DIRECCIÓN NACIONAL DE PROPIEDAD INTELECTUAL PARAGUAY | PARAGUÁI TETÃYGUA AKÃPYROKY MBA'ETEE MOAKÃHA

MEMORANDUM DINAPI/DAII N° 236/2025

PARA : **Gabriela Villalba, Directora**
Dirección de Comunicación Institucional
Sr. José Ramírez, Director Interino
Dirección de Informática

C.C. : **Abg. CLAUDIA FRANCO Q., Directora Nacional (Para conocimiento)**
Dirección Nacional de Propiedad Intelectual

DE : **C.P. Sergio D. Penayo, Director Interino**
Dirección de Auditoria Interna Institucional

REF. : **Remisión de Informe Final DAII/AI N° 02/2025 – Auditoría a la Seguridad de la Plataforma Web Institucional**

FECHA : 24/11/2025

Me dirijo a Ustedes, en referencia a la Auditoria de la Seguridad de la Plataforma Web Institucional Ejercicio Fiscal 2025, realizado en base al Plan de Trabajo Anual aprobado por **Resolución DINAPI N° 566/2024** *"Por la cual se aprueba el Plan de Trabajo Anual Versión 3 para el periodo 2025 de la Dirección de Auditoría Interna Institucional de la Dirección Nacional de Propiedad Intelectual – DINAPI ".*

En tal sentido, se remite adjunto el Informe Final de la Auditoría realizada, y se solicita a la Dirección de Comunicación Institucional la elaboración de un Plan de Mejoramiento Funcional sobre las observaciones ratificadas con sus recomendaciones, estableciendo las acciones de mejora, un cronograma de ejecución, los responsables del cumplimiento, seguimiento y elevarlo a la Dirección de Auditoria Interna Institucional 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.

Plazo para la presentación del Plan de Mejoramiento Funcional, **10 (diez) días hábiles** a partir de la recepción de presente Informe Final.

Sin otro particular, me despido atentamente.

Lic. Gabriela Villalba
Directora
Dirección de Comunicación Institucional
Dirección Nacional de Propiedad Intelectual

Lic. Gabriela Villalba
Directora
Dirección de Comunicación Institucional
Dirección Nacional de Propiedad Intelectual

24/11/25 12:50

24.11.2025

P/ Acuse

INFORME FINAL
DAII/AI N° 02/2025
"AUDITORÍA A LA SEGURIDAD DE LA PLATAFORMA WEB INSTITUCIONAL "

AÑO 2025

INDICE

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

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

INFORME FINAL DAII/AI N° 02/2025

AUDITORÍA INFORMÁTICA – SEGURIDAD INFORMATICA PLATAFORMA WEB INSTITUCIONAL

I. IDENTIFICACIÓN DE LA INSTITUCIÓN

La Dirección Nacional de Propiedad Intelectual, fue creada por Ley N° 4.798 de fecha 31 de diciembre de 2012, como persona jurídica de derecho público, con carácter autárquico y patrimonio propio, como órgano de ejecución de la Política Nacional de Propiedad Intelectual. Inició sus actividades con presupuesto propio en el año 2014, igualmente, tiene por objetivo la aplicación en el área administrativa de las normas destinadas a la protección de los derechos de propiedad intelectual, de acuerdo con lo dispuesto en la Constitución Nacional, las leyes que rigen la materia y los tratados y convenios internacionales atinentes, suscriptos y ratificados por la República del Paraguay.

MISIÓN

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

VISIÓN

Institución reconocida por su gestión de excelencia en la salvaguarda de los derechos de Propiedad Intelectual.

FUNCIONES DE LA INSTITUCIÓN

a) 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.
b) 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.
c) Administrar eficazmente los Activos de Propiedad Intelectual para propiciar la protección y uso consentido, en beneficio de nuestro país, de nuestros recursos genéticos autóctonos.
d) Fomentar la creación y desarrollo de empresas culturales.
e) Propiciar el reconocimiento y la utilización de los conocimientos tradicionales indígenas, a favor de los pueblos originarios.
f) Fomentar la innovación, la investigación y el acceso a la ciencia, favoreciendo la transferencia de tecnología.
g) Representar a los intereses nacionales, en tratados y convenios de cooperación con entidades y países en materia de Propiedad Intelectual.
h) 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.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

i) Promover iniciativas y desarrollar actividades conducentes al mejor conocimiento y protección de la Propiedad Intelectual, en el orden nacional.
j) Dictar las reglamentaciones técnicas para la ejecución de cualquier actividad de su competencia en todo el territorio nacional, de acuerdo con la legislación pertinente.
k) 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.
l) 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.
m) 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.
n) 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.
o) Establecer y percibir las tasas que por diversos conceptos se deban abonar, de conformidad con las normas vigentes y la presente Ley.
p) Establecer y percibir aranceles por servicios prestados.
q) 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° 566/2024*** *"Por la cual se aprueba el Plan de Trabajo Anual – Versión N° 03 Periodo 2025 de la Dirección de Auditoría Interna Institucional de la Dirección Nacional de Propiedad Intelectual – DINAPI ".*

III. OBJETIVOS DE LA AUDITORÍA

• OBJETIVO GENERAL

La presente auditoría informática tiene como objetivo general; determinar el nivel actual de seguridad de la plataforma web institucional, identificar riesgos de seguridad críticos que podrían afectar la continuidad operativa y la confianza pública, y evaluar el cumplimiento de estándares de Ciberseguridad y buenas prácticas relevantes para entidades gubernamentales.

• OBJETIVOS ESPECÍFICOS

1. Identificación y clasificación de vulnerabilidades en aplicaciones web (OWASP Top 10).
2. Evaluación de la configuración de seguridad de la infraestructura.
3. Revisión de los mecanismos de autenticación.
4. Análisis de fugas de información.

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

5. Evaluar el impacto potencial de las vulnerabilidades detectadas.
6. Determinar la exposición a ataques de denegación de servicio.
7. Verificación del cumplimiento con la Normativa de Ciberseguridad de la MITIC.
8. Evaluación de la adherencia a los controles de seguridad de ISO/IEC 27002.

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° 566/2024*** *"Por la cual se aprueba el Plan de Trabajo Anual – Versión N° 03 Periodo 2025 de la Auditoría Interna Institucional de la Dirección Nacional de Propiedad Intelectual – DINAPI".*

V. PROCEDIMIENTOS DE AUDITORÍA

1. Reconocimiento de infraestructura pública y recabada de registros DNS.

Se realizó reconocimiento de la infraestructura pública asociada al dominio dinapi.gov.py mediante SHODAN. Se identificaron las IPs 181.94.237.83, 201.222.53.153 y 201.222.53.154, servidores DNS gestionados por COPACO y el uso de Google Workspace para correo electrónico.

Evidencia: Análisis SHODAN.

2. Inspección de encabezados HTTP para verificación de políticas de seguridad.

Se revisaron los encabezados HTTP devueltos por el servidor y se observaron controles de seguridad como Strict-Transport-Security, Content-Security-Policy, X-Frame-Options, X-XSS-Protection y X-Content-Type-Options.

Evidencia: Análisis SHODAN.

3. Extracción y análisis del certificado X.509.

Se extrajo y analizó el certificado X.509 presentado por el servidor. El certificado incluye *.dinapi.gov.py y SANs que confirman cobertura wildcard. El emisor corresponde a GlobalSign (GlobalSign RSA OV SSL CA 2018).

Evidencia: Análisis SHODAN.

4. Inventario de subdominios y mapeo IP.

Se generó un inventario de subdominios con su correspondiente mapeo IP. Se detectó que servicios como Gitlab y www responden en más de una IP, lo que sugiere balanceo o redundancia.

Evidencia: Análisis SHODAN.

5. Verificación de infraestructura de correo y registros SPF/DKIM.

El dominio utiliza Google Workspace para el servicio de correo y presenta registros TXT relacionados con DKIM y SPF.

Evidencia: Análisis SHODAN.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna

6. Análisis pasivo de HTTPS y certificado SSL/TLS.

Se validó el uso de HTTPS en el portal, confirmándose la existencia de un certificado SSL/TLS vigente y el uso de cifrado moderno, asegurando la confidencialidad de la comunicación.

Evidencia: Informe Autenticación Dinapi.docx

7. Revisión de encabezados de seguridad HTTP.

Se revisaron encabezados de seguridad HTTP del portal; se identificaron algunos activos, aunque se recomienda reforzar configuraciones como CSP y X-Frame-Options en todas las páginas del sitio.

Evidencia: Informe Autenticación Dinapi.docx

8. Evaluación de mecanismos de autenticación en la web pública.

Se constató que el portal público no requiere autenticación de usuarios ni maneja credenciales, por lo que los riesgos asociados a autenticación indebida no aplican en este contexto.

Evidencia: Informe Autenticación Dinapi.docx

9. Verificación de configuración y manejo de cookies visibles.

Se verificó la existencia de una cookie estrictamente necesaria para funcionalidad del portal; se recomienda exigir el uso de flags Secure y HttpOnly cuando se manejen datos sensibles.

Evidencia: Informe Autenticación Dinapi.docx

10. Análisis de carga de recursos externos y dependencia de proveedores.

Se identificó la carga de recursos externos mediante servicios de proveedores internacionales. Se recomienda aplicar validación de integridad (por ejemplo SRI hashes) y monitoreo continuo de versiones.

Evidencia: Informe Autenticación Dinapi.docx

11. Escaneo de Vulnerabilidades No Autenticado (Vulnerability Assessment) de caja negra, ejecutado sobre los servicios de red expuestos del portal (dinapi.gov.py).

Este proceso empleó la herramienta Nessus Essentials con el objetivo de identificar debilidades en la configuración de cifrado (TLS/SSL) y fallas en la gestión de certificados digitales.

Evidencia: Análisis de fugas de información.docx

12. Análisis de footprinting riguroso que complementa la búsqueda por IP realizada previamente en Shodan.

Al utilizar la herramienta viewdns.info y buscar por nombre de dominio, se han descubierto 24 subdominios que revelan una visión más clara de la segmentación de la infraestructura de la DINAPI.

Evidencia: subdominios encontrados por nombre de host.docx.

13. Descargo de los hallazgos observados durante el proceso de Auditoría.

14. Borrador de Informe Final.

15. Informe Final.

VI. RIESGO E IMPORTANCIA RELATIVA

- La no provisión en tiempo y forma de los documentos relacionados a la Auditoría.
- Que las muestras seleccionadas contengan errores significativos.
- Debilidad en el Sistema de Control Interno.
- Que el área auditada no colabore durante el proceso de Auditoría.

VII. TIPOS DE INFORMES

- Borrador de Informe para descargo.
- Informe Final.

VIII. DESARROLLO DE LA AUDITORIA

HALLAZGO Nº 01

Soporte de cifrados débiles (SWEET32: 64-bit block ciphers, p. ej. 3DES)

El escaneo de Nessus reporta que el servicio HTTPS acepta suites de cifrado con bloques de 64 bits (por ejemplo 3DES), vulnerables a la explotación conocida como SWEET32. Esto permite, en sesiones largas o con mucho tráfico repetido, realizar ataques de colisión que afecten la confidencialidad.

Evidencia: Salida de Nessus: SSL Medium Strength Cipher Suites Supported (SWEET32) — CVSS 7.5.

Impacto alto en la confidencialidad para sesiones largas; un atacante pasivo o MITM (man in the midle) con suficiente volumen de tráfico podría recuperar fragmentos de datos.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que realizó la evaluación de la configuración SSL mediante la herramienta en línea https://hackertarget.com/ssl-check, donde no se encontró presencia del cifrado citado. Asimismo, se analizaron documentos y manuales de configuración de NGINX e implementación de SSL de los siguientes sitios: - https://javierin.com/guia-para-securizar-nginx - https://nginx.org/en/docs/http/configuring_https_servers.html (entre otros). Esto permitió identificar y asignar los parámetros de mitigación correspondientes. Como resultado, se aplicaron en la configuración del proxy los siguientes parámetros, dejando implícito los cifrados permitidos: EVIDENCIA DE EVALUACIÓN: https://hackertarget.com/ssl-check

Opinión del Auditor:
En el descargo de la respuesta remitida por la Dirección de Informática se evalúa la configuración del SSL mediante herramientas en línea en donde no encuentran el cifrado citado como hallazgo por esta auditoría adjuntando la captura de pantalla de la evaluación realizada a través de los procedimientos citados en el MEMO DIT Nº 089/2025 de Fecha 12/11/2025 remitido a la Dirección de Comunicaciones.
Esta Auditoría levanta el hallazgo mencionado, no obstante al momento de realizar este análisis a través de la herramienta de fuentes abiertas Nessus, en fecha 21/10/2025, el mismo se encontraba activo, en la sección de anexos se incluye la documentación que muestra dicha evidencia.

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

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la instraestructura de la plataforma web institucional.

HALLAZGO Nº 02

Nessus reporta que SSL Certificate Cannot Be Trusted — el certificado presentado no es de una CA de confianza o la cadena de certificación está incompleta. Esto impide que clientes validen correctamente la identidad del servidor.

Evidencia: Salida resumen de Nessus: SSL Certificate Cannot Be Trusted (CVSS 6.5). Esto representa un impacto medio en los usuarios/clientes que en algunos casos verán advertencias en navegadores; aumenta la probabilidad de ataques MITM y pérdida de confianza.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que; se evaluó el sitio web con las siguientes herramientas públicas, las cuales resolvieron correcta y satisfactoriamente la validez del certificado OV del sitio y el CA de su proveedor www.dinapi.gov.py.
https://www.sslshopper.com/ssl-checker.html#hostname=www.dinapi.gov.py.
https://hackertarget.com/ssl-check.
https://www.ssllabs.com/ssltest/analyze.html?d=www.dinapi.gov.py&s=201.222.53.154.

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 03

Nessus marca SSL Self-Signed Certificate indicando que el servidor podría estar presentando un certificado autofirmado en lugar de uno emitido por una CA de confianza.

Evidencia: Salida de Nessus: SSL Self-Signed Certificate (CVSS 6.5).

Esto representa un impacto medio ya que los certificados autofirmados no permiten validación de identidad y son fácilmente usados en ataques de suplantación.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que; las acciones tomadas para mitigar este hallazgo son las mismas aplicadas al HALLAZGO 02

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

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

HALLAZGO Nº 04

Ausencia de cabeceras HTTP de seguridad esencial.
Durante la revisión de las cabeceras HTTP se constató que el servidor no implementa controles como: Strict-Transport-Security (HSTS), X-Frame-Options, X-Content-Type-Options, Referrer-Policy
Estas cabeceras son mecanismos fundamentales de protección en navegadores web. Su ausencia puede permitir:

- Ataques de Clickjacking (por falta de X-Frame-Options).
- Ejecución de scripts maliciosos (XSS) mediante contenido mixto o mal interpretado (sin X-Content-Type-Options).
- Exposición de URLs internas o tokens sensibles (sin Referrer-Policy).
- Downgrade de HTTPS a HTTP o ataques de intermediario (MITM) si no se aplica HSTS.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que; se han corregido las cabeceras para el dominio www.dinapi.gov.py segun la documentacion del
servidor nginx y otros manuales consultados
Algunos parámetros de seguridad dependen de un trabajo conjunto con el equipo de desarrollo para aplicar adicionar parámetros o corregir el comportamiento de componentes externos (google y facebook apis), por lo que se aconseja una mesa de trabajo conjunta con nueva evaluación de seguridad durante esos trabajos.
add_header Strict-Transport-Security "max-age=63072000; includeSubDomains; preload" always;
add_header X-Content-Type-Options "nosniff" always;
add_header X-Frame-Options "SAMEORIGIN" always;
add_header X-XSS-Protection "1; mode=block" always;
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
add_header Permissions-Policy "geolocation=(), microphone=(), camera=(), payment=()" always;
add_header Content-Security-Policy "default-src 'self'; script-sre 'self 'unsafe-inline' 'unsafe-eval';
style-src 'self 'unsafe-inline'; img-src 'self' data: https:; font-src "self; connect-stc "self; frame-ancestors
'self;" always;
add_header Set-Cookie "Path=/; HttpOnly; Secure" always;

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 05

Ausencia de autenticación de correo institucional (SPF, DKIM, DMARC).
El análisis DNS no evidenció registros SPF, DKIM ni DMARC activos para el dominio institucional.
La falta de estos mecanismos permite la suplantación del dominio (@dinapi.gov.py) en correos electrónicos falsos (phishing), lo que puede afectar la confidencialidad y reputación institucional.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Inst

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que se constató la existencia, en los registros DNS de Teisa y Copaco, de: Registros MX apuntando al servicio de Google Workspace, donde se encuentra alojado el servicio de correo. Un registro TXT con un parámetro DKIM y subparámetro rsa, además de la validación TXT del servicio de Google. Posteriormente, se adicionó el registro SPF y se coordinará con el proveedor la obtención de los parámetros DKIM y DMARC correctos, programando su implementación en un horario que no afecte el uso de los servicios.

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 06

Validación incompleta de protocolos TLS.
El análisis preliminar no pudo confirmar si las versiones TLS 1.2 y 1.3 están habilitadas ni si TLS 1.0/1.1 permanecen activas.
Versiones antiguas de TLS (1.0 y 1.1) presentan vulnerabilidades conocidas (POODLE, BEAST, etc.).
Si permanecen habilitadas, podrían permitir ataques de interceptación de tráfico cifrado.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que; inicialmente la versión del servidor proxy nmginx contaba con la configuración en TLS-1.2 y TLS-1.3.
Se ha revisado la configuración y ajustado para que trabaja únicamente sobre cifrado TLS 1.2 y TELS 1.3 cómo se lee a continuación:
EVIDENCIA DE VERIFICACIÓN:
Igualmente el servicio de analisis ssl indica que solo estan habilirados los protocolos 1.2 y 1.3 (https: / / domsignal.com/test/i8qfev1s070te506bju9f2bmhc7z5nf7).
ssl_ciphers
'ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-RSA-AES256-GCM-SHA384:ECDHE-EC
DSA-AES128-GCM-SHA256:ECDHE-RSA-AES128-GCM-SHA256';
ssl_protocols TLSy1.2 TLSv1.3;
ssl_prefer_server_ciphers on;

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

HALLAZGO Nº 07

Falta de validación de cookies seguras.
No se confirmó la presencia de los flags Secure y HttpOnly en las cookies emitidas por el sitio.
Sin el flag Secure, las cookies pueden transmitirse en texto plano si se fuerza HTTP.
Sin el flag HttpOnly, el contenido de las cookies podría ser accedido por scripts maliciosos (XSS).

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que; tras verificar la documentación de nginx y se han activado en la configuración proxy el
parámetro:
add_header Set-Cookie "Path=/; HttpOnly; Secure";

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 08

Exposición de rutas internas y recursos públicos (A05 – Security Misconfiguration).
El portal expone directorios internos y rutas como /portal/v3/assets/ y /plugins/, las cuales son accesibles desde el navegador.
Esto puede permitir a un atacante obtener información sobre la estructura interna de la aplicación o localizar componentes vulnerables.

Descargo de la Dependencia Auditada:
La Dirección de Informática informa que, en el servidor proxy se han agregado los siguientes parámetros para que la consulta a dichos directorios sin un archivo específico envíe a la portada:
rewrite ""/portal/v3/assets$" "/portal/v3/" permanent;
rewrite ""/portal/v3/assets/$" "/portal/v3/" permanent;
rewtite ""/portal/v3/plugins$" "/portal/v3/" permanent;
rewrite ""/portal/v3/plugins/$" "/portal/v3/" permanent;

Opinión del Auditor:
Esta Auditoría levanta el hallazgo mencionado formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 09

Librerías JavaScript desactualizadas (A06 – Vulnerable and Outdated Components).

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 Inst.

Se detectó el uso de jQuery 3.5.1, versión que presenta vulnerabilidades conocidas.
Las dependencias desactualizadas pueden ser explotadas para ejecutar XSS o ataques de inyección de código en el cliente.

Descargo de la Dependencia Auditada:
La corrección de este punto corresponde a una optimización del código fuente del sitio web, esta tarea deberá ser realizada por la empresa responsable del desarrollo y mantenimiento de la aplicación. En este sentido, se conformarán mesas de trabajo técnicas con dicha empresa, a fin de coordinar las acciones necesarias para la mejora del sitio web y de las herramientas interconectadas con el mismo.

Opinión del Auditor:
Esta Auditoría se ratifica en el hallazgo mencionado, a razón de que no se remitieron las acciones de mejora para la corrección de mismo.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 10

Formularios sin token CSRF (A04 – Insecure Design).
Se observó la ausencia de tokens antifalsificación (CSRF) en formularios de búsqueda y contacto.
Un atacante podría inducir al usuario a ejecutar acciones no deseadas en su nombre.

Descargo de la Dependencia Auditada:
La corrección de este punto corresponde a una optimización del código fuente del sitio web, esta tarea deberá ser realizada por la empresa responsable del desarrollo y mantenimiento de la aplicación. En este sentido, se conformarán mesas de trabajo técnicas con dicha empresa, a fin de coordinar las acciones necesarias para la mejora del sitio web y de las herramientas interconectadas con el mismo.

Opinión del Auditor:
Esta Auditoría se ratifica en el hallazgo mencionado, a razón de que no se remitieron las acciones de mejora para la corrección de mismo.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 11

Parámetros manipulables en URLs (A01 – Broken Access Control – Potencial).
Se identificaron URLs con parámetros del tipo ?id=, que podrían permitir acceso o manipulación de datos si no existen validaciones en backend.
Posible exposición de información sensible o ejecución de ataques de enumeración o inyección.

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

Descargo de la Dependencia Auditada:
La corrección de este punto corresponde a una optimización del código fuente del sitio web, esta tarea deberá ser realizada por la empresa responsable del desarrollo y mantenimiento de la aplicación. En este sentido, se conformarán mesas de trabajo técnicas con dicha empresa, a fin de coordinar las acciones necesarias para la mejora del sitio web y de las herramientas interconectadas con el mismo.

Opinión del Auditor:
Esta Auditoría se ratifica en el hallazgo mencionado, a razón de que no se remitieron las acciones de mejora para la corrección de mismo.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

HALLAZGO Nº 12

Parámetros manipulables en URLs (A01 – Broken Access Control – Potencial)
Se identificaron URLs con parámetros del tipo ?id=, que podrían permitir acceso o manipulación de datos si no existen validaciones en backend.

Descargo de la Dependencia Auditada:
La corrección de este punto corresponde a una optimización del código fuente del sitio web, esta tarea deberá ser realizada por la empresa responsable del desarrollo y mantenimiento de la aplicación. En este sentido, se conformarán mesas de trabajo técnicas con dicha empresa, a fin de coordinar las acciones necesarias para la mejora del sitio web y de las herramientas interconectadas con el mismo.

Opinión del Auditor:
Esta Auditoría se ratifica en el hallazgo mencionado, a razón de que no se remitieron las acciones de mejora para la corrección de mismo.

Recomendación:
Recomendamos incorporar este procedimiento para ser realizado de manera periódica formando parte de una política de seguridad de la infraestructura de la plataforma web institucional.

IX. CONCLUSION FINAL

De las verificaciones realizadas concluimos que: Existen hallazgos y debilidades dentro de la Plataforma Web Institucional.

X. RECOMENDACIÓN FINAL

A la Dirección de Informática:

- Implementar la Política de Seguridad Informática aprobada por Resolución Dinapi Nº 247/2023.
- Utilizar el Formulario de Reporte de Incidentes de Seguridad citado en la sección 6.4.1.2 dentro de la Política de Seguridad Informática aprobada por Resolución Dinapi Nº 247/2023.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

- Implementar una política de control periódico de vulnerabilidades de seguridad en base al informe quincenal enviado por CERT-PY dependiente de la MITIC.

Al Encargado de Desarrollo y Mantenimiento del Sitio Web de la DINAPI:

- Elaborar un Plan de Mejoramiento Funcional para el fortalecimiento de la Seguridad de la Plataforma Web de la Institución en base a los HALLAZGOS 09, 10, 11 y 12 remitidos por esta Auditoría.

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, um Plan de Mejoramiento Funcional** sobre las observaciones ratificadas con sus recomendaciones, estableciendo las acciones de mejora, un cronograma de ejecución, establecer los responsables del cumplimiento, seguimiento y elevarlo a la Dirección de Auditoria Interna Institucional 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.

Asunción, 21 de noviembre de 2025.

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

Análisis Realizado con Shodan

Análisis realizado a la ip 181.94.237.83 con SHODAN

General Information

Hostnames	**dinapi.gov.py** host-81181-94-237**personal.net.py**
Domains	dinapi.gov.py personal.net.py
Country	**Paraguay**
City	**Asunción**
Organization	**Núcleo S.A.**
ISP	**Núcleo S.A.**
ASN	AS27895

Web Technologies

Security

HSTS

Open Ports

4434

Hashes

```
hash            -765815424
http.dom_hash   -1830446565
http.html_hash  -1454941180
```

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

4434 / TCP

HTTP/1.1 200 OK
Date: Tue, 14 Oct 2025 04:41:41 GMT
ETag: Nrxr863r6zzqqygsbQ0kxbp88r96m0HN
Cache-Control: max-age=0, must-revalidate
Accept-Ranges: bytes
Content-Length: 131
Content-Type: text/html
X-Frame-Options: SAMEORIGIN
Content-Security-Policy: frame-ancestors 'self'; object-src 'self'; script-src 'self' https: 'unsafe-eval' 'unsafe-inline' blob:;
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Strict-Transport-Security: max-age=31536000

SSL Certificate

Certificate:
Data:
Version: 3 (0x2)
Serial Number:
73:dd:33:44:58:20:0c:3a:b5:18:c3:52
Signature Algorithm: sha256WithRSAEncryption
Issuer: C=BE, O=GlobalSign nv-sa, CN=GlobalSign RSA OV SSL CA 2018
Validity
Not Before: May 30 22:41:02 2024 GMT
Not After : Jul 1 22:41:01 2025 GMT
Subject: C=PY, ST=Asunci\xC3\xB3n, L=Asunci\xC3\xB3n, O=DIRECCION NACIONAL DE PROPIEDAD INTELECTUAL, CN=*.dinapi.gov.py
Subject Public Key Info:
Public Key Algorithm: rsaEncryption
Public-Key: (2048 bit)
Modulus:
00:a2:34:68:2d:1c:4e:dc:10:33:13:cf:de:49:1f:
62:6e:d3:ad:7b:9e:ab:5a:e4:c4:d8:b1:eb:12:f6:
88:9a:a0:e9:a2:54:23:db:fd:d9:1f:9a:8d:f5:71:
0b:d0:ff:5d:2e:67:89:36:a9:96:e2:49:1b:4a:98:
91:d6:c3:04:3b:f6:77:b9:e0:0b:40:83:19:63:e5:
df:84:ca:95:59:33:9c:2b:02:1c:9a:e1:24:16:54:
4e:53:9f:c1:cc:bb:e8:df:1f:29:28:86:77:c0:52:
cb:e3:f8:46:c3:97:94:60:4c:36:fa:2e:44:ca:b3:
93:e7:8c:c0:bf:04:a2:7b:c1:e7:e2:c9:c8:8d:1e:
e4:b4:d0:ce:45:41:45:17:9d:35:79:07:ff:c7:83:
93:04:10:9f:ff:f5:c3:51:02:c8:37:24:91:a9:cd:
7e:64:92:ef:7e:58:f2:ce:55:c1:8e:13:8a:ec:d1:
62:4e:05:f0:a8:00:74:eb:e1:73:93:c4:e5:75:43:
52:a1:1a:02:b2:a8:78:aa:e4:8a:f3:ec:1e:33:e0:
a5:e1:b7:a7:fc:c7:20:b0:c4:5c:39:0f:f2:84:ea:
88:75:36:34:ef:ce:18:c4:82:61:7f:8e:f9:7d:6e:
1d:eb:55:b6:98:ab:64:c0:6a:7b:80:69:cf:61:b2:
a5:53
Exponent: 65537 (0x10001)
X509v3 extensions:
X509v3 Key Usage: critical
Digital Signature, Key Encipherment
X509v3 Basic Constraints: critical
CA:FALSE
Authority Information Access:
CA Issuers - URI:http://secure.globalsign.com/cacert/gsrsaovsslca2018.crt
OCSP - URI:http://ocsp.globalsign.com/gsrsaovsslca2018
X509v3 Certificate Policies:
Policy: 1.3.6.1.4.1.4146.1.20
CPS: https://www.globalsign.com/repository/
Policy: 2.23.140.1.2.2
X509v3 Subject Alternative Name:
DNS:*.dinapi.gov.py, DNS:dinapi.gov.py
X509v3 Extended Key Usage:
TLS Web Server Authentication, TLS Web Client Authentication
X509v3 Authority Key Identifier:
F8:EF:7F:F2:CD:78:67:A8:DE:6F:8F:24:8D:88:F1:87:03:02:B3:EB

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

X509v3 Subject Key Identifier:
56:F8:43:8A:AD:E2:08:65:EF:7F:4A:75:32:0F:86:0A:00:89:F7:3C
CT Precertificate SCTs:
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : AF:18:1A:28:D6:8C:A3:E0:A9:8A:4C:9C:67:AB:09:F8:
BB:BC:22:BA:AE:BC:B1:38:A3:A1:9D:D3:F9:B6:03:0D
Timestamp : May 30 22:41:04.688 2024 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:21:00:FA:24:0D:74:84:48:D5:F0:6B:93:F5:
A6:80:E3:FF:48:3D:26:43:21:09:21:3D:6E:C3:BB:DC:
2D:BE:73:57:64:02:20:65:E0:F4:16:20:09:7F:25:B6:
E8:6D:9C:2B:C5:5A:41:14:22:A6:89:F6:40:2C:F3:80:
48:59:EC:9A:FD:B0:F3
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 12:F1:4E:34:BD:53:72:4C:84:06:19:C3:8F:3F:7A:13:
F8:E7:B5:62:87:88:9C:6D:30:05:84:EB:E5:86:26:3A
Timestamp : May 30 22:41:04.694 2024 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:46:02:21:00:84:B7:49:BA:32:93:F8:FF:52:96:9D:
AE:8A:03:B0:73:94:65:C2:E7:8C:B6:EF:8F:AC:1C:01:
44:AC:C7:37:BE:02:21:00:C3:7D:E8:41:5E:4A:39:FA:
D1:24:85:B5:EE:93:FE:34:D4:28:D8:5C:D2:DE:02:31:
B0:4D:8E:AC:7C:0D:8C:27
Signed Certificate Timestamp:
Version : v1 (0x0)
Log ID : 1A:04:FF:49:D0:54:1D:40:AF:F6:A0:C3:BF:F1:D8:C4:
67:2F:4E:EC:EE:23:40:68:98:6B:17:40:2E:DC:89:7D
Timestamp : May 30 22:41:04.511 2024 GMT
Extensions: none
Signature : ecdsa-with-SHA256
30:45:02:20:17:7E:9E:FE:09:01:81:F3:AA:BF:23:1D:
54:0C:B5:5D:EB:CE:A4:26:27:AB:A5:0C:0C:57:D0:A0:
3D:B0:33:BA:02:21:00:A5:65:9E:C9:00:9C:40:63:CB:
52:32:E8:E3:A8:58:56:94:B2:FB:49:FA:0D:B6:EB:95:
15:4C:64:5A:93:44:E7
Signature Algorithm: sha256WithRSAEncryption
Signature Value:
95:c4:a1:7d:cb:23:a4:42:26:95:10:63:ff:d7:56:39:50:fa:
de:6b:f8:f7:87:5a:71:e2:9a:e9:d0:2a:01:53:ab:60:87:c4:
e7:d5:25:ed:c2:12:9b:cf:ff:a0:5c:39:69:5e:d8:d0:a6:06:
97:08:bc:e1:f0:5a:29:2e:cd:36:b2:30:03:68:a5:9c:18:6c:
aa:d3:4c:e2:4d:db:a8:08:71:50:2c:18:6a:90:18:8d:2d:63:
21:19:b1:8a:3d:c0:39:c8:89:a0:c4:d9:0f:bf:a3:52:03:f7:
44:23:ba:36:4e:d7:66:72:21:7c:47:9b:e6:f6:b1:86:7f:53:
b9:38:18:55:69:c8:19:53:a3:f9:c4:6e:61:0f:0c:33:eb:9a:
52:f3:b4:ee:4d:d3:19:c5:b9:16:e7:ba:5e:f4:9c:9b:2d:1d:
d8:73:ea:16:36:0d:60:29:e9:13:f4:69:0a:25:1b:fa:db:07:
5b:90:20:17:12:ca:a2:82:9d:24:79:4d:eb:39:5e:24:db:f9:
3f:b9:de:20:95:7e:0e:c0:7d:82:1e:ff:34:c3:b8:b8:d1:c4:
5d:19:34:de:14:8b:a1:f6:1f:c1:78:a2:26:7d:ac:1f:1b:dc:
e6:e2:06:46:11:a9:2e:c9:cd:69:9e:94:cd:39:62:4b:25:fe:
a9:1b:06:b9

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

Lic. Diego González
Auditor Informático
Direccion de Auditoria Interna Institucional

Registros **de dominio**

A	**181.94.237.83**
A	**201.222.53.153**
A	**201.222.53.154**
MX	alt1.aspmx.l.google.com
MX	alt2.aspmx.l.google.com
MX	alt3.aspmx.l.google.com
MX	alt4.aspmx.l.google.com
MX	aspmx.l.google.com
NS	ns1.copaco.com.py
NS	ns2.copaco.com.py
NS	ns3.copaco.com.py
SOA	ns1.copaco.com.py
TXT	MS=ms42323707
TXT	RgzV2SW591FBk9ePRx/1nGLOcEmEIYHpk2JdTkGeMo4=
TXT	verificación del sitio de Google=hzjmMtMUcGdpChjOce2H-xDysuRAFw_yOcyxOHfCr2A
TXT	v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDJOJkQ//g0Y4jHncb1OICaRv0JxpULdaSoFSD5wcR4RL8Ef7Kr/Ta+T7hWNcSShw7UE/78B82i7z81vOgAJ9AO5taQIW/WbrERQPVewesBxpiqXH9g2BZti23/VKn/6r4Oud7CiVdJQMYxB8wmekoJSSM+lo8cOM+bm7l4HfzTDG+QIDAQAB

Tipo de Registro	Registro Detalle	Significado y Observación
A (Dirección IP)	181.94.237.83	Esta es la **dirección IP principal** del servidor web que aloja la página.
A (Dirección IP)	201.222.53.153 201.222.53.154	Estas son **direcciones IP adicionales** o alternativas. La presencia de múltiples registros A con diferentes IPs sugiere que el sitio podría estar configurado para: 1) balanceo de carga, o 2) tener múltiples servidores para redundancia/falla, o 3) que algunas de estas IPs sean antiguas o para subdominios.
MX (Mail Exchanger)	alt1.aspmx.l.google.com alt2.aspmx.l.google.com	Estos registros MX indican que el correo electrónico del dominio es gestionado por **Google Workspace (Gmail)**. Esto significa que el dominio usa la infraestructura de correo de Google.
NS (Name Server)	ns1.copaco.com.py ns2.copaco.com.py ns3.copaco.com.py	Los Servidores de Nombre indican que la gestión de la zona DNS (dónde se guardan y modifican todos estos registros) está a cargo de **COPACO (Compañía Paraguaya de Comunicaciones S.A.)**.
SOA (Start of Authority)	ns1.copaco.com.py	Confirma que el servidor de nombre primario que administra la zona es **https://www.google.com/url?sa=E&source=gmail&q=ns1.copaco.com.py**.
TXT (Texto)	Varios registros largos (incluyendo v=DKIM1, RGSV2W..., verificación del sitio de Google...)	Estos son registros utilizados principalmente para: 1) **Verificación de Propiedad** (como el registro de Google visible en uno de ellos), 2) **Seguridad de Correo (SPF/DKIM/DMARC)**: Sirven para confirmar que el servidor que envía el correo está autorizado, lo que ayuda a prevenir el *spam* y el *phishing*.

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

En resumen y en relación a la presente tabla podemos decir que el sitio está alojado en una o varias direcciones ip(181.94.237.83 es la principal), el servicio de correo está externalizado y es gestionado por Google Workspace, la administración de los registros DNS está a cargo de COPACO.

IP's de SUB-DOMINIOS dentro del Portal de DINAPI

#	Nombre de Sub-Dominio	IP
1	Gitlab	**181.94.237.83**
2	Gitlab	**201.222.53.154**
3	Joaju	**181.94.237.83**
4	Joaju	**201.222.53.154**
5	mail	**201.217.43.242**
6	mosaico	**181.94.237.83**
7	proyectos	**181.94.237.83**
8	redpi	**181.94.237.83**
9	redpi	**201.222.53.154**
10	sfe-tp	**181.94.237.83**
11	sfe-tp	**201.222.53.154**
12	sprint	**201.217.43.242**
13	www	**181.94.237.83**
14	www	**201.222.53.154**

Subdomains

- gitlab
- joaju
- mail
- mosaico
- proyectos
- redpi
- sfe-tp
- sprint
- www

Additional Insights

Google verified

Microsoft Office 365

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

ANEXO 2

Análisis Realizado con Nessus

RESUMEN DEL ANALISIS REALIZADO A TRAVES DE LA HERRAMIENTA NESSUS REFERENTE A POSIBLES FUGAS DE INFORMACION

Vulnerabilidades Detectadas

1- Crítica / HIGH (CVSS 7.5): SSL Medium Strength Cipher Suites Supported (SWEET32) → el servidor acepta cifrados con bloques de 64 bits (p. ej. 3DES), vulnerables a ataques de colisión / recuperación de datos en sesiones largas.
2- Media / MEDIUM (CVSS 6.5): SSL Certificate Cannot Be Trusted → el certificado presentado no es de una CA de confianza (cadena incompleta o CA desconocida).
3- Media / MEDIUM (CVSS 6.5): SSL Self-Signed Certificate → el certificado es autofirmado (no emitido por CA pública o interna confiable).

Riesgo e Impacto:

SWEET32 (alto): riesgo de que, en sesiones largas (o tráfico repetido), un atacante pasivo/mitm pueda explotar colisiones en cifrados de 64 bits y recuperar fragments de datos sensibles. Afecta confidencialidad.
Certificado no confiable / Self-signed (medio): usuarios y sistemas no pueden validar identidad del servidor → facilita ataques man-in-the-middle y genera advertencias en navegadores / clientes.
En conjunto: tráfico TLS no está correctamente endurecido; riesgo de interceptación o exposición de datos críticos y pérdida de confianza operativa.
El servicio HTTPS acepta suites de cifrado con bloques de 64 bits (p.ej. 3DES) — CVE asociado: vulnerabilidad SWEET32 — y presenta un certificado autofirmado/cadena incompleta, por lo que los clientes no pueden validar la identidad del servidor.

Prioridades:

- Eliminar cifrados débiles (SWEET32) — alta prioridad.
- Reemplazar certificado autofirmado / cadena incompleta por certificado válido alta/medio prioridad según si el sitio es público o interno.
- Re-evaluar configuración TLS completa (protocolos, PFS, headers) — media.

C.P. SERGIO DANIEL PRIETO
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad [illegible]

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

Verificaciones rápidas realizas (comandos para confirmar y evidencias)
Se procedió a realizar las comprobaciones de manera manual desde una terminal Kali Linux en una VM.

 # 1) Verificar cifrados y TLS con nmap (rápido)

nmap --script ssl-enum-ciphers -p 443 dinapi.gov.py

```
┌──(root㉿kali-vm)-[/opt/nessus/sbin]
└─# nmap --script ssl-enum-ciphers -p 443 dinapi.gov.py
Starting Nmap 7.94 ( https://nmap.org ) at 2025-10-21 10:01 -05
Nmap scan report for dinapi.gov.py (192.168.50.1)
Host is up (0.00049s latency).
Other addresses for dinapi.gov.py (not scanned): 192.168.50.2
rDNS record for 192.168.50.1: DC1.DINAPI.GOV.PY

PORT    STATE    SERVICE
443/tcp filtered https

Nmap done: 1 IP address (1 host up) scanned in 0.45 seconds
```

 # 2) Probar conexión TLS y ver certificados

echo | openssl s_client -connect dinapi.gov.py:443 –showcerts

```
CONNECTED(00000003)
depth=2 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", CN = Go Daddy Root Certificate Authority - G2
verify return:1
depth=1 C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure
Certificate Authority - G2
verify return:1
depth=0 CN = ejemplo.com
verify return:1
---
Certificate chain
 0 s:CN = ejemplo.com
   i:C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure Certificate
Authority - G2
   a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
   v:NotBefore: Aug 10 18:28:07 2025 GMT; NotAfter: Aug 10 18:28:07 2026 GMT
-----BEGIN CERTIFICATE-----
MIIGfjCCBWagAwIBAgIILbTAWAxlFGswDQYJKoZIhvcNAQELBQAwgbQxCzAJBgNV
BAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQHEwpTY290dHNkYWxlMRow
GAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UECxMkaHR0cDovL2NlcnRz
LmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQDEypHbyBEYWRkeSBTZWN1
cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwHhcNMjUwODEwMTgyODA3WhcN
MjYwODEwMTgyODA3WjAWMRQwEgYDVQQDEwtlamVtcGxvLmNvbTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALOk872/AJNcY2QneFsM98vQPSpOyRLdO2De
DJgngqk58rDOOIffE88sD9SlS10ysNw0yjq9qBegsKBsi0yPM3zyKmWZtWLKeCdi
r0zl5ReFZbROyTSCkyEwiAG7Qtn+k8xV+0B3hlucM/+ts9SBXAa6Kb1zWxu3M/hm
897C6Z/lh5CLNOkUvjsXrVQKzw/p3VG/Px2KivanalxTjgBoYOHViyafqsC+Axg7
+F3ESGQWO84vjPMPr3K+0OqPMBML0pkABgB39nYj3ZRzJ0uv3NDOeNH03j4XjZ+x
nqTWO8L5nj4O3KUBD1KzTcLY4pN1U3gCgPXYtitTLZ6o8v6iSV8CAwEAAaOCAy8w
ggMrMAwGA1UdEwEB/wQCMAAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMC
MA4GA1UdDwEB/wQEAwIFoDA5BgNVHR8EMjAwMC6gLKAqhihodHRwOi8vY3JsLmdv
ZGFkZHkuY29tL2dkaWcyczEtNTgwMjguY3JsMF0GA1UdIARWMFQwSAYLYIZIAYb9
bQEHFwEwOTA3BggrBgEFBQcCARYraHR0cDovL2NlcnRpZmljYXRlcy5nb2RhZGR5
LmNvbS9yZXBvc2l0b3J5LzAIBgZngQwBAgEwdgYIKwYBBQUHAQEEajBoMCQGCCsG
AQUFBzABhhhodHRwOi8vb2NzcC5nb2RhZGR5LmNvbS8wQAYIKwYBBQUHMAKGNGh0
dHA6Ly9jZXJ0aWZpY2F0ZXMuZ29kYWRkeS5jb20vcmVwb3NpdG9yeS9nZGlnMi5j
```


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

cnQwHwYDVR0jBBgwFoAUQMK9J47MNIMwojPX+2yz8LQsgM4wFgYDVR0RBA8wDYIL
ZWplbXBsby5jb20wHQYDVR0OBBYEFEu1pXs3HZitLw9ehdpA2g2WMJY9MIIBgAYK
KwYBBAHWeQIEAgSCAXAEggFsAWoAdwDXbX0Q0af1d8LH6V/XAL/5gskzWmXh0LMB
cxfAyMVpdwAAAZiVPW2bAAAEAwBIMEYCIQCXNgQ/ExFdFjainlxJW9wDAE2sylMn
TSLy7WB+7QiwTglhAP2kWyOEj/vbJhR35O/C9DQbypSibxU+vYAyw4cPxTJnAHYA
rKswcGzr7lQx9BPS9JFfER5CJEOx8qaMTzwrO6ceAsMAAAGYlT1u4gAABAMARzBF
AiEA9/zwS8b7AFr3fTZ8UbQkYXWVm+4hJMyN4E7eRFV9SiMCIAVu7MxdeaLBZgmw
8LfVqrFSiiMVTdFu6znYTqyLEuJaAHcAyzj3FYl8hKFEX1vB3fvJbvKaWc1HCmkF
hbDLFMMUWOcAAAGYlT1vXAAABAMASDBGAiEAkM5BU7HG8cU6GeacvFWFtEyB1LVl
+CjICf8db5bzni0ClQDvRWR5P5kvk4dfEOnbosrtVWVfE77V7pMf1cW6aC1FRjAN
BgkqhkiG9w0BAQsFAAOCAQEAjBxGi2yxCCHGXbsSbT8BBu0N2DI/lA1QG2QG/Byb
qjCoOJv2V2mthhZodohnVeceC4ZHa/QC9/VmXPscT/zNlwuY7TOQB9IIF7GjBPch
D3Hrf70+JQKZVkYukf879VLROU9aG+zRZZhF3p4g61rJUxYHSeVt0D68wQgIQnlg
KUa9Iw/N+ncKr3cL1Fao8ssmEtfkM+DtgAGcJML28EHmL2X/gtUcaqLUIsOBSQFU
gSzowWzq0soYnRZ4ePkMI84OwCn/gKqvKQEzOGOd/iU/l+ogNIjZJd/f6IUguVjF
rA0sMB2QMPQ6o88Kry1D7ghp3T73x6UCUKvEiUPYF/GABA==
-----END CERTIFICATE-----
1 s:C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure Certificate Authority - G2
i:C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", CN = Go Daddy Root Certificate Authority - G2
a:PKEY: rsaEncryption, 2048 (bit); sigalg: RSA-SHA256
v:NotBefore: May 3 07:00:00 2011 GMT; NotAfter: May 3 07:00:00 2031 GMT
-----BEGIN CERTIFICATE-----
MIIE0DCCA7igAwIBAgIBBzANBgkqhkiG9w0BAQsFADCBgzELMAkGA1UEBhMCVVMx
EDAOBgNVBAgTB0FyaXpvbmExEzARBgNVBAcTClNjb3R0c2RhbGUxGjAYBgNVBAoT
EUdvRGFkZHkuY29tLCBJbmMuMTEwLwYDVQQDEyhHbyBEYWRkeSBSb290IENlcnRp
ZmljYXRlIEF1dGhvcml0eSAtIEcyMB4XDTExMDUwMzA3MDAwMFoXDTMxMDUwMzA3
MDAwMFowgbQxCzAJBgNVBAYTAlVTMRAwDgYDVQQIEwdBcml6b25hMRMwEQYDVQQH
EwpTY290dHNkYWxlMRowGAYDVQQKExFHb0RhZGR5LmNvbSwgSW5jLjEtMCsGA1UE
CxMkaHR0cDovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkvMTMwMQYDVQQD
EypHbyBEYWRkeSBTZWN1cmUgQ2VydGlmaWNhdGUgQXV0aG9yaXR5IC0gRzIwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC54MsQ1K92vdSTYuswZLiBCGzD
BNliF44v/z5lz4/OYuY8UhzaFkVLVat4a2ODYpDOD2lsmcgaFItMzEUz6ojcnqOv
K/6AYZ15V8TPLvQ/MDxdR/yaFrzDN5ZBUY4RS1T4KL7QjL7wMDge87Am+GZHY23e
cSZHjzhHU9FGHbTj3ADqRay9vHHZqm8A29vNMDp5T19MR/gd71vCxJ1gO7GyQ5HY
pDNO6rPWJ0+tJYqlxvTV0KaudAVkV4i1RFXULSo6Pvi4vekyCgKUZMQWOlDxSq7n
eTOvDCAHf+jfBDnCaQJsY1L6d8EbyHSHyLmTGFBUNUtpTrw700kuH9zB0lL7AgMB
AAGjggEaMIIBFjAPBgNVHRMBAf8EBTADAQH/MA4GA1UdDwEB/wQEAwIBBjAdBgNV
HQ4EFgQUQMK9J47MNIMwojPX+2yz8LQsgM4wHwYDVR0jBBgwFoAUOpqFBxBnKLbv
9r0FQW4gwZTaD94wNAYIKwYBBQUHAQEEKDAmMCQGCCsGAQUFBzABhhhodHRwOi8v
b2NzcC5nb2RhZGR5LmNvbS8wNQYDVR0fBC4wLDAqoCigJoYkaHR0cDovL2NybC5n
b2RhZGR5LmNvbS9nZHJvb3QtZzIuY3JsMEYGA1UdIAQ/MD0wOwYEVR0gADAzMDEG
CCsGAQUFBwIBFiVodHRwczovL2NlcnRzLmdvZGFkZHkuY29tL3JlcG9zaXRvcnkv
MA0GCSqGSIb3DQEBCwUAA4IBAQAIfmyTEMg4uJapkEv/oV9PBO9sPpyIBslQj6Zz
91cxG7685C/b+LrTW+C05+Z5Yg4MotdqY3MxtfWoSKQ7CC2iXZDXtHwlTxFWMMS2
RJ17LJ3lXubvDGGqv+QqG+6EnriDfcFDzkSnE3ANkR/0yBOtg2DZ2HKocyQetawi
DsoXiWJYRBuriSUBAA/NxBti21G00w9RKpv0vHP8ds42pM3Z2Czqrpv1KrKQ0U11
Gio/ikGQI31bS/6kA1ibRrLDYGCD+H1QQc7CoZDDu+8CL9IVVO5EFdkKrqeKM+2x
LXY2JtwE65/3YR8V3Idv7kaWKK2hJn0KCacuBKONvPi8BDAB
-----END CERTIFICATE-----

Server certificate
subject=CN = ejemplo.com
issuer=C = US, ST = Arizona, L = Scottsdale, O = "GoDaddy.com, Inc.", OU = http://certs.godaddy.com/repository/, CN = Go Daddy Secure Certificate Authority - G2

No client certificate CA names sent
Peer signing digest: SHA256
Peer signature type: RSA-PSS
Server Temp Key: X25519, 253 bits

SSL handshake has read 3447 bytes and written 507 bytes
Verification: OK

New, TLSv1.3, Cipher is TLS_AES_128_GCM_SHA256

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

```
Server public key is 2048 bit
Secure Renegotiation IS NOT supported
Compression: NONE
Expansion: NONE
No ALPN negotiated
Early data was not sent
Verify return code: 0 (ok)
---
---
Post-Handshake New Session Ticket arrived:
SSL-Session:
    Protocol  : TLSv1.3
    Cipher    : TLS_AES_128_GCM_SHA256
    Session-ID: 305A72D260D6780CF559339416C6D63799BBC98D7E59969D053143421B279647
    Session-ID-ctx:
    Resumption PSK: F38E2B7084824AE58BD870ED2DF81BB3FAB270268D6E4DB5785DCD74B849A402
    PSK identity: None
    PSK identity hint: None
    SRP username: None
    TLS session ticket lifetime hint: 604800 (seconds)
    TLS session ticket:
    0000 - b9 40 18 c8 11 f3 7e fb-99 82 80 e8 d7 35 d0 ea   .@....~.....5..
    0010 - c8 53 27 17 2e 17 67 c5-ad b0 06 a9 6a 55 54 1c   .S'...g.....jUT.
    0020 - 01 a0 53 5b 1f f3 d6 28-53 2a e8 0b 01 88 ce f2   ..S[...(S*......
    0030 - 43 cd b7 39 32 54 b3 65-be 80 4c ee 9c 8e 99 91   C..92T.e..L.....
    0040 - 10 63 db 0b 66 7c 89 27-c8 d6 db 38 a1 5e 63 87   .c..f|.'...8.^c.
    0050 - b7 10 c7 19 0f a1 ca 17-cc d3 42 c0 7a 91 f0 34   ..........B.z..4
    0060 - 17 61 ec 0e 3f 9a 1e 27-6c                        .a..?..'l

    Start Time: 1761059999
    Timeout   : 7200 (sec)
    Verify return code: 0 (ok)
    Extended master secret: no
    Max Early Data: 0
---
read R BLOCK
DONE
```

Recomendaciones:

I. Eliminar suites 3DES/64-bit y habilitar solo TLS1.2/1.3 con suites ECDHE+AES-GCM o CHACHA20-POLY1305.

II. Reemplazar el certificado autofirmado por un certificado emitido por CA confiable y enviar la cadena de certificados completa.

III. Re-scanear con Nessus y SSL para verificar corrección. Prioridad: Alta.

C.P. SERGIO DANIEL PEÑAYO
Director Interino
Dirección de Auditoría Interna institucional
Dirección Nacional de Propiedad Intelectual

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

tenable Nessus

basic scan web dinapi

Report generated by Tenable Nessus™ Tue, 21 Oct 2025 09:35:39 -05

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

TABLE OF CONTENTS

Vulnerabilities by Host

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

Vulnerabilities by Host

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

DC2.DINAPI.GOV.PY

Vulnerabilities Total: 49

SEVERITY	CVSS V3.0	VPR SCORE	EPSS SCORE	PLUGIN	NAME
HIGH	7.5	6.1	0.406	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	-	-	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.5	-	-	57582	SSL Self-Signed Certificate
MEDIUM	6.5	-	-	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	-	-	157288	TLS Version 1.1 Deprecated Protocol
INFO	N/A	-	-	42255	NFS Server Superfluous
INFO	N/A	-	-	10223	RPC portmapper Service Detection
INFO	N/A	-	-	45590	Common Platform Enumeration (CPE)
INFO	N/A	-	-	10736	DCE Services Enumeration
INFO	N/A	-	-	11002	DNS Server Detection
INFO	N/A	-	-	54615	Device Type
INFO	N/A	-	-	12053	Host Fully Qualified Domain Name (FQDN) Resolution
INFO	N/A	-	-	43829	Kerberos Information Disclosure
INFO	N/A	-	-	25701	LDAP Crafted Search Request Server Information Disclosure
INFO	N/A	-	-	20870	LDAP Server Detection
INFO	N/A	-	-	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	-	-	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure

C.P. SERGIO DANIEL PEÑA[illegible]
Director Interino
Dirección de Auditoría Interna Institucional
Dirección Nacional de Propiedad Intelectual

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

INFO	N/A	-	-	26917	Microsoft Windows SMB Registry : Nessus Cannot Access the Windows Registry
INFO	N/A	-	-	11011	Microsoft Windows SMB Service Detection
INFO	N/A	-	-	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	-	-	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remc check)
INFO	N/A	-	-	11219	Nessus SYN scanner
INFO	N/A	-	-	19506	Nessus Scan Information
INFO	N/A	-	-	10884	Network Time Protocol (NTP) Server Detection
INFO	N/A	-	-	209654	OS Fingerprints Detected
INFO	N/A	-	-	11936	OS Identification
INFO	N/A	-	-	117886	OS Security Patch Assessment Not Available
INFO	N/A	-	-	10180	Ping the remote host
INFO	N/A	-	-	11111	RPC Services Enumeration
INFO	N/A	-	-	53335	RPC portmapper (TCP)
INFO	N/A	-	-	10940	Remote Desktop Protocol Service Detection
INFO	N/A	-	-	70657	SSH Algorithms and Languages Supported
INFO	N/A	-	-	149334	SSH Password Authentication Accepted
INFO	N/A	-	-	10881	SSH Protocol Versions Supported
INFO	N/A	-	-	10267	SSH Server Type and Version Information
INFO	N/A	-	-	56984	SSL / TLS Versions Supported
INFO	N/A	-	-	10863	SSL Certificate Information
INFO	N/A	-	-	70544	SSL Cipher Block Chaining Cipher Suites Supported
INFO	N/A	-	-	21643	SSL Cipher Suites Supported
INFO	N/A	-	-	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	-	-	156899	SSL/TLS Recommended Cipher Suites

DC2.DINAPI.GOV.PY

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

INFO	N/A	-	-	96982	Server Message Block (SMB) Protocol Version 1 Enabled (uncredentialed check)
INFO	N/A	-	-	22964	Service Detection
INFO	N/A	-	-	121010	TLS Version 1.1 Protocol Detection
INFO	N/A	-	-	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	-	-	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	-	-	64814	Terminal Services Use SSL/TLS
INFO	N/A	-	-	10287	Traceroute Information
INFO	N/A	-	-	10150	Windows NetBIOS / SMB Remote Host Information Disclosure

* indicates the v3.0 score was not available; the v2.0 score is shown

DC2.DINAPI.GOV.PY

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

ANEXO 3

Análisis Realizado con Security Headers

Revisión de los Mecanismos de Autenticación de www.dinapi.gov.py

1. Objetivo

Evaluar la seguridad y los mecanismos de autenticación dentro del portal institucional.

2. Alcance

- Portal público: www.dinapi.gov.py
- Análisis pasivo y revisión de:
  - HTTPS y certificado SSL/TLS
  - Encabezados de seguridad HTTP
  - Cookies visibles y configuración pública
  - Recursos externos cargados por la web

3. Metodología

- Inspección visual y análisis de la web pública.
- Uso de herramientas pasivas de verificación de seguridad (ej. SecurityHeaders.io).
- Documentación de hallazgos y recomendaciones basadas en observaciones públicas.

4. Hallazgos

Ítem	Descripción	Estado / Observación
HTTPS / SSL	El portal utiliza HTTPS con certificado válido y cifrado TLS moderno.	Cumple buenas prácticas.
Encabezados de seguridad	Algunos encabezados estándar están presentes; se recomienda implementar medidas adicionales como CSP o X-Frame-Options.	Se recomienda optimización.
Cookies	Cookies visibles cumplen funciones básicas; se sugiere revisar internamente para asegurar flags Secure y HttpOnly si se manejan datos sensibles.	Se recomienda revisión.
Formularios	No existen formularios de login; la web pública no requiere autenticación.	No aplica.
Recursos externos	Se cargan recursos de terceros; se recomienda verificar integridad y seguridad.	Se recomienda mayor control.

5. Recomendaciones

1. **Reforzar encabezados de seguridad HTTP** para proteger la integridad de la web.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

2. **Auditar cookies visibles** y garantizar flags Secure y HttpOnly para datos sensibles.

3. **Revisar seguridad de recursos externos** utilizados en la web.

4. Mantener actualizado el **certificado SSL/TLS** y utilizar cifrado moderno.

5. Informe del Desarrollador Web según memo DCI nº 87/2025 recibido en DAII el 17/10/25

- Lista de **recursos externos** utilizados en la web y su gestión de seguridad.

Los recursos externos utilizados en nuestro sitio web son los siguientes:

Fuentes de Google:
https://fonts.googleapis.com
Google Analytics y Tag Manager:
https://www.google-analytics.com/analytics.js
https://www.googletagmanager.com/gtag/js?id=G-6ETLXB6V59&cx=c&gtm=4e5af1
API de Facebook:
https://connect.facebook.net/es_LA/sdk.js?hash=f833a9e6ed7af47551a08cec77bd7999
API de Twitter:
https://platform.twitter.com/widgets/widget_iframe.2f70fb173b9000da126c79afe2098f02.html?origin=https%3A%2F%2Fwww.dinapi.gov.py
Gestión de seguridad: Estos recursos se integran siguiendo buenas prácticas de seguridad y se cargan a través de conexiones seguras (HTTPS). Se aplican políticas de actualización y control conforme a los lineamientos internos de la DINAPI.

- **Configuración interna de encabezados de seguridad HTTP** implementados en el portal.

Ya due enviada por la Dirección de Informàtica.

- **Políticas de cookies** y manejo de datos visibles en la web pública.

Políticas de cookies y manejo de datos visibles en la web pública
Nuestro sitio web no utiliza cookies con fines de seguimiento o marketing.
El sistema de gestión de contenidos (CMS) implementa únicamente una cookie de sesión estrictamente necesaria para la funcionalidad básica del sitio. Esta cookie es temporal, no almacena datos personales y no se utiliza para rastrear a los usuarios.

- Procedimientos de **actualización y mantenimiento del certificado SSL/TLS**.?

Ya fue enviado por la Dirección de Informática.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

ANEXO 4

ANALISIS CON VALIDADORES DNS, SSL LABS

EVALUACIÓN DE LA CONFIGURACIÓN DE SEGURIDAD DE LA INFRAESTRUCTURA DEL SITIO WEB INSTITUCIONAL DE LA DINAPI

1. Introducción

En el marco de la auditoría informática realizada sobre el portal institucional de la Dirección Nacional de Propiedad Intelectual (DINAPI), cuyo dominio principal es http://www.dinapi.gov.py, se efectuó una evaluación de la configuración de seguridad de la infraestructura tecnológica que soporta el sitio web institucional.

El propósito de esta evaluación fue determinar el grado de exposición ante riesgos de seguridad derivados de configuraciones inadecuadas, servicios innecesarios, protocolos obsoletos o ausencia de controles técnicos recomendados.

2. Alcance

El análisis abarcó los siguientes componentes:

- Dominio principal y subdominios asociados.
- Servidor web y tecnologías visibles públicamente.
- Certificados digitales y configuración TLS/SSL.
- Cabeceras HTTP de seguridad.
- Puertos y servicios detectados expuestos a Internet.
- Registros DNS relevantes (SPF, DKIM, DMARC).

*No se incluyó el acceso interno a servidores ni la realización de pruebas intrusivas, respetando los límites de una auditoría no invasiva.

3. Metodología

Se aplicaron técnicas de auditoría pasiva y activa controlada.

Herramientas utilizadas: Shodan, Nmap, curl, SSL Labs, SecurityHeaders.io y validadores DNS.

4. Resultados del Análisis

4.1 Servidor Web y Tecnologías Detectadas

Servidor Web: nginx (versión no divulgada)

Puerto abierto: 443/tcp (HTTPS) únicamente

Puertos cerrados/no visibles: 80/tcp (HTTP) y servicios administrativos no expuestos

Riesgo: Bajo. La exposición limitada a un único puerto seguro (HTTPS) disminuye el riesgo de ataques remotos.

Observación: El servidor está configurado para redirigir HTTP → HTTPS, lo que refuerza la seguridad de la comunicación.

Recomendación: Mantener la configuración actual y asegurar que cualquier otro puerto administrativo permanezca inaccesible públicamente.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

4.2 Certificados Digitales y Cifrado

El sitio usa HTTPS sobre el puerto 443

TLS/SSL habilitado (detalles completos requieren SSL Labs)

Redirección 301 asegura tráfico HTTPS

Recomendación: Validar que TLS 1.2 y 1.3 estén habilitados y deshabilitar versiones obsoletas.

4.3 Cabeceras HTTP de Seguridad

Content-Security-Policy: upgrade-insecure-requests → ayuda a forzar HTTPS

Access-Control-Allow-Origin: → revisable según política interna

Cabeceras de seguridad adicionales como HSTS, X-Frame-Options, X-Content-Type-Options y Referrer-Policy no detectadas

Riesgo: Medio. Se recomienda implementar cabeceras adicionales para reforzar seguridad frente a clickjacking, XSS y filtrado de información.

4.4 DNS y Políticas de Correo

Verificar registros DNS A, MX, CNAME, TXT

SPF, DKIM y DMARC no verificados en esta prueba (recomendable auditar)

Recomendación: Implementar autenticación de correo institucional para prevenir suplantación.

4.5 Otros controles

Redirección HTTP → HTTPS: Correcta

Indexación de directorios: No detectada

Banner del servidor: Oculto → bueno para seguridad

Cookies: Revisar flags Secure y HttpOnly

5. Conclusiones Generales

La infraestructura web de la DINAPI presenta una exposición mínima con un único puerto seguro (443/tcp) y redirección a HTTPS.

No obstante, se identifican oportunidades de mejora en la configuración de cabeceras HTTP, autenticación de correo y revisión de TLS/SSL.

6. Recomendaciones Finales

- Mantener puerto 443 como único expuesto y proteger servicios internos.
- Implementar cabeceras HTTP adicionales: HSTS, X-Frame-Options, X-Content-Type-Options, Referrer-Policy.
- Validar y reforzar TLS 1.2/1.3, deshabilitando versiones obsoletas.
- Auditar y configurar SPF, DKIM y DMARC para correo institucional.
- Revisar seguridad de cookies ("Secure", "HttpOnly").
- Documentar configuraciones críticas y establecer revisiones periódicas.

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

Lic. Diego González
Auditor Informático
Dirección de Auditoría Interna Institucional

ANEXO 5

OPWASP TOP TEN

Informe Técnico de Auditoría Web – DINAPI - Owasp

Tema: Identificación y Clasificación de Vulnerabilidades en Aplicaciones Web (OWASP Top 10)

Auditor: Diego González

Fecha: 14/10/2025

Entidad auditada: Dirección Nacional de Propiedad Intelectual (DINAPI)

URL auditada: https://www.dinapi.gov.py

1. Introducción

El presente informe tiene por objeto identificar y clasificar vulnerabilidades potenciales en la aplicación web institucional de la Dirección Nacional de Propiedad Intelectual (DINAPI), conforme al estándar OWASP Top 10 (2021). El análisis se realizó de **forma no intrusiva**, sin ejecutar **pruebas de penetración o alteración de servicios**, limitándose al reconocimiento pasivo, inspección de cabeceras, revisión de código visible en cliente y verificación de buenas prácticas de seguridad en la capa web.

2. Alcance y Metodología

Alcance:

- Portal principal: https://www.dinapi.gov.py/portal/v3/
- Formularios de contacto y búsqueda pública
- Certificados y configuración HTTPS
- Revisión de componentes JavaScript visibles

Metodología aplicada:

1. Recolección de información pública (WHOIS, cabeceras, certificados TLS).
2. Revisión de configuración de seguridad del servidor web.
3. Identificación de librerías y frameworks del lado del cliente.
4. Clasificación de vulnerabilidades según OWASP Top 10 (2021).
5. Evaluación de riesgo (bajo, medio, alto).
6. Recomendaciones correctivas.

3. Resultados del análisis

N°	Riesgo OWASP	Descripción del Hallazgo	Evidencia / Indicio	Nivel de Riesgo	Recomendación
1	A05 – Security Misconfiguration	El sitio expone rutas y recursos estáticos que podrían revelar estructura interna (por	Recursos accesibles vía navegador sin restricción.	Medio	Revisar permisos y ocultar directorios públicos innecesarios mediante reglas

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

		ejemplo: /portal/v3/assets/ y /plugins/).			del servidor.
2	A02 – Cryptographic Failures	Aunque usa HTTPS, algunos subrecursos podrían cargarse desde fuentes sin HTTPS.	Referencias mixtas detectadas en el código fuente del portal v3.	Medio	Forzar HSTS y eliminar contenido mixto.
3	A06 – Vulnerable and Outdated Components	Se observan librerías JavaScript potencialmente desactualizadas (por ejemplo jQuery 3.5.1).	Código fuente visible en el cliente.	Medio	Actualizar jQuery y dependencias JS a versiones seguras.
4	A09 – Security Logging and Monitoring Failures	No se evidencian indicadores visibles de registro o monitoreo de accesos.	Sin aviso de monitoreo ni detección de intentos fallidos.	Bajo	Implementar mecanismos de registro centralizado de accesos.
5	A04 – Insecure Design	El sitio no parece implementar protección CSRF visible en formularios simples de búsqueda o contacto.	Formularios sin tokens CSRF visibles en el código fuente.	Medio	Incluir token antifalsificación y validación en backend.
6	A01 – Broken Access Control (potencial)	Algunos enlaces con parámetros (?id=) podrían ser vulnerables a manipulación si no existe control en backend.	Observado en URL pública /ver_detalle.php?id=xxx (ejemplo).	Medio	Validar en servidor que el usuario tenga permiso para acceder a cada recurso solicitado.
7	A07 – Identification and Authentication Failures	Formularios de login no visibles desde el portal principal, pero podrían existir en subsistemas.	Referencias a sistemas externos de autenticación.	Bajo	Aplicar política unificada de autenticación segura (bloqueo de intentos, MFA).
8	A08 – Software and Data Integrity Failures	No se observa uso de firma digital o integridad en scripts de terceros.	Scripts externos cargados sin atributos integrity ni crossorigin.	Medio	Incluir atributos SRI (Subresource Integrity) en scripts externos.

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

Lic. Diego González
Auditor informático
Dirección de Auditoría Interna Institucional

4. Análisis General

El portal institucional de DINAPI presenta una estructura web funcional, con uso adecuado de HTTPS, pero aún se observan mejoras posibles en configuraciones de seguridad, actualización de componentes y controles de validación en formularios. No se detectaron vulnerabilidades críticas visibles de forma pasiva, pero se recomienda realizar una evaluación más profunda (autorizada) sobre los módulos de trámites en línea y autenticación de usuarios.

5. Recomendaciones Generales

1. Implementar cabeceras de seguridad: Content-Security-Policy, X-Frame-Options: DENY, X-Content-Type-Options: nosniff, Strict-Transport-Security.
2. Actualizar frameworks y librerías JavaScript regularmente.
3. Revisar accesos directos a recursos y restringir directorios públicos.
4. Incluir tokens CSRF en formularios sensibles.
5. Implementar registro de eventos de seguridad con alertas automáticas.
6. Aplicar auditorías periódicas OWASP y análisis SCA/SAST a futuro.

6. Conclusión

El análisis permite concluir que la aplicación web de DINAPI se encuentra en un nivel aceptable de seguridad básica, aunque con riesgos medios y mejorables en cuanto a configuración, diseño y actualización de componentes. Se recomienda mantener un programa continuo de revisión y capacitación en desarrollo seguro conforme al marco OWASP Top 10.

Lic. Diego González
Auditor Informático
Direccion de Auditoria Interna Institucional

C.P. SERGIO DANIEL P...
Director Interino
Dirección de Auditoría Interna ...
Dirección Nacional de Propie...