Ministerio de Defensa

INSTITUTO DE AYUDA FINANCIERA PARA PAGO DE RETIROS Y PENSIONES MILITARES

INFORME DE AUDITORIA	N°: 25/2021
	Fecha: 30/07/2021
	SISAC Nº: 21

CARACTER: Auditoría de Cumplimiento Normativo.

TEMA: Evaluación Resolución N° 48/05 SIGEN.

NUEVO PLAN UAI 2021 **Proyecto de Auditoría N° 3**

INFORME DE AUDITORIA Nº 25/2021:

Carácter: Auditoría de Cumplimiento Normativo
Tema: Evaluación Resolución N° 48/05 SIGEN
Referencia: Plan UAI 2021 - Proyecto de Auditoría Nº 3 SISAC N° 21

1. INTRODUCCION

1.1. Objeto y alcance de la auditoría

Esta auditoría tiene por objetivo realizar el análisis y verificación del nivel de cumplimiento y adecuación de las reglamentaciones emanadas por la Resolución N° 48/2005 “Normas de Control Interno para Tecnología de la Información para el Sector Público Nacional” de la Sindicatura General de la Nación (SIGEN) y el seguimiento de las observaciones pendientes de regularización vinculadas al objeto de revisión.

El alcance de las tareas llevadas a cabo abarcará las comprobaciones establecidas en la Resolución N° 152 del 17 de octubre de 2002 de la Sindicatura General de la Nación (SGN) (“Normas de Auditoría Interna Gubernamental”), las Normas Generales de Control Interno para el Sector Público Nacional (Resolución N°172 del 28 de noviembre de 2014) y los lineamientos fijados mediante el “Manual de Control Interno Gubernamental” aprobado por Resolución N° 03 del 14 de enero de 2011 de la SGN.

La presente revisión abarca los siguientes aspectos:

1. ORGANIZACIÓN INFORMATICA
2. PLAN ESTRATÉGICO DE TI
3. ARQUITECTURA DE LA INFORMACIÓN
4. POLÍTICAS Y PROCEDIMIENTOS
5. CUMPLIMIENTO DE REGULACIONES EXTERNAS
6. ADMINISTRACIÓN DE PROYECTOS
7. DESARROLLO, MANTENIMIENTO Y ADQUISICIÓN DE SOFTWARE
8. ADQUISICIÓN Y MANTENIMIENTO DE LA ESTRUCTURA TECNOLÓGICA
9. SEGURIDAD INFORMÁTICA
10. SERVICIO DE PROCESAMIENTO Y/O SOPORTE PRESTADO POR TERCEROS
11. SERVICIOS DE INTERNET, EXTRANET E INTRANET
12. MONITOREO DE PROCESOS

Seguimiento de observaciones y recomendaciones no regularizadas, para su actualización en el SISAC.

1.2. Marco normativo y de referencia

La resolución 48/2005 de la Sindicatura General de la Nación fija las Normas Generales de Control Interno para las actividades de las Tecnologías de Información en el sector público nacional.
La mencionada norma establece los controles mínimos que deben ser implementados por las áreas responsables de la tecnología, abarcando los sistemas y demás recursos tecnológicos.

Se puede definir el control interno como "cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que puedan afectar al funcionamiento de un sistema para lograr o conseguir sus objetivos".
El control interno es un proceso integral aplicado por la máxima autoridad, la dirección y el personal de cada entidad, que proporciona seguridad razonable para el logro de los objetivos institucionales y la protección de los recursos. El control interno está orientado a promover eficiencia y eficacia de las operaciones de una organización y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control.

El control interno de las organizaciones para alcanzar la misión institucional, deberá contribuir al cumplimiento de los siguientes objetivos:

- ✓ Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- ✓ Garantizar la confiabilidad, integridad y oportunidad de la información.
- ✓ Cumplir con las disposiciones legales y la normativa de la entidad para otorgar bienes y servicios de calidad.
- ✓ Proteger y conservar el patrimonio contra pérdida, uso indebido, irregularidad o acto ilegal.

Es de suma importancia aclarar que, conforme a la Matriz de Exposición del Plan UAI 2021, el proceso que nos ocupa posee un Riesgo Extremo.

Con estos fundamentos se ha considerado la siguiente normativa de aplicación:

- RES 48/05 SG (Normas de Control Interno para Tecnología de la Información para el Sector Público Nacional).
- Programa de auditoría previsto en la Circular N° 3/05 SIGEN.
- DISP 1423/2016 (Primera apertura de estructura).
- RES 10963/2017 (Estructura organizativa de segundo nivel del Instituto).
- RES 10.990 /2017(Estructura organizativa de tercer y cuarto nivel del Instituto).
- PV-2020-18121656-APN-DIR#IAF (Aprobación Plan de acción y Presupuesto).
- RESFC-2018-127-APN-DIR#IAF (Adquisición, diseño y desarrollo de Sistemas: procedimiento para la Separación de Ambientes).
- RESFC -2020-108-APN-DIR # IAF (Reglamento Comité de Sistemas).
- RESFC-2018-126-APN-DIR#IAF (Ciclo de Vida de Sistemas).
- DISP 619/2017 IAF (Gestión de Activos y Riesgo en Seguridad de la Información).
- RESFC-2018-124-APN-DIR#IAF (ANEXO: Inventario de Activos).
- RESFC 124/2018 IAF (Procedimientos de activos y riesgo).
- RESFC-2019-53-APNDIR#IAF (Plan de contingencia).
- RESFC-2019-89-APN-DIR#IAF (Procedimiento de Monitoreo y Control de Equipamiento Tecnológico).
- RES 10.717/2016 (Acceso a red privada del IAF).
- RESFC 89/2019 IAF (Tecnología Infraestructura y Seguridad).

Asimismo, se considerarán como antecedentes, los siguientes Informes de Auditorías realizados por esta UAI:

IA N° 19/20 Evaluación Resolución N° 48/05 SIGEN.
IA N° 08/20 Evaluación del Nuevo Sistema Informático del IAF (NSIAF).
IA N° 11/2021- Evaluación del NSIAF - Seguimiento Obs. IA N° 08/2020

1.3. Notas emitidas y recibidas

El requerimiento para cumplimentar el objetivo se realizó a través de las NO-2021- 53794765 -APN-UAI#IAF y NO-2021-53792066-APN-UAI#IAF a las áreas de STIyC y a GRHyL siendo la documentación enviada por las áreas auditadas por NO-2021-53794765-APN-STIYC#IAF y NO-2021-62285220-APN-GRHYL#IAF respectivamente.

1.4 Tarea realizada

Es tarea de esta auditoría tomar conocimiento del cumplimiento de los ítems desarrollados en la Res. 48-05 SIGEN, a fin de controlar y poder analizar los riesgos en todas las actividades desarrolladas en materia de tecnologías de la información. 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 Nuevo Plan UAI 2021.
- Armado del requerimiento inicial de documentación.
- Análisis de las evidencias aportadas por el área auditada.
- Detección de posibles observaciones.
- Propuesta constructiva de recomendaciones como oportunidades de mejora.

Comprendió el análisis de la información enviada a esta UAI relativa a:

- Comité de Sistemas
- Independencia del área de TI
- Descripción documentada y aprobada de puesto de trabajo
- Separación de Funciones
- Elaboración e implementación de un Plan Estratégico
- Evaluación de la Infraestructura Tecnológica
- Aprobación de la Dirección
- Actualización del Plan Informático
- Presupuesto
- Grado de avance del Plan Informático
- Modelo de Arquitectura de la Información
- Desarrollo y Documentación de Políticas y Procedimientos
- Metodologías de Administración de Proyectos
- Monitoreo del Plan de Proyecto
- Metodología para desarrollo, mantenimiento o adquisición de sistemas
- Adquisiciones de Bienes y Servicios
- Prueba de Productos
- Mantenimiento Preventivo
- Gestión de Licencias
- Procedimientos específicos para relaciones con terceros
- Contratos con terceros
- Contrataciones de Servicios Externos
- Contenido y Estructura del sitio Web
- Level Agreement (Nivel de Servicio)
- Indicadores de Gestión
- Informes de Gestión

Asimismo, cabe mencionar que, para la presente revisión, se ha tomado como período auditado el comprendido entre el **mes de mayo de 2020 y junio de 2021**.

1.5 Aclaraciones previas y antecedentes principales

La última revisión sobre la materia bajo análisis fue la plasmada en el IA N° 19/20, en el cual se registraron las siguientes Observaciones, susceptibles de ser monitoreadas en la presente auditoría:

ITEM RESOL.48/05 SGN	N° DE OBSERVACIÓN	RECOMENDACIONES
1.Organización Informática	1) Comité de Sistemas	Actualizar las normas vigentes que definen la actuación del Comité de Sistemas y cumplimentar lo definido por la normativa
	2) Descripción documentada y aprobada de los puestos de trabajo	Estimar la asignación de los responsables faltantes a las áreas mencionadas con el objeto de favorecer la especificidad de funciones a cubrir y contar con la responsabilidad individual del agente en el logro de las tareas bajo su competencia.
	3) Plan de capacitación	La STIyC debe formular un plan de capacitación anual del sector de TI en función del Plan estratégico de TI y/o Plan de acción 2020 (Microsoft-Oracle-PHP para SARHA, MS SQL-herramientas para NSIAF.) Asimismo, debe formular las recomendaciones de capacitación anual de las áreas usuarias (no técnicas) para ser presentadas en el Comité de Sistemas consensuadas por las distintas Gerencias coordinando e integrando las necesidades de Capacitación a usuarios en uso de recursos informáticos, servicios y aplicaciones para remitirse a RRHH a integrar el plan anual de capacitación.
2. Plan Estratégico de TI	4) Elaboración e implementación de un Plan Estratégico	Formular y aprobar el Plan Informático Estratégico
3. Arquitectura de la Información	5) Modelo de Arquitectura de la Información	Implementar el proceso de registro que permita contar con la documentación que defina el modelo de arquitectura de la información (modelo de funcionamiento y datos y demás información requerida) que permita poder administrar el ciclo de vida de todos los sistemas de manera eficiente.
4. Políticas y Procedimientos	6) Desarrollo y Documentación de Políticas y Procedimientos	Completar y actualizar la documentación relacionada con la totalidad de las actividades desarrolladas en la STIyC y sus dependencias, determinando las prioridades pertinentes.
7. Desarrollo, Mantenimiento y Adquisición de Software	7) Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas	Reformular los procedimientos, mencionados privilegiando de ser posible, la intervención del responsable del área en la nueva definición, aún de manera transitoria, de manera de ser rápidamente implementada, habida cuenta de los inconvenientes encontrados en el aplicativo NSIAF
8. Adquisición y Mantenimiento de la Infraestructura Tecnológica	8) Prueba de Productos y Mantenimiento Preventivo	Implementar el procedimiento de Monitoreo y Control del Equipamiento Tecnológico.
9. Seguridad Informática	9) Actividades desarrolladas en el sector	Esta UAI recomienda fortalecer el área con el objeto de incrementar las actividades que permitan: a) Intensificar la concientización a usuarios sobre seguridad informática de manera de reducir riesgos a través comportamientos no deseados . b) Definir y/o implementar controles (como es el Procedimiento de Control de Accesos, registros en BBDD sobre el NSIAF, y sobre otros recursos de significativa importancia) c) Monitorear controles y administrar incidentes de seguridad d) Aplicación de estándares
11. Servicios de Internet, Extranet e Intranet	10) Contenido y Estructura del sitio Web	Actualizar e implementar el Procedimiento para la publicación de información en el Sitio Web del Instituto.
12. Monitoreo de Procesos	11) Indicadores de Gestión	Definir e implementar los indicadores de desempeño para monitorear la gestión y las excepciones de las actividades de TI.

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

En la revisión efectuada, se relevaron los siguientes puntos:

1. Comité de Sistemas:

Se ha restablecido la única autoridad de TI en la figura de la Subgerencia de Tecnología de Información y las Comunicaciones en el organismo. Respecto del Comité de Sistemas, cuyas atribuciones están definidas en la normativa como de asesoría y no están superpuestas con la Subgerencia mencionada en el alcance de sus funciones, se ha encontrado evidencia de la realización de una reunión del Comité de Sistemas el día 30/06/2021, conforme al nuevo REGLAMENTO DEL COMITÉ DE TECNOLOGÍAS DE LA INFORMACIÓN DEL I.A.F.P.R.P.M aprobado el 9 de diciembre de 2020 por RESFC -2020-108-APN-DIR # IAF el que establece una periodicidad semestral para las reuniones ordinarias, entendidas como aquellas a las que asisten todos los miembros que conforman el Comité, las mismas se realizarán DOS (2) veces por año, la primera de ellas en el curso del primer semestre y la restante durante el segundo semestre. Si bien no se ha realizado ninguna reunión durante el pasado año la exigencia se ha cumplimentado este semestre en tiempo y forma.

2. Separación de Funciones:

La asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses.

En el IA N° 11/2021- Evaluación del NSIAF - Seguimiento Obs. IA N° 08/2020, se regularizaron las siguientes observaciones mediante la implementación de la Separación de ambientes y la revocación de los accesos indebidos al ambiente de desarrollo:

- Obs 5d: Acceso indebido al ambiente de desarrollo
- Obs 4j: Incumplimiento de los Procedimientos de separación de ambientes
- Obs 3c: Falta de cumplimiento de la separación de ambientes

3. Infraestructura tecnológica:

Durante el periodo auditado se realizaron las siguientes acciones:

- Contratación de la provisión del servicio para el INSTITUTO y Comunicaciones CPA (internet + housing) para mantener el Centro de Proceso Alternativo.
- Adquisición de 75 Notebooks para cubrir la demanda de nuevos puestos de trabajos remotos.
- Contratación licencias período 2021 al 2023. Sistema de misión crítica (Base de datos y SO) + paquete de oficina.
- Adquisición y actualización de Discos NetApp (Almacenamiento Masivo).
- Se ha implementado nuevo firewall, capacidad de administración de VPNs, como nuevas necesidades ante requerimientos funcionales ante la nueva modalidad de trabajo

4. Regulaciones externas:

La unidad de TI debe garantizar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software, seguridad de la información, así como de las demás normas que resulten aplicables.

En relación a este ítem la STIyC expresa: "*Se cumple con todas las Regularizaciones Externas, Seguridad de la Información, Datos Personales y Firma Digital, según lo establecido por la ONTI y el Ministerio de Defensa*."

Se han incorporado nuevas necesidades que permiten definir la exigencia de cumplir con registros de BBDD en la Agencia de acceso a la información pública (AAIP) autoridad de aplicación de la ley de protección de datos personales.
Debido a los cambios de normativa en materia de seguridad de la información dictaminadas por DA 641-2021- *Requisitos mínimos de Seguridad de la Información para Organismos,* las observaciones en esta materia serán plasmadas en el IA N° 24/2021- Evaluación de la seguridad de la información.

5. Metodologías de Administración de Proyectos

La unidad de TI debe disponer de una metodología de administración de proyectos que se aplique en todos los proyectos informáticos encarados.
El área presentó documentación de seguimiento de los siguientes proyectos desarrollados durante el periodo auditado:

- Códigos de Trámites Propios –GDE.
- CREDITOS
- eIAF Empleados
- Implementaciones Tramites A Distancia- 2°Etapa
- Nsiaf
- Interfaz Apoderados
- Interfaz CBU
- Interfaz IIGG
- Portal BNA.NET
- Central telefónica
- Renaper -Aprobación del texto del Convenio único de confronte de datos personales entre el Registro Nacional de las personas y el IAF.

6.Informes de Gestión

La unidad de TI debe presentar informes periódicos de gestión, a la Dirección de la organización para que ésta supervise el cumplimiento de los objetivos planteados.
La STIYC realizó el envío a la Dirección de la siguiente documentación:

- ✓ Estado de situación NSIAF por NO-2020-41267133-APN-STIYC#IAF de junio 2020.
- ✓ Informe del Estado de situación de STIyC de fecha mayo 2021.
- ✓ Acuerdo Específico con UNDEF -Pruebas de Intrusión con fecha marzo 2021.
- ✓ Informe y Acta de Comité de Tecnología de la Información del 30-06-2021.

7. Modelo de Arquitectura de la Información

La unidad de TI ha definido una metodología según el relevamiento efectuado que implica:

a) Una descripción del proceso (descripción de la función desarrollada)
b) Soportes tecnológicos utilizados
c) Las características básicas de la información administrada
d) Condiciones limitantes que se han considerado
e) Interacción del proceso con otros componentes tecnológicos del sistema general
f) Cursograma del proceso administrativo (esto es las principales actividades y controles dentro del accionar de la organización que cubren esta funcionalidad.

Se ha desarrollado sobre las nuevas funciones de manera de contar con una descripción general lo más precisa posible del puente de interacción entre la actividad o proceso de negocio y los componentes del sistema (software y hardware) con el

objeto de ir configurando en detalle el modelo de arquitectura de la información de la organización, orientado a asegurar que tratamiento se da a la información y en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad, exactitud o formato, entre otras.
Este modelo de arquitectura de la información debe documentarse y mantenerse actualizado y debe ser completado oportunamente en las bases de datos especificando los controles de consistencia, integridad, confidencialidad y validación, todos ellos documentados y administrados a través de un administrador de BBDD.

Si bien no se dispone de la información total para contar con un mapa de detalle de los módulos que conforman la arquitectura de la información, se conocen sus procesos e interacción sobre soporte de datos del NSIAF y se va avanzando en función de la metodología descripta. El área de STIYC continuará con la tarea de documentación y será materia de análisis en el próximo informe de auditoría.

8. Indicadores de Gestión

Se ha configurado una serie de indicadores de gestión que configuran una base mínima a tener en cuenta para su profundización.
Se ha relevado:

1) Estadísticas sobre tickets por solicitudes de usuarios por sistema.
2) Estadísticas de monitoreo de incidentes en firewall de frecuencia trimestral.
3) Registro de vulnerabilidades y su tratamiento sobre la misma fuente.
4) Seguimiento trimestral de indicadores de la planificación anual remitidos a la Subgerencia de Planeamiento.

Se deben profundizar los indicadores de desempeño con el objeto de monitorear la gestión de los sectores dentro del área de TI a fin de potenciar las ventajas obtenidas o de tomar acciones correctivas si se detecta un aprovechamiento ineficiente de los recursos, existencia de riesgos no administrados o desvíos en la ejecución de tareas.
STIYC deberá continuar con la tarea, la cual será materia de análisis en el próximo informe de auditoría.

2.2 Observaciones y recomendaciones:

Del análisis efectuado sobre el nivel de cumplimiento de la Res N° 48/05 (SIGEN), surgen los resultados que se exponen:

Obs. 1- Falta de asignación de Jefes de División:

La RESFC-2017-10996-APN-DIR#IAFde 27/03/2017 nombra en su Anexo I, a los jefes de Departamentos y en su Anexo II los Jefes de División de todas las áreas del Instituto, observándose que los puestos de los Jefes de División dependientes de la STIyC se encuentran vacantes.
Luego, por RESFC-2020-47-APN-DIR#IAF del 19/03/2020, se nombra al Jefe de División Tecnología y Seguridad y al Jefe de División Infraestructura.
Se evidenció que el resto de las Divisiones: Desarrollo e Innovación, Mantenimiento de Sistemas, Gestión de Proyectos y Control de Procesos y Calidad no tienen jefes asignados en su cargo y cuyas funciones son (RESFC 10990/17):
Departamento de Gestión de Proyectos, Control de Procesos, Base de Datos y Calidad

División Control de Procesos y Calidad

- Asistir en el control de los procesos informáticos

- Ejecutar cuadros estadísticos de ejecución de procesos
- Verificar el cumplimiento de las normas vigentes referidas al Sistema de Calidad del IAF
- Ejecutar el monitoreo de los procesos

División Gestión de Proyectos

- Asistir en el análisis y diseño de proyectos
- Verificar el cumplimiento de las normas vigentes referidas al “Ciclo de vida de los Sistemas Informáticos” en las etapas de análisis preliminar y pruebas integral.
- Ejecutar el monitoreo de la implementación del proyecto.
- Verificar el cumplimiento de la metodología utilizada para la gestión de proyectos.

Departamento de Desarrollo y Mantenimiento de Sistemas:

División Desarrollo e Innovación

- Asistir al Departamento en la realización de estudios de factibilidad en la utilización de nuevas herramientas para el desarrollo y ejecución de los sistemas.
- Ejecutar las etapas necesarias para el cumplimiento del ciclo de vida de los sistemas informáticos conforme a los estándares y buenas prácticas en la materia
- Entender en los nuevos desarrollos de sistemas propios o realizados por terceros.
- Participar en las decisiones técnicas a tomar en conjunto con proveedores externos.

División Mantenimiento de Sistemas

- Ejecutar y verificar la realización del mantenimiento correctivo, evolutivo y perfectivo de los sistemas en ejecución.
- Entender en el establecimiento de interfaces informáticas con otros sistemas internos y externos.
- Elaborar la documentación técnica y/o funcional de los sistemas desarrollados.
- Asegurar la disponibilidad de los sistemas informáticos con el fin de cumplir el cronograma definido por el INSTITUTO para cada uno de sus procesos.

El alcance de las tareas de desarrollo y control de la seguridad informática alcanza a todas las actividades de la Subgerencia, debiendo ejercerse de manera más autónoma dado que interactúa con todas las áreas y asignándose las responsabilidades correspondientes dada la especificidad del tema y el crecimiento y profundización de las tareas que este sector tiene en materia de Seguridad de la Información. Asimismo, la incorporación de plataformas tecnológicas de uso masivo en mercado (base Microsoft) potencia exigencias en materia de seguridad y se observa que parte de las vulnerabilidades encontradas si bien pueden y son tratadas deberían considerar la nominación de personal responsable para cubrirlos.

Recomendación: Asignar los responsables faltantes a las áreas mencionadas con el objeto de favorecer la especificidad de funciones a cubrir y contar con la responsabilidad individual del agente en el logro de las tareas bajo su competencia.

Fortalecer el sector de Seguridad Informática, constituido hoy en una División con otras funciones, definiendo su separación y dependencia directa al máximo nivel de conducción.

Obs. 2- Falta Plan de capacitación de TI del organismo:

Se evidenció que la capacitación en materia de interna de la subgerencia se ha previsto y desarrollado hasta la fecha habida cuenta de las debilidades detectadas en el NSIAF, en su construcción, tanto técnicas (faltas en seguridad, en documentación, excesivo mantenimiento) como funcionales (reformulación de circuitos, debilidades de control, cobertura operacional limitada), agravadas además por considerar en un futuro el reemplazo del sistema AS400 y el sistema de gestión documental.
Faltan definir los planes de capacitación del personal administrativo en las herramientas vinculadas a TI e informar a RRHH para que éste los integre al Plan de capacitación del Instituto.
Asimismo, deberá considerarse en este ítem la incorporación de la concientización en materia de seguridad informática dado que capacitan al personal en prácticas que atienden al control de vulnerabilidades en el manejo de información.
Recomendación: Actualizar las acciones desarrolladas y formular el Plan de Capacitación en materia de TI articulando con las áreas externas a la Subgcia. la atención a sus necesidades en el manejo de herramientas tecnológicas y presentándolo a RRHH para su integración al Plan General y su aprobación por las autoridades.

Obs. 3- Falta de actualización del Plan Informático Estratégico:

Se evidenció que el Plan Informático Estratégico requiere una redefinición y reformulación de sus objetivos en el mediano plazo, debido al balance de situación sobre lo desarrollado hasta la fecha en el Sistema NSIAF, encontrando debilidades detectadas en su construcción, tanto técnicas (faltas en seguridad , en documentación, excesivo mantenimiento) como funcionales (reformulación de circuitos, debilidades de control, cobertura operacional limitada) , agravadas además de considerar el reemplazo del sistema AS400 y el sistema de gestión documental.
Se debe formular un plan de acción del año 2021-2023
Recomendación: Formular y aprobar el Plan Informático 2021-2023

Obs. 4- Falta de actualización de Política y Procedimientos de TI a partir de una metodología

La documentación de políticas y procedimientos del área de STIyC cubre distintos aspectos de la organización interna durante su historia y en general no han sido actualizados ni ante el cambio tecnológico que produjo cambios en la lógica del proceso ni ante procesos nuevos, es decir que no han sido completados a la fecha. Hay procedimientos que se encuentran desarrollados como el procedimiento de Control de accesos, para ser implementados en el presente año. Debe establecerse una metodología común que establezca las necesidades mínimas de información a contener debiendo ser lo suficientemente modular para permitir cambios que no requieran su reemplazo.
Recomendación: Actualizar la documentación relacionada con la totalidad de las actividades desarrolladas en la STIyC y sus dependencias. Implementar los procedimientos según la metodología acordada en lo posible previamente con la Auditoría.

Obs.5- Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas:
La Subgerencia debe contar con una metodología segura para la documentación de

desarrollo y mantenimiento de sistemas, si bien cuenta con documentación de requerimientos por parte de las áreas usuarias, ya sea para nuevos desarrollos o cambios a los sistemas existentes, incluyendo la definición de las necesidades que motivan el requerimiento.
Se recuerda que las actividades comprenden a) documentación, registro y monitoreo de actividades. b) El establecimiento de prioridades. c) El tratamiento de las solicitudes de emergencia. d) La aprobación, de las especificaciones de diseño. e) La participación de la Unidad de Auditoría Interna durante el desarrollo. f) La utilización de estándares de diseño, programación y documentación. g) La realización de pruebas suficientes que deben contemplar la participación y aprobación formal del usuario solicitante. h) El pasaje del sistema aprobado desde el ambiente de desarrollo / prueba al de producción. i) El control de las versiones del software j) La preparación de documentación de soporte para el usuario y el personal técnico. k) La capacitación al personal de las áreas usuarias y la de TI.
Por RESFC IAF 127/2018, el Directorio aprueba el "Procedimiento de Separación de ambientes" que trata los procesos de desarrollo de software, resguardo de fuentes, procesos de prueba, aprobación y tratamiento de pase a producción con las condiciones de explotación.
Asimismo, por RESFC IAF 126/2018 se aprueba el "Procedimiento de ciclo de vida de los sistemas" que describe los cambios a producirse en un aplicativo en función de los requerimientos o necesidades solicitadas, y los movimientos (ABM) que reflejan transformaciones funcionales a lo largo de su vida útil.
Del análisis de las medidas tomadas a partir de tomar el control el año ppdo sobre las operaciones y tener una mejora sensible en las acciones de desarrollo se debe profundizar el aspecto metodológico de documentación y registro de las modificaciones.
Recomendación: Esta UAI recomienda revalidar el actual desarrollo metodológico con las premisas señaladas en función de los desvíos encontrados.

Obs. 6- Debilidades en Seguridad Informática:

Se han registrado avances en esta materia ante la implementación de equipamiento y planes de mejora. Sin embargo, las debilidades de seguridad encontradas en el presente año requieren un mayor control en los procesos, estándares a cumplir y concientización en el uso de recursos.
Cabe mencionar que se han informado dos actividades significativas como son la instalación y configuración del nuevo firewall (realizada en el 1er semestre del año) y la tramitación de un test de intrusión (actualmente en ejecución). Se destaca que el cambio tecnológico produce una mayor exposición en tanto los nuevos recursos son de uso masivo en el mercado (plataforma Microsoft) y si bien se cuenta con nuevo firewall, no se ha hecho desde hace varios años un nuevo test de intrusión, a pesar de contar con un aplicativo de alcance corporativo (NSIAF) que permita conocer el nivel de vulnerabilidad de lo implementado.
Se estima un fortalecimiento del sector no solo en relación al personal involucrado sino al alcance de actividades que le competen. Esta situación se encuentra agravada además por las vulnerabilidades encontradas en el proyecto NSIAF.
Recomendación: Esta UAI recomienda fortalecer el área con el objeto de incrementar las actividades que permitan:
a) Intensificar la concientización a usuarios sobre seguridad informática de manera de reducir riesgos a través comportamientos no deseados.

b) Definir y/o implementar controles (como es el Procedimiento de Control de Accesos, registros en BBDD sobre el NSIAF, y sobre otros recursos de significativa importancia)
c) Monitorear controles y administrar incidentes de seguridad

Obs 7 - Contenido y Estructura del sitio Web:

El contenido y la estructura del sitio web de la organización deben basarse en un modelo aprobado por las autoridades, en el que estén documentados los siguientes aspectos:

- Contenido y estructura del sitio
- Fuentes de ingresos de datos
- Frecuencias de las actualizaciones
- Necesidades de disponibilidad del sitio.
- Recursos afectados
- Responsable de los contenidos

Mediante Res N° 10.776/2016, el Directorio aprueba el Procedimiento para la publicación de información en el Sitio Web del Instituto.
Se evidenció que el mismo se encuentra desactualizado en relación a las áreas responsables del proceso como ser: el Área de Coordinación General no existe actualmente en el organigrama institucional, por otro lado, el Área de Comunicación Institucional en la actualidad es el Dto. De Comunicación Institucional Y Ceremonial y la Gerencia de Tecnologías de la Información es actualmente la Subgerencia de Tecnologías de la Información y las Comunicaciones.
No se encontró evidencia del circuito que se realiza actualmente respecto al ABM de novedades del Sitio Web Institucional.
El área de STIYC informa: *"Se encuentra en proceso un nuevo procedimiento para la publicación y modificaciones de contenido en Internet, Extranet e Intranet, se adjunta Manual de Uso de Cargos para Entidades y de Archivos para Banco Nación de Embargos Judiciales"*
Recomendación: Actualizar e implementar el Procedimiento para la publicación de información en el Sitio Web del Instituto que incluya el circuito que se realiza actualmente respecto al ABM de novedades.

2.3. Observaciones de Seguimiento del IA N° 19/2020:

Obs. 1: Relacionada al Comité de Sistemas

Dicho hallazgo se relaciona con lo expuesto en la Verificación 1 del presente Informe por lo cual se da por regularizada.

Obs.2: Relacionada a la Descripción documentada y aprobada de los puestos de trabajo

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar N° 1 Falta de asignación de Jefes de División del presente Informe.

Obs.3: Relacionada al Plan de capacitación

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 2- Falta de Plan de capacitación del presente informe.

Obs.4. Relacionada a la Elaboración e implementación de un Plan Estratégico

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 3- Falta de actualización del Plan informático Estratégico del presente informe.

Obs.5: Relacionada al Modelo de Arquitectura de la información

Dicho hallazgo se relaciona con lo expuesto en la verificación 7 del presente informe por lo cual se da como regularizada.

Obs. 6: Relacionada al Desarrollo y Documentación de Políticas y Procedimientos

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 4- Falta de actualización de Políticas y Procedimientos de TI.

Obs. 7: Relacionada a la Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 5- Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas.

Obs. 8: Relacionada a la Prueba de Productos y Mantenimiento Preventivo

Dicho hallazgo se relaciona con lo expuesto en la Verificación 3 del presente Informe por lo cual se da por regularizada.

Obs. 9: Relacionada a la Actividades desarrolladas en el sector.

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 6- Debilidades en Seguridad Informática del presente informe

Obs.10: Relacionada al Contenido y Estructura del sitio Web

La situación continúa vigente, por lo tanto, se mantiene la Observación bajo análisis como pendiente de regularización y se la encuadra en la Obs. Preliminar Nº 7- Contenido y Estructura del sitio Web del presente informe.

Obs. 11: Relacionada a los Indicadores de Gestión

Dicho hallazgo se relaciona con lo expuesto en la verificación 8 del presente informe por lo cual se da como regularizada.

2.4. Tratamiento ulterior del Informe con las áreas auditadas

Mediante NO-2021- NO-2021-66507790-APN-UAI#IAF del 23/07/2021, esta UAI remitió el IA Preliminar a la STIYC. A través de la NO-2021-68158880-APN-STIYC#IAF, la STIYC expresó su opinión sobre el mismo, detallando las acciones correctivas que implementará junto con el plazo que estima para su regularización. A continuación, el detalle de sus respuestas textuales:

NRO	OBSERVACION	Acción correctiva comprometida	Fecha estimada de Regularización
1	Falta de asignación de Jefes de División	*Se elevará a autoridad superior la necesidad de designar resonsables*	*Agosto 2021*
2	Falta Plan de capacitación de TI del organismo	*Se formulará el Plan de Capacitación articulando con las áreas externas*	*2do. Semestre 2021*
3	Falta de actualización del Plan Informático Estratégico	*Se formulará el Plan Informpático Estratégico 2021-2023*	*2do. Semestre 2021*
4	Falta de actualización de Política y Procedimientos de TI a partir de una metodología	*Se continuará con el proceso de actualización de documentación y se acordará con la UAI la metodología*	*2do. Semestre 2021 1er. Trimestre 2022*
5	Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas	*Se realizará una revisión de las metodologías para desarrollo, mantenimiento y adquisición de sistemas*	*2do. Semestre 2021*
6	Debilidades en Seguridad Informática	*Se elevará a autoridad superior la necesidad de fortalecer el área de Seguridad Informática*	*2do. Semestre 2021*
7	Contenido y Estructura del sitio Web	*Se actualizará e implementará el procedimiento para la publicación de información en el Sitio Web*	*2do. Semestre 2021*

3. CONCLUSIONES

3.1. Conclusión de carácter general

Se ha analizado y verificado el nivel de cumplimiento de las reglamentaciones emanadas por la Res 48/2005 “Normas de Control Interno para la Tecnología de la Información para el Sector Público Nacional” de la Sindicatura General de la Nación y el seguimiento de las observaciones pendientes de regularización del IA 19/2020.

Como síntesis de lo observado y ante las condiciones impuestas por el teletrabajo y la situación general descripta el año ppdo. se considera destacable mencionar que se ha avanzado en las debilidades existentes, estando alguna de ellas en tratamiento como a) cubrir puestos definidos en la estructura, b) finalizar el plan de capacitación c) implementar procedimientos en el área de desarrollo, estimándose próximamente su total implementación.

Se destaca la importancia de la necesidad de reformular el Plan Informático Estratégico del organismo dados los avances en el conocimiento y mayor control de las actividades. El

mismo requiere tanto la mejora funcional del NSIAF (integrando los módulos faltantes) como también incorporar el uso de herramientas de software que permitan administrar la información de manera integrada, en una nueva concepción que permita el cambio en las modalidades de trabajo en cualquier circunstancia.

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

Número	OBSERVACION	IMPACTO	RECOMENDACIÓN
1	Falta de asignación de Jefes de División	Medio	Asignar los responsables faltantes a las áreas mencionadas con el objeto de favorecer la especificidad de funciones a cubrir y contar con la responsabilidad individual del agente en el logro de las tareas bajo su competencia.
2	Falta Plan de capacitación de TI del organismo	Bajo	Actualizar las acciones desarrolladas y formular el Plan de Capacitación en materia de TI articulando con las áreas externas a la Subgcia. la atención a sus necesidades en el manejo de herramientas tecnológicas y presentándolo a RRHH para su integración al Plan General y su aprobación por las autoridades
3	Falta de actualización del Plan Informático Estratégico	Alto	Formular y aprobar el Plan Informático 2021-2023
4	Falta de actualización de Política y Procedimientos de TI a partir de una metodología	Medio	Actualizar la documentación relacionada con la totalidad de las actividades desarrolladas en la STIyC y sus dependencias. Implementar los procedimientos según la metodología acordada en lo posible previamente con la Auditoría
5	Metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas	Medio	Esta UAI recomienda revalidar el actual desarrollo metodológico con las premisas señaladas en función de los desvíos encontrados
6	Debilidades en Seguridad Informática	Medio	Esta UAI recomienda fortalecer el área con el objeto de incrementar las actividades que permitan:a) Intensificar la concientización a usuarios sobre seguridad informática de manera de reducir riesgos a través comportamientos no deseados.b) Definir y/o implementar controles (como es el Procedimiento de Control de Accesos, registros en BBDD sobre el NSIAF, y sobre otros recursos de significativa importancia)c) Monitorear controles y administrar incidentes de seguridad
7	Contenido y Estructura del sitio Web	Medio	Actualizar e implementar el Procedimiento para la publicación de información en el Sitio Web del Instituto que incluya el circuito que se realiza actualmente respecto al ABM de novedades.

Unidad de Auditoría Interna, 30 de julio 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-2021-68861023-APN-UAI#IAF

CIUDAD DE BUENOS AIRES
Viernes 30 de Julio de 2021

Referencia: IA N° 25/2021 Definitivo

El documento fue importado por el sistema GEDO con un total de 15 pagina/s.

Digitally signed by Gestion Documental Electronica
Date: 2021.07.30 14:45:47 -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: 2021.07.30 14:45:48 -03:00