INFORME EJECUTIVO CORRESPONDIENTE AL I. A. N° 08/19

El presente informe tiene por objeto sintetizar las tareas de auditoría llevadas a cabo a fin de emitir el I.A. N° **08/19.**

Tema: Evaluación Seguridad de la Información - Seguimiento IA N° 18/18

Referencia: Plan Anual de Auditoría 2019- (Proyecto N° 20 – SISIO N° 09).

Objetivo y Alcance

El **objetivo** de la tarea a realizar comprende el seguimiento de Informes anteriores, el análisis y verificación del nivel de cumplimiento y adecuación de las reglamentaciones vigentes e implementación de la Norma ISO/IEC 27001:2005 Anexo A – "Objetivos de Control y Controles de Seguridad de la Información".
El **alcance** de las tareas llevadas a cabo abarcó las comprobaciones fijadas en la Resolución 152/02-SGN (Normas de Auditoría Gubernamental), los lineamientos fijados en el "Manual de Control Interno Gubernamental" aprobado por Resolución N° 03/11 SGN, la Disposición ONTI N° 01/2015 de fecha 19/02/2015, por medio de la cual se aprueba la "Política de Seguridad de la Información Modelo", que reemplaza a los mismos fines a la aprobada por Disposición ONTI N° 3/2014, los estándares de la serie ISO IEC/2700X en particular ISO/IEC 27001:2005 y el Programa de Trabajo de Revisión de la Política de Seguridad de la Información publicado por SGN.
Este alcance comprende el seguimiento de observaciones y recomendaciones no regularizadas, para su actualización en el SISIO 3 - Sistema de Seguimiento de Informes y Observaciones versión 3 (I.A. N° 18/18).
El período auditado corresponde al comprendido entre el mes de julio de 2018 y marzo 2019.

.
La presente revisión abarca los siguientes aspectos, a saber:

a. Evaluación y tratamiento de riesgos
b. Política de Seguridad de la Información
c. Organización de la Seguridad de la Información
d. Plan de anual de capacitación
e. Gestión de Activos de Información
f. Seguridad de los Recursos Humanos –Gestión de accesos
g. Seguridad Física y ambiental
h. Servicios de Procesamiento y/o soporte de Terceros
i. Gestión de Operaciones y comunicaciones
j. Gestión de Incidentes de Seguridad de Información
k. Cumplimiento de Regulaciones Externas

Posición de Auditoría

La revisión se efectuó a fin de evaluar el contexto donde se procesa y almacena la información sensible del Instituto, y que debe asegurar la integridad, confiabilidad, confidencialidad y disponibilidad de dicha información
Definir, lograr, mantener y mejorar la seguridad de la información es esencial para mantener una eficacia en la operación de las actividades del Instituto. La seguridad que se puede lograr a través de medios técnicos es limitada, y ser apoyada por la gestión con los procedimientos adecuados.
Dicha revisión se basó en las buenas prácticas y la normativa vigente, que deben interpretarse como un compendio de mejores prácticas públicas y adaptadas a la realidad, recursos y operatoria del Instituto.

RESULTADOS
Verificaciones y hallazgos

Aclaraciones de Previo y Especial Pronunciamiento

El Comité de Seguridad de la Información del IAFPRPM fue conformado con fecha 30/09/2005 mediante Disposición de Presidencia N° 209, en atención a la Decisión Administrativa MinDef N° 669 del 20/12/2004. Mediante las Resoluciones Nos. 10.166 del 07/11/2012; 10.563 del 16/04/2015 y RESFC-2019-2-APN-DIR#IAF del 24/01/2019; se fueron adecuando las reglas de funcionamiento del Comité de Seguridad de la Información al contexto vigente y a las estructuras organizativas sucesivas, siendo la última de ellas la plasmada en la Decisión Administrativa MinDef N° 1423 del 06/12/2016 y sus relacionadas Resoluciones IAFPRPM Nos. 10.963 del 24/01/2017; 10.990 del 23/02/2017 y RESFC-2018-58-APN-DIR#IAF del 22/03/2018.
En tal sentido, el Comité de Seguridad de la Información ha venido realizando un extraordinario trabajo en aras de alinear al Instituto con los mejores estándares vigentes a la fecha en la materia. Este Comité, se ha venido dedicando a la mejora contínua en temas de Seguridad de la Información, en línea, entre otros, con los parámetros emanados de la Dirección General de Ciberdefensa dependiente del Ministerio de Defensa. Todo esto representa un trabajo gradual y secuencial que de ninguna manera puede imaginarse como de realización instantánea. Es por ello que se advierte que determinados hallazgos y comprobaciones de la presente auditoría tienen lógica fuente instrumental en las Actas del Comité a la cual se le debe prestar atención como reveladoras de temas pendientes de mejora.

1- Evaluación de riesgos

De resultas de las presentes actuaciones y en línea con lo mencionado en la aclaración previa; se puede destacar que a la fecha existe la definición del Inventario Inicial de Activos de Información conforme Minuta N° 3 del Comité de Seguridad de la Información (16/08/2018) y se ha definido que el Análisis de Riesgos inherentes a los mismos sería efectuado por cada Responsable del Activo (gerente o similar) conducido por el Área de Seguridad de la Información. Sin embargo, no obra evidencia de la existencia a la fecha de una actualización integral (de todas las áreas involucradas y con su correspondiente análisis de atributos) del inventario. Se destaca como hecho positivo el que a la fecha en la Subgerencia de Créditos y en la Jefatura de Seguridad, dependiente de la DEj. se haya podido constatar la finalización de los mencionados procesos, esto es, actualización de inventario y matriz de riesgo. Cabe señalar que, en el Comité de Seguridad de la Información se han conformado los equipos de trabajo para la actualización del Inventario de Activos y confección del análisis de exposición al riesgo para las siguientes áreas:

- GRF/SPC/Departamento de Presupuesto y Departamento Contable.
- GRF/SFI/Departamento de Tesorería – División Pagos y Departamento de Operaciones Financieras.
- GRF/Scr/Departamento de Administración de Carteras y División Amortizaciones.
- GRHyL/Subgerencia de Logística.
- GRHyL/Subgerencia de RR.HH.
- GRP/División Estadística y Control
- GAJ/SAJ/Depto. Contencioso/Div. Procuradores
- GAJ/SAL/Depto. Sentencias Judiciales
- STIyC/Depto. Tecnología Infraestructura y Seguridad.

Sobre los seis primeros se ha efectuado una capacitación el pasado 17/01/2019.

Opinión UAI: Continuar con los trabajos realizados en relación con Inventario de Activos de la Información. Se recomienda determinar los atributos para cada activo, esto es, el propietario, la criticidad, amenazas, controles de seguridad, etc., para poder accionar correctamente ante incidentes o desastres, conforme las definiciones del procedimiento de Gestión de Activos y Riesgos del Instituto y en línea con las conclusiones del Comité de Seguridad de la Información.

Recomendación: Seleccionar los activos para el estudio de riesgo y avanzar con la constitución del inventario de activos de información del Instituto.

2- Normativa y Manuales de Procedimiento

En línea con lo mencionado en la aclaración previa, según la Minuta N° 3/2018 del Comité de Seguridad de la Información de fecha 16/08/2018; lo cual la ubica dentro del período auditado, se reconoce la necesidad de actualizar el cuerpo Normativo de Seguridad de la Información y formar un cuerpo uniforme y funcional a las necesidades del IAF.

En este sentido, se ha constatado que con fecha 24/01/2019 se aprobaron las "Políticas Específicas de Seguridad de la Información" (IF-2018-65124823-APN-SPYMC#IAF y ACDIR-2019-1-APN-DIR#IAF), elaboradas por el Área de Seguridad de la Información con la colaboración de la Subgerencia de Planeamiento y Mejora Continua.

Se destaca que, si bien se encuentra fuera del período auditado, la Reunión Ordinaria N° 1/2019 del Comité de Seguridad de la Información, celebrada el 11/04/2019, su temario y conclusiones son elemento válido para el presente análisis. De la misma se desprende un detallado cuadro de situación del plexo normativo del IAF en materia de seguridad de la información a tal fecha.

De esta Acta de Reunión se infiere que los siguientes procedimientos se encuentran en proceso de elevación y aprobación por parte del Directorio:

a) Gestión y Control de Accesos: Procedimiento del NSIAF sobre registro de ingresos (accesos) al sistema, identificaciones y autorizaciones.

b) Seguridad Física y Ambiental:

- La misma involucra:

1. La definición de las áreas protegidas y protección del equipamiento contenido, tratamiento de eventos para conservar la operatividad del Instituto en general.
2. La definición y condiciones de protección ambiental y del personal en el perímetro IAFPRPM.
3. La protección de activos de información específicos, especialmente documentación en traslado y depósito
4. La protección de activos físicos y servicios de infraestructura.

- La casuística abordada por el Comité y atinente a esta dimensión del riesgo abarca los eventos de:

1. Incendio, alarmas y extintores.

2. Evacuación.
3. Inundación.
4. Seguridad Física
5. Documentación

c) Gestión de la Continuidad Operativa: En relación a una eventual falta de suministro eléctrico, temática bajo el dominio de la SLo, restaría definir su Procedimiento de Contingencia.

d) Adquisición, diseño y desarrollo de Sistemas: Es una observación recurrente ante diversos procedimientos de auditoria la ausencia de la Metodología de Gestión de Proyectos. Esto se debe a la reglamentaria necesidad de su existencia integrada a la organización del IAF. Por ello, se reitera el punto propiciando su redacción y aprobación. En el mismo sentido, se destaca la necesidad de aprobación formal de un Marco General o Modelo de Confidencialidad para las nuevas contrataciones de Sistemas, en salvaguarda de la Seguridad de la Información.

e) Operaciones y comunicaciones: En virtud de la presente auditoría, se ha requerido el detalle de la Política, Procedimientos y acuerdos con otros organismos para el intercambio de información en relación a la Gestión de Comunicaciones y Operaciones. La respuesta recibida remite a la Política de Gestión de la Continuidad Operativa integrante de las Políticas Específicas de Seguridad de la Información, manifestando que a la fecha se encuentra pendiente de actualización el Procedimiento correspondiente. No se ha remitido evidencia de los acuerdos con otros organismos para el intercambio de información, como por ejemplo, el SINTyS.

Opinión UAI: La aprobación pendiente de los procedimientos mencionados y su consecuente implementación son parte de un programa de trabajo en plena ejecución, lo cual se destaca como un aspecto positivo. Estas aprobaciones permitirán mejorar la gestión y administración de los activos de información del Instituto y mejorar la la seguridad de la información mitigando sus riesgos vinculados, por lo cual esta Auditoría no formula observaciones ni recomendaciones.

3- Centro de Procesamiento de datos del Instituto

De la visita realizada al CPD el día 13/05/2019 pudo observarse que no se realizaron las mejoras sugeridas por esta UAI en I.A. N° 18/18, a saber:

1. La pared divisoria del recinto contiene paneles de vidrio, las mismas no tienen un nivel de blindaje adecuado.

2. El lugar cuenta con dos puertas de acceso, la salida de emergencia debe poseer una cerradura especial que permita la rápida salida desde el interior del pero no la entrada al mismo (ej. Barra antipánico).

Se encontró evidencia del cumplimiento de normas de seguridad física y ambiental del Centro de Procesamiento Alternativo (CPA) que se encuentra en ARSAT (Empresa Argentina de Soluciones Satelitales SA), localidad de Benavidez, provincia de Buenos Aires.

Opinión UAI: Si bien es deseable adecuar el centro de cómputos ajustándolo a las medidas de seguridad mencionadas, es necesario reconocer la escasa relevancia e impacto en el cumplimiento de la misión y funciones del área auditada, no puede dejar de reconocerse la situación de austeridad presupuestaria que dificultaría su financiamiento en el corto plazo, por lo cual esta Auditoría decide no insistir en la observación de informes anteriores.

Recomendación: Tomar nota para ejercicios futuros.

4- Gestión de Incidentes de Seguridad de Información

Mediante requerimiento esta UAI procuró establecer expresamente cual habría sido el último informe de amenazas detectadas contra los sistemas y los métodos utilizados, así como evaluar los resultados del último Test de Intrusión.

Se menciona que la última evidencia obrante previa al presente procedimiento es de Enero de 2014, según consta en el I.A. N° 18/18.

A tenor de la respuesta recibida por esta UAI, se puede observar que:

a) Se encuentra vigente a la fecha la Norma de Gestión de Incidentes basada en la Disposición N° 335 del 03/08/2011, cuyos antecedentes se encuentran derogados.
b) Estos Procedimientos estarían complementados por lo establecido en el Manual de Procedimientos para la Gestión de Activos de Información y Riesgos.
c) Se reconoce en la respuesta al requerimiento que "El test de intrusión es un mecanismo preventivo que estudia las vulnerabilidades para evitar que ocurra el incidente" y que "..se informa que el test de intrusión está en la órbita de la STIyC para su tramitación."

Por ello, se puede concluir que a la fecha no se encuentra evidencia de la realización de un Test de Intrusión Interno, Externo, Web e Ingeniería Social del Instituto.

Se evidenció la existencia de dos Informes de Seguridad Informática, realizados en los períodos de febrero y marzo de 2019 por la STIyC, Departamento de Infraestructura, Tecnología y Seguridad.

Opinión UAI: El test de intrusión es sólo una parte de un conjunto de medidas que hacen a la seguridad informática que permite tomar los planes de acción y recomendaciones necesarios ante nuevas vulnerabilidades de seguridad informática que pueden afectar a los equipos y servicios instalados. Considerando la actual complejidad del entorno y la especialización creciente de los intrusos y que existen indicios claros que el sistema de protección informática del IAFPRPM posee adecuados niveles seguridad a tenor de los Informes de Seguridad Informática elaborados por el Departamento de Infraestructura, Tecnología y Seguridad dependiente de la STIyC, esta Auditoría puede aceptar que el test de intrusión se efectúe cuando estén dadas las condiciones presupuestaria para su contratación o cuando la División de Ciberdefensa dependiente del Ministerio de Defensa así lo requiera.

Recomendación: Considerar la posibilidad de llevar a cabo pruebas de intrusión periódicas a fin de detectar vulnerabilidades, su corrección y consecuente elevación del nivel de seguridad real del Instituto en cuanto estén dadas las condiciones presupuestarias y/o tomar nota para la próxima formulación presupuestaria.

5- Indicadores de Gestión

El Instituto ha mostrado importantes avances en relación a la Política de Seguridad de la Información. Conforme a los lineamientos de SIGEN, la Resolución SGN N° 162/2014 - ANEXO III, la Resolución SIGEN N° 128/2015 que aprueba el Documento Técnico N° 9 "Guía para la construcción de indicadores y técnicas de uso", entre otros, es necesario plasmar estos avances mediante indicadores de gestión. De momento, estos indicadores no se encuentran disponibles dentro del Tablero de Control Operativo del IAF elaborado por la SPyMC. Este Tablero, que compila un conjunto de índices de gestión del ente, no muestra evidencia de la existencia de indicadores que detallen registro, evaluación y reporte de la gestión del Área de Seguridad de la Información. Esta UAI, sugiere a modo de ejemplo, y al sólo efecto enunciativo, la siguiente nómina de indicadores útiles y posibles:

1. Indicador de Eficiencia en el tratamiento de eventos relacionados la seguridad de la información (eventos exitosos / eventos totales).
2. Indicador de Nivel de preparación del recurso humano y su apropiación en cuanto a la seguridad de la información y los equipos de cómputo (¿se han definido lineamientos de trabajo – capacitaciones sobre seguridad información y de protección física instalaciones? si/no).
3. Indicador de Cumplimiento de políticas de seguridad y privacidad de la información en el organismo (si/no).
4. Indicador de Número de activos críticos de información incluidos en el alcance de implementación del modelo, derivado del Inventario a definir.
5. Indicadores de Identificación de existencia o no de lineamientos, normas o estándares en cuanto a la adquisición o desarrollo de aplicaciones.
6. Porcentaje de ataques informáticos recibidos en la entidad que impidieron la prestación de alguno de sus servicios.

Opinión UAI: La formalización del esquema de indicadores de gestión de un área satisface requisitos normativos y exhibe los estándares de control y mejora continua de la misma.

Recomendación: Incorporar formalmente indicadores de desempeño y métricas para monitorear la gestión del Área de Seguridad de la Información, del mismo modo que lo actuado con otras áreas del ente.

Seguimiento de Observaciones del Informe de Auditoría N° 18/2018

En relación a las observaciones pendientes de regularización del Informe de Auditoría *I.A. N° 18/2018, Tema:* Evaluación de la Seguridad de la Información, cabe destacar que las siguientes observaciones fueron **regularizadas** en el Comité de Control N° 25 del 21 de noviembre de 2018:

- *I.A. N° 18/2018 - Observación 2.3.a : Evaluación y Tratamiento de Riesgos*
- *I.A. N° 18/2018 - Observación 2.3.b: Organización de la Seguridad de la Información.*
- *I.A. N° 18/2018 - Observación 2.3.d: Gestión de Activos de Información.*
- *I.A. N° 18/2018 - Observación 2.3.f: Servicios de procesamiento y/o soporte de terceros.*
- *I.A. N° 18/2018 - Observación 2.3.i: Cumplimiento de Regulaciones Externas*

Por lo tanto, continúan En trámite las siguientes observaciones:

2.3.e. Seguridad de los Recursos Humanos - *Gestión de accesos: Relacionada a la observación "f-Seguridad de los Recursos Humanos - Gestión de accesos" del I.A. N° 12/2017. No se encontró evidencia de un procedimiento formalizado y actualizado de Gestión y control de accesos referentes al NSIAF.*

2.3. g. Gestión de Operaciones y comunicaciones: *Esta Observación se reitera año tras año a partir del I.A. 13/14, señalándose que estos procedimientos datan de 2014 y se tratan de aspectos o normas ya superados, tales como la entrega de información mediante discos compactos (CD´s), siendo que a la fecha el intercambio de información con las fuerzas se hace mediante GDE. Dado su registro en el SISAC (ex SISIO) se cumple con su formal seguimiento. Relacionada a la observación "i - Gestión de Operaciones y comunicaciones" del I.A. N° 12/2017". Se mantiene la situación enunciada en los I.A. N° 13/14, 15/15 ,13/16 y 12/17. Se constató la existencia de documentos relacionados con la gestión de las operaciones y comunicaciones, que a la fecha se encuentran desactualizados. Se reiteran las recomendaciones realizadas en los informes previos.*

2.3. h. Gestión de Incidentes de Seguridad de Información: *No se encontró evidencia de la realización de un Test de Intrusión Interno, Externo, Web e Ingeniería Social del Instituto. El último Test realizado data de enero de 2014.*

Recomendaciones

Se detallan las recomendaciones respectivas en cada ítem de la observación.

Tratamiento del Informe con el área auditada

Mediante NO-2019-48854543-APN-UAI#IAF de fecha 24/05/2019, esta UAI remitió a la Subgerencia de Tecnologías de la Información y las Comunicaciones, Subgerencia de Métodos Y Seguridad de la Información, Subgerencia de Planeamiento y Mejora Continua, Gerencia de Recursos Humanos y Logística-Subgerencia de Logística y Jefe de Seguridad, una copia del IA Preliminar de la presente revisión. Al respecto, las áreas auditadas remitieron sus respuestas el dial 27/05/2019.

CONCLUSIONES

De los resultados obtenidos se puede concluir que se evidencian acciones y esfuerzos de autoridades y personal orientados a la regularización de observaciones señaladas en Informes anteriores y concluir que el estado del tratamiento de la Seguridad de la Información en el periodo bajo análisis se encuentra en forma razonablemente SATISFACTORIA sujeto al tratamiento y eventual aprobación por parte de las Máximas Autoridades de los avances esbozados por las áreas responsables.

Sin perjuicio de lo enunciado precedentemente, esta UAI queda a disposición del Directorio, del Comité de Seguridad de la Información y de la Dirección Ejecutiva para participar preventiva y proactivamente, a modo de veedora, en las distintas actividades que se desarrollen.

Unidad de Auditoría Interna, 18 de Junio de 2019.-

DE MARCELO L. GARCÍA
AUDITOR INTERNO TITULAR
UNIDAD DE AUDITORÍA INTERNA