación ordinaria, identificar la arquitectura de tecnologías expuestas (frontend/backend) y definir la superficie de ataque inicial.

Evidencia: Registro de identificación tecnológica (*fingerprinting*) obtenido a partir del análisis de código y cabeceras del sitio <https://joaju.dinapi.gov.py> (los datos técnicos presentados a continuación se encuentran respaldados y detallados en las páginas 10, 12, 18, 19 y 24 del documento Escaneo Joajú del **Anexo 3**):

- a. **Componente Analizado:** Servidor Web
 - *Detalle Técnico Detectado:* Nginx
 - *Indicador / Evidencia Técnica:* Cabecera de respuesta HTTP: Server: nginx
 - *Ubicación en Respaldo:* **Páginas 10 y 12**
- b. **Componente Analizado:** Arquitectura Base
 - *Detalle Técnico Detectado:* Single Page Application (SPA)
 - *Indicador / Evidencia Técnica:* Estructura de enrutamiento por bloques mediante archivos estáticos .js (Ej: chunk-FKBIZCJJ.js)
 - *Ubicación en Respaldo:* **Páginas 18 y 19**
- c. **Componente Analizado:** Herramientas de Terceros
 - *Detalle Técnico Detectado:* Google Tag Manager
 - *Indicador / Evidencia Técnica:* Script de analítica indexado en el DOM: src="https://www.googletagmanager.com/gtag/js?id=G-E7S0ZWGY21"
 - *Ubicación en Respaldo:* **Páginas 12 y 24**

3. Escaneo Automatizado con OWASP ZAP:

Se procedió a la ejecución de las pruebas dinámicas automatizadas sobre la plataforma utilizando la herramienta de auditoría **OWASP ZAP (Zed Attack Proxy) Versión 2.17.0 (Checkmarx)**.

Este procedimiento se llevó a cabo en un ambiente controlado, utilizando un equipo informático provisto para el efecto por la Dirección de Informática de la institución.



Las pruebas técnicas se ejecutaron con el acompañamiento y presencia en el sitio de la **Lic. Claudia Dacak** y el **Lic. Adan Gray**, ambos funcionarios técnicos de la dependencia citada, garantizando la supervisión directa del procedimiento, asimismo se aplicaron políticas de escaneo estandarizadas de la herramienta para identificar fallos de configuración de seguridad, debilidades en los encabezados de respuesta y vectores potenciales de ataque en el entorno evaluado.

Evidencia: El marco institucional, la autorización del entorno controlado y las reglas de compromiso técnico de este procedimiento se encuentran formalizados en el documento **MINUTA DE REUNIÓN N° 02**, (Ver **Anexo 2** de este informe), cuyos datos de trazabilidad se resumen a continuación:

- **Tema Oficial:** Escaneo con el Software OWASP ZAP Proxy sobre la aplicación web <https://joaju.dinapi.gov.py/>.
- **Fecha y Ventana Horaria:** 07 de mayo de 2026 | Inicio: 14:18 hs. - Fin: 14:37 hs.
- **Lugar de Ejecución:** Dirección de Informática (DINAPI).
- **Responsable de Auditoría:** Lic. Diego González Quiroz (Auditor Informático).
- **Funcionarios Técnicos Intervinientes (Testigos de Carga):**
 - Lic. Claudia Dacak (Dpto. Control de Calidad).
 - Lic. Adan Gray (Dpto. de Infraestructura).
- **Aspectos Técnicos Tratados y Asentados:**
 - Inicio del escaneo de la aplicación web institucional con la herramienta OWASP ZAP configurada en modo ataque / escaneo pentest.
 - Monitoreo y constatación del correcto comportamiento del servidor durante las pruebas.
 - Conclusión exitosa del proceso y generación del informe técnico de escaneo en formato HTML.

4. Pruebas Manuales de Validación:

Una vez concluidas las fases de reconocimiento superficial y escaneo automatizado, se procedió a una etapa de **validación analítica manual** sobre los resultados preliminares obtenidos por la herramienta OWASP ZAP. Este procedimiento es indispensable en la metodología de auditoría para filtrar falsos positivos, comprobar la explotabilidad real de las alertas y asegurar el correcto diagnóstico del entorno. Las acciones ejecutadas comprendieron:

- **Análisis y Descarte de Falsos Positivos:** Se revisaron manualmente las cabeceras de respuesta y los códigos de estado HTTP devueltos por el servidor para confirmar si las alertas de riesgo clasificadas por el software correspondían a vulnerabilidades efectivas en el contexto de la aplicación Joajú.
- **Constatación en Ambiente Controlado:** En concordancia con lo asentado en la **Minuta de Reunión N° 02**, se verificó visual y técnicamente el comportamiento de la aplicación web durante la ejecución de las sondas automáticas, asegurando que los vectores de ataque lanzados fueran procesados por el backend sin alterar la disponibilidad del servicio.
- **Validación de la Superficie de Exposición:** Se examinaron de forma dirigida los puntos de entrada (formularios y scripts de terceros como Google Tag Manager) identificados en el escaneo para determinar el impacto real de la ausencia de directivas de seguridad en las cabeceras HTTP expuestas.

Evidencia: El soporte técnico e instrumental de estas validaciones analíticas se encuentra consolidado directamente en el encabezado y volcado de datos del reporte digital generado por la herramienta OWASP ZAP (**Anexo 3 Escaneo Joajú**).

Este registro certifica de manera objetiva la trazabilidad en tiempo real de las peticiones de análisis y la inspección de cabeceras, ejecutadas de forma automatizada y síncrona entre las 14:18:00 y las 14:36:24 hs; consolidando en su estructura las respuestas directas emitidas por el backend de la aplicación para validar analíticamente los códigos de estado y la ausencia de directivas de seguridad en el entorno evaluado.

5. Análisis y Evaluación de Riesgos:

La herramienta **OWASP ZAP** realizó de manera autónoma la estructuración y contextualización de los riesgos asociados a los hallazgos identificados. Dicho software determinó el nivel de exposición de la plataforma Joajú mediante la aplicación de los siguientes criterios metodológicos incorporados en el procedimiento de análisis y evaluación de los riesgos encontrados:

- **i. Clasificación Automática de Criticidad:** Las vulnerabilidades detectadas fueron categorizadas y ponderadas de forma automatizada por el algoritmo de la herramienta en niveles de severidad **Alta, Media o Baja**, atendiendo a la naturaleza técnica intrínseca de cada fallo registrado en el reporte.
- **ii. Evaluación Automatizada de Impacto Potencial:** El motor analítico del software calculó de manera directa cómo la explotación de cada alerta podría llegar a comprometer los pilares de **Confidencialidad, Integridad y Disponibilidad** en el entorno evaluado, asignando un factor de criticidad estándar según el vector detectado.
- **iii. Estimación de Probabilidad de Explotación:** A partir del análisis de la superficie de exposición, la herramienta determinó sincronamente la probabilidad de que un actor malicioso aproveche con éxito las debilidades y la ausencia de cabeceras de seguridad identificadas en las solicitudes.
- **iv. Generación de Matriz de Riesgos y Prioridades:** Los datos analíticos recopilados por el software fueron consolidados de forma nativa en un esquema ordenado que vincula cada hallazgo técnico con su nivel de riesgo y su nivel de confianza, sirviendo como matriz operativa para definir la prioridad de las acciones de mitigación.

Evidencia: El soporte técnico e instrumental de este análisis de riesgos se encuentra indexado en las secciones de métricas y en el resumen de alertas por severidad del reporte digital generado por **OWASP ZAP** (ver **Anexo 3**), cuyo sistema de escaneo procesó de manera síncrona los hallazgos clasificados en la ventana de control establecida.

6. Documentación y Elaboración del Informe:

El motor analítico de la herramienta **OWASP ZAP** ejecutó de manera autónoma el procesamiento, registro y estructuración documental de los resultados obtenidos sobre la plataforma Joajú, cumpliendo de forma automatizada con los siguientes requerimientos informativos:

- **i. Registro Automatizado de Evidencias Técnicas:** El software indexó y almacenó de manera sistemática la totalidad de los hallazgos identificados durante el escaneo, adjuntando de forma nativa las evidencias técnicas correspondientes a las peticiones (*requests*) y respuestas (*responses*) HTTP completas que justifican cada alerta en el entorno evaluado.
- **ii. Generación de Recomendaciones y Medidas de Mitigación:** La base de conocimiento integrada en el algoritmo de la herramienta asoció de forma automática a cada vulnerabilidad detectada una descripción técnica detallada, junto con sus



respectivas soluciones sugeridas y pautas globales de mitigación para su posterior aplicación por parte de la dependencia técnica.

- **iii. Consolidación de Hallazgos en Reporte Técnico:** La aplicación informática unificó la totalidad de las métricas, criticidades y descargas técnicas de la sesión en un único formato estructurado, sirviendo este documento digital generado de manera inmediata como la base informativa e instrumental tanto para el análisis preliminar como para el cierre del informe final de auditoría.

Evidencia: El soporte técnico e instrumental de esta fase documental se encuentra consolidado en la estructura del reporte técnico final generado de forma automatizada por la herramienta OWASP ZAP (ver **Anexo 3**), cuyo sistema de exportación unificó de manera sincrónica la totalidad de los datos de prueba e inyecciones, las soluciones recomendadas y el desglose de alertas en la ventana de control establecida.

VI. RIESGO E IMPORTANCIA RELATIVA

- **Falta de autorización para pruebas técnicas:** La auditoría requiere permiso formal del área de informática para ejecutar escaneos automatizados y pruebas manuales. La ausencia de esta autorización puede impedir la ejecución del plan.
- **Acceso limitado a la aplicación o módulos restringidos:** La imposibilidad de acceder a ciertos módulos, endpoints o servicios puede limitar la cobertura de la auditoría y dejar vulnerabilidades sin identificar.
- **Impacto en la disponibilidad de la aplicación:** Las pruebas activas podrían, de manera inadvertida, afectar temporalmente el funcionamiento de JO'AJU. Se requiere coordinación y pruebas controladas.
- **Colaboración insuficiente del área de informática:** La falta de respuesta o apoyo del personal encargado de la aplicación puede retrasar la auditoría o impedir la recolección de información crítica.
- **Limitaciones técnicas de las herramientas:** Algunas vulnerabilidades complejas (XSS avanzado, deserialización insegura, control de acceso específico) requieren validación manual y podrían no ser detectadas automáticamente por OWASP ZAP.
- **Confidencialidad de la información:** La exposición involuntaria de datos sensibles durante la auditoría debe gestionarse adecuadamente para garantizar la protección de la información de usuarios y la institución.

VII. TIPOS DE INFORMES

- Borrador de Informe para descargo.
- Informe Final.

VIII. DESARROLLO DE LA AUDITORIA

Durante la ejecución del escaneo de vulnerabilidades con OWASP ZAP sobre el portal <https://joaju.dinapi.gov.py>, se identificaron cinco (5) hallazgos relacionados a la configuración de seguridad (Hardening) perimetral, los cuales se detallan a continuación:

HALLAZGO N° 01

Título del Hallazgo: Cabecera de Política de Seguridad de Contenidos (CSP) no configurada.

- **Gravedad:** Media
- **Confianza del Escáner:** Alta

- **Identificadores:** CWE-693, WASC-15, OWASP 2025-A02

Se ha verificado que la aplicación bajo análisis no cuenta con el encabezado estándar Content-Security-Policy (CSP) configurado en el servidor web. Esto fue evidenciado de manera consistente al solicitar recursos del sitio como por ejemplo <https://joaju.dinapi.gov.py/sitemap.xml>, donde la respuesta HTTP 200 OK del servidor web Nginx omite por completo la declaración de directivas CSP.

La falta de este control técnico significa que el navegador web del usuario final no cuenta con restricciones explícitas dictadas por el portal de la DINAPI sobre qué orígenes son válidos para la ejecución de scripts, imágenes, hojas de estilo o conexiones web sockets, elevando significativamente el impacto de explotación si existiera un vector secundario de vulnerabilidad Cross-Site Scripting (XSS).

Evidencia: Ver Evidencia Técnica en Anexo 4.

Descargo de la Dependencia Auditada:

La Dirección de Informática informa que dicho hallazgo ha sido mitigado formalmente mediante la inyección y el despliegue del encabezado HTTP de control de directivas en el servidor perimetral. La configuración restringe los orígenes para recursos críticos y fuerza solicitudes de transporte seguro.

Nota de Mitigación: Se mantuvieron activos ciertos parámetros de compatibilidad de forma temporal debido a dependencias heredadas de la arquitectura del aplicativo web, cuya remoción estructural será analizada para futuras actualizaciones del sistema.

Opinión del Auditor:

Esta Auditoría levanta el hallazgo mencionado con base en las acciones de despliegue informadas por la dependencia auditada. No obstante, considerando la subsistencia de parámetros de compatibilidad temporal derivados de dependencias heredadas de la arquitectura, se determina que la mitigación reviste un carácter condicional. La persistencia de excepciones en las directivas de seguridad restringe de forma parcial la efectividad de la protección esperada, por lo que la efectividad real del encabezado implementado quedará sujeta a una validación analítica complementaria en el siguiente ciclo de seguimiento técnico, con el fin de constatar que no existan vectores residuales permisivos.

Recomendación:

Se recomienda a la Dirección de Informática planificar y ejecutar un análisis de reingeniería estructural sobre el backend de la aplicación Joajú, orientado a la remoción definitiva de las dependencias heredadas que limitan la aplicación estricta de la seguridad perimetral. Asimismo, se insta a implementar un procedimiento de control continuo y monitoreo pasivo sobre las directivas del encabezado *Content-Security-Policy* (CSP), asegurando que cualquier actualización del sistema mantenga una configuración restrictiva y alineada con las mejores prácticas de OWASP, documentando técnicamente cada excepción autorizada bajo un esquema formal de gestión de riesgos tecnológicos.

HALLAZGO N° 02

Título del Hallazgo: Falta de Atributo de Integridad de Recursos Secundarios (Sub-resource Integrity - SRI) en scripts externos.



- **Gravedad:** Media
- **Confianza del Escáner:** Alta
- **Identificadores:** CWE-345, WASC-15, OWASP 2025-A02

Se constató que la aplicación web Joajú realiza la importación de scripts dinámicos desde plataformas e infraestructuras ajenas al dominio institucional sin implementar los mecanismos criptográficos de verificación correspondientes.

Al no contar con validación SRI, la plataforma confía ciegamente en la legitimidad de dicho recurso dinámico de terceros. Si un atacante comprometiera la infraestructura del proveedor externo (ataque de cadena de suministro), podría inyectar y ejecutar código malicioso de forma invisible para la DINAPI directamente en las sesiones activas de los usuarios concurrentes.

Evidencia: Como prueba objetiva de esta omisión técnica, el reporte de la herramienta indexó la llamada al gestor analítico externo dentro del código fuente de la plataforma (ver **Anexo 3**):

`<script async src="https://www.googletagmanager.com/gtag/js?id=G-E7S0ZWGY21"></script>` sin incluir el atributo integrity y su firma SHA-256/384.

Se verifica que dicha etiqueta omite la inclusión del atributo integrity (junto con su respectiva firma criptográfica SHA-256, SHA-384 o SHA-512) y el atributo crossorigin.

Descargo de la Dependencia Auditada:

La Dirección de Informática informa que el estado actual de dicho hallazgo se encuentra en proceso de adecuación. La inyección de los atributos criptográficos de integridad (integrity y crossorigin) en las llamadas a recursos o librerías externas compete al área de Desarrollo de Software, dado que requiere la modificación del código (frontend) del aplicativo y no puede ser resuelto estrictamente desde la capa de infraestructura perimetral. El área de desarrollo evaluará la eliminación de fuentes de terceros o la implementación de hashes estáticos, estimando su adecuación en los próximos ciclos de despliegue de código.

Opinión del Auditor:

Conforme al descargo, esta Auditoría se ratifica en el hallazgo mencionado.

Recomendación:

Se recomienda a la Dirección de Informática, a través de su Departamento de Desarrollo de Software, establecer una política de desarrollo seguro que obligue a la generación e inyección estricta de atributos *Sub-resource Integrity* (SRI) para cualquier librería, *script* o recurso externo que sea invocado en el *frontend* de las aplicaciones institucionales, y se solicita la elaboración de un Plan de Mejoramiento Funcional sobre el hallazgo en cuestión.

HALLAZGO N° 03

Título del Hallazgo: Exposición a Secuestros de Clicks por Ausencia de Cabecera Anti-Click Jacking.

- **Gravedad:** Media
- **Confianza del Escáner:** Media
- **Identificadores:** CWE-1021, WSTG-v42-CLNT-09, OWASP 2025-A02

La respuesta del servidor en su raíz no declara las directivas X-Frame-Options ni la política de CSP unificada frame-ancestors. Esta debilidad de configuración técnica permite que la interfaz del portal de Joajú pueda ser encuadrada o embebida arbitrariamente a través de elementos <iframe> en sitios webs controlados por atacantes externos.

Este escenario expone a los usuarios de la DINAPI a vectores de secuestro de clics (Clickjacking), donde mediante engaños visuales e ingeniería social, se puede manipular al usuario para que realice acciones involuntarias dentro del sistema web legítimo creyendo que interactúa con un entorno diferente.

Descargo de la Dependencia Auditada:

La Dirección de Informática informa que ha mitigado de forma definitiva el presente hallazgo mediante la declaración activa de la cabecera de protección de marcos en el servidor web, trabajando en sinergia con las directivas declaradas en la CSP, impidiendo por completo que la interfaz de Joajú sea embebida en contextos externos maliciosos o no autorizados.

Opinión del Auditor:

Esta Auditoría levanta el hallazgo mencionado con base en las acciones de reconfiguración técnica descritas por la dependencia auditada. No obstante, debido a que la efectividad declarada se vincula directamente a la sinergia con la Política de Seguridad de Contenidos (CSP)—la cual posee excepciones temporales por compatibilidad heredada—, la validación final del estado de seguridad queda supeditada a las verificaciones instrumentales automatizadas que serán ejecutadas en el próximo periodo de seguimiento técnico de la auditoría.

Recomendación:

Se recomienda a la Dirección de Informática estandarizar la directiva de enmarcamiento asegurando que la cabecera *X-Frame-Options* se encuentre explícitamente configurada con los valores estrictos DENY o SAMEORIGIN en el servidor web Nginx, operando de forma redundante e independiente a las directivas de la CSP. Asimismo, se insta a documentar formalmente esta regla de endurecimiento (*hardening*) dentro de las políticas de configuración segura de servidores de la institución, estableciendo pruebas de regresión técnica periódicas que eviten la desactivación accidental de estas cabeceras anti-clickjacking durante futuros despliegues o actualizaciones de la plataforma Joajú.

HALLAZGO N° 04

Título del Hallazgo: Ausencia de Hardening de Transporte Seguro (Strict-Transport-Security - HSTS) en Recursos Auxiliares.

- **Gravedad:** Baja
- **Confianza del Escáner:** Alta
- **Identificadores:** CWE-319, WASC-15, OWASP 2025-A02

Se evidenció que el servidor web no devuelve la directiva Strict-Transport-Security (HSTS) durante la entrega de ciertos scripts internos fundamentales de lógica y comportamiento (ej. <https://joaju.dinapi.gov.py/chunk-FKBIZCJJ.js>).

Si bien la navegación principal fuerza el tráfico HTTPS, la ausencia de una regla HSTS aplicada de forma global y exhaustiva en sub-recursos y *chunks* (fragmentos de código) del lado del cliente deja abierta la puerta a ataques locales de degradación de protocolo de comunicación (SSL

Stripping). En tales escenarios, un atacante que intercepte el canal local (ej. una red Wi-Fi no segura) podría intentar forzar la descarga de estos fragmentos dinámicos en texto plano (HTTP), comprometiendo la integridad de la aplicación.

Descargo de la Dependencia Auditada:

La Dirección de Informática informa que ha mitigado de forma definitiva el presente hallazgo mediante la inclusión global del encabezado HSTS en el servidor, garantizando que todas las conexiones entrantes y sus subdominios asociados operen obligatoriamente bajo canales cifrados HTTPS por un periodo extendido. En adición, se ejecutó un robustecimiento complementario a nivel del protocolo criptográfico TLS para optimizar el intercambio de claves seguras.

Opinión del Auditor:

Esta Auditoría levanta el hallazgo mencionado basándose en la declaración de inyección global de la política de transporte seguro implementada por la dependencia auditada.

Recomendación:

Se recomienda a la Dirección de Informática controlar la configuración del servidor perimetral Nginx para validar que la directiva *Strict-Transport-Security* (HSTS) incluya explícitamente los parámetros estructurales `includeSubDomains` y `preload`, asegurando que la cabecera se adjunte de forma irrestricta en todas las respuestas HTTP, independientemente del tipo de recurso solicitado (*scripts*, imágenes o estilos). Asimismo, se insta a documentar este nivel de robustecimiento de seguridad de la infraestructura tecnológica, estableciendo como procedimiento de control la verificación periódica de los perfiles de cifrado TLS del portal de la DINAPI frente a estándares internacionales vigentes.

HALLAZGO N° 05

Título del Hallazgo: Omisión del Encabezado de Protección de Tipos MIME (X-Content-Type-Options).

- **Gravedad:** Baja
- **Confianza del Escáner:** Media
- **Identificadores:** CWE-693, WASC-15

Se verificó que los encabezados de respuesta para componentes y recursos de imagen estática (como por ejemplo el favicon institucional `/assets/img/faviconFinal.png`) no incluyen la directiva de cabecera X-Content-Type-Options: nosniff.

La carencia de este control facilita que navegadores heredados u obsoletos intenten interpretar el tipo de recurso analizando su contenido binario interno ("MIME sniffing") en lugar de respetar rígidamente el tipo MIME (`image/png`) enviado por Nginx. Este factor, aunque de severidad baja, podría ser explotado si se lograra combinar con fallos de carga de archivos que posibilitaran el enmascaramiento de scripts activos bajo extensiones estáticas inofensivas.

Descargo de la Dependencia Auditada:

La Dirección de Informática informa que ha mitigado el presente hallazgo mediante la declaración activa de la directiva de restricción de tipos de contenido, desactivando la capacidad de los navegadores de alterar el tipo de recurso (MIME Sniffing) y forzando la ejecución estricta según lo declarado por el servidor institucional.

Opinión del Auditor:

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual


Página web: www.dinapi.gov.py
Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional
Página 13 de 58



Esta Auditoría levanta el hallazgo mencionado tomando como base las acciones correctivas de configuración ejecutadas por la dependencia auditada. No obstante, y con el propósito de garantizar la exclusión absoluta del vector de riesgo en toda la plataforma Joajú, la validación definitiva de la mitigación queda supeditada a una inspección analítica posterior que corrobore la presencia de la cabecera en todas las respuestas del servidor, incluyendo recursos dinámicos y páginas de error del cliente.

Recomendación:

Se recomienda a la Dirección de Informática estandarizar la inyección de la cabecera *X-Content-Type-Options* con el valor estricto *nosniff* a nivel global dentro del archivo principal de configuración del servidor Nginx, asegurando que afecte de manera general a la totalidad de los dominios, subdominios y tipos de archivos despachados por la institución. Asimismo, se insta a incorporar la validación de esta directiva dentro de las listas de control técnico obligatorias para la puesta en producción de cualquier nuevo módulo o actualización de la aplicación web Joajú.

IX. CONCLUSION FINAL

De las verificaciones realizadas concluimos que: Existen hallazgos pero no revisten de gravedad ni criticidad alta siendo estos de carácter medio y bajo (en cuanto a riesgos se refiere).

X. RECOMENDACIÓN FINAL

A la Dirección de Informática:

- Se recomienda a la Dirección de Informática unificar las acciones de mitigación mediante la implementación de una Línea Base de Configuración Segura (*Hardening*) y la adopción formal de un Ciclo de Vida de Desarrollo Seguro (SDLC), asegurando de esta forma la sostenibilidad de las correcciones y la eliminación del riesgo residual en la plataforma Joajú.

XI. PLAN DE MEJORAMIENTO

Se deberá presentar en un **plazo de 10 (diez) días hábiles, a ser contados a partir del día siguiente de la recepción del presente informe, un Plan de Mejoramiento Funcional** sobre la observación ratificada con sus recomendaciones, estableciendo las acciones de mejora, un cronograma de ejecución, establecer los responsables, las evidencias del cumplimiento, y elevarlo a la Dirección de Auditoría Interna Institucional antes de su carga en el Sistema de la Auditoría General del Poder Ejecutivo (SIAGPE), con el fin de verificar su razonabilidad, constatando si se han detectado y analizado las causas que las motivaron, la coherencia de las acciones programadas y si las mismas han de contribuir a subsanarlas para su evaluación y aprobación correspondiente.


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977

Asunción, 5 de Junio de 2026.


Página web: www.dinapi.gov.py

Página 14 de 58

Lic. Diego González
Auditor Informático

Dirección de Auditoría Interna Institucional

Elaborado por:

Equipo auditor



Lic. Diego González
Auditor Informático

Dirección de Auditoria Interna Institucional

Aprobado por:



C.P Sergio Penayo
Director Interino

Dirección de Auditoria Interna Institucional



ANEXO 1

Minuta de Reunión 01



C.P. SERGIO DANIEL PENAYO
Director Interno
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual



Página web: www.dinapi.gov.py



Dirección de Auditoría Interna Institucional

MINUTA DE REUNIÓN				01
Tema de la Reunión:	Auditoría al Sistema Joa'ju utilizando OWASP Top10 como marco de referencia			
Institución/es:	DINAPI			
Autor:	Diego González			
Fecha:	08/04/2026	Hora Inicio:	14:00	Hora Fin: 14:44
Lugar:	DIRECCION DE INFORMATICA			
Referencias:				

LISTA DE PARTICIPANTES		
Nombre y Apellido	Dependencia/Cargo	Firma
LIC. CLAUDIO TACAR	DPTO. CONTROL CALIDAD	
LIC. SONIA BENITEZ	DPTO. ANALISIS DE SISTEMAS	
ING. ALFONSO MEDINA	INGENIERIA DE SOFTWARE	
LIC. DIEGO GONZALEZ	AUDITOR TI	

ASPECTOS TRATADOS

- ① DEFINIR HORARIO Y LUGAR
- ② NOTIFICAR CUALQUIER RESTRICCIÓN TÉCNICA
- ③ DESIGNAR UN PUNTO DE CONTACTO TÉCNICO
- ④ TENER EN CONSIDERACIÓN ESTA ACTIVIDAD (SERVICIO ZAP) A EFECTOS DE EVITAR PROBLEMAS POR PARTE DE MECANISMOS DE SEGURIDAD. (Firewall, WAF, IDS/IPS)

Avda. España N° 323 c/ Estados Unidos - Asunción, Paraguay

Teléf.: +595 21 216 7000 - www.dinapi.gov.py

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual



LISTA DE ACCIONES

- ① SE REALIZARÁ EN HORARIO NORMAL EN DÍA HÁBIL
PREVIO ANÁLISIS DE HORARIO POR PARTE DE INFORMÁTICA
ASIMISMO SE REALIZARÁ EN DÍA Y HORA QUE NO HAYA
ATENCIÓN AL PÚBLICO, PREFERENTEMENTE MARTES O JUEVES.
- ② INFORMÁTICA VA A VERIFICAR EXISTENCIA RESTRICCIÓN TÉCNICA
Y PROVOCAR UN EQUIPO ESPECIAL P/EL ESCANEO A SER
REALIZADO.
- ③ EL DIRECTOR DE INFORMÁTICA DESIGNA A LA LIC. CLAUDIA
DACAIL COMO CONTACTO TÉCNICO.
- ④ EL EQUIPO A SER PROVOCADO POR LA DIR. DE INFORMÁTICA
SERÁN ~~ESOS~~ CARGADOS COMO EXCEPCIÓN EN EL SISTEMA DE SEGURIDAD
LO MISMO QUE LA IP ASIGNADA AL MENCIONADO EQUIPO.

Avda. España N° 323 c/ Estados Unidos - Asunción, Paraguay

Teléf.: +595 21 216 7000 - www.dinapi.gov.py

2

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977

Página web: www.dinapi.gov.py
Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

Página 18 de 58



ANEXO 2

Minuta de Reunión 02

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual



Dirección de Auditoría Interna Institucional

MINUTA DE REUNIÓN				02
Tema de la Reunión:	Escaneo con el Software OWASP Zap Proxy sobre la aplicación web https://joaju.dinapi.gov.py/ , según lo coordinado con la Lic. Claudia Dacak en representación de la Dirección de Informática			
Institución/es:	DINAPI			
Autor:	Lic. Diego González Quiroz			
Fecha:	07/05/2026	Hora Inicio:	14:15	Hora Fin: 14:37
Lugar:	DIRECCIÓN DE INFORX			
Referencias:	ESCANEADO A SISTEMA WEB JOAJU			

LISTA DE PARTICIPANTES		
Nombre y Apellido	Dependencia/Cargo	Firma
Lic. Claudia Dacak	DIRTO. CONTROL CALIDAD	
Lic. ADRIAN GRAY	DIRTO. INFORX	
Lic. DIEGO GONZALEZ	AUDITORIA INFORMATICA	

ASPECTOS TRATADOS

SE INICIO EL ESCANEADO DE LA APLICACION WEB INSTITUCIONAL JOAJU. DINAPI.GOV.PY CON LA HERRAMIENTA OWASP ZAP CONFIGURADA EN MOD ATQUE Y COMO POLITICA DE ESCANEADO PENTEST, COMO NAVEGADOR PREDETERMINADO SE CONCLUYO EL ESCANEADO TUDIENDOSE CONSTATAR QUE NO SE GENERARON ALERTAS ALTA.

SE GENERO UN INFORME DEL ESCANEADO EN FORMATO HTML

Avda. España N° 323 c/ Estados Unidos - Asunción, Paraguay

Teléf.: +595 21 216 7000 - www.dinapi.gov.py

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977

Página web: www.dinapi.gov.py

Página 20 de 58

Lic. Diego González
Auditor Informático

Dirección de Auditoría Interna Institucional



ANEXO 3

Escaneo Joajú

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual



Escaneo Joaju

Generado con ZAP el 7 de mayo de 2026 a las 14:36:24

ZAP Versión: 2.17.0

ZAP de Checkmarx

Contenido

- Acerca de este informe
 - Parámetros del informe
- Resúmenes
 - Recuento de alertas por riesgo y nivel de confianza
 - Recuento de alertas por sitio y riesgo
 - Recuento de alertas por tipo de alerta
 - Perspectivas
- Alertas
 - Riesgo = Medio , Confianza = Alta (2)
 - Riesgo = Medio , Confianza = Media (2)
 - Riesgo = Bajo , Confianza = Alta (1)
 - Riesgo = Bajo , Confianza = Media (2)
 - Riesgo = Informativo , Confianza = Medios (3)
 - Riesgo = Informativo Confianza = Baja (1)



18/5/26, 9:48

Escaneo Joaju

- [Apéndice](#)
- [Tipos de alerta](#)

Acerca de este informe

Parámetros del informe

Contextos

No se seleccionó ningún contexto, por lo que se incluyeron todos los contextos por defecto.

Sitios

Se incluyeron los siguientes sitios:

- <https://firefox.settings.services.mozilla.com>
- <https://joaju.dinapi.gov.py>

(Si no se seleccionó ningún sitio, se incluyeron todos los sitios por defecto).

Para que sus datos se incluyan en el informe, un sitio web seleccionado debe estar dentro de uno de los contextos incluidos.

Niveles de riesgo

Incluido : Alto , Medio , Bajo , Informativo

Excluidos : Ninguno

Niveles de confianza

Incluido : Confirmado por Usuario , Alta , Media , Baja

Excluido : Confirmado por Usuario , Alta , Media , Baja , Falso positivo

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ... 2/35



Resúmenes

Recuento de alertas por riesgo y nivel de confianza

Esta tabla muestra el número de alertas para cada nivel de riesgo y confianza incluidas en el informe.

(Los porcentajes entre paréntesis representan el recuento como porcentaje del número total de alertas incluidas en el informe, redondeado a una cifra decimal).

		Confianza			
		Confirmado	Medios de		
		por	Alta	comunicación	Baja
		Usuario			Total
Riesgo	Alto	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)	0 (0,0 %)
	Medio	0 (0,0 %)	2 (18,2 %)	2 (18,2 %)	0 (0,0 %)
	Bajo	0 (0,0 %)	1 (9,1 %)	2 (18,2 %)	0 (0,0 %)
	Informativo	0 (0,0 %)	0 (0,0 %)	3 (27,3 %)	1 (9,1 %)
	Total	0 (0,0 %)	3 (27,3 %)	7 (63,6 %)	1 (9,1 %)

Recuento de alertas por sitio y riesgo



18/5/26, 9:48

Escaneo Joaju

Esta tabla muestra, para cada sitio en el que se generó una o más alertas, el número de alertas generadas en cada nivel de riesgo.

Las alertas con un nivel de confianza de "Falso positivo" se han excluido de estos recuentos.

(Los números entre paréntesis indican la cantidad de alertas generadas para el sitio con un nivel de riesgo igual o superior a ese valor).

		Riesgo			
		Alto	Medio	Bajo	Informativo
		(= Alto)	(>= Medio)	(>= Bajo)	(>= Informativo)
Sitio	https://firefox.set	0	1	0	1
	tings.services.mozila.com	(0)	(1)	(1)	(2)
	https://joaju.dinapi.gov.py	0	3	3	3
		(0)	(3)	(6)	(9)

Recuento de alertas por tipo de alerta

Esta tabla muestra el número de alertas de cada tipo, junto con el nivel de riesgo de cada tipo de alerta.

(Los porcentajes entre paréntesis representan cada recuento como un porcentaje, redondeado a una cifra decimal, del número total de alertas incluidas en este informe).

Tipo de alerta	Riesgo	Contar
Cabecera Política de seguridad de contenidos (CSP) no configurada	Medio	4 (36,4 %)
Configuración incorrecta entre dominios	Medio	3 (27,3 %)
Total		11

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026 Auditoría a la aplicación web joajú/Escaneos ... 4/35



18/5/26, 9:48

Escaneo Joaju

Tipo de alerta	Riesgo	Contar
<u>Falta atributo de integridad de recursos secundarios</u>	Medio	4 (36,4 %)
<u>Falta de cabecera Anti-Clickjacking</u>	Medio	4 (36,4 %)
<u>Falta encabezado X-Content-Type-Options</u>	Bajo	5 (45,5 %)
<u>Inclusión de archivos fuente JavaScript entre dominios</u>	Bajo	4 (36,4 %)
<u>Encabezado Strict-Transport-Security No Establecido</u>	Bajo	5 (45,5 %)
<u>Aplicación Web Moderna</u>	Informativo	4 (36,4 %)
<u>Recuperado de la Caché</u>	Informativo	4 (36,4 %)
<u>Reexaminar las Directivas de Control de Caché</u>	Informativo	7 (63,6 %)
<u>Fuzzer de agente de usuario</u>	Informativo	5 (45,5 %)
Total		11

Perspectivas

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joajú/Escaneos ...

5/35



18/5/26, 9:48

Escaneo Joaju

Esta tabla muestra información que probablemente le resulte muy relevante, pero que no está relacionada con vulnerabilidades, ni siquiera con la aplicación en cuestión.

Nivel	Razón	Sitio	Descripción	Estadística
Bajo	Advertencia		Se han registrado advertencias de ZAP; consulte el archivo zap.log para obtener más detalles.	46
Información	Informativo		Porcentaje de fallos de red	2 %
Información	Informativo	http://joaju.dinapi.gov.py	Porcentaje de respuestas con código de estado 3xx	100 %
Información	Informativo	http://joaju.dinapi.gov.py	Porcentaje de respuestas lentas	75 %
Información	Informativo	https://firefox.settings.services.mozilla.com	Porcentaje de respuestas con código de estado 2xx	100 %
Información	Informativo	https://firefox.settings.services.mozilla.com	Porcentaje de puntos finales con tipo de contenido application/json	100 %

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ... 6/35



18/5/26, 9:48

Escaneo Joaju

Nivel	Razón	Sitio	Descripción	Estadística
Información	Informativo	https:// firefox .setting s.servi ces.mo zilla.co m	Porcentaje de puntos finales con método GET	100 %
Información	Informativo	https:// firefox .setting s.servi ces.mo zilla.co m	Recuento total de puntos finales	3
Información	Informativo	https:// firefox .setting s.servi ces.mo zilla.co m	Porcentaje de respuestas lentas	100 %
Información	Informativo	https:// joaju. dinapi. gov.py	Porcentaje de respuestas con código de estado 2xx	65 %
Información	Informativo	https:// joaju. dinapi. gov.py	Porcentaje de respuestas con código de estado 3xx	16 %
Información	Exceder bajo	https:// joaju. dinapi. gov.py	Porcentaje de respuestas con código de estado 4xx	9 %
Información	Exceder bajo	https:// joaju.	Porcentaje de respuestas con	8 %

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 7/35



18/5/26, 9:48

Escaneo Joaju

Nivel	Razón	Sitio	Descripción	Estadística
n		dinapi. gov.py	código de estado 5xx	
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido application/javas cript	38 %
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido application/json	4 %
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido font/woff2	4 %
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido image/png	23 %
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido text/css	4 %
Infor mació n	Inform ativo	https:// joaju. dinapi. gov.py	Porcentaje de puntos finales con tipo de contenido text/html	23 %

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ...

8/35



18/5/26. 9:48

Escaneo Joaju

Nivel	Razón	Sitio	Descripción	Estadística
Información	Informativo	https://joaju.dinapi.gov.py	Porcentaje de puntos finales con método GET	100 %
Información	Informativo	https://joaju.dinapi.gov.py	Recuento total de puntos finales	21
Información	Informativo	https://joaju.dinapi.gov.py	Porcentaje de respuestas lentas	4 %

Alertas

Riesgo = Medio , Confianza = Alta (2)

<https://joaju.dinapi.gov.py> (2)

Cabecera Política de seguridad de contenidos (CSP) no configurada (1)

▼ OBTENER <https://joaju.dinapi.gov.py/sitemap.xml>

etiquetas de alerta

- [OWASP 2021 A05](#)
- [POLÍTICA_QA_STD =](#)
- [POLÍTICA_PENTEST =](#)
- [SISTÉMICO](#)
- [CWE-693](#)
- [OWASP 2017 A06](#)
- [OWASP 2025 A02](#)

Descripción de la alerta

La Política de seguridad de contenido (CSP) es una capa adicional de

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

9/35



18/5/26, 9:48

Escaneo Joaju

seguridad que ayuda a detectar y mitigar ciertos tipos de ataques, incluidos Cross Site Scripting (XSS) y ataques de inyección de datos. Estos ataques se utilizan para todo, desde el robo de datos hasta la desfiguración del sitio o la distribución de malware. CSP proporciona un conjunto de encabezados HTTP estándar que permiten a los propietarios de sitios web declarar fuentes de contenido aprobadas que los navegadores deberían poder cargar en esa página; los tipos cubiertos son JavaScript, CSS, marcos HTML, fuentes, imágenes y objetos incrustados como applets de Java, ActiveX, archivos de audio y video.

Pedido

▼ Sección de línea y encabezado de solicitud (251 bytes)

```
GET
https://joaju.dinapi.gov.py/sitemap.xml HTTP/1.1
host: joaju.dinapi.gov.py
user-agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de encabezado y línea de estado (236 bytes)

```
HTTP/1.1 200 OK
Server: nginx
```

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

10/35



18/5/26, 9:48

Escaneo Joaju

Date: Thu, 07 May 2026 17:25:28 GMT
Content-Type: text/html
Content-Length: 108463
Connection: keep-alive
Last-Modified: Wed, 26 Mar 2025
16:38:04 GMT
ETag: "67e42d6c-1a7af"
Accept-Ranges: bytes

► Cuerpo de la respuesta (108463 bytes)

Solución

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. esté configurado para establecer la cabecera Content-Security-Policy.

Falta atributo de integridad de recursos secundarios (1)

▼ OBTENER <https://joaju.dinapi.gov.py/>

etiquetas de alerta

- [CWE-345](#)
 - [OWASP_2021_A05](#)
 - POLÍTICA_QA_STD =
 - POLÍTICA_PENTEST =
 - [SISTÉMICO](#)
 - [OWASP_2017_A06](#)
 - [OWASP_2025_A02](#)
 -
- POLÍTICA_DE_DESARROLLO_ESTÁNDAR =

Descripción de la alerta

Falta el atributo de integridad en una etiqueta de script o enlace servido por un servidor externo. La etiqueta de integridad evita que un atacante que haya obtenido acceso a este servidor inyecte un contenido malicioso.

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos... 11/35



18/5/26, 9:48

Escaneo Joaju

Pedido

▼ Sección de línea y encabezado de la solicitud (240 bytes)

```
GET https://joaju.dinapi.gov.py/  
HTTP/1.1  
host: joaju.dinapi.gov.py  
user-agent: Mozilla/5.0 (Windows  
NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/141.0.0.0  
Safari/537.36  
pragma: no-cache  
cache-control: no-cache
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de encabezado y línea de estado (236 bytes)

```
HTTP/1.1 200 OK  
Server: nginx  
Date: Thu, 07 May 2026 17:25:28 GMT  
Content-Type: text/html  
Content-Length: 108463  
Connection: keep-alive  
Last-Modified: Wed, 26 Mar 2025  
16:38:04 GMT  
ETag: "67e42d6c-1a7af"  
Accept-Ranges: bytes
```

► Cuerpo de la respuesta (108463 bytes)

Evidencia

```
<script async  
src="https://www.googletagmanager.c  
om/gtag/js?id=G-E7S0ZWGY21">  
</script>
```

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ...

12/35



18/5/26, 9:48

Escaneo Joaju

Solución

Proporcionar un atributo de integridad válido a la etiqueta.

Riesgo = Medio , Confianza = Media (2)

<https://firefox.settings.services.mozilla.com> (1)

Configuración incorrecta entre dominios (1)

▼ OBTENER

[https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-exceptions/changeset?
_expected=1777016927120](https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-exceptions/changeset?_expected=1777016927120)

etiquetas de alerta

- [OWASP 2021 A01](#)
- [POLÍTICA_QA_STD =](#)
- [POLÍTICA_PENTEST =](#)
- [SISTÉMICO](#)
- [OWASP 2025 A01](#)
- [OWASP 2017 A05](#)
- [CWE-264](#)

Descripción de la alerta

La carga de datos del navegador web puede ser posible, debido a una mala configuración de Cross Origin Resource Sharing (CORS) en el servidor web.

Otra información

La configuración incorrecta de CORS en el servidor web permite aplicaciones de lectura entre dominios de terceros arbitrarios, utilizando API no autenticadas en este dominio. Sin embargo, las implementaciones de los navegadores web no permiten que terceros arbitrarios lean la respuesta de las API autenticadas. Esto reduce un poco el riesgo. Esta configuración incorrecta podría ser utilizada por un atacante para acceder a datos que están disponibles de forma no

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

13/35



18/5/26, 9:48

Escaneo Joaju

Pedido

autenticada, pero que utilizan alguna otra forma de seguridad, como la lista blanca de direcciones IP.

▼ Sección de línea y encabezado de solicitud (425 bytes)

```
GET
https://firefox.settings.services.mozilla.com/v1/buckets/main/collecti
ons/url-classifier-
exceptions/changeset?
_expected=1777016927120 HTTP/1.1
host:
firefox.settings.services.mozilla.c
om
User-Agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64; rv:150.0)
Gecko/20100101 Firefox/150.0
Accept: application/json
Accept-Language: es-ES,es;q=0.9,en-
US;q=0.8,en;q=0.7
Content-Type: application/json
Connection: keep-alive
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de encabezado y línea de estado (840 bytes)

```
HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 373720
cache-control: max-age=3600
strict-transport-security: max-
age=31536000
access-control-expose-headers:
Retry-After, Content-Length,
Backoff, Content-Type, Alert
via: 1.1 google, 1.1 varnish, 1.1
varnish, 1.1 varnish
```

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joajú/Escaneos ... 14/35



18/5/26, 9:48

Escaneo Joaju

x-content-type-options: nosniff
server: nginx
expires: Thu, 07 May 2026 17:30:20
GMT
access-control-allow-origin: *
last-modified: Sat, 02 May 2026
00:00:06 GMT
content-security-policy: default-
src 'none'; frame-ancestors
'none'; base-uri 'none';
content-type: application/json
Accept-Ranges: bytes
Age: 0
Date: Thu, 07 May 2026 17:25:40 GMT
X-Served-By: cache-bfi-kbfi7400080-
BFI, cache-bfi-kbfi7400080-BFI,
cache-eze2230038-EZE
X-Cache: MISS, MISS, MISS
X-Cache-Hits: 0, 0, 0
X-Timer:
S1778174740.691663,VS0,VE538
Vary: Accept-Encoding

► Cuerpo de la respuesta (373720
bytes)

Evidencia

access-control-allow-origin: *

Solución

Asegúrese de que los datos
confidenciales no estén disponibles de
forma no autenticada (por ejemplo,
mediante listas blancas de direcciones
IP).

Configure el encabezado HTTP
"Access-Control-Allow-Origin" en un
conjunto más restrictivo de dominios,
o elimine todos los encabezados CORS
por completo, para permitir que el
navegador web aplique la Política del

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

15/35



18/5/26, 9:48

Escaneo Joaju

Mismo Origen (SOP) de una manera más restrictiva.

<https://joaju.dinapi.gov.py> (1)

Falta de cabecera Anti-Clickjacking (1)

▼ OBTENER <https://joaju.dinapi.gov.py/>

etiquetas de alerta

- [OWASP 2021 A05](#)
- [POLÍTICA_QA_STD](#) =
- [POLÍTICA_PENTEST](#) =
- [CWE-1021](#)
- [SISTÉMICO](#)
- [WSTG-v42-CLNT-09](#)
- [OWASP 2017 A06](#)
- [OWASP 2025 A02](#)

Descripción de la alerta

La respuesta no protege contra ataques de "ClickJacking". Debes incluir Content-Security-Policy con la directiva "frame-ancestors" o X-Frame-Options.

Pedido

▼ Sección de línea y encabezado de la solicitud (240 bytes)

```
GET https://joaju.dinapi.gov.py/  
HTTP/1.1  
host: joaju.dinapi.gov.py  
user-agent: Mozilla/5.0 (Windows  
NT 10.0; Win64; x64)  
AppleWebKit/537.36 (KHTML, like  
Gecko) Chrome/141.0.0.0  
Safari/537.36  
pragma: no-cache  
cache-control: no-cache
```

▼ Cuerpo de la solicitud (0 bytes)

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ...

16/35



18/5/26, 9:48

Escaneo Joaju

Respuesta

▼ Sección de encabezado y línea de estado (236 bytes)

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 May 2026 17:25:27 GMT
Content-Type: text/html
Content-Length: 108463
Connection: keep-alive
Last-Modified: Wed, 26 Mar 2025 16:38:04 GMT
ETag: "67e42d6c-1a7af"
Accept-Ranges: bytes

► Cuerpo de la respuesta (108463 bytes)

Parámetro

x-frame-options

Solución

Los navegadores web modernos admiten las cabeceras HTTP Content-Security-Policy y X-Frame-Options. Asegúrese de que una de ellas esté configurada en todas las páginas web devueltas por su sitio/aplicación.

Si espera que la página esté marcada solo por páginas en su servidor (por ejemplo, si forma parte de un FRAMESET), utilice SAMEORIGIN; De lo contrario, si no espera que la página esté marcada, utilice DENY. Alternativamente, considere implementar la directiva "frame-ancestors" de la Política de Seguridad de Contenidos.

Riesgo = Bajo , Confianza = Alta (1)

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

17/35



18/5/26, 9:48

Escaneo Joaju

<https://joaju.dinapi.gov.py> (1)

Encabezado Strict-Transport-Security No Establecido (1)

▼ OBTENER <https://joaju.dinapi.gov.py/chunk-FKBIZCJJ.js>

etiquetas de alerta

- [OWASP_2021_A05](#)
- [POLÍTICA_QA_STD =](#)
- [POLÍTICA_PENTEST =](#)
- [SISTÉMICO](#)
- [CWE-319](#)
- [OWASP/2017_A06](#)
- [OWASP_2025_A02](#)

Descripción de la alerta

HTTP Strict Transport Security (HSTS) es un mecanismo de política de seguridad web mediante el cual un servidor web declara que los agentes de usuario conformes (como un navegador web) deben interactuar con él utilizando únicamente conexiones HTTPS seguras (es decir, HTTP superpuesto a TLS/SSL). HSTS es un protocolo de seguimiento de estándares del IETF y se especifica en RFC 6797.

Pedido

▼ Sección de línea y encabezado de solicitud (296 bytes)

```
GET
https://joaju.dinapi.gov.py/chunk-
FKBIZCJJ.js HTTP/1.1
host: joaju.dinapi.gov.py
user-agent: Mozilla/5.0 (Windows NT
10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/141.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer:
```

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 18/35



18/5/26, 9:48

Escaneo Joaju

<https://joaju.dinapi.gov.py/>

▼ Cuerpo de la solicitud (0 bytes)

▼ Sección de encabezado y línea de estado (245 bytes)

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 May 2026 17:25:28 GMT
Content-Type: application/javascript
Content-Length: 1726
Connection: keep-alive
Last-Modified: Wed, 26 Mar 2025
16:38:04 GMT
ETag: "67e42d6c-6be"
Accept-Ranges: bytes

▼ Cuerpo de la respuesta (1726 bytes)

```
import{b as p,c as d}from"./chunk-  
MF4P7VKM.js";import{C as a,Db as  
f,e as g,f as l,m as c,vb as u,z as  
m}from"./chunk-NM2LVTNH.js";var  
s=g(d());var B=((=>{let e=class  
e{constructor(o,t)  
{this.router=o,this.http=t,this.API_  
ROUTES={login:  
(=>`${p.baseUrl.urlBackApi}login`)  
isLoggedIn()  
{return!!sessionStorage.getItem("tok  
en")}}login(o){return  
l(this,null,function*(){try{let  
t=yield  
c(this.http.post(this.API_ROUTES.log  
in(),  
{cedula:o.cedula,password:o.password  
});t&&t.token?  
sessionStorage.setItem("token",t.tok  
en):s.default.mixin({toast:!0,positi
```

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

19/35



18/5/26, 9:48

Escaneo Joaju

```
on:"center",showConfirmButton:!1,tim
er:2e3,timerProgressBar:!0,didOpen:n
=>
{n.onmouseenter=s.default.stopTimer,
n.onmouseleave=s.default.resumeTimer
}}.fire({icon:"warning",title:t.msg
})}catch(t){console.error("Hubo un
problema con la consulta:",t);let
r;t instanceof
TypeError&&t.message=="Failed to
fetch"?r="El servicio no se
encuentra en estos momentos, favor
intentar m\xE1s
tarde.":r="Ocurri\xF3 un error
inesperado. Por favor, int\xE9ntelo
de nuevo m\xE1s
tarde.",s.default.mixin({customClass
:{confirmButton:"btn btn-success ml-
3"},buttonsStyling:!1}).fire({title:
"",text:r,icon:"error",confirmButton
Text:"OK",reverseButtons:!0})}finall
y{console.log("Petici\xF3n
finalizada"),this.isLoggedIn()&&
(location.href="index.html")}}}}logo
ut()
{sessionStorage.removeItem("token"),
this.router.navigate(["/login"])}dec
odeToken()
{if(sessionStorage.getItem("token"))
{let
t=sessionStorage.getItem("token")?.s
plit(".");if(t?.length!==3)throw
new Error("El JWT no es
v\xE1lido");let
r=t[1],n=atob(r);return
JSON.parse(n)}else
return""};e.\u0275fac=function(t)
{return new(t||e)
(a(f),a(u))},e.\u0275prov=m({token:e
,factory:e.\u0275fac,providedIn:"roo
t"});let i=e;return i})();export{B
as a};
```

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ... 20/35



18/5/26, 9:48

Escaneo Joaju

Solución

Asegúrese de que su servidor web, servidor de aplicaciones, balanceador de carga, etc. está configurado para aplicar Strict-Transport-Security.

Riesgo = Bajo , Confianza = Media (2)

<https://joaju.dinapi.gov.py> (2)

Falta encabezado X-Content-Type-Options (1)

▼ OBTENER

<https://joaju.dinapi.gov.py/assets/img/faviconFinal.png>

etiquetas de alerta

- [OWASP 2021 A05](#)
- [POLÍTICA_QA_STD =](#)
- [POLÍTICA_PENTEST =](#)
- [SISTÉMICO](#)
- [CWE-693](#)
- [OWASP 2017 A06](#)
- [OWASP 2025 A02](#)

Descripción de la alerta

La cabecera Anti-MIME-Sniffing X-Content-Type-Options no se ha establecido en 'nosniff'. Esto permite que las versiones anteriores de Internet Explorer y Chrome realicen MIME-sniffing en el cuerpo de la respuesta, lo que puede provocar que el cuerpo de la respuesta se interprete y se muestre como un tipo de contenido distinto del tipo de contenido declarado. Las versiones actuales (principios de 2014) y heredadas de Firefox utilizarán el tipo de contenido declarado (si se establece uno), en lugar de realizar MIME-sniffing.

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

21/35



18/5/26 9:48

Escaneo Joaju

Otra información

Este problema aún se aplica a las páginas de tipo error (401, 403, 500, etc.), ya que esas páginas a menudo se ven afectadas por problemas de inyección, en cuyo caso aún existe la preocupación de que los navegadores husmeen las páginas lejos de su tipo de contenido real.

En el umbral «Alto» esta regla de análisis no alertará sobre respuestas de error del cliente o servidor.

Pedido

▼ Sección de línea y encabezado de la solicitud (317 bytes)

```
GET
https://joaju.dinapi.gov.py/assets/
img/faviconFinal.png HTTP/1.1
host: joaju.dinapi.gov.py
user-agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/141.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
referer:
https://joaju.dinapi.gov.py/sitemap
.xml
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de línea de estado y encabezado (234 bytes)

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 May 2026 17:25:28 GMT
Content-Type: image/png
Content-Length: 26449
```

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ... 22/35



18/5/26, 9:48

Escaneo Joaju

Connection: keep-alive
Last-Modified: Mon, 02 Dec 2024
11:05:32 GMT
ETag: "674d947c-6751"
Accept-Ranges: bytes

► Cuerpo de la respuesta (26449 bytes)

Parámetro

x-content-type-options

Solución

Asegúrese de que la aplicación/servidor web establece el encabezado Content-Type adecuadamente, y que establece el encabezado X-Content-Type-Options a 'nosniff' para todas las páginas web.

Si es posible, asegúrese de que el usuario final utilice un navegador web moderno y compatible con los estándares que no realizan MIME-sniffing en absoluto, o que puede ser dirigido por la aplicación web/servidor web para que no realice MIME-sniffing.

Inclusión de archivos fuente JavaScript entre dominios (1)

▼ OBTENER <https://joaju.dinapi.gov.py/sitemap.xml>

etiquetas de alerta

- [OWASP 2025 A08](#)
- POLÍTICA_QA_STD =
- POLÍTICA_PENTEST =
- [SISTÉMICO](#)
- [OWASP 2021 A08](#)
- [CWE-829](#)
-

POLÍTICA_DE_DESARROLLO_ESTÁN
DAR =

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 23/35



18/5/26, 9:48

Escaneo Joaju

Descripción de la alerta

La página incluye uno o más archivos
de script de un dominio de terceros.

Pedido

▼ Sección de línea y encabezado de
solicitud (251 bytes)

```
GET
https://joaju.dinapi.gov.py/sistema
p.xml HTTP/1.1
host: joaju.dinapi.gov.py
user-agent: Mozilla/5.0 (Windows
NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/141.0.0.0
Safari/537.36
pragma: no-cache
cache-control: no-cache
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de encabezado y línea de
estado (236 bytes)

```
HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 May 2026 17:25:28
GMT
Content-Type: text/html
Content-Length: 108463
Connection: keep-alive
Last-Modified: Wed, 26 Mar 2025
16:38:04 GMT
ETag: "67e42d6c-1a7af"
Accept-Ranges: bytes
```

► Cuerpo de la respuesta (108463
bytes)

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ... 24/35



18/5/26: 9:48

Escaneo Joaju

Parámetro

<https://www.googletagmanager.com/gtag/js?id=G-E7S0ZWGY21>

Evidencia

```
<script async  
src="https://www.googletagmanager.  
com/gtag/js?id=G-E7S0ZWGY21">  
</script>
```

Solución

Asegúrese de que los archivos fuente JavaScript se cargan solo desde fuentes de confianza, y que las fuentes no pueden ser controladas por los usuarios finales de la aplicación.

Riesgo = Informativo , Confianza = Medios (3)

<https://firefox.settings.services.mozilla.com> (1)

Recuperado de la Caché (1)

▼ OBTENER

[https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-exceptions/changeset?
_expected=1777016927120](https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-exceptions/changeset?_expected=1777016927120)

etiquetas de alerta

- [OWASP 2025 A07](#)
- [CWE-525](#)
- [POLÍTICA_PENTEST =](#)
- [OWASP 2021 A07](#)
- [SISTÉMICO](#)
- [WSTG-v42-ATHN-06](#)
- [OWASP 2017 A02](#)

Descripción de la alerta

El contenido se ha recuperado de un caché compartido. Si los datos de respuesta son sensibles, personales o específicos del usuario, esto puede resultar en la filtración de información sensible. En algunos casos, esto puede

file:///trueñasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ...

25/35



18/5/26, 9:48

Escaneo Joaju



incluso resultar en que un usuario obtenga el control completo de la sesión de otro usuario, dependiendo de la configuración de los componentes de caché en uso en su entorno. Este problema se produce principalmente cuando los servidores de caché, como los "proxy", están configurados en la red local. Esta configuración se encuentra ampliamente en entornos corporativos o educativos, por ejemplo.

Otra información

La presencia de la cabecera 'Age' indica que se está utilizando un servidor de caché compatible con HTTP/1.1.

Pedido

▼ Sección de línea y encabezado de solicitud (425 bytes)

```
GET
https://firefox.settings.services.mozilla.com/v1/buckets/main/collections/url-classifier-exceptions/changeset?_expected=1777016927120 HTTP/1.1
host:
firefox.settings.services.mozilla.com
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:150.0)
Gecko/20100101 Firefox/150.0
Accept: application/json
Accept-Language: es-ES,es;q=0.9,en-US;q=0.8,en;q=0.7
Content-Type: application/json
Connection: keep-alive
```

▼ Cuerpo de la solicitud (0 bytes)

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 26/35



18/5/26, 9:48

Escaneo Joaju

Respuesta

▼ Sección de encabezado y línea de estado (840 bytes)

HTTP/1.1 200 OK
Connection: keep-alive
Content-Length: 373720
cache-control: max-age=3600
strict-transport-security: max-age=31536000
access-control-expose-headers: Retry-After, Content-Length, Backoff, Content-Type, Alert
via: 1.1 google, 1.1 varnish, 1.1 varnish, 1.1 varnish
x-content-type-options: nosniff
server: nginx
expires: Thu, 07 May 2026 17:30:20 GMT
access-control-allow-origin: *
last-modified: Sat, 02 May 2026 00:00:06 GMT
content-security-policy: default-src 'none'; frame-ancestors 'none'; base-uri 'none';
content-type: application/json
Accept-Ranges: bytes
Age: 0
Date: Thu, 07 May 2026 17:25:40 GMT
X-Served-By: cache-bfi-kbfi7400080-BFI, cache-bfi-kbfi7400080-BFI, cache-eze2230038-EZE
X-Cache: MISS, MISS, MISS
X-Cache-Hits: 0, 0, 0
X-Timer: S1778174740.691663,VS0,VE538
Vary: Accept-Encoding

► Cuerpo de la respuesta (373720 bytes)

Evidencia

Age: 0

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos... 27/35



18/5/26, 9:48

Escaneo Joaju

Solución

Válida que la respuesta no contiene información confidencial, personal o específica del usuario. Si es así, considere el uso de los siguientes encabezados de respuesta HTTP para limitar o evitar que otro usuario almacene y recupere el contenido de la memoria caché:

Control de caché: sin caché, sin almacenamiento, debe revalidarse, privado

Pragma: no-cache

Caduca: 0

Esta configuración indica a los servidores de almacenamiento en caché compatibles con HTTP 1.0 y HTTP 1.1 que no almacenen la respuesta ni la recuperen (sin validación) de la memoria caché en respuesta a una solicitud similar.

<https://joaju.dinapi.gov.py> (2)

Aplicación Web Moderna (1)

► OBTENER <https://joaju.dinapi.gov.py/sitemap.xml>

Fuzzer de agente de usuario (1)

▼ OBTENER <https://joaju.dinapi.gov.py/api>

etiquetas de alerta

- CUSTOM_PAYLOADS =
- POLÍTICA_PENTEST =
- SISTÉMICO

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 26/35



18/5/26, 9:48

Escaneo Joaju

Descripción de la alerta

Compare las diferencias en la respuesta según el fuzzeo de User Agent (por ejemplo, sitios móviles, acceso como un motor de búsqueda). Compara el código de estado de la respuesta y el hash del cuerpo de la respuesta con la respuesta original.

Pedido

▼ Sección de línea y encabezado de solicitud (238 bytes)

```
GET
https://joaju.dinapi.gov.py/api
HTTP/1.1
host: joaju.dinapi.gov.py
user-agent: Mozilla/4.0
(compatible; MSIE 8.0; Windows NT
6.1)
pragma: no-cache
cache-control: no-cache
referer:
https://joaju.dinapi.gov.py/chunk-
MF4P7VKM.js
```

▼ Cuerpo de la solicitud (0 bytes)

Respuesta

▼ Sección de encabezado y línea de estado (193 bytes)

```
HTTP/1.1 503 Service Temporarily
Unavailable
Server: nginx
Date: Thu, 07 May 2026 17:29:22 GMT
Content-Type: text/html
Content-Length: 3849
Connection: keep-alive
ETag: "68f5fc85-f09"
```

► Cuerpo de la respuesta (3849 bytes)

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joaju/Escaneos ... 29/35



18/5/26, 9:48

Escaneo Joaju

Parámetro

Header User-Agent

Ataque

Mozilla/4.0 (compatible; MSIE 8.0;
Windows NT 6.1)

Riesgo = Informativo, Confianza = Baja (1)

<https://joaju.dinapi.gov.py> (1)

Reexaminar las Directivas de Control de Caché (1)

► OBTENER <https://joaju.dinapi.gov.py/sitemap.xml>

Apéndice

Tipos de alerta

Esta sección contiene información adicional sobre los tipos de alertas que aparecen en el informe.

Cabecera Política de seguridad de contenidos (CSP) no configurada

Fuente

levantado por un escáner pasivo (Cabecera Content Security Policy (CSP) no configurada)

ID de CWE

693

ID de WASC

15

Referencia

▪ <https://developer.mozilla.org/en-US/docs/Web/HTTP/Guides/CSP>

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joaju/Escaneos ... 30/35



18/5/26, 9:48

Escaneo Joajú



- https://cheatsheetseries.owasp.org/cheatsheets/Content_Security_Policy_Cheat_Sheet.html
- <https://www.w3.org/TR/CSP/>
- <https://w3c.github.io/webappsec-csp/>
- <https://web.dev/articles/csp>
- <https://caniuse.com/#feat=contentsecuritypolicy>
- <https://content-security-policy.com/>

Configuración incorrecta entre dominios

Fuente	levantado por un escáner pasivo (Configuración Incorrecta Cross-Domain)
ID de CWE	264
ID de WASC	14
Referencia	▪ https://vulncat.fortify.com/en/detail?category=HTML5&subcategory=Overly%20Permissive%20CORS%20Policy

Falta atributo de integridad de recursos secundarios

Fuente	planteado por un escáner pasivo (Falta atributo de integridad de recursos secundarios)
ID de CWE	345
ID de WASC	15

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joajú/Escaneos ... 31/35



18/5/26, 9:48

Escaneo Joaju

Referencia

- https://developer.mozilla.org/en-US/docs/Web/Security/Subresource_Integrity

Falta de cabecera Anti-Clickjacking

Fuente

activado por un escáner pasivo ([Cabecera Anti-Clickjacking](#))

ID de CWE

[1021](#)

ID de WASC

15

Referencia

- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/X-Frame-Options>

Falta encabezado X-Content-Type-Options

Fuente

generado por un escáner pasivo ([Falta encabezado X-Content-Type-Options](#))

ID de CWE

[693](#)

ID de WASC

15

Referencia

- [https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941\(v=vs.85\)](https://learn.microsoft.com/en-us/previous-versions/windows/internet-explorer/ie-developer/compatibility/gg622941(v=vs.85))
- <https://owasp.org/www-community/Security-Headers>

Inclusión de archivos fuente JavaScript entre dominios

Fuente

levantado por un escáner pasivo ([Inclusión de archivos fuente JavaScript entre dominios](#))

file://truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ... 32/35



18/5/26, 9:48

Escaneo Joaju

ID de CWE	829
ID de WASC	15

Encabezado Strict-Transport-Security No Establecido

Fuente	generado por un escáner pasivo (<u>encabezado Strict-Transport-Security</u>)
ID de CWE	319
ID de WASC	15
Referencia	▪ https://cheatsheetseries.owasp.org/cheatsheets/HTTP_Strict_Transport_Security_Cheat_Sheet.html ▪ https://owasp.org/www-community/Security-Headers ▪ https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security ▪ https://caniuse.com/stricttransportsecurity ▪ https://datatracker.ietf.org/doc/html/rfc6797

Aplicación Web Moderna

Fuente	levantado por un escáner pasivo (<u>Aplicación Web Moderna</u>)
--------	---

Recuperado de la Caché

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ... 33/35



18/5/26, 9:48

Escaneo Joaju

Fuente

levantado por un escáner pasivo ([Recuperado de la Caché](#))

ID de CWE

525

Referencia

- <https://datatracker.ietf.org/doc/html/rfc7234>
- <https://datatracker.ietf.org/doc/html/rfc7231>
- <https://www.rfc-editor.org/rfc/rfc9110.html>

Reexaminar las Directivas de Control de Caché

Fuente

levantado por un escáner pasivo ([Reexaminar las Directivas de Control de Caché](#))

ID de CWE

525

ID de WASC

13

Referencia

- https://cheatsheetseries.owasp.org/cheatsheets/Session_Management_Cheat_Sheet.html#web-content-caching
- <https://developer.mozilla.org/en-US/docs/Web/HTTP/Reference/Headers/Cache-Control>
- <https://grayduck.mn/2021/09/13/cache-control-recommendations/>

Fuzzer de agente de usuario

Fuente

generado por un escáner activo ([User Agent Fuzzer](#))

file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoría a la aplicación web joajú/Escaneos ... 34/35

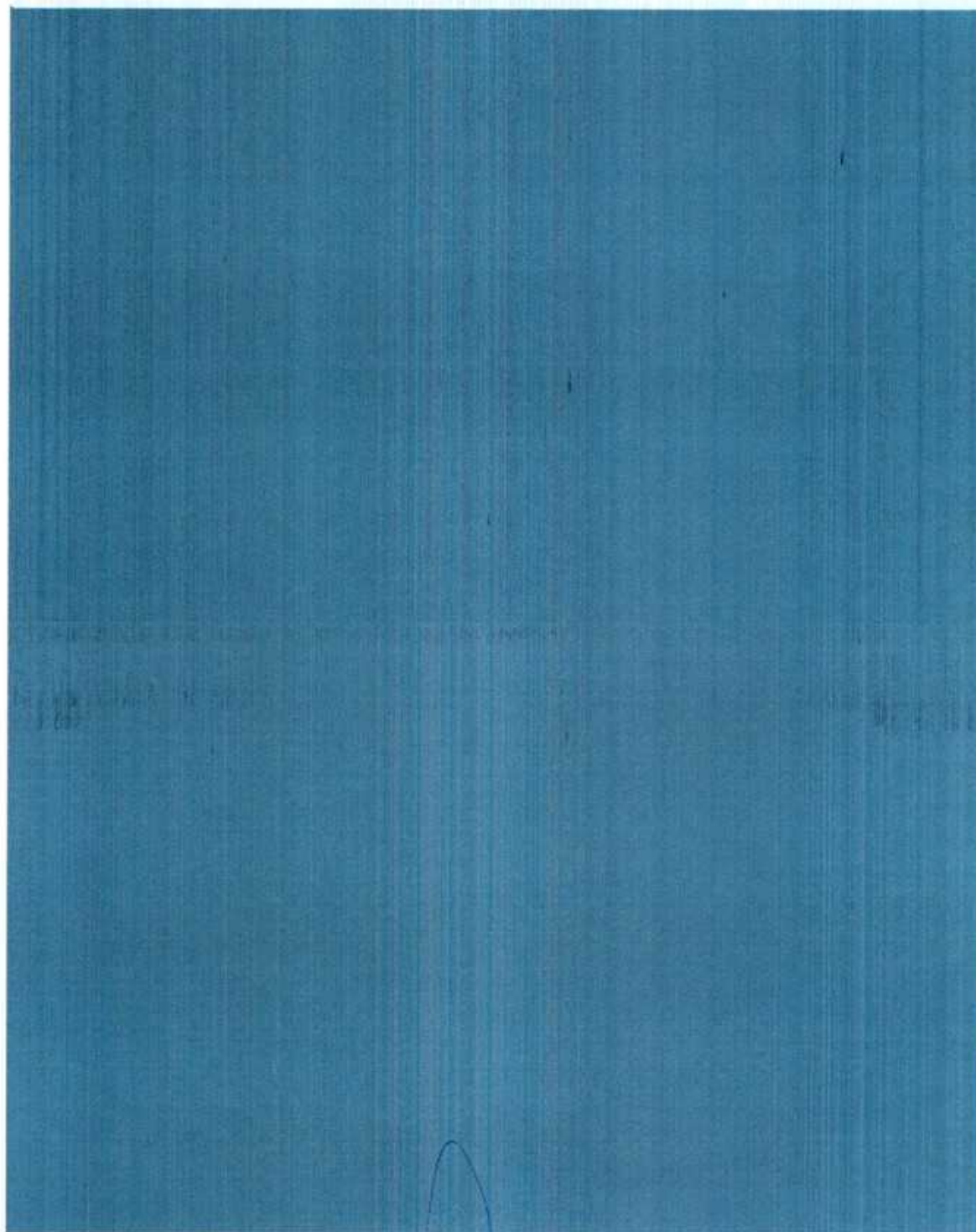


18/5/26, 9:48

Escaneo Joajú

Referencia

▪ <https://owasp.org/wstg>



file:///truenasws02/netdir_auditoria/auditoria_interna/AÑO 2026/AUDITORIA INFORMATICA 2026/Auditoria a la aplicación web joajú/Escaneos ... 35/35

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual


Página web: www.dinapi.gov.py
Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional
Página 56 de 58



ANEXO 4

EVIDENCIAS TÉCNICAS (EXTRACTOS DE CABECERAS HTTPS)

C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional



A continuación, se documenta la respuesta HTTP en crudo obtenida durante las pruebas técnicas automatizadas por OWASP ZAP, sirviendo como evidencia de la ausencia de las cabeceras recomendadas de seguridad descritas en los hallazgos:

```
GET
[https://joaju.dinapi.gov.py/sitemap.xml] (https://joaju.dinapi.gov.py/sitemap.xml) HTTP/1.1
Host: joaju.dinapi.gov.py
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/141.0.0.0 Safari/537.36
Pragma: no-cache
Cache-Control: no-cache

HTTP/1.1 200 OK
Server: nginx
Date: Thu, 07 May 2026 17:25:28 GMT
Content-Type: text/html
Content-Length: 108463
Connection: keep-alive
Last-Modified: Wed, 26 Mar 2025 16:38:04 GMT
ETag: "67e42d6c-1a7af"
Accept-Ranges: bytes
```

(Se constata visualmente que en la respuesta del servidor Nginx no se declara Content-Security-Policy, X-Frame-Options ni X-Content-Type-Options).


C.P. SERGIO DANIEL PENAYO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Dirección: Avda. España N° 323 c/ EE.UU.
Teléf.: 021 210977


Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

Página web: www.dinapi.gov.py

Página 58 de 58