Instituto Nacional de las Mujeres
(INAMU)

Informe de Auditoría de Sistemas y Tecnologías de Información

CG-TI 2024

Informe final

San José, 05 de junio del 2025.

Señor (es)(as)
Instituto Nacional de las Mujeres (INAMU)
Unidad de Informática
Presidencia Ejecutiva
Junta Directiva

Estimados (as) señor (es)(as):

Según nuestro contrato de servicios, efectuamos la visita de auditoría externa de TI del período 2024 al Instituto Nacional de las Mujeres (INAMU) y con base en el examen efectuado, observamos ciertos aspectos referentes al sistema de control interno y procedimientos de Tecnología de Información, basados en las "Normas técnicas para el gobierno y gestión de las tecnologías de información" del MICITT, y los estándares establecidos como buenas prácticas según los Objetivos de Control para Información y Tecnología Relacionada – COBIT®., los cuales sometemos a consideración de ustedes en esta carta de gerencia CG-TI 2024.

Considerando el carácter de pruebas selectivas en que se basa nuestro examen, ustedes pueden apreciar que se debe confiar en métodos adecuados de comprobación y de control interno, como principal protección contra posibles irregularidades que un examen basado en pruebas selectivas puede no revelar, si es que existiesen. Las observaciones no van dirigidas a colaboradores en particular, sino únicamente tienden a fortalecer el sistema de control interno y los procedimientos relacionados con las tecnologías de información.

Es importante señalar que la estructura de control interno establecida, incluyendo los procedimientos de control para la actividad sujeta a evaluación, son de entera responsabilidad de la administración de la INAMU.

La auditoría realizada fue requerida por la administración de INAMU, producto de lo anterior, los resultados expresados en el presente informe son de carácter confidencial y deben ser utilizados exclusivamente por las personas autorizadas para tal fin.

DESPACHO CARVAJAL & COLEGIADOS
CONTADORES PÚBLICOS AUTORIZADOS

GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Firmado digitalmente por GERARDO MIGUEL MONTERO MARTINEZ (FIRMA)
Fecha: 2025.06.17 16:52:21 -06'00'

Lic. Gerardo Montero Martínez
Contador Público Autorizado N° 1649
Póliza de Fidelidad Nº 0116FID000680013
Vence el 30 de setiembre de 2025

"Exento del timbre de Ley número 6663. del Colegio de Contadores Públicos de Costa Rica. por disposición de su artículo número 8".

TABLA DE CONTENIDO

I. INTRODUCCIÓN

ORIGEN DEL ESTUDIO

Como parte de la evaluación a los estados financieros del INAMU, realizamos una revisión de los controles generales de la gestión de tecnología de información, con el objetivo de medir el grado de riesgo de la información en lo que respecta a seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica.

La evaluación la realizamos basados en los Objetivos de Control de Tecnologías de Información (COBIT por sus siglas en inglés) emitidos por la "Information Systems Audit and Control Association" (ISACA por sus siglas en inglés) y en general las mejores prácticas de la industria de tecnología de información.

ALCANCE

En esta visita el trabajo fue enfocado principalmente a las siguientes áreas:

1. Verificación del control interno en materia tecnológica con base en la normativa interna establecida.
2. Oportunidades de mejora identificadas en la evaluación.
3. Seguimiento a recomendaciones emitidas en cartas de gerencia de periodos anteriores.

OBJETIVO DEL ESTUDIO

1. Establecer un entendimiento integral de la entidad, así como de la plataforma tecnológica que soporta sus operaciones y documentación asociada.

2. Con el propósito de cumplir con los requerimientos estipulados en la Norma Internacional de Auditoría 315, Entendiendo de la realidad y su entorno y evaluación de representación errónea de importancia relativa y en la Norma Internacional de Auditoría 330, procedimientos del auditor en respuesta a los riesgos evaluados, analizamos la gestión de las tecnologías de información de la INAMU.

PERIODO DE LA AUDITORÍA

El estudio se realizó durante el mes de mayo del 2025 y corresponde a la auditoría del periodo 2024.

LIMITACIONES DEL ESTUDIO

No se presentaron limitaciones durante el estudio de auditoría.

METODOLOGÍA

Para llevar a cabo este trabajo utilizamos una modalidad de análisis de la información suministrada por la administración del INAMU, se realizaron consultas de control interno relacionados con la administración del departamento de TI, seguridad física y lógica de los sistemas de información, continuidad de las operaciones, planificación de las TI, gestión de riesgo tecnológico, proyectos, respaldos, entre otras áreas.

Además, se formularon preguntas sobre la existencia de controles informáticos y se realizaron entrevistas a algunas áreas usuarias, en todos los casos necesarios solicitamos a los colaboradores las evidencias en documentos escritos o en formato digital que respaldaran sus afirmaciones.

II. HALLAZGOS Y RECOMENDACIONES IDENTIFICADAS EN LA EVALUACIÓN

No se identificaron nuevos hallazgos durante el estudio.

III. MATRIZ DE SEGUIMIENTO A RECOMENDACIONES DE AUDITORIAS ANTERIORES

CG 2023	
HALLAZGO 01: POSIBLE DESACTUALIZACIÓN DE LA METODOLOGÍA PARA LA ADMINISTRACIÓN PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIONES	**A la Unidad de Informática:** 1. Actualizar, o en caso de ser necesario, elaborar una nueva metodología para la gestión de proyectos de TI, considerando los siguientes aspectos: a. Acta constitutiva. b. Alcance del proyecto. c. Entregables a desarrollar en el proyecto. d. Recursos no financieros (personal, equipo, materiales, etc.). e. Estimación de recursos financieros (costos, presupuesto). f. Roles/Responsabilidades de involucrados internos y externos. g. Estructura de división de trabajo. h. Hitos/Planes de lanzamiento. i. Dependencias claves. j. Identificación del camino crítico (línea base). k. Cronograma del proyecto. l. Plan de comunicación del proyecto. m. Interesados del proyecto (stakeholders). n. Gestión de riesgos. o. Gestión de la calidad. p. Medición del desempeño (desviaciones, impacto, medidas correctivas). q. Acta de cierre (aprobación de los entregables, análisis de los beneficios obtenidos, lecciones aprendidas).

	2. Establecer una periodicidad para la revisión y actualización (esto último cuando sea necesario) de la metodología de proyectos y sus entregables, para atender esta actividad se recomienda asignar a un colaborador como responsable. 3. A la hora de las revisiones y posibles actualizaciones considerar la normativa nacional en materia de TI, buenas prácticas como COBIT 2019, así como normativa institucional asociada a la gestión de calidad. 4. Mantener registro de las revisiones y actualizaciones en una sección dentro del mismo documento.
COMENTARIOS ADMINISTRACIÓN	La Administración considera que una vez revisadas las recomendaciones la metodología cumple con lo solicitado, a continuación, el detalle: a. Acta constitutiva, si cuenta la metodología con la elaboración del acta respectiva la cual incluye en la fase de inicio los entregables o producto requerido. b. Alcance del proyecto, si cuenta la metodología con este detalle de alcance. c. Entregables a desarrollar en el proyecto, son parte del análisis de requerimientos y el acta constitutiva y en la fase de inicio de un proyecto de TI. d. Recursos no financieros (personal, equipo, materiales, etc.), pero como parte del desarrollo del proyecto se identifican los recursos no financieros. e. Estimación de recursos financieros (costos, presupuesto) la metodología cuenta con el Estudio de Costos que permite identificar los recursos económicos, esto permite presentar el proyecto al Comité Institucional de TI para su valoración e inclusión en el POI del año siguiente. f. Roles/Responsabilidades de involucrados internos y externos, la metodología cuenta con un apartado donde se identifican los involucrados. El Anexo No. 4 contiene la plantilla de la Matriz de identificación de involucrados. g. Estructura de división de trabajo, se ha considerado la matriz de involucrados como parte de la WBS. h. Hitos/Planes de lanzamiento, la metodología cuenta con la identificación y actividades como un entregable correspondiente al Cronograma del proyecto. i. Dependencias claves, corresponde en la metodología a la matriz de involucrados. j. Identificación del camino crítico (línea base), se parte del cronograma de trabajo. k. Cronograma del proyecto, si se cuenta con este documento como parte de la metodología

	l. Plan de comunicación del proyecto, si cuenta la metodología con este apartado. m. Interesados del proyecto (stakeholders), si de identifican en el Acta Constitutiva. n. Gestión de riesgos, si se desarrollan los riesgos como parte de la metodología. o. Gestión de la calidad, si es parte de la metodología. p. Medición del desempeño (desviaciones, impacto, medidas correctivas), este apartado se lleva durante el seguimiento de los proyectos a través de las sesiones de seguimiento. q. Acta de cierre (aprobación de los entregables, análisis de los beneficios obtenidos, lecciones aprendidas), si cuenta la metodología con este apartado el cual culmina un proyecto y da pie a la cancelación de compromisos económicos. Por lo anterior, se considera que al revisar la metodología no requiere de ningún cambio, hasta el momento, está pendiente desarrollar un proceso de revisión anual de la metodología. Se adjunta la aprobación respectiva y el documento vigente, apartado No. 9.
ESTADO	**EN PROCESO** En el manual interno de procedimientos para la formulación, seguimiento y evaluación de proyectos de inversión pública se establece que, los proyectos vinculados a las tecnologías de información y comunicaciones son considerados como proyectos de inversión pública fija, para lo cual se define el capítulo 9, donde se detallan la metodología a seguir para garantizar un adecuado proceso de planificación, desarrollo, revisión, verificación, control y cierre de los proyectos de TI. Esta metodología contiene: introducción, definiciones y el detalle de las fases del ciclo de vida de los proyectos: Inicio, planeación, ejecución, seguimiento y control, y cierre. Además, se nos suministró evidencia de las plantillas utilizadas para la documentación de cada una de las fases del proyecto. Según se indica, esta metodología se encuentra basada en el marco de trabajo del PMBOK 4.0 y se respalda con el Marco de Referencia COBIT 4.1, especificación en el proceso de Administración de Proyectos, por lo cual, es posible que no se incluyan elementos importantes para la realidad actual de la gestión de proyectos de acuerdo con las nuevas versiones de las metodologías y estándares mencionados.

	Se recomienda realizar una comparación entre la metodología establecida y las versiones más recientes del PMBOK y COBIT, así como otros estándares relacionados a la gestión de proyectos.
HALLAZGO 02: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE ACTIVOS. RIESGO BAJO.	
RECOMENDACIONES	**A la Unidad de informática:** 1. Desarrollar, documentar, aprobar y divulgar una propuesta para el desarrollo de una política de escritorio limpio. Considerar que esta política debe ser aplicada a todo el personal que se le haya otorgado permiso de acceso a la documentación, sistemas de información, bases de datos, equipos informáticos o servicios de tecnología de información de la entidad.
COMENTARIOS ADMINISTRACIÓN	Ya fue desarrollada, se adjunta a este documento, la misma está en proceso de revisión por parte del Comité Institucional de TI. Ver evidencia en la carpeta "HALLAZGO 02"
ESTADO	**EN PROCESO** Por medio de la revisión a la documentación suministrada por el INAMU, se identificó la existencia de una política de escritorio limpio por medio del documento **SPTABINV-INAMU-2024 - Política de Pantalla y Escritorio Limpio**, no obstante, la misma se encuentra en proceso de revisión por parte del Comité Institucional de Tecnologías de Información. Por lo anterior, el estado del hallazgo se define en proceso.
HALLAZGO 03: OPORTUNIDADES DE MEJORA EN LA GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. RIESGO MEDIO.	
RECOMENDACIONES	**Al área encargada de la seguridad de la información y ciberseguridad en el INAMU:**

	1. Emitir una política o actualizar lineamientos (según convenga) para gestionar la implementación de un plan de ciberseguridad para la institución de manera que se respalde con las políticas existentes. 2. Comunicar el plan en cuestión a todas las áreas de la institución que se vean implicadas. 3. Revisar y actualizar (esto último cuando sea necesario) el plan de ciberseguridad al menos una vez al año, mantener el registro en el control de versiones.
COMENTARIOS ADMINISTRACIÓN	Mediante la contratación N° 2024LD-000018-0015800001, sobre la adquisición de servicios para el acortamiento de la brecha del INAMU se adquirió el Diseño, desarrollo e implementación de un Sistema de Gestión de la Seguridad de la Información y actualmente se encuentran en proceso de la revisión final de la documentación por parte del Comité Institucional de TI y posteriormente la formalización ante la Junta Directiva.
ESTADO	**EN PROCESO** Por medio del documento denominado **SPTABINV-INAMU-2024 - Plan de Monitoreo y Revisión del SGSI**, se evidencia que se han realizado acciones para subsanar las recomendaciones del hallazgo. Cabe destacar que dicho documento se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva. Por lo anterior, se determina que el estado del hallazgo en proceso.
HALLAZGO 04: EXFUNCIONARIOS ACTIVOS EN EL ACTIVE DIRECTORY INSTITUCIONAL. RIESGO MEDIO.	
RECOMENDACIONES	**Al Departamento de Recursos Humanos:** 1. Tomar en cuenta la normativa vigente y comunicar activamente a la unidad de Tecnologías de Información y Comunicación los funcionarios que cesan actividades en la institución para que TI proceda con la desactivación de las cuentas respectivas de forma proactiva. **A la Unidad de Tecnologías de la Información**

	1. Valorar la actualización o deshabilitación de las cuentas de usuario de colaboradores según su situación actual en la institución y lo informado por el Departamento de Recursos Humanos.
COMENTARIOS ADMINISTRACIÓN	La Unidad de Informática, atiende todas las solicitudes que el Departamento de Recursos Humanos se realiza mediante el Formulario de Servicio Técnico. Por lo que es la única dependencia autorizada en solicitar crear, actualizar, desactivar y eliminar una cuenta de una Personas funcionaria. Ver evidencia en la carpeta HALLAZGO 04, donde se muestran imágenes del Sistema y adicionalmente el procedimiento respectivo.
ESTADO	**CORREGIDO** Producto de la revisión a la información suministrada, fue posible evidenciar la inactivación de las cuentas de los funcionarios que dejaron de laborar en el 2024. Además, se evidenció que cuentan con procedimiento para la gestión de cuentas, roles y perfiles, el cual fue actualizada en el año 2023, además, se nos suministró evidencia de la revisión de los roles y perfiles de los funcionarios del INAMU.
HALLAZGO 05: OPORTUNIDADES DE MEJORA EN EL SISTEMA SARI. RIESGO MEDIO.	

RECOMENDACIONES	**A la Unidad de Informática:** 1. Verifica si los manuales de usuario del sistema SARI están disponibles y en un formato accesible para todos los usuarios. 2. Capacitar a los usuarios para que puedan acceder a las funcionalidades que permiten visualizar el registro de las pistas de auditoría, de acuerdo con los roles de cada usuario. 3. Valorar implementar en los sistemas una única sesión simultánea por usuario (de modo que no se pueda abrir una sesión con un mismo usuario en lugares distintos al mismo tiempo). **A los usuarios expertos de los sistemas:** 1. Una vez que se habilite el registro de pistas de auditoría en los sistemas del INAMU, considerar el realizar revisiones periódicas de dichas pistas de auditoría, con tal de identificar y rastrear irregularidades en las actividades que se realizan dentro del sistema.
COMENTARIOS ADMINISTRACIÓN	1. Los manuales de usuario del Sistema SARI, están disponibles en formato Word y fueron enviados por correo electrónico, ver evidencia en carpeta Hallazgo 5. 2. Conforme con el oficio No. Se da prioridad a la implementación del nuevo sistema SIPGAF. 3. Actualmente el sistema SARI solo permite el inicio sesión desde el equipo de cómputo de la persona funcionaria experta, debido que el sistema es cliente- servidor y requiere una configuración específica para cada persona usuaria y equipo de cómputo. Ver evidencia en la carpeta HALLAZGO 05. Con respecto a la Valoración de implementar en los sistemas una única sesión simultánea por usuario (de modo que no se pueda abrir una sesión con un mismo usuario en lugares distintos al mismo tiempo), no es recomendable con el sistema SIPGAF, dado que si es factible que pueda ingresar a dos sesiones diferentes para facilidad.

ESTADO	**NO APLICA** Por medio de la revisión a la documentación suministrada por el INAMU, se identifica que el sistema SARI será sustituido por el nuevo sistema SIPGAF, el cual, según los informes de avance **20122024 Informe Avance del Proyecto del Sistema SIPGAFv1.0** y **11072024 Informe Avance del Proyecto del Sistema SIPGAF v1_With Digital Signature**, se encuentra actualmente en proceso de implementación en tiempo real. En este contexto, las recomendaciones relacionadas con manuales, capacitación sobre pistas de auditoría y la restricción de sesiones simultáneas pierden vigencia, dado que el enfoque institucional está dirigido a la migración y fortalecimiento del SIPGAF. Por lo anterior, se define el estado del hallazgo en no aplica.

CG 2021	
Actualización de versiones en la documentación interna. Riesgo Normal.	
RECOMENDACIONES	Establecer un mecanismo de control para realizar una revisión anual y en los casos aplicables la actualización de los documentados dejarla referenciada en la bitácora del documento. Actualizar el plan y procedimientos señalados con el objetivo de mantener continuidad razonable de los servicios y la interrupción por eventos o salida de personal no afecte la operativa de las actividades. Establecer un procedimiento para la creación, actualización y cambios de los diferentes documentos normativos, con el objetivo de establecer homogeneidad y estandarizar el proceso de la gestión documental institucional.

COMENTARIOS ADMINISTRACIÓN	La Unidad de informática creó el Protocolo de Actualización de Documentos v1.0 y solicitó la respectiva formalización a la Presidencia Ejecutiva, el cual está en proceso de aprobación, ver carpeta con la evidencia "Actualización de versiones en la documentación interna"
ESTADO	**EN PROCESO** Fue posible evidenciar la existencia del Protocolo de Actualización de Documentos, elaborado en diciembre del 2023 por la Unidad de Informática. Sin embargo, el protocolo se encuentra en proceso de aprobación por parte de la Presidencia Ejecutiva. Además, se nos indicó que existe documentación que no ha sido actualizada desde su elaboración, y se encuentran a la espera de la aprobación del protocolo para realizar las respectivas actualizaciones. Cabe resaltar que, es importante mantener un control de las revisiones y actualizaciones realizadas a la documentación general mediante el control de versiones que contiene cada documento.
Gobierno Corporativo de Tecnologías de Información. Riesgo Elevado	
RECOMENDACIONES	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. 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.

COMENTARIOS ADMINISTRACIÓN	Se adjunta el documento: "Normas-MICITT-Matriz-Guía-Implementación-Prácticas-de-Gobierno-y-Gestión-2021. Ver evidencia en la capeta CG2021.
ESTADO	**EN PROCESO** Se nos suministró la hoja de ruta actualizada de la implementación del Marco de Gestión de TI, donde se muestran las actividades que se encuentran en proceso de implementación. La hoja de ruta detalla aspectos como: proceso, práctica de gobierno o gestión, recomendaciones y el tiempo de implementación. Además, se evidenció que durante el 2024 se trabajó en la gestión de la continuidad, los BIAs y la seguridad de la información. De acuerdo con las pruebas realizadas se considera que este hallazgo se encuentra en proceso y de acuerdo con la hoja de ruta y los documentos mencionados previamente el tiempo de implementación abarca del 2023 al 2025.
Administrador de la base de datos. Riesgo Elevado	
RECOMENDACIONES	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. 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.
COMENTARIOS ADMINISTRACIÓN	Como parte de la Reestructuración del INAMU se está considerando una plaza para bases de datos y otra para ciberseguridad, el proceso está en espera de formalización institucional.

ESTADO	**PENDIENTE** De acuerdo con lo indicado en el comentario de la administración, la reestructuración institucional se encuentra en proceso, ya que actualmente se está considerando una plaza para la administración de bases de datos, con el objetivo de atender las recomendaciones brindadas. No obstante, no se aportó evidencia que respalde esta gestión, por lo tanto, se define el estado del hallazgo en pendiente.
CG 2020	
Evaluación de los SLA´s. Riesgo Normal	
RECOMENDACIONES	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.
COMENTARIOS ADMINISTRACIÓN	La última evaluación fue en el 2023 dado que los sistemas críticos están en proceso de sustitución, tales como SARI, Fomujeres y el Sistema BOSHT. Los sistemas nuevos son: SisRuap y Sipgaf, por lo que se deben actualizar los acuerdos nivel de servicio, debido a que estos sistemas se encuentran en desarrollo e implementación y corresponden al cambio total tecnológico en estos sistemas. Así mismo, se realizó un análisis de impacto BIA que permitió realizar una nueva identificación de los sistemas críticos a nivel institucional.
ESTADO	**PENDIENTE** Según las pruebas realizadas, el INAMU no cuenta un cronograma para la evaluación periódica de los SLA para el periodo auditado, por lo cual no se puede monitorear los indicadores de los acuerdos de

	niveles de servicios definidos, con el fin de delimitar, cumplir y mejorar los servicios. Por lo anterior, este hallazgo se encuentra pendiente.
Gestión del proyecto SIPGAF. Riesgo Elevado	
RECOMENDACIONES	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. 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. 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. Establecer un plan de acción para la depuración y actualización de datos, con el fin de lograr una migración con información confiable y segura.
COMENTARIOS ADMINISTRACIÓN	El sistema SIPGAF se encuentra en etapa de implementación en tiempo real y se realizan informes mensuales de seguimiento para la Auditoría Interna y la Presidencia Ejecutiva. Se adjuntan las evidencias en carpeta CG 2020.
ESTADO	**CORREGIDO** Fue posible evidenciar mediante los informes de seguimiento suministrados por el INAMU que el sistema SIPGAF se encuentra en etapa de implementación en tiempo real, además, se nos indicó que, se realizan capacitaciones a los funcionarios sobre la utilización del sistema.

Sistema de Gestión de la Seguridad de la Información. Riesgo Inaceptable	
RECOMENDACIONES	Definir y documentar de acuerdo con la política de seguridad, la estrategia y el plan de seguridad de la información. 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. Establecer revisiones sobre la aplicación de controles a los equipos utilizados para el teletrabajo, ya sean computadores del INAMU o personales. 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.
COMENTARIOS ADMINISTRACIÓN	Mediante la contratación N° 2024LD-000018-0015800001, sobre la adquisición de servicios para el acortamiento de la brecha del INAMU con la normativa vigente, se solicita el diseño, desarrollo e implementación de un Sistema de Gestión de la Seguridad de la Información mediante, la aplicación de la norma internacional ISO 27001:2022, se desarrollaron los documentos, los cuales están pendientes de revisión y formalización, ver carpeta con las evidencias “Sistema de Gestión de la Seguridad de la Información”. Con respecto a la seguridad de los sistemas de información e infraestructura tecnológica: 1- Actualmente la Unidad de informática cuenta software para equipos cómputo y Servidores, por ejemplo: Licencia de Watchguard EPDR, Licencia de Antivirus de Watchguard, Licenciamiento de Watchguard MDR e integración firewall principal, Licenciamiento SOC Watchguard 24x7x365 que incluye monitoreo, detección de amenazas, respuesta y contención de incidentes y análisis forense sobre todos los equipos de cómputo del dominio de INAMU, Licenciamiento de Cisco Umbrella y Monitoreos 24 x7x365 por parte del MICITT y Licenciamiento de CrowdStrike.

	2- Se cuenta con una contratación en proceso de ejecución N° 2025LD-000001-0015800001 "Servicio de análisis, gestión, control y administración de análisis de vulnerabilidades de la plataforma Tecnológica del INAMU", con el objetivo de obtener un servicio de Análisis de vulnerabilidades para los sistemas de información e infraestructura tecnológica, mediante una herramienta.
ESTADO	**EN PROCESO** Por medio del documento denominado **SPTABINV-INAMU-2024 - Plan de Monitoreo y Revisión del SGSI**, se evidencia que se han realizado acciones para subsanar las recomendaciones del hallazgo. Cabe destacar que dicho documento se encuentra en proceso de revisión y aprobación final. Por lo anterior, se determina que el estado del hallazgo en proceso.
Obsolescencia tecnológica. Riesgo Elevado.	
RECOMENDACIONES	Dar seguimiento a la implementación del equipo indicado para enfrentar oportunamente las necesidades de reemplazo y actualización con el fin de mantener una infraestructura tecnológica.
COMENTARIOS ADMINISTRACIÓN	La Unidad de informática durante los años ha venido de forma progresiva adquiriendo y reemplazando los equipos tecnológicos, por lo tanto, en el año 2024 se realizaron las siguientes contrataciones: • Contratación N° 2024LD-000032-0015800001 "Compra de computadoras portátiles con garantía extendida para el INAMU", se adquirieron 42 laptop para las Personas Funcionaria del INAMU actuales y nuevas. • Contratación N° 2024LD-000056-0015800001 "Compra, configuración, instalación y migración de Equipos Tecnológico para el INAMU", se adquirió 11 impresoras de Alto rendimiento, 9 Ups Rack alto rendimiento y 72 Monitores Ver evidencia en la carpeta denominada "Obsolescencia tecnológica".
ESTADO	**EN PROCESO**

	Por medio de la evidencia suministrada, se constató que la administración ha ejecutado acciones relacionadas con la adquisición de nuevo equipo tecnológico y la contratación de un nuevo sistema de información. Dado lo anterior, las acciones por parte del INAMU aún se encuentran en proceso de implementación, por lo que se define el estado del hallazgo en proceso.
Falta de automatización e integración de los sistemas de información. Riesgo Elevado	
RECOMENDACIONES	Establecer un plan de acción en conjunto con la Unidad de Planificación para atender la gestión del riesgo de fraude. Sensibilizar y enfocar programas de capacitación a los usuarios sobre fraudes informáticos. 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.
COMENTARIOS ADMINISTRACIÓN	Se realizan campañas semanales de culturización del personal en materia de TI y se incluyó como parte de la contratación del Sistema de Seguridad de la Información el desarrollo de las campañas para el 2024, todo lo anterior bajo la supervisión del Comité Institucional de TI, no solo de la Unidad de Planificación e Informática, ver correo con resumen de campañas 2024 en carpeta CG 2020, “Falta de automatización e integración de los sistemas de información”. Mediante la contratación N° 2022LN-000002-0015800001, se adquirió el sistema SIPGAF se encuentra en implementación en tiempo real, por parte de las personas funcionarias del INAMU.

	Durante el año 2024 se realizaron informes de avances del proyecto los cuales se adjuntan. Así mismo, se cuenta con la estructura del Equipo Director del proyecto, conformado inicialmente por la Dirección Administrativa, Jefatura de la Unidad de Planificación y la Unidad de Informática. Ver evidencia en la carpeta CG2020 "Falta de automatización e integración de los sistemas de información".
ESTADO	**CORREGIDO** Por medio de la revisión a la documentación suministrada por el INAMU, se adjuntan los informes de avance **20122024 Informe Avance del Proyecto del Sistema SIPGAFv1.0** y **11072024 Informe Avance del Proyecto del Sistema SIPGAF v1_With Digital Signature**, y se concluye que el sistema SIPGAF se encuentra en implementación en tiempo real, por parte de las personas funcionarias del INAMU. Por lo anterior, se determina que el estado del hallazgo en corregido.
Pruebas al plan de Continuidad de TI (DRP). Riesgo Elevado	
RECOMENDACIONES	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: Pruebas de escritorio: un método para el ejercicio de los planes en los que los participantes revisan y discuten las acciones que se toman sin tener que realizar las acciones. 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. 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.

	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.
COMENTARIOS ADMINISTRACIÓN	Se adjunta el Plan de Continuidad de TI y el Plan de Recuperación ante Desastres, así como el archivo de prueba realizado. Ver la carpeta evidencia "Pruebas al Plan de Continuidad de TI".
ESTADO	**EN PROCESO** Por medio de la revisión a la documentación suministrada por el INAMU, se identificó la existencia de un Plan de Continuidad del Negocio (BCP) y (UIN) por medio de los documentos **Plan de Pruebas de los procedimientos del BCP** y **Plan de Pruebas de los procedimientos del BCP - UIN**, no obstante, esta documentación se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva. Por lo anterior, se determina que el estado del hallazgo en proceso.
D.2 Plan de capacitación sobre continuidad. Riesgo Inaceptable	
RECOMENDACIONES	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.
COMENTARIOS ADMINISTRACIÓN	Mediante la contratación N° 2024LD-000018-0015800001, sobre la adquisición de servicios para el acortamiento de la brecha del INAMU, se adquirió el diseño y desarrollo de los componentes necesarios para la correcta implementación de un Sistema de Gestión de Continuidad de los Servicios y actualmente se encuentran en proceso de revisión final de la documentación por parte del Comité Institucional de TI y posteriormente la formalización ante la Junta Directiva. Ver evidencia en la carpeta "Plan de capacitación sobre continuidad".
ESTADO	**EN PROCESO**

	Por medio de la revisión a la documentación suministrada por el INAMU, se identificó la existencia de un plan de Capacitación y Concientización del Sistema de Gestión de Continuidad de Negocio por medio del documento **SPTABINV-INAMU-2024 - Plan de Capacitación y concientización SGCN**, no obstante la misma se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva. Por lo anterior, se determina que el estado del hallazgo en proceso.
CG 2019	
Capacitación sobre seguridad de la información. Riesgo Inaceptable	
RECOMENDACIONES	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.
COMENTARIOS ADMINISTRACIÓN	Mediante la contratación N° 2024LD-000018-0015800001, sobre la adquisición de servicios para el acortamiento de la brecha del INAMU, se adquirió el diseño, desarrollo e implementación de un Sistema de Gestión de la Seguridad de la Información y actualmente se encuentran en proceso de la revisión final de la documentación por parte del Comité Institucional de TI y posteriormente la formalización ante la Junta Directiva Ver evidencia en la carpeta “Capacitación sobre seguridad de la información”
ESTADO	**EN PROCESO** Por medio del documento denominado **SPTABINV-INAMU-2024 - Informe de Capacitación SGSI**, se evidencia que se han realizado acciones para subsanar las recomendaciones del hallazgo. Cabe destacar que dicho documento se encuentra en proceso de revisión final por parte del Comité Institucional de TI

	y, posteriormente, será formalizado ante la Junta Directiva. Por lo anterior, se determina que el estado del hallazgo en proceso.
Continuidad de los servicios de TI. Riesgo Elevado	
RECOMENDACIONES	Asegurarse que el plan de recuperación ante desastres incluya los siguientes aspectos: Procedimiento para declarar un desastre. 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. Recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI. Medidas que permitan prevenir un desastre. Realizar capacitaciones sobre el plan de recuperación ante desastres y relacionadas con la continuidad de los servicios de TI, al personal respectivo. Elaborar un plan de pruebas para el plan de recuperación ante desastres. Ejecutar el plan de pruebas al menos una vez al año y documentar los resultados.
COMENTARIOS ADMINISTRACIÓN	Mediante la contratación N° 2024LD-000018-0015800001, sobre la adquisición de servicios para el acortamiento de la brecha del INAMU, se adquirió el diseño y desarrollo de los componentes necesarios para la correcta implementación de un Sistema de Gestión de Continuidad de los Servicios y actualmente se encuentran en proceso de revisión final de la documentación por parte del Comité Institucional de TI y posteriormente la formalización ante la Junta Directiva.

ESTADO	**EN PROCESO** Por medio de la revisión a la documentación suministrada por el INAMU, se identificó la existencia de un plan de Capacitación y Concientización del Sistema de Gestión de Continuidad de Negocio por medio de los documentos **SPTABINV-INAMU-2024 - Plan de Capacitación y concientización SGCN** y el documento **Plan de Recuperación ante Desastres (DRP) v4.0**, no obstante la misma se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva. Por lo anterior, se determina que el estado del hallazgo en proceso.
Cuarto de servidores. Riesgo Elevado	
RECOMENDACIONES	Subsanar los siguientes aspectos referentes al cuarto de servidores: 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. 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. 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. 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.

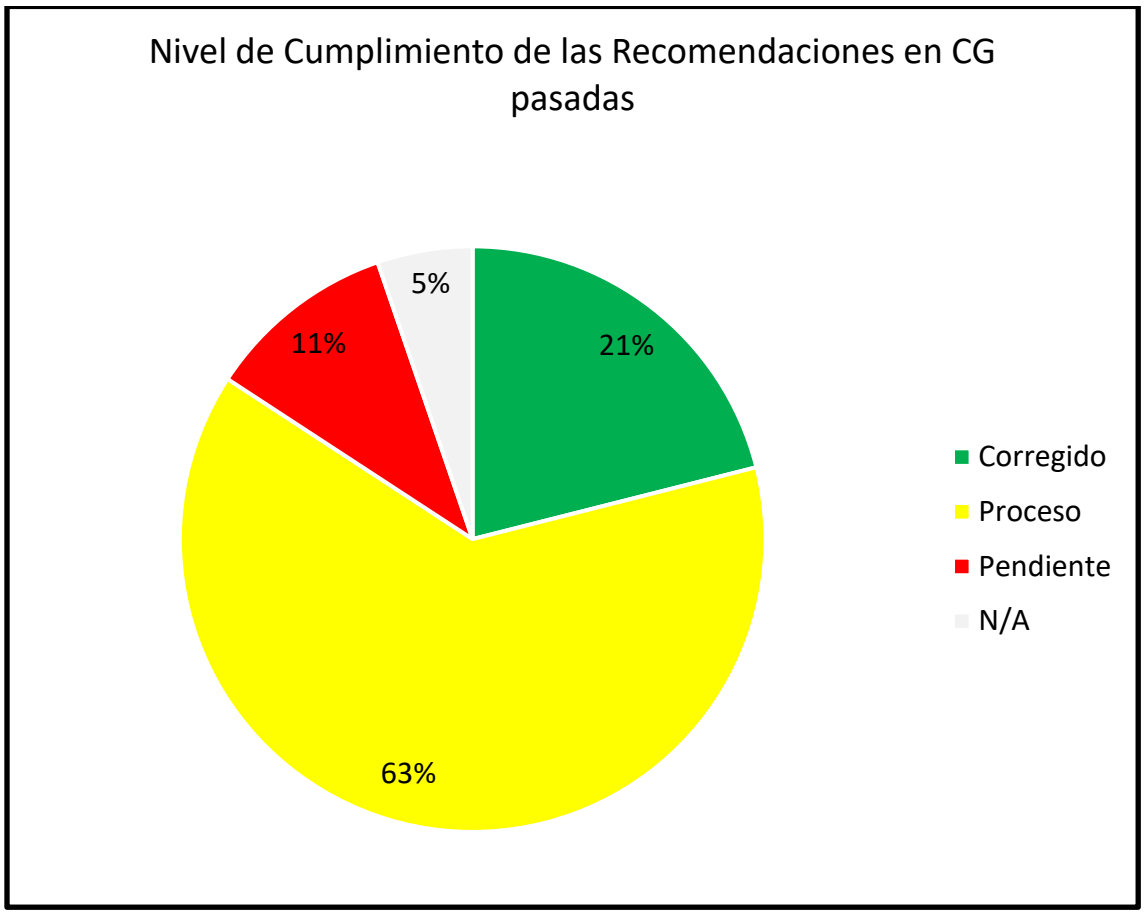
COMENTARIOS ADMINISTRACIÓN	Se envía oficio No. Oficio INAMU-PE-UIN-071-2024, aún sin avances por parte de la Administración.
ESTADO	**EN PROCESO** La Unidad Informática envío una propuesta económica del Edificio SIGMA para agregar una puerta al cuarto de servidores esto con el fin de comenzar a trabajar en la atención del hallazgo, sin embargo, a la fecha no han recibido respuesta por parte de la administración. Por este motivo el hallazgo se encuentra en proceso. Es importante recalcar que la atención del hallazgo es vital para garantizar la integridad y seguridad de las instalaciones de TI y la información gestionada y almacenada.
CG 2018	
Modelo de arquitectura empresarial. Riesgo Elevado	
RECOMENDACIONES	• Elaborar un modelo de arquitectura integral que permita la interrelación de los componentes, con el propósito de que se pueda recopilar información verídica para la toma de decisiones. Se debe considerar al menos lo siguiente: • Objetivo y alcance del modelo de arquitectura de información. • Entradas, salidas y métricas de desempeño del proceso. • Desarrollar modelos de arquitectura del negocio y tecnológica, de manera que se relacionen con el modelo de datos, aplicación y los datos de la Institución con los recursos brindados por la unidad. • Relación entre las aplicaciones y los procesos del negocio (casos de uso por cada uno de los procesos). • Descripción general de las capacidades de los sistemas y el hardware necesarios para asegurar el intercambio de la información entre los componentes. • Definir cómo se aplican los patrones de arquitectura a la Institución, al igual que los patrones de comunicación. • Definir el contexto que describe las relaciones y las interacciones con su entorno en cada una de las vistas (lógica, desarrollo, procesos, física/despliegue).

	• Escenarios para realizar pruebas de concepto. • Identificar por el nombre cada uno de los modelos elaborados. • Valorar el uso de marcos de referencia como guía para crear un modelo de arquitectura de información robusto como TOGAF (The Open Group Architecture Framework) y/o COBIT 5 (Control Objectives for Information and related Technology).
COMENTARIOS ADMINISTRACIÓN	Se elaboró el Modelo de Arquitectura de la Información el cual está vigente y se actualizaron los diagramas de infraestructura en el PETIC 2022-2027, que se pueden visualizar en las páginas 94 y 100.
ESTADO	**CORREGIDO** Se nos suministró el Modelo de Arquitectura de Información del INAMU, el cual se encuentra vigente. Además, se evidenció que en abril del 2024, mediante el PETIC 2022-2027 se actualizaron los modelos de arquitectura actual y propuesta por parte de la Unidad de Informática, específicamente en el apartado: Impacto de la planeación estratégica sobre la arquitectura de la información del INAMU.

A continuación, se resume por periodo el cumplimiento de las recomendaciones emitidas en periodos anteriores:

PERIODO	CORREGIDO	EN PROCESO	PENDIENTE	NO APLICA	TOTAL
2023	1	3	0	1	**5**
2021	0	2	1	0	**3**
2020	2	4	1	0	**7**
2019	0	3	0	0	**3**
2018	1	0	0	0	**1**
TOTAL	**4**	**12**	**2**	**1**	**19**

A continuación, se resume el cumplimiento de las recomendaciones emitidas en informes de auditorías anteriores de manera gráfica:



IV. APÉNDICE

APÉNDICE I: ANÁLISIS DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Periodo 2024

Tipos de Riesgo	
ALTO	A
MEDIO	M
BAJO	B

Alto ☑	Requiere una atención inmediata por su impacto en seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. No se han establecido controles en este nivel de riesgo.
Medio ☑	Requiere una atención intermedia ya que su impacto representaría riesgos sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles insuficientes en este nivel de riesgo.
Bajo ☑	Requiere una atención no prioritaria ya que su impacto no es directamente sobre seguridad, integridad, efectividad, eficiencia, confidencialidad, confiabilidad, disponibilidad y continuidad de la plataforma tecnológica. Se han establecido controles adecuados en este nivel de riesgo.

I. PLANIFICACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

A. PLANIFICACIÓN ESTRATÉGICA DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
A.1.	Se tiene definido un plan estratégico de TI formalmente aprobado y alineado a los objetivos organizacionales.		✓	Se cumple con la condición.	B
A.2.	Se define anual un plan anual operativo de TI con los proyectos y actividades que realiza el área de TI y se encuentra alineado a las iniciativas y objetivos del PETI.		✓	Se cumple con la condición.	B
A.3.	Se le da seguimiento periódico al cumplimiento del PAO.		✓	Se cumple con la condición.	B

B. GESTIÓN DE LA ARQUITECTURA DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
B.1.	Se cuenta con un modelo de arquitectura de información formalmente establecido y aprobado.		✓	Se cumple con la condición.	B

C. GESTIÓN DEL RECURSO HUMANO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
C.1.	Se cuenta con un plan de capacitaciones formalmente establecido.		✓	Se cumple con la condición.	B
C.2.	Las capacitaciones se encuentran justificadas (proyectos de TI, evaluaciones del desempeño).		✓	Se cumple con la condición.	B
C.3.	Se realizan evaluaciones anuales del desempeño de los colaboradores de TI.		✓	Se cumple con la condición.	B
C.4.	Se realizan medidas correctivas para el personal que obtiene calificaciones deficientes en las evaluaciones del desempeño.		✓	Se cumple con la condición.	B

D. GESTIÓN DE PROVEEDORES DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
D.3.	Se realiza un seguimiento al cumplimiento contractual de las responsabilidades de los proveedores.		✓	Se cumple con la condición.	B

E. GESTIÓN DE LA CALIDAD DE LOS SERVICIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
E.4.	La normativa y demás documentación de TI es revisada y actualizada periódicamente.	✗		No se cumple con la condición.	M

F. GESTIÓN DE RIESGOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
F.1.	Se tiene una metodología formalmente establecida y aprobada para la gestión de riesgos de TI.		✓	Se cumple con la condición.	B
F.2.	La evaluación de riesgos de TI es periódica y se encuentra revisada y aprobada por la administración (de acuerdo con el nivel de tolerancia al riesgo organizacional).		✓	Se cumple con la condición.	B

G. GESTIÓN DE ACUERDOS DE NIVEL DE SERVICIO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.1.	Se cuenta con un catálogo de servicios de TI actualizado y aprobado por el Comité de TI.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
G.2.	Se cuenta con una política o procedimiento para la gestión de los acuerdos de nivel de servicio (SLAs) de TI.	✗		No se cumple con la condición, dicha situación está relacionada con el Hallazgo 01-2020Evaluación de los SLA´s.	M
G.3.	Se tiene definido acuerdos de nivel de servicio para cada uno de los servicios activos que se encuentran definidos en el catálogo.		✓	Se cumple con la condición.	B
G.4.	Cada uno de los SLAs tiene establecido las responsabilidades de las partes, indicadores (disponibilidad, capacidad, confiabilidad, etc.) y requerimientos de soporte.		✓	Se cumple con la condición.	B

IV. IMPLEMENTACIÓN DE LAS TECNOLOGÍAS DE INFORMACIÓN.

H. GESTIÓN DE PROYECTOS DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.1.	Se cuenta con una metodología para la gestión de proyectos de TI formalmente establecida.	✗		Se recomienda realizar una comparación entre la metodología establecida y las versiones más recientes del PMBOK y COBIT, así como otros estándares relacionados a la gestión de proyectos.	M

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
H.2.	Se documenta cada una de las fases del ciclo de vida del proyecto para cada uno de los proyectos ejecutados por el área de TI (constitución, estimación de recursos, responsabilidades, cronograma, desempeño, riesgos, calidad, cambios y cierre del proyecto.)	✗			M

I. GESTIÓN DE DESARROLLOS DE SOFTWARE.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
I.1.	Se cuenta con una metodología para el desarrollo e implementación del software.		✓	Se cumple con la condición.	B

J. GESTIÓN DE CAMBIOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.1.	Se cuenta con una política y/o procedimiento para la gestión de cambios de TI.		✓	Se cumple con la condición.	B
J.2.	Los cambios se realizan a través de solicitudes formales y se documenta todo el proceso realizado (ciclo de vida).		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
J.3.	La documentación de los cambios se mantiene de forma centralizada (mesa de servicios).		✓	Se cumple con la condición.	B

K. GESTIÓN DE ACTIVOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
K.1.	Se mantienen controles para el ingreso y salida de equipo tecnológico a la organización.		✓	Se cumple con la condición.	B
K.2.	Se mantiene un inventario actualizado del catálogo de software permitido en la organización.		✓	Se cumple con la condición.	B
K.3.	Se mantiene una política de escritorio limpio.	✗		No se cumple con la condición, dicha situación está relacionada con el hallazgo 02-2023 oportunidades de mejora en la gestión de activos.	B

V. SOPORTE Y SERVICIOS DE TECNOLOGÍAS DE INFORMACIÓN.

L. GESTIÓN DE INCIDENTES.

Ítem	Condición	Vulnerabilidad			Riesgo
		SÍ	NO		
L.1.	Se cuenta con un procedimiento para la gestión de incidentes de TI.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad			Riesgo
		SÍ	NO		
L.2.	La gestión de incidentes se mantiene centralizada (mesa de servicios).		✓	Se cumple con la condición.	B

M. GESTIÓN DE PROBLEMAS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
M.1.	Se cuenta con un procedimiento para la gestión de problemas de TI.		✓	Se cumple con la condición.	B
M.2.	Se identifica, clasifica y analiza la causa raíz de los problemas de TI.		✓	Se cumple con la condición.	B

N. GESTIÓN DE LA CONTINUIDAD DE TECNOLOGÍAS DE INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
N.1.	Se cuenta con un plan de continuidad del negocio (con el componente de TI), formalmente establecido y aprobado por la administración o el Comité de TI.	✗		Se cuenta con un plan de continuidad del negocio y de TI, sin embargo, se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva.	M
N.2.	Se realizan pruebas y capacitaciones sobre el plan de continuidad del negocio.	✗			M
N.3.	Se cuenta con una política y/o procedimiento para la realización de respaldos de información.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
N.4.	Se realizan pruebas a los respaldos de información.		✓	Se cumple con la condición.	B
N.5.	Se tienen medidas de seguridad para los respaldos de información (acceso restringido, traslado de respaldos a un sitio externo).		✓	Se cumple con la condición.	B

O. GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
O.1.	Se cuenta con una política de seguridad de la información formalmente aprobado por la administración y divulgado a nivel organizacional.	✗		Se cuentan con políticas sobre la seguridad de la información, sin embargo, se encuentra en proceso de revisión final por parte del Comité Institucional de TI y, posteriormente, será formalizado ante la Junta Directiva.	M
O.2.	Se le brinda seguimiento al cumplimiento de la política de seguridad de la información (se aplican medidas correctivas) y se le comunica los resultados a la administración.	✗			M
O.3.	Se cuenta con una política de uso de recursos de TI (correo electrónico, equipos, red).		✓	Se cumple con la condición.	B
O.4.	Se cuenta con una política y/o procedimiento para la gestión de cuentas de usuario.		✓	Se cumple con la condición.	B

VI. EVALUACIÓN DE TECNOLOGÍAS DE INFORMACIÓN.

P. VALORAR EL CONTROL INTERNO.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
P.1.	Se han establecido normas para la evaluación del control interno de TI.		✓	Se cumple con la condición.	B
P.2.	Se realizan autoevaluaciones periódicas para que TI identifique de manera proactiva las debilidades de control.		✓	Se cumple con la condición.	B
P.3.	Se ejecutan estudios de auditoría periódicos (internos o externos) para identificar debilidades en el cumplimiento de obligaciones con normativas relativas a TI.		✓	Se cumple con la condición.	B

VII. SISTEMAS DE INFORMACIÓN.

Q. SEGURIDAD LÓGICA Y AUTOMATIZACIÓN DE PROCESOS.

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
Q.1.	Existencia de pistas de auditoría o bitácoras en los sistemas de información que permitan tener una trazabilidad en las transacciones realizadas por los usuarios.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
Q.2.	Se revisan periódicamente las bitácoras de los sistemas de información para identificar comportamientos irregulares en las operaciones de la organización.		✓	Se cumple con la condición.	B
Q.3.	Los sistemas de información permiten solo una única sesión simultánea por usuario, de modo que no se pueda abrir una sesión con un mismo usuario en lugares distintos al mismo tiempo.		✓	Se cumple con la condición, se menciona que para efectos del sistema SIPGAF, es factible operativamente que se pueda ingresar a dos sesiones diferentes para facilidad.	B
Q.4.	Los sistemas de información cuentan con validación de usuarios a través de cuentas y contraseñas (Active Directory, LDAP, otros).		✓	Se cumple con la condición.	B
Q.5.	Se han implementado medidas de seguridad lógica en los sistemas de información (vencimiento, histórico, tamaño y complejidad de la contraseña).		✓	Se cumple con la condición.	B
Q.7.	Los procesos de la organización están totalmente automatizados, evitando la realización de tareas manuales.		✓	Se cumple con la condición.	B
Q.8.	Los sistemas de información se encuentran integrados entre sí, de modo que no se deba enviar información a través de medios externos a los sistemas.		✓	Se cumple con la condición.	B

Ítem	Condición	Vulnerabilidad		Observación	Riesgo
		SÍ	NO		
Q.9.	Se restringe la entrada de datos de modo que el registro de información sea lo más estándar posible.		✓	Se cumple con la condición.	B
Q.10.	Se brindan capacitaciones periódicas en el uso de los sistemas a los usuarios de la organización.		✓	Se cumple con la condición.	B

--Fin del documento--