

**INFORME DE
SEGUIMIENTO
FINAL**

**Construir, Adquirir e Implementar
- Sistemas desarrollados por áreas
independientes de la SDG SIT
CSI 13/2024**

Palabras Clave

Sistemas - Desarrollo - Metodología - Centralización - Procesos

**Índice del
Informe**

Temática	Pág. N.º
Síntesis Ejecutiva	3
Informe Analítico	4
Destinatarios	4
Tipo de auditoría	4
Marco de referencia	4
Alcance	4
Aclaraciones previas	5
Conclusión	6
Detalle de Observaciones, Causas, Efectos y Recomendaciones	7
1. Debilidades en la gestión y control de cambios desarrollados por fuera de la SDG SIT	7
2. Deficiencias en la administración de los ambientes producción, homologación y desarrollo	8
3. Ausencia de documentación para la correcta trazabilidad de los cambios	10
Anexos	
A. Unidad auditada y Normativa aplicable	13
B. Datos Referenciales	16
C. Comunicación con la Dirección y otras áreas con competencia	18
D. Análisis del Sistema de Control Interno	20

OBJETO
Sistemas desarrollados por áreas independientes a la SDG SIT
OBJETIVO
Analizar la implementación de la metodología de desarrollo vigente y el alineamiento a los procedimientos e infraestructura definida por la SDG SIT para la gestión de cambios.
CONCLUSIÓN
<p>En virtud de las tareas de seguimiento realizadas, se puede concluir que no se ha efectuado un avance respecto de la definición sobre centralizar los desarrollos en el área de la Subdirección General de Sistemas y Telecomunicaciones, o si se coordinarán actividades conjuntas entre las áreas para alinear y actualizar los sistemas ya desarrollados, conforme lo indica la metodología establecida, y bajo la supervisión de la mencionada Subdirección.</p> <p>Esta situación incrementa el riesgo de que surjan nuevos desarrollos que no cuenten con las medidas de seguridad requeridas y que pueda verse afectada la integridad, confidencialidad y disponibilidad de la información..</p>

ESTADO DE SITUACIÓN DE LAS OBSERVACIONES Y RECOMENDACIONES DE AUDITORÍA INTERNA

En función de las tareas de seguimiento realizadas, se pudo conocer que no se han efectuado avances respecto de los planes de acción remitidos oportunamente. Hasta el momento no se ha creado un Comité, como tampoco se evidencian tareas de relevamiento para conocer las aplicaciones desarrolladas por áreas ajenas a la Subdirección General de Sistemas y Telecomunicaciones.

Por otro lado, en cuanto a la segregación de la administración de servidores pertenecientes a la Dirección de Seguridad de la Información, han dejado supeditado el traspaso al área de competencia, hasta tanto se resuelva la organización de la estructura del Organismo.

Finalmente, se observaron avances en la regularización de permisos de agentes en ambientes bajos (Desarrollo y Homologación), como también en la mejora de la documentación de las solicitudes de cambios, gestionadas a través de Redmine.

ÁREAS RESPONSABLES DE IMPLEMENTACIÓN DE ACCIONES

- ⇒ Dirección de Seguridad de la Información (ARCA)
- ⇒ Dirección de Gestión del Riesgo (SDG CAD)
- ⇒ Dirección Regional Aduanera Noroeste (SDG OAI)
- ⇒ Subdirección General Sistemas y Telecomunicaciones (AFIP)

Ciudad Autónoma de Buenos Aires.

Destinatarios

- Subdirección General de Control Aduanero
- Dirección de Seguridad de la Información (ARCA)
- Subdirección General de Operaciones Aduaneras del Interior
- Subdirección General Sistemas y Telecomunicaciones

**Tipo de
auditoría**

- Según su origen: Programada
- Según su extensión: Operacional
- Según su temática: Sistemas Informáticos

**Marco de
referencia**

Mediante la Instrucción General AFIP N° 1/2023 SDG SIT – “Procedimiento. Ciclo de vida de los productos informáticos. Responsabilidad de las áreas que desarrollan, administran o los gestionan” del 04 de agosto de 2023, se derogó la instrucción general que establecía la exclusiva responsabilidad de los desarrollos de sistemas y páginas web en la Subdirección General de Sistemas y Telecomunicaciones, en adelante SDG SIT.

En virtud de lo mencionado, se establece que cualquier área a la que el titular del Organismo haya otorgado misiones y funciones de desarrollo, mediante actos dispositivos, podrá llevar a cabo el desarrollo de aplicaciones cumpliendo las pautas establecidas por la Instrucción General N° 2/2021 (SDG SIT) – “Lineamientos Generales para el Desarrollo de Software de la AFIP”.

Asimismo, instruye que los sistemas desarrollados por las áreas responsables deberán desarrollarse, testearse, homologarse, instalarse, mantenerse y ejecutarse en la “infraestructura AFIP” la cual es administrada por la SDGSIT, que será responsable de proveer los diferentes ambientes para cumplir el ciclo de desarrollo de software (Desarrollo, Testing, Producción). En caso de que las áreas intervenientes que se encuentran alcanzadas por la presente tengan ambientes fuera de la “infraestructura AFIP”, éstas deberán incluir en su planificación las tareas de migración de esos ambientes, priorizándose en función a su complejidad, impacto operativo, riesgo y criticidad de los productos informáticos en cuestión.

Por último, establece que el Departamento Monitoreo y Evaluación de Seguridad dependiente de la DI SEIN, en función de sus competencias, efectuará el monitoreo de todos los sistemas en trato a través de los registros ingestados en la herramienta de Gestión de Logs con características SIEM (Security Information and Event Management).

Alcance

Las tareas se desarrollaron según la metodología establecida por el Manual de Auditoría Interna de la Unidad de Auditoría Interna de la Agencia de Recaudación y Control Aduanero en un todo de acuerdo con las Normas de

Auditoría Interna Gubernamental (Resolución SIGEN N.º152/02) en el marco de la Ley N.º24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.

El trabajo abarcó el relevamiento y análisis del cumplimiento de la normativa aplicable y las actividades y procedimientos de control relativos a la gestión de Sistemas desarrollados por áreas independientes a la SDGSIT por el período comprendido entre el 15 de febrero de 2024 y el 30 de abril de 2024 (*Unidad auditable y Normativa aplicable en el Anexo A*).

El período de seguimiento transcurrió entre el 21 de agosto de 2024 y el 24 de septiembre de 2025 (*mayor detalle en el Anexo B*).

Se solicitó la opinión de las áreas auditadas y/o con injerencia en el tema aquí tratado (*mayor detalle en el Anexo C*).

El presente informe se encuentra referido a las observaciones, efectos y opiniones sobre el objeto de la tarea realizada hasta el 24 de septiembre de 2025 y no contempla la eventual ocurrencia de hechos posteriores que puedan modificar su contenido.

Las observaciones y/o hallazgos presentados en este informe corresponden a la situación observada al momento de realizar el trabajo. Al ser el control interno y su ejecución, aspectos dinámicos y dependientes en mayor o menor medida de factores humanos, existe un margen de riesgo que no puede ser cubierto en su totalidad.

El trabajo realizado incluyó un análisis de pistas electrónicas –ya sean pistas de auditoría, registros de eventos en los sistemas, archivos generados en los sistemas, etc., basándose en el principio de confianza en que toda información suministrada por los responsables, es íntegra, completa y veraz.

La evaluación de la efectividad del control de aquellos riesgos que se han pretendido mitigar ayuda a disuadir la concreción de fraude. Cabe aclarar, que en el desempeño de la labor de auditoría pueden realizarse pruebas adicionales dirigidas a la identificación de indicadores de fraude ante deficiencias significativas de control, así como proceder a informar situaciones presuntamente anómalas o irregulares detectadas en las tareas de auditoría que resulten contrarias a los valores, principios básicos y pautas de comportamiento según lo establecido en el Código de Ética y demás normativa vigente en la materia, para su eventual evaluación por parte del área pertinente.

Se deja constancia de que la presente auditoría tiene como objetivo principal la evaluación del sistema del control interno del proceso auditado, siendo las áreas auditadas, en el marco del sistema de control interno establecido por la Ley N.º 24.156, los responsables de determinar los mecanismos de control adecuados a fin de prevenir, detectar y tratar las posibles actividades fraudulentas, así como de las investigaciones de carácter disciplinario.

Se destaca que el presente no constituye un dictamen técnico y/o jurídico ni instrucción de servicio, los cuales deberán ser expedidos por las instancias de gestión competentes. Se procura poner en conocimiento de las áreas de gestión, desvíos o posibles desvíos para que éstas analicen si comparten esa calificación y, en su caso, decidan la adopción de cursos de acción correctivos, tomando en cuenta los sugeridos por la Unidad de Auditoría Interna, o si están dispuestas a asumir el riesgo que los mismos implican.

Las tareas realizadas incluyeron:

- Consulta a las áreas auditadas con competencia en la solución sobre el grado de avance en la resolución de los aspectos observados.
- Análisis y revisión de la documentación recibida.
- Elaboración del Informe de Seguimiento Final (ISF).

Aclaraciones
previas

El Informe Preliminar de Auditoría Interna fue emitido el 16 de julio de 2024; el Informe de Auditoría Interna el 21 de agosto de 2024.

Cabe destacar que al momento de la emisión de los informes en sus versiones Preliminar e Informe de Auditoría, la Dirección de Seguridad de la Información dependía de la Subdirección General Institucional. A instancias del presente informe la Dirección de Seguridad de la Información depende en forma directa de la máxima autoridad del Organismo, es por ello que se actualizan los destinatarios.

Con la emisión del presente informe se procede al archivo de las actuaciones.

Reserva Documental

En cumplimiento de lo establecido por los artículos 1º; 7º inciso a) y 32 inciso i), concordantes y complementarios de la Ley N.º27.275 de Derecho de Acceso a la Información Pública, las actuaciones vinculadas a la presente auditoría, mantendrán el carácter de "Reservado", asignado por la Disposición DI-2018-8-E-AFIP-AFIP, hasta la fecha en que sea incorporado en la base de datos del micrositio "Transparencia Activa" el Informe de Seguimiento Final o el último Informe de Auditoría correspondiente a la misma.

En tal sentido, hasta que se verifique dicha incorporación, el contenido de los Informes de Auditoría y de las actuaciones relacionadas a los mismos sólo serán de acceso pleno para las áreas auditadas, las áreas de las que ellas dependan y demás dependencias responsables de la regularización de los desvíos observados, incluidas las autoridades superiores del Organismo en función de sus competencias.

El acceso al contenido de los mismos por parte de una dependencia distinta, cuando existan motivos que justifiquen tal proceder, deberá ser expresamente habilitado por la Unidad de Auditoría Interna, a fin de evitar la indebida divulgación de la información vinculada con asuntos de criticidad institucional durante la sustanciación de la auditoría, con fundamento en lo normado en la disposición referida anteriormente.

En virtud de lo establecido en el artículo 32 inciso i) de la Ley N.º27.275, la publicación en el micrositio "Transparencia Activa" del último Informe de Auditoría de la auditoría en cuestión se efectuará con ajuste a las previsiones del artículo 8º de la citada ley, con estricto cumplimiento de los institutos de secreto fiscal (art. 101 Ley N.º11.683) y de estadística (art. 10 Ley N.º17.622), y la protección de los datos personales sensibles (Ley N.º25.326); en función de lo instruido sobre el tema por la Sindicatura General de la Nación.

Conclusión

En virtud de las tareas de seguimiento realizadas, se puede concluir que no se ha efectuado un avance respecto de la definición sobre centralizar los desarrollos en el área de la Subdirección General de Sistemas y Telecomunicaciones, o si se coordinarán actividades conjuntas entre las áreas para alinear y actualizar los sistemas ya desarrollados, conforme lo indica la metodología establecida, y bajo la supervisión de la mencionada Subdirección.

Esta situación incrementa el riesgo de que surjan nuevos desarrollos que no cuenten con las medidas de seguridad requeridas y que pueda verse afectada la integridad, confidencialidad y disponibilidad de la información.

Detalle de Observaciones, Causas,
Efectos y Recomendaciones

1. Debilidades en la gestión y control de cambios desarrollados por fuera de la SDG SIT

Observación

La Resolución 87/2022 de la SIGEN, establece que: "La responsabilidad por las actividades de Tecnología de la Información (TI) de la organización debe recaer en una única unidad (de TI) que asegure la homogeneidad y unicidad de criterios y objetivos en la materia.

Ante casos excepcionales en que esto no fuera factible –los que deben estar justificados formalmente por la máxima autoridad de la organización-, debe instrumentarse un Comité de TI o figura similar que se encargue de la coordinación de objetivos y lineamientos para inversiones en TICs, desarrollos, políticas y procedimientos, etc., asegurando que respondan a un criterio unificado."

Durante los relevamientos efectuados hemos verificado que existen áreas que realizan desarrollos de software por fuera de la Subdirección General de Sistemas y Telecomunicaciones, y no se ha creado un comité o figura similar que coordine objetivos y/o lineamientos. Al respecto de dicho relevamiento, surgió que la mencionada Subdirección desconoce el universo total de sistemas desarrollados por áreas ajenas a su incumbencia.

Hasta el momento, y a través de relevamientos efectuados, se pudieron identificar las siguientes Direcciones que poseen desarrollos propios:

- Dirección de Gestión del Riesgo (SDG CAD). Sistemas: "xxxxx", "xxxxx", "xxxxx".
- Dirección de Seguridad de la Información (SDG CTI). Sistemas: "xxxxx", "xxxxx", "xxxxx", "xxxxx", "xxxxx", "xxxxx".
- Dirección Regional Aduanera Noroeste (SDG OAI). Sistema: "xxxxx".

Adicionalmente, la Instrucción General AFIP N° 1/2023 menciona: "...atento a las misiones y funciones otorgadas por la Administración Federal mediante diferentes actos dispositivos, existen otras áreas dentro del organismo que tienen a su cargo tareas de desarrollo de aplicaciones informáticas."

Asimismo, indica que "los sistemas desarrollados por las áreas responsables deberán desarrollarse, testearse, homologarse, instalarse, mantenerse y ejecutarse en la "infraestructura AFIP" la cual es administrada por la SDG SIT".

A partir de lo detallado en el párrafo anterior, hemos podido verificar que la Dirección Regional Aduanera Noroeste (SDG OAI) ha desarrollado el sistema "xxxxx", siendo que no posee dentro de sus Misiones y Funciones la potestad de desarrollar sistemas, y tampoco gestiona los cambios conforme la normativa vigente.

Causa

Necesidad de las áreas de dar respuesta en tiempo y forma a sus requerimientos por ausencia de sistemas que cubran sus necesidades.

Desconocimiento de las normativas internas relacionadas con la metodología de desarrollo.

Efecto

El desarrollo, administración y mantenimiento de aplicaciones productivas de manera descentralizada y fuera del alcance de la Subdirección General con competencia, dificulta asegurar que los desarrollos se lleven a cabo utilizando las herramientas destinadas a tal fin y bajo el esquema de control y procedimientos que rigen la gestión de cambios. En este sentido, se incrementa el riesgo de duplicar esfuerzos en tareas al existir diversos responsables, distintas áreas realizando tareas similares, llevar a cabo acciones improvisadas y omisión de controles específicos que aseguren un adecuado desarrollo de software seguro.

Recomendación

Atento que la Dirección Regional Aduanera Noroeste (SDG OAI) no posee entre sus misiones y funciones el desarrollo de sistemas, se recomienda coordinar y planificar con la Subdirección General de Sistemas y Telecomunicaciones el traspaso del sistema desarrollado, a los efectos de centralizar la gestión de cambios en el área correspondiente y bajo la normativa y controles adecuados. En caso de considerarse que debiera tener competencia para el desarrollo de sistemas, debiera impulsarse justificadamente una adecuación de la estructura.

Por otro lado, se recomienda a la Subdirección General de Sistemas y Telecomunicaciones, definir un procedimiento de relevamiento, que permita identificar desarrollos realizados por distintas áreas, que deban ser incorporados a la infraestructura de SDG SIT o traspasados para una gestión centralizada. Se sugiere contemplar la creación de un Comité de TI o figura similar, tal como lo indica la RG 87/2022 (SIGEN).

Plan de acción	
Área/s Responsable/s con Competencia	Fecha prevista
Subdirección General de Sistemas y Telecomunicaciones (AFIP)	No informa
Dirección Regional Aduanera Noroeste (SDG OAI)	No informa

Opinión/Plan de Acción de la Dirección/Responsable con Competencia

Dirección Regional Aduanera Noroeste (SDG OAI)

Mediante el informe IF-2025-01790702-AFIP-DIRANO#SDGOAI del 12 de mayo de 2025, la Dirección informó: "...*Esta instancia se encuentra a la espera de instrucciones relacionadas al plan de acción a implementarse, y lleva a conocimiento de la Subdirección General de Operaciones Aduaneras del Interior el presente requerimiento.*".

Por medio de correo electrónico del 16 de mayo de 2025, la Dirección informó que no hubo avance en las acciones desde el último informe.

Subdirección General de Sistemas y Telecomunicaciones

Por medio del informe IF-2025-01920287-AFIP-SDGSIT del 19 de mayo de 2025 la Subdirección expresó: "*En virtud del cargo en trato y del estado actual de la observación efectuada por el área auditora, corresponde mencionar que la Organización atravesó y atraviesa profundas modificaciones estructurales, que han hecho que se reconfiguren las competencias en la materia que nos ocupa. En esta línea de acontecimientos y en función de lo mencionado, se tiene presente que aún falta delinear detalles para consolidar si la creación del comité, tal como se mencionara en la respuesta obrante en el expediente EX-2024-2081293 -AFIP-EQDIAUIC1DEAUTI#SDGAU1: "la creación del comité de TI se encuentra dentro del Plan de Tecnología del presente año", se encontrará bajo la órbita de la SDG SIT.*"

Opinión de Auditoría Interna

En virtud de las respuestas recibidas, se recomienda que las áreas con competencia trabajen en conjunto a los efectos de lograr un acuerdo de traspaso o la implementación de la metodología de desarrollo, acorde a las normativas del organismo.

El avance sobre las acciones que se lleven a cabo será analizado en futuras auditorías.

Criticidad del Riesgo Residual				Efectividad del Control Interno					Estado de la observación		
Ext	Alt	Mod	Baj	Mín	In	Def	Déb	Mod	Fue	Ópt	
								Mod			Sin acción correctiva informada

2. Deficiencias en la administración de los ambientes producción, homologación y desarrollo

Observación

La Instrucción General AFIP N° 1/2023 menciona: "(3) Los sistemas desarrollados por las áreas responsables deberán desarrollarse, testearse, homologarse, instalarse, mantenerse y ejecutarse en la "infraestructura AFIP" la cual es administrada por la SDG SIT, que será responsable de proveer los diferentes ambientes para cumplir el ciclo de desarrollo de software (Desarrollo, Testing, Producción). En caso de que las áreas intervinientes que se encuentran alcanzadas por la presente tengan ambientes fuera de la "infraestructura AFIP", estas deberán incluir en su planificación las tareas de migración de esos ambientes, priorizándose en función a su complejidad, impacto operativo, riesgo y criticidad de los productos informáticos en cuestión."

Adicionalmente, la Disposición N°7/2021 (AFIP) – "Políticas Específicas de Seguridad de la Información" - Capítulo VII: "Política de Seguridad en las Operaciones", en relación a la segregación de funciones, establece que, "Se deberá separar aquellas funciones que por su especificidad no deben ser ejecutadas por una misma área o persona responsable, a fin de reducir el riesgo de modificaciones no autorizadas o mal uso de la información o los servicios, por falta de independencia en la ejecución de funciones críticas." En el mismo sentido, en cuanto a la separación entre ambientes, define que "un mismo usuario no deberá ser utilizado para acceder a más de un ambiente."

En las tareas de campo de la presente auditoría se verificó que:

- En relación a los servidores que soportan los ambientes de desarrollo, homologación y producción, correspondientes a los sistemas que desarrolla y/o mantiene la Dirección de Seguridad de la Información, si bien se encuentran dentro de la sala Cofre, no son administrados por la Subdirección General de Sistemas y Telecomunicaciones, son administrados por Departamento de Arquitectura de Seguridad de Aplicaciones (DI SEIN). Asimismo, se detectaron agentes con permiso de acceso a más de un ambiente.
- En relación al servidor que soporta el sistema desarrollado por la Dirección Regional Aduanera Noroeste (SDG OAI), se encuentra fuera de dominio, y no está administrado por la Subdirección General de Sistemas y Telecomunicaciones ni se aloja dentro de la sala Cofre. En el mismo se encuentran los ambientes de desarrollo, homologación y producción, ya que, es un único usuario quién desarrolla, homologa e implementa los cambios en un mismo servidor.
- Por último, se constató que en el sistema "xxxxx", administrado por la Subdirección General de Control Aduanero (DG ADUA), existen agentes con permisos de acceso a más de un ambiente.

Por otro lado, en el ambiente de homologación correspondiente a los sistemas "xxxxx", "xxxxx" y "xxxxx" se observó la existencia de usuarios sobre los cuales la Dirección no tenía conocimiento de sus respectivos permisos de acceso.

Causa

Fallas en la implementación de una adecuada segregación de ambientes.
Recursos insuficientes en la estructura de las áreas
Ausencia de un control de revisión de accesos.

Efecto

- La gestión descentralizada de los ambientes, no permite garantizar que los entornos de desarrollo y homologación sean representativos de producción, pudiendo esto afectar a las implementaciones.
- La coexistencia de entornos (desarrollo, homologación y producción) en un mismo ambiente, podrá ocasionar pérdida de información y falta de disponibilidad de los mismos frente a caídas de servicios o incidentes.
- Potenciales cambios a sistemas desarrollados, homologados y puestos en producción por una sola persona.

Recomendación

Se sugiere adecuarse a las normativas vigentes, relativas a la segregación de ambientes y funciones.
Evaluar los recursos para poder realizar una adecuada segregación de funciones en cada ambiente y efectuar anualmente el control de accesos otorgados en cada uno de los ambientes.
Asimismo, se recomienda la elaboración de un plan de acción, en conjunto con la Subdirección General de Sistemas y Telecomunicaciones, para subsanar las debilidades mencionadas y dar cumplimiento a lo dispuesto por la Instrucción General AFIP N°1/2023 y la Disposición N°7/2021 (AFIP).

Plan de acción

Área/s Responsable/s con Competencia	Fecha prevista
Dirección Regional Aduanera Noroeste (SDG OAI)	No informa
Dirección de Seguridad de la Información (ARCA)	No informa
Dirección de Gestión del Riesgo (SDG CAD)	No informa
Subdirección General de Sistemas y Telecomunicaciones (ARCA)	No informa

Opinión/Plan de Acción de la Dirección/Responsable con Competencia**Dirección de Seguridad de la Información (ARCA)**

Por medio del Informe IF-2025-01914068-AFIP-SECUMP#SDGPCI del 19 de mayo de 2025 la Dirección expresó: *"Teniendo en cuenta la actual coyuntura de la Agencia, de público conocimiento, esta Dirección consideró inoportuno incorporar al plan de gestión una modificación sobre estructura y funciones, habida cuenta de los cambios de autoridades en la Subdirección General a cargo. Se acuerda en la necesidad de actualizar la estructura y segregar las funciones de acuerdo al punto a) de la Observación.*

Acción Correctiva propuesta: Cuando resulte posible, solicitar la modificación sobre estructura y funciones, a quien corresponda, con el fin de segregar las funciones de acuerdo al punto a) de la Observación.

Dirección Regional Aduanera Noroeste (SDG OAI)

Mediante el informe IF-2025-01790702-AFIP-DIRANO#SDGOAI del 12 de mayo de 2025, la Dirección informó: *"...Esta instancia se encuentra a la espera de instrucciones relacionadas al plan de acción a implementarse, y lleva a conocimiento de la Subdirección General de Operaciones Aduaneras del Interior el presente requerimiento.*

Por medio de correo electrónico del 16 de mayo de 2025, la Dirección informó que: *"no hubo avance en las acciones desde el último informe. Esto se adjuntó en el último requerimiento efectuado. Sin perjuicio de ello, resulta oportuno destacar que esta Instancia no cuenta con herramientas concretas para avanzar y regularizar las observaciones oportunamente efectuadas; ello porque excede el marco jurisdiccional de esta Dirección. Estimo oportuno que el tema del asunto sea planteado y tratado en Instancias jerárquicamente superior y con competencia en el asunto."*

Dirección de Gestión del Riesgo (SDGCAD)

A pedido del DE CUMA, la Dirección de Seguridad de la Información, mediante correo electrónico del 10 de junio de 2025, informó los usuarios de los ambientes de homologación y desarrollo correspondientes a los sistemas "xxxxx", "xxxxx" y "xxxxx".

Al consultar sobre los usuarios pertenecientes de la Dirección de Seguridad de la Información, mediante correo electrónico del 27 de junio de 2025, la Dirección de Seguridad de la Información informó: *"...El acceso es utilizado para hacer el re-check de esas vulnerabilidades encontradas/reportadas. Cuando estén solucionadas todas las vulnerabilidades, uds. mismos pueden eliminar los accesos. Les paso el número de ticket relacionado con el tema: "xxxxx".*

Subdirección General de Sistemas y Telecomunicaciones

Por medio del informe IF-2025-01920287-AFIP-SDGSIT del 19 de mayo de 2025 la Subdirección expresó: *"En virtud del cargo en trato y del estado actual de la observación efectuada por el área auditora, corresponde mencionar que la Organización atraviesa y atraviesa profundas modificaciones estructurales, que han hecho que se reconfiguren las competencias en la materia que nos ocupa. En esta línea de acontecimientos y en función de lo mencionado, se tiene presente que aún falta delinear detalles para consolidar si la creación del comité, tal como se mencionará en la respuesta obrante en el expediente EX-2024-2081293 -AFIP-EQDIAUIC1DEAUTI#SDGAU1: "la creación del comité de TI se encuentra dentro del Plan de Tecnología del presente año", se*

encontrará bajo la órbita de la SDG SIT. Ahora bien, más allá de lo antedicho, resulta conducente mencionar que desde la SDGSIT y la DI SEIN, oportunamente se dictaron instrucciones que encuadran las problemáticas bajo análisis a los efectos de que se permita sanear las observaciones, no teniendo estas áreas facultades de contralor, aunque sí de recepción. Cabe destacar que a la fecha desde la SDG SIT no se han recepcionado solicitudes de desarrollos efectuados fuera de su ámbito."

Opinión de Auditoría Interna

De acuerdo al análisis realizado sobre la evidencia enviada por el Departamento Centro Único de Monitoreo Aduanero se pudo verificar que se ha regularizado la situación relacionada con la segregación de funciones planteadas en el presente cargo. Con respecto a los usuarios correspondientes a la Dirección de Seguridad de Información, esta instancia entiende que estarían correctamente asignados. Se recomienda dar la baja de los mismos en el momento que no sean necesarios.

En lo que respecta a las respuestas acerca de la implementación de la normativa y /o armado de un Comité, se refuerza la necesidad de homogeneizar el desarrollo de aplicaciones, conforme la normativa vigente, para poder ordenar y obtener adecuada trazabilidad de los cambios y aplicaciones con las que cuenta el Organismo, además de asegurar una adecuada gestión y segurización de la información que se administra.

Se recomienda a la Dirección Regional Aduanera Noroeste (SDG OAI) registrar la solicitud de desarrollo/traspaso de la herramienta, en la herramienta Redmine Unificado, para iniciar la gestión con la Subdirección General de Sistemas y Telecomunicaciones.

Criticidad del Riesgo Residual				Efectividad del Control Interno					Estado de la observación		
Ext	Alt	Mod	Baj	Mín	In	Def	Déb	Mod	Fue	Ópt	
											Con Acción Correctiva Informada

3. Ausencia de documentación para la correcta trazabilidad de los cambios

Observación

La Instrucción General N° 2/2021 (SDG SIT), "Lineamientos Generales para el Desarrollo de Software de la AFIP", establece la implementación de prácticas que proporcionen: "a los involucrados en los Procesos de Desarrollo de Software, pautas y herramientas apropiadas, que permitan:

- A. Establecer los puntos de control necesarios en todo desarrollo.
- B. Establecer mecanismos que aseguren la trazabilidad.
- C. Fomentar la comunicación entre las partes interesadas.
- D. Estandarizar herramientas y actividades del Ciclo de Vida de Desarrollo de Software."

Asimismo, en el apartado N°4 menciona: "La trazabilidad consiste en poder identificar únicamente el origen, trayecto y cambios de una necesidad a lo largo de las diferentes etapas del Ciclo de Vida de Desarrollo de Software, es decir, desde que se origina hasta supuesta en producción".

De la revisión efectuada sobre el proceso de gestión de cambios a sistemas se han identificado las siguientes debilidades:

- La Dirección Regional Aduanera Noroeste (SDG OAI) no documenta los cambios que realiza sobre el sistema "xxxxx".
- La Dirección de Gestión del Riesgo (SDG CAD) utiliza la herramienta Redmine Unificado para documentar la solicitud inicial, luego se generan documentos en directorios compartidos propios del área.
- En la Dirección de Seguridad de la Información (SDG CTI), si bien utiliza Redmine unificado, se observaron desarrollos que no poseen solicitud formal de requerimiento y/o sin evidencia de pruebas en homologación (o que están incompletas) y/o sin el detalle del directorio donde se deposita el objeto a pasar a producción.

Asimismo, respecto del cumplimiento de los lineamientos generales para el desarrollo de software de AFIP, las tres áreas informaron la ausencia del documento formal de pistas de auditoría.

Causa

Debilidades en la implementación de los "Lineamientos Generales para el Desarrollo de Software de la AFIP" y su documentación soporte.

Efecto

- Se desarrollan sistemas que no satisfacen los requerimientos del usuario o que no fueron requeridos ni consensuados con ningún usuario.
- Cambios a programas que no fueron solicitados por el área usuaria del sistema.
- Conflictos entre las áreas de Sistemas y las áreas usuarias.
- Imposibilidad de efectuar controles y realizar seguimientos sobre el avance de los desarrollos e implementaciones.

Recomendación

Se sugiere a la Dirección Regional Aduanera Noroeste (SDG OAI), en tanto mantenga la administración del sistema desarrollado analizar en conjunto con la Subdirección General de Sistemas y Telecomunicaciones (AFIP) cómo avanzar en la utilización de las

herramientas para una adecuada gestión de cambios sobre el sistema "xxxxx" o nuevos proyectos. Asimismo, interiorizarse en las actividades y documentación soporte de carácter obligatorio y aplicarlo.

Se aconseja a la Dirección de Gestión del Riesgo (SDG CAD) centralizar en una única herramienta la gestión de cambios incluyendo la totalidad de las actividades relacionadas a dicha gestión sobre los sistemas propios de la Subdirección, ya sean nuevos proyectos y/o actualizaciones de los ya existentes, de manera tal de contar con un repositorio único de gestión que permita un adecuado seguimiento y trazabilidad como es la herramienta Redmine Unificado.

Se recomienda a la Dirección Seguridad de la Información (SDG CTI) adecuar las actividades de gestión de cambios a sus sistemas a los Lineamientos Generales para el Desarrollo de Software de la AFIP. Para ello, se sugiere establecer un control de cumplimiento, que sea periódico, basado en dichos lineamientos (actividades, documentación soporte, etc.).

Plan de acción		Fecha prevista
Área/s Responsable/s con Competencia		
Dirección Regional Aduanera Noroeste (SDG OAI)		No informa
Dirección de Gestión del Riesgo (SDG CAD)		No informa
Dirección de Seguridad de la Información (ARCA)		Junio 2025

Opinión/Plan de Acción de la Dirección/Responsable con Competencia

Dirección de Seguridad de la Información

Por medio del Informe IF-2025-01914068-AFIP-SECUMP#SDGPCI del 19 de mayo de 2025 la Dirección manifestó: *"Se adjunta documento con el procedimiento comprometido para junio del 2025 (versión borrador), cuyo nombre de archivo es "Borrador_CSI 13_2024_Auditoria_Desarrollo_Software.pdf".*

Mediante correo electrónico del 24 de septiembre de 2025 la Dirección confirmó que puede tomarse como documento definitivo ya que *"no recibió actualizaciones dado que refleja correctamente nuestra forma de trabajo."*

Dirección Regional Aduanera Noroeste (SDG OAI)

Mediante el informe IF-2025-01790702-AFIP-DIRANO#SDGOAI del 12 de mayo de 2025, la Dirección informó: *"...Esta instancia se encuentra a la espera de instrucciones relacionadas al plan de acción a implementarse, y lleva a conocimiento de la Subdirección General de Operaciones Aduaneras del Interior el presente requerimiento.*

Por medio de correo electrónico del 16 de mayo de 2025, la Dirección informó: *"...no hubo avance en las acciones desde el último informe. Esto se adjuntó en el último requerimiento efectuado."*

Dirección de Gestión del Riesgo (SDG CAD)

Mediante Nota del 16 de mayo de 2025, informó: *"...En atención a lo solicitado por el cuerpo auditor, se procedió a realizar la consulta en el Sistema Redmine Unificado, en la Bandeja de Requerimientos (CUMA), descargando todas aquellas peticiones procesadas en el período comprendido entre septiembre de 2024 y la fecha, y que al momento de la consulta se encontraban cerradas. Estas solicitudes pueden ser consultadas por el cuerpo auditor directamente a través de la herramienta Petición Tipo Asunto Estado Prioridad Cerrada %Realizado.*

Por otra parte, se embebe un documento en formato Word que contiene una descripción de las tareas realizadas para la obtención de la información correspondiente a las peticiones detalladas en la tabla."

Opinión de Auditoría Interna

Dirección de Seguridad de la Información

En virtud de lo manifestado por la Dirección, se observa que se ha definido un documento con detalles del procedimiento de desarrollo llevado a cabo por el área, y se han establecido pautas para la gestión y control de la trazabilidad. No obstante, y dado que se encuentra en borrador, se recomienda proporcionar mayor detalle de cómo se realizarán los controles, con qué periodicidad y quién será el responsable por su ejecución.

Dirección de Gestión del Riesgo(SDGCAD)

Del análisis realizado de la muestra enviada por la Dirección de Gestión del Riesgo (SDG CAD) mediante nota NO-2025-01900447-AFIP-DECUMA#SDGCAD del 16 de mayo del 2025, se verificó que las peticiones han sido procesadas y la documentación se encuentra resguardada en el Sistema Redmine Unificado.

Dirección Regional Aduanera Noroeste (SDG OAI)

Se recomienda a la Dirección Regional Aduana Noroeste (SDG OAI) registrar la solicitud de desarrollo/traspaso de la herramienta, en la herramienta Redmine Unificado, para iniciar la gestión con la Subdirección General de Sistemas y Telecomunicaciones.

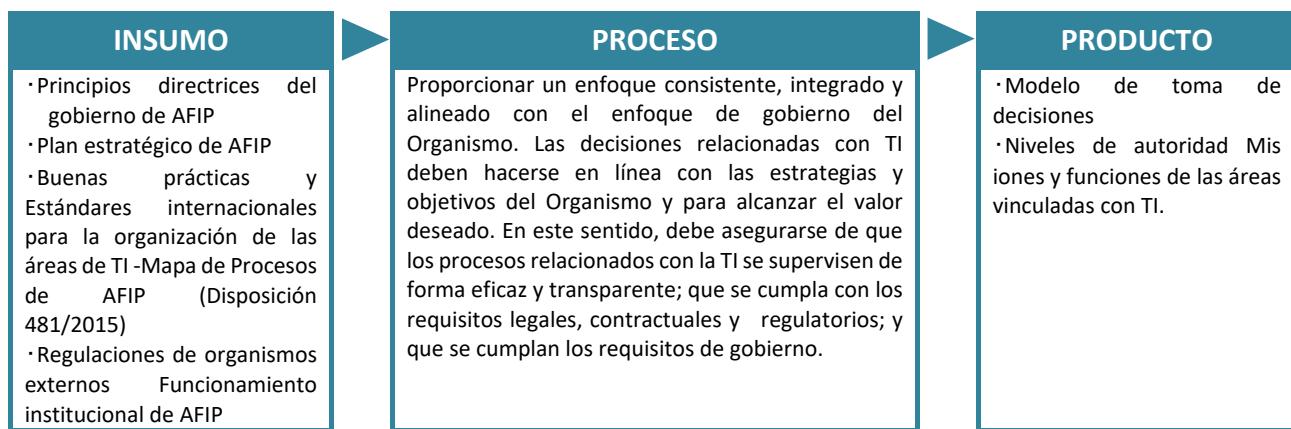
En relación a los planes de acción pendientes, los mismos serán analizados en futuras auditorías.

Criticidad del Riesgo Residual				Efectividad del Control Interno					Estado de la observación		
Ext	Alt	Mod	Baj	Mín	In	Def	Déb	Mod	Fue	Ópt	
											Con Acción Correctiva Informada

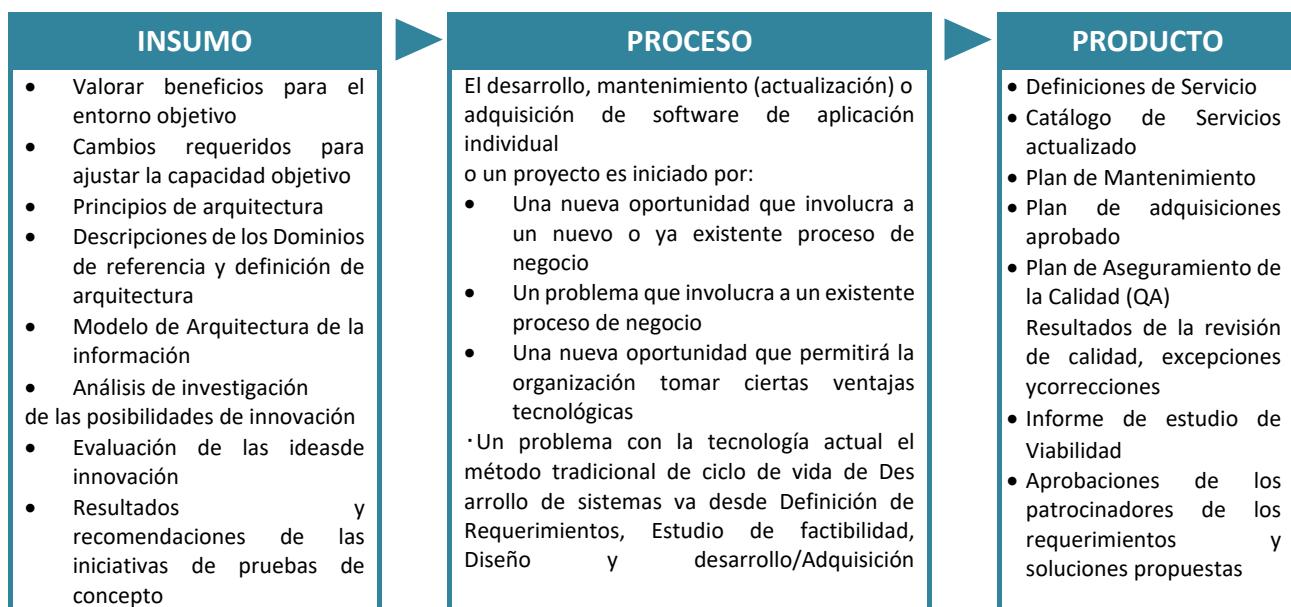
Conclusión

En virtud de las tareas de seguimiento realizadas, se puede concluir que no se ha efectuado un avance respecto de la definición sobre centralizar los desarrollos en el área de la Subdirección General de Sistemas y Telecomunicaciones, o si se coordinarán actividades conjuntas entre las áreas para alinear y actualizar los sistemas ya desarrollados, conforme lo indica la metodología establecida, y bajo la supervisión de la mencionada Subdirección.

Esta situación incrementa el riesgo de que surjan nuevos desarrollos que no cuenten con las medidas de seguridad requeridas y que pueda verse afectada la integridad, confidencialidad y disponibilidad de la información.

Unidad auditada y Normativa aplicable**ORGANIZACIÓN INFORMÁTICA**

Riesgos relevantes	1. Falta de homogeneidad de criterios, por ejemplo, en la aplicación de métodos o técnicas de desarrollo o en la planificación estratégica de la tecnología de información
Controles asociados auditados (*)	1.1. Mantener un enfoque estándar en la gestión de programas: Mantener un enfoque estándar para la gestión de programas que permita la revisión del gobierno y la gestión, la toma de decisiones y las actividades de gestión de la entrega. Estas actividades deben centrarse consistentemente en el valor y los objetivos del Organismo (es decir, los requisitos, riesgo, costes, calendario y objetivos de calidad).
Objetivos de Auditoría (**)	1.1.1. De acuerdo a la Instrucción General AFIP N° 1/2023 "Procedimiento. Ciclo de vida de los productos informáticos. Responsabilidad de las áreas que desarrollan, administran o los gestionan", que establece que todas aquellas áreas que contengan entre sus misiones y funciones, cuestiones relacionadas con el desarrollo, homologación, implementación y mantenimiento de sistemas, y hayan sido avaladas por el Administrador Federal mediante actos dispositivos, deberán dar cumplimiento a las pautas establecidas por la Instrucción General N° 2/2021 (SDG SIT) – "Lineamientos Generales para el Desarrollo de Software de la AFIP". Verificar cumplimiento de la normativa.

DESARROLLO, MANTENIMIENTO O ADQUISICIÓN DE SOFTWARE DE APLICACIÓN

- Asignaciones de presupuesto
- Comunicación del presupuesto
- Plan y presupuesto TI
- Definición de mejoras potenciales de proyectos
- Resultado de las revisiones de efectividad del SGC.
- Plan de gestión de la calidad
- Confirmar los criterios de aceptación por las partes interesadas
- Repositorio de la definición de requerimientos
- Registro de peticiones de cambios en los requerimientos
- Plan de alto nivel de Adquisidores/Desarrollo
- Informe de estudio de viabilidad
- Acciones de mitigación de riesgos.
- Aprobación del patrocinador de los requerimientos y soluciones propuestas
- Configuración de la línea de referencia
- Aprobación de cambios a la línea de referencia

parametrización, sigue por las pruebas para terminar con la Implementación.

Dados los 3 aspectos clave de la seguridad: confidencialidad, integridad y disponibilidad el objetivo es:

- Asegurar la inclusión de controles de seguridad y validación de datos en la adquisición y el desarrollo de los sistemas de información.
- Definir y documentar las normas y procedimientos que se aplicarán durante el ciclo de vida de los aplicativos y en la infraestructura de base en la cual se apoyan.
- Definir los métodos de protección de la información crítica o sensible.

Aplica a todos los sistemas informáticos, tanto a desarrollos propios o de terceros, y a todos los Sistemas Operativos y/o Software que integren cualquiera de los ambientes administrados por la organización en donde residan los desarrollos mencionados.

Los requisitos de seguridad deberían ser identificados y consensuados previamente al desarrollo y/o implantación de los sistemas de información.

Todos los requisitos de seguridad deberían identificarse en la fase de recogida de requisitos de un proyecto y ser justificados, aceptados y documentados como parte del proceso completo para un sistema de información.

- Acuerdos de niveles de Servicio y Acuerdo de nivel de Operaciones (ANSs y OLAs)
- Aprobación de las especificaciones del diseño de alto nivel
- Documentar los componentes de la solución
- Aprobación de las especificaciones del diseño de alto nivel
- Documentar los componentes de la solución
- Componentes de la solución actualizados y documentación relacionada
- Componentes de la solución integrados y configurados
- Registro de todas las peticiones de cambio aprobadas y aplicadas
- Plan de Pruebas
- Procedimientos de pruebas
- Registros de Resultados de pruebas y pistas de auditoría
- Comunicaciones del resultado de las pruebas.
- Documentar los componentes de la solución
- Documentar los componentes de la solución

Riesgos relevantes	2. Las tareas de desarrollo de sistemas se llevan a cabo de acuerdo al criterio y capacidad del responsable de turno.
Controles asociados auditados (*)	2.1. Ciclo de vida de desarrollo de software: Establecer una metodología adecuada y una estrategia segura, eficaz y eficiente. Identificar necesidades y requisitos para el desarrollo del software, elaborar un diseño del mismo o un prototipo, asegurar que el mismo se realice conforme al diseño detallado propuesto por el área definidora, en colaboración con las áreas correspondientes, ejecutar procedimientos de pruebas exhaustivos para evaluar el funcionamiento de la solución en condiciones reales, asegurando que las pruebas evalúen la idoneidad de los controles a aplicar. Finalmente, implementar adecuadamente en un entorno seguro y asegurar su mantenimiento.
Objetivos de Auditoría (**)	2.1.1. Existe una Instrucción General N° 2/2021 (SDG SIT) – “Lineamientos Generales para el Desarrollo de Software de la AFIP” que establece los procesos del ciclo de vida de desarrollo de software desde el requerimiento inicial hasta la finalización del proyecto. ¿Las áreas que desarrollan de manera independiente de la SDG SIT se encuentran alineadas a la metodología definida en dicha instrucción?

(*) Se enumeran únicamente los controles seleccionados para ser auditados durante las tareas de campo, considerando su relevancia respecto de la criticidad de los riesgos que pretenden mitigar.

(**) Referencias: (A): Alcance - (AP): Aclaraciones Previas - (S/O): Sin observación - (N.º): N.º de Observación correspondiente.

Normativa aplicable

Normativa general	Norma	Vigencia
	Resolución N.º152/2002 (SGN) - Normas de Auditoría Interna Gubernamental	17/10/2002
	Resolución N.º172/2014 (SGN) - Normas Generales de Control Interno para el Sector Público Nacional.	04/12/2014
	Instrucción General N. °1/2016 (AFIP) - Servicio de auditoría interna. Su alcance. Tratamiento a observar por las unidades de estructura dependientes de la AFIP respecto de las actuaciones originadas en la SDG AUI (Unidad de Auditoría Interna).	01/03/2016
	Instrucción General N. °1/2016 (SDG AUI) Instrucción General N. °1/2016 (AFIP). Su reglamentación por la SDG AUI, conforme Punto XI- Disp. Grales. Apartado 7.	08/03/2016
	Disposición N. °7-2019 (SDG AUI) - DI-2019-7-E-AFIP-SDGAUI - Manual de Auditoría Interna versión 6.2.	21/05/2019
	Resolución N.º300/2022 (SGN) - Aprobación de metodología "Papeles de Trabajo Digitales".	01/01/2023

Normativa específica	Norma	Vigencia
	Resolución SIGEN N°87/2022 – Normas de Control Interno para Tecnología de la Información para el Sector Público Nacional	04/02/2022
	Instrucción General AFIP N° 2/2021 - Lineamientos Generales para el Desarrollo de Software de la AFIP. Instrucción General N° 1/19 (SDG SIT). Su sustitución.	07/09/2021
	Disposición AFIP N. °192/2021 – Política de Seguridad de la Información. Sustituye a la Disposición AFIP N°29/2019	26/11/2021
	Disposición AFIP N° 7/2021 (DI SEIN) - Política de Seguridad de la Información de la AFIP Disposición N° 192/2021 (AFIP). Su complementaria	26/11/2021
	Instrucción General AFIP N° 1_2023 (SDG SIT) Procedimiento. Ciclo de vida de los productos informáticos. Responsabilidad de las áreas que des arrollan, administran o los gestionan.	04/08/2023

Datos Referenciales

Equipo de Auditoría	Cargo	(Título) Apellido y Nombre
	Director de Auditoría Interna	C.P. DEMARCHI, Javier Darío
	Dept. Auditoría de Procesos Centrales	C.P. MARRONETTI, Laura
	Jefa de División Auditoría de Tecnología de la Información	Ing. PACINI, Luz María
	Supervisor	Lic. LEMA, Alejandro
	Auditor	A.S. KALEDJIAN, Daniel

Autoridades y/o Responsables del área auditada	Cargo	Durante las Tareas de Campo	Durante el Período Auditado
	Director de Tecnología	Lic. CAMPOS, Luis Alejandro	Lic. Perez Trípodi, Joaquin
	Director de Gestión del Riesgo	Tec. ANGREHS MELENDEZ, Pablo Sebastián	PATRONE, Paula
	Director de Seguridad de la Información	Lic. PORRAS, Ariel	Lic. PORRAS, Ariel
	Director Regional Aduanera Noroeste	Tec. CORNEJOSANMIGUEL, Gustavo Adolfo	Tec. CORNEJO SANMIGUEL, Gustavo Adolfo
	Jefe de Departamento de Fiscalización y Operativa Aduanera	Esp. RODRIGUEZ, Sebastián Patricio	Sr. RODRIGUEZ, Sebastián Patricio
	Jefe de Departamento Gobierno, Riesgos y Cumplimiento	A.S PEDREIRA, Pablo	A.S PEDREIRA, Pablo
	Jefe Depto. Centro Unico de Monitoreo Aduanero	Lic. BLASCO, Christian	Lic. BLASCO, Christian

TAREAS REALIZADAS:

Descripción	Fecha desde/hasta
Envío solicitud de información	9/5/2025 – 5/6/2025
Análisis de la información y documentación aportada por las áreas	16/5/2025 al 27/6/2025
Elaboración del Informe	20/5/2025 al 24/9/2025

REFERENCIAS DEL INFORME

En el presente informe se interpreta de la siguiente manera los conceptos que seguidamente se detallan:

1. La criticidad del Riesgo Residual de las observaciones: 2. La Efectividad del Control Interno evaluado:

Ext	Extrema	In	Inexistente
Alt	Alta	Def	Deficiente
Mod	Moderada	Déb	Débil
Baj	Baja	Mod	Moderado
Mín	Mínima	Fue	Fuerte
		Ópt	Óptimo

Comunicación con la Dirección y otras áreas con competencia

A continuación, se presenta un detalle de la comunicación establecida entre la comisión auditora y los distintos responsables de las áreas involucradas:

COMUNICACIONES ENVIADAS

Área Fecha	Comunicación	Asunto	¿El área auditada respondió? (SI/NO)
Dirección Regional Aduanera Noroeste			
5/05/2025	EX-2025-01683197- -AFIP-EQDIAUIC1DEAUTI#SDGAI	Solicitud de información a la DI RANO	SI
15/05/2024	Correo electrónico	Solicitud de información a la DI RANO	SI
Dirección de Seguridad de la Información			
5/05/2025	EX-2025-01683697- -AFIP-EQDIAUIC1DEAUTI#SDGAI	Solicitud de información a la DI SEIN	SI
24/9/2025	Correo electrónico	Consulta novedades documento borrador	SI
Subdirección General de Sistemas y Telecomunicaciones			
5/05/2025	EX-2025-01684078- -AFIP-EQDIAUIC1DEAUTI#SDGAI	Solicitud de información a la SDG SIT	SI
Subdirección General de Control Aduanero			
5/05/2025	EX-2025-01682229- -AFIP-EQDIAUIC1DEAUTI#SDGAI	Solicitud de información a la SDG CAD	SI
Dept. Centro Único de Monitoreo Aduanero			
5/06/2025	Correo electrónico	Solicitud de información al CUMA	SI
10/06/2025	Correo electrónico	Solicitud de información al CUMA	SI
12/06/2025	Correo electrónico	Solicitud de información al CUMA	SI
17/06/2025	Correo electrónico	Solicitud de información al CUMA	SI
25/06/2025	Correo electrónico	Solicitud de información al CUMA	SI

COMUNICACIONES RECIBIDAS

Área Fecha	Comunicación	Asunto
Dirección Regional Aduanera Noroeste		
12/05/2025	EX-2025-01683197- -AFIP-EQDIAUIC1DEAUTI#SDGAI	Respuesta a EX-2025-01684078- -AFIP-EQDIAUIC1DEAUTI#SDGAI
16/05/2025	Correo electrónico	Respuesta a correo del 15/05/2025
Dirección de Seguridad de la Información		
19/05/2025	IF-2025-01914068-AFIP-SECUMP#SDGPCI	Respuesta a EX-2025-01684078- -AFIP-EQDIAUIC1DEAUTI#SDGAI
10/06/2025	Correo electrónico	Respuesta primera parte del correo enviado el 10/06/2025.
27/06/2025	Correo electrónico	Respuesta ampliación del correo enviado el 25/06/2025 a CUMA.
24/09/2025	Correo electrónico	Re: Consulta novedades documento borrador

Subdirección General de Sistemas y Telecomunicaciones		
19/05/2025	IF-2025-01920287-AFIP-SDGSIT	Respuesta a EX-2025-01684078- -AFIP- EQDIAUIC1DEAUTI#SDGAUI
Subdirección General de Control Aduanero		
16/05/2025	NO-2025-01900447-AFIP-DECUMA#SDGCAD	Respuesta a EX-2025-01682229- -AFIP-EQDIAUIC1DEAUTI#SDGAUI Solicitud de información a la SDG CAD
Dept. Centro Único de Monitoreo Aduanero		
10/06/2025	Correo electrónico	Respuesta correo de fecha 5/06/2025
13/06/2025	Correo electrónico	Respuesta correo de fecha 12/06/2025
17/06/2025	Correo electrónico	Respuesta correo de fecha 17/06/2025
27/06/2025	Correo electrónico	Respuesta correo de fecha 25/06/2025

**Análisis del
SCI****Anexo D**

Por las características del presente informe, no corresponde la exhibición del detalle enunciado en el anexo.

ARCA

AGENCIA DE RECAUDACIÓN Y CONTROL ADUANERO
“2025 - AÑO DE LA RECONSTRUCCIÓN DE LA NACIÓN ARGENTINA”

Hoja Adicional de Firmas
Informe gráfico firma conjunta

Número:

Referencia: ISF CSI 13/2024 - Sistemas desarrollados por áreas independientes de la SDG SIT - SIGEN

El documento fue importado por el sistema GEDO con un total de 20 pagina/s.