

INFORME FINAL UAI-ORSNA N° 15/2024

Unidad de Auditoría Interna

**Organismo Regulador Del Sistema Nacional De Aeropuertos
(ORSNA)**

**“Tecnología de la Información y Políticas de Seguridad de la
Información”**

Diciembre 2024

Contenido

INFORME EJECUTIVO.....	3
INFORME ANALÍTICO.....	4
I. Objeto de Auditoría	4
II. Alcance.....	4
III. Marco Normativo	5
IV. Aclaraciones Previas	6
V. Tareas Realizadas	10
a) Cumplimiento de la Resolución SIGEN N°87/22 - "Normas de Control Interno para Tecnología de la Información - Sector Público Nacional":.....	10
b) Políticas de Seguridad de la Información	14
VI. Conclusión	15

INFORME EJECUTIVO

- **Tipo de Informe:** Gestión.
- **Periodo Auditado:** Ejercicios 2024 (Enero/Noviembre).
- **Objeto de Auditoría:** Verificar el cumplimiento de las “Normas de Control Interno para Tecnología de la Información” del Sector Público Nacional (Resolución SIGEN N°87/22) y la incorporación y cumplimiento de las Políticas de Seguridad de la Información del Organismo.
- **Observaciones:**
 - ✓ Falta de presentación del Plan Estratégico de TI
 - ✓ Falta de independencia del Departamento de Sistemas y Tecnología Informática
 - ✓ Falta de procedimientos y metodologías aprobados formalmente
- **Conclusión**

De acuerdo al análisis realizado sobre el accionar del Departamento de Sistemas y Tecnología Informática, dependiente de la Gerencia de Administración y Presupuesto, respecto a la Resolución SIGEN N°87/2022, esta Unidad ha observado un avance significativo respecto de regularización de las observaciones planteadas en informes anteriores.

No obstante, la falta de un Plan Estratégico impide contar con una herramienta que establezca el rumbo del Organismo en materia de Sistemas y Tecnología de la Información, que debería establecer una serie de acciones tendientes a cumplir con los objetivos allí planteados en base a los lineamientos que establezca oportunamente el Directorio.

Dicho Plan posteriormente debe ser aprobado por el Directorio del ORSNA.

Por otra parte, y en función de sus tareas específicas, el Departamento debería concluir la elaboración de los procedimientos necesarios para el desarrollo de dichas tareas, y elevarlos, para su aprobación, al Directorio del ORSNA, a fin de darle un marco apropiado a la responsabilidad y la importancia que dichos procedimientos tienen en la realización de sus tareas.

INFORME ANALÍTICO

I. Objeto de Auditoría

Verificar el cumplimiento de las "Normas de Control Interno para Tecnología de la Información" del Sector Público Nacional (Resolución SIGEN N°87/22) y la incorporación y cumplimiento de las Políticas de Seguridad de la Información del Organismo.

II. Alcance

Las tareas de auditoria se llevaron a cabo de acuerdo a los criterios establecidos en las Normas de Auditoría Interna Gubernamental contenidos en la Resolución N°152/02, Resolución SGN N°172/14, Normas Generales de Control Interno para el Sector Público Nacional y los conceptos y procedimientos estipulados en el Manual de Control Interno Gubernamental de la SIGEN, Resolución SGN N° 03/11 y normas particulares.

Asimismo, en lo que respecta a la evaluación de riesgos se tuvo en cuenta la metodología aprobada mediante la Resolución SIGEN N°176/18, la cual prevé la elaboración de una Matriz de Exposición, que muestre los niveles de riesgo asociados a cada proceso a partir de la estimación de la combinación de los niveles de Impacto y Probabilidad, y obtener una visión integral de la situación de los distintos procesos del Organismo.

Estimación del Impacto: Como criterio, se asocia el Impacto de cada proceso a su trascendencia o relevancia en el conjunto de actividades llevadas a cabo por la organización.

Estimación de la Probabilidad: el criterio utilizado para determinar la probabilidad de los riesgos considera que ésta se verá directamente afectada por la calidad del control interno. Cuanto menor sea la calidad del control interno, mayor será la probabilidad de ocurrencia del riesgo, entendiendo por tal el incumplimiento de los objetivos planteados para el proceso.

La combinación de los Niveles de Probabilidad e Impacto por Proceso, permite confeccionar la Matriz de Exposición, según el siguiente criterio:

Probabilidad	Impacto			
	1	2	3	4
4	M	C	S	S
3	P	M	C	S
2	P	P	M	C
1	P	P	P	M

Referencias:

S: Significativo
M: Medio

C: Considerable
P: Poco Significativo

De acuerdo a los criterios expuestos se ha elaborado la siguiente matriz de exposición correspondiente al objeto de auditoría del presente informe, y que ha sido incluido en el Plan Anual de Trabajo (PAT) de la Unidad de Auditoría Interna correspondiente al ORSNA:

Matriz de Exposición ORSNA

Probabilidad	Impacto			
	1	2	3	4
4				
3				
2				
1	Tecnología de la Información y Políticas de Seguridad de la Información			

Esta auditoría integra el PAT de la Unidad de Auditoría Interna correspondiente al ORSNA, aprobado por la Sindicatura General de la Nación (SIGEN), para su ejecución en el año 2024, mediante resolución RESOL-2024-25-APN-SIGEN.

Las tareas de campo referidas al análisis y verificación se llevaron a cabo desde el 20 de noviembre al 15 de diciembre del corriente ejercicio.

III. Marco Normativo

- Decisión Administrativa N°641/2021: Requisitos mínimos de Seguridad de la Información para Organismos.
- Disposición DI-2021-7-APN-DNCIB#JGM: Créase en el ámbito de la Dirección Nacional de Ciberseguridad el “Registro de Puntos Focales en Ciberseguridad del Sector Público Nacional”.
- Resolución SIGEN N° 87/2022: Normas de Control Interno para Tecnología de la Información Sector Público Nacional.

- Resolución ORSNA RESFC-2022-39-APN-ORSNA#MTR: Política de Seguridad de la Información del ORSNA.
- Resolución ORSNA RESFC-2023-71-APN-ORSNA#MTR: Políticas Específicas de la Política de Seguridad de la Información.
- Decisión Administrativa N°161/19: Aprueba la estructura organizativa de primer nivel operativo y las aperturas inferiores al primer nivel operativo del ORSNA.
- Resolución ORSNA RESFC-2021-46-APN-ORSNA#MTR: Manual de Descripción de Puestos de Trabajo (IF-2021-44273577-APN-GRRHH#ORSNA).

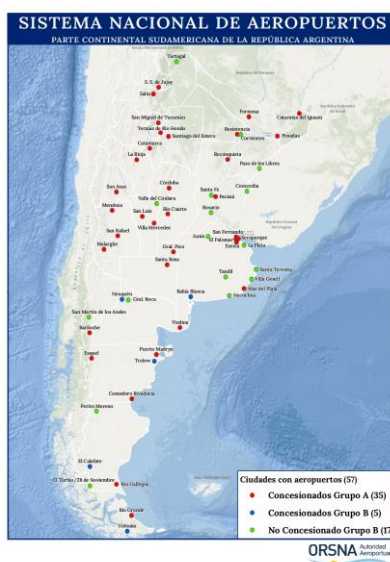
IV. Aclaraciones Previas

El ORSNA es el organismo encargado de regular, controlar y fiscalizar, por sí o en coordinación con otros organismos, los servicios que se prestan en los aeropuertos integrantes del Sistema Nacional de Aeropuertos (SNA), compuesto por 57 aeropuertos, a saber:

- ✓ Grupo A (35 aeropuertos); aquellos otorgados en concesión por el Estado Nacional a Aeropuertos Argentina 2000 S.A. y;
- ✓ Grupo B (22 aeropuertos): compuesto por aeropuertos no concesionados y por aeropuertos concesionados por las provincias.

El mapa a continuación grafica los aeropuertos pertenecientes al Sistema Nacional de Aeropuertos.

Gráfico N° 1: Sistema Nacional Aeroportuario



Cuadro elaborado por la Gerencia de Regulación Económica y Financiera.

El presente informe ha sido elaborado, considerando los aspectos que hacen al óptimo desarrollo de la Tecnología de la Información en el Organismo.

Para ello se han considerado dos aspectos principales:

a) Normas de Control Interno para Tecnología de la Información del Sector Público Nacional:

El 05 de mayo del 2005, mediante la Resolución N°48/05 SGN, la SIGEN aprueba las Normas de Control Interno para Tecnología de la Información del Sector Público Nacional.

Dicha norma es modificada mediante Resolución SIGEN N° 87/2022.

En ella se establecen una serie de temas a evaluar para establecer el grado de control imperante en cada Organización:

- Organización Informática,
- Plan Estratégico de TI,
- Arquitectura de la Información,
- Política de Seguridad y Procedimientos de Gestión de la TI,
- Cumplimiento de Regulaciones Externas,
- Administración de Proyectos,
- Desarrollo, Mantenimiento o Adquisición de Software de Aplicación,
- Adquisición y Mantenimiento de la Infraestructura Tecnológica,
- Servicios de Procesamiento y/o Soporte Prestado por Terceros,
- Publicación de Información Digital
- Monitoreo de Actividades de TI,
- Auditoría Interna de Sistemas.

b) Políticas de Seguridad de la Información:

El 22 de diciembre de 2004, mediante la Decisión Administrativa N° 669/04, se estableció que los organismos del Sector Público Nacional comprendidos en los incisos a) y c) del artículo 8° de la Ley N° 24.156 y sus modificatorias debían dictar o bien adecuar sus políticas de seguridad de la información conforme a la Política de Seguridad Modelo a dictarse dentro del plazo de ciento ochenta días de aprobada dicha Política de Seguridad Modelo.

En ese orden, mediante Disposición N°6/2005 de la Oficina Nacional de Tecnologías de Información (ONTI), se aprobó la "Política de Seguridad de la Información Modelo", la cual sirve como base para la elaboración de las respectivas políticas a dictarse por cada organismo alcanzado por la Decisión Administrativa 669/2004.

A raíz de ello, el 8 de noviembre de 2007, mediante Resolución ORSNA N°51/07, el Organismo aprueba la Política de Seguridad de la Información del ORSNA, la cual será de aplicación a todas las personas físicas y jurídicas, privadas o públicas que presten servicios al o en el Organismo o participen de los procesos de contratación.

El 24 de mayo de 2019, mediante Resolución RESOL-2019-829-APN-SGM#JGM de la Secretaría de Gobierno de Modernización, dependiente de la Jefatura de Gabinete de Ministros, se aprueba la Estrategia Nacional de Ciberseguridad.

En base a ello, el 12 de septiembre de 2019, mediante Resolución RESOL-2019-1523-APN-SGM#JGM la mencionada Secretaría, aprobó la definición de Infraestructuras Críticas y de Infraestructuras Críticas de Información, la enumeración de los criterios de identificación y la determinación de los sectores alcanzados.

Se define entonces:

Las Infraestructuras Críticas: son aquellas que resultan indispensables para el adecuado funcionamiento de los servicios esenciales de la sociedad, la salud, la seguridad, la defensa, el bienestar social, la economía y el funcionamiento efectivo del Estado, cuya destrucción o perturbación, total o parcial, los afecte y/o impacte significativamente.

Las Infraestructuras Críticas de Información: son las tecnologías de información, operación y comunicación, así como la información asociada, que resultan vitales para el funcionamiento o la seguridad de las Infraestructuras Críticas.

SECTORES IDENTIFICADOS

- Energía
- Tecnologías de Información y Comunicaciones
- Transportes
- Hídrico
- Salud
- Alimentación
- Finanzas
- Nuclear
- Químico
- Espacio
- Estado

El 25 de junio de 2021, se dicta la Decisión Administrativa N°641/2021, estableciendo los Requisitos mínimos de Seguridad de la Información para las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156 de Administración Financiera y de los Sistemas de Control del Sector Público Nacional y sus modificatorias y a los proveedores que contraten con esas entidades y jurisdicciones, en todo aquello que se encuentre relacionado con las tareas que realicen y en los términos que establezca cada una de ellas, normativa o contractualmente.

Dichos requisitos son establecidos en base al intenso uso de las Tecnologías de la Información y las Comunicaciones, lo que conlleva asimismo a un notable aumento de los riesgos y amenazas a los activos de información y a los sistemas esenciales utilizados para brindar de manera eficiente y constante los múltiples servicios que desde el Sector Público Nacional se prestan.

Las nuevas formas de ataques informáticos y la actividad maliciosa en general avanzan y se modifican en forma vertiginosa, obligando a mantener actualizadas las herramientas, protocolos y marcos normativos, con el fin de proteger adecuadamente la infraestructura, los activos de información y principalmente los datos personales, que son en definitiva un patrimonio de los ciudadanos en su conjunto.

A continuación, se exponen los aspectos más destacados de la citada norma:

- Se aprueban los Requisitos Mínimos de Seguridad de la Información para los Organismo del Sector Público Nacional.
- Se establece su aplicación a las entidades y jurisdicciones del Sector Público Nacional comprendidas en el inciso a) del artículo 8° de la Ley N° 24.156.
- Los Planes de Seguridad deberán ser aprobados por las entidades y jurisdicciones del Sector Público Nacional en el plazo máximo de noventa días desde la entrada en vigencia de la norma.
- Dichos Planes deberán establecer los plazos en que se dará cumplimiento a cada uno de los "Requisitos Mínimos de Seguridad de la Información"; plazo que no podrá ser posterior al 31 de diciembre de 2022.
- Los Planes de Seguridad deberán ser remitidos a la Dirección Nacional de Ciberseguridad de la Secretaría de Innovación Pública, dependiente de la Jefatura de Gabinete de Ministros, dentro de un plazo máximo de noventa días desde la entrada en vigencia de la presente (Fecha límite 05/11/2021).
- Las máximas autoridades de las entidades y jurisdicciones comprendidas en la citada norma deberán asignar las funciones relativas a la seguridad de sus sistemas de información al área con competencia en la materia e informar, mediante Comunicación Oficial a través del Sistema de Gestión Documental Electrónica (GDE) a la Dirección Nacional de Ciberseguridad, el nombre, apellido y datos de contacto del responsable del área designada, dentro del plazo de sesenta días corridos desde la entrada en vigencia de la presente medida.
- Las entidades y jurisdicciones deberán reportar a la Dirección Nacional de Ciberseguridad los incidentes de seguridad que se produzcan dentro de sus ámbitos, dentro de las cuarenta y ocho horas de tomado conocimiento de su ocurrencia o de su potencial ocurrencia.
- La Dirección de Ciberseguridad verificará el cumplimiento de las disposiciones de la presente medida, sin perjuicio de las competencias asignadas a la Sindicatura General de la Nación.

V. Tareas Realizadas

El presente informe ha sido elaborado, considerando los aspectos que hacen al óptimo desarrollo de la Tecnología de la Información en la Organización:

Para ello se ha procedido a recopilar y analizar los procedimientos y la normativa vigente.

El análisis ha sido realizado, abarcando los dos aspectos más importantes, en relación a la Tecnología de la Información:

- a) Cumplimiento de la Resolución SIGEN N°87/22 - “Normas de Control Interno para Tecnología de la Información - Sector Público Nacional”.**
- b) Políticas y Planes de Seguridad de la Información.**

De las tareas de campo, se desprende lo siguiente:

- a) Cumplimiento de la Resolución SIGEN N°87/22 - “Normas de Control Interno para Tecnología de la Información - Sector Público Nacional”:**

a.1) Organización Informática

- El Departamento de Sistemas y Tecnología Informática tiene asignada la responsabilidad por las actividades de Tecnología de la Información.
- No posee independencia respecto de las áreas usuarias ya que se encuentra en el Organigrama, dependiendo de la Gerencia de Administración y Presupuesto, aunque presta servicios a todos los sectores del ORSNA y sus puestos de trabajo se encuentran detallados en el Manual de Descripción de Puestos de Trabajo (IF-2021-44273577-APN-GRRHH#ORSNA) aprobada por el Directorio del ORSNA el 23 de junio, mediante RESFC-2021-46-APN-ORSNA#MTR.
- A través del mencionado manual, el personal del Departamento de Sistemas y Tecnología Informática se encuentra notificado de sus deberes y responsabilidades.
- Existe una descripción de funciones de cada puesto, pero no existe un control por oposición de intereses respecto de otros puestos dentro del Departamento.
- El Departamento no cuenta con un procedimiento formalmente aprobado, para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios de información ni existe un plan de capacitación informático que abarque a usuarios finales y técnicos.

a.2) Plan Estratégico de TI

- A la fecha del presente Informe, el área de Sistemas no cuenta con un Plan Estratégico para el año 2024 aprobado formalmente, ni existe documentación que acredite la elaboración de un proyecto de Plan Estratégico para ser implementado durante el ejercicio 2025.

a.3) Arquitectura de la Información

- Se encuentra definido el modelo de arquitectura de la información del ORSNA, aunque dicho modelo no se encuentra documentado.
- Existen controles de consistencia, integridad, confidencialidad y validación de los datos.

a.4) Políticas y Procedimientos

- El Organismo dispone de una política de seguridad de la información basada en la Decisión Administrativa N° 641/2021:
 - ✓ Resolución ORSNA RESFC-2022-39-APN-ORSNA#MTR: Política de Seguridad de la Información del ORSNA.
 - ✓ Resolución ORSNA RESFC-2023-71-APN-ORSNA#MTR: Políticas Específicas de la Política de Seguridad de la Información.
- Mediante las políticas específicas, el ORSNA ha aprobado una amplia mayoría de procedimientos, y de acuerdo a las Políticas de Seguridad de la Información aprobadas, se ha comprometido a aprobar los que se relacionan con:
 - ✓ Propiedad y clasificación de la información
 - ✓ Generación de backups y pruebas de recuperación.
 - ✓ Tratamiento ante contingencias y para la continuidad operativa. (Plan de Contingencias)
 - ✓ Gestión de incidentes.

a.5) Cumplimiento de Regulaciones Externas

- Mediante las políticas específicas, el ORSNA ha establecido que todo algoritmo o código fuente desarrollado por el ORSNA o por terceros es de propiedad exclusiva del ORSNA, quedando prohibida su copia parcial, total y distribución de la misma a terceros sin la debida autorización (Capítulo 9.2.9 de las Políticas Específicas de las Políticas de Seguridad de la Información).
- Los convenios o contratos formales con aquellos terceros con los que existan intercambios de información o prestación de servicios relacionados con la TI son revisados periódicamente a fin de asegurar que se mantengan actualizados, solo en lo que corresponde a la Seguridad de la Información

- El Organismo incluye en los pliegos de bases y condiciones particulares cláusulas vinculadas a la Seguridad de la Información, de cumplimiento efectivo y obligatorio por parte de los contratantes. Estas disposiciones consideran los aspectos pertinentes a la protección de la Información y los servicios que se brinden.

a.6) Administración de Proyectos

- El Departamento de Sistemas y Tecnología Informática no posee una metodología de administración de proyectos documentada y aprobada formalmente.

a.7) Desarrollo, Mantenimiento o Adquisición de Software de Aplicación

- El Departamento de Sistemas y Tecnología Informática utiliza procedimientos definidos, para las actividades de desarrollo, mantenimiento o adquisición de sistemas, pero los mismo no se encuentran documentados y aprobados formalmente.

a.8) Adquisición y Mantenimiento de la Infraestructura Tecnológica

- Para la adquisición de bienes y servicios informáticos son tenidos en cuenta los estándares vigentes para la Administración Pública.
- No existe un plan de mantenimiento preventivo del hardware.
- No existen procedimientos documentados y aprobados formalmente, para la gestión de licencias de software.

a.9) Servicios de procesamiento, soporte y/o almacenamiento prestados por terceros

- La decisión de contratar servicios a terceros debe estar debidamente justificada.
- Se establecen contratos formales con los terceros antes de comenzar el trabajo, identificando los objetivos a alcanzar, los niveles de servicio esperados, las obligaciones de las partes y los responsables de las interacciones.
- Actualmente no existe en el ORSNA servicios de procesamientos contratados.

a.10) Publicación de información digital

- La página web del ORSNA se encuentra dentro del Portal oficial del Estado argentino. Argentina.gob.ar.
- El Organismo no ha asignado formalmente las responsabilidades por la publicación de contenidos en la web del ORSNA que se encuentra dentro del portal Argentina.gob.ar.

a.11) Monitoreo de los Procesos

- El Departamento de Sistemas y Tecnología Informática no cuenta con indicadores de desempeño para hacer el seguimiento de la gestión y las excepciones de las actividades de TI, y no presenta informes periódicos de gestión a la dirección de la organización.

OBSERVACION a.1: Falta de presentación del Plan Estratégico de TI

Se reitera lo observado en Informes Anteriores (Último Informe UAI N°13/2023):

La Gerencia de Administración y Presupuesto, a través del Departamento de Sistemas y Tecnología Informática no ha presentado formalmente aún, el Plan Estratégico de TI correspondiente al año 2024 ni existe documentación respecto de un proyecto de Plan Estratégico para el año 2025.

Recomendación:

Resultaría necesario que la Gerencia de Administración y Presupuesto realice las gestiones necesarias para elaborar un Plan Estratégico que considere los requerimientos de todas las áreas de la Organización y, establezca las prioridades correspondientes, basado en el Presupuesto presentado por el Organismo ante la Oficina Nacional de Presupuesto, en lo que corresponde al ejercicio 2025, y durante dicho año establezca una estrategia de trabajo para el ejercicio 2026 a fin de definir un presupuesto que se ajuste a dicha estrategia y que la misma pueda ser plasmada en un Plan aprobado.

Opinión del Auditado:

Departamento de Sistemas y Tecnología Informática: El Informe ha sido puesto a consideración del auditado quien comparte lo manifestado en el mismo.

OBSERVACION a.2: Falta de independencia del Departamento de Sistemas y Tecnología Informática

Se reitera lo manifestado en Informes Anteriores (informe UAI N°13/2023):

El Departamento de Sistemas y Tecnología Informática tiene asignada la responsabilidad por las actividades de Tecnología de la Información, sin embargo, al depender de la Gerencia de Administración y Presupuesto no posee independencia respecto de las áreas usuarias, siendo una de ellas, precisamente la Gerencia de Administración y Presupuesto.

Dicha falta de independencia se evidencia no solo respecto de la autoridad jerárquica, ya que depende de una gerencia con misiones y funciones diversas, sino que queda de manifiesto ante la falta de decisión presupuestaria, ya que el departamento depende del área que tiene a su cargo la ejecución de los fondos presupuestarios del ORSNA, por encima de las necesidades del Departamento de Sistemas, lo que provoca un conflicto por oposición de intereses entre la Gerencia y el Departamento.

Recomendación:

El Departamento de Sistemas y tecnología Informática, debería depender del Directorio del ORSNA, recuperando así la independencia suficiente que le permita establecer de manera correcta las políticas a implementar respecto de la tecnología de la información del ORSNA, según lo establecido por SIGEN en su Resolución N° 87/2022.

Opinión del Auditado:

Departamento de Sistemas y Tecnología Informática: El Informe ha sido puesto a consideración del auditado quien comparte lo manifestado en el mismo.

OBSERVACION a.3: Falta de procedimientos y metodologías aprobados formalmente

Se reitera lo manifestado en Informes Anteriores (informe UAI N°13/2023):

El Departamento de Sistemas cuenta y utiliza procedimientos y metodologías para la realización sus tareas, muchos de los cuales han sido incorporados formalmente en las Políticas Específicas de la Política de Seguridad de la Información, no obstante ello, se han identificado procedimientos que aún no han sido elaborados y procedimientos que, aunque se encuentran elaborados, aún no han sido aprobados.

Recomendación:

El Departamento de Sistemas, debido a la cantidad y diversidad de procedimientos internos que realiza, debería elaborar, sobre la base de los procedimientos aprobados y los procedimientos que aún resta aprobar, un manual en el que se vuelquen todos los procedimientos utilizados.

Opinión del Auditado:

Departamento de Sistemas y Tecnología Informática: El Informe ha sido puesto a consideración del auditado quien comparte lo manifestado en el mismo.

b) Políticas de Seguridad de la Información

Cumplimiento de la Decisión Administrativa N°641/2021

El 11/05/2022, mediante Acta de Directorio N°5/2022, el Directorio del ORSNA resuelve aprobar la “Política de Seguridad de la Información del ORSNA, dejando sin efecto la Resolución ORSNA N°51/2007, que contenía la anterior Política de Seguridad de la Información, a fin de cumplir con los requerimientos establecidos en la Decisión Administrativa N° 641/2021 y en base al “Modelo Referencial de Política de Seguridad de la Información” aprobado por la Disposición N° 1/2022 de la Dirección Nacional de Ciberseguridad.

Lo resuelto mediante Acta de Directorio, es ratificado por la Resolución ORSNA RESFC-2022-39-APN-ORSNA#MTR de fecha 12/05/2022.

El 17/10/2023, con el objetivo de desarrollar y profundizar los lineamientos de la seguridad de la información, el Directorio del ORSNA resuelve aprobar las “Políticas Específicas de la Política de Seguridad de la Información del ORSNA, mediante Acta de Directorio N°8/2023, ratificada el 18/10/2023, mediante Resolución ORSNA RESFC-2023-71-APN-ORSNA#MTR.

De acuerdo al análisis realizado de las Políticas Específicas de la Política de Seguridad de la Información del ORSNA, en base a lo establecido en la Resolución SIGEN N°87/22 - “Normas de Control Interno para Tecnología de la Información - Sector Público Nacional, se desprende que aún queda pendientes de realización algunos procedimientos mencionados en dichas políticas, encontrándose los mismos en elaboración.

VI. Conclusión

De acuerdo al análisis realizado sobre el accionar del Departamento de Sistemas y Tecnología Informática, dependiente de la Gerencia de Administración y Presupuesto, respecto a la Resolución SIGEN N°87/2022, esta Unidad ha observado un avance significativo respecto de regularización de las observaciones planteadas en informes anteriores.

No obstante, la falta de un Plan Estratégico impide contar con una herramienta que establezca el rumbo del Organismo en materia de Sistemas y Tecnología de la Información, que debería establecer una serie de acciones tendientes a cumplir con los objetivos allí planteados en base a los lineamientos que establezca oportunamente el Directorio.

Dicho Plan posteriormente debe ser aprobado por el Directorio del ORSNA.

Por otra parte, y en función de sus tareas específicas, el Departamento debería concluir la elaboración de los procedimientos necesarios para el desarrollo de dichas tareas, y elevarlos, para su aprobación, al Directorio del ORSNA, a fin de darle un marco apropiado a la responsabilidad y la importancia que dichos procedimientos tienen en la realización de sus tareas.

Ciudad Autónoma de Buenos Aires 30 de diciembre de 2024.

Cdor. Gabriel V. Rossi
Auditor Interno Titular

Organismo Regulador del Sistema Nacional de Aeropuertos

EQUIPO DE TRABAJO

- Dra. CASTRO, María del Huerto.
- Lic. FERRARA, Marcela.
- Cdor. POGGI, Darío.
- Arq. FANTINELLI Juan Manuel

