Ministerio de Defensa

INSTITUTO DE AYUDA FINANCIERA PARA PAGO DE RETIROS Y PENSIONES MILITARES

INFORME DE AUDITORIA	N°: 11/2021
	Fecha: 30/04/2021
	SISAC Nº: 11

CARACTER: Auditoría de Sistemas.

TEMA: Evaluación del NSIAF - Seguimiento Obs. IA N° 08/2020

PLAN UAI 2021 **Proyecto de Auditoría N° 20**

INFORME DE AUDITORIA Nº 11/2021:

Carácter: Auditoría de Sistemas.

Tema: **Evaluación del NSIAF - Seguimiento Obs. IA N° 08/2020.**

Referencia: Plan UAI 2021 - Proyecto de Auditoría Nº 20 -SISAC N° 11.

1. INTRODUCCION

1.1. Objeto y alcance de la auditoría

Esta auditoría tiene por objetivo evaluar el estado actual de las observaciones emitidas en el **IA N° 08/2020 tema: Evaluación del Nuevo Sistema Informático del IAF (NSIAF) de fecha 19/06/2020** que tuvo como temática el análisis del Sistema, sus vínculos e interfases, junto con el estado de su implementación, la actualización de los manuales de los procesos operativos involucrados y su adecuación conforme a la normativa aplicable. Asimismo, se cotejó la metodología de proyectos y la política de seguridad utilizadas, la cantidad y temática de los tickets ingresados y la definición de responsabilidades y tareas de supervisión involucradas.

El alcance de las tareas llevadas a cabo contemplará las comprobaciones fijadas en las Normas de Auditoría Interna Gubernamental aprobadas por Resolución SGN N° 152/2002, las Normas Generales de Control Interno para el Sector Público Nacional (Resolución SGN N° 172/2014) y los lineamientos establecidos en el "Manual de Control Interno Gubernamental" aprobado por la Resolución SGN N° 03/11. Se incluirá también el seguimiento de Observaciones y Recomendaciones no regularizadas, para su actualización en el SISAC.

El período auditado corresponde al comprendido entre julio 2020 a marzo 2021.

1.2. Marco normativo y de referencia

El sistema NSIAF es una plataforma informática compuesta por diversos módulos integrados. El sistema está desarrollado en un lenguaje de programación denominado .NET, el cual fue concebido bajo el paradigma de orientación a objetos, y utiliza como Base de Datos a MS-SQL Server más una herramienta denominada Reporting Services. Es de relevante importancia debido a que hace a la misión crítica del Instituto. Podemos mencionar que el alcance definido comprende módulos cómo Haberes, Créditos, Juicios, Contabilidad, Compras, Logística, Presupuesto y Finanzas, dividiéndose a su vez los mismos en submódulos. Asimismo, el NSIAF posee interfaces con otros sistemas tales como FFAA, Anses, BNA, COMPR.AR., SARHA, entre otros.

Cabe mencionar que el sistema NSIAF, reemplaza al anterior Sistema SIIAF y que a la fecha no están implementados todos sus módulos, por lo que el SIIAF bajo la anterior plataforma AS400 funciona con el módulo de liquidaciones judiciales.
Es de suma importancia aclarar que, conforme a la Matriz de Exposición del Plan UAI 2020, el proceso que nos ocupa posee un Riesgo Extremo.

En base a dichos fundamentos, se ha considerado la siguiente normativa de aplicación:

- RES. SIGEN 48/2005 (Normas de Control Interno para TI del Sector Público Nacional).

A su vez, se considerará como antecedente, el siguiente Informe de Auditoría realizada por esta UAI:

- IA N° 08/2020 tema: Evaluación del Nuevo Sistema Informático del IAF (NSIAF).

1.3. Notas emitidas y recibidas

Los requerimientos para cumplimentar el objetivo se realizaron a través de la nota NO-2021-26824873-APN-UAI#IAF de fecha 26 de marzo al área de STIyC, recibiendo su respuesta por NO-2021-36060452-APN-STIYC#IAF de fecha 26 de abril.

1.4 Tarea realizada

La presente auditoría abarca las tareas efectuadas para evaluar el estado actual de las observaciones emitidas en el **IA N° 08/2020 y su posible regularización en el sistema SISAC de Sigen.**

En esa inteligencia se desarrollan las tareas de relevamiento que se describen a continuación.

- Estudio de la materia a auditar y de su normativa aplicable.
- Definición de los tópicos a verificar conforme al Plan UAI 2021.
- Armado del requerimiento inicial de documentación.
- Análisis de las evidencias aportadas por el área auditada.
- Detección de posibles verificaciones/observaciones.
- Propuesta constructiva de recomendaciones como oportunidades de mejora.

Asimismo, cabe mencionar que, para la presente revisión, se ha tomado como período auditado al comprendido entre julio 2020 a marzo 2021.

1.5 Aclaraciones previas y antecedentes principales

El IA **N° 08/2020** tuvo por objeto evaluar al Nuevo Sistema Informático del IAF (NSIAF).
El alcance del mencionado informe comprendió desde el inicio de su desarrollo (junio 2016) dado que a la fecha de la auditoría enunciada no se había realizado ninguna evaluación previa del desarrollo del proyecto y de su marco de control.
Su evaluación comprendió los siguientes aspectos:

1) El desarrollo del proyecto a través de los contratos formalizados con el proveedor que describen: el desarrollo del proyecto, sus características y productos, las condiciones técnicas exigidas, los compromisos en materia de documentación, fuentes, metodologías de desarrollo, recursos, capacitación, pruebas y demás condiciones que hacen al cumplimiento del objetivo final de entrega del software desarrollado.
2) El esquema organizacional que condujo el proyecto, las actividades que intervinieron en la definición, desarrollo y administración de recursos, los mecanismos de monitoreo y control definidos e instrumentados.
3) El desarrollo de software, las acciones desplegadas por personal de STIyC, quien

tuvo a su cargo participar cómo Área de Desarrollo Seguimiento y Control del Proyecto NSIAF en materia del desarrollo y control de las tecnologías de Información (TI) del proyecto como su título lo indica.

4) La infraestructura tecnológica, las acciones desplegadas por el Dpto. de Tecnología Infraestructura y Seguridad en el funcionamiento de la infraestructura de TI tanto para el desarrollo como para la faz productiva del NSIAF.
5) Los resultados en la implementación del Sistema, a través de la operatoria del usuario, las principales fortalezas y debilidades en el uso del Sistema y el estado del universo de control requerido en las operaciones para su correcto funcionamiento.

Se destacan, dada la importancia del tema, las principales conclusiones que se enunciaron:

a) Incumplimientos contractuales cómo módulos no desarrollados, falta de documentación sin entregar, capacitación insuficiente, falta de gestiones para su corrección / desarrollo.
b) Desarrollos de contratos sin una planificación de proyecto, sin una evaluación que permita justificar las necesidades planteadas y los presupuestos del proveedor para realizarlo.
c) Un producto implementado con importantes vulnerabilidades relevadas, falta de seguridad en la construcción del aplicativo y en su operación, tanto en materia de programación como de datos.
d) Relación IAF - Proveedor excediendo el mero vínculo contractual (integrando el Comité de Sistemas).
e) Implementaciones que generan procesos iterativos de ajustes sin lograr una cobertura de todas las funciones y controles que el área requiere.
f) Dependencia en el mantenimiento del aplicativo, en algunos casos de misión crítica.

Se detallan finalmente las 52 observaciones surgidas de las 5 temáticas enunciadas precedentemente y que son materia de consulta con el objeto de conocer el grado de avance de su tratamiento correctivo tanto en los cambios metodológicos necesarios ante nuevas acciones como en la solución de fuertes debilidades existentes en el momento del informe.

1.6 Limitaciones al alcance

A partir del Decreto 297/2020 Aislamiento Social Preventivo y Obligatorio del 20/3/2020 se realizaron tareas en la modalidad teletrabajo con entrevistas virtuales y consultas que permitieron realizar el presente análisis.

2. RESULTADOS

2.1. Verificaciones:

A continuación, se expondrán las respuestas enviadas por STIYC y la Opinión UAI a fin de considerar la regularización de las observaciones realizadas que podemos resumir en el siguiente cuadro:

N° DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
Obs. N° 1 - Contratos celebrados	a) Falta de evaluaciones previas.	La contratación de los servicios externos de desarrollo debe estar debidamente justificada, documentada y respaldada por un análisis de los objetivos y recursos a emplear como la evaluación de actividades y riesgos involucrados, debiendo ser autorizadas por el responsable de la unidad de TI.	Las contrataciones externas serán autorizadas por el responsable de la unidad de TI, luego de una evaluación detallada del proyecto y riesgos involucrados.	Regularizada
	b) Incumplimiento de los contratos.	Evaluar el estado de situación del proyecto a fin de determinar los pasos a seguir. Los incumplimientos detectados pueden derivar en inconvenientes de carácter operativo que pueden requerir ser solucionadas.	Ante incumplimientos detectados se optó por la no continuidad de contratación de los servicios del proveedor externo de NSIAF.	Regularizada
	c) Falta de registro de tareas por Mantenimiento y Mejoras.	Se recomienda, en el marco del proyecto explicitar las actividades a contratar y tener registro de seguimiento definiendo objetivos contractuales explícitos comprobables y medibles con un mecanismo de aceptación que estudie la viabilidad funcional y las condiciones técnico-económicas de la propuesta como las necesidades de recursos a emplear, documentación y transferencia de conocimiento	La implementación de proyectos de TI que incluyen las tareas de mantenimiento y mejoras consideran los principios de documentación de las tareas, análisis de recursos técnico-económicos, transferencia de conocimiento, condiciones de seguridad, viabilidad funcional, necesarios para un cumplimiento eficiente de los objetivos planteados.	Regularizada
	d) Incumplimiento de prácticas de control.	Cumplimentar actividades de control en el desarrollo del proyecto por parte de la autoridad de TI y con la participación de la UAI a fin de fortalecer las alertas ante debilidades en el control de actividades de TI de los procesos contractuales.	La autoridad de TI documenta la planificación y desarrollo de las acciones con el objeto de fortalecer el seguimiento y control de lo realizado.	Regularizada
Obs. N° 2 - Organización del Proyecto	a) Falta de intervención de la Autoridad de TI.	Cumplimentar la Res SGN 48/05 como Autoridad de TI en la función del Subgerente de Tecnologías de Información y Comunicaciones a cargo de la gestión de las actividades y proyectos de TI en el Organismo.	La Subgerencia de Tecnologías de la Información y las Comunicaciones ejerce como única autoridad de TI del Organismo las misiones y funciones definidas en la normativa vigente.	Regularizada
	b) Falta de ejecución de las funciones propias del Departamento de Desarrollo y Mantenimiento de Sistemas, asignadaso en la Res IAF 10990/2017.	Cumplimentar las funciones definidas para el sector Departamento de Desarrollo y mantenimiento de Sistemas según Normativa Res 10990/2017, que incluyen al Proyecto NSIAF como responsabilidad del Área y como actividad a gestionar.	Se ha cumplimentado la res IAF 10990/2017 en fortalecer el ejercicio de las funciones asignadas al Departamento de Desarrollo y Mantenimiento de Sistemas incrementando, entrenando y reorganizando su personal, en un proceso que, si bien no ha terminado, garantiza el mínimo estándar de operatividad y seguridad a fin de suplir las fuertes debilidades encontradas	Regularizada
	c) Debilidades del Sistema en los procesos administrativos.	Dada la definición de las características funcionales del NSIAF materializadas en el desarrollo e implementación del producto, se recomienda revisar con los usuarios la posible reformulación implícita que hubo en los circuitos administrativos, habida cuenta que el nuevo aplicativo requiere ajustes y establece una interacción usuario/sistema distinta que el anterior, redefiniendo procesos como validaciones, aprobaciones, controles y roles que no están debidamente documentados y/o explicitados en los procesos de negocio integrados al sistema.	Se analizaron distintos circuitos administrativos habida cuenta de la cantidad de ajustes requeridos por los usuarios. Se analizaron y redefinieron en su totalidad los circuitos de préstamos personales y créditos hipotecarios. Se continúa con el análisis de los demás circuitos	No regularizada
	d) Creación de un Área con funciones propias de una ya existente.	Derogar la Disp. 526/2016 que crea el Área de Desarrollo Seguimiento y Control del NSIAF, dadas las funciones del Departamento de Desarrollo y mantenimiento de Sistemas que las cubre.	Se está tramitando ante la autoridad superior la regularización normativa originada en la existencia de un área creada para cumplir funciones ya existentes.	No regularizada

N° DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
Obs. N° 2 - Organización del Proyecto	e) Dependencia del Proveedor en misiones críticas.	Se debe realizar con la mayor prioridad un plan para tomar el control de la administración del aplicativo en función del riesgo que implica la dependencia externa de los distintos niveles de soporte del sistema, en particular a los que responden a la misión crítica del Organismo. Se estima que dicho tratamiento requiere tener el conocimiento necesario para mantener la explotación del software de manera independiente del proveedor.	Se definieron e implementaron medidas para tomar el control de la administración del aplicativo y eliminar la dependencia del proveedor.Se optó por la no continuidad de contratación de los servicios del proveedor externo de NSIAF.	Regularizada
	f) Atribuciones incorrectas del Proveedor.	Se requiere que la autoridad de TI concentre el control de la interacción con el proveedor centralizando su interlocución, interactúe con todos los usuarios y con el exterior en esta materia y gestione las actividades del proyecto en las condiciones fijadas por el punto 6 y 7 Res SGN 48/05.	La autoridad de TI gestiona las actividades del proyecto.	Regularizada
Obs. N° 3 - Desarrollo del software	a) Falta de homologación de perfiles.	Implementar una metodología de gestión de proyectos para el NSIAF, que permita cumplimentar los plazos de entrega y responder a las necesidades del usuario. Documentar el desarrollo del software poniendo hincapié en los perfiles asignados a cada usuario cumpliendo con la normativa en política de seguridad de la información.	Se implementó metodología para gestionar proyectos para lograr cumplimentar los plazos de entrega y responder las necesidades del usuario, con prioridad en el cumplimiento de las políticas de Seguridad de la Información	Regularizada
	b) Falta de implementación de procedimientos promulgados.	Implementar el Manual de Procedimientos sobre accesos a Servicios y aplicaciones en Tecnologías de Información aprobado por RESFC-2019-90-DIR#IAF, en el sistema NSIAF, garantizando la confidencialidad e integridad de la información que se procesa en el Instituto.	Se han iniciado las tareas tendientes a implementar el Manual de Procedimientos sobre accesos a servicios y aplicaciones en Tecnologías de Información aprobado por RESFC-2019-90-DIR#IAF, en el sistema NSIAF. El estado actual de roles y perfiles que dan privilegios de acceso a los usuarios no responde a estándares técnicos, lo que dificulta su correcta implementación. El circuito operativo de información y autorización dentro de la Subgerencia ha sido modificado en el marco de la RESOLUCION antes mencionada.	No regularizada
	c) Falta de cumplimiento de la separación de ambientes.	Implementar el procedimiento “Separación de ambientes” del Instituto en el entorno NSIAF, definiendo las actividades que se pueden desarrollar en cada uno de los ambientes, los responsables de su ejecución, para asegurar la correcta segregación de funciones y los controles que se deben aplicar para autorizar el pasaje de componentes de software al ambiente de producción.	Se ha implementado la separación de ambientes para asegurar la correcta segmentación de funciones.	Regularizada
	d) Falta de confidencialidad en la BBDD.	Se recomienda implementar el uso de enmascaramiento de datos a fin de asegurar la confidencialidad de la información que se procesa y se transmite por la red.	Se están analizando distintas alternativas para fortalecer la confidencialidad de la BBDD. No obstante, la falta de aplicación de las mejores prácticas y estándares de seguridad en el desarrollo de NSIAF, elevan la complejidad para avanzar en este punto.	No regularizada
	e) Falta de documentación funcional de procesos de negocios.	Documentar los procesos de negocios que fueron relevados e implementados en el NSIAF oportunamente.	Se ha comenzado a generar la documentación funcional de los procesos de negocios, como ser préstamos personales y créditos hipotecarios.	No regularizada
	f) Falta de documentación técnica detallada.	Documentar manuales técnicos y manuales de usuarios sobre los flujos de proceso faltantes y actualizar los ya elaborados. Asimismo, desarrollar manuales y/o instructivos sobre especificaciones generales del sistema, de sus componentes y de planes integrales de prueba y mantenimiento del NSIAF.	Se ha comenzado a generar la documentación técnica detallada. Es importante destacar que el proveedor externo responsable del sistema no ha entregado la documentación correspondiente	No regularizada
	g) Falta de estándares de diseño Cliente-Servidor.	Definir en forma clara y precisa las capas que conforman el sistema, incluyendo la capa de presentación que es la ve el usuario, la capa del negocio donde residen los programas que se ejecutan y la capa de datos, donde se encuentran los datos y se accede a ellos, implementando tales principios para corregir irregularidades.	Debido a la falta de aplicación de las mejores prácticas y estándares de diseño en el desarrollo de NSIAF, la adecuación de los desarrollos existentes es viable sólo con la reingeniería completa del sistema que requeriría una recodificación total.	No regularizada

Nº DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
Obs. Nº 3 - Desarrollo del software	h) Diseño inseguro de la BBDD.	Implementar un sistema de gestión de base de datos (MS SQL SERVER), definiendo restricciones que aseguren la integridad de datos y el uso de vistas e índices que ayuden a acelerar las consultas en las tablas.	Si bien se han implementado alternativas que fortalecen la integridad de los datos, debido a la falta de aplicación de mejores prácticas y estándares de diseño en el desarrollo de NSIAF, lograr el diseño adecuado sólo es factible a través de una reingeniería total del sistema	No regularizada
	i) Migración con faltante de datos.	Completar la migración total de las bases de datos desde el sistema anterior (AS400) al sistema NSIAF, para que el usuario no tenga necesidad de utilizar el sistema anterior (AS400) para realizar consultas fundamentales sobre sus procesos diarios, más aún considerando que el sistema anterior no se encuentra actualizado y ya no se realiza mantenimiento.	Se ha logrado migrar algunos datos faltantes. No obstante, al no haber sido relevados y analizados al momento de desarrollar NSIAF los procesos de negocios, las necesidades de los usuarios y la información existente de sistemas anteriores, es marcadamente difícil migrar los datos faltantes.	No regularizada
	j) Estructura organizacional insegura en la administración de datos.	Centralizar la responsabilidad sobre la BBDD en un responsable de manera de ir tratando las dificultades observadas como son los permisos de acceso registros o logs, y buenas prácticas de uso.	Se han restringido accesos sobre las BBDD y se realizará una capacitación específica para fortalecer el rol de DBA (Administrador de Base de Datos) que centralizará la responsabilidad sobre la BBDD.	No regularizada
	k) Falta de estándares de programación.	Se sugiere revisar dichas características como también realizar test de penetración que permitan determinar la seguridad del código, evaluando los principales riesgos de seguridad existentes en la aplicación web, conforme a estándares (Ej. Standard OWASP para evaluar el grado de producción de código seguro).	Se ha comenzado con el test de intrusión, a través de un acuerdo con UNDEF y la Subsecretaría de Ciberdefensa, relevando de manera exhaustiva el código fuente según estándares	No regularizada
Obs. Nº 4 - Infraestructura tecnológica	a) Accesos no permitidos en la operación y uso del NSIAF.	Asignar responsabilidades de administración de la BBDD para cumplimientos de los estándares definidos por el sector de Desarrollo. Restringir el uso en producción de uso de la BBDD a las tareas de mantenimiento habituales que garanticen su disponibilidad, integridad y confidencialidad.	Se ha restringido el uso en producción de la BBDD para fortalecer la seguridad y se han designado responsables transitorios en la administración de la BBDD	No regularizada
	b) Falta de protección en Servidores NSIAF expuestos.	Instalar el nuevo firewall que garantice la cobertura de aplicaciones web.	Se ha instalado el nuevo firewall y se implementaron medidas para fortalecer la seguridad. Está en proceso de compra un WAF (Web Application Firewall) para proteger adecuadamente el sistema, ya que el módulo incluido en NSIAF para cumplir esa función tiene funcionalidades mínimas	No regularizada
	c) Existencia de conexiones no permitidas.	Disponer de un inventario de equipamiento propio en la infraestructura de red y garantizar una configuración segura de sus componentes.	Se dispone de un inventario de equipamiento que garantiza una configuración segura de los componentes y se han dado de baja todas las conexiones no permitidas.	Regularizada
	d) Falta de actualización de los Servidores productivos.	Mantener el software de base de manera actualizada evitando vulnerabilidades producto de patches no realizados.	Las actualizaciones de los servidores productivos se realizan actualmente en forma periódica.	Regularizada
	e) Falta de documentación de procesos de producción.	Requerir al área de Desarrollo las necesidades de información para garantizar la operatividad ante inconvenientes.	Se está avanzando con la documentación de los procesos de producción, iniciados en 2020.	No regularizada
	f) Existencia de Hardware en uso no permitido.	Disponer de un inventario de equipamiento propio en la infraestructura de red y garantizar una configuración segura de sus componentes.	Se ha eliminado el hardware no permitido y se dispone de un inventario del equipamiento	Regularizada
	g) Falta de seguridad en el sistema en producción.	Implementar buenas prácticas en el sector Seguridad. Instrumentar las medidas necesarias para realizar un Test de Intrusión a la red del Organismo a fin de evaluar las vulnerabilidades existentes. El Organismo cuenta con una nueva plataforma tecnológica sobre servidores Windows y un nuevo Firewall que debe ser evaluado en su conjunto.	Se ha comenzado con el test de intrusión a través de un acuerdo con UNDEF y la Subsecretaría de Ciberdefensa y se han implementado medidas complementarias para fortalecer la seguridad	No regularizada
	h) Configuración inapropiada y sin control de servidores.	Configurar los servidores en forma correcta y mantener el software de base de manera actualizada evitando vulnerabilidades producto de patches no realizados.	Se han mejorado la configuración de los servidores productivos y se están llevando a cabo las actualizaciones necesarias.	No regularizada

Nº DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
Obs. N° 4 - Infraestructura tecnológica	i) Habilitación de pedidos de conexión remota sin fundamentación.	Definir limitaciones y controles en los puertos de red, protocolos y servicios, administrando los dispositivos, escaneando puertos según servicios y documentando e informando las anomalías detectadas.	Se han limitado los accesos y se realizaron controles de puertos y servicios de red. Se ha comenzado el test de intrusión permitiendo detectar anomalías.	Regularizada
	j) Incumplimiento de los Procedimientos de separación de ambientes.	Transferencia de información y reconocimiento del estado de producción del aplicativo bajo jurisdicción del Departamento de Tecnología Infraestructura y Seguridad. Implementar la separación de ambientes en el sistema.	Se ha implementado separación de ambientes y se ha transferido información del estado de producción del aplicativo bajo jurisdicción del Departamento de Tecnología, Infraestructura y Seguridad.	Regularizada
	k) Falta de un CPA.	Rehabilitar el Centro de Cómputos alternativo de manera de contar con servicio de contingencia cumpliendo con la ACDIR. IAF 1/2019 "Políticas específicas de Seguridad de la Información " que establece :"De la problemática de la gestión de la continuidad es prioritario definir los procesos/servicios críticos que requieren un plan de continuidad de las actividades y que en cuyo detalle se expliciten los recursos utilizados para permitir/garantizar la disponibilidad del proceso/servicio". Para tal fin, se define la RESFC-2018-143-APN-DIR-IAF " que aprueba el Manual de Procedimientos de Gestión para la Continuidad Operativa Informática del IAF (PGCOI)",	Se ha habilitado el CPA en ARSAT.	Regularizada
Obs. N° 5 - Implementación NSIAF 5.a - Tickets electrónicos	a) Falta de procedimiento para la generación de tickets electrónicos	Desarrollar e implementar un procedimiento que contemple un Sistema de requerimientos general que incluya a todas las aplicaciones vigentes en el instituto y que se acceda por fuera del Sistema NSIAF, no permitiendo otro tipo de solicitud que no sea por el mencionado sistema de requerimientos, y que se normalice su registro de manera de mantener la consistencia e integridad en los datos cargados. Cabe aclarar que el Manual de Procedimientos Sobre Accesos a Servicios y Aplicaciones en Tecnologías de la Información Res FC 90/2019 contempla los permisos de acceso que deberá articularse en su implementación con el sistema general de requerimientos de modificación a sistemas mencionado anteriormente.	Se está actualizando el procedimiento y se ha definido la implementación de un nuevo sistema para la gestión de tickets electrónicos. El proceso de compra se encuentra aceptado.	No regularizada
5.b - Listado de usuarios del Sistema	a) Desactualización del listado de usuarios del Sistema.	Actualizar el listado de usuarios del Sistema, y realizar un debido control de accesos al mismo para identificar los usuarios de cada módulo y verificar si se trata de accesos permitidos.	Se han revisado los usuarios del sistema y se han controlado los accesos. Se está coordinando con las áreas usuarios para revisar más detalladamente usuarios y accesos.	No regularizada
	b) Incorrecta asignación de perfil	Revocar a la persona proveedora del Sistema, los permisos, roles y accesos que no le corresponden, para asegurar la integridad y confidencialidad de la información que procesa el Instituto.	Se han revocado los permisos al proveedor externo del sistema.	Regularizada
	c) Falta de descripción de perfiles y roles dentro del menú del Sistema	Agregar en la pantalla de cada módulo del NSIAF los agentes usuarios del mismo, con su perfil y descripción, a fin de que su superior pueda controlar los permisos adjudicados a su personal.	Se ha analizado y se implementará una solución.	No regularizada
	d) Acceso indebido al ambiente de desarrollo	Verificar que el personal del IAF, usuarios del Sistema, no tengan acceso al ambiente de desarrollo.	Se han revocado los accesos indebidos.	Regularizada

N° DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
5.c.1 Módulo Créditos	a) Falta de Migración de la base de datos	Completar la migración de las bases de datos, de manera de tener una base integra y actualizada que permita la realización de la operatoria sin necesidad de efectuar tareas manuales por parte del usuario que conlleven a una carga horaria extra y la posibilidad de cometer errores.	Se ha logrado migrar algunos datos faltantes. No obstante, al no haber sido relevados y analizados al momento de desarrollar NSIAF los procesos de negocios, las necesidades de los usuarios y la información existente de sistemas anteriores, es marcadamente difícil migrar los datos faltantes.	No regularizada
	b) Falta de datos para los Contratos en Gestión Judicial	Implementar la funcionalidad solicitada por el área, a fin de poder realizar los cálculos necesarios con los datos del sistema NSIAF, sin necesidad de recurrir al anterior sistema AS400 que se encuentra desactualizado y sin mantenimiento.	Si bien cuando se detectan faltantes por parte del usuario se tratan de regularizar, al no haber sido relevados y analizados al momento de desarrollar NSIAF los procesos de negocios, las necesidades de los usuarios y la información existente de sistemas anteriores, es muy complejo migrar los datos del sistema anterior.	No regularizada
	c) Falta del porcentaje inicial comprometido (PIC):	Migrar los datos necesarios del PIC a fin de poder realizar los cálculos correctamente a partir del sistema NSIAF y no tener que recurrir a documentación física del beneficiario a fin de facilitar la tarea diaria.	Se procedió a solucionar la observación	Regularizada
	d) Estado incorrecto de mora en Contratos cancelados por fallecimiento	Resolver a la brevedad posible, el inconveniente presentado en los contratos cancelados por fallecimiento del beneficiario, migrando correctamente la información y los datos del mismo, a fin de poder establecer el correcto estado de los créditos.	Se procederá a su solución en función de otras prioridades del módulo del sistema.	No regularizada
	e) Cálculo erróneo en la generación de la última cuota	Implementar la funcionalidad necesaria que permita que los préstamos otorgados presenten el estado correcto que le corresponde calculando el saldo de la última cuota en forma precisa.	Se procedió a la corrección del problema.	Regularizada
	f) Falta de ingreso del Contrato NPP 7396	Se recomienda quitar el acceso al ambiente de desarrollo a los empleados de las áreas usuarios del NSIAF.	Se procedió a la corrección del problema.	Regularizada
	g) Detección de números de contrato duplicados	Controlar que el sistema no emita duplicados de los contratos otorgados.	Se implementó la solución.	Regularizada
	h) Falta de reportes generados por el Área de Control de carteras de créditos	Implementar el mecanismo necesario para que el Área de contabilidad pueda acceder a la información requerida en el sistema NSIAF, y no dependa del envío de información de otra Área.	Se procedió a implementar la solución.	Regularizada
	i) Asignación errónea del estado de préstamos precancelados	Asignar en forma automática a los créditos mencionados su correspondiente y correcto estado en el sistema NSIAF.	Se implementó la solución.	Regularizada
5.c.2 Módulo Contabilidad y Presupuesto	a) Falta de generación de Asientos Automáticos de Haberes Militares	Implementar a la brevedad posible, la funcionalidad de generar asientos contables automáticos a fin de evitar cálculos erróneos en la tarea manual que deben realizar y controlar los usuarios del área, aumentando la carga operativa de la misma. Cumplir con la normativa del Ministerio de Hacienda.	Se está analizando la implementación de la solución. Es importante indicar que la solución a desarrollar tiene un alto grado de complejidad debido a que el proceso no fue considerado en el momento del desarrollo del sistema	No regularizada
	b) Falta de Conciliación bancaria automática	Implementar la realización de la conciliación bancaria automática en el sistema NSIAF reflejando los movimientos diarios solicitados por el Área.	Se está analizando la implementación de la solución. Es importante indicar que la solución a desarrollar tiene un alto grado de complejidad debido a que el proceso no fue considerado en el momento del desarrollo del sistema	No regularizada

Nº DE OBS.	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES	Estado actual según STIYC	Opinión UAI
5.c.3 Módulo de Retiros y Pensiones	a) Falta de Migración de la base de datos	Implementar la migración de la totalidad de las tablas solicitadas por el área, a fin de poder realizar los cálculos necesarios con los datos del sistema NSIAF, sin necesidad de recurrir al anterior sistema AS400 que se encuentra desactualizado y sin mantenimiento.	Si bien cuando se detectan faltantes por parte del usuario se tratan de regularizar, al no haber sido relevados y analizados al momento de desarrollar NSIAF los procesos de negocios, las necesidades de los usuarios y la información existente de sistemas anteriores, es muy complejo migrar los datos del sistema anterior.	No regularizada
	b) Falta de Controles en el proceso de liquidación de haberes de retiros y pensiones	Implementar a la brevedad posible, los controles requeridos por el área de manera que el NSIAF los realice en forma automática.	Se han agregado controles al proceso, no obstante, se analizan e implementan continuamente nuevos.	No regularizada
	c) Incorrecta Metodología de implementación del módulo con los usuarios	Ante esta situación, esta UAI sugiere implementar un mecanismo de mayor asistencia y acompañamiento al usuario del sistema en respuesta a sus requerimientos.	Se implementó una mayor asistencia y acompañamiento al usuario en respuesta a sus requerimientos	Regularizada
	d) Suspensión del aplicativo de Control biométrico de supervivencia	Se recomienda que los proyectos de base tecnológica utilicen estándares definidos por la Administración Pública (punto 8.1 Res Sigen 48/05). Explorar dichas posibilidades a partir del SID Sistema de Identidad Digital (Validación remota de identidad en tiempo real con el RENAPER mediante factores de autenticación biométrica (reconocimiento facial) y fotografía del DNI). Esta recomendación está sujeta a la decisión de las autoridades de restablecer el proyecto en función de los objetivos planteados. Se recomienda derogar la RESFC 94/2019 dado su imposible cumplimiento.	Se tramitará la suspensión de la normativa que lo habilita dada la falta de congruencia técnica, económica y de seguridad que implicaba su implementación. Se suplantó por la validación a través del SID (Sistema de Identificación Digital) de RENAPER. Se ha elaborado un convenio con el RENAPER pendiente de la firma para la puesta en funcionamiento.	No regularizada

2.3 Tratamiento ulterior del Informe con el área auditada

Mediante Nota NO-2021-36945910-APN-UAI#IAF de fecha 28/04/2020, esta UAI remitió el IA Preliminar al área auditada. A través de la NO-2021-37657721-APN-STIYC#IAF de fecha 29/04/2021, la misma emitió sus opiniones, acción correctiva comprometida por el área y fecha estimada de regularización que se encuentran plasmadas en el **ANEXO I** del presente informe. Cabe aclarar que el Área Auditada expresó su total conformidad a todas las Observaciones regularizadas por Opinión UAI realizadas en el actual Informe.

3. CONCLUSION

3.1. Conclusión de carácter general

Se enuncia a continuación las principales características del actual estado de situación del NSIAF:

- Se advierte un importante avance sobre las observaciones realizadas, solucionándose el 48% del total formulado el pasado año.
- Los problemas derivados de la organización del proyecto han sido subsanados en tanto la Subgerencia de Tecnologías de Información y Comunicación ha tomado el control de las actividades de TI del Organismo como única autoridad de TI, en concordancia con la normativa vigente.
- Se ha logrado la independencia operativa en reemplazo del proveedor consolidando el manejo y control de los módulos de misión crítica.

- Los problemas derivados de la metodología en la gestión de los proyectos consideran, a la fecha, un marco adecuado de administración y tratamiento.
- En materia de seguridad de la información y de la Infraestructura Tecnológica se observa nuevo equipamiento y medidas de control en la disponibilidad operativa ante contingencias, integridad de datos y confidencialidad de la información, alcanzando a solucionar de manera integral las observaciones pendientes en el presente año.
- Se ha avanzado en tareas de fortalecimiento de TI con la Subsecretaría de Ciberdefensa del Ministerio de Defensa y el RENAPER en la definición de pautas y apoyo instrumental al organismo.
- La plataforma de software, de significativa importancia y de mayor debilidad técnica por las fallas de control en el proyecto tiene pendiente el 81% de las observaciones formuladas, estimándose regularizar mitad de en el presente año. El resto de las observaciones en esta temática, de índole estructural, requieren medidas de mayor complejidad y recursos, debiendo ser integradas a una planificación que alcance toda la actividad de TI, habida cuenta de la interacción con nuevos servicios tecnológicos y de los objetivos y prioridades que sean fijados.
- Sobre el sistema NSIAF, podemos resumir que hay módulos con deficiencias al haber sido implementados sin el control y los procedimientos necesarios que se van perfeccionando en el tiempo y módulos que no han sido implementados o con grandes carencias funcionales. Estos últimos requieren decidir su reingeniería o su completitud y como se mencionó en el punto anterior deben sumarse al planeamiento integral de TI para su definitiva solución.
- En materia de organización y en función de las buenas prácticas ante las debilidades existentes la Subgerencia instrumentará:
    - el control funcional directo con el área de Seguridad Informática.
    - asignar responsabilidades de administración de BBDD.
    - la normalización del Departamento de Desarrollo y Mantenimiento de Sistemas cómo área interviniente en el desarrollo y mantenimiento de aplicaciones del Instituto.

En suma, de la revisión efectuada, esta UAI arribó a las observaciones que se exponen en el siguiente cuadro:

N° OBS. IA Nº 08-20	Nº OBS. IA Nº 11-21	IMPACTO	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES
2 - Organización del Proyecto	1	**Medio**	c) Debilidades del Sistema en los procesos administrativos.	Dada la definición de las características funcionales del NSIAF materializadas en el desarrollo e implementación del producto, se recomienda revisar con los usuarios la posible reformulación implícita que hubo en los circuitos administrativos, habida cuenta que el nuevo aplicativo requiere ajustes y establece una interacción usuario/sistema distinta que el anterior, redefiniendo procesos como validaciones, aprobaciones, controles y roles que no están debidamente documentados y/o explicitados en los procesos de negocio integrados al sistema.
	2	**Medio**	d) Creación de un Área con funciones propias de una ya existente.	Derogar la Disp. 526/2016 que crea el Área de Desarrollo Seguimiento y Control del NSIAF, dadas las funciones del Departamento de Desarrollo y mantenimiento de Sistemas que las cubre.
3 - Desarrollo del software	3	**Medio**	b) Falta de implementación de procedimientos promulgados.	Implementar el Manual de Procedimientos sobre accesos a Servicios y aplicaciones en Tecnologías de Información aprobado por RESFC-2019-90-DIR#IAF, en el sistema NSIAF, garantizando la confidencialidad e integridad de la información que se procesa en el Instituto.
	4	**Alto**	d) Falta de confidencialidad en la BBDD.	Se recomienda implementar el uso de enmascaramiento de datos a fin de asegurar la confidencialidad de la información que se procesa y se transmite por la red.
	5	**Alto**	e) Falta de documentación funcional de procesos de negocios.	Documentar los procesos de negocios que fueron relevados e implementados en el NSIAF oportunamente.
	6	**Alto**	f) Falta de documentación técnica detallada.	Documentar manuales técnicos y manuales de usuarios sobre los flujos de proceso faltantes y actualizar los ya elaborados. Asimismo, desarrollar manuales y/o instructivos sobre especificaciones generales del sistema, de sus componentes y de planes integrales de prueba y mantenimiento del NSIAF.
	7	**Medio**	g) Falta de estándares de diseño Cliente-Ser	Definir en forma clara y precisa las capas que conforman el sistema, incluyendo la capa de presentación que es la ve el usuario, la capa del negocio donde residen los programas que se ejecutan y la capa de datos, donde se encuentran los datos y se accede a ellos, implementando tales principios para corregir irregularidades.
	8	**Medio**	h) Diseño inseguro de la BBDD.	Implementar un sistema de gestión de base de datos (MS SQL SERVER), definiendo restricciones que aseguren la integridad de datos y el uso de vistas e índices que ayuden a acelerar las consultas en las tablas.
	9	**Medio**	i) Migración con faltante de datos.	Completar la migración total de las bases de datos desde el sistema anterior (AS400) al sistema NSIAF, para que el usuario no tenga necesidad de utilizar el sistema anterior (AS400) para realizar consultas fundamentales sobre sus procesos diarios, más aún considerando que el sistema anterior no se encuentra actualizado y ya no se realiza mantenimiento.
	10	**Medio**	j) Estructura organizacional insegura en la administración de datos.	Centralizar la responsabilidad sobre la BBDD en un responsable de manera de ir tratando las dificultades observadas como son los permisos de acceso registros o logs, y buenas prácticas de uso.
	11	**Medio**	k) Falta de estándares de programación.	Se sugiere revisar dichas características como también realizar test de penetración que permitan determinar la seguridad del código, evaluando los principales riesgos de seguridad existentes en la aplicación web, conforme a estándares (Ej. Standard OWASP para evaluar el grado de producción de código seguro).
4 - Infraestructura tecnológica	12	**Medio**	a) Accesos no permitidos en la operación y uso del NSIAF.	Asignar responsabilidades de administración de la BBDD para cumplimientos de los estándares definidos por el sector de Desarrollo. Restringir el uso en producción de uso de la BBDD a las tareas de mantenimiento habituales que garanticen su disponibilidad, integridad y confidencialidad.
	13	**Medio**	b) Falta de protección en Servidores NSIAF expuestos.	Instalar el nuevo firewall que garantice la cobertura de aplicaciones web.
	14	**Medio**	e) Falta de documentación de procesos de producción.	Requerir al área de Desarrollo las necesidades de información para garantizar la operatividad ante inconvenientes.
	15	**Medio**	g) Falta de seguridad en el sistema en producción.	Implementar buenas prácticas en el sector Seguridad. Instrumentar las medidas necesarias para realizar un Test de Intrusión a la red del Organismo a fin de evaluar las vulnerabilidades existentes. El Organismo cuenta con una nueva plataforma tecnológica sobre servidores Windows y un nuevo Firewall que debe ser evaluado en su conjunto.
	16	**Medio**	h) Configuración inapropiada y sin control de servidores.	Configurar los servidores en forma correcta y mantener el software de base de manera actualizada evitando vulnerabilidades producto de patches no realizados.

N° OBS. IA Nº 08-20	Nº OBS. IA Nº 11-21	IMPACTO	DETALLE DE LAS OBSERVACIONES PRELIMINARES	RECOMENDACIONES
5.a - Tickets electrónicos	17	**Medio**	a) Falta de procedimiento para la generación de tickets electrónicos	Desarrollar e implementar un procedimiento que contemple un Sistema de requerimientos general que incluya a todas las aplicaciones vigentes en el instituto y que se acceda por fuera del Sistema NSIAF, no permitiendo otro tipo de solicitud que no sea por el mencionado sistema de requerimientos, y que se normalice su registro de manera de mantener la consistencia e integridad en los datos cargados. Cabe aclarar que el Manual de Procedimientos Sobre Accesos a Servicios y Aplicaciones en Tecnologías de la Información Res FC 90/2019 contempla los permisos de acceso que deberá articularse en su implementación con el sistema general de requerimientos de modificación a sistemas mencionado anteriormente.
5.b - Listado de usuarios del Sistema	18	**Medio**	a) Desactualización del listado de usuarios del Sistema.	Actualizar el listado de usuarios del Sistema, y realizar un debido control de accesos al mismo para identificar los usuarios de cada módulo y verificar si se trata de accesos permitidos.
	19	**Medio**	c) Falta de descripción de perfiles y roles dentro del menú del Sistema	Agregar en la pantalla de cada módulo del NSIAF los agentes usuarios del mismo, con su perfil y descripción, a fin de que su superior pueda controlar los permisos adjudicados a su personal.
5.c.1 Módulo de Créditos	20	**Medio**	a) Falta de Migración de la base de datos	Completar la migración de las bases de datos, de manera de tener una base integra y actualizada que permita la realización de la operatoria sin necesidad de efectuar tareas manuales por parte del usuario que conlleven a una carga horaria extra y la posibilidad de cometer errores.
	21	**Medio**	b) Falta de datos para los Contratos en Gestión Judicial	Implementar la funcionalidad solicitada por el área, a fin de poder realizar los cálculos necesarios con los datos del sistema NSIAF, sin necesidad de recurrir al anterior sistema AS400 que se encuentra desactualizado y sin mantenimiento.
	22	**Medio**	d) Estado incorrecto de mora en Contratos cancelados por fallecimiento	Resolver a la brevedad posible, el inconveniente presentado en los contratos cancelados por fallecimiento del beneficiario, migrando correctamente la información y los datos del mismo, a fin de poder establecer el correcto estado de los créditos.
5.c.2 - Módulo de Contabilidad y Presupuesto	23	**Alto**	a) Falta de generación de Asientos Automáticos de Haberes Militares	Implementar a la brevedad posible, la funcionalidad de generar asientos contables automáticos a fin de evitar cálculos erróneos en la tarea manual que deben realizar y controlar los usuarios del área, aumentando la carga operativa de la misma. Cumplir con la normativa del Ministerio de Hacienda.
	24	**Alto**	b) Falta de Conciliación bancaria automática	Implementar la realización de la conciliación bancaria automática en el sistema NSIAF reflejando los movimientos diarios solicitados por el Área.
5.c.3 Módulo de Retiros y Pensiones	25	**Medio**	a) Falta de Migración de la base de datos	Implementar la migración de la totalidad de las tablas solicitadas por el área, a fin de poder realizar los cálculos necesarios con los datos del sistema NSIAF, sin necesidad de recurrir al anterior sistema AS400 que se encuentra desactualizado y sin mantenimiento.
	26	**Medio**	b) Falta de Controles en el proceso de liquidación de haberes de retiros y pensiones	Implementar a la brevedad posible, los controles requeridos por el área de manera que el NSIAF los realice en forma automática.
	27	**Medio**	d) Suspensión del aplicativo de Control biométrico de supervivencia	Se recomienda que los proyectos de base tecnológica utilicen estándares definidos por la Administración Pública (punto 8.1 Res Sigen 48/05). Explorar dichas posibilidades a partir del SID Sistema de Identidad Digital (Validación remota de identidad en tiempo real con el RENAPER mediante factores de autenticación biométrica (reconocimiento facial) y fotografía del DNI). Esta recomendación está sujeta a la decisión de las autoridades de restablecer el proyecto en función de los objetivos planteados. Se recomienda derogar la RESFC 94/2019 dado su imposible cumplimiento.

Unidad de Auditoría Interna, 30 de abril de 2021.-

República Argentina - Poder Ejecutivo Nacional
2021 - Año de Homenaje al Premio Nobel de Medicina Dr. César Milstein

Hoja Adicional de Firmas
Anexo

Número: IF-2021-37902252-APN-UAI#IAF

CIUDAD DE BUENOS AIRES
Viernes 30 de Abril de 2021

Referencia: IA N° 11/2021 Definitivo

El documento fue importado por el sistema GEDO con un total de 13 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.04.30 13:31:20 -03:00

Mauro Sergio Carnelli
Auditor Interno Titular
Unidad de Auditoría Interna
Instituto de Ayuda Financiera para Pago de Retiros y Pensiones Militares

Digitally signed by Gestion Documental Electronica
Date: 2021.04.30 13:31:20 -03:00