INFORME ESPECIAL DE CONTROL INTERNO RELACIONADO CON EL DIAGNÓSTICO DE TODOS LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIÓN EN PRODUCCIÓN DEL INAMU - (EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA, RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL INAMU PARA PERIODO 2022).

INAMU-JD-AI-In-014-2022

(Remitido con oficio INAMU-JD-AI-009-2023)

Firma de validación del informe
Elaborado por
RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Firmado digitalmente por RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Fecha: 2023.01.16 15:18:45 -06'00'
Randall Umaña Villalobos **AUDITOR INTERNO**

INSTITUTO NACIONAL DE LAS MUJERES.

INFORME ESPECIAL DE CONTROL INTERNO RELACIONADO CON EL DIAGNÓSTICO DE TODOS LOS SISTEMAS INFORMÁTICOS Y DE COMUNICACIÓN EN PRODUCCIÓN DEL INAMU - (EVALUACIÓN DE LOS PROCESOS DE SEGURIDAD FÍSICA Y LÓGICA, RELATIVOS A LAS TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN DEL INAMU PARA PERIODO 2022).

El presente proyecto se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2022, el objetivo general del trabajo es evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte del INAMU en su ambiente de tecnologías de información y obtener un informe sobre los aspectos observados que constituyan oportunidades de mejora en dichos procesos, así como las recomendaciones respectivas.

Es importante evidenciar que los resultados del presente estudio forman parte de la Contratación de los Servicios Profesionales de Auditoria en TI, para el periodo 2022, definido en el Plan de Compras 2022, mediante el proceso de Contratación 2022CD-000004-0015800001, cuyo objetivo es obtener el criterio técnico y profesional en relación con los siguientes temas:

A. Realizar un diagnóstico del alineamiento del Plan Estratégico de TI y el Plan Estratégico Institucional, sus políticas y el mapeo de los riesgos de la Unidad de Informática emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

B. Realizar un diagnóstico de la seguridad física y lógica para determinar fuentes de amenazas a los sistemas informáticos y de comunicación en producción del INAMU., emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

C. Realizar el levantamiento y diagnóstico de todos y cada uno de los sistemas informáticos y de comunicación en producción del INAMU., el diagnostico debe determinar al menos el nivel de integración, estabilidad, obsolescencia, emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

Enero - 2023

Tabla de contenido

Tabla de Imágenes

Tabla de Nomenclaturas

Nomenclatura	Significado
GpRD	Gestión para los resultados de desarrollo.
INAMU	Instituto Nacional de las Mujeres.
MIDEPLAN	Ministerio de Planificación Nacional y Política Económica.
NGASP	Normas Generales de Auditoría para el Sector Público.
PEI	Plan Estratégico Institucional.
POI	Plan Objetivo Institucional.
SEVRI	Sistema Específico de Valoración del Riesgo Institucional.
PETIC	Plan estratégico de tecnologías de información y comunicaciones.
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica
CGR	Contraloría General de la Republica
BIA	Bussiness Impact Analysis
UIN	Unidad de Informática.

1 RESUMEN EJECUTIVO

¿QUÉ EXAMINAMOS?

El proyecto de auditoria es de carácter especial tuvo como objetivo realizar un diagnóstico de la seguridad física y lógica de la información para determinar fuentes de amenazas a los sistemas informáticos y de comunicación en producción del INAMU, para permitir asegurar, de manera razonable, el buen desempeño de los procesos sustantivos y la continuidad de los servicios.

¿POR QUÉ ES IMPORTANTE?

El INAMU es la institución responsable formular e impulsar las políticas para la igualdad y equidad de género, además de proteger los derechos de la mujer consagrados tanto en declaraciones, convenciones y tratados internacionales como en el ordenamiento jurídico costarricense; dentro de las estrategias para cumplir de manera eficiente y eficaz con estos mandatos se han establecido nueve servicios esenciales, los cuales requieren de tecnologías de información alineadas a un plan estratégico institucional, para apoyar los procesos sustantivos y la toma de decisiones efectiva y oportuna, ya que actualmente el IMAMU, recopila, clasifica, procesa interpreta y resume una cantidad de datos considerable , pero aún más importante sensible por lo que debe ser gestionada mediante un buen Gobierno de Tecnologías de Información que brinde seguridad, continuidad y eficiencia a los procesos relacionados.

¿QUÉ ENCONTRAMOS?

Una vez concluido el presente proyecto de auditoría se determinó que el INAMU, no ha formalizado y comunicado el nuevo marco de gestión de TI de gobierno y gestión de las tecnologías de información, de acuerdo con lo regulado en la resolución de la

Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información.

Además, el INAMU carece de una “Política de Clasificación de la Información” que le permita determinar el nivel de criticidad, confidencialidad, sensibilidad y seguridad de la información propiedad de éste y/o en su custodia, durante todo el ciclo de vida.

Se logro determinar la ausencia de un Plan de seguridad de la Información en el INAMU., debidamente declarado, aprobado y divulgado, como herramienta de gestión para minimizar los riesgos de fallas y proteger la integridad del software y de la información.

Al mismo tiempo el sistema de gestión de la continuidad del negocio del INAMU., fue actualizado por última vez en el 2017, por lo tanto, el Análisis de Impacto del Negocio (BIA) Bussiness Impact Analysis) que forma parte fundamental del plan de continuidad del negocio del INAMU, puede que no respondan a las necesidades actuales del Instituto,

También se determinó que la Unidad de Informática no actualiza forma continua y permanente la Metodología y Proceso para la Gestión del Riesgo de TI y Seguridad de la Información, con el propósito de que se gestionen riesgos relacionados con temas regulatorios o de cumplimiento, amenazas con temas reputacionales y de gobierno corporativo y otros emergentes, con el objetivo evitar que situaciones como las presentadas con el aplicativo denominado SEANI se materialicen.

¿QUÉ SIGUE?

Dados los hallazgos del presente informe, se emitieron una serie de recomendaciones tales como, que se oficialice y comunique el nuevo marco de gestión de las tecnologías de información y comunicación, que se establezca una política para de clasificación de la Información Institucional, también que se realice una evaluación y

reformulación del proyecto para la implementación del “Plan de gestión de seguridad de la Información a nivel institucional y que se trabaje en el “Plan de continuidad del negocio” en línea con las buenas prácticas y la normativa vinculante.

Así mismo realizar actualizaciones periódicas del Instrumento denominado “Metodología y Proceso para la Gestión del Riesgo de TI y Seguridad de la Información” y que se dote a la Unidad de Informática de recurso humano especializado en ciberseguridad, y, por último, el cumplimiento de recomendaciones y disposiciones emitidas por una cantidad de días importante de atraso.

2 INTRODUCCIÓN

El presente estudio especial de Auditoría de Tecnologías de la Información se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2022, el cual fue aprobado en la Sesión Ordinaria 30-2021, celebrada el 18 de noviembre del 2021, mediante acuerdo de Junta Directiva 06.

Es importante mencionar que a partir de 1998, con la Ley 7801 el legislador trasforma el Centro Nacional para el Desarrollo de la Mujer y la Familia en el Instituto Nacional de las Mujeres, en adelante el Instituto, ha existido una limitada supervisión por parte de los entes fiscalizadores en materia de tecnologías de la Información., esto derivado principalmente por un escaso recurso humano a lo interno de la Auditoria, por lo que para el periodo 2022 se decide contratar bajo la modalidad de servicios profesionales una consultoría, guía y/o acompañamiento para el diagnóstico de todos los sistemas informáticos y de comunicación en producción del INAMU., con el propósito de obtener información suficiente y competente en tres ejes principales a saber:

A. Realizar un diagnóstico del alineamiento del Plan Estratégico de TI y el Plan Estratégico Institucional, sus políticas y el mapeo de los riesgos de la Unidad de Informática emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

B. Realizar un diagnóstico de la seguridad física y lógica para determinar fuentes de amenazas a los sistemas informáticos y de comunicación en producción del INAMU., emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

C. Realizar el levantamiento y diagnóstico de todos y cada uno de los sistemas informáticos y de comunicación en producción del INAMU., el diagnostico debe determinar al menos el nivel de integración, estabilidad, obsolescencia, emitir las correspondientes conclusiones y recomendaciones mediante un informe final.

Dicha consultoría, guía y/o acompañamiento, será documentada mediante memorias, que dan sustento técnico a los hallazgos presentados y desarrollados en el presente informe.

2.1 ORIGEN DEL ESTUDIO

El presente estudio especial se realizó de conformidad con el artículo 20 de la Ley 7801 de Creación del Instituto Nacional de la Mujer[1], el artículo 21 y el 22 de la Ley 8292, Ley General de Control Interno[2], Normas para el Ejercicio de la Auditoría Interna en el Sector Público[3], Normas de Control Interno para el Sector Público[4] Normas Técnicas para la Gestión y el Control de las Tecnologías de Información5, Normas técnicas para la gestión y el control de las Tecnologías de Información 2021[6], EL Reglamento de Operación del Comité Institucional de Tecnología de la Información[7]. así como en cumplimiento del Plan de Trabajo Anual del año 2022 de la Auditoría Interna[8].

2.2 OBJETIVO DEL ESTUDIO

El objetivo general del estudio de carácter especial es evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte del INAMU, en su ambiente de tecnologías de información y obtener un informe sobre los aspectos observados que constituyan oportunidades de mejora en dichos procesos, así como las recomendaciones respectivas. Para la consecución del objetivo general del estudio fueron necesarios los siguientes objetivos específicos de auditoría:

I. *Revisar el marco de gestión de las tecnologías de información y comunicación del INAMU., en línea con la Deroga las normas técnicas para la gestión y el control de las tecnologías de información (N-2prue-2007-CO-DFOE), resolución N° R-CO-26-2007, y modifica las normas de control interno para el sector público.*

[1] Ley del 29 de abril de 1998 Publicada en La Gaceta No. 94 del 18 de mayo de 1998.
[2] Ley del 30 de julio de 2002 Publicada en La Gaceta No. 169 del 04 de setiembre de 2002.
[3] Publicada en La Gaceta n.º 28 de 10 de febrero de 2010
[4] Publicada en La Gaceta No. 26 del 06 de febrero del 2009
[5] Publicada en La Gaceta Nro.119 del 21 de junio, 2007. En el periodo 2015-2020 dichas normas se encontraban vigentes y eran de aplicación obligatoria, previo a ser derogadas a partir del 31 diciembre 2021.
[6] Normas técnicas para la gestión y el control de las Tecnologías de Información que sustituyen las Normas técnicas para la gestión y el control de las Tecnologías de Información (N2-2007-CODFOE) derogadas por la Contraloría General de la República mediante la resolución N° R-DC-17-2020 del diecisiete de marzo del dos mil veinte.
[7] Del 09 de noviembre de 2021 Publicado en la Gaceta 216
[8] Aprobado en el Acta 30-2021, del 18 de noviembre del 2021.

II. Revisión de las Políticas y lineamientos generales de TI.

III. Análisis de la Matriz del SEVRI de TI.

IV. Pruebas de seguridad física, Cuarto de Servidores Edificio SIGMA.

V. Pruebas selectivas de seguridad lógica.

VI. Análisis de la estructura de la UIN.

2.3 ALCANCE DEL ESTUDIO

El estudio es de carácter especial y tuvo como objetivo general evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte del INAMU en su ambiente de tecnologías de información y obtener un informe sobre los aspectos observados que constituyan oportunidades de mejora en dichos procesos y cualquier otro aspecto relevante según las buenas prácticas para las Tecnologías de información en el Sector Público.

2.4 METODOLOGÍA APLICADA

De conformidad con los criterios expuestos, la Auditoría Interna realizó un análisis y verificación de las políticas relacionadas con la seguridad física y lógica de aplicación por parte del INAMU, en su ambiente de tecnologías de información y la metodología para la identificación de riesgos, esto mediante distintas pruebas de cumplimiento y sustantivas, aunado a lo anterior, se aplicaron entrevistas y reuniones virtuales mediante la plataforma Teams con los titulares subordinados responsables de los procesos vinculados, a quienes se les realizaron consultas específicas, vía oficio y correo electrónico, de igual forma se trabajó en la verificación de datos mediante la aplicación de varios instrumentos, tales como: entrevistas, matrices de cumplimiento, cuadros comparativos, cuestionarios, entre otros.

2.5 COMUNICACIÓN PRELIMINAR DE LOS RESULTADOS DE LA AUDITORÍA INTERNA.

En cumplimiento de la norma 2.10 “Comunicación de los resultados” de las “Normas para el ejercicio de la auditoría interna en el Sector Público” y, de conformidad con la norma 205 del “Manual de normas generales de auditoría para el Sector Público”, que establecen que “Las instancias correspondientes deben ser informadas, verbalmente y por escrito, sobre los principales resultados, las conclusiones y las disposiciones o recomendaciones producto de la auditoría que se lleve a cabo…” y que “El auditor debe efectuar una conferencia final con la Administración de la entidad u órgano auditado, antes de emitir la respectiva comunicación por escrito”, el día jueves 12 de enero de 2023, se realizó dicha conferencia final mediante sesión presencial en la sala de sesiones de Junta Directiva, con la participación de la Sra. Adilia Caravaca Zuñiga -presidenta ejecutiva, la Sra. Alexandra Gomez Ruiz, personal apoyo del despacho, la Sra. Ingrid Trejos Marín, Jefatura de la Unidad de Informática, y por parte de la Auditoría Interna las Señoras: Klansy Flores Salguero y Dylanna Villalobos Guzmán y el Sr. Randall Umaña Villalobos, consideraron las observaciones expuestas por parte de los presentes.

2.6 IMPLANTACIÓN DE LAS RECOMENDACIONES DE LA AUDITORÍA INTERNA

La Ley N.º 8292 de Control Interno, en su Artículo 37. —Informes dirigidos al jerarca. establece lo siguiente:

> *“Cuando el informe de auditoría esté dirigido al jerarca, este deberá ordenar al titular subordinado que corresponda, en un plazo improrrogable de treinta días hábiles contados a partir de la fecha de recibido el informe, la implantación de las recomendaciones. Si discrepa de tales recomendaciones, dentro del plazo indicado deberá ordenar las soluciones alternas que motivadamente”*

En la misma Ley el Artículo 38. —Planteamiento de conflictos ante la Contraloría General de la República establece:

> *"Firme la resolución del jerarca que ordene soluciones distintas de las recomendadas por la auditoría interna, esta tendrá un plazo de quince días hábiles, contados a partir de su comunicación, para exponerle por escrito los motivos de su inconformidad con lo resuelto y para indicarle que el asunto en conflicto debe remitirse a la Contraloría General de la República, dentro de los ocho días hábiles siguientes, salvo que el jerarca se allane a las razones de inconformidad indicadas.*
>
> *La Contraloría General de la República dirimirá el conflicto en última instancia, a solicitud del jerarca, de la auditoría interna o de ambos, en un plazo de treinta días hábiles, una vez completado el expediente que se formará al efecto. El hecho de no ejecutar injustificadamente lo resuelto en firme por el órgano contralor, dará lugar a la aplicación de las sanciones previstas en el capítulo V de la Ley Orgánica de la Contraloría General de la República, N° 7428, de 7 de setiembre de 1994."*

En relación con lo anterior, la normativa promulgada por la Contraloría General de la República señala que el esquema de implementación de recomendaciones debe contener los planes y proyectos para las acciones correctivas que debe de incorporar, además, la definición de un plazo de referencia para el cumplimiento de la recomendación. En este sentido, el artículo 12 de la citada Ley N.º 8292 establece, respecto a los deberes del jerarca y de los titulares subordinados en el sistema de control interno, lo siguiente:

> ***"Artículo 12. —****Deberes del jerarca y de los titulares subordinados en el sistema de control interno. En materia de control interno, al jerarca y los titulares subordinados les corresponderá cumplir, entre otros, los siguientes deberes:*

a) Velar por el adecuado desarrollo de la actividad del ente o del órgano a su cargo.

b) Tomar de inmediato las medidas correctivas, ante cualquier evidencia de desviaciones o irregularidades.

c) Analizar e implantar, de inmediato, las observaciones, recomendaciones

d) y disposiciones formuladas por la auditoría interna, la Contraloría General de la República, la auditoría externa y las demás instituciones de control y fiscalización que correspondan.

e) Asegurarse de que los sistemas de control interno cumplan al menos con las características definidas en el artículo 7 de esta Ley.

f) Presentar un informe de fin de gestión y realizar la entrega formal del ente o el órgano a su sucesor, de acuerdo con las directrices emitidas por la Contraloría General de la República y por los entes y órganos competentes de la administración activa."

(El destacado no forma parte del texto original).

Por su parte, las "Normas para el ejercicio de la auditoría interna en el Sector Público" señalan en la norma 2.11 lo siguiente:

"El auditor interno debe establecer, mantener y velar porque se aplique un proceso de seguimiento de las recomendaciones, observaciones y demás resultados derivados de los servicios de la auditoría interna, para asegurarse de que las acciones establecidas por las instancias competentes se hayan implementado eficazmente y dentro de los plazos definidos por la administración. Ese proceso también debe contemplar los resultados conocidos por la auditoría interna, de estudios de auditores externos, la Contraloría General de la República y demás instituciones de control y fiscalización que correspondan". (…)

2.7 RIESGOS DE AUDITORÍA

La Auditoría Interna debido a la naturaleza de la labor que realiza se ve expuesta a los siguientes riegos:

Riesgo Inherente.

Es la susceptibilidad del saldo de una cuenta o clase de transacciones a una representación errónea que pudiera ser de importancia relativa, individualmente o cuando se agrega con representaciones erróneas en otras cuentas o clases, asumiendo que no hubo controles internos relacionados.

Riesgo de Control.

El riesgo de control es el riesgo de que una representación errónea, que pudiera ser de importancia relativa individualmente o en conjunto con otras, no sea prevenida o detectada y corregida oportunamente por los sistemas de contabilidad y de control interno.

Riesgo de Detección.

Este tipo de riesgo está directamente relacionado con los procedimientos de auditoría por lo que se trata de la posibilidad que existe en todo tipo de estudio, de no detectar la existencia de errores en el proceso realizado.

2.8 EQUIPO DE TRABAJO A CARGO DEL ESTUDIO

El trabajo de campo, la aplicación de los procedimientos de auditoría y la redacción del informe final de estudio estuvo a cargo del Sr. Carlos Morales Pacheco profesional en auditorias de tecnologías de la información y comunicación, subcontratado como

auditor de TI por parte de la Auditoría Interna, Sra. Klansy Flores Salguero profesional especialista del área como recurso de apoyo y la revisión final por parte del Sr. Randall Umaña Villalobos, Auditor Interno del INAMU.

2.9 GENERALIDADES DEL ESTUDIO

Con la entrada en vigor de la Ley 7801 de Creación del Instituto Nacional de la Mujer, se establece dentro de sus fines:

> a) Formular e impulsar la política nacional para la igualdad y equidad de género, en coordinación con las instituciones públicas, las instancias estatales que desarrollan programas para las mujeres y las organizaciones sociales.
>
> b) Proteger los derechos de la mujer consagrados tanto en declaraciones, convenciones y tratados internacionales como en el ordenamiento jurídico costarricense; promover la igualdad entre los géneros y propiciar acciones tendientes a mejorar la situación de la mujer.
>
> c) Coordinar y vigilar que las instituciones públicas establezcan y ejecuten las políticas nacionales, sociales y de desarrollo humano, así como las acciones sectoriales e institucionales de la política nacional para la igualdad y equidad de género.
>
> d) Propiciar la participación social, política, cultural y económica de las mujeres y el pleno goce de sus derechos humanos, en condiciones de igualdad y equidad con los hombres.

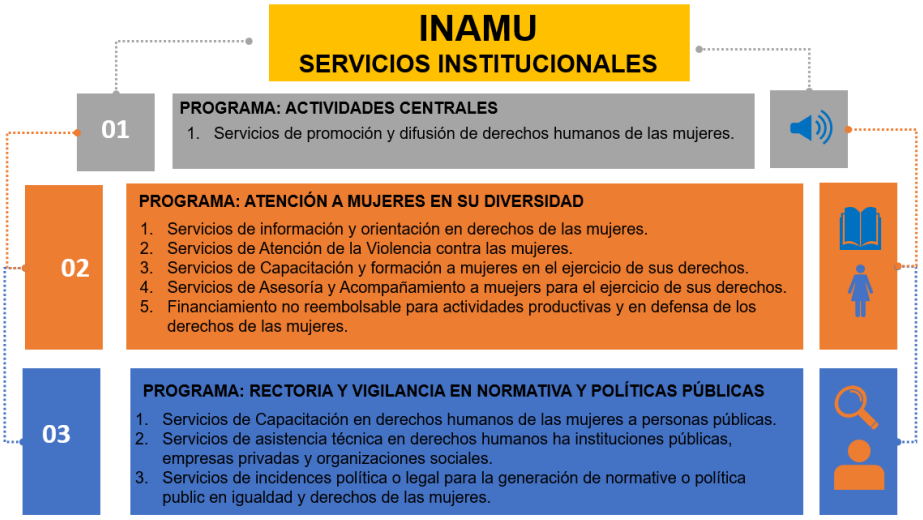
Además, la Institución tiene la obligación de velar por el cumplimiento de la Política Nacional para la Igualdad Efectiva entre Mujeres y Hombres en Costa Rica 2018-2030 la cual responde a los compromisos internacionales sobre derechos humanos y la igualdad efectiva, sustentado en la convencionalidad ratificadas por Costa Rica que protegen los derechos de las mujeres; en particular la Convención sobre la Eliminación de todas las Formas de Discriminación contra la Mujer (CEDAW, 1984)

y, en la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra las Mujeres (Convención Belem Do Pará, OEA 1994), así como las declaraciones, Acuerdos, Plataformas sobre la materia, y los Objetivos de Desarrollo Sostenible, que tiene como objetivo que nadie se quede atrás en el Desarrollo.

Además, la Política Nacional para la Atención y Prevención contra la Violencia hacia las Mujeres de Todas las Edades 2017-2032, la cual es consensuada a nivel interinstitucional e intersectorial, desde un enfoque de derechos humanos, en concordancia con lo que establece la Convención Interamericana para Prevenir, Sancionar y Erradicar la Violencia contra la Mujer (conocida como Convención de Belém do Pará).

Lo anterior se realiza mediante 9 servicios distribuidos en tres programas institucionales a saber:

IMAGEN 1.- Cartera de Servicios Institucionales del INAMU



Fuente: Elaborado por la Auditoría Interna, con los insumos de la Dirección Estratégica Circular DE-0027-2021 del 24\09\2021.

Derivado de los servicios públicos que brinda el INAMU., mantiene información y datos de terceros que debe gestionar de acuerdo con lo dispuesto en la Ley de Protección de la persona frente al tratamiento de sus datos Ley 89689, esto implica la implementación de mejores prácticas para crear y mantener un sistema de gestión de seguridad de la información, y la clasificación de la información como elemento determinante dentro de sus sistemas.

Dentro del contexto descrito, las tecnologías de la información y comunicación son herramientas que contribuyen a la Institución, suministrando trazabilidad a sus procesos, así como información sistematizada y confiable para la toma de decisiones y la rendición de cuentas, eso incluye planes de seguridad de la información que detallen cómo se implementa la seguridad, como se definen sus políticas, controles y soluciones.

El plan de seguridad de la información se desarrolla considerando todos los recursos de TI en función de los niveles de seguridad alcanzados y los aspectos pendientes por lo que la evaluación de las acciones relacionadas con la seguridad física y la seguridad lógica son sensibles para lograr niveles más altos de seguridad. **(Ver Conclusión 01)**

3 RESULTADOS DE LA AUDITORÍA.

El presente proyecto especial de auditoría se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2022, cuyo objetivo general fue evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte del INAMU en su ambiente de tecnologías de información y obtener un informe sobre los aspectos observados que constituyan oportunidades de mejora en dichos procesos y cualquier otro aspecto relevante.

[9] Publicada en La Gaceta n.º 170 de 05 de setiembre de 2011

3.1 HALLAZGO 01: Ausencia de un Marco de Gestión de Tecnologías de Información debidamente formalizado y comunicado.

Condición:

El INAMU, carece de un Marco de Gestión de Tecnologías de Información debidamente formalizado y comunicado como proceso orientador del gobierno y gestión de la tecnología de información en la Institución, alineado a la estrategia institucional, que garantiza un balance adecuado de las inversiones, la organización de recursos y actividades sustantivas, respetando la normativa institucional y nacional, basado en las buenas prácticas y ajustado al contexto, tamaño, naturaleza, restricciones y estrategia institucional.

Es importante evidenciar que la Sra. Ingrid Trejos Marín, en calidad de jefatura de la Unidad de Informática, presento ante la presidenta ejecutiva y la Junta Directiva del INAMU, el documento INAMU-UIN-CITI-0002-2021 de fecha 15 de diciembre de 2021, titulado Informe sobre derogatoria de Normas Técnicas para la Gestión y Control de las Tecnologías de Información y Plan de Acción a seguir, para contar con el nuevo marco de tecnologías de información para el INAMU, el cual detalla la ruta establecida para que el INAMU, a más tardar a diciembre 2022, cuente con un nuevo marco de gestión de tecnologías de información para la Institución, tal y como se detalla a continuación:

> *(…) Al respecto, con el visto bueno del Comité Institucional de Tecnologías de Información (sesión No. 9 del 20 de octubre del 2021, acuerdo No. 10) y con base en el Marco Normativo de Gobierno y Gestión de las Tecnologías de Información, emitido por la Dirección de Gobernanza Digital del MICITT, conforme oficio No. MICITT–DGD-OF-215-2021, el cual se anexa, (oficio de formalización de las nuevas normas técnicas de Tecnologías de Información, las cuales entrarán en vigor a partir del 1 de enero del 2022), la Unidad de Informática ha planificado y ha venido laborando en el siguiente plan de acción para la alineación con las Normas de Gestión Operativa Institucionales existentes y los nuevos lineamientos. Lo anterior, con el fin de logar contar a diciembre 2022, con u nuevo marco de gestión de tecnologías de información para la Institución, se adjunta el cronograma establecido. (…)*

De igual manera es necesario indicar que a la fecha del presente estudio, el INAMU, cuenta con los siguientes instrumentos regulatorios que son parte esencial de un marco de gestión de tecnologías de la Información:

a. Modelo de arquitectura institucional de Tecnologías de Información[10]
b. Políticas para la gestión Operativa de Tecnologías de Información.[11]
c. Metodología Proceso para la Gestión del Riesgo de TI y Seguridad de la Información.[12]

Si bien los instrumentos arriba citados, son parte fundamental de un marco de gestión de tecnologías de la información, no excluye o sustituye el citado "Marco" ya que este, tiene como objetivo principal el crear valor, a través de la obtención de beneficios, a un costo favorable, mientras se optimiza el riesgo, es decir, un conjunto de elementos tales como estructuras, procesos y mecanismos relacionados entre sí. Tal y como lo describe el Marco de referencia COBIT 2019 en sus Objetivos de Gobierno y Gestión.

> ***APO01.01 Diseñar el sistema de gestión para la I&T de la empresa***
>
> *Diseñar un sistema de gestión adaptado a las necesidades de la empresa. Las necesidades de gestión de la empresa se definen a través del uso de la cascada de metas y por la aplicación de factores de diseño. Hay que asegurar que los componentes de gobierno están integrados y alineados con el gobierno, la filosofía de gestión y estilo operativo de la empresa.*

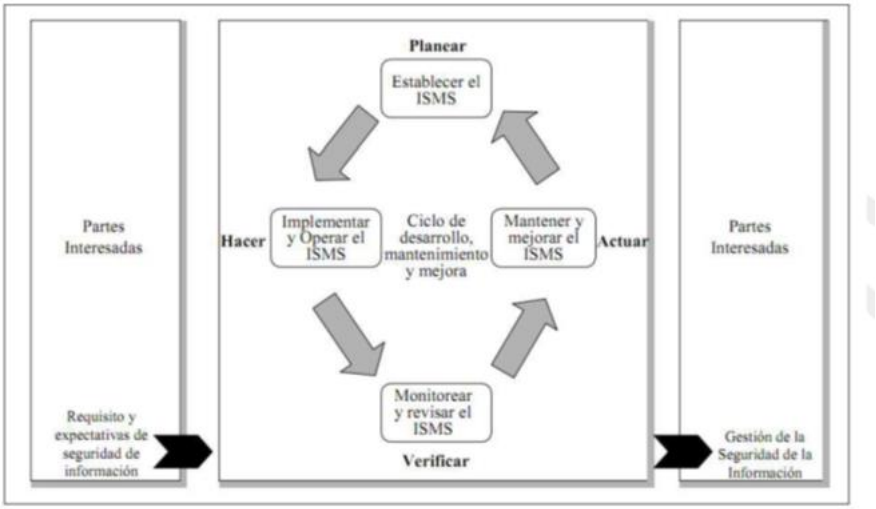
En la misma línea la familia ISO 27000 contiene un conjunto de buenas prácticas para el establecimiento, implementación, mantenimiento y mejora de Sistemas de Gestión de la Seguridad de la Información, en específico la ISO 27003, la cual es una guía de ayuda en la implementación de un Sistema de Gestión de Seguridad de la Información (SGSI), el cual sirve como apoyo a la norma 27001, indicando las directivas generales

[10] Formalizado mediante CIRCULAR INAMU-PE-0002-2022 PRESIDENCIA EJECUTIVA del 09 de marzo de 2022.
[11] Aprobado por Junta Directiva en Sesión Ordinaria No. 13-2014 del 2 de febrero del 2014.
[12] Memorando emitido por Presidencia Ejecutiva, INAMU-PE-0175-2020 de fecha 25 de marzo del 2020.

necesarias para la correcta implementación de un SGSI. Incluye instrucciones sobre cómo lograr la implementación de un SGSI con éxito.

Este sistema de gestión incluye la estructura organizacional, políticas, actividades de planificación, responsabilidades, practicas, procedimientos, procesos y recursos, basado en el modelo PDCA.

IMAGEN 2.- MODELO Plan (planificar), Do (hacer), Check (verificar) y Act/Adjust (actuar o ajustar).



Fuente: NTP 27001:2008

Por último, pero no menos importante las Normas técnicas para la gestión y el Control de las tecnologías de la información[13] del Ministerio de Ciencia, Innovación, Tecnologías y Telecomunicaciones (MICITT), indican que es responsabilidad de las instancias institucionales en materia de Tecnologías de Información y comunicaciones como ente rector dentro de la organización, el velar por la implementación y seguimiento del Marco Normativo para la aplicación de sanas prácticas y adecuar su realidad basándose en este documento como referencia, además señala que este Marco Normativo es de acatamiento obligatorio para las instituciones y órganos sujetos a la fiscalización de la Contraloría General de la

[13] Versión 2.0 del 08 de noviembre de 2022

República, y su inobservancia generará las responsabilidades que correspondan de conformidad con el marco jurídico que resulte aplicable.

(…)

"El máximo jerarca institucional, es responsable del establecimiento del Gobierno Corporativo que apoye y supervise la adecuada implementación de Marco Normativo y su gestión, por parte de la instancia competente en materia de I&T.

(…)

Las Normas técnicas para la gestión y el Control de las tecnologías de la información del MICITT, indican que, para asegurar la disponibilidad del Marco de Gestión de Tecnología de Información Institucional, la institución debe establecer los procesos al nivel de Tecnologías de información, que permitan brindar servicios efectivos para mantener la operativa institucional, salvaguardar los datos que se capturan, procesan, organizan, distribuyen y resguardan, para lo cual menciona al menos 15 procesos:

I. Gobernanza de TI
II. Gestión de TI
III. Planificación tecnológica Institucional.
IV. Gestión de Riesgos tecnológicos.
V. Arquitectura empresarial.
VI. Calidad de los procesos tecnológicos.
VII. Recursos humanos.
VIII. Contratación y adquisiciones de bienes y servicios tecnológicos.
IX. Gestión de Proyectos que implementan recursos tecnológicos.
X. Desarrollo, implementación y mantenimiento de sistemas de información.
XI. Seguridad y ciberseguridad.
XII. Administración Infraestructura tecnológica.
XIII. Continuidad y disponibilidad operativa de los servicios tecnológicos.
XIV. Aseguramiento.

Criterio:

Según resolución de la Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las

Tecnologías de Información, se decide, además de derogar las normas mencionadas, modificar los ítems 5.9 y 5.10 de las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE) incorporando los siguientes transitorios:

> *TRANSITORIO I.- Todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República* ***deberán haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación*** *requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), a más tardar el 1° de enero del 2022.*
>
> ***(Lo resaltado no forma parte del original)***

> *TRANSITORIO II. Tratándose de instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República, que —por el sector al que pertenecen— ya han declarado, aprobado y divulgado un marco de gestión de las tecnologías de información y comunicación, establecido por sí misma o por un órgano supervisor, se tendría por cumplido el Transitorio I de la presente resolución.*

Adicionalmente, se hace referencia a la Ley General de Control Interno, Ley 8292; al respecto, su artículo 16, relacionado con los sistemas de información, destaca la necesidad de armonizar estos sistemas con los objetivos institucionales y contar con información confiable, relevante, pertinente, oportuna y segura para el cuido y manejo de los recursos públicos.

Causa

Dentro de las principales causas identificadas, para que a la fecha el INAMU., carezca de un “Marco de gestión de las tecnologías de información y comunicación” como lo señala en la resolución de la Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información, es que la Institución, cuenta con un Instrumento denominado “Políticas para la gestión Operativa de Tecnologías de Información” el

cual es utilizado como marco de referencia, no obstante, este, no puede llegar a sustituir el “Marco de gestión de las tecnologías de información y comunicación”

Efecto:

La ausencia de un “Marco de gestión de las tecnologías de información y comunicación” debidamente declarado y aprobado, debilita el control interno institucional permitiendo dar una trazabilidad oportuna a sus procesos, así como obtener información sistematizada y confiable para la toma de decisiones y la rendición de cuentas, de acuerdo con las particularidades del INAMU.

Además de posibles incumplimientos por parte del INAMU., a lo regulado en la resolución de la Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información, dado que, la ausencia de un marco de gestión de TI de gobierno y gestión de las tecnologías de información es una limitante para que la institución logre orientar sus esfuerzos a la implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva, los servicios brindados a través del uso y administración de los recursos tecnológicos de forma tal que garanticen la continuidad de las operaciones institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. **(Ver Conclusión 02 y Recomendación 01).**

3.2 HALLAZGO 02: Ausencia de una política de clasificación de la información.

Condición:

Durante la revisión realizada a las “Políticas para la gestión Operativa de Tecnologías de Información” no se logró identificar ni ubicar la “Política relacionada con la Clasificación de los datos e información del INAMU”, la misma es un proceso en el

cual el INAMU, evalúa los datos que posee y el nivel de protección que cada uno requiere, se trata de uno de los aspectos más complejos, pero sin duda más sensibles, en la gestión de la seguridad de la información.

Criterio:

La Ley de protección de la persona frente al tratamiento de sus datos personales[14] ley 8968, establece en su Artículo- 9.- Categorías particulares de los datos- de la siguiente manera:

- ✓ ***Datos sensibles****: Ninguna persona estará obligada a suministrar datos sensibles. Se prohíbe el tratamiento de datos de carácter personal que revelen el origen racial o étnico, opiniones políticas, convicciones religiosas, espirituales o filosóficas, así como los relativos a la salud, la vida y la orientación sexual, entre otros.*
- ✓ ***Datos personales de acceso restringido:*** *Datos personales de acceso restringido son los que, aun formando parte de registros de acceso al público, no son de acceso irrestricto por ser de interés solo para su titular o para la Administración Pública. Su tratamiento será permitido únicamente para fines públicos o si se cuenta con el consentimiento expreso del titular.*
- ✓ ***Datos personales de acceso irrestricto:*** *Datos personales de acceso irrestricto son los contenidos en bases de datos públicas de acceso general, según lo dispongan las leyes especiales y de conformidad con la finalidad para la cual estos datos fueron recabados.*
- ✓ ***Datos referentes al comportamiento crediticio:*** *Los datos referentes al comportamiento crediticio se regirán por las normas que regulan el Sistema Financiero Nacional, de modo que permitan garantizar un grado de riesgo aceptable por parte de las entidades financieras, sin impedir el pleno ejercicio del derecho a la autodeterminación informativa ni exceder los límites de esta ley.*

En la misma línea la ISO 27001, cita: ‹‹*Las organizaciones que se toman en serio la protección de su información deben seguir las pautas establecidas en ISO 27001. La norma describe las mejores prácticas para crear y mantener un sistema de gestión de seguridad de la información, y la clasificación de la información, según ISO 27001 es un elemento determinante dentro de ese sistema.* ››

[14] Publicada en La Gaceta n.º 170 de 05 de setiembre de 2011

El objetivo de control A8.2 - Clasificación de la Información-

"Deben asegurarse de que la información reciba un nivel adecuado de protección".

El estándar no explica cómo hacerlo. Pero el proceso de clasificación de la información según ISO 27001 se puede llevar a cabo siguiendo estos cuatro pasos:

1. ***Ingresar activos en un inventario***

El primer paso es recopilar toda la información en un inventario, que denominamos registro de activos. También se debe tener en cuenta quién es responsable (quién lo posee) y en qué formato está (documentos electrónicos, bases de datos, documentos en papel, otros medios de almacenamiento, etc.).

2. ***Clasificar la información***

Los propietarios de los activos son responsables de ello, pero es una buena idea que la alta dirección proporcione pautas basadas en los resultados de la evaluación de riesgos de la organización.

La clasificación de la información según ISO 27001 sigue parámetros específicos. Las organizaciones, generalmente clasifican la información en términos de confidencialidad; es decir, según a quién se le otorga acceso a ella.

Un sistema típico, debería incluir cuatro niveles de confidencialidad:

- ✓ ***Confidencial:*** *acceso restringido a la alta dirección.*
- ✓ ***Restringido:*** *directores de área y empleados clave tienen acceso.*
- ✓ ***Interno:*** *relativo a la información accesible solo los miembros de la organización, pero en cualquier nivel.*
- ✓ ***Público:*** *todas las personas, dentro y fuera de la organización, tienen acceso.*

3. ***Etiquetar la información***

Una vez que se haya clasificado la información, el propietario del activo debe crear un ***sistema para etiquetarla****. Necesita diferentes procesos para la información que se almacena digital y físicamente, y debe ser lo más coherente y clara posible.*

4. Manejo de la información

Finalmente, se deben ***establecer reglas sobre cómo proteger cada información en función de su clasificación y formato****. Por ejemplo, puede decidirse que los documentos en papel internos deben colocarse en un gabinete desbloqueado en una parte de las instalaciones a la que todos los empleados puedan acceder. Mientras, los documentos restringidos podrían almacenarse en un gabinete cerrado.*

Causa

Una de las principales causas que se pueden determinar es la ausencia de sistema de clasificación de la información, tendiente a asegurar la confidencialidad, integridad y disponibilidad de la misma, donde la información se clasifica para señalar la necesidad, la prioridad y el grado de protección que ésta requiere, tomando en cuenta su valor, requerimientos legales y contractuales e importancia para el Instituto, esto sumado a la ausencia de un hilo conductor que articule y coordine entre las diferentes áreas, departamentos y/o procesos, para crear una política de clasificación de la información.

Efecto

Dentro de los principales riesgos de no contar con una política de clasificación de la información están:

- La institución cuenta con una Política de seguridad de la información poco efectiva, la cual carece de la identificación clara, precisa y oportuna de criterios que le permiten a la institución, garantizar la confidencialidad, integridad y disponibilidad de la información que se custodia.

- Además, no se identifican en dicha política, elementos esenciales a nivel institucional, tales como: el compromiso sobre la seguridad y protección física de una persona sea esta usuaria o funcionaria, el tipo de riesgos que se asumen ante la amenaza directa o indirecta a la vida o la salud, independientemente de la relación de la persona con la Institución (personal o

terceros), la potencial pérdida o violación de la privacidad, la discriminación, el daño a la reputación u otra desventaja social significativa, o cuando una persona interesada, podría verse privada de sus derechos y libertades o impedida de ejercer control sobre sus datos personales.

- Para el INAMU, la ausencia de una "Política de Clasificación de la Información" representa un efecto negativo hacia el compromiso sobre la operación y administración efectiva de la organización y sus diversas actividades, así como para la toma de decisiones internas libres e independientes y las investigaciones (internas); incumplimientos sobre la información cubierta por algún privilegio legal.

- La ausencia de la "Política de Clasificación de la Información" le imposibilita al INAMU, determinar el nivel de criticidad, confidencialidad, sensibilidad y seguridad de la información propiedad de éste y/o en su custodia, durante todo el ciclo de vida de esta incluyendo su creación, modificación, alteración, almacenamiento, transmisión y/o eliminación. La clasificación de la información determina el nivel al que la información debe ser controlada o asegurada y es indicativa del valor que la misma tiene como activo preferente del Instituto **(Ver Conclusión 03 y Recomendación 02).**

3.3 HALLAZGO 03: Necesidad de actualización de la Metodología y Proceso para la Gestión del Riesgo de TI y Seguridad de la Información.

Condición

Derivado de la revisión efectuada a la Metodología y proceso para la Gestión del Riesgo de TI y Seguridad de la Información, se determinó que la misma debe actualizarse ya que está enfocada en los riesgos más operativos relacionados con la pérdida debido a las deficiencias o fallas de los procesos, los recursos y los sistemas internos, o bien a causa de acontecimientos externos, como se muestra a continuación:

IMAGEN 3.- FRAP (Facilitated Risk Assessment Process)

	Probabilidad		Impacto	
Categoría Evaluada	**Inherente**	**Escala 1:3**		**Escala 1:5**
1. Políticas de seguridad de la información	2,33	1,00	15,44	1,00
2. Estructura organizativa	3,67	2,00	42,89	3,00
3. Recurso Humano	3,00	1,00	23,77	2,00
4. Control de Activos	3,78	2,00	39,71	2,00
5. Control de Acceso	3,29	1,00	53,43	3,00
6. Criptografía	4,00	2,00	49,26	3,00
7. Seguridad física y ambiental	3,56	2,00	61,52	4,00
8. Seguridad de las operaciones	3,58	2,00	73,28	4,00
9. Seguridad de las redes	3,36	2,00	97,79	5,00
10. Seguridad de las aplicaciones	3,43	2,00	89,46	5,00
11. Relación con los proveedores	1,00	1,00	75,00	4,00
12. Incidentes de seguridad	5,33	2,00	98,28	5,00
13. Planeación y recuperación ante desastres	4,55	2,00	99,75	5,00
14. Cumplimiento	3,33	2,00	100,00	5,00

Fuente: Herramienta SEVRTI-TI Unidad Informática INAMU

La metodología de valoración aplicada por la UIN denomina FRAP (Facilitated Risk Assessment Process), se basa en la aplicación de técnicas de gestión de riesgos usando metodologías formales cualitativas de análisis de riesgos y utilizando análisis de vulnerabilidad, análisis del impacto del riesgo, análisis de amenazas y cuestionarios. Las evaluaciones cualitativas como FRAP utilizan una escala de atributos de clasificación para describir la magnitud de las posibles consecuencias (por ejemplo, baja, media y alta) y la probabilidad de que esas consecuencias se produzcan.

Sin perjuicio de lo anterior, no se logró determinar que la Unidad de Informática identifique amenazas que imposibiliten la realización exitosa de la estrategia de tecnologías de la información, dificultades para la integración de soluciones, el uso de sistemas heredados ineficientes y un portafolio de inversiones en tecnologías no alineado o priorizados a la estrategia Institucional, como por ejemplo los riesgos identificados con el Hardware (Servidor), y el “SISTEMA DE EVENTOS DE ATENCIÓN NO INMEDIATA” (SEANI), el cual soporta el servicio tanto la Delegación de la Mujer y el Centro de Información y Orientación, respaldando la información de las personas usuarias que acceden a los servicios que estas unidades brindan, un Hardware (Servidor), y un aplicativo (SEANI), los cuales actualmente pertenecen al

Sistema de Emergencias 9-1-1, situación que puede exponer a INAMU a la materialización de riesgos relacionados con acceso no autorizado a información sensible, perdida de datos, interrupción de los servicios, que brindan las instancias que utilizan el aplicativo SEANI.

La situación descrita anteriormente fue ampliamente expuesta ante la Administración Activa mediante el documento INAMU-JD-AI-0129-2022 del 14 de octubre del 2022 con el asunto: "***SERVICIO PREVENTIVO SOBRE EL ESTADO DEL HARWARE Y SOFTWARE DEL SISTEMA DE EVENTOS DE ATENCIÓN NO INMEDIATA (SEANI) UTILIZADO EN LA UNIDAD DELEGACIÓN DE LA MUJER Y EL CENTRO OPERATIVO DE ATENCIÓN A LA VIOLENCIA INTRAFAMILIAR (COAVIF).***"

> *(…)*
> *Por consiguiente, el criterio imperante en nuestro régimen jurídico en lo concerniente al deber de mantener la integridad de los procesos de implementación y mantenimiento de software e infraestructura tecnológica y evitar el acceso no autorizado, daño o pérdida de información, además en garantizar la seguridad de los datos de carácter personal y evitar su alteración, destrucción accidental o ilícita, pérdida, tratamiento o acceso no autorizado es que se emite el siguiente servicio de* ***ADVERTENCIA*** *a la Presidencia Ejecutiva del INAMU, para que, de forma inmediata se inicien las siguientes gestiones:*

A. *Que se realicen las acciones legales para que el aplicativo SEANI (Sistema de Eventos de Atención No Inmediata) junto con sus códigos fuentes, pasen formalmente a formar parte de los activos tecnológicos del INAMU.*

B. *Que se realicen las acciones pertinentes para que el aplicativo SEANI (Sistema de Eventos de Atención No Inmediata), se aloje en un Hardware (servidor) del INAMU, y se administre de acuerdo con las políticas de seguridad física y lógica del INAMU.*

C. *Una vez alojado el aplicativo SEANI (Sistema de Eventos de Atención No Inmediata) en un Hardware (servidor) propiedad del INAMU, se requiere iniciar y documentar la viabilidad de que la base de datos alojada en la citada herramienta, pueda ser migrada a la solución tecnología en la cual se trabaja a nivel institucional para documentar la atención a personas usuarias, denominada: Sistema de Registro Único a Personas Usuarias (SISRUAP), la cual está en proceso de adjudicación a través de la plataforma SICOP (**procedimiento***

2022LA-000001-0015800001 Contratación para analizar, diseñar, desarrollar e implementar el sistema de Registro y Referencia Único de Atención a Personas usuarias de los servicios del INAMU*) por parte del INAMU.*

Se debe considerar que, si no fuera posible por determinado motivo, concretar la migración de la base de datos alojada en el sistema SEANI, se recomienda iniciar lo antes posible, con las medidas de contingencia que permitan a la institución, asegurar la continuidad de los servicios dados tanto por la Unidad Delegación de la Mujer como por el COAVIF.
(…)

A la luz de lo anterior, se torna sensible que la Institución establezca un proceso formal de gestión de riesgos de tecnológicos que no solo respondan a la operación, si no que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable, como, por ejemplo:

Riesgos regulatorios o de cumplimiento:
Las nuevas leyes tienen un impacto en las Instituciones, ya que pueden afectar a nuestro modelo de negocio, acarrear nuevas responsabilidades legales, requerir tecnologías innovadoras (lo que entronca con el riesgo al cambio digital).

Riesgo reputacional:
Se trata del conjunto de situaciones que aparecen y dañan a la imagen de la Institución, afectando a la percepción que tienen de nuestra organización actores importantes de los grupos de interés de nuestra entidad, como usuarias, clientes y empleados. Esa pérdida de renombre suele repercutir en una pérdida de confianza en la organización.

Riesgos de gobierno corporativo:
Malas prácticas de gobierno corporativo pueden suponer un riesgo para las Instituciones. En concreto, hay dos situaciones que pueden dañan mucho el buen gobierno corporativo. Nos referimos a la falta de transparencia en la gestión empresarial y a la incapacidad para determinar eficazmente la responsabilidad en la organización.

Criterio

Al tenor, fundamentalmente, de las Normas técnicas para la gestión y el control de las Tecnologías de Información 2021, las cuales indican:

> *(…)*
> ***GESTIÓN DE RIESGOS TECNOLÓGICOS***
> *La institución debe establecer un proceso formal de gestión de riesgos que responda a las amenazas que puedan afectar el logro de los objetivos institucionales, basado en una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considerando el Marco de Gestión de TI que le resulte aplicable.*
>
> *La Unidad de TI debe aplicar el marco de gestión de riesgo tecnológico, con el fin de identificar, valorar, priorizar y gestionar los riesgos al nivel de TI en cualquiera de sus escenarios, que impliquen una eventual afectación a la continuidad operacional, así como la integridad y confidencialidad de la información y el cumplimiento regulatorio de la institución.*
> *(…)*

Causa

Una de las principales causas de que la metodología de valoración aplicada por la Unidad de Informática denomina FRAP (Facilitated Risk Assessment Process), contemple principalmente la gestión de riesgos operativos, está en la ausencia de actualización del SEVRI Institucional el cual data del 2013, esto sumado a la no integración formal de ambas metodologías en un proceso sistemático para estimar la magnitud de los riesgos a los que se encuentra expuesta la Institución.

Efecto

La situación descrita anterior limita el establecer criterios para la gestión de riesgo tecnológico, ya que algunos fallos y amenazas pueden afectar severamente la seguridad y el desempeño Institucional, comprometiendo en muchos casos, su reputación, el cumplimiento normativo entre otros riesgos más allá de los operativos. **(Ver Conclusión 04 y recomendación 03).**

3.4 HALLAZGO 04: Rezago de las recomendaciones emitidas por las Auditorías Externas con respecto a la Seguridad Física del Cuarto de Servidores INAMU – EDIFICIO SIGMA.

Condición

Como parte integral de las pruebas realizadas a la seguridad física del cuarto de servidores del INAMU, ubicado en el tercer piso del Edificio Sigma, se determinó un rezago importante en el cumplimiento de las recomendaciones emitidas por las auditorías externas durante el periodo 2019 al 2020 relacionas con las ventanas, puertas y el monitoreo, estas situaciones han sido clasificadas con un nivel de riesgo “no aceptado” por parte de los entes fiscalizadores, como se indica a continuación:

- ***CARTA DE GERENCIA CG-TI 2019. ESPACHO CARVAJAL & COLEGIADOSCONTADORES PÚBLICOS AUTORIZADOS***

  HALLAZGO 10: *DEBILIDADES ENCONTRADAS EN LA SEGURIDAD FÍSICA DEL CUARTO DE SERVIDORES DEL INAMU.* ***RIESGO ALTO.***

  a) Con respecto a las ventanas en el cuarto de servidores:

  Se comprobó que existen ventanas en las paredes del cuarto de servidores, una pared limita al pasillo del edificio, y la otra pared limita con la Unidad de Informática. Por lo que se corre el peligro, de que las ventanas se quiebren y el cuarto de servidores quede expuesto. (…)

  b) Con respecto a la puerta principal del cuarto de servidores:

  Se comprueba que la puerta principal del cuarto de servidores corresponde a una puerta de vidrio. Cabe destacar que la Unidad de Informática cuenta con un llavín electrónico para controlar el ingreso al Data Center, donde se puede configurar las políticas de ingreso al cuarto de servidores.

c) *Con respecto al monitoreo de los ingresos al Cuarto de Servidores:*

Se determinó que el INAMU no cuenta con cámaras de seguridad dentro del cuarto de servidores que permitan monitorear las acciones realizadas por las personas internas o externas a la Institución que por algún motivo tenga acceso al cuarto de servidores.

- **CARTA DE TECNOLOGÍA DE INFORMACIÓNAL 31DE DICIEMBREDE 2021 CROWE HORWATH CR, S.A.**

E.13- CG-TI-2019- Observación # 24 del estudio seguimiento de observaciones y recomendaciones del periodo 2020 de la Unidad de Informática - Debilidades encontradas en la seguridad física del cuarto de servidores del INAMU.

Subsanar los siguientes aspectos referentes al cuarto de servidores:

a. *Aumentar la seguridad en la puerta del cuarto de servidores, ya que actualmente la puerta del cuarto de servidores es una puerta de vidrio y el cuarto de servidores puede quedar expuesto si se logra forzar o quebrar la puerta.*
b. *Eliminar las ventanas de vidrio de las paredes del cuarto de servidores, ya que están propensas a quebrarse y dejar expuestos los equipos que se encuentran dentro de este.*
c. *También se puede considerar reforzar las paredes de vidrio con algún material dentro del cuarto de servidores, que permita cerrar y aislar el sitio del pasillo y las oficinas colindantes.*

Nota: Se puede valorar la opción de mover o cambiar de lugar el cuarto de servidores, reestructurando las oficinas cercanas al cuarto de servidores, para que no esté colindando con el pasillo general del edificio.

d. *Instalar un sistema de vigilancia o monitoreo en el interior del cuarto de servidores, que permita monitorear las acciones que se realizan en el cuarto de servidores por colaboradores o externos de la Institución.*

Comentario de la Administración:

Se adjunta el informe de la Auditoría Externa 2019 denominado "CG-TI 2019 INAMU", donde se evidencia que la Dirección Administrativa no va a brindar ningún presupuesto y tampoco va a realizar ningún cambio físico al Centro de Datos respectivo para subsanar este hallazgo.

Para el 2022 no se descarta el traslado de las oficinas centrales del INAMU, por consiguiente, no se puede realizar ninguna erogación de este tipo en inmuebles actual que es arrendado.

(…)

Dentro de los aspectos expuestos por la firma de Auditoría Externa sobre este mismo tema, se muestra la evaluación de algunos elementos relacionados con calificación aceptable:

- ✓ El cuarto cuenta con instalación eléctrica y cajas de interruptores.
- ✓ Cableado estructurado.
- ✓ Planta eléctrica y UPS de respaldo eléctrico para equipos.
- ✓ Detectores de humo y temperatura.
- ✓ Aires acondicionados y de soporte.
- ✓ Extintores.
- ✓ Bitácora de acceso

Criterio

Las Normas técnicas para la gestión y el control de las Tecnologías de Información 2021, del MICITT., establece en su numeral XI. SEGURIDAD Y CIBERSEGURIDAD:

(…)

La Institución debe propiciar un ambiente seguro, considerando la seguridad física y ambiental como un componente básico en el esquema de protección requerido para prevenir el acceso físico no autorizado, daños e interferencia a la información y los activos de información de la institución.

(…)

Adicionalmente la Norma ISO-27001, en el objetivo de control y controles de su Anexo A, apartado A.9 “Seguridad física y ambiental” indica:

> *A.9.1.1 Perímetro de Control Seguridad física*
>
> *Control: Se deben de utilizar perímetros de seguridad (Barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.*
>
> *A.9.1.2 Controles de entrada físicos*
>
> *Control: Se deben proteger las áreas seguras mediante controles de entradas apropiados para asegurar que* sólo *se permita el acceso al personal autorizado*

Causa

Como se muestra en la *CARTA DE TECNOLOGÍA DE INFORMACIÓN DEL 31 DE DICIEMBREDE 2021*, suscrita por CROWE HORWATH CR, S.A. las inconsistencias relacionadas con la seguridad fisca del cuarto de servidores del INAMU Edificio Sigma., se mantienen desde el 2019, y lo clasifican como “Riesgo Inaceptable” no obstante, la Administración Activa una vez analizado y cuantificado estos riesgos, así como el impacto que tienen en los planes estratégicos y operativos, tomo la decisión de aceptar y asumir las posibles consecuencias y probabilidad de estos riesgos en particular, sin adelantar acciones de reducción, control o mitigación.

Las estrategias dentro de un plan de respuesta a riesgos tienen que ver básicamente con el apetito de riesgo de la organización, esto lo que significa es que, algunas instituciones prefieren “digerir” algunas cosas y otras no, ya sea por su naturaleza, por el sector económico en el que se desenvuelvan o sencillamente por su política de negocios, pueden estar dispuestas a “vivir en el peligro” es por ello por lo que, cuando usamos como estratégica: el aceptar el riesgo, se trata de no hacer nada. simplemente, sabemos que no tenemos como evitarlo y debemos convivir con él. Las organizaciones deciden aceptar un riesgo, cuando este es de muy baja probabilidad de ocurrencia.

En línea con lo anterior, y la estrategia de la Administración Activa del INAMU, de aceptar las recomendaciones emitidas por los entes fiscalizadores externos, pero no realizar las gestiones necesarias para su debida implantación e implementación, derivan en posibles incumplimientos tanto normativos como regulativos, como un aumento en las amenazas relacionadas con la seguridad e integridad de la información y de los componentes que integran el centro de datos. **(Ver conclusión 05 y Recomendación 04.)**

3.5 HALLAZGO 05: Sobre la seguridad lógica y ciberseguridad

3.5.1 Seguridad lógica.

Condición:

En las acciones de inspecciones realizadas a la infraestructura de la red de datos, a la revisión documental aportada, se determinó un rezago en el diseño e implementación del Plan de Seguridad de la Información.

Calificación del impacto				
Crítico	Alto	Medio	Bajo	Informativo
☑				

Un Plan de Seguridad de la Información se diseña para proteger la información y datos críticos de una institución; esto se realiza para salvaguardar los recursos organizacionales de una amplia gama de amenazas (tanto físicas como virtuales) de forma que se pueda garantizar la continuidad del negocio, minimizar los riesgos, maximizar el retorno de las inversiones y las oportunidades de negocio.

La seguridad de la tecnología de la información (TI) se logra mediante la implementación de un conjunto adecuado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizativas y funciones de software y hardware. Estos controles deben establecerse, aplicarse, supervisarse, revisarse y mejorarse cuando sea necesario, para garantizar que la seguridad específica de la organización y cumplir con el logro de los objetivos institucionales.

Mediante el oficio INAMU-PE-DAF-0593-2021, del 05 de Noviembre de 2021, donde las acciones específicas a nombre de la Dirección Administrativa Financiera dentro de las “Propuestas de Mejora Plan de Acción de Tecnologías de Información 2020-2023” indican que la atención del riesgo de compromiso de los equipos de hardware para el procesamiento de la información en el centro de datos y/o pérdida de servicios esenciales (electricidad, conectividad), tiene fecha de implementación el 30/12/2023; y la estrategia que administraría el mencionado riesgo sería desarrollar un proyecto para implementar un plan de gestión de seguridad de la información a nivel institucional, roles e involucrados, políticas, procedimientos, proceso general de gestión de la seguridad a nivel institucional.

IMAGEN 4.- “Propuestas de Mejora Plan de Acción de Tecnologías Información 2020-2023”

Nº. RIESGO	EVENTO	DETALLE DE LA ESTRATEGIA (medida de mejora)	FECHA DE IMPLEMENTACIÓN	PRODUCTO FINAL	RESPONSABLE DE IMPLEMENTACIÓN
1	1_Riesgo de pérdida de información y de la operativa de TI y por tanto afectación a la operación de la institución.	1.1_Implementar un proceso de gestión de continuidad institucional conformando un equipo de trabajo multidisciplinario, elaborando un plan de continuidad de los servicios de INAMU.	30/12/2022		_Dirección Administrativa
		1.3_Ejecutar un proceso de análisis de impacto a los procesos de negocio	30/12/2022		_Dirección Administrativa
3	3_Riesgo de compromiso de los equipos de hardware para el procesamiento de la información en el centro de datos y/o pérdida de servicios esenciales (electricidad, conectividad)	2.1_Desarrollar un proyecto para implementar un plan de gestión de seguridad de la información a nivel institucional, roles e involucrados, políticas, procedimientos, proceso general de gestión de la seguridad a nivel institucional.	30/12/2023		_Dirección Administrativa
5	5_Riesgo de escucha o interferencia que compromete la información y su integridad	5.1_Proyecto de clasificación de la información institucional basado en las actividades de cada dependencia.	29/01/2021		_Dirección Administrativa _Dirección Estratégica

Fuente: Oficio INAMU-PE-DAF-0593-2021

La situación mencionada indica el INAMU, no cuenta con un Plan de Seguridad de la Información ya que el mismo se tendría previsto implementar para el 30/12/2023. Esto se comprueba al no recibirse los informes de avance de las actividades realizadas por el equipo técnico encargado del diseño e implementación de dicho plan, los cuales fueron solicitados mediante el oficio INAMU-JD-AI-104-2022 del 4 de agosto del 2022.

Criterio

Al respecto, las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE) de la Contraloría General de la República, en referencia a la Seguridad, el enunciado 5.7.4 establecen:

> *"Deben instaurarse los controles que aseguren que la información que se comunica resguarde sus características propias de calidad, y sea trasladada bajo las condiciones de protección apropiadas, según su grado de sensibilidad y confidencialidad. Así también, que garanticen razonablemente su disponibilidad y acceso por parte de los distintos usuarios en la oportunidad y con la prontitud que la requieran."*

Por otra parte, las Directrices Generales para el establecimiento y funcionamiento del Sistema Específico de Valoración del Riesgo Institucional (SEVRI) (D-3-2005-CO-DFOE) de la Contraloría General de la República, en referencia a la Revisión de riesgo, el enunciado 4.6 establece:

> *En relación con los riesgos identificados, se deberá dar seguimiento, al menos, a:*
>
> *a) el nivel de riesgo;*
>
> *b) los factores de riesgo;*
>
> *c) el grado de ejecución de las medidas para la administración de riesgos;*
>
> *d) la eficacia y la eficiencia de las medidas para la administración de riesgos ejecutadas.*

La revisión de riesgos deberá ejecutarse de forma continua y la información que se genere en esta actividad deberá servir de insumo para:

a) elaborar los reportes del SEVRI;

b) ajustar de forma continua las medidas para la administración de riesgos; y

c) evaluar y ajustar los objetivos y metas institucionales.

Causa

A criterio de esta Auditoría, esta situación se podría estar dando debido a que el tema de la seguridad de la información no ha sido visto como un asunto estratégico a nivel organizacional y por tanto no ha contado con el tiempo y los recursos suficientes para su despliegue.

Efecto

La integridad de la situación planteada conlleva a la eventual exposición del INAMU a vulnerabilidades frente a ataques o una reacción limitada para afrontarlos. Algunas formas en que se dan estos ataques malintencionados son: denegación de servicios, escaneos, ingeniería social, entre otros. Por ende, se expone la institución a ser víctima del robo o secuestro de la información sensible por no contar con un marco robusto que muestre la ruta de implementación y medición en los temas de Seguridad de la Información.

La ausencia de un Plan de seguridad de la Información en el INAMU, debidamente declarado, aprobado y divulgado, limita el establecimiento de las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información. Para ello debe: **(Ver conclusión 06 y Recomendación 05.)**

"a. Implementar los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información.

b. Establecer procedimientos para proteger la información almacenada en cualquier tipo de medio fijo o removible (papel, cintas, discos, otros medios), incluso los relativos al manejo y desecho de esos medios.

c. Establecer medidas preventivas y correctivas con respecto a software "malicioso" o virus.

3.5.2 Sobre la Ciberseguridad y la Estructura organizativa de la UIN.

Condición

Los controles de ciberseguridad son un subconjunto de la seguridad de información que involucra las actividades desarrolladas por el negocio amparado en tecnología de información, que suele ser administrado por TI, y que permite mitigar una serie de riesgos que enfrenta la infraestructura tecnológica desde el punto de vista de su diseño y operación. Estos controles en la mayoría de los casos son configurables y funcionan de manera automatizada para prevenir ataques, intrusiones, disrupciones en el servicio, pérdida o fuga de información, etc. En buena medida dependen de dispositivos (equipo computacional como firewalls, switches, servidores, etc.) así como de software especializado como sistemas para la detección y la prevención de intrusos, prevención de pérdida de datos, antimalware, herramientas de virtualización, gestión de bases de datos entre muchos otros, no obstante, se requiere de personal altamente capacitado y motivado.

La estructura de la Unidad de Informática se compone de seis plazas a saber:

- 1 jefe de Unidad
- 2 profesional Especialistas
- 3 profesional Operativo 2

Una de las plazas de los Profesionales Especialistas tiene la condición de "interina" desde hace 4 años; mientras que la otra plaza de Profesional Especialista está cedida al Despacho de la Presidencia, en calidad de préstamo hasta el 2026. Dos de las

plazas de profesionales operativos 2 tienen la propiedad del cargo, mientras que la tercer plaza está interina hasta que se resuelva la situación del préstamo de la plaza, si se hace un análisis de las necesidades actuales con respecto al funcionamiento de los sistemas y equipos informáticos con los que cuenta la institución, los avances tecnológicos, amenazas y vulnerabilidad se puede identificar que, no se cuenta con recurso humano suficiente para llevar a cabo las funciones de una forma eficiente.

Lo anterior sumado a una escaza o nula presupuestación de recursos financieros para capacitación a nivel institucional, afectando con ello la actualización profesional y aumentando el riesgo de amenazas en temas se seguridad y ciberseguridad.

Criterio

Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007- CO-DFOE, establece en el artículo 2.4 lo siguiente:

> *"El jerarca debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada,* ***suficiente, competente*** *y a la que se la haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones". (Lo resaltado no es parte del original)*

En la misma línea las Normas técnicas para la gestión y el control de las Tecnologías de Información 2021 del MICITT, apartado XI- Seguridad y Ciberseguridad señala:

> *(…)*
>
> *La Unidad de TI debe establecer un plan efectivo de capacitación, formación y actualización tecnológica para los funcionarios que se destaquen en este ámbito, el mismo debe contemplar la participación o involucramiento de los usuarios finales, dueños de procesos y responsables de los diferentes procesos y servicios institucionales.*

Causa

El no contar con todas las plazas autorizadas para la UIN, de forma permanente, sumado a la ausencia de un plan de capacitación y concientización en materia de ciberseguridad, limita la capacitad de respuesta de la UIN y del INAMU, ante posibles ataques de incidentes de seguridad, de acuerdo con los lineamientos institucionales y los objetivos estratégicos de TI.

Efecto

La ciberseguridad impacta los tres principios básicos de la seguridad, en ese sentido, la ausencia de controles de cifrado incide sobre la confidencialidad de la información, lo cual también aplica para la suspensión de acceso por inactividad, mientras que la ausencia de controles sobre vulnerabilidades conocidas pone en riesgo la disponibilidad de los sistemas y servicios. En esa misma línea, la ausencia de controles sobre los dispositivos móviles expone a la información contenida, a pérdida de confidencialidad e integridad.

Los constantes avances tecnológicos hace que la UIN del INAMU, se convierta cada vez más en pilar fundamental para el buen funcionamiento de estas, por lo tanto se le debe dar un buen grado de importancia al establecimiento de una estructura organizativa de esta Unidad, tomando en cuenta aspectos fundamentales como la administración de los proyectos, los cuales van de la mano con todo el quehacer de los servicios institucionales, además la Seguridad que se debe implementar a nivel físico y lógico. **(Ver conclusión 07 y recomendación 06)**

3.5.3 Continuidad de los servicios para la generación de valor público en el INAMU.

Condición:

El sistema de gestión de la continuidad del negocio del INAMU, fue actualizado por última vez en el 2017, pero la Institución carece de la fase de Análisis de Impacto del Negocio (BIA), por sus siglas en inglés (Bussiness Impact Analysis) como parte del

plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas. Además, la Institución cuenta con una serie de instrumentos que permiten responder a posibles eventos que pueden afectar, de manera parcial o total, su continuidad operativa, entre ellos:

- El Plan de Recuperación ante Desastres (DRP)
- El Protocolo de continuidad de almacenamiento.
- El Protocolo de continuidad de las bases de datos.
- El Protocolo de continuidad de servidores.
- El Protocolo de continuidad del centro de datos.
- El Protocolo de continuidad del equipo de red, y
- El Protocolo de continuidad del servicio de TI.

Como parte de las pruebas realizadas a la gestión de continuidad de los servicios que brinda el INAMU, se verifico el proceso de respaldo de los siguientes sistemas: SIMAPU, SINIRUBE Y BOSH-T obteniendo resultados satisfactorios:

Criterio

Normas técnicas para la gestión y el control de las Tecnologías de Información 2021 en su numeral XIII. CONTINUIDAD Y DISPONIBILIDAD OPERATIVA DE LOS SERVICIOS TECNOLÓGICOS, establece:

> *(…)*
>
> *La institución debe establecer formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.*

Causa

La ausencia de una metodología formalmente aprobada que le permita a la Administración el análisis de impacto del negocio, y que este alineado con el Plan General de Continuidad del Negocio de la Entidad; que contenga la gestión de los objetivos globales de la INAMU, con respecto a las dimensiones de disponibilidad de datos, infraestructura tecnológica y recurso humano, es de las principales limitantes para que el INAMU, cuente el BIA (Bussiness Impact Analysis).

Efecto

La carencia de un proceso de Análisis de Impacto negocio (BIA) limita al INAMU, el poder monitorear y reconocer las amenazas más importantes de incidentes que afecten la normal operatividad de los servicios y los sistemas, de tal manera que se debe garantizar la continuidad del negocio a través de mecanismos de recuperación previamente probados y ajustados y que respondan en el menor tiempo posible a las soluciones de los problemas de interrupción generados.

El Plan de continuidad del negocio, se conforma de un conjunto de directrices y procedimientos plasmados en un documento técnico, para que cada institución de acuerdo con sus particularidades pueda tomar las acciones pertinentes con miras a la recuperación y restablecimiento de los servicios e infraestructuras de TI interrumpidas por situaciones de desastre o emergencias ocurridas en cualquier instante dentro de las organizaciones. El análisis de impacto del negocio como parte del plan de continuidad del negocio, debe entenderse como un marco conceptual sobre el cual las entidades deben planear integralmente los alcances y objetivos, que permiten proteger la información, en todas sus áreas críticas. **(Ver conclusión 08 y recomendación 07)**

4 CONCLUSIONES.

La Auditoría Interna, realizó el presente estudio con el objetivo de evaluar los aspectos referentes a la seguridad física y lógica de aplicación por parte del INAMU en su ambiente de tecnologías de información y obtener un informe sobre los aspectos

observados que constituyan oportunidades de mejora en dichos procesos, para lo cual presentamos las siguientes conclusiones:

CONCLUSIÓN N ° 01.

A la fecha del presente estudio el INAMU, mediante su Dirección Estratégica a identificado y mapeado nueve servicios que brinda a las mujeres en toda su diversidad, derivado de los servicios públicos que brinda la Institución, mantiene información y datos de terceras que debe gestionar de acuerdo con lo dispuesto en la Ley de Protección de la persona frente al tratamiento de sus datos Ley 8968, esto implica la implementación de mejores prácticas para crear y mantener un sistema de gestión de seguridad de la información, y la clasificación de la información como elemento determinante dentro de sus sistemas.

Dentro del contexto descrito, las tecnologías de la información y comunicación son herramientas que contribuyen a la Institución, suministrando trazabilidad a sus procesos, así como información sistematizada y confiable para la toma de decisiones y la rendición de cuentas, eso incluye planes de seguridad de la información que detallen cómo se implementa la seguridad, políticas definidas, controles y soluciones.

CONCLUSIÓN N ° 02.

La Auditoría Interna detecto posibles incumplimientos por parte del INAMU., a lo regulado en la resolución de la Contraloría General de la República número R-DC-17-2020 sobre la Derogatoria de las Normas técnicas para la gestión y el control de las Tecnologías de Información, esto originado a la ausencia de gestiones para formalizar y comunicar el nuevo marco de gestión de TI de gobierno y gestión de las tecnologías de información como instrumento de implementación de buenas prácticas que permiten la adecuada gestión de los procesos requeridos para brindar de forma oportuna y efectiva, los servicios brindados a través del uso y administración de los recursos tecnológicos, de forma tal que, garanticen la continuidad de las operaciones

institucionales, la salvaguarda de la información gestionada, la entrega de valor y el cumplimiento normativo. **(Ver Recomendación 01)**

CONCLUSIÓN N ° 03.

El INAMU carece de una “Política de Clasificación de la Información” que le permita determinar el nivel de criticidad, confidencialidad, sensibilidad y seguridad de la información propiedad de éste y/o en su custodia, durante todo el ciclo de vida de esta incluyendo su creación, modificación, alteración, almacenamiento, transmisión y/o eliminación. La clasificación de la información determina el nivel al que la información debe ser controlada o asegurada y es indicativa del valor que la misma tiene como activo preferente del Instituto **(Ver Recomendación 02)**

CONCLUSIÓN N ° 04.

Derivado de la revisión realizada por parte de la Auditoría Interna se concluye la necesidad que tiene la Institución, de que la Unidad de Informática actualice de forma continua y permanente la Metodología y Proceso para la Gestión del Riesgo de TI y Seguridad de la Información, con el propósito de que se gestionen riesgos relacionados con temas regulatorios o de cumplimiento, amenazas con temas reputacionales y de gobierno corporativo y otros emergentes, con el objetivo que situaciones como las presentadas con el aplicativo denominado SEANI (**Sistema de Eventos de Atención No Inmediata).** **(Ver Recomendación 03)**

CONCLUSIÓN N ° 05.

La Auditoría Interna Como parte integral de las pruebas realizadas a la seguridad física del cuarto de servidores del INAMU, ubicado en el tercer piso del Edificio Sigma., determinó un rezago importante en el cumplimiento de las recomendaciones emitidas por las auditorías externas durante el periodo 2019 al 2020 relacionas con las ventanas,

puertas y el monitoreo, estas situaciones han sido clasificadas con un nivel de riesgo “no aceptado” lo anterior deriva en un posible aumento de las amenazas relacionadas con la seguridad e integridad de la información, los componentes que integran el centro de datos y la continuidad del negocio. **(Ver Recomendación 04).**

CONCLUSIÓN N ° 06

La ausencia de un Plan de seguridad de la Información en el INAMU., debidamente declarado, aprobado y divulgado, limita el establecimiento las medidas de seguridad relacionadas con la operación de los recursos de TI y las comunicaciones, minimizar su riesgo de fallas y proteger la integridad del software y de la información, como por ejemplo la Implementación de los mecanismos de control que permitan asegurar la no negación, la autenticidad, la integridad y la confidencialidad de las transacciones y de la transferencia o intercambio de información entre otros. **(Ver Recomendación 05).**

CONCLUSIÓN N ° 07

Los constantes avances tecnológicos hacen que la UIN del INAMU, se convierta cada vez más en pilar fundamental para el buen funcionamiento institucional, por lo tanto se le debe dar el grado de importancia que amerita el debido establecimiento de su estructura organizativa, optimizando los recursos humanos asignados a dicha unidad operativa, tomando en cuenta aspectos fundamentales como la administración de los proyectos, los cuales van de la mano con todo el quehacer de los servicios institucionales, además la seguridad que se debe implementar a nivel físico y lógico. **(Ver Recomendación 06).**

CONCLUSIÓN N ° 08

El sistema de gestión de la continuidad del negocio del INAMU., fue actualizado por última vez en el 2017, por lo tanto, el Análisis de Impacto del Negocio (BIA) Bussiness Impact Analysis) que forma parte fundamental del plan de continuidad del negocio del

INAMU, puede que no respondan a las necesidades actuales del Instituto, esto aumenta el riesgo que la Institución no pueda proteger la información, en todas sus áreas críticas. **(Ver Recomendación 07).**

5 RECOMENDACIONES

De conformidad con las competencias asignadas en los artículos 21 y 22 de la Ley N.º 8292, Ley General de Control Interno, se emiten las siguientes recomendaciones y/o oportunidades de mejora, las cuales, una vez aceptadas por la Administración Activa, deberán ser cumplidas dentro del plazo meta establecido.

En adición a lo anterior, deberá observarse lo establecido en el punto N.º 2.6, de este informe sobre la implantación de las recomendaciones de la auditoría interna en apego a lo señalado en la Ley N.º 8292, Ley General de Control Interno.

A LA JEFATURA DE LA UNIDAD DE INFORMATICA.

RECOMENDACIÓN N°.01

En un máximo de sesenta (60) días naturales, realizar las gestiones necesarias para que de acuerdo con lo regulado en la resolución N° R-CO-26-2007, y el transitorio I, el INAMU cuente con un marco de gestión de las tecnologías de información y comunicación debidamente declarado, aprobado y divulgado esto en línea con las buenas prácticas y requerimientos institucionales (tamaño y complejidad de la institución, procesos críticos que se apoyan con las TI, riesgos asociados, entre otros).

Durante la revisión efectuada se determinó que existe una brecha entre lo indicado en el Transitorio I de en la resolución N° R-CO-26-2007, que indica: ‹‹*Todas las instituciones, entidades, órganos u otros sujetos pasivos de la fiscalización de la Contraloría General de la República deberán haber declarado, aprobado y divulgado el marco de gestión de las tecnologías de información y comunicación requerido en la modificación incorporada en esta resolución a las Normas de Control Interno para el Sector Público (N-2-2009-CODFOE), a más tardar el 1° de enero del 2022.*›› ya que el INAMU., cuenta con un instrumento denominado Políticas para la gestión Operativa de Tecnologías de Información, sin perjuicio de lo anterior, no se logra evidenciar que estas cumplan a cabalidad con lo que indican las Normas técnicas para la gestión y el control de las Tecnologías de Información 2021 del MICITT en su apartado PROCESOS DEL MARCO DE GESTIÓN DE TI.

La recomendación anterior tiene como objetivo validar el cumplimiento de la Derogatoria de las normas técnicas para la gestión y el control de las tecnologías de información (N-2-2007-CO-DFOE), resolución N° R-CO-26-2007, y modifica las normas de control interno para el sector público.

A LA PRESIDENCIA EJECUTIVA.

RECOMENDACIÓN N°.02

Girar las instrucciones a quien corresponda para que un plazo no mayor seis (6) meses, a partir de formalizada la presente recomendación, el INAMU cuente con una política de clasificación de la Información Institucional donde se establezcan las bases de un sistema de clasificación de la información Institucional, tendiente a asegurar la confidencialidad, integridad y disponibilidad de esta. La información debe clasificarse para señalar la necesidad, la prioridad y el grado de protección que ésta requiere, tomando en cuenta su valor, requerimientos legales y contractuales e importancia para el Instituto.

Durante la revisión realizada a las “Políticas para la gestión Operativa de Tecnologías de Información” no se logró ubicar la “Política relacionada con la Clasificación de los datos e información del INAMU”, la misma es un proceso en cual el INAMU evalúa los datos que posee y el nivel de protección que cada uno requiere, se trata de uno de los aspectos más complejos, pero sin duda más sensibles, en la gestión de la seguridad de la información.

La implementación de la presente recomendación tiene como objetivo, cumplir con lo normado en la Ley de protección de la persona frente al tratamiento de sus datos personales Ley 8968, y lo que establece en su Artículo- 9.- Categorías particulares de los datos- además de las buenas prácticas como la ISO-27001 que indica: “*Deben asegurarse de que la información reciba un nivel adecuado de protección”.*

A LA JEFATURA DE LA UNIDAD DE INFORMATICA.

RECOMENDACIÓN N°.03

En un plazo máximo de sesenta (60) días hábiles, se implementen las acciones de control necesarias que permitan la actualización periódica y constante del Instrumento denominado” Metodología y Proceso para la Gestión del Riesgo de TI y Seguridad de la Información” esto con el propósito de que el INAMU, a través de la Unidad de Información, gestione oportunamente no solo sus amenazas operativas en materia de riesgos tecnológicos, si no aquellos relacionados con la reputación, políticos, de gobierno corporativo y/o cualquiera que puedan impactar los objetivos institucionales en materia de Tecnologías de la información y comunicación.

La metodología de valoración aplicada por la UIN denomina FRAP (Facilitated Risk Assessment Process), se basa en la aplicación de técnicas de gestión de riesgos usando metodologías formales cualitativas de análisis de riesgos y utilizando análisis de vulnerabilidad, análisis del impacto del riesgo, análisis de amenazas y cuestionarios., la metodología es aplicada principalmente a las amenazas operativas

(procesos internos y externos, recursos humanos y tecnologías de la Información), pero se deben identificar amenazas que imposibiliten la realización exitosa de la estrategia de tecnologías de la información, dificultades para la integración de soluciones, el uso de sistemas heredados ineficientes y un portafolio de inversiones en tecnologías no alineado o priorizados a la estrategia Institucional.

La implementación de la presente recomendación tiene como objetivo cumplir Normas técnicas para la gestión y el control de las Tecnologías de Información 2021 del MICITT., específicamente con lo indicado a continuación:

> *‹‹La organización debe responder adecuadamente a las amenazas que puedan afectar la gestión de las TI, mediante una gestión continua de riesgos que esté integrada al sistema específico de valoración del riesgo institucional y considere el marco normativo que le resulte aplicable››*

A LA PRESIDENCIA EJECUTIVA.

RECOMENDACIÓN N°.04

En un plazo máximo de noventa (90) días hábiles, solicitar a la Unidad de Informática, en coordinación con la Dirección Administrativa Financiera, un plan remedial para subsanar las debilidades identificadas por parte de las Auditorías Externas con relación al Centro de Datos ubicado en el edificio SIGMA, el Plan debe contener al menos los requerimientos funcionales y económicos para que pueda ser aprobado por el Jerarca, y así cumplir con los dispuesto por los entes fiscalizadores externos y debidamente aceptados por las Administración Activa del INAMU.

Como se muestra en la CARTA DE TECNOLOGÍA DE INFORMACIÓN DEL 31 DE DICIEMBREDE 2021, suscrita por CROWE HORWATH CR, S.A. las inconsistencias relacionadas con la seguridad fisca del cuarto de servidores del INAMU Edificio Sigma., se mantienen desde el 2019, y lo clasifican como “Riesgo Inaceptable” no obstante, la Administración Activa una vez analizado y cuantificado estos riesgos, así

como el impacto que tienen en los planes estratégicos y operativos, tomo la decisión de aceptar las consecuencias y probabilidad de estos riesgos en particular, sin adelantar acciones de reducción, control o mitigación.

La implementación de la supra citada recomendación tiene como objetivo cumplir con lo normado en el “Manual de Normas Generales de Auditoría para el Sector Público” y la auditoría financiera que comprende la auditoría de estados financieros que tiene por objetivo emitir un dictamen independiente sobre la razonabilidad de los estados financieros de la entidad auditada, de conformidad con el marco normativo aplicable, y el análisis de otros aspectos específicos relacionados con la información financiera como son las tecnologías que soportan esta información.

A LA PRESIDENCIA EJECUTIVA.

RECOMENDACIÓN N°.05

En un plazo no mayor a sesenta (60) días solicitarle al Comité de Tecnologías de la Información realizar una evaluación y reformulación del proyecto para la implementación de un “Plan de gestión de seguridad de la Información a nivel institucional, sus roles e involucrados, políticas y procedimientos, proceso general de gestión de la seguridad a nivel institucional”. Con el propósito de establecer los requerimientos financieros, humanos y tecnológicos para que el INAMU, cuente en un tiempo razonable con el instrumento que le permita gestionar la seguridad de la información de acuerdo con el marco normativo aplicable.

A la fecha del estudio se determinó que el INAMU, carece de un Plan de seguridad de la Información, integral, se cuenta con una iniciativa o proyecto, pero la ausencia de una gestión articulada que permita una definición de requerimientos, necesidades, seguimiento y control del plan de seguridad limita a la UIN el establecer mecanismos efectivos para prevenir, detectar, impedir, valorar, evaluar y corregir transgresiones a la seguridad que pudieran generarse al nivel de acceso a sistemas, infraestructura e instalaciones en las que se almacena, procesa y transmite información, previendo que

el personal y los proveedores tengan accesos mínimos necesarios para la ejecución de sus funciones; se apliquen controles para proteger la confidencialidad, autenticidad, privacidad e integridad de la información.

La supra citada recomendación tiene como objetivo principal cumplir con las Normas técnicas para la gestión y el control de las Tecnologías de Información 2021, en lo especifico con la Seguridad lógica.

A LA JEFATURA DE LA UNIDAD DE INFORMATICA

RECOMENDACIÓN N°.06

En línea con la estructura aprobada para la Unidad de Informativa del INAMU, en un plazo no mayor a las seis (6) meses a partir de formalizada la presente recomendación, gestionar ante el Jerarca de la Institución, el retorno de la plaza 252 de profesional especialista la cual se encuentra cedida en calidad de préstamo de forma temporal, al Despacho de la Presidencia hasta el 2026, esto justificado en la necesidad de que el INAMU, cuente con un recurso en ciberseguridad y se gestione de forma adecuada el funcionamiento de los sistemas y equipos informáticos con los que cuenta la institución, los avances tecnológicos, amenazas y vulnerabilidad en materia de seguridad y ciberseguridad.

Derivado del análisis realizado a la Estructura organizativa de la UIN, y las necesidades actuales de recurso humano especializado en ciberseguridad con respecto al funcionamiento de los sistemas y equipos informáticos con los que cuenta la institución, los avances tecnológicos, amenazas y vulnerabilidad se puede identificar que, es necesario el retorno de la plaza cedida en calidad de préstamo temporal al Despacho de la Presidencia, lo anterior aunado a una escaza o nula presupuestación de recursos financieros para temas de capacitación y actualización profesional a nivel institucional, aumentan el riesgo de amenazas en temas se seguridad y ciberseguridad.

La recomendación anterior tiene como objetivo cumplir con Las Normas técnicas para la gestión y el control de las Tecnologías de Información (N-2-2007- CO-DFOE, establece en el artículo 2.4, referente a que: *El jerarca debe brindar el apoyo necesario para que dicha Función de TI cuente con una fuerza de trabajo motivada,* ***suficiente, competente*** *y a la que se la haya definido, de manera clara y formal, su responsabilidad, autoridad y funciones"*

A LA PRESIDENCIA EJECUTIVA.

RECOMENDACIÓN N°.07

Girar las instrucciones y/o lineamientos a los titulares subordinados responsables para que en un máximo de un año el INAMU tenga debidamente formalizado, aprobado y comunicado el "Plan de continuidad del negocio" en línea con las buenas prácticas y la normativa vinculante, citado Plan debe contener como mínimo las siguientes etapas: 1. Fase de análisis de impacto del negocio (BIA) y todas actividades, 2. Fase de gestión del riesgo y 3. Roles y responsabilidades, esto con el propósito que la Institución se asegure de forma razonable la continuidad de las operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes.

En el instrumento denominado Matriz SEVRI de TI, se mantiene un el riesgo identificado como "*Riesgo de pérdida de información y de la operativa de TI y por lo tanto afecta la operación de la institución"*, dicho riesgo, presenta la siguiente medida de administración: "*Revisión y actualización del Plan existente utilizando las mejores prácticas de la industria (27031)*; dicha medida tiene fecha de implementación para el 30/05/2020.

La implementación de la presente recomendación tiene como propósito dotar al INAMU de un instrumento de gestión que establezca formalmente prácticas que le permitan realizar valoraciones sobre la resiliencia institucional, disponiendo de una estrategia viable y rentable que coadyuve a mantener la continuidad de las

operaciones habilitadas por el uso de recursos tecnológicos, la recuperación ante un desastre y la respuesta ante incidentes, disponiendo de un plan de continuidad elaborado a través de la identificación y análisis de procesos y activos críticos, base para establecer las acciones ante materialización de eventos de interrupción, estableciendo roles y responsabilidades adecuadas para responder a situaciones adversas.

Cc. Señoras y Señor Junta Directiva
Sra. Kattia Calvo Cruz, jefatura, Despacho de la Presidencia Ejecutiva
Sra. Zaida Barboza Hernandez, directora a.i., Dirección Administrativa Financiera.
Sra. Ana Victoria Naranjo Porras, jefatura, Unidad de Planificación Institucional.
Sra. Ingrid Trejos Marín, jefatura, Unidad de Informática
Comité Institucional de Tecnologías de la Información
Archivo