INFORME DE CONTROL INTERNO RELACIONADO CON EL SEGUIMIENTO A LOS RESULTADOS OBTENIDOS EN LA "APLICACIÓN DEL INSTRUMENTO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES PÚBLICAS" ASÍ COMO A LA IMPLEMENTACIÓN DEL DECRETO N° 37549-JP REGLAMENTO PARA LA PROTECCIÓN DE LOS PROGRAMAS DE CÓMPUTO EN LOS MINISTERIOS E INSTITUCIONES ADSCRITAS AL GOBIERNO CENTRAL.

INAMU-JD-AI-In-002-2024

(Remitido con oficio INAMU-JD-AI-027-2024)

Firmas de validación del informe	
Realizado por	**Revisado por**
DILANA DE LOS ANGELES VILLALOBOS GUZMAN (FIRMA) Firmado digitalmente por DILANA DE LOS ANGELES VILLALOBOS GUZMAN (FIRMA) Fecha: 2024.02.06 16:09:19 -06'00'	RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Firmado digitalmente por RANDALL ALONSO UMAÑA VILLALOBOS (FIRMA) Fecha: 2024.02.06 16:07:56 -06'00'
Dilana Villalobos Guzmán Profesional Especialista Encargada del estudio Auditoría Interna	Randall Umaña Villalobos Auditor Interno Auditoría Interna

INSTITUTO NACIONAL DE LAS MUJERES.

INFORME DE CONTROL INTERNO RELACIONADO CON EL SEGUIMIENTO A LOS RESULTADOS OBTENIDOS EN LA "APLICACIÓN DEL INSTRUMENTO DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES PÚBLICAS" ASÍ COMO A LA IMPLEMENTACIÓN DEL DECRETO N° 37549-JP REGLAMENTO PARA LA PROTECCIÓN DE LOS PROGRAMAS DE CÓMPUTO EN LOS MINISTERIOS E INSTITUCIONES ADSCRITAS AL GOBIERNO CENTRAL.

El presente estudio de auditoría se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2023, el objetivo consistió en verificar el avance de las recomendaciones pendientes de cumplimiento que fueron dirigidas a la Unidad de Informática por parte de la Auditoría Interna y de las auditorías externas de los periodos 2018, 2019, 2020 y 2021.

El proceso de seguimiento realizado permite a la Administración Activa, para la toma de decisiones sobre posibles desviaciones en los objetivos institucionales en materia de tecnologías de la información, así como el fortalecimiento del control interno institucional.

El propósito de este proyecto es coadyuvar a la Administración Activa en el establecimiento una cultura de supervisión constante y seguimiento de las oportunidades de mejoras y observaciones expuestas a nivel institucional, sin tener que esperar a que se emita por parte de la auditoría interna este tipo de seguimiento para que sean atendidas oportunamente, esto con el fin de eliminar el exceso de observaciones vencidas de periodos anteriores.

Febrero, 2024.

TABLA DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE GRÁFICAS

TABLA DE NOMENCLATURAS

Nomenclatura	Significado
INAMU	Instituto Nacional de las Mujeres.
MIDEPLAN	Ministerio de Planificación Nacional y Política Económica.
MICITT	Ministerio de Ciencia, Innovación, Tecnología y Telecomunicaciones de Costa Rica.
NGASP	Normas Generales de Auditoría para el Sector Público.
SEVRI	Sistema Especifico de Valoración de Riesgo Institucional.
CGR	Contraloría General de la Republica.
GC	Gobierno Corporativo
LGCI	Ley General de Control Interno.
MACU	Matriz de Cumplimiento
PEI	Plan Estratégico Institucional
PETIC	Plan Estratégico de tecnologías de información y comunicaciones

1 RESUMEN EJECUTIVO

¿QUÉ EXAMINAMOS?

El presente estudio se realizó en cumplimiento al Plan de Trabajo de la Auditaría Interna para el periodo 2023, la auditoría fue de carácter especial con el objetivo de evaluar el cumplimiento de las recomendaciones y oportunidades de mejora emitidas a la Unidad de Informática mediante estudios de control emitidos por parte de la Auditoría Interna, Auditoría Externa u otros Órganos de Fiscalización.

¿POR QUÉ ES IMPORTANTE?

El presente informe de seguimiento permite la retroalimentación a la Administración Activa sobre el grado de avance que se presenta en el cumplimiento de las recomendaciones, validando que se atiendan con prontitud de conformidad con lo estipulado en el artículo 17 de la Ley General de Control Interno, la cual trata sobre el seguimiento del sistema de control interno y el asegurar que los hallazgos de la auditoría y los resultados de otras revisiones se atiendan con prontitud.

¿QUÉ ENCONTRAMOS?

Como parte del estudio realizado, se identificaron deficiencias asociadas al cumplimiento de los plazos establecidos para la ejecución de las recomendaciones pendientes de aplicación las cuales se dividieron en siete (7) recomendaciones emitidas por la auditoría interna y veintidós (22) recomendaciones emitidas por la auditoría externa, donde solo una se da por cumplida en el periodo 2023 y las todas las demás mantienen plazos vencidos.

El objetivo correspondiente a la implementación de la derogatoria de la Norma Técnica de Gestión y Control de las Tecnologías de Información se da por cumplido con la aprobación y divulgación del Marco de Gestión de Tecnologías de Información y Comunicación. Este punto corresponde al mismo que se detalla en el párrafo anterior como cumplido y que también formaba parte de las recomendaciones pendientes emitidas por la auditoría interna del INAMU.

No se logró determinar avances significativos a las respuestas negativas que se obtuvieron de la aplicación del Instrumento denominado “Practicas de Seguridad de la Información en las Instituciones Públicas”, el cual fue solicitado por la CGR. Posterior a un año de la aplicación de este Instrumento no se evidencia mejora en las condiciones que se mantenían en su primera aplicación y por consiguiente en la aplicación de prácticas de seguridad de la información.

Como oportunidad de mejora se recomienda realizar un análisis integral del Decreto 37549-JP con la intención de identificar cuales prácticas de las establecidas en este documento se pueden implementar por parte del INAMU, para prevenir y combatir el uso ilegal de programas de cómputo.

¿QUÉ SIGUE?

La Unidad de Informática debe de establecer y mantener estrategias y mecanismos de control para velar por el cumplimiento de las recomendaciones pendientes de implementación en el plazo establecido, evitando así que se den desviaciones a los objetivos institucionales y se fortalezcan las gestiones de seguimiento, cumpliendo con las fechas propuestas, manteniendo informada de las actividades y avances llevados a cabo a la auditoría interna.

Además, realizar un análisis sobre la viabilidad de implementar aspectos contemplados dentro del Decreto 37549-JP, con el fin de prevenir y combatir el uso ilegal de programas de cómputo y así cumplir con las disposiciones sobre derechos de autor que establece la Ley 6683 y sus reformas y la Ley 8039 y sus reformas.

2 INTRODUCCIÓN

El presente estudio de auditoría se realizó en cumplimiento del Plan de Trabajo de la Auditoría Interna para el periodo 2023, el objetivo principal consistió analizar el nivel de implantación e implementación de las recomendaciones emitidas por parte de la Auditoría Interna del INAMU y de las Auditorías Externas de los periodos 2018, 2019, 2020 y 2021, las cuales mantienen estados de pendientes o en proceso con plazos ya cumplidos por parte de la Unidad de Informática al periodo 2023.

2.1 ORIGEN DEL ESTUDIO

El estudio 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], las Normas de Control Interno para el Sector Público[3], Política para la Gestión Operativa de Tecnologías de Información, Manual de Calidad de los Servicios de TI, Plan de Calidad de los Servicios de TI, Plan de Calidad de los Respaldos de los Servicios de TI, Procedimientos de Respaldo y Recuperación, Extracto del Modelo de Arquitectura de Información Fichas de Servicios, Técnicas de Seguridad- Sistemas de Gestión de la Seguridad de la Información- Requisitos (INTE/ISO/IEC 27001:2014) y la Matriz de Cumplimiento MACU-2023.

[1] Ley del 29 de abril de 1998, publicada en La Gaceta N°94 del 18 de mayo de 1998.
[2] Ley del 30 de julio del 2002, publicada en La Gaceta N°169 del 04 de setiembre del 2002.
[3] Norma del 26 de enero del 2009 Publicada en La Gaceta N°26 del 6 de febrero del 2009.

2.2 OBJETIVO DEL ESTUDIO

Evaluar el grado de cumplimiento de las recomendaciones y oportunidades de mejora emitidas tanto por la Auditoría Interna, así como las Auditorías Externas u otros Órganos de Fiscalización que fueron dirigidas a la Unidad de Informática y al 2023 se encuentran en proceso con plazos vencidos. Para la consecución del objetivo general del estudio fueron necesarios los siguientes procedimientos de auditoría:

- Validar el grado de avance en la implementación de la derogatoria de la Norma Técnica de Gestión y Control de las Tecnologías de Información (N-2-2007-CO-DFOE).

- Determinar el grado de cumplimiento de las recomendaciones emitidas en los informes de auditoría interna “Informes Especiales de Control Interno” Relacionado con el Diagnóstico de todos los Sistemas Informáticos y de Comunicación en Producción del INAMU.

- Evaluar el grado de implementación de las oportunidades de mejora que se plantearon en la asesoría sobre el Instrumento de aplicación de Prácticas de Seguridad de la Información en las Instituciones Públicas.

- Analizar la viabilidad de implementación de las buenas prácticas del Decreto N°37549-JP Reglamento para la protección de los Programas de Cómputo en los Ministerios e Instituciones Adscritas al Gobierno Central.

2.3 ALCANCE DEL ESTUDIO

El estudio es de carácter especial y comprendió la evaluación de la gestión realizada por parte de la Unidad de Informática en relación con la atención de las recomendaciones emitidas por parte de la Auditoría Interna del INAMU, Auditorías

Externas de los periodos 2018, 2019, 2020 y 2021, así como observaciones emitidas por la Contraloría General de la Republica que se encuentran pendientes de cumplimiento al periodo 2023.

2.4 METODOLOGÍA APLICADA

El estudio se realizó de conformidad con las Normas Generales de Auditoría para el Sector Público, las Normas de control interno para el Sector Público (N-2-2009-CO-DFOE), el Manual de Normas generales de auditoría para el Sector Público, el Reglamento de Organización y Funcionamiento de la Auditoría Interna del Instituto Nacional de la Mujer[4], Política para la Gestión Operativa de Tecnologías de Información, Manual de Calidad de los Servicios de TI, Plan de Calidad de los Servicios de TI, Plan de Calidad de los Respaldos de los Servicios de TI, Procedimientos de Respaldo y Recuperación, Extracto del Modelo de Arquitectura de Información Fichas de Servicios, Técnicas de Seguridad- Sistemas de Gestión de la Seguridad de la Información- Requisitos (INTE/ISO/IEC 27001:2014) y la Matriz de Cumplimiento MACU-2023.

De conformidad con los criterios expuestos, la Auditoría Interna realizó una recopilación y actualización de las acciones de cumplimiento realizadas por la Administración Activa, sustentadas en la verificación de insumos varios que conforman las evidencias que respaldan el estado actual de las acciones ejecutadas.

La ejecución de este estudio se realizó aplicando reuniones virtuales mediante la plataforma Teams con los responsables de los procesos vinculados a quienes se les aplicaron consultas específicas, vía oficio, correo electrónico y chat, de igual forma se trabajó en la verificación de datos mediante la aplicación de varios instrumentos, tales como: correos, entrevistas, cuadros comparativos, matrices de cumplimiento, procedimientos, entre otros.

[4] Reglamento del 15 de febrero de 2011 Publicada en La Gaceta No. 32 del 15 de febrero de 2011.

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 pasado 01 de febrero del presente año, se realizó dicha conferencia final en modalidad presencial, la sesión de trabajo se llevó a cabo en la sala de sesiones de la Junta Directiva, se contó con la participación de las siguientes personas funcionarias:

- ✓ Sra. Adilia Caravaca Zúñiga, presidenta ejecutiva, Presidencia Ejecutiva.
- ✓ Sra. Alexandra Gómez Ruiz, asesora, Despacho de la Presidencia Ejecutiva.
- ✓ Sr. Ingrid Trejos Marín, jefatura, Unidad de Informática.
- ✓ Sra. Klansy Flores Salguero, profesional especialista, Auditoría Interna.
- ✓ Sra. Dilana Villalobos Guzmán, profesional especialista, Auditoría Interna.

En dicha sesión de trabajo se consideraron las observaciones expuestas por parte de los presentes en función de las conclusiones y recomendaciones expuestas.

2.6 IMPLANTACIÓN DE LAS RECOMENDACIONES DE LA AUDITORÍA INTERNA

En la misma Ley N.º 8292 el Artículo 37. —Informes dirigidos al jerarca, establece lo siguiente:

Artículo 37—Informes dirigidos al jerarca.

"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 disponga; todo ello tendrá que comunicarlo debidamente a la auditoría interna y al titular subordinado correspondiente"

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 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 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.

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

e) *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 texto en negrita 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 de la Profesional Especialista de Auditoría Interna, Dilana Villalobos Guzmán, y la revisión por parte de Randall Umaña Villalobos, Auditor Interno del INAMU.

2.9 GENERALIDADES DEL ESTUDIO

El presente proyecto está relacionado con el seguimiento de recomendaciones y se realizó con el fin de determinar el grado de cumplimiento y de avance de las recomendaciones emitidas producto de los proyectos de la Auditoría Interna, las Auditorías Externas y otros Órganos de Fiscalización y que fueron dirigidas a la Unidad de Informática del INAMU., esto como parte de las funciones orgánicas de la Auditoría Interna entre las que están el establecer y velar por la aplicación de un proceso de seguimiento de recomendaciones, observaciones y demás resultados derivados de los servicios emitidos, y así asegurar que las acciones establecidas por las instancias competentes se implementen eficazmente, dentro de los plazos definidos por la Administración Activa.

Es fundamental que este estudio coadyuve a la Administración Activa a gestionar de forma oportuna las recomendaciones que se han emitido por los diferentes órganos de fiscalización y poder contribuir con la toma de decisiones de relevancia e impacto Institucional.

3 RESULTADOS DE LA AUDITORÍA.

El objetivo principal del presente proyecto de auditoria consistió en evaluar el grado de implementación y cumplimiento de las recomendaciones dirigidas a la Unidad de Informática que no han sido implementadas durante el periodo 2023 y se encuentran con plazos vencidos, las recomendaciones a las cuales se les dio seguimiento fueron emitidas por los diferentes Órganos Fiscalizadores como lo son: la Auditoría Interna, Auditorías Externas y la Contraloría General de la República.

Los resultados que presentamos a continuación son producto de la evaluación y análisis de los datos consignados dentro de este estudio.

3.1 IMPLEMENTACIÓN DE LA DEROGATORÍA DE LA NORMA TÉCNICA DE GESTIÓN Y CONTROL DE LAS TECNOLOGÍAS DE INFORMACIÓN (N-2-2007-CO-DFOE).

Mediante resolución R-CO-26-2007 del 7 de junio del 2007, la Contraloría General de la Republica emitió las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), estás normas establecían los criterios básicos que deben ser observados por los entes u órganos sujetos a su fiscalización, como parte de la gestión y el control institucional de las tecnologías de información.

Sin embargo, el constante avance de las tecnologías de la información y la heterogeneidad de los recursos disponibles en las Instituciones Públicas, hacen necesario el establecimiento de medidas que permitan la definición de un nuevo marco regulatorio, atendiendo las distintas realidades institucionales. Esto llevo a la derogatoria de las Normas Técnicas para la Gestión y el Control de las Tecnologías de Información (N-2-2007-CO-DFOE), a partir del 1° de enero del 2022 de esta norma y se da a conocer mediante el artículo 1° de la resolución N° R-DC-17-2020 del 17 de marzo del 2020.

Complementariamente en la resolución N° R-DC-17-2020 fueron modificados los ítems 5.9 y 5.10 de las Normas de Control Interno para el Sector Público (n-2-2009CO-DFOE), quedando su texto como sigue:

5.9 Tecnologías de información.

El jerarca y los titulares subordinados, según sus competencias, deben propiciar el aprovechamiento de tecnologías de información que apoyen la gestión institucional mediante el manejo apropiado de la información y la implementación de soluciones ágiles y amplio alcance. En todo caso, deben instaurarse los mecanismos y procedimientos manuales que permitan garantizar razonablemente la operación continua y correcta de los sistemas de información. En esa línea, de conformidad con el perfil tecnológico de la institución, órgano o ente, en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, el jerarca deberá aprobar el marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes.

Para la determinación del perfil tecnológico institucional se podrán considerar variables como las siguientes: marco de procesos para la gestión de TI, mapeo de procesos y subprocesos de negocio, organigrama de la entidad, conformación del Comité de TI, proveedores de TI, servicios de TI, inventario y criticidad de tipos documentales, centros de procesamiento y almacenamiento de datos, inventario de equipos y sistemas de información que soportan los servicios, software, proyectos de TI, planes de adquisición sobre TI, canales electrónicos y riesgos de TI.

5.10 Sistemas de información y tecnologías de información en instituciones de menor tamaño.

El jerarca y los titulares subordinados de las instituciones de menor tamaño, según sus competencias, deben establecer los procedimientos manuales, automatizados o ambos, necesarios para obtener, procesar, controlar, almacenar y comunicar la información sobre la gestión institucional y otra relevante para la consecución de los objetivos institucionales. Dicha información debe ser de fácil acceso y estar disponible en un archivo institucional que, de manera ordenada y conforme a las

regulaciones que en esa materia establece el Sistema Nacional de Archivos, pueda ser consultado por usuarios internos o por parte de instancias externas.

De igual forma, dichos sujetos, de acuerdo con sus competencias y su perfil tecnológico, definido en función de su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su dependencia tecnológica, deberán aprobar su marco de gestión de tecnologías de información y establecer un proceso de implementación gradual de cada uno de sus componentes.

La derogatoria de la Norma Técnica insta a la Administración Activa para que defina y apruebe su marco de gestión de tecnologías de información, el cual debe estar acorde con su naturaleza, complejidad, tamaño, modelo de negocio, volumen de operaciones, criticidad de sus procesos, riesgos y su grado de dependencia en las tecnologías, mismo que deberá mantenerse actualizado con su realidad tecnología.

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.

En el caso del INAMU se acuerda por parte de la Presidencia Ejecutiva la aprobación y divulgación del Marco de Gestión de Tecnologías de Información y Comunicación mediante la circular ***INAMU-PE-005-2023*** del ***31 de agosto del 2023***. Dicho informe se aprobó en la Sesión Ordinaria de Junta Directiva 16-2023 celebrada el 16 de agosto del 2023.

El Marco de Gestión será revisado anualmente, para su respectiva actualización, el mismo cuenta con un tiempo de implementación que abarca 3 años (periodo 2023, 2024 y 2025).

Este tema forma parte de una recomendación incluida dentro del punto 3.2.1 Recomendaciones en Informes de Auditoría Interna. Esta recomendación la

categorizamos como cumplida, luego de revisar el documento denominado “Informe de Situación Actual- Marco de Gestión de TI”, cuyo objetivo general es definir las prácticas que regirán las Tecnologías de Información de uso institucional, logrando que los sistemas de información e infraestructura tecnológica de la organización sean de calidad, tengan los controles adecuados y se asegure la confiabilidad de los servicios, contribuyendo en alcanzar una mayor efectividad en las actividades relacionadas con las tecnologías de información.

3.2 CUMPLIMIENTO DE LAS RECOMENDACIONES EN LOS INFORMES DE LA AUDITORÍA INTERNA Y AUDITORÍA EXTERNA.

Al periodo 2023 se tienen recomendaciones de periodos anteriores que no presentan el debido proceso de implementación en los plazos determinados por la administración.

Estas recomendaciones corresponden a informes emitidos por parte de la auditoría interna y por los auditores externos de los periodos 2018, 2019, 2020 y 2021.

A continuación, detallamos las recomendaciones que se mantienen pendientes de aplicación:

3.2.1 RECOMENDACIONES EN INFORMES DE AUDITORÍA INTERNA:

Las recomendaciones pendientes de cumplimiento que fueron emitidas por parte de la Auditoría Interna son el resultado de una serie de estudios e informes que formaron parte de la Contratación de los servicios profesionales de Auditoría en TI para el periodo 2022, mediante el proceso de Contratación 2022CD-000004-0015800001, está contratación tuvo como resultado tres entregables y se denominaron de la siguiente forma:

Informe Especial Relacionado con el Diagnostico de todos los Sistemas Informáticos y de Comunicación en Producción del INAMU, durante el Periodo 2022, el cual se subdividió en las siguientes memorias:

- **Entregable Uno:** Evaluación de las Gestiones Entorno a la Planificación Estratégica del INAMU Relacionadas con el PEI, el PETIC y el Mapeo de los Riesgos de la Unidad de Informática.

- **Entregable Dos:** Evaluación de los Procesos de Seguridad Física y Lógica, Relativos a las Tecnologías de Información y Comunicación del INAMU para el periodo 2022.

- **Entregable Tres:** Para Determinar los Niveles de Integración, Estabilidad, Obsolescencia.

Producto de estos entregables se identificaron un total de trece (13) recomendaciones de las cuales siete (7) aún no se implementan al periodo 2023.

Tabla 1.- Recomendaciones pendiente- emitidas por la Auditoría Interna del INAMU al 2023

Número del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
INAMU-JD-AI-136-2022\ Informe: INAMU-JD-AI-In-009-2022	En un máximo de ciento veinte (120) días naturales de acuerdo a buenas prácticas para la gestión de proyectos se diseñe, elabore y formalice los instrumentos necesarios para apoyar la gestión del Comité, en torno a la cartera de proyectos y/o iniciativas de TI; con el fin de establecer controles relacionados con la recepción, valoración, priorización, aprobación, seguimiento y cierre de cada una de las iniciativas y/o proyectos, estas acciones deben contener al menos los criterios de priorización, además indicadores que permitan medir la efectividad del cumplimiento de la cartera de iniciativas y su impacto en el alcance de los objetivos estratégicos y operativos institucionales.	28/2/2023	N\A	Pendiente con plazo vencido
INAMU-JD-AI-136-2022\ Informe: INAMU-JD-AI-In-009-2022	En un plazo máximo de noventa (90) días hábiles, en coordinación con las instancias que se consideren oportunas, se diseñen, elaboren y formalicen los mecanismos de control que establezcan una adecuada gestión de riesgos con terceros, y así permitir que cuando se decida que el modelo de negocio en materia de tecnologías de la información es la tercerización, se realice una evaluación de riesgos inicial como parte del proceso de toma de decisiones y se asegure un proceso de transferencia	31/1/2023	N\A	Pendiente con plazo vencido

Número del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
	tecnológica que minimice la dependencia de la organización respecto de terceros contratados para la implementación y mantenimiento de software e infraestructura tecnológica. los controles implementados deben lograr identificar de forma razonable el riesgo relacionado con el grado de dependencia de los proveedores de servicios tecnológicos a partir de su interrelación con los activos, servicios y procesos de negocio. Esta asociación, ayudará en la identificación de amenazas y particularmente vulnerabilidades; adicionalmente garantizará que el INAMU tiene los controles apropiados para la protección de los activos y continuidad del servicio.			
INAMU-JD-AI-009-2023 Informe INAMU-JD-AI-In-014-2022	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).	16/3/2023	N\A	**Cumplida** Se da la aprobación y divulgación mediante la Circular INAMU-PE-005-2023.
INAMU-JD-AI-009-2023 Informe INAMU-JD-AI-In-014-2022	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.	24/4/2023	N\A	En proceso con plazo vencido

Número del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
INAMU-JD-AI-009-2023 Informe INAMU-JD-AI-In-014-2022	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.	30/7/2023	N\A	Pendiente con plazo vencido
INAMU-JD-AI-024-2023 Informe INAMU-JD-AI-In-003-2023	En un plazo máximo de sesenta (60) días hábiles, actualizar el portafolio de todos y cada uno de los servicios y/o herramientas tecnológicas del INAMU, indistintamente si estas son gestionadas mediante la mesa de servicios de TI, o un tercero, para asegurar de forma razonable que los servicios de TI se encuentran alineados con la estrategia del negocio. Durante la revisión efectuada se determinó que el catálogo de servicios y/o sistemas de la UIN., no muestra la totalidad de aplicaciones del INAMU, ya que no se logró ubicar el aplicativo SEANI (Sistema de Eventos de Atención No Inmediata), el cual administra la base de datos de la Unidad Delegación de la Mujer, además sistemas que se encuentran dentro del catálogo no son administrados por parte de la Unidad de informática como es el caso del BOS-HT, que gestiona la información financiera y contable del Instituto, a través de la subcontratación del proveedor TECAPRO.	30/5/2023	N\A	Pendiente con plazo vencido
INAMU-JD-AI-024-2023 Informe INAMU-JD-AI-In-003-2023	En un máximo de 90 (noventa) días hábiles realizar los ajustes a nivel de la metodológica que se utiliza en lo relativo al mapeo de la Arquitectura de TI, para que esta contemple la interrelación de los componentes tecnológicos y su transición a lo largo del tiempo hasta llegar al estado deseado (meta), además que estos ajustes sean realizados a nivel del Plan Estratégico de TI 2022-2027, con el propósito de reflejar los cambios en el tiempo, en la Arquitectura de TI y a partir de esos estados, justificar y alinear las inversiones tecnológicas requeridas.	10/7/2023	N\A	Pendiente con plazo vencido.

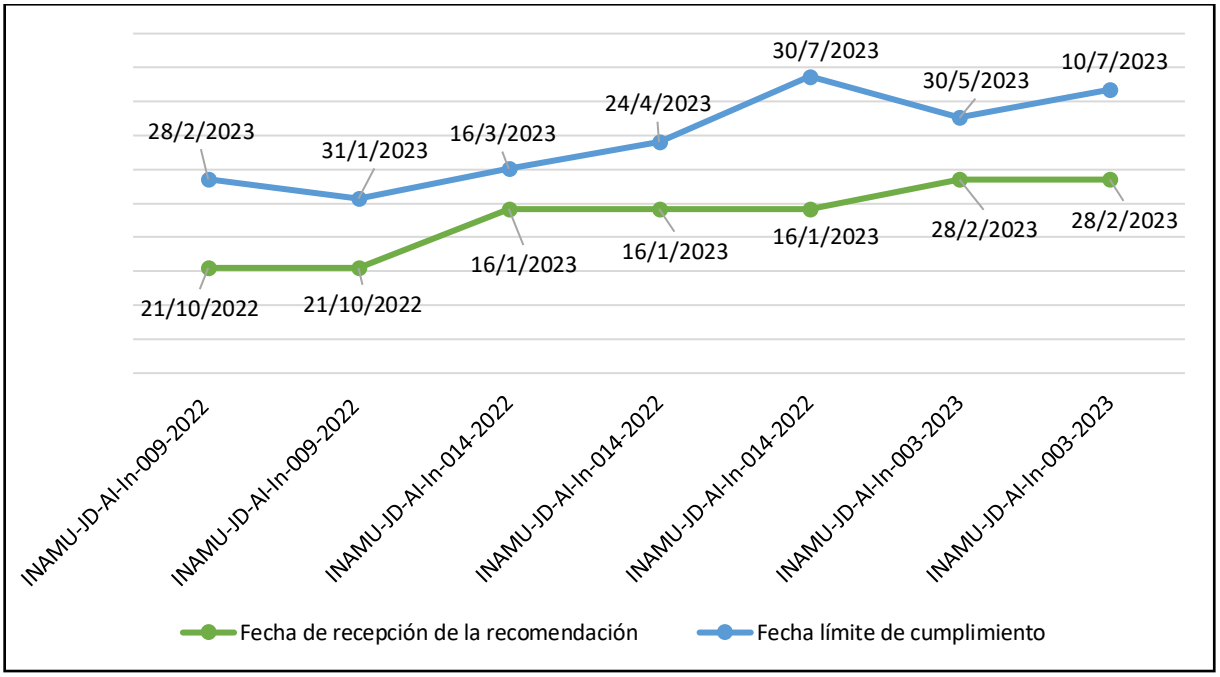
Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

Las recomendaciones que indican en proceso corresponden a las que están siendo atendidas en alguna medida y que aún no se puede catalogar como cumplidas por parte de esta Auditoría Interna.

Las que indican pendientes, corresponde a las recomendaciones a las que aún no se les realiza ningún proceso de avance para su cumplimiento, normalmente corresponden a observaciones que se pueden categorizar como resientes, pero en este caso corresponde a observaciones que ya cuentan el plazo de implementación vencido y en algunos casos el titular subordinado solicitó ampliación para poder cumplir con su implementación.

En este caso en particular ninguna de las recomendaciones detalladas anteriormente cuenta con aprobación para una prórroga o ampliación de plazo, sin embargo, la tabla que se muestra a continuación presenta el detalle de los vencimientos en las fechas de cumplimiento que han tenido cada una de las siete (7) recomendaciones.

Gráfica 1.- Fechas de vencimientos de las recomendaciones emitidas por la AI.



Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

De la gráfica anterior se desprende que las dos (2) recomendaciones pendientes del informe INAMU-JD-AI-In-009-2022 las cuales fueron recibidas por la administración el 21/10/2022 ambas presentan atrasos de cumplimiento de 306 y 334 días respectivamente, de igual manera las tres (3) recomendaciones del informe INAMU-JD-AI-In-014-2022 las cuales fueron recibidas por la administración el 16/01/2023, una (1) se está señalada como cumplida a la fecha de este informe y las dos (2) pendientes mantienen atrasos entre 251 y 154 días. Las recomendaciones del informe INAMU-JD-AI-In-003-2023 las cuales fueron recibidas por la administración con fecha del 28/02/2023 presentan atrasos entre 215 y 174 días.

3.2.2 RECOMENDACIONES EN INFORMES DE AUDITORÍAS EXTERNAS:

En lo que respecta al seguimiento de recomendaciones emitidas por las auditorías externas se presenta un avance poco significativo en el cumplimiento de las recomendaciones ya que corresponden a los periodos 2018, 2019, 2020 y 2021.

A la fecha de revisión se presentan veintidós (22) recomendaciones pendientes de implementación, las cuales se mantienen en su mayoría en un estado de en proceso con plazo vencido.

El detalle de las recomendaciones pendiente se presenta a continuación y se separan por año de carta de gerencia en la cual se presentaron a la administración.

Tabla 2.-Recomendaciones pendiente- emitidas por la AE periodo 2018.

Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-TI-2018	Establecer, realizar y cumplir con pruebas de calidad periódicamente, atendiendo los resultados obtenidos y documentarlos, con el propósito de brindarle trazabilidad a los problemas resultantes y de esta manera determinar la causa para resolverlo con mayor facilidad.	30/12/2020	31/1/2023	En proceso con plazo vencido

Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

Tabla 3.-Recomendaciones pendiente- emitidas por la AE periodo 2019.

Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-TI-2019	2. Coordinar las fechas para llevar a cabo lo más pronto posible, el curso virtual sobre Políticas de Gestión Operativa de TI desarrollado por la Unidad de Informática mediante la plataforma virtual Aprende Conmigo. Esto con el fin de ir creando una cultura de seguridad en la Institución, se posea un claro entendimiento de las políticas de seguridad de la información y así evitar o reducir los incidentes asociados con esta.	31/12/2020	31/12/2022	En Proceso con plazo vencido
Carta de gerencia CG-TI-2019	1. Asegurarse que el plan de recuperación ante desastres incluya los siguientes aspectos: a. Procedimiento para declarar un desastre. b. Identificar los planes de recuperación básicos (procedimientos que puedan hacer que los servicios críticos de TI vuelvan a funcionar en caso de un fallo). Tomar en cuenta los pasos para poner en operación el sitio alterno ante un eventual fallo en los servicios que este soporta. c. Recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI. d. Medidas que permitan prevenir un desastre. 2. Realizar capacitaciones sobre el plan de recuperación ante desastres y relacionadas con la continuidad de los servicios de TI, al personal respectivo. 3. Elaborar un plan de pruebas para el plan de recuperación ante desastres. 4. Ejecutar el plan de pruebas al menos una vez al año y documentar los resultados.	31/12/2020	31/12/2022	En proceso con plazo vencido
Carta de gerencia CG-TI-2019	5. Revisar y aprobar el plan de recuperación ante desastres una vez que se realicen las actualizaciones respectivas.	31/12/2020	31/12/2022	En proceso con plazo vencido
Carta de gerencia CG-TI-2019	3. Aprobar formalmente el procedimiento de respaldos y restauración de datos elaborado por la Unidad de Informática.	31/12/2020	31/12/2022	En proceso con plazo vencido
Carta de gerencia CG-TI-2019	2. Validar y aprobar formalmente el procedimiento para la gestión de cambios, generado por la unidad de informática.	31/12/2020	31/12/2022	En proceso con plazo vencido

Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

Tabla 4.-Recomendaciones pendiente- emitidas por la AE periodo 2020.

Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-TI-2020	Establecer un cronograma para la evaluación periódica de los SLA´s con el objetivo de velar por el cumplimiento de los acuerdos y minimizar el riesgo sobre el desempeño del servicio. Monitorear los indicadores de los acuerdos de niveles de servicios definidos, con el fin de delimitar, cumplir y mejorar los servicios.	31/12/2022	31/12/2022	En proceso con plazo vencido
Carta de gerencia CG-TI-2020	a. Establecer un enfoque de gestión de riesgo al proyecto alineado con el marco de referencia, en donde se enfoque la identificación, análisis, respuesta, mitigación, supervisión y control del riesgo de forma preventiva. b. Valorar la capacidad instalada del recurso humano para el proceso final de implementación y la etapa de post implementación del proyecto, para evitar falsas expectativas de los tiempos de cumplimiento y la atención de las actividades diarias de la Institución. c. Documentar las lecciones aprendidas de cada etapa del proyecto SIPGAF y al cierre se realice un informe integral, identificando las causas que originaron los eventos para futuros proyectos y la estrategia de negociación para lograr tener un sistema de información integrado. d. Establecer un plan de acción para la depuración y actualización de datos, con el fin de lograr una migración con información confiable y segura.	31/12/2022	31/12/2023	En proceso
Carta de gerencia CG-TI-2020	a. Definir y documentar de acuerdo con la política de seguridad, la estrategia y el plan de seguridad de la información. b. Monitorear el cumplimiento y los resultados de la aplicación de la estrategia y plan de seguridad para reforzar los criterios de integridad, confidencialidad y disponibilidad de la información, la infraestructura tecnológica para minimizar el impacto de vulnerabilidades e incidentes de seguridad. c. Establecer revisiones sobre la aplicación de controles a los equipos utilizados para el teletrabajo, ya sean computadores del INAMU o personales. d. Aplicar pruebas de vulnerabilidades a los sistemas de información e infraestructura tecnológica, con el objetivo de velar por la integridad, disponibilidad, confidencialidad de la información y la atención a los riesgos de fraude informático.	31/12/2022	31/12/2023	En proceso

Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-TI-2020	a. Establecer un plan de acción en conjunto con la Unidad de Planificación para atender la gestión del riesgo de fraude. b. Sensibilizar y enfocar programas de capacitación a los usuarios sobre fraudes informáticos. c. Dar seguimiento e informar a los Órganos de Dirección sobre el proyecto Sistema Integrado de Planificación y Gestión Administrativo Financiero (SIPGAF), basado en una metodología de gestión de proyectos, en donde exista un grupo o unidad de control del proyecto que genere informes de avances periódicos por medio de un control presupuestario y contable para la capitalización de costos del proyecto en desarrollo.	31/12/2022	31/12/2023	En proceso
Carta de gerencia CG-TI-2020	a. Confeccionar y aplicar un plan de pruebas al plan de Continuidad de TI, en alineación al Plan de Continuidad de Operaciones, entre las pruebas a incluir se pueden tomar en cuenta las siguientes: b. Pruebas de escritorio: un método para el ejercicio de los planes en los participantes revisan y discuten las acciones que se toman sin tener que realizar las acciones. ü Prueba de componente: estas pruebas se realizan con el objetivo de probar, encontrar, reparar fallas, verificar la efectividad del protocolo de recuperación y documentar las mejoras del comportamiento de los módulos independientes. ü Prueba integral: prueba en la cual se incluyen como parte del alcance de esta, toda la plataforma tecnológica que soporta un Sistema crítico de TI. ü Prueba de punta a punta: prueba en la cual se evalúan todos los componentes de todos los servicios críticos de la institución, considerando desde un sitio principal hasta un segundo sitio.	31/12/2022	31/12/2022	En proceso con plazo vencido
Carta de gerencia CG-TI-2020	Confeccionar un plan de capacitación en temas de continuidad de operaciones con el objetivo de concientizar y entrenar a todo el recurso humano ante siniestros y eventos no planificados.	31/12/2022	N\A	En proceso con plazo vencido

Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

Tabla 5.-Recomendaciones pendiente- emitidas por la AE periodo 2021.

Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-2021	Establecer por parte de la Administración un proyecto institucional para el cumplimiento en el cual se definan fechas claras mediante cronogramas, responsables de cada una de las tareas, recursos y gestores para las actividades de los procesos, puntos de avance con fechas específicas por medio de informes, además de un adecuado seguimiento, con la finalidad de asegurar el cumplimiento de lo requerido en 2 años y minimizar el riesgo de incumplimiento de aspectos normativos.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-2021	Divulgar y concientizar a toda la Institución en este nuevo ambiente de cambio del marco normativo, para implementar procesos de gobierno y de TI con un marco de trabajo integral, que ayude a entidad a lograr sus objetivos estratégicos mediante el alineamiento de los objetivos de Tecnología con los objetivos institucionales, creando valor y generando beneficios dentro y fuera de la institución.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Revisar e incorporar al cronograma para la implementación del Marco de Gestión de TI los gestores y dueños de procesos, con el objetivo de ir conociendo y aplicando las actividades y prácticas de gestión de los procesos.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Establecer por parte de la Administración del Proyecto fechas acordadas y fijas para el rendimiento de cuentas sobre el avance para cada uno de los responsables de las tareas, con la finalidad de asegurar el cumplimiento de lo requerido para los 2 años de implementación y minimizar el riesgo de incumplimiento de aspectos normativos.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Alinear el monitoreo del Gobierno de TI de acuerdo con el cumplimiento de los planes, indicadores, procesos, servicios, métricas de manera periódica de los procesos y servicios que TI ofrece a la Institución con el fin de contribuir al soporte de las metas estratégicas institucionales bajo un enfoque de gestión de riesgos integral para el Gobierno de TI y el Gobierno Corporativo.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Aplicar e implementar de acuerdo con “la guía de implementación para prácticas de gobierno y gestión” el proceso de la Gobernanza de TI, por medio de los objetivos de gobierno y de gestión que apliquen a los procesos del Marco Normativo	31/12/2022	N\A	En proceso con plazo vencido

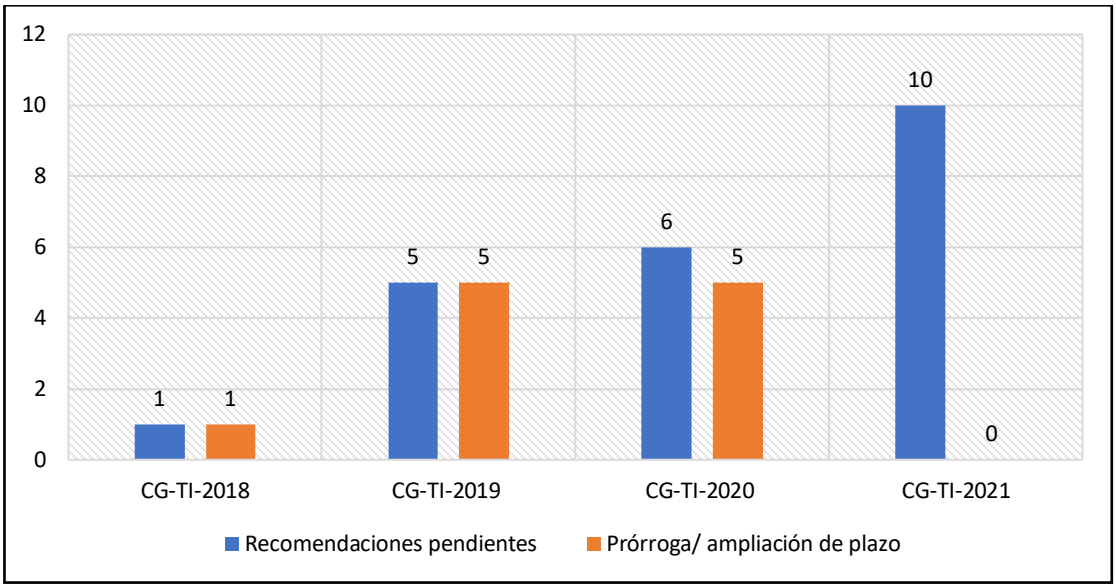
Nombre del informe	Recomendaciones de Auditoría	Fecha límite de cumplimiento	Prórroga/ ampliación de plazo	Condición de la recomendación
Carta de gerencia CG-TI-2021	Revisar y actualizar la versión del procedimiento en la bitácora de control documental, con el fin de mantener un marco normativo con una práctica de actualización anual, aunque no haya sufrido cambio el documento. Valorar la inclusión en el procedimiento de la elaboración de reportes e informes sobre la revisión de perfiles de usuario.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Revisar la regularidad de la participación del personal en talleres y cursos sobre la gestión de la seguridad de la información, reforzar y evaluar los objetivos de aprendizaje para que sean tomados en cuenta en las actividades diarias.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Considerar la incorporación de un recurso para el desarrollo de las tareas como administrador de bases, de acuerdo con el cumplimiento de la implementación de las normas técnicas del MICITT y la implementación de los proyectos de sistemas de información.	31/12/2022	N\A	En proceso con plazo vencido
Carta de gerencia CG-TI-2021	Confeccionar y aprobar un plan de trabajo documentado con las tareas de un administrador de base de datos y controlar dichas actividades por medio de bitácoras de control que sean revisadas periódicamente para control de la segregación de funciones.	31/12/2022	N\A	En proceso con plazo vencido

Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

Las recomendaciones que indican en proceso corresponden a las que están siendo atendidas en alguna medida y que aún no se puede catalogar como cumplidas por parte de esta Auditoría Interna.

Las que indican pendientes, corresponde a las recomendaciones a las que aún no se les realiza ningún proceso de avance para su cumplimiento, normalmente corresponden a observaciones que se pueden categorizar como resientes, pero en este caso corresponde a observaciones que ya cuentan el plazo de implementación vencido y en algunos casos el titular subordinado solicitó ampliación para poder cumplir con su implementación.

Gráfica 2.- Recomendaciones de AE con prorroga o ampliación de plazo vencido.



Fuente: Elaborado por la Auditoría Interna, con información tomada de la MACU.

De la gráfica anterior se logra determinar que únicamente una recomendación del periodo 2020 y todas las recomendaciones del periodo 2021 se encuentran en proceso de implementación con plazos vencidos y no cuentan con gestiones de prorrogas, sin embargo se hace la observación que aplicando un corte al 31 de diciembre del 2023, únicamente tres (3) de estas recomendaciones mantienen un retraso de cero días (esto con respecto a la fecha de la ampliación de plazo, pero si no se toma en cuenta esta ampliación el vencimiento es de 365 días), una (1) recomendación mantienen un atraso de 334 días y las veintidós (22) restantes mantienen más 365 días de atraso en su fecha original de cumplimiento.

3.3 GRADO DE IMPLEMENTACIÓN DE LAS OPORTUNIDADES DE MEJORA QUE SE PLANTEARON EN LA ASESORÍA SOBRE EL INSTRUMENTO DE APLICACIÓN DE PRÁCTICAS DE SEGURIDAD DE LA INFORMACIÓN EN LAS INSTITUCIONES PÚBLICAS.

Mediante oficio INAMU-JD-AI-107-2022, del 29 de agosto del 2022 se realizó la remisión del instrumento denominado “Aplicación de Prácticas de Seguridad de la Información en las Instituciones Públicas” el cual fue solicitado por la Contraloría General de la Republica mediante los oficios 12584 y 12680.

Este instrumento tiene como propósito determinar la aplicación de prácticas de seguridad de la información en las instituciones públicas, con base en el marco regulatorio y prácticas aplicables, con el fin de generar insumos para la toma de decisiones que permitan a la Administración promover mejoras en dicha gestión.

A continuación, se detallan las situaciones que se determinaron producto de la revisión realizada, además de que en el **Anexo 1** presenta la tabla comparativa que incluye todos aquellos rubos en los cuales se obtuvo una respuesta negativa por parte de la Administración Activa en el periodo 2022 y que se compararon contra las respuestas que obtuvimos en el periodo 2023:

Dimensión 1: Estrategia y Estructura:

- No se dispone de un Sistema de Gestión de la Seguridad de la Información (SGSI) alineado con la estrategia institucional.

- En lo que respecta a procedimiento y/o políticas debidamente formalizadas de ciberseguridad, para el periodo 2023, se nos indica que se cuenta con la 16.Política para la Seguridad Física de las Instalaciones de Tecnologías de Información y la 17.Política para la seguridad Lógica de la Plataforma Tecnológica, ambas incluidas dentro del documento Políticas para la Gestión Operativa de Tecnologías de Información el cual fue aprobado por Junta Directiva en la Sesión Ordinaria N° 13-2014 del 2 de febrero del 2014.

La Unidad de Informática, basado en la Política de seguridad de información /ciberseguridad, debe establecer los mecanismos necesarios para asegurar una protección razonable de los activos tecnológicos, activos de información institucionales, dando énfasis en su clasificación como elemento definitorio para establecer los requerimientos de preservación de la confidencialidad, integridad y disponibilidad de la información.

Los procesos institucionales deben considerar los requerimientos de seguridad de la información, de forma tal que proteja y propicie el cumplimiento de los objetivos institucionales, como las responsabilidades que impone el ordenamiento jurídico, normativa vigente y demás compromisos.

Se debe de 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.

- La institución no tiene implementados lineamientos sobre los roles y responsabilidades para el personal encargado de la protección de la información, así como de la ciberseguridad, entendida como el conjunto de herramientas, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, método de gestión de gestión de riesgos, acciones, formalización, prácticas idóneas, seguros y tecnologías que pueden utilizarse para proteger los activos de la organización y los usuarios en el ciberespacio.

- El INAMU no ha formalizado el Plan de contingencia basado en el análisis de impacto al negocio, los Planes de continuidad de negocio para los servicios críticos de la Institución y los Planes, procesos y procedimientos para el manejo de incidentes de seguridad y ciberseguridad (Planes de respuesta).

- La Institución no cuenta con una matriz de riesgos de todos los activos relacionados con la información crítica o sensible.

- No se realizan estudios de impacto sobre el funcionamiento de la entidad, en caso de materializarse riesgos relacionados con la pérdida de activos de información.

- No se han efectuado auditorias para medir la efectividad del sistema de Gestión de Seguridad de la Información.

Dimensión 2: Liderazgo y Cultura:

- Para el periodo 2023 se indica que se aplican mecanismos hacia el personal institucional con el fin de evaluar su percepción y conciencia en material de ciberseguridad, esto mediante comunicamos de la Unidad de Informática.

- No se ha incorporado en el código de ética o de conducta el comportamiento esperado del personal acerca de la recolección y manejo de la información sensible o critica.

Dimensión 3: Procesos e Información:

- La Institución no cuenta con certificaciones relacionadas con el Sistema de Gestión de Seguridad de la Información.

- No se ha identificado y clasificado la información crítica y/o sensible de la institución.

- No se encripta la información almacenada clasificada como crítica o sensible.

- No se cuenta con un Plan de Gestión de Incidentes, la Institución lo que cuenta es con una plataforma tecnológica donde se gestionan los incidentes, solicitudes y servicios de TI, formalmente establecidos.

- El INAMU no ha realizado simulacros o pruebas de manejo de incidentes durante el 2023, se indica que una vez se cuente con el sistema se realizaran simulacros.

- La Institución no cuenta con indicadores que midan el grado de seguridad alcanzado.

- Al 2023 se indica que se realizan pruebas de seguridad de Pentesting, mediante monitoreo y revisión diarias. (Un ***pentesting*** es un conjunto de ataques simulados dirigidos a un sistema informático con una única finalidad: detectar posibles debilidades o vulnerabilidades para que sean corregidas y no puedan ser explotadas).

Dimensión 4: Competencias y Equipos:

- La Institución no cuenta con especialista en seguridad de la información y ciberseguridad.

- En el periodo 2023 se cuenta con planes de capacitación institucionales sobre temas de ciberseguridad, así como con comunicados de la Unidad de Informática.

De acuerdo con lo establecido en las Normas de Control Interno para el Sector Público (N-2-2009-CO-DFOE), en especial en los numerales 1.4 Responsabilidad del jerarca y los titulares subordinados sobre el SCI, 5.8 Control de sistemas de información y 5.9 Tecnologías de información, el jerarca y los titulares subordinados deben velar por que se cumpla al menos los siguientes puntos:

Que los objetivos de seguridad informática estén establecidos, que cumplan los requisitos de la institución y estos se encuentren integrados en los procesos principales.

Que las políticas de seguridad informática sean efectivas desde su implementación.

Hay que asegurar que la implementación de todos los controles de seguridad informática sea coordinada en toda la Institución.

El jerarca Institucional y el Encargado de Informática deben valorar realizar una evaluación de riesgos, orientada a determinar los sistemas que, en su conjunto o en

cualquiera de sus partes, pueden verse afectados directa o indirectamente por amenazas, valorando los riesgos y estableciendo sus niveles a partir de posibles amenazas, las vulnerabilidades existentes y el impacto que pueda causar a la Institución.

Se debe de valorar realizar una Gestión de Riesgos, que implique reducir la probabilidad de que una amenaza ocurra y limitar el impacto si está se manifiesta.

A la fecha de elaboración de este informe no se logró identificar una mejora sustancial en cuanto a la aplicabilidad del Instrumento "***Aplicación de Prácticas de Seguridad de la Información en las Instituciones Públicas"*** y se valida que las preguntas que habían tenido una respuesta negativa en la primera aplicación del instrumento al periodo 2022, se mantienen igual luego de transcurrido un año de aplicado por primera vez.

Es relevante tomar las medidas y técnicas pertinentes para asegurar dentro de la institución la seguridad de la información, la cual se refiere a las medidas y técnicas para asegurar que, dentro de la institución, la información y los sistemas implicados en su tratamiento estén protegidos contra la divulgación a usuarios no autorizados, modificación inadecuada y su falta de acceso cuando se la necesite, ante cualquier amenaza y de cualquier que tenga intensiones maliciosas.

3.4 IMPLEMENTACIÓN DEL DECRETO N°37549-JP REGLAMENTO PARA LA PROTECCIÓN DE LOS PROGRAMAS DE CÓMPUTO EN LOS MINISTERIOS E INSTITUCIONES ADSCRITAS AL GOBIERNO CENTRAL.

Este decreto fue publicado el viernes 1° de marzo del 2013 en La Gaceta N°43, entre sus disposiciones generales se ordena que todo el Gobierno Central e Instituciones Adscritas se propongan diligentemente prevenir y combatir el uso ilegal de programas de cómputo.

Este decreto indica la obligatoriedad de realizar anualmente una auditoría para determinar el cumplimiento de las disposiciones tendientes a la protección de los derechos de autor, relativos a los programas de cómputo. Mediante la auditoría se

deberá verificar los equipos existentes y los programas que tengan las computadoras, así como el número de copias autorizadas de cada programa, comprobando la fecha de instalación, versión de cada uno y ajustado a los términos de licenciamiento.

Si bien es cierto que este Decreto no es de aplicación obligatorio o vinculante para el INAMU, es necesario su análisis como buenas prácticas que permita tener un mayor control en los siguientes puntos:

Garantizar que las computadoras de la institución se utilicen única y exclusivamente con programas de cómputo que cumplan con los derechos de autor correspondientes.

Verificación de los equipos existentes y los programas que tienen instalados estas computadoras, así como el número de copias autorizadas de cada programa, comprobando la fecha de instalación, versión de cada uno y ajustado a los términos de licenciamiento, llevando un control para cada equipo de cómputo, donde conste el funcionario responsable de autorizar la instalación, fecha en que se realiza y la persona responsable de realizar dicha instalación.

Tener un mayor control sobre la fecha de instalación, el vencimiento de las licencias de Software y las fechas de pago de estas, así como la cantidad con que cuenta la institución y los equipos en los cuales están instaladas, respetando así los Derechos de la Propiedad Intelectual.

Establecer y mantener una política de manejo de programas de cómputo para garantizar la adquisición y adecuado uso de programas.

Nuestro país a firmado compromisos internacionales en materia de derechos de autor y ha desarrollado normativa para garantizar su cumplimiento, es por esto por lo que las Instituciones públicas deben mejorar sus esfuerzos para incorporar la propiedad intelectual en la cultura organizacional, en busca de que nuestras Instituciones se desarrollen al ritmo de países desarrollados.

4 CONCLUSIONES.

La Auditoría Interna, realizó el presente estudio con el fin de evaluar el grado de implementación de las recomendaciones pendientes de aplicación por parte de la Unidad de Informática durante el periodo 2023 y es sobre está evaluación que presentamos las siguientes conclusiones:

El seguimiento de las recomendaciones pendientes de implementación se da como parte de un proceso de mejoramiento continuo a nivel institucional que permite el accionar en forma oportuna en los casos en los cuales se mantenga un retraso en la aplicación de procedimientos.

Se debe tener presente que las recomendaciones emitidas por la Auditoría Interna, auditoría externa o cualquier otro ente fiscalizador buscan fortalecer los controles internos institucionales, por lo que es de suma importancia el cumplimiento y aplicación con la mayor brevedad posible, cumpliendo con todo lo indicado para la mejora del proceso.

En lo que respecta a la aplicación del Marco de Gestión de TI, esta recomendación se da por cumplida, sin embargo, se hace la aclaración que dicho Marco cuenta con un tiempo de implementación que abarca tres periodos y se le dará revisión anualmente con el fin de validad su aplicabilidad y actualización correspondiente.

El seguimiento a las recomendaciones emitidas por parte de la auditoría interna y auditorías externas evidencian el vencimiento de los plazos de implementación de todas las recomendaciones pendientes de aplicación, ya que se detalla cómo se han venido modificando los plazos sin que se llegue a una implementación exitosa del proceso solicitado. De la revisión efectuada se concluye que existen atrasos importantes y significativos en la implementación de las recomendaciones, esto originado que a la fecha no existe una estrategia oficializada que permita dar

seguimiento al proceso que se solicitó, esto evidencia que las acciones realizadas no fueron del todo oportunas.

En algunos casos, se consideró que la evidencia aportada por la administración con respecto a algunas recomendaciones no fue suficiente y pertinente se procedió a dejarlas en el estado de avance en el cual se mantenían en la MACU.

En el transcurso de un año calendario no se muestra un avance significativo de las respuestas negativas que se habían obtenido de la aplicación del Instrumento denominado Prácticas de Seguridad de la Información en las Instituciones Públicas, el fin de este instrumento era generar a las Instituciones los insumos necesarios para la toma de decisiones y permitir promover mejoras en materia de seguridad de la información.

Realizar un análisis sobre la aplicabilidad en la Institución del Decreto 37549-JP, esto con el fin de prevenir y combatir el uso ilegal de programas de cómputo y con el fin de cumplir con las disposiciones sobre derechos de autor que establece la Ley N° 6683 y sus reformas y la Ley N°8039 y sus reformas, esto mediante el establecimiento de sistemas y controles previamente establecidos para este fin.

5 RECOMENDACIONES Y OPORTUNIDADES DE MEJORA

De conformidad con las competencias asignadas en los artículos 21 y 22 de la Ley 8292, Ley General de Control Interno, se emiten las siguientes oportunidades de mejora para que sean tomadas en cuenta por parte del jerarca y los titulares subordinados a quienes se dirige este estudio.

RECOMENDACIÓN 1

A LA PRESIDENCIA EJECUTIVA:

En un plazo no mayor a treinta (30) días solicitarle a la Unidad de Informática un informe detallado con las motivaciones de los retrasos en la implementación de las recomendaciones asignadas a la UIN las cuales se dividen de la siguiente forma: Siete (7) recomendaciones emitidas por la auditoría interna, seis con plazo vencido en el periodo 2023 y una cumplida, Veintidós (22) recomendaciones emitidas por la auditoría externa, todas con plazo vencido, algunas de estas presentaron vencimientos desde el periodo 2020 y se les dio una ampliación de plazos los cuales también vencieron sin la debida implementación de la recomendación (*las últimas tres vigentes con ampliación de plazo van a quedar vencidas al 31/12/2023*), el informe debe contener como minino los planes de acción con las fechas estimadas, así como las necesidades tanto de recurso humano como financiero para que la UIN, logre la implementación de las supra recomendaciones.

Durante la revisión efectuada se determina que se presenta poca o nula implementación en el cumplimiento de las recomendaciones, lo que está generando que no se cumpla con los plazos establecidos.

El objetivo de esta recomendación tiene como propósito el poder tomar medidas preventivas sobre el retraso que se presenta en los plazos de cumplimiento de las recomendaciones dirigidas a la Unidad de Informática por parte de los informes emitidos por la auditoría interna y externa.

OPORTUNIDAD DE MEJORA

A LA UNIDAD DE INFORMATICA

En línea con las buenas prácticas Institucionales, realizar un análisis integral del "Decreto 37549-JP" el cual contiene el "***Reglamento para la protección de los programas de cómputo en los Ministerios e Instituciones adscritas al Gobierno Central"*** con el propósito de determinar cuáles practicas pueden o deben implementarse en el INAMU, para prevenir y combatir el uso ilegal de programas de

cómputo, y así cumplir con las disposiciones sobre derechos de autor que establece la Ley 6683 y sus reformas, y la Ley 8039 y sus reformas, derivado de los resultados del análisis indicado presentan a la Presidencia Ejecutiva la ruta de implementación de las acciones de control pertinentes.

6 ANEXOS

Se adjuntan al presente informe los siguientes anexos:

a. **Anexo No.1** Tabla comparativa respuestas de la aplicación del Instrumento de Seguridad de la Información en las Instituciones Públicas.

Anexo 1. Tabla Comparativa Instrume

Cc. Sra. Kattia Calvo Cruz, jefatura, Despacho de la Presidencia Ejecutiva
Sra. Alexandra Gómez Ruiz, asesora, Despacho de la Presidencia Ejecutiva
Sra. Ingrid Trejos Marín, jefatura, Unidad de Informática.
Archivo