Tecnología de la Información y la Comunicación

INFORME UAI Nº 16/2022

25 de Noviembre de 2022

UNIDAD DE AUDITORÍA INTERNA

TABLA DE CONTENIDOS O INDICE

Detalle	Folio
Informe Ejecutivo	2
Informe Analítico	3 a 6
Objeto	3
Alcance de la tarea	3
Limitaciones al alcance	3
Tarea realizada	3
Marco de Referencia	5
Circuito, Temas y Aspectos aud.	5
Observaciones	5
Recomendaciones	5
Opinión del auditado	6
Conclusión	6

Ministerio de Obras Públicas
Secretaría de Infraestructura
y Política Hídrica
Instituto Nacional del Agua

INFORME DE AUDITORÍA N°16 /2022
INFORME EJECUTIVO
Título: Tecnología de la Información y la Comunicación

I. Síntesis

Se realizó un relevamiento integral en materia de Tecnología de la Información y Comunicación, desarrolladas en el Instituto, considerando las pautas establecidas por la Resolución N° 87/2022 de SIGEN,

II. Observaciones

1. surge la necesidad de adecuar algunas cuestiones que resultan de vital importancia a fin de contar con procedimientos que permitan mejorar el Sistema de Control Interno existente, todo ello a la luz de lo establecido en la Resolución N° 87/2022 SIGEN.

III. Recomendaciones

1. Adecuar las actividades actualmente desarrolladas a la luz de las sugerencias expuestas en el Informe de Auditoría, comenzando con la elaboración de un Plan Estratégico Informático que evalúe el accionar con miras a regularizar las cuestiones observadas.

IV. Conclusión

Teniendo en cuenta lo expuesto precedentemente se puede concluir que resulta de importancia la readecuación de actividades, a la luz de las sugerencias expuestas en el Instructivo de la Resolución N° 87/2022 SGN. En el mismo se exponen las cuestiones que no se cumplen y los riesgos inherentes a que está expuesto la falta de acción sobre la misma.

Ezeiza, 25 de Noviembre de 2022

FRASER Daniel Osvaldo

Firmado digitalmente por FRASER Daniel Osvaldo
Fecha: 2022.11.25 09:46:49 -03'00'

Ministerio de Obras Públicas
Secretaría de Infraestructura
y Política Hídrica
Instituto Nacional del Agua

INFORME DE AUDITORÍA N° 16-2022

Título: TIC Tecnología de la Información y la Comunicación

I. Objeto de la Auditoría

Efectuar un análisis a la luz de la Resolución48/2005 SIGEN, modificada por la Resolución 87/2022, respecto a las actividades en materia de Tecnología de la Información y Comunicación, desarrolladas en el Instituto

II. Alcance

Las tareas de auditoría realizadas tuvieron como base las Normas de Auditoría Gubernamental, aprobados por Resolución N° 152 SGN, los lineamientos impartidos por la Sindicatura General de la Nación y lo planificado en nuestro Plan de Auditoría para el corriente ejercicio.

III. Limitaciones al Alcance

La labor de auditoría fue realizada teniendo en cuenta los lineamientos de la Resolución 87/2022, donde en su punto 12.1 determina que las Unidades de Auditoría Interna definidas en la Ley 24156, deben ejecutar auditorías de sistemas con una periodicidad acorde al nivel de informatización organizacional, debiendo reunir los responsables de llevarlas a cabo, los requisitos de competencia técnica, independencia y autoridad para efectuar revisiones objetivas de los controles informáticos y preparar informes sobre sus hallazgos y recomendaciones.
A tal fin y atento que en la UAI no hay personal calificado, se procedió a contratar a un Ingeniero en Informática, quien procedió a suscribir un Informe circunstanciado, así como también confeccionar el Anexo I de la Resolución 87/2022.

IV. Tarea realizada

La labor de auditoría se llevó a cabo en los meses de Octubre y Noviembre, habiendo insumido un total de 70 horas en su elaboración.

El Profesional en Informática contratado para la realización de la auditoría, efectuó un relevamiento de las actividades desarrolladas en el Instituto, habiendo tenido reuniones con el personal del Área Informática y de esta Unidad de Auditoría Interna.

Como resultado de su tarea emitió un Informe Ejecutivo donde vuelca sus resultados, un Cuadro resumen indicando los hallazgos no cumplidos de la Resolución 87/2022, sus Conclusiones y cumplimentado el Anexo 1 de la Resolución.

Los hallazgos verificados requieren de un accionar conjunto entre la Presidencia del Instituto, algunos de ellos, y por parte del Área de Informática otros, razón por la cual se considera de suma importancia efectuar un plan de acción con miras a implementar las sugerencias esgrimidas en el Informe de Auditoría.

Dichos hallazgos se pueden resumir:

1. Necesidad de dependencia de la Unidad Informática con la Presidencia
2. La UI no posee implementado un Diccionario de datos
3. Operaciones en nuevos niveles de monitoreo y controles remotos
4. Importancia de la intervención de la Unidad Informática en los procesos que se llevan a cabo en el Instituto en las distintas áreas
5. Intervención de la Unidad Informática en lo concerniente a adquisición, desarrollo e implementación que involucren las TIC, software, seguridad.
6. No se tiene implementado controles tendientes a cumplimentar regulaciones relativas a privacidad de información, propiedad intelectual de software.

Actualmente el área de Informática depende de la Subgerencia de Administración, pero se encuentra directamente desarrollando actividades con la Gerencia de Programas y Proyectos.

La estructura actual del área es reducida, por lo que poder llevar a cabo la adaptación de los hallazgos detectados, requiere de un proceso y un análisis integral de acciones, partiendo de la elaboración de un Plan Estratégico Informático, la determinación de necesidades de Recursos Humanos e infraestructura física, a la luz de las distintas actividades desarrolladas en el Instituto.

La implementación de las Recomendaciones sugeridas en el Informe de Auditoría deberían ser aplicadas a todas las áreas operativas y de apoyo del Instituto, considerando asimismo la importancia de contar con una política de seguridad de la información que garantice la no vulnerabilidad de todas las actividades desarrolladas.

V. Marco de referencia

La normativa principal aplicada es:

- Ley 24156 Ley de Administración Financiera y de los Sistemas de Control del Sector Público Nacional.
- Resolución SIGEN N° 87/2022

VI. Circuitos, Temas y Aspectos Auditados

Se analizó el circuito existente relacionado con las actividades de Tecnología de la Información, interactuando entre la Unidad Informática y los Sectores que llevan a cabo tareas sustantivas y de apoyo.
Se confección el Anexo I de la Resolución N° 87/2022 SIGEN "Normas de Control Interno para Tecnología de la Información".

VII. Observaciones

1. Del análisis de cuestiones relacionadas con las Normas de Control Interno para Tecnología de la Información – Sector Público Nacional, aprobadas por la Resolución N° 87/2022 de la SIGEN, surge la necesidad de adecuar algunas cuestiones que resultan de vital importancia a fin de contar con procedimientos que permitan mejorar el Sistema de Control Interno existente.

VIII. Recomendaciones

1. Adecuar las actividades actualmente desarrolladas a la luz de las sugerencias expuestas, comenzando con la elaboración de un Plan Estratégico Informático que evalúe el accionar con miras a regularizar las cuestiones observadas.

Ezeiza, 16 de Noviembre de 2022

FRASER Daniel Osvaldo

Firmado digitalmente por FRASER Daniel Osvaldo
Fecha: 2022.11.25 09:47:19 -03'00'

Ministerio de Obras Públicas
Secretaría de Infraestructura
y Política Hídrica
Instituto Nacional del Agua

INFORME DE AUDITORÍA N°15/2022

Título: TIC Tecnología de la Información y la Comunicación

I. Opinión del Auditado

Con fecha 23 de Noviembre se recibió la NO-2022-126497176-APN-GPYP#INA, donde la Unidad Informática coincide con lo manifestado. Asimismo informa que mediante GDE NO-2022-126425912-AAPN-GPYP#INA fue presentado el "Plan Estratégico Informático 2022-2025" que por error involuntario se omitió su envío en una fecha más temprana.

I. Conclusión

Teniendo en cuenta lo expuesto precedentemente se puede concluir que resulta de importancia la readecuación de actividades, a la luz de las sugerencias expuestas en el Instructivo de la Resolución N° 87/2022 SGN. En el mismo se exponen las cuestiones que no se cumplen y los riesgos inherentes a que está expuesto la falta de acción sobre la misma.
De vital importancia para contar con un adecuado Sistema de Control Interno, es la adopción de un plan de trabajo que contemple las distintas etapas y un seguimiento de acciones tendientes a su regularización.

Ezeiza, 25 de Noviembre de 2022

FRASER Daniel Osvaldo

Firmado digitalmente por FRASER Daniel Osvaldo
Fecha: 2022.11.25 09:47:33 -03'00'

INA
Instituto Nacional del Agua

INFORME DE AUDITORÍA

Realizado por: Ingeniero JUAN JOSÉ BENÍTEZ

Al INSTITUTO NACIONAL DEL AGUA.

De la Resolución 87/21 de la SIGEN y de la Política de Seguridad de La Información y Procedimientos de Backup

Inicio 04 de octubre de 2022
Fin 30 de octubre de 2022

Notificación

El presente documento es para el uso del Instituto Nacional del Agua (en adelante "INA") al que está dirigido.

Control de versiones	
Cliente	Instituto Nacional del Agua (INA)
Proyecto	Seguridad de la Información
Título	Cumplimiento de la: • Resolución87/21de la SIGEN NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN 2021 • LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROCEDIMIENTOS DE BACKUP
Versión	1.0
Autor	Ing. Juan José Benítez
Fecha de Entrega	20 de octubre de 2022

Lista de Distribución	
INA Auditoría	Auditor del INA
Auditor,	Ing. Juan José Benítez
INA Unidad Informática.	UI

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

25 de octubre de 2022

INSTITUTO NACIONAL DEL AGUA

Au. Ezeiza–Cañuelas, tramo Jorge Newbery Km 1,620, B1804 Ezeiza, Ciudad Autónoma de Buenos Aires

Informe de la auditoria de IT "Cumplimiento de la Resolución87/22 de la SIGEN" realizada entre el 04 y el 20 de octubre de 2022. Este informe incluye las conclusiones arribadas, las propuestas de mejoras con una descripción de cómo se realizó el trabajo.

JUAN JOSE BENITEZ
INGENIERO

ÍNDICE

Tabla de contenido

1 INTRODUCCIÓN 4
1.1 DESCRIPCIÓN DEL NEGOCIO 4
1.2 BREVE EXPLICACIÓN DE LA ESTRUCUTRA TI 4
1.3 OBJETIVO DE LA AUDITORÍA 4
1.4 ALCANCE DE LAS TAREAS 4
1.5 AREAS PARTICIPANTES 4
1.6 AGENDA DEL TRABAJO 4
2 RESUMEN EJECUTIVO. 5
2.1 CUADRO RESUMEN DE LOS HALLAZGOS NO CUMPLIDOS RESOLUCION 87/21 6
2.2 CUADRO RESUMEN DE HALLAZGOS NO CUMPLIDOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROCEDIMIENTOS DE BACKUP 8
3 CONCLUSIONES 11
..... 11

Índice Tabla e Ilustraciones

Ilustración 1 Tabla Resumen Resultados por Cláusulas 6
Ilustración 2 Cumplimientos por Cláusulas 7
Ilustración 3 Relación Cumplimiento 7
Ilustración 4 Total Cumplimientos 8

1 INTRODUCCIÓN

1.1 DESCRIPCIÓN DEL NEGOCIO

El Instituto Nacional del Agua es un organismo científico tecnológico descentralizado que tiene por objetivo satisfacer los requerimientos de estudio, investigación, desarrollo y prestación de servicios especializados en el campo del aprovechamiento y preservación del agua. Depende de la Secretaría de Infraestructura y Política Hídrica de la Nación, perteneciente al Ministerio del Interior, Obras Públicas y Viviendas del de la República Argentina.

1.2 BREVE EXPLICACIÓN DE LA ESTRUCUTRA TI

La estructura TI que dispone el INA cuenta como Jefa a la Sra. Andrea Viviana Rodríguez y consta de un equipo de cuatro personas para tareas técnicas. Este equipo de gente le permiten llevar adelante las operaciones de TIC que comprenden la ejecución de tareas técnicas propias de la operatoria diaria, además de cumplir con responsabilidades en aspectos de gestión, planeamiento, presupuesto, etc.

1.3 OBJETIVO DE LA AUDITORÍA

Realizar un análisis de las disponibilidad de planes, documentados y aprobados, para los proyectos que involucren actividades y servicios informáticos, evaluados a la luz de la Resolución 87/21 de la SIGEN.

1.4 ALCANCE DE LAS TAREAS

Las tareas de auditoría se llevaron a cabo sobre la Unidad Informática exclusivamente.

1.5 AREAS PARTICIPANTES

Unidad de Auditoría Interna (UAI)

Unidad Informática (UI)

Gerencia de Programas y Proyectos (GPP)

Ing. JUAN JOSÉ BENITEZ
Perito Forense
TEC Nº I-6668

1.6 AGENDA DEL TRABAJO

Actividades

- Reunión previa con las autoridades que solicitaron la auditoría externa.
- Reunión con el equipo de trabajo de la UI del INA
- Primer control en base a la "lista de control" de la Resolución 87/21 de la SIGEN.
- Reuniones de trabajo sobre los puntos a ser controlados.
- Reunión con la UI para ver las conclusiones surgidas.
- Elevación del informa a la Unidad de Auditoría Interna.

Ing. JUAN JOSE BENITEZ
Perito Forense
COPITEC Nº I-6663

2 RESUMEN EJECUTIVO.

Actualmente toda organización se encuentra expuesta a amenazas que atentan contra la seguridad de su información y la continuidad de sus servicios. En este contexto el INA, cuyas operaciones hacen un uso intensivo de las tecnologías de información y comunicaciones (TIC), no está exento de los riesgos señalados.

Es necesario detectar la posible coexistencia de amenazas y vulnerabilidades para reducir la materialización de acciones que pongan en peligro a las operaciones y la información del Instituto.

El nivel de riesgos estimado para los diferentes dominios de seguridad analizados hace necesario el cumplimiento de la estrategia sustentable de gestión de riesgos de seguridad en base a conceptos fundamentales tales como CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD de la información y de los diferentes servicios y activos relacionados, de tal manera que los niveles finales de riesgo operativo puedan manejarse y mantenerse acotados a valores aceptables.

A continuación se grafican los ítems evaluados consignando el cumplimiento, no cumplimiento o cumplimiento parcial de las mismas. Vale aclarar que de los 16 puntos indicados como "no cumple" sólo en dos controles es responsabilidad de la Unidad Informática *(ver 2.1 Cuadro resumen de los hallazgos no cumplidos, página 8).*

Ilustración 1 Tabla Resumen Resultados por Cláusulas

Nro	Cláusula	Cumple	No Cumple	Cumple Parcial	N/A
1	Organización Informática	8	1	1	1
2	Plan Estratégico de TI	11	0	3	0
3	Arquitectura de la Información	0	1	2	0
4	Políticas y Procedimientos	16	2	2	0
5	Cumplimiento y Regulaciones	0	1	1	0
6	Administración de Proyectos	0	8	0	0
7	Administración y Adquisición de Software y Aplicación	18	1	2	0
8	Adquisición y Mantenimiento de Infraestructura Tecnológica	7	1	0	0
9	Serv de Proc y/o Sop de Terceros	6	0	1	1
10	Publicación Info Digital	2	0	0	0
11	Monitoreo Activos TI	0	1	1	0
12	Auditoría Interna	2	0	0	0
	Total cumplimiento Resolución 87	70	16	13	2

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

Ilustración 2 Cumplimientos por Cláusulas

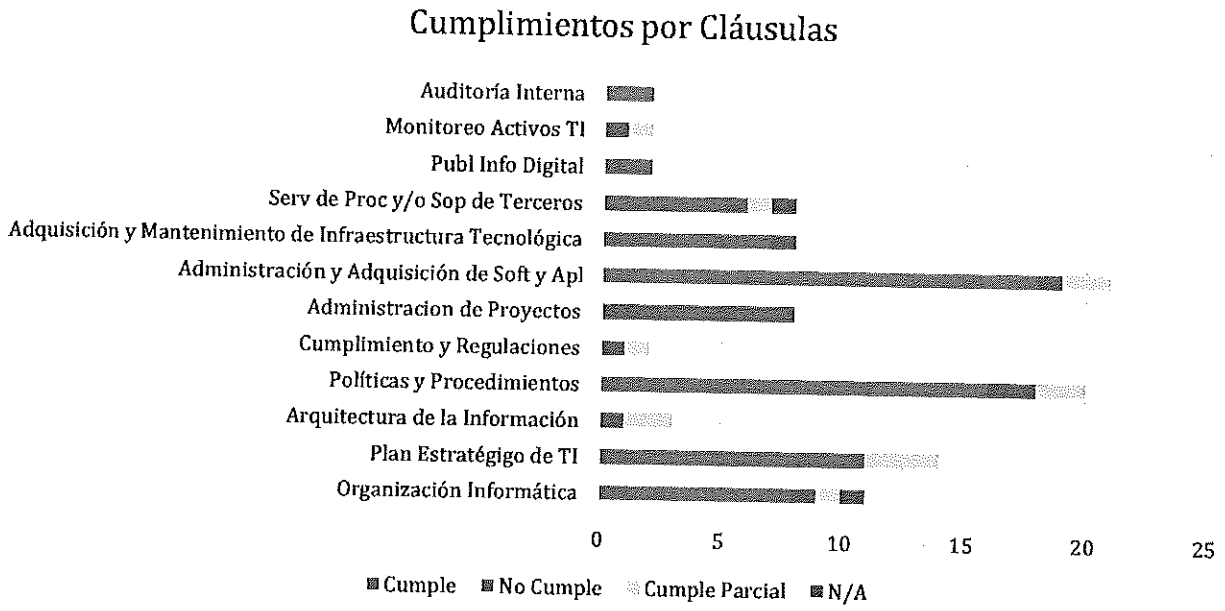
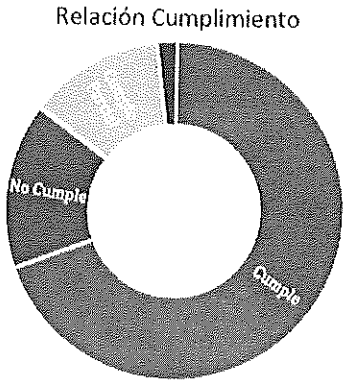


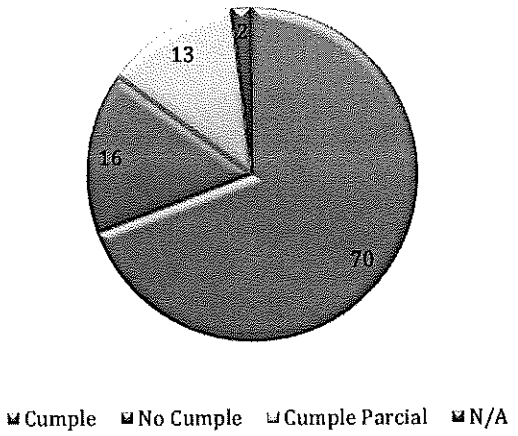
Ilustración 3 Relación Cumplimiento



Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-6668

Ilustración 4 Total Cumplimientos

Total cumplimiento Resolución 87



2.1 CUADRO RESUMEN DE LOS HALLAZGOS NO CUMPLIDOS RESOLUCION 87/21

	Interrogante	Hallazgo	Riesgo	Plan de Acción	Área Responsable
1.2	La unidad de TI ¿se encuentra ubicada dentro de la estructura orgánica de modo de poseer independencia respecto de las áreas usuarias?	Depende de la subgerencia de administración pero la línea de mando es el Gerente de Programas y Proyectos GPP	'• Administración de prioridades no alineada con las necesidades y estrategia organizacional. • Atención "preferencial" del área de TI a la gerencia usuaria de la cual depende.	Generar el cambio de la dependencia y en el Organigrama de la organización.	Presidencia
3.1	¿Está documentado el modelo de arquitectura de la información mediante un diccionario de datos corporativo? ¿Se encuentra actualizado?	No posee implementado el INA un diccionario de datos	'• Datos inconsistentes, redundantes, no accesibles, etc. por un erróneo diseño de las bases de datos. • Información pobre para la toma de decisiones. • Mayores costos y dificultades para el mantenimiento de sistemas y bases de datos o archivos de información.	Debe desarrollarse el Diccionario de Datos de uso general, que abarque al INA en su totalidad.	UI
4.2	Propiedad y clasificación de la información	No posee. Tarea a desarrollar por el comité de	• Falta de aplicación de procedimientos y controles uniformes.	Urgente la información debe ser clasificada en	Comité de la Información

Ing. JUAN JOSÉ DEN[illegible]
Perito Forens[illegible]
COPITEC Nº 1-06[illegible]

		Seguridad de la Información.	• Dificultades para delimitar responsabilidades y exigir rendiciones de cuentas. • Dependencia de determinado personal. Desconocimiento de la operatoria por parte del personal. • Dificultades para capacitar nuevo personal. • Uso ineficiente de tiempo y recursos. • Errores o fallas en las actividades por la transmisión oral de las prácticas de trabajo. • Por la informalidad, se presentan dificultades para comprobar si se ejecutaron o no tareas o controles dentro del proceso. • Dificultades para encarar mejoras en los procesos (ya que no se cuenta con un esquema claro del cual partir).	base a su criticidad y ser tratada en consecuencia	
	Administración de proyectos informáticos	La UI debe conocer sobre los proyectos informáticos en curso		Los proyectos en donde intervienen las TIC debe intervenir la UI para asegurar la interoperabilidad y niveles de seguridad exigidos, de los mismos	Presidencia
5.1	¿Se han implementado controles suficientes tendientes a asegurar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software, seguridad y otras normas que fueran aplicables?	No se encuentran son las misiones y funciones asignadas a la UI. Debe ser resuelto quien lo hace	• Litigios, juicios, sanciones o sumarios por incumplimiento de normativa. • Perjuicio económico para la organización. • Uso ineficiente de los recursos públicos.	Este punto no está determinado en la Política de Seguridad de la información y debe ser considerado para determinar quién es el responsable de este control.	Presidencia
6	La unidad de TI debe disponer de una metodología de administración de proyectos que se aplique en todos los proyectos informáticos encarados.	Hay proyectos que se realizan y materializan sin la intervención ni conocimiento de la UI.	• Cada proyecto informático se gestiona de acuerdo a la capacidad del responsable, sin requisitos mínimos unificados Resultados inciertos en cada caso. • Responsabilidades no claras para las tareas dentro del proyecto. • Se encaran proyectos no autorizados o sin presupuesto.	Es crítico la intervención de una elemento de la INA, que podrá ser la UI para tener un conocimiento de los proyectos en todo su ciclo de vida y poder asesorar en aspecto de compatibilidad, seguridad, interoperabilidad , etc. para	Presidencia

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

			• Las recomendaciones de la UAI llegan una vez finalizado el proyecto (por no haber participado desde etapas tempranas). • Proyectos informáticos que no son aprovechados por todas las áreas involucradas. • • Insuficiente planificación para los proyectos.	garantizar su calidad	
7.1.5	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla la participación de la unidad de auditoría durante el desarrollo?	Al igual que en los proyectos debe intervenir la UI en este punto	• Se desarrollan sistemas que no incorporan controles suficientes, o bien no contemplan requerimientos del área de Auditoría como registros de transacciones o logs, alertas automáticas, etc. • Las recomendaciones de la Auditoría Interna llegan con el sistema en funcionamiento, y obligan a reformular y modificar el sistema.	Ídem punto 6	Presidencia
8.4	¿Existen procedimientos documentados para la gestión de licencias de software?	No y debe ser elaborada	Litigios, reclamos económicos, conflictos con terceros. Instalación y/o utilización de software no autorizado y/o que no responde a los objetivos organizacionales (software de oficina sin licencia, software para otros fines como juegos, etc.). Esto acarrea riesgos de virus informáticos o la inclusión de debilidades en la seguridad informática. Dificultades para planificar actualizaciones de productos de software. Sanciones y/o inconvenientes por incumplimiento de normas aplicables. • Dificultades para obtener el inventario de licencias de software adquiridas por la Organización, y para su adecuado registro patrimonial y contable.	El asesoramiento y determinación de este punto debe pasar por la UI para tener un conocimiento y control de las licencias de software que se adquieren	Presidencia

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

11.2	La unidad de TI ¿presenta informes periódicos de gestión a la dirección de la organización?	Ya lo regularice y esta presentado por GDE el Plan Informático Anual 2022 No lo está haciendo	• Inadecuada gestión de prioridades para los proyectos informáticos • Mayores costos o plazos respecto a lo previsto. • Descoordinación entre las actividades informáticas y la estrategia organizacional. • Dificultades para detectar y corregir desvíos en la ejecución de proyectos informáticos.	Debe implementar un mecanismo para informar a su cadena de mando los informes de su gestión	UI

2.2 CUADRO RESUMEN DE HALLAZGOS NO CUMPLIDOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y PROCEDIMIENTOS DE BACKUP

[illegible]	[illegible]			[illegible]
	[illegible]	[illegible]	[illegible]	
[illegible]				
2.1. ¿Se realizan backups periódicos de los datos, programas y configuración?	X			
2.2. ¿Existe un procedimiento documentado para la realización de backups?			X	
2.2.1. El procedimiento ¿se basa en un análisis documentado en que se hayan definido los datos y sistemas críticos y su prioridad de recuperación?			X	En proceso del armado del proceso documentado
2.2.2. El procedimiento documentado ¿se encuentra aprobado formalmente?		X		
2.2.3. ¿Indica claramente los roles y responsabilidades de los equipos de trabajos encargados?		X		Se contempla en el armado del documento final
2.2.4. ¿Especifica los registros que se deben mantener sobre la realización de tareas y controles del procedimiento?		X		Se contempla en el armado del documento final
2.2.5. De lo que surge en registros ¿Se aplica en la práctica?		X		Se contempla en el armado del documento final

Existe una Política de Seguridad y procedimientos de Backup ya implementados por el INA. A fin de dar cumplimiento a lo exigido en este documento y requerido en la auditoría es que se ajustarán los mismo y se elaborará la documentación faltantes.

3 CONCLUSIONES

En un mundo cada vez más interconectado, con sobrecarga de información y mayores niveles de exigencias en la aplicación de modelos de generación de valor, las empresas acuden a los referentes tecnológicos para apalancar las mismos y optimizar las utilidades con disminución de costos. Esta tendencia a maximizar las utilidades con mayor eficiencia

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

tecnológica, requiere niveles de inversión altos en operaciones integradas, simplificadas y alineadas con las demandas del mercado, su rápida reacción frente a las oportunidades y una alta sensibilidad al cambio.

El Instituto Nacional del Agua, empresa informáticamente integrada, es conveniente que sistematice digitalmente sus procesos internos a fin de ser más eficiente en su funcionamiento.

En este contexto abierto e interconectado la información se ve expuesta a múltiples amenazas y escenarios vulnerables, lo que requiere una revisión y atención permanente y de detalle ya que se transforma en un activo sensible y crítico que puede llegar a comprometer a la empresa.

Los hallazgos críticos pueden ser resumidos en:

- La necesidad de la dependencia de la UI a la Presidencia del INA y no a una Gerencia.
- Las operaciones que deba llevar a cabo el INA estarán cada vez más apalancadas en nuevos sistemas de monitoreo y controles remotos, que se suma a una cada vez mayor espectro de operaciones integradas donde las redes de datos y comunicaciones son parte inherente de la cadena de suministro de un negocio de alto riesgo y mucha coordinación.
- Los sistemas de supervisión y control remoto con el uso de sensores distribuidos en el país que se encuentran en proceso de implementación y que serán procesados en la red del INA, el emplazamientos de radares meteorológicos e hidrológicos hace que haya aplicaciones operativos críticas que están comunicadas y se alimentan desde el exterior, es importante que intervenga la UI en estos procesos y que el INA prevea tener un equipo en capacidad de monitorear los eventos y conformar un equipo de respuesta ante los posibles incidente que pueda suceder.
- Se debe trabajar para que en forma gradual y con los recursos humanos necesarios la UI, dependa directamente y la vez asesore a la Presidencia del INA, en todo lo concerniente a los proyectos de adquisición, desarrollo e implementaciones que involucren las TICs, software y aspectos de Seguridad Informática, en todo el ámbito de responsabilidad del Organismo, con el objetivo de brindar una adecuada visión de los mismos, que se encuentren encuadrados dentro de las buenas prácticas y cumplan, como base, con las normas de la

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

Administración Pública, a saber: la Resolución 87 de la SIGEN, la Decisión Administrativa 641 de la DGC y las ETAPs[1] de la ONTI.

- De esta manera la Presidencia del INA, por intermedio de la UI, tendrá una visión global, seguridad y una trazabilidad de la situación en temas relativos a interoperabilidad, confidencialidad, integridad y disponibilidad de la información, tanto interna al INA como así también entre los elementos dependientes.
- Respecto a la Política de Seguridad de la Información y procedimientos de Backup que se realizó una auditoria complementaria y faltan ajustar la documentación y parte de los procedimientos a lo que se establece en la documentación.

JUAN JOSE BENITEZ
Ingeniero

[1] Estándares Tecnológicos de la Administración Pública
https://www.argentina.gob.ar/noticias/nueva-version-de-los-etap

Anexo 1 Resolución 87/21 de la SIGEN. NORMAS DE CONTROL INTERNO PARA TECNOLOGÍA DE LA INFORMACIÓN 2021.

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple				Comentarios	Riesgos
1.1	La responsabilidad por las actividades de Tecnología de la Información (TI) de la organización debe recaer en una única unidad (unidad de TI) que asegure la homogeneidad y unicidad de criterios y objetivos en la materia. Ante casos excepcionales en que esto no fuera factible--los que deben estar justificados formalmente por la máxima autoridad de la organización-, debe instrumentarse un Comité de TI o figura similar que se encargue de la coordinación de objetivos y lineamientos para inversiones en TICs, desarrollos, políticas y procedimientos, etc., asegurando que respondan a un criterio unificado.	¿Se ha asignado la responsabilidad por las actividades de Tecnología de la Información (TI) de la organización a una única unidad de TI, o ante casos excepcionales se ha conformado formalmente un comité de Sistemas o figura similar?	X					• Dificultades para la delimitación de incumbencias y la correspondiente rendición de cuentas, lo que permite que los distintos sectores informáticos vean diluidas sus responsabilidades ante la ocurrencia de problemas. • Falta de homogeneidad de criterios, por ejemplo, en la aplicación de métodos o técnicas de desarrollo o en la planificación estratégica de la tecnología de Información. • Compras informáticas de elementos que no contribuyen a una estrategia unificada, no compatibles entre sí, etc. • Duplicación de esfuerzos en tareas informáticas, al existir diversos responsables, distintas áreas realizando tareas similares, o no existir la posibilidad de compartir conocimientos y recursos para el desarrollo de las tareas (módulos desarrollados, productos de software, utilitarios, bases comunes, etc.). • En organizaciones que gestionan información de alta criticidad, si Seguridad de la Información depende de la unidad de TI pueden presentarse riesgos de conflictos de intereses.
	En aquellas organizaciones que manejen importantes volúmenes monetarios y/o gestionen información o infraestructuras de alta criticidad para el Estado Nacional, deberán asignarse las responsabilidades por la Seguridad de la Información a un área independiente de la unidad de TI, constituyendo de ese modo, un mecanismo de control por oposición.	¿Se ha asignado la responsabilidad por la Seguridad de la Información a un área independiente de la unidad de TI?				X	No aplica para la INA	
1.2	La ubicación de la unidad de TI dentro de la estructura orgánica debe garantizar su independencia respecto de las áreas usuarias, asegurando la atención de todos los sectores de la organización.	La unidad de TI ¿se encuentra ubicada dentro de la estructura orgánica de modo de poseer independencia respecto de las áreas usuarias?		X			Depende de la subgerencia de administración pero la linea de mando es el generende de programas y proyectos GPP	• Administración de prioridades no alineada con las necesidades y estrategia organizacional. • Atención "preferencial" del área de TI a la gerencia usuaria de la cual depende.
		¿Se prestan servicios a todos los sectores de la organización?	X					
1.3	Debe existir una descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de TI, la cual debe contemplar tanto la autoridad como la responsabilidad. El personal de TI debe notificarse de sus deberes y responsabilidades. De igual forma, en aquellas organizaciones que cuenten con el área de Seguridad de la Información, deben documentarse y aprobarse los puestos de trabajo, contemplando la autoridad y la responsabilidad, notificando formalmente al personal de sus deberes y responsabilidades.	¿Se posee una descripción documentada y aprobada de los puestos de trabajo que conforman la unidad de TI?	X				Cada pesonal técnico tiene su función documentada	• Dificultades para exigir rendiciones de cuentas. • Dificultades para el planeamiento, la ejecución y el control de las tareas. • Dilución de responsabilidades.
		¿Existe una descripción de la autoridad y responsabilidad de los mismos?	X					
		¿Se encuentra el personal de TI notificado de sus deberes y responsabilidades?	X				Si y documentado	
		¿Se posee una descripción documentada y aprobada de los puestos de trabajo que conforman el área de Seguridad de la Información?			X		No poseemos un área específica de Seguridad de la Información, pero dichas tareas son llevadas a cabo por el personal de la UI	
1.4	La asignación de responsabilidades debe garantizar una adecuada separación de funciones, que fomente el control por oposición de intereses, propiciándose rotaciones periódicas de personal afectado a tareas críticas.	La asignación de responsabilidades efectuada ¿presenta una adecuada separación de funciones fomentando el control por oposición de intereses?	X					• Dificultades para detectar errores por falta de controles por oposición. • Fraude o irregularidades por concentración de funciones. • Dificultades para exigir rendiciones de cuentas.
1.5	En concordancia con el plan estratégico, la dirección de la organización debe establecer y mantener procedimientos para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios de información. Se debe establecer un plan de capacitación para cada grupo de empleados, tanto los usuarios finales como el personal técnico informático. Deben contemplarse medidas de concientización sobre la seguridad informática para todo el personal y para los usuarios de los servicios que brinda el organismo.	¿Existe un procedimiento para identificar y documentar las necesidades de capacitación de todo el personal que utiliza los servicios de información?	X				Anualmente por medio de encuesta y entrevistas se determina la necesidad de capacitación, como base de la actividad a realizar	• Pobre aprovechamiento de recursos informáticos organizacionales. • Falta de capacitación en tecnología por parte del personal (tanto técnicos del área de sistemas como usuarios finales). • Por falta de actualización en materia tecnológica, la organización pierde valor en su capital humano, afectando por consiguiente, su capacidad innovadora y mecanismos para mantener los objetivos y métodos de trabajo acordes con las tecnologías informáticas vigentes.
		¿Existe un plan de capacitación informático que abarque a usuarios finales y técnicos? ¿Incluye medidas de concientización sobre la seguridad informática?	X				Si y documentado. Debe ser aprobado por la GPP	
		Organización Informática	8	1	1	1		

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
CODITEC Nº 1-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple			Comentarios	Riesgos
				No			
2.1	A partir de la definición que realicen las autoridades organizacionales respecto del nivel de soporte tecnológico que se brindará a la gestión de las actividades, la unidad de TI debe elaborar e implementar un **plan informático estratégico, el cual deberá estar alineado con el plan estratégico y el presupuesto de la organización.** Para la elaboración de dicho plan se deben considerar, evaluar y priorizar los requerimientos de todas las áreas de la organización, contemplando por su parte, el análisis pertinente de los riesgos en materia de gestión. Deben considerarse asimismo, los lineamientos estratégicos en materia de TI que se dicten desde el Gobierno Nacional.	¿Se ha elaborado e implementado un plan informático estratégico?	X			Poseemos una Planificación Informatica anual que abarca hasta 2021. Se ha elaborado unPE para el 2022-2025 que debe ser firmado por las autoridades del INA.	▪ Descoordinación entre las acciones del área informática y la estrategia organizacional. ▪ Desequilibrio en el grado de informatización de las áreas: algunos sectores muy tecnificados, otros con escaso nivel de apoyo informático. ▪ Incorrecta administración de prioridades para los proyectos informáticos. ▪ Que se encaren proyectos informáticos no autorizados o que no cuenten con presupuesto. ▪ Que se encaren proyectos informáticos que no responden a la estrategia dispuesta por el Gobierno Nacional.
		¿Se encuentra alineado con el plan estrátegico y el presupuesto de la organización?	X			Plan Estrategico INA 2021-2023	
		¿Se consideran los requerimientos de todas las áreas de la organización? ¿Se contempla análisis de riesgo en materia de gestión y lineamientos estratégicos en materia de TI que se dicten desde el Gobierno Nacional?	X				
2.2	La unidad de TI debe **incluir en el plan informático, consideraciones respecto de la evolución de la infraestructura tecnológica,** contemplando un esquema de actualización orientado a evaluar la conveniencia de incorporar nuevas tecnologías disponibles en el mercado y evitar la obsolescencia tecnológica	¿El Plan contempla un esquema de actualización orientado a evaluar la convivencia de incorporar nuevas tecnologías disponibles en el mercado y evitar la obsolescencia tecnológica?	X			Se realizan relevamientos de la tecnología de manera habitual. Actualmente se licitó la renovación la tecnología LAN en la red GPON en la sede Ezeiza	▪ Retraso de la organización en la capacidad informática, lo que puede redundar en menor prestación de servicios, información de menor calidad para la toma de decisiones, etc. ▪ Obsolescencia del equipamiento tecnológico de la organización.
2.3	El plan informático **debe ser aprobado por la dirección de la organización** considerando, para cada uno de los proyectos involucrados, la razonabilidad de los plazos, beneficios a obtener y costos asociados.	El plan informático de la organización ¿se encuentra aprobado por la dirección?	X				▪ Que se encaren proyectos informáticos no autorizados. ▪ Proyectos informáticos incorrectamente planificados, que no se basan en análisis de costos y beneficios. ▪ Proyectos informáticos no integrales o aislados.
		El plan informático ¿describe para cada uno de los proyectos, los plazos, los beneficios a obtener así como sus costos asociados?			X	Hay sectores del INA que desarrlan proyectos que abarcan las TICs sin poner en conocimiento a la UI	
2.4	El plan informático debe mantenerse **actualizado.**	¿Existe una revisión sistemática que asegure a la organización la actualización permanente del plan informático?			X	En el área de responsabilidad y conocimiento de la UI sí, en otras gerencias y elementos dependientes NO	▪ Pérdida de validez del Plan original (dando lugar a los riesgos enunciados en 2.1). ▪ Dificultades para detectar oportunamente los desvíos en la ejecución del Plan y para requerir rendiciones de cuentas.
2.5	**La unidad de TI debe elaborar un presupuesto asociado a la ejecución del plan informático y el desarrollo de sus actividades,** el cual debe ser evaluado y aprobado por la dirección, e incorporado al presupuesto anual de la organización.	¿Se encuentra elaborado el presupuesto asociado a la ejecución del plan informático?	X				▪ Imposibilidad de llevar a cabo los proyectos informáticos planificados por no disponer de presupuesto.
		¿Está aprobado por la dirección?	X				
		¿Se encuentra incorporado al presupuesto anual de la organización?			X	La disponibilidad del presupuesto esta a cargo de la SGA	
2.6	La dirección de la organización **debe controlar en forma periódica, el grado de avance del plan informático,** a efectos de detectar y evitar desvíos en los plazos, costos y metas previstas	La dirección de la organización ¿supervisa en forma periódica el grado de avance del plan informático?	X				▪ Que la organización no obtenga oportunamente los resultados informáticos planificados. ▪ Mayores costos a los previstos ▪ Dificultades para detectar oportunamente los desvíos en la ejecución del Plan y para requerir rendiciones de cuentas. ▪ Proyectos informáticos que no se finalizan en los plazos previstos, o que no logran los objetivos planificados.
2.7	Las adquisiciones de hardware, software u otros servicios informáticos, deben responder a los proyectos incluidos en el plan informático de la organización. **Las situaciones de excepción deben ser autorizadas** por la dirección de la organización y auditadas por la unidad de auditoría interna.	Las adquisiciones de hardware, software u otros servicios informáticos ¿responden al plan informático de la organización?	X				▪ Que se realicen compras que no contribuyan con los proyectos incluidos en el plan informático aprobado, sino a otro tipo de objetivos que no cuentan con aprobación. ▪ Que se insuma el presupuesto para informática en proyectos sin autorización. ▪ Compras que no responden a la estrategia informática organizacional (incompatibles, no consistentes con otros productos existentes o que se prevé incorporar, etc.).
		¿Existen situaciones de excepción?	X				
		¿Estas situaciones de excepción están autorizadas por la dirección de la organización y auditadas por la unidad de auditoría interna?	X				

Ing. JUAN JOSE BENITEZ
Perito Forense
COPITEC Nº I-6663

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple			Comentarios	Riesgos
			[illegible]	Nc	[illegible]		
3.1	La unidad de TI debe definir el **modelo de arquitectura de la información de la organización, orientado a asegurar que los datos se encuentren organizados eficientemente y de manera homogénea**, adoptando todas las medidas a su alcance para que estos se encuentren disponibles para su utilización, en concordancia con las necesidades operativas de las diferentes áreas usuarias en cuanto a oportunidad, integridad o formato, entre otras. Este modelo de arquitectura de la información debe documentarse y mantenerse actualizado en un **diccionario de datos corporativo**, especificando los controles de **consistencia, integridad, confidencialidad y validación aplicables.**	¿Esta definido el modelo de arquitectura de la información de la organización?			X	En la UI respecto a las aplicaciones de desarrollo propio sí pero no hay integración con el resto de la INA	• Datos inconsistentes, redundantes, no accesibles, etc. por un erróneo diseño de las bases de datos. • Información pobre para la toma de decisiones. • Mayores costos y dificultades para el mantenimiento de sistemas y bases de datos o archivos de información.
		¿Esta documentado el modelo de arquitectura de la información mediante un diccionario de datos corporativo? ¿Se encuentra actualizado?		X		Debe desarrollarse en Diccionario de Datos de uso general y que abraque al INA en su totalidad	
		¿Existen controles de consistencia, integridad, confidencialidad y validación?			X	Si en la aplicaciones bajo control de la UI.	
		Arquitectura de la información	0	1	2	0	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

4.1	Se debe garantizar el cumplimiento de las normas establecidas en cuanto al deber de disponer de una política de seguridad de la información (Decisión Administrativa N° 641/2021 y normas complementarias o modificatorias, en base al estándar IRAM - ISO/IEC 27001, 27002 y 20000-1). Todos los aspectos de la seguridad deben definirse considerando la clasificación de los recursos y la información, de modo de establecer un adecuado balance entre los controles y el recurso a proteger. El requisito de disponer de una política de seguridad y adecuadas medidas de seguridad de la información (en base al estándar IRAM- ISO/IEC 27001, 27002 y 20000-1), alcanza a todos los organismos, empresas, universidades y demás entidades que conforman el Poder Ejecutivo Nacional.	¿Se dispone de una política de seguridad de la información basada en la Decisión Administrativa N° 641/2021 y normas Complementarias o modificatorias, en base al estándar IRAM - ISO/IEC 27001, 27002 y 20000-1?	X			Se completó e informó la DA 641/2021	• Dificultades o imposibilidad para acceder a información necesaria para las operaciones o para la toma de decisiones. • Información no confiable (datos incorrectos, faltantes, sobrantes, inconsistentes, etc.) • Acceso a la información organizacional por parte de personas no autorizadas. • Interrupciones a las operaciones y/o servicios informáticos. • Exposición de información confidencial. • Pérdidas económicas. • Pérdida de información organizacional. • Dificultades para exigir rendiciones de cuentas • Fraude o irregularidades. • Dificultades para detectar errores por falta de controles por oposición.
4.2	La unidad de TI debe desarrollar, documentar, aprobar y comunicar políticas y procedimientos respecto de las actividades relacionadas con la TI. Tales políticas y procedimientos deben mantenerse actualizados. Deben especificar las tareas y controles a realizar en los distintos procesos, así como los responsables y las sanciones disciplinarias Asociadas con su incumplimiento.	¿Existe un análisis de costo/beneficio y evaluación de riesgos asociada a la contratación de servicios a terceros?	X				• Falta de aplicación de procedimientos y controles uniformes. • Dificultades para delimitar responsabilidades y exigir rendiciones de cuentas. • Dependencia de determinado personal. Desconocimiento de la operatoria por parte del personal. • Dificultades para capacitar nuevo personal. • Uso ineficiente de tiempo y recursos. • Errores o fallas en las actividades por la transmisión oral de las prácticas de trabajo. • Por la informalidad, se presentan dificultades para comprobar si se ejecutaron o no tareas o controles dentro del proceso. • Dificultades para encarar mejoras en los procesos (ya que no se cuenta con un esquema claro del cual partir).
		Tales políticas y procedimientos ¿se encuentran actualizadas?			X		
		¿Están definidas las tareas y controles a realizar en los distintos procesos?	X				
		¿Están debidamente identificados los responsables de llevar a cabo las distintas actividades y controles? ¿Existen sanciones disciplinarias asociadas con su incumplimiento?			X	Estan identificados los controles pero NO las sanciones disciplinarias	
	Las políticas y/o procedimientos que deben desarrollar, documentar, aprobar y comunicar –según corresponda en cada organismo-, abarcan entre otros:	¿Existen, al menos, los siguientes procedimientos aprobados?					
	• Gestión de inventario de recursos informáticos y licencias.	• Gestión de inventario de recursos informáticos y licencias	X				
	• Propiedad y clasificación de la información.	• Propiedad y clasificación de la información		X		No posee Tarea del comité de seg de info	
	• Generación de backups y pruebas de recuperación.	• Generación de backups y pruebas de recuperación.	X				
	• Tratamiento ante contingencias y para la continuidad operativa.	• Tratamiento ante contingencias y para la continuidad operativa. (Plan de Contingencias)	X				
	• Gestión de incidentes.	• Gestión de incidentes.	X				
	• Atención de la mesa de ayuda/servicios informáticos	• Atención de la mesa de ayuda/servicios informáticos	X				
	• Administración y control de Acceso a Sistemas y Aplicaciones (considerando vínculos de comunicaciones involucrados) –abarcando la gestión de altas, bajas y modificaciones sobre los permisos de acceso, gestión de usuarios críticos y de emergencia.	• Administración y control de Acceso a Sistemas y Aplicaciones (considerando vínculos de comunicaciones involucrados) –abarcando la gestión de altas, bajas y modificaciones sobre los permisos de acceso, gestión de usuarios críticos y de emergencia.	X				
	• Control contra software malicioso	• Control contra software malicioso	X				
	• Registro y revisión de registros de transacciones o logs	• Registro y revisión de registros de transacciones o logs	X				
	• Administración de la configuración de software de base, de comunicaciones y seguridad	• Administración de la configuración de software de base, de comunicaciones y seguridad	X				
	• Administración de proyectos informáticos	• Administración de proyectos informáticos		X		La UI debe conocer sobre los proyectos informáticos en curso	
	• Accesos y medidas de control a la seguridad física sobre los recursos informáticos –en particular sobre aquellos considerados críticos-;	• Accesos y medidas de control a la seguridad física sobre los recursos informáticos –en particular sobre aquellos considerados críticos-;	X				
	• Metodología de administración sitios web y redes sociales (responsabilidades por el ABM de contenidos, periodicidad de actualización, lineamientos de imagen, etc.)	• Metodología de administración sitios web y redes sociales (responsabilidades por el ABM de contenidos, periodicidad de actualización, lineamientos de imagen, etc.)	X			La UI administra el sitio web y la intranet del Ina. El proceso de alta, baja y modificación de contenidos está establecido a través de un sistema de autorizaciones relacionado a las autoridades de cada subgerencia y a personas designadas como referentes de intranet y web por ellos.	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-6668

	• Trabajo remoto • Procedimientos particulares según el caso (seguridad en dispositivos móviles, criptografía, seguridad y gestión de servicios y almacenamiento en la nube, etc.)	• Trabajo remoto	X				
		• Procedimientos particulares según el caso (seguridad en dispositivos móviles, criptografía, seguridad y gestión de servicios y almacenamiento en la nube, etc.)	X				
		• *Otro..*					
	La elaboración de procedimientos deberá sujetarse a lo establecido en el art. 101 del Dec. 1344/2007, en cuanto a que se deberá pedir opinión previa favorable de la correspondiente Unidad de Auditoría Interna, la cual verificará los criterios de contenido y forma según la Res. SIGEN N°162/2014.	¿Para la implementación de los procedimientos se pide opinión previa favorable a la Unidad de Auditoría Interna con el fin de verificar criterios de contenido y forma?					Se esta creando actualmente la norma, se envio a revision de la GPP y una vez autorizada y previa a la firma presidencial se elevara para consideracion a la UAI
		Políticas y Procedimientos	15	2	2	0	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple				Comentarios	Riesgos
				NO				
5.1	La unidad de TI **debe garantizar el cumplimiento de las regulaciones** relativas a protección de datos personales, propiedad intelectual del software, seguridad de la información, utilización de estándares, sistemas o plataformas definidas en Sector Público Nacional, acceso a la información pública, así como de las demás normas que resulten aplicables.	¿Se han implementado controles suficientes tendientes a asegurar el cumplimiento de las regulaciones relativas a privacidad de la información, propiedad intelectual del software, seguridad y otras normas que fueran aplicables?		X			No se encuen transon las misi ones y fun ciones asi gn adasa la UI. Debe ser resu elto quien lo hace	• Litigios, juicios, sanciones o sumarios por incumplimiento de normativa. • Perjuicio económico para la organización. • Uso ineficiente de los recursos públicos.
5.2	La unidad de TI debe establecer **convenios o contratos formales con aquellos terceros** con los que existan intercambios de información o prestación de servicios relacionados con la TI, los cuales deben ser revisados periódicamente a fin de asegurar que se mantengan actualizados.	¿Los convenios o contratos formales son revisados periódicamente a fin de asegurar que se mantengan actualizados?			X		La U ilo hace con los con tatos que pasan por ella, pero n opuede respon der por los que se firman en otras depen den cas.	• Inconvenientes para delimitar responsabilidades. • Reclamos por parte de terceros hacia la organización. • Baja calidad o bajo nivel de servicios por parte de la contraparte. • Incumplimientos por parte de la contraparte, dificultades para realizar los reclamos pertinentes. • Exposición de información de la Organización por parte de terceros con los que no se suscribió un adecuado acuerdo de confidencialidad o no divulgación.
		Cumplimiento y Regulaciones	0	1	1	0		

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple				Comentarios	Nro Observación en Informe	Riesgos
				NO					
6.1	La unidad de TI debe disponer de una metodología de administración de proyectos que se aplique en todos los proyectos informáticos encarados.	¿Se dispone de una metodología de administración de proyectos documentada?		X			Hay proyectos que se realizan y materializan sin la intervención ni conocimiento de la UI		• Cada proyecto informático se gestiona de acuerdo a la capacidad del responsable, sin requisitos mínimos unificados. Resultados inciertos en cada caso. • Responsabilidades no claras para las tareas dentro del proyecto. • Se encaran proyectos no autorizados o sin presupuesto. • Las recomendaciones de la UAI llegan una vez finalizado el proyecto (por no haber participado desde etapas tempranas). • Proyectos informáticos que no son aprovechados por todas las áreas involucradas. • Insuficiente planificación para los proyectos.
	Debe contemplar procedimientos detallados, mínimamente para:								
6.1.1	La documentación y aprobación de la justificación que origina el proyecto, así como la definición clara del plan, especificando sus objetivos, alcance, asignación de responsabilidades y facultades a los miembros del grupo de proyecto, y el presupuesto de los recursos a utilizar en el mismo. Se debe contemplar la elaboración del plan de pruebas y de capacitación que fueran necesarios.	La metodología de administración de proyectos ¿contempla la documentación y aprobación de la justificación que origina los proyectos encarados?		X			Lo realiza la GPyP . No aplica a la UI		
		¿Incluye el requisito de definir claramente el plan, detallando objetivos, alcance, asignación de responsabilidades y facultades a los miembros del grupo de proyectos?		X					
		¿Contempla la definición del presupuesto de los recursos a utilizar?		X					
		¿Indica que se debe elaborar el plan de pruebas y de capacitación?		X					
6.1.2	La realización de los estudios de factibilidad pertinentes y del análisis de los riesgos del proyecto.	La metodología de administración de proyectos ¿contempla la realización de estudios de factibilidad y análisis de riesgo de los proyectos encarados?		X					
6.1.3	La participación formal de todas las áreas involucradas en el proyecto y de la unidad de auditoría interna.	La metodología de administración de proyectos ¿incluye el requerimiento respecto de la participación de todas las áreas involucradas en el proyecto y de la unidad de auditoría interna?		X					
6.2	Se debe monitorear la ejecución del plan del proyecto considerando el cumplimiento de los objetivos planteados, plazos y costos.	¿Se realiza el seguimiento de la ejecución del plan de los proyectos encarados, considerando el cumplimiento de objetivos planteados, plazos y costos?		X					• No se alcanzan las expectativas de las autoridades organizacionales por no cumplirse los objetivos del proyecto, por no cumplirse los plazos previstos y/o excederse en costos. • Desvíos en la ejecución de proyectos informáticos que no se detectan, o se detectan tarde. • Mayores costos.

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumplimiento Si	No	Parc	N/A	Comentarios	Riesgos
7.1	La unidad de TI debe disponer de un **procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas** (incluyendo sus distintas modalidades: web, aplicaciones móviles, etc.), que debe estar **documentado y aprobado**, y debe aplicarse en forma complementaria a las normas relativas a administración de proyectos.	¿Se cuenta con un procedimiento o metodología para las actividades de desarrollo, mantenimiento o adquisición de sistemas?	x				Se recibe por escrito (correo, nota, gedo) la necesidad del área o usuario. Se evalúa con el equipo UI la forma de satisfacerla. Se notifica al usuario de las posibles soluciones. Comienza el proceso de adquisición o desarrollo. Se testea el producto o servicio con el personal interesado para determinar la necesidad o no de ajustes.	• Las tareas de desarrollo de sistemas se llevan a cabo de acuerdo al criterio y capacidad del responsable de turno. • Dependencia del personal que desarrolla cada sistema. • Inconvenientes para delimitar responsabilidades.
		La metodología de desarrollo, mantenimiento o adquisición de sistemas ¿se aplica en todos los casos y se aplica en forma complementaria a las normas relativas a administración de proyectos?	x					
	Debe contemplar procedimientos detallados, mínimamente para:							
7.1.1	La formulación y documentación de **requerimientos por parte de las áreas usuarias**, ya sea para nuevos desarrollos, adquisiciones o cambios a los sistemas existentes, incluyendo la definición detallada de las **necesidades** que motivan el requerimiento y la **especificación de los niveles de servicio esperados.**	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contiene procedimientos detallados para la formulación y documentación de los requerimientos por parte de las áreas usuarias?	x				Para el caso de desarrollos web o de la Intranet. El procedimiento implica recibir por escrito el pedido, reuniones, pruebas, testeos y publicación.	• Se desarrollan sistemas que no satisfacen los requerimientos del usuario o que no fueron requeridos ni consensuados con ningún usuario. • Cambios a programas que no fueron solicitados por el área usuaria del sistema. • Conflictos entre el área de Sistemas y las Áreas.
7.1.2	El criterio para el establecimiento de **prioridades** entre los distintos **requerimientos** recibidos por la unidad de TI.	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla el criterio para el establecimiento de prioridades entre los distintos requerimientos recibidos por la unidad de TI?	x					• Se encaran desarrollos que no responden a la estrategia organizacional. • Sistemas atiende primero los pedidos de las áreas "amigas". • Conflictos en la relación con las áreas porque todos solicitan sistemas "urgentes" y no está claro cómo deben ser administrados.
7.1.3	El tratamiento de **solicitudes de emergencia**, incluyendo la **autorización** del responsable de la unidad de TI, el **registro y monitoreo** de las tareas realizadas.	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contiene procedimientos para el tratamiento de solicitudes de emergencia?	x					• Tratamiento de los cambios de emergencia de acuerdo al criterio y capacidad del responsable (puede obstaculizar su ejecución pidiendo formalidades y otros controles propios de cambios de rutina, o realizar los cambios sin ningún tipo de control o registraciones). • Dificultades para reconstruir la situación previa en caso de fallas, o imposibilidad de determinar responsables. • Cambios a programas o datos que no dejan rastros, son fraudulentos o encubren otras situaciones irregulares.
		¿El procedimiento considera la autorización del responsable de la unidad de TI?	x					
		¿El procedimiento incluye el registro y monitoreo de las tareas realizadas ante solicitudes de emergencia?	x					
7.1.4	La **aprobación** por parte de los responsables de las áreas usuarias afectadas, de las especificaciones de diseño elaboradas.	El procedimiento ¿contempla la aprobación por parte de los responsables de las áreas usuarias afectadas sobre las especificaciones de diseño elaboradas?	x					• Se desarrollan sistemas que no satisfacen los requerimientos del usuario. • Conflictos entre el área de Sistemas y las Áreas.
7.1.5	La **participación de la unidad de auditoría interna** durante el desarrollo.	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla la participación de la unidad de auditoría durante el desarrollo?		x			Al igual que en los proyectos debe intervenir la UI en este punto	• Se desarrollan sistemas que no incorporan controles suficientes, o bien no contemplan requerimientos del área de Auditoría como registros de transacciones o logs, alertas automáticas, etc. • Las recomendaciones de la Auditoría Interna llegan con el sistema en funcionamiento, y obligan a reformular y modificar el sistema.
7.1.6	La utilización de **estándares de diseño, programación y documentación.**	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿define estándares de diseño, programación y documentación?	x					• El diseño, programación o documentación del sistema se realiza de acuerdo al criterio, conocimientos y capacidad del responsable de turno. Pueden resultar ininteligibles para otros agentes del área. • Dependencia del personal de sistemas afectado a la labor. • Dificultades para controlar y auditar el sistema.
7.1.7	La **realización de pruebas suficientes** en las distintas etapas del desarrollo, conforme a un **plan de pruebas y de control de calidad aprobado, en un ambiente específico representativo del ambiente operativo futuro y distinto del ámbito de producción.** Se deben establecer los criterios para concluir el proceso de prueba y dar por aceptada la implementación del sistema. Dichas **pruebas deben contemplar la participación y aprobación formal del usuario solicitante.**	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla la planificación y realización de pruebas en las distintas etapas del desarrollo?	x					• Se implementan sistemas que no satisfacen los requerimientos del usuario. • Se implementan sistemas que funcionan incorrectamente, arrojan errores o no responden a lo esperado. • Se pierden o afectan datos de las bases de datos, por sistemas que funcionan erróneamente.
		¿Establece que las pruebas deben realizarse en un ambiente específico representativo del ambiente operativo y distinto del ámbito de producción?	x					
		¿El proceso de prueba contempla la participación y aprobación formal del usuario solicitante?	x					
7.1.8	La apropiada **segregación de ambientes** y el **pasaje del sistema aprobado desde el ambiente de desarrollo/prueba al de producción.**	¿El procedimiento contempla la segregación de ambientes y la aprobación del sistema desde el ambiente de desarrollo/prueba a producción?	x					• Se implementan sistemas o versiones de programas fraudulentos, irregulares y/o que no se encuentran autorizados. • Se agregan, borran o modifican datos de las bases de datos, por cambios a programas que no fueron probados y aprobados.

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

7.1.9	**El control de las versiones del software** por parte del área responsable de las tareas de desarrollo y mantenimiento de sistemas.	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla procedimientos para controlar las versiones del software por parte del área responsable de las tareas de desarrollo y mantenimiento de sistemas?	x				• Se pierde el registro y control sobre las versiones de los programas implementados, con lo que puede desconocerse sobre cuál versión deben realizarse las próximas modificaciones. • Se implementa una versión de un programa que –si bien incluye el cambio requerido en esta oportunidad- no incluye arreglos que fueron realizados previamente.
7.1.10	La preparación de **documentación de soporte para el usuario y el personal técnico.**	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla los requerimientos de documentación para usuarios y personal técnico?	x				• Dependencia del personal técnico que desarrolló el sistema (único que conoce los detalles de programación y diseño del sistema). • Dificultades para efectuar el mantenimiento y actualización del sistema. • Dificultades para capacitar usuarios para operar el sistema. Los procedimientos se transmiten solo oralmente, con el consiguiente riesgo de errores, olvidos, etc. • Dificultades para integrar nuevo personal técnico al equipo de trabajo.
7.1.11	La capacitación **al personal de las áreas usuarias y de la unidad de TI.**	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla mecanismos para la capacitación al personal de las áreas usuarias y de la unidad de TI?	x			Cada desarrollo web o de la Intranet conlleva un instructivo para el usuario que se envía por correo como cierre del proceso y se consigan en la Intranet. También se dictan capacitaciones complementarias de ser requeridas.	• Usuarios no capacitados para operar el sistema, que cometen errores o no lo pueden aprovechar al máximo. • Personal técnico encargado de funciones de desarrollo, que no se actualiza, no conoce nuevas técnicas de diseño, programación, lenguajes, etc.
7.1.12	El criterio a seguir según envergadura, características e interacciones con **terceros** del sistema, para el registro de la **propiedad intelectual del sistema a favor del Estado Nacional**, así como los pasos a seguir para dicho registro.	El procedimiento para las actividades de desarrollo, mantenimiento o adquisición de sistemas ¿contempla el criterio a seguir según envergadura, características e interacciones con terceros del sistema, para el registro de la propiedad intelectual del sistema a favor del Estado Nacional, así como los pasos a seguir para dicho registro?	x				• Reclamos o pérdidas económicas por la falta de registro oportuno de la propiedad del sistema en caso de acceso y registro por parte de un tercero o un agente no autorizado.
7.2	La **contratación de servicios externos** de desarrollo de sistemas debe estar justificada por escrito y autorizada por el responsable de la unidad de TI. El contrato debe estipular que el **software, la documentación y demás ítems adquiridos se sometan a prueba y revisión antes de la aceptación por parte de la unidad de TI** y de **las áreas usuarias**, incluyendo aspectos relativos a la **seguridad de los desarrollos**. Salvo justificación documentada y aprobada en contrario, la **propiedad intelectual del software resultante debe pertenecer a la organización contratante**, lo cual debe constar en el contrato. Asimismo, deben establecerse en el citado contrato, **los criterios de aceptación del producto.**	La contratación de servicios externos de desarrollo de sistemas ¿Es justificada y aprobada por el responsable de la unidad de TI? En caso que la propiedad intelectual del software resultante no pertenezca a la organización contratante ¿existe justificación documentada y aprobada al respecto? ¿Consta en el contrato a quien pertenecerá la propiedad intelectual?			x	Solo aquellas contrataciones realizadas por la UI, actualmente no todos los servicios a contratar pasan por la supervisión de la UI	• Dependencia de terceros para el uso de un sistema organizacional. • Compras informáticas de elementos que no contribuyen a una estrategia unificada, no compatibles entre sí, etc. • Duplicación de esfuerzos en tareas informáticas, al existir diversos responsables, distintas áreas realizando tareas similares, o no existir la posibilidad de compartir conocimientos y recursos para el desarrollo de las tareas (módulos desarrollados, productos de software, utilitarios, bases comunes, etc.). • Sistemas que funcionan incorrectamente o presentan debilidades de control. • La información que produce el sistema no resulta confiable. • Litigios, reclamos económicos con terceros. • Aceptación de sistemas provistos por terceros que no cumplen lo requerido por la organización o no responden a lo que se contrató.
7.3	En el **desarrollo de sistemas debe procurarse incluir controles automatizados** que contribuyan a reducir los riesgos que puedan afectar el logro de los objetivos, debiendo contemplarse particularmente controles de: • Integridad: debe asegurarse el tratamiento, procesamiento y registro de la totalidad de las transacciones u operaciones. • Exactitud: debe asegurarse la registración oportuna y correcta de las operaciones. • Validez: las transacciones registradas deben representar con precisión las operaciones ejecutadas, considerando los procedimientos establecidos.	¿El desarrollo de sistemas incluye controles automatizados que contribuyan a reducir los riesgos que puedan afectar el logro de los objetivos? ¿Los controles contemplan la integridad, exactitud y validez de las transacciones/operaciones?			x	Se realizan los controles de aquellos software administrados y alojados en la UI	• Sistemas que funcionan incorrectamente o presentan debilidades de control. • La información que produce el sistema no resulta confiable. • Errores en los controles manuales. • Pérdidas de tiempo por no contar con controles automatizados.
7.4	El desarrollo de sistemas, particularmente en el caso de sistemas que contengan **algoritmos de análisis masivos de datos** (inteligencia artificial, análisis de patrones, ubicación geográfica, datos de salud, etc.), debe contemplar **reglas éticas de diseño y funcionamiento, que aseguren la apropiada protección de los derechos de los ciudadanos.**	¿El desarrollo de sistemas contempla reglas éticas de diseño y funcionamiento, que aseguren la apropiada protección de los derechos de los ciudadanos?	X			Trabajamos en el marco de la Ley N° 26.653 de "Accesibilidad Web" y de las disposiciones de la Oficina Nacional de Tecnologías de Información.	
		Administración y Adquisición de Soft y Apl	18	1	2	0	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple				Comentarios	Riesgos
				NO				
8.1	**Las adquisiciones de bienes y servicios informáticos** deben basarse en los **estándares vigentes para la Administración Pública**, y deben estar debidamente **justificadas, documentadas y respaldadas por el análisis de costo/beneficio y la evaluación de riesgos pertinentes.** Se debe garantizar el cumplimiento de la normativa de contrataciones aplicable. Las adquisiciones deben responder a los proyectos contemplados en el Plan estratégico y operativo informático, debiendo las excepciones, encontrarse justificadas y autorizadas por los niveles pertinentes.	Para la adquisición de bienes y servicios informáticos ¿Se tienen en cuenta los estándares vigentes para la Administración Pública?	X					• Sanciones y/o inconvenientes por incumplimiento de la normativa. • Adquisiciones que no respetan los estándares vigentes en la Administración Pública o que no responden a la estrategia informática organizacional (incompatibles, no consistentes con otros productos existentes o que se prevé incorporar, etc.). • Adquisiciones informáticas incorrectamente planificadas, que no se basan en análisis de costos y beneficios. • Que la organización no obtenga oportunamente los resultados informáticos planificados. • Mayores costos a los previstos • Que se realicen compras que no contribuyan con los proyectos incluidos en el plan informático aprobado, sino a otro tipo de objetivos que no cuentan con aprobación.
		¿Las adquisidores de bienes y servicios se encuentran debidamente documentadas, justificadas y respaldadas por el análisis de costo/beneficio y la evaluación de riesgos pertinente?	X					
		¿Las adquisiciones responden a los proyectos contemplados en el Plan estratégico y operativo informático, debiendo las excepciones, encontrarse justificadas y autorizadas por los niveles pertinentes?	X					
8.2	**Los productos deben ser analizados y probados antes de proceder a su aceptación definitiva.**	¿Se analizan y prueban los productos antes de proceder a su aceptación definitiva?	X					• Pagos a proveedores de equipamiento sin verificar la entrega de todos los productos comprometidos. • Incorporación de productos informáticos fallados o que no responden a lo contratado.
8.3	La unidad de TI **debe planificar y realizar el mantenimiento preventivo periódico del hardware,** a fin de reducir la frecuencia y el impacto de las fallas en su desempeño.	¿Existe un plan de mantenimiento preventivo del hardware?	X					• Fallas en el equipamiento o dispositivos de hardware. • Interrupciones en operaciones—a mayor o menor escala- por fallas en el equipamiento (Ej. deja de funcionar un servidor relevante, o inconvenientes porque falla una impresora de menor relevancia).
		¿Se realiza el mantenimiento preventivo de acuerdo a lo planificado?	X					
8.4	Deben existir **procedimientos documentados para la gestión de licencias de software** a fin de asegurar que en la organización solamente se utilicen productos adquiridos por vías oficiales.	¿Existen procedimientos documentados para la gestión de licencias de software?		X				• Litigios, reclamos económicos, conflictos con terceros. • Instalación y/o utilización de software no autorizado y/o que no responde a los objetivos organizacionales (software de oficina sin licencia, software para otros fines como juegos, etc.). Esto acarrea riesgos de virus informáticos o la inclusión de debilidades en la seguridad informática. • Dificultades para planificar actualizaciones de productos de software. • Sanciones y/o inconvenientes por incumplimiento de normas aplicables. • Dificultades para obtener el inventario de licencias de software adquiridas por la Organización, y para su adecuado registro patrimonial y contable.
8.5	Las **bajas de equipamiento y Residuos de Aparatos Eléctricos y Electrónicos (RAEES)** deben enmarcarse en criterios preestablecidos considerando el **borrado seguro de datos y la política ambiental organizacional** –de corresponder- los mecanismos aplicables de gestión de residuos que puedan afectar el ambiente.	¿Existe un procedimiento que contemple las bajas de equipamiento y Residuos de Aparatos Eléctricos y Electrónicos (RAEES)?	X					• Exposición no autorizada de información organizacional. • Afectación negativa del ambiente.
		Adquisición y Mantenimiento de Infraestructura Tecnológica	7	1	0	0		

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple			Comentarios	Riesgos
			Sí	No			
9.1	La decisión de contratar **servicios a terceros** debe estar debidamente **justificada, documentada** y respaldada por el **análisis de costo/beneficio y la evaluación de riesgos pertinentes.**	En caso de contratos de servicios a terceros, ¿se justifican por escrito?	X				• Contrataciones innecesarias o que no responden a una relación de costo – beneficio adecuada. • Dependencia de terceros, exposición de información de la organización, etc. por la falta de análisis de riesgos.
		¿Existe un análisis de costo/beneficio y evaluación de riesgos asociada a la contratación de servicios a terceros?	X				
9.2	La dirección de la organización debe definir **procedimientos** específicos para garantizar que cada vez que se implementen **relaciones con proveedores externos de servicios**, se defina y se acuerde un **contrato formal** antes de que comience el trabajo, el cual debe identificar claramente los objetivos a alcanzar y servicios a proveer, las obligaciones de ambas partes, los métodos y responsables de las interacciones y las políticas de la organización que deben ser respetadas por el tercero, incluyendo los aspectos de confidencialidad y soberanía sobre los datos, de ser aplicables. Tales procedimientos deben asegurar el cumplimiento de la normativa para las Contrataciones aplicables.	En caso de servicios provistos por terceros, ¿se establece un contrato formal antes de comenzar el trabajo?	X				• Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos. • Litigios o conflictos, dificultades para determinar responsabilidades. • Sanciones por incumplimientos normativos.
		Los contratos ¿identifican claramente los claramente los objetivos a alcanzar y servicios a proveer, las obligaciones de ambas partes, los métodos y responsables de las interacciones y las políticas de la organización que deben ser respetadas por el tercero, incluyendo los aspectos de confidencialidad y soberanía sobre los datos?	X				
9.3	Los contratos con terceros proveedores de servicios deben incluir la **especificación formal de acuerdos de nivel de servicio**, identificando explícitamente los respectivos a seguridad –por ejemplo los acuerdos de no divulgación- y al cumplimiento de los requisitos legales aplicables. **Se debe aclarar expresamente que la propiedad de los datos corresponde a la organización contratante.**	Los contratos por servicios de terceros ¿incluyen la especificación formal de acuerdos de nivel de servicio? ¿Consta expresamente que la propiedad de los datos corresponde a la organización contratante?	X				• Interrupciones a los servicios contratados, fallas en la seguridad informática (corrupción de datos, información no confiable, accesos no autorizados, etc.) • Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos. • Exposición no autorizada de la información de la organización.
9.3	La dirección de la organización debe monitorear el servicio prestado por los terceros contratados, para garantizar que se cumplan las obligaciones comprometidas.	¿El servicio prestado por los terceros contratados es debidamente monitoreado por la dirección de la organización?	X				• Pérdidas / perjuicio económico para la organización por pagos a proveedores que no prestan adecuadamente el servicio. • Incumplimiento por parte del proveedor, baja calidad de los servicios recibidos. Interrupciones o inconvenientes en las operaciones informáticas de la organización. • Dificultades para detectar desvíos o incumplimientos de terceros.
9.5	En caso de contrataciones de servicios externos en los que el **proveedor realice el procesamiento de la información de la organización mediante sistemas que pertenecen al tercero**, careciendo la organización de los programas fuente, deben tomarse las previsiones necesarias para **asegurar la disponibilidad de los mismos** por parte de la organización **en caso de alguna contingencia o salida del mercado del proveedor** -por ejemplo, dejando una copia de los fuentes bajo custodia de escribano para el caso de una eventual quiebra del proveedor-, o bien estableciendo otro mecanismo de contingencia para la continuidad operativa. En caso de tratarse de algún tipo de procesamiento o almacenamiento en la **"nube"**, debe constar la autorización formal correspondiente, incluyendo el análisis de riesgos y beneficios (considerando la criticidad de la información en cuestión, la posible exposición de la misma a terceros, los costos asociados, las implicancias en cuanto a disponibilidad y agilidad, la modalidad que se utilizará para asegurar la eliminación de los datos una vez que sea necesario, etc.). La información tratada en estos casos debe estar formalmente clasificada, en base a los criterios definidos en la Política de Seguridad de la información.	En caso de servicios de procesamiento contratados, en los que el sistema pertenece al tercero y la organización carece de los programas fuente ¿existen previsiones para asegurar la disponibilidad de los programas fuente ante alguna contingencia o salida del mercado de parte del proveedor?			X	Cuando el soft es contratado por la UI si, pero existen casos en los que no participamos y tuvimos que dar soluciones a dicha situacion. Ej SABEN / SIU/ RELOJ etc	• Interrupciones a las operaciones organizacionales. • Dependencia de terceros. • Exposición de información del Estado Nacional.
		En caso de tratarse de algún tipo de procesamiento o almacenamiento en la "nube", ¿consta la autorización formal correspondiente, incluyendo el análisis de riesgos y beneficios, entre otros aspectos?			X	No poseemos procesamientos en la nube No Aplica	
		¿La información tratada en estos casos se encuentra formalmente clasificada, en base a los criterios definidos en la Política de Seguridad de la información?	X				
		Serv de Proc y/o Sop de Terceros	5	0	1	1	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple		N/A	Comentarios	Riesgos
			SI	NO			
10.1	Deben asignarse formalmente las responsabilidades por la publicación de contenidos en medios digitales (sitios web institucionales, redes sociales organizacionales, etc.), debiendo seguir, dichas publicaciones, los criterios aprobados por las autoridades.	¿Se han asignado formalmente las responsabilidades por la publicación de contenidos en medios digitales?	X			La UI maneja el sitio web institucional y la Intranet. Para ambas plataformas el procedimiento para publicación de contenidos está establecido e informado al personal.	• Publicación de información no autorizada, incorrecta, no actualizada, contradictoria, inconsistente, etc. • Impacto negativo en la imagen pública de la organización por incorrecto funcionamiento del sitio Web, o problemas en la información publicada. Sanciones, inconvenientes o litigios.
10.2	Debe establecerse un acuerdo de nivel mínimo de servicios con los proveedores de los servicios de comunicaciones, a fin de asegurar que la prestación de los mismos se corresponda con los requerimientos de la organización.	¿Existe un acuerdo de nivel mínimo de prestaciones con los proveedores de los servicios de comunicaciones?	X				• Interrupciones en los servicios de comunicaciones, o baja calidad de los servicios. Incumplimiento por parte del proveedor. • Dificultades para detectar desvíos o incumplimientos, o para delimitar responsabilidades.
		Publ Info Digital	2	0	0	0	

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC Nº I-6668

	Norma según Res. 87-SGN	Aspecto a Evaluar	Cumple			Comentarios	Riesgos
				No			
11.1	Se deben definir indicadores de desempeño para monitorear la gestión y las excepciones de las actividades de TI y de seguridad de la información.	¿Se utilizan indicadores de desempeño para hacer el seguimiento de la gestión y las excepciones de las actividades de TI y de Seguridad de la Información?			X	Para sitio web e Intranet se obtienen métricas.	• Los sectores dentro del área no responden adecuadamente a las tareas asignadas o planificadas. Trabajo descoordinado entre sectores. • Aprovechamiento ineficiente de los recursos. • Existencia de riesgos no administrados en la gestión informática. • Los desvíos en la ejecución de tareas no se detectan, o se detectan en forma inoportuna. • Gestión informática ineficaz o ineficiente.
11.2	La unidad de TI debe presentar informes periódicos de gestión a la dirección de la organización para que esta supervise el cumplimiento de los objetivos planteados. De igual forma, deben elevarse reportes periódicos sobre la situación de la seguridad de la información.	La unidad de TI ¿presenta informes periódicos de gestión a la dirección de la organización?		X		No lo esta haciendo	• Inadecuada gestión de prioridades para los proyectos informáticos • Mayores costos o plazos respecto a lo previsto. • Descoordinación entre las actividades informáticas y la estrategia organizacional. • Dificultades para detectar y corregir desvíos en la ejecución de proyectos
		Monitoreo Activos TI	0	1	1		

Ing. JUAN JOSÉ BENÍTEZ
Perito Forense
COPITEC N° I-5668