N° DE INFORME	5.24.10
TIPO DE INFORME	AUDITORIA AL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACIÓN SGSSI
PROCESO	TECNOLOGÍAS DE LA INFORMACIÓN
RESPONSABLES	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN - OTI

EQUIPO AUDITOR

Auditor Líder: Marisol Gutierrez Hernandez
Auditor 1: Jhon Alexander Monroy Trigos (Experto técnico)
Auditor 2: Leney Solarte Zambrano

1. OBJETIVO GENERAL

Verificar que el Sistema de Gestión de Seguridad de la Información -SGSI- implementado en la Agencia de Renovación del Territorio se mantiene de manera eficaz, eficiente y efectiva conforme a los requisitos de la norma ISO/IEC 27001:2022

2. OBJETIVOS ESPECÍFICOS

- Determinar la conformidad del Sistema de Seguridad de la Información acuerdo con los requisitos de la norma NTC/ISO 27001:2022.
- Evaluar la gestión de la información y eficacia de los controles implementados en las dependencias y los procesos de la ART para garantizar que los activos de información estén adecuadamente protegidos de acuerdo a los criterios de seguridad de la información (disponibilidad, confidencialidad, integridad).
- Verificar la implementación de Políticas de Seguridad de la información en los procesos de la ART

3. ALCANCE

La auditoría abarca la evaluación del SGSI sobre el cumplimiento de requisitos de la ISO 27001:2022 en el periodo comprendido entre diciembre de 2024 a noviembre de 2025 y se aplicó a 7 procesos de la Agencia de Renovación del Territorio y las dependencias que los ejecutan o lideran en el nivel central.

4. CRITERIOS (NORMATIVIDAD)

- Norma ISO/IEC 27001:2022
- MI-TI-01.V5 Manual de políticas de seguridad de la información. 2025
- MI-TI-02.V1 Manual de políticas de Tecnologías de la Información. 2021
- MI-TI-03.V3. Manual de Políticas y Procedimientos para la Protección de Datos Personales. 2025
- POL-TI-01 V3 Política General de Seguridad de la Información - 2025
- POL-TI-02.V2 Política de Protección de datos personales 2022
- Documentos del Proceso Tecnologías de la Información CP-TI-03. V1 y demás documentación del SGSI.
- Lineamientos de MinTIC del Modelo de Seguridad y Privacidad de la Información
- Mapa de riesgos de seguridad de la información.
- Directiva Presidencial 03 de marzo 2021.
- Resolución 0500 de 2021 de MinTIC.
- Resolución 0423 de 2021 ART. Por la cual se asignan funciones de oficial de protección de datos personales a la secretaria general y se fijan obligaciones de las áreas.
- Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales

5. PERSONAL ENTREVISTADO

Delegados de cada uno de los procesos auditados

6. METODOLOGÍA

La presente auditoria se ejecutó con base en la norma de auditoria ISO 19011:2018 y el procedimiento de Auditorias al Sistema Integrado de Gestión de la ART (SIG PD-SEM-08 V1) para lo cual se seleccionaron 7 procesos de la entidad y se aplicaron los siguientes procedimientos específicos de auditoría:

- Consulta: Realización de entrevistas y aplicación de listas de verificación o cuestionarios con participación del auditado;
- Observación: Observando el trabajo realizado por el auditado y evidencias (Remoto por aplicativo TEAMS).
- Revisión: Verificando documentos y soportes con participación del auditado
- Inspección: Visita in-situ aplicada para realizar inspecciones en centro de cómputo y área administrativa

Con el fin de cumplir con los objetivos de la presente auditoría, el equipo auditor generó una lista de chequeo con 216 preguntas para verificar el cumplimiento y conformidad de los requisitos de los numerales de la ISO 27001:2022 alineadas con requisitos del Manual de Políticas de SI de la ART y los controles del anexo técnico de la ISO; de acuerdo a lo expuesto en el Plan de Auditoría, se aplicaron las preguntas correspondientes a los numerales (criterios) citados, en cada una de las dependencias que lideran los procesos evaluados; se hicieron pruebas de auditoría con el fin de evaluar los controles y políticas de seguridad implementados en cada dependencia para garantizar que los activos de información estén adecuadamente protegidos. Adicionalmente, se generaron algunas preguntas por la herramienta FORMS para aplicar a los funcionarios de los procesos evaluados.

Dentro de los riesgos de la auditoría se determinaron los siguientes, no materializados en la ejecución:

Riesgo 1. Generar recomendaciones a la Alta Dirección, procesos o áreas evaluadas, que impidan identificar acciones de mejora para el cumplimiento de los objetivos institucionales debido al desconocimiento de los procesos y/o normatividad aplicable por parte del equipo auditor, o por el hecho de no haber detectado debilidades significativas del proceso evaluado.

Acción/tratamiento: Se realizó el conocimiento de área por parte del equipo auditor

Riesgo 2. Posibilidad de que el equipo auditor omita información que podría modificar por completo la opinión dada en el informe, debido a la falta de disponibilidad del responsable del proceso y/o auditados, para atender la visita de auditoría y/o entregar las evidencias o porque no cuentan con las evidencias.

Acción/tratamiento: Se socializó el Plan de Auditoría con memorando 20251010087673 del 20 de noviembre de 2025 y se solicitó y remitió la Carta de Salvaguarda firmada por parte del Líder del Proceso y/o Sistema Auditado (Jefe de la OTI).

Dentro de la presente auditoría no se materializaron los riesgos descritos ni se presentaron limitaciones que afectaran los resultados de la misma; las reuniones y entrevistas se realizaron de acuerdo al cronograma acordado con los lideres de proceso auditados que dio como origen un Plan de Auditoría

ajustado sobre el presentado en la reunión de apertura; sin embargo, en la reunión de cierre se puso a consideración lo siguiente:

- No se contó con la disponibilidad de los recursos humanos respecto al equipo auditor debido a la falta de disponibilidad de funcionarios capacitados como auditores en la norma de manera que se pueda dar un mayor alcance y se ejecuten las auditorias en menor tiempo; en cuanto al cumplimiento de fechas estimadas en el Plan, debido al cruce de actividades relevantes de la mayoría de las dependencias por actividades de cierre de año y planeación 2026, se tuvo que extender y ajustar en términos de tiempo. Para ello se recomienda que se programe la auditoria y se presente la necesidad de conformación y capacitación de un equipo y de acuerdo al procedimiento de Auditorias al SIG, en el primer trimestre del año 2026 con la aprobación de la Alta Dirección en Comité de Gestión y Desempeño.

- En cuanto a la participación de la evaluación a partir del formulario virtual establecido para la presente auditoría, debido a la escaza participación de la evaluación por este medio en algunas de las dependencias auditadas, se requiere mayor compromiso y es pertinente recordar que:

  *La alta dirección debe garantizar que el sistema de gestión de la seguridad de la información logre los resultados previstos.

  *Apoyar las actividades en Seguridad y privacidad de la Información.

  *Dirigir y apoyar a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información.

  *Apoyar a otros roles gerenciales relevantes para demostrar su liderazgo en lo que se refiere a sus áreas de responsabilidad.

Lo anterior, debe atenderse en próximas oportunidades pues podría vislumbrar aparentes debilidades en la implementación del numeral 5.1 Liderazgo y Compromiso, de la ISO 27001: 2022 y numeral 7.3 Conciencia *Las personas que realicen trabajos bajo el control de la organización deberán ser conscientes de:*

a) la política de seguridad de la información;

b) su contribución a la eficacia del sistema de gestión de la seguridad de la información, incluidos los beneficios de un mejor desempeño de la seguridad de la información; y

c) las implicaciones de no cumplir con los requisitos del sistema de gestión de seguridad de la información

7. DESARROLLO

De acuerdo con lo mencionado en la metodología, a continuación se presentan los resultados por numeral y por proceso, de la evaluación realizada a cada uno de los mismos conforme a los numerales de la norma y demás criterios de evaluación.

Numeral 4: Contexto.

Se realizó mesa de trabajo con los delegados del proceso de Direccionamiento Estratégico y Proceso de Tecnologías de la Información, en la cual se indago por:

4. Contexto de la organización

4.1 Comprensión de la organización y de su contexto

4.2 Comprensión de las necesidades y expectativas de las partes interesadas

4.3 Determinación del alcance del sistema de gestión de la seguridad de la información

4.4 Sistema de gestión de la seguridad de la información

Al respecto se observó conformidad en la implementación del Sistema respecto a los criterios señalados anteriormente; de manera general se resalta que: se tiene en Plan Estratégico 2023-2026 Indicador del SGSSI y el Plan de Acción de la OTI alineado al Plan de Acción Institucional. Se aprobó la Estrategia de Seguridad de la Información en Comité de Gestión y Desempeño del mes de Julio del 2025. Se ajusto el documento del Modelo de Operación por procesos en cuanto al contexto (numeral 7), cambios de versión de ISO 27001:2013 a 27001:2022 y en la revisión se mantuvo la información de partes interesadas (numeral 8).

Numeral 5: Liderazgo

De acuerdo con lo revisado en mesas de trabajo con los delegados de los procesos de: Direccionamiento Estratégico, Tecnologías de la Información, Gestión de Proyectos, Gestión del Talento Humano, Fortalecimiento y Desarrollo de Capacidades, Contratación y Gestión Administrativa, se revisaron aspectos asociados a los siguientes numerales:

5. Liderazgo
5.1 Liderazgo y Compromiso
5.2 Política
5.3 Funciones, responsabilidades y autoridades de la organización

Al respecto se observó de manera general Conformidad en la implementación de requisitos y se resalta lo siguiente: se actualizó la Política del Sistema Integrado de Gestión de la ART (SIGART), se integró en el Plan Institucional de Capacitación el programa de capacitaciones del SGSI, se cuenta con el marco normativo conformado por Manuales, políticas y procedimientos documentados y publicados en el repositorio de SIGART, la alta dirección suministra los recursos para el funcionamiento del SGSI y se incluyeron los recursos necesarios para el SGSI dentro de la planeación organizacional, desde al GIT de TH y Comunicaciones se brinda apoyo con las actividades de formación y socializándolas.

En cada uno de los procesos se asignaron los delegados con el fin de cumplir con la implementación del SGSI y Políticas, teniendo en cuenta las funciones de los funcionarios asignados se impartieron las responsabilidades.

De acuerdo a las preguntas realizadas por el FORMS a los funcionarios y contratistas de los procesos auditados, se evaluaron los siguientes temas y se presentan a continuación sus respuestas, observando algunas debilidades en cuanto al conocimiento de generalidades del SGSI de los servidores públicos:

Pregunta	SI	NO / No estoy seguro	Nivel de conocimiento
El líder del proceso, coordinador o jefe de la dependencia, realizo la asignación de roles y responsabilidades de acuerdo a las necesidades y usos de la información del proceso/ dependencia	12	6	67%
Conoce los roles y responsabilidades tiene ud sobre al uso de la información	16	2	89%
Conoce la política de Seguridad de la Información	13	5	72%
Conoce si la política de S.I se encuentra disponible y se comunicó dentro de la ART	12	6	67%
Conoce el /los responsables del sistema SGSI para informar situaciones relacionadas con el mismo	16	2	89%

Se Designó por parte del Jefe/director/ coordinador, un servidor público de su área como delegado de seguridad de la información	15	3	83%
Sabe si se establecieron responsabilidades y deberes de seguridad de la información que sigan siendo válidos después de la terminación del contrato	11	7	61%

Fuente: Resumen cuestionario FORMS – Elaboración propia – Papeles de trabajo equipo auditor

Con lo anterior, se concluye que, si bien se han ejecutado acciones para la implementación de los requisitos de la norma, es importante fortalecer el conocimiento al interior de las dependencias, en lo referido a las responsabilidades y responsables o delegados para socializar la información y velar por la implementación de los lineamientos del sistema en cada dependencia.
Nota: Cabe resaltar que la muestra no es representativa por lo mencionado en las limitaciones del informe debido a la baja participación, no obstante, se requiere incluir dentro de las oportunidades de mejora, la capacitación obligatoria en los aspectos generales del SGSI tal como se menciono en la reunión de cierre.

Numeral 6. Planificación

Se reviso en mesa de trabajo con los delegados del proceso de Tecnologías de la Información el cumplimiento del numeral 6 de la norma con 23 preguntas de las cuales 17 aspectos se evaluaron como "CUMPLE" (74%), un aspecto en "No Cumple" y 5 aspectos como "Cumple Parcialmente"; 18 preguntas se realizaron a los procesos auditados relacionadas con Datos personales y Activos de Información de las cuales consolidando resultados, 13 se evaluaron como Cumple (72%) y 5 con Cumple Parcialmente sobre las cuales se hicieron las observaciones respectivas por proceso. Los numerales evaluados fueron los siguientes, alineados con el Manual de Políticas de Seguridad de la Información MI-TI-01. V5 numerales: 6.1. *ROLES Y RESPONSABILIDADES* y 6.4*. GESTIÓN DE ACTIVOS DE INFORMACIÓN:*
6.1 Acciones para tratar riesgos y oportunidades
6.2 Objetivos de seguridad de la información y planificación para cumplirlos
6.3 Planificación de cambios

Respecto a los criterios evaluados como "CUMPLE" se encuentra conformidad en cuanto a que se demuestra una alineación entre los objetivos y la Política de Seguridad de la Información, el compromiso de la Alta dirección se plasma en la Política de Seguridad de la Información y se materializa en la asignación de recursos, se cuenta con un plan de tratamiento de riesgos de seguridad de la información elaborado en la vigencia 2025, se está realizando la actualización del Mapa de Riesgos, controles y acciones sobre la base del inventario de activos de información; se cumple este numeral en un 73%.

Observación 1:

Criterios: la ISO/CEI 27001:2022 - 6.1.2 Evaluación de riesgos de seguridad de la información, Anexo A 5.7 Inteligencia de amenazas y el MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN Numeral 6.2. INTELIGENCIA DE AMENZAS
Respecto a la definición del plan de implementación de inteligencia de amenazas que debe tener como fin proteger la seguridad de la información y los datos y el seguimiento a su ejecución, se determinó como "NO CUMPLE", dado que se presentó en su lugar un Plan de mantenimiento de Servicios Tecnológicos. Según lo revisado, se hacen seguimientos, se ha trabajado con el equipo del SOC y COLCER para evaluar tendencias y adaptar la infraestructura a partir de los análisis de vulnerabilidades que se generan además a través del contrato con Datasec; Sin embargo, el procedimiento de PD-TI-10 GESTIÓN DE VULNERABILIDADES TÉCNICAS, menciona la elaboración de Plan de tratamiento de vulnerabilidades técnicas y el documento presentado no cumple con lo mencionado tanto en el Manual como en el

procedimiento y no identifica si se definieron los *controles, lineamientos y documentación necesaria para realizar una adecuada identificación de amenazas que permitan recopilar procesar, identificación y analizar ciber amenazas que puedan poner en riesgo la seguridad de la información de la Entidad.*
Recomendación*:* Se sugiere documentar un plan de implementación de amenazas a partir de los seguimientos y resultados de análisis realizados con los contratistas SOC y DATASEC que cumpla con la finalidad y objetivos de acuerdo al procedimiento, manual y la norma.

Las demás observaciones en este numeral se hacen respecto a los aspectos evaluados con "Cumple Parcialmente" referidos a lo siguiente:

Observación 2:
Se tiene procedimiento PD-TI-05.V5 Incidentes de seguridad de la Información de marzo del 2024, en el cual se menciona en condiciones generales la utilización del formato FM-TI-20 Formato de Gestión Incidentes de Seguridad, el cual no se encuentra en uso toda vez que los reportes se hacen a través de la mesa de ayuda y se genera un Excel. En los registros de las actividades del procedimiento, no se encuentra relacionado el formato mencionado, uso o aplicación; por otra parte, una vez revisado algunos de los casos reportados como incidentes en la vigencia 2025 (en su mayoría por disponibilidad de la información y varios por situaciones externas), para los mismos, no se ejecutan las actividades establecidas en el procedimiento.
Recomendación: Revisar y ajustar el procedimiento y adaptar o especificar en qué casos aplica y si se requiere determinar un nivel de impacto o evaluación de los incidentes incluirlo en las políticas del procedimiento. El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información, lo cual debe estar debidamente documentado.

Observación 3:
En la verificación sobre si la ART cuenta con un plan para mantener la seguridad de la información en un nivel adecuado durante interrupciones o se tiene un Plan de continuidad del negocio con los requisitos de continuidad de las TIC, se presenta un documento de 2024 sin embargo no es claro si debe actualizarse cada año y cómo se incluyen las actividades realizadas y presentadas en el Documento Plan de Pruebas 2025, considerando que el mismo, no hace parte de los documentos formales del proceso en SIGART; se tiene un informe de plan de pruebas de julio de 2025 pero no se observa el documento que contenga los requisitos del MinTic para la continuidad del negocio.
Recomendación: Revisar y adaptar los documentos de manera que permita observarse el cumplimiento de requisitos normativos.

Observación 4:
Respecto a la articulación de gestión de incidentes y riesgos de ciberseguridad con la inteligencia de amenazas con el fin de prevenir incidentes de alto impacto para la Entidad, a través del SOC se reportan eventos de seguridad de la información asociados al tema de ciberseguridad, a medida que se reciben se van gestionando; se tiene informe de pruebas de julio de 2025 y se tiene boletín de seguridad de URL maliciosas remitido por FORTINET, sin embargo, no se tiene articulado a nivel de procedimiento y, si bien se ejecutan actividades y se tiene un control, no se tienen documentadas las actividades; Se tiene en un archivo Excel el cual debería hacer parte del procedimiento y se realizan reuniones de seguimiento sobre los casos incluidos en MDS pero no se incluyen todos y no se reportan para efectos del indicador de incidentes, dado que son eventos que se gestionan por el procedimiento de gestión de vulnerabilidades.

Recomendación: considerando que no es clara la articulación de los procedimientos de gestión de incidentes y gestión de vulnerabilidades, se sugiere que se definan las situaciones analizadas y categorizadas de vulnerabilidades y amenazas que harán parte de los reportes de indicadores y para evaluar y prevenir incidentes de alto impacto.

Observación 5:
Para la transferencia o intercambio de información , se verificó si se firman acuerdos de confidencialidad, no divulgación o transferencia. Se tiene Documento técnico de entendimiento con las entidades CGR y MinVivienda, en ambos se observa periodicidad y tipo de información a transferir con clasificación; se observan acuerdos de confidencialidad con CGR (actualizado en sep/2024) y con MinVivienda un convenio (documento técnico) firmado en 2023, sin embargo se observó que no se tiene acuerdo de confidencialidad con MINVIVIENDA.
Recomendación: Suscribir acuerdo de confidencialidad con el fin de dar cumplimiento a los lineamientos establecidos en el Manual de Políticas de SI V5 numeral 8 Transferencia o intercambio de información, numeral 35 Seguridad de las Comunicaciones y numeral 42. Política de Control de Accesos[1]

Numeral 7. Soporte
Se hizo la revisión de la implementación de los siguientes numerales de la ISO 27001:2022 con los delegados de los procesos del Proceso de Tecnologías de la Información, Gestión Administrativa, Gestión del Talento Humano, Contratación y Misionales, con la aplicación de 36 preguntas asociadas a estos ítems y a los requisitos del Anexo técnico así como a las Políticas de Seguridad del SGSI de la ART (11 al proceso de TI y 25 a los demás procesos algunas generales aplicadas a todos y otras específicas de acuerdo a las responsabilidades; 2 determinadas como No Aplica), se cumple con el 94% de los requisitos:

7.1 Recursos
7.2 Competencia
7.3 Toma de conciencia
7.4 Comunicación
7.5 Información documentada
Anexo A numerales: 5.31 Requisitos legales, estatutarios, reglamentarios y contractuales, A 5.33 Protección de registros, 5.36 Cumplimiento de políticas, normas y estándares de seguridad de la información; 6.1 Antecedentes funcionarios; 6.2 Términos y condiciones de empleo; 6.3 Concientización, educación y capacitación en seguridad de la información; 6.4 Proceso Disciplinario; 6.5 Responsabilidades después de la terminación o cambio de empleo; 6.6 Acuerdos de confidencialidad o no divulgación; 6.7 Trabajo remoto, 7.2 Entrada física , 7.3 Asegurar oficinas, salas e instalaciones, 7.4 Monitoreo de seguridad física, 7.5 Protección contra amenazas físicas y ambientales, 7.6 Trabajar en áreas seguras, 7.8 El equipo se colocará de forma segura y protegida, 7.10 Medios de almacenamiento,

[1] Si una Entidad pública, privada, o personal externo requiere acceso a información sensible o crítica, se deben suscribir acuerdos de confidencialidad o de no divulgación para la salvaguarda de la información, y acogerse a los protocolos de intercambio de información establecidos por la Oficina de Tecnologías de la Información, mediante la aplicación de un anexo técnico que se deberá coordinar con las áreas institucionales con competencia en la materia; así como realizar el cumplimiento de la normatividad vigente para la Agencia

7.11 Utilidades de apoyo, 7.12 seguridad del cableado, 7.13 Mantenimiento de equipo, 7.14 Eliminación segura o reutilización de equipos.

Al respecto, se observa cumplimiento de los ítems con algunos aspectos por mejorar, resaltando el cumplimiento de lo siguiente:

7.1 Recursos y 7.2 Competencia:

La Agencia determinó y proporcionó los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del sistema de gestión de seguridad de la información, los servidores públicos a cargo del desempeño del SGSI (en la OTI y en cuanto a los delegados de los procesos) son designados de cuanto a sus perfiles y conocimientos o experiencia, para apoyar el funcionamiento del SGSI y se han tomado acciones para que el personal adquiera la competencia necesaria lo cual se observa en la programación de actividades del PIC; se incluyó en las jornadas de capacitación evaluación de cierre de brechas para analizar la apropiación de conceptos. Para el caso de las asignaciones de delegados para el tema de protección de datos personales, se optó por dejar a los mismos delegados para SI y se realizaron las respectivas capacitaciones con la Superintendencia de Industria y Comercio SIC. Se ajustó el lineamiento disciplinario para tomar acciones contra el personal y otras partes interesadas relevantes que hayan cometido una violación a la política de seguridad de la información con la actualización del Manual de Políticas V5.

7.3 Toma de conciencia

Para la evaluación de este numeral, se aplicó la encuesta de evaluación a los funcionarios y contratistas de los procesos evaluados, en la cual se indagó sobre el conocimiento y aplicación de políticas asociadas al numeral 7 de la norma y a las Políticas de SI de la ART, se observan debilidades asociadas a la Toma de Conciencia considerando que de las 32 preguntas, se obtuvo un nivel de conocimiento del 62% no obstante la oferta y ejecución de capacitaciones de la vigencia 2025; esto se asocia posiblemente a la baja participación de los servidores de la ART en las actividades de capacitación; A continuación se presentan los resultados:

Pregunta	SI	NO/No estoy seguro	Nivel de conocimiento
Conoce como se reportan incidentes	11	7	61%
Conoce sus responsabilidades frente al SGSI	13	5	72%
Ud o su equipo u oficina participó en las inducciones o sensibilizaciones del SGSI	14	4	78%
Conoce si los acuerdos contractuales de trabajo establecen las responsabilidades en materia de SI	14	4	78%
Según sus responsabilidades, debe acceder a información sensible y/o datos semiprivados?	11	7	61%
Los funcionarios y contratistas de su dependencia, cuentan con acuerdos de confidencialidad firmados	16	2	89%
Conoce las sanciones disciplinarias por incumplimiento o violación a las Políticas de Seguridad de la Información	12	6	67%
Conoce quien es el oficial de Protección de Datos de la ART	8	10	44%
Conoce la política de protección de datos y sus lineamientos	13	5	72%
Conoce Cuáles son las bases de datos que se manejan en su dependencia	11	7	61%

Conoce en que actividades de su proceso se recopilan datos de grupos de interés de la ART	13	5	72%
Conoce los mecanismos se aplican para la protección de datos personales de partes interesadas	11	7	61%
Conoce el responsable del manejo de bases de datos y protección de los mismos para salvaguardar la confidencialidad en la dependencia	8	10	44%
Conoce Como se generan y conservan los documentos que recopilen información de las partes interesadas y grupos de interés	12	6	67%
Se pone a consideración del Oficial de Protección de datos nuevas bases de datos o se reportan a este las bases que maneje la Dependencia	5	13	28%
Conoce Medidas de seguridad cuando el contratista trabaje de forma remota para proteger la información	8	10	44%
Como servidor público es consciente de la política de seguridad de la información, su contribución a la mejora del SGSI y las implicaciones de no cumplir con los requisitos	14	4	78%
Conoce los lineamientos en las comunicaciones internas y externas relacionadas con el SGSI	13	5	72%
Conoce cuáles son los procesos establecidos para la comunicación externa sobre el SGSI	10	8	56%
Conoce si existe un procedimiento o plan de comunicación en caso de incidentes de seguridad de la información	12	6	67%
La información documentada en el proceso o dependencia al que pertenece, se encuentra controlada para garantizar la disponibilidad	13	5	72%
Conoce si Se tienen diseñadas e implementas medidas para la protección contra amenazas físicas y ambientales	8	10	44%
Conoce si existe una política de control de accesos	12	6	67%
Conoce e implementa controles para la autenticación segura	13	5	72%
Conoce los activos de información del proceso o dependencia a la cual está vinculado	11	7	61%
Los activos de información tienen asignado un responsable de velar por su seguridad	11	7	61%
Conoce los riesgos asociados a los activos de información a su cargo o de la dependencia	10	8	56%
Los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finalizada la vinculación o relación contractual con la Agencia	15	3	83%
Conoce los lineamientos para realizar la clasificación de la información, de acuerdo con la normativa legal	13	5	72%
Conoce la política de seguridad de los equipos y los lineamientos para el uso adecuado de los equipos de cómputo dentro y fuera de las instalaciones	14	4	78%
Se consumen bebidas o alimentos en los puestos de trabajo cerca de los equipos de cómputo, instalaciones eléctricas, entre otros	6	12	33%
Conoce la política de establecimiento, uso y protección de claves	6	12	33%

Fuente: Resumen cuestionario FORMS – Elaboración propia – Papeles de trabajo equipo auditor

Observación 6:

Si bien se han tomado acciones para adquirir la competencia necesaria o conocimiento de funcionarios a través de las jornadas de capacitación y a los contratistas en el SGSI incluso incluyendo en las minutas obligaciones generales o especificas relacionadas con la seguridad de la información y se exige la firma de acuerdos de confidencialidad los cuales reposan en los expedientes, no se ha evaluado la efectividad de dichas acciones para la toma de conciencia toda vez que no existe la obligatoriedad de presentar un soporte de participación en actividades y aunque se remiten mensualmente los listados de parte del GIT Contratos de los contratistas que ingresan, no se identifica si el 100% adquirieron el conocimiento. Se evidenciaron debilidades de conocimientos generales del SGSI en los resultados de la encuesta de evaluación aplicada a los funcionarios y contratistas de los procesos evaluados que presentaron bajo nivel de conocimiento en los temas indagados referidos en el presente informe como Observaciones puntuales en los procesos evaluados referidas mas adelante, para que se tomen las acciones tanto para funcionarios como para contratistas.

Recomendación: Con el fin de brindar la competencia necesaria de los contratistas, así como la apropiación de conceptos y toma de conciencia en ejercicio de las actividades relacionadas con la seguridad de la información, es importante asegurar que el 100% de los mismos reciben la capacitación, inducción o sensibilización, por lo que se considera necesario establecer en los procedimientos que al inicio de la ejecución contractual o cómo mínimo con la entrega del primer informe, cada contratista y supervisor evidencie la sensibilización sobre el SGSI. Adicionalmente, teniendo en cuenta que desde los GIT de Talento Humano y Contratación se disponen mensualmente de los listados de funcionarios y contratistas que ingresan a la entidad, se realicen las respectivas socializaciones al momento de su ingreso.

7.4 Comunicación

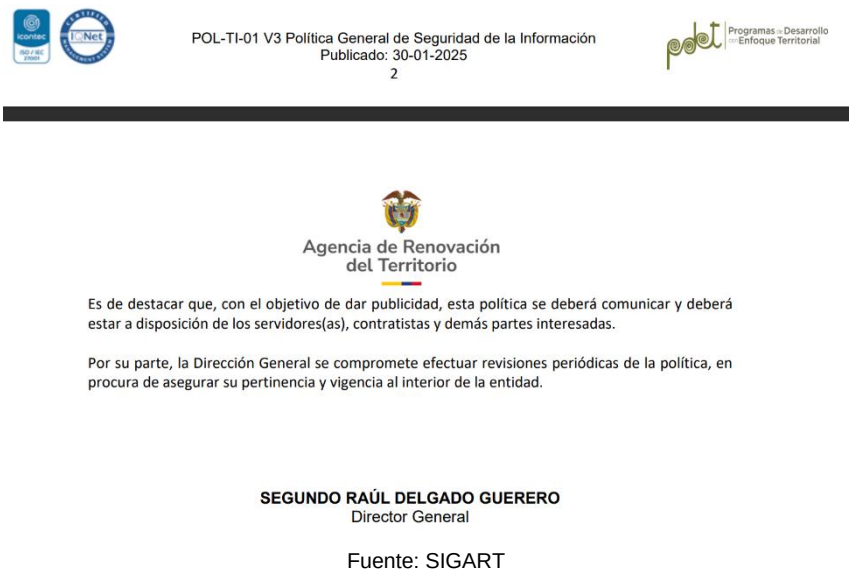
Se tiene claro en las comunicaciones internas el que, cuando, con quien, y como se va a comunicar lo relacionado al SGSI, sin embargo, esta misma dinámica no se observa para las comunicaciones externas en temas de SI. En el Plan de Mejoramiento sobre la Oportunidad de Mejora "Los documentos de Gestión de la Comunicación Externa y Protocolo de Comunicaciones, no incluyen cómo se deben abordar los casos específicos de seguridad de la información, y las comunicaciones en caso de que se materialicen riesgos de seguridad de la información o incidentes para las comunicaciones externas en temas de SI", no se presentaron evidencias de la subsanación de dicha situación y la actividad se determinó como " sin ejecutar" no siendo posible determinar la conformidad del requisito en cuanto a lo mencionado.

Observación 7:

Por otra parte, dentro de la revisión de registros de auditoría, se encontró que la política de S.I se encuentra disponible para las partes interesadas y se comunicó dentro de la entidad, sin embargo, al revisar el enlace en la página web donde se comunica la política, se observó que no se encuentra actualizada la publicación de políticas en el link de transparencia. Se sugiere actualizar la información y el nombre el menú/link https://www.renovacionterritorio.gov.co/#/es/acerca-de-la-entidad/Proteccion-de-datos-personales

Fuente página web ART: https://www.renovacionterritorio.gov.co/#/es/acerca-de-la-entidad/Proteccion-de-datos-personales

Adicionalmente, la política del SGSI actualizada, fue aprobada en Comité de Gestión y Desempeño y el documento que se encuentra publicado en el repositorio SIGART no tiene la firma establecida del Director General por lo cual se recomienda revisar y ajustar:



Fuente: SIGART

7.5 Información documentada:

Se tienen establecidos los métodos de identificación, clasificación y valoración de activos de información, así como la definición de la asignación de responsabilidades, manteniendo mecanismos acordes para el control de riesgos de la información y se hace seguimiento a los activos de información de las dependencias por parte del GIT de Administrativa, quien además realiza capacitaciones y asesorías en cuanto a la disposición de la información; en las dependencias, se han establecido de acuerdo a sus actividades y funciones, roles y reglas para el acceso a la información y conservación, se han establecido lineamientos desde el GIT de Administrativa y en el caso de los proyectos, se definieron los lineamientos y controles de seguridad que se deben tener en cuenta durante el ciclo de vida de los proyectos y se aplica la Guía para el manejo de la gestión documental por cada convenio. La información documentada requerida por el SGSI de la Agencia se encuentra controlada y protegida para garantizar la disponibilidad en los repositorios dispuestos por la entidad (SIGART, MARTE, ONEDRIVE). De manera general, se observa que se aplican las reglas de control de acceso a los sistemas de información, aplicativos de la ART y activos de información de las dependencias**.**

Los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finaliza la relación contractual con la Agencia para lo cual se firma paz y salvo y en las

dependencias se tienen delegados que conservan o revisan la información que hace parte tanto de los activos como de las TRD que fueron objeto de actualización en la vigencia 2025, igualmente se actualizaron los activos de información de las dependencias auditadas (excepto una).
Se llevaron a cabo los controles de verificación de antecedentes de todos los candidatos que ingresaron a la ART en la vigencia tanto de planta como contratistas y se aplican Lista de chequeo con documentos para ingreso aplicada para a verificación de antecedentes, estudios y demás documentos, las cuales reposan en los expedientes. Adicionalmente, se firman los acuerdos de confidencialidad y se conservan en dichos expedientes por funcionario o por contrato. Para el caso de los contratistas, se incluyeron cláusulas especificas relacionadas con la Seguridad de la Información. No se han aplicado sanciones disciplinarias a funcionarios por incumplimiento o violación a las Políticas de Seguridad de la Información.

En cuanto a la verificación de instalaciones para la seguridad de los activos y equipos, se verificó lo siguiente:
Los cables que transportan energía, datos o servicios de información están protegidos contra intercepciones, interferencias o daños: en la inspección realizada se verificó que el cableado está protegido por canaleta metálica y/o bandeja. Se tienen definidos los perímetros de seguridad para proteger las áreas que contienen información sensible y otros activos asociados, las áreas de seguridad donde se custodie información sensible y de acceso restringido cuentan con controles de entrada o seguridad física: El datacenter tiene acceso biométrico para personal de la OTI autorizado, así mismo al ingreso de esta área se debe diligenciar una minuta con los datos de los visitantes con su hora de ingreso y hora de salida y el propósito del ingreso. El área de las ups se tiene ingreso controlado con llave, con acceso por parte de la OTI y de Administrativa. El archivo de las hojas de vida de talento humano se tiene ingreso controlado con llave. Se tiene un circuito cerrado de tv para proteger las áreas sensibles, entre las que se incluyen las que almacenen información, sin embargo, se detectaron 2 cosas por mejorar, la primera es que el área donde se encuentran los expedientes de los contratos no tiene una cámara exclusiva a ésta área y la segunda es que la hora que refleja el circuito de tv estaba al momento de la inspección 4 minutos adelantada, se debe verificar la responsabilidad de esta verificación y por consiguiente sincronización periódica.
Se realizan pruebas de restauración mensualmente sobre diferentes activos que se tienen, entre los que se pueden mencionar, servidores, bases de datos, y backups de usuarios, Hay 2 UPS, una para el datacenter de 20 kva y otra para los computadores de escritorio y demás equipos a través de la red regulada de 60 kva, así mismo, el edificio cuenta con 2 plantas eléctricas distribuidas por pisos, la primera atiende a los pisos 1-26 y la segunda atiene a los pisos 27-41;
Los elementos de los equipos que contienen medios de almacenamiento son verificados para garantizar que todos los datos confidenciales y el software con licencia se hayan eliminado o sobrescrito de forma segura antes de su eliminación o reutilización: De un equipo entregado, se realizan inicialmente los respectivos backups y posteriormente se realiza un borrado seguro utilizando la herramienta “blanco”, garantizando así la confidencialidad de la información

Resultados por Proceso (Oportunidades de mejora sobre los numerales 6 y 7 de la ISO 27001:2022):

Proceso de Fortalecimiento
De los 18 aspectos evaluados con el papel de trabajo de acuerdo a los ítems de la ISO 27001:2025 definidos en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información, activos de información y Política de Protección de Datos personales, se observa cumplimiento en 13 ítems, 3

no cumplen y 2 cumplen parcialmente, un ítem clasifica como No Aplica referido a la transferencia o intercambio de información y si se firman acuerdos de confidencialidad, no divulgación o transferencia.

La Alta Dirección apoya las sensibilizaciones en Seguridad y privacidad de la Información, apoya a las personas para que contribuyan a la eficacia del sistema de gestión de la seguridad de la información, se asignaron las responsabilidades del sistema para informar situaciones relacionadas con el mismo y el delegado cumple con el perfil y funciones asociadas para temas de SI e incluso el tema hace parte de sus compromisos laborales, participa en las capacitaciones realizadas, los activos de información referidos en la matriz actualizada en 2025 tienen asignado un responsable de velar por su seguridad y se identificaron e implementaron reglas para el uso aceptable y para el manejo/acceso de la información con lo cual aseguran que todos los activos de información reciben un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad; la dependencia se asegura que los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual o laboral, se cumple lo estipulado en la política de no almacenamiento de información personal y Política de pantalla limpia de los que están presentes en la reunión. los activos de información a su cargo se encuentran etiquetados con base en los lineamientos establecidos por el GIT de Servicios Administrativos. A través del delegado verifican y supervisan el cumplimiento de las Políticas de Seguridad de la Información en su área de responsabilidad. Los servidores públicos que según sus responsabilidades deban acceder a información sensible cuentan con acuerdos de confidencialidad firmados

Hallazgo 1:

Criterios: ISO/CEI 27001:2022 Numerales 4.2a Comprender las necesidades y expectativas de las partes interesadas, 6.1 Acciones para abordar riesgos y oportunidades, 7.5 Información documentada, 8.3 Tratamiento de riesgos de seguridad de la información; Anexo A numerales; 5.9 Inventario de información y otros activos asociados, 5.33 Protección de registros, 5.34 *Privacidad y protección de la información de identificación personal (PII) Control -La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información.* Anexo A 5.9 *Inventario de información y otros activos asociados. Control: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios.* ANEXO A 5.10 *Uso aceptable de la información y otros activos asociados.* ANEXO A 5.15 *Control de acceso. Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio*

MI-TI-01. V5 Manual de Políticas de Seguridad de la Información. 13. CUMPLIMIENTO (*analiza los requisitos legales aplicables a…la protección de datos personales)*. 6.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

MI-TI-03.V2. Manual de Políticas y Procedimientos para la Protección de Datos Personales *D. LISTADO DE BASES DE DATOS, TRATAMIENTO Y FINALIDAD - 9. Base de datos con el registro de asistentes a las sesiones institucionales y las mesas de impulso. Su finalidad es el control y soporte documental de las sesiones institucionales y mesas impulso llevadas a cabo en el marco de la estrategia Nación-Territorio, a través de ayudas de memoria y lista de asistencia de quienes participan en la sesión.*

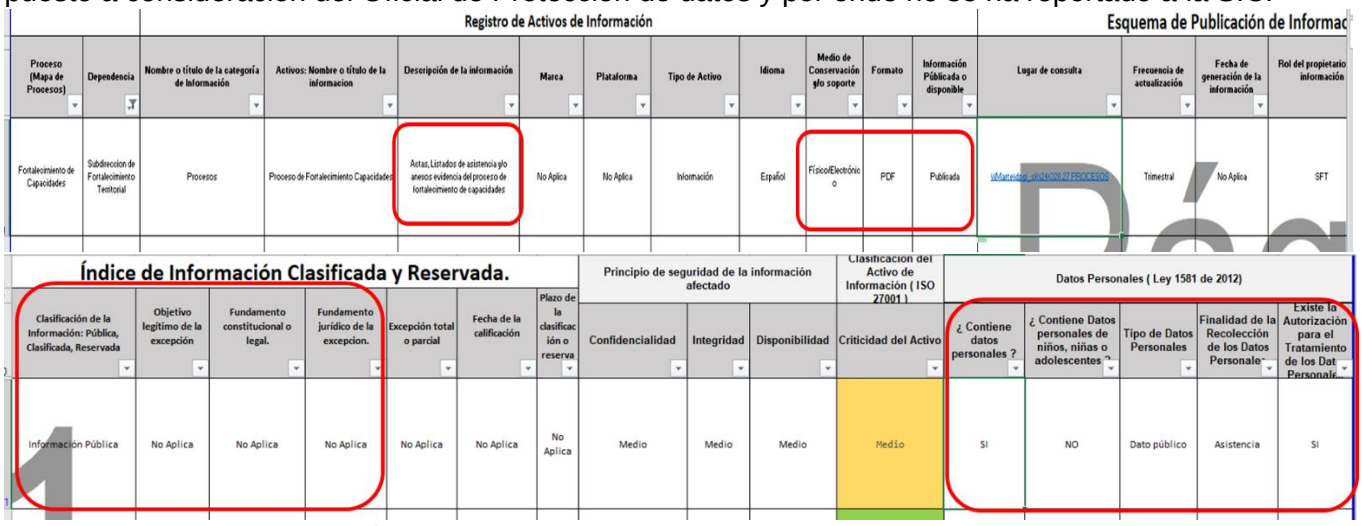
GU-TI-02.V2 Guía de Gestión y Clasificación de Activos de Información. *Todos los activos de información identificados deben etiquetarse de acuerdo con los criterios de confidencialidad, integridad y disponibilidad. Toda información que contenga datos personales deberá sujetarse a las disposiciones legales contenidas en la Ley 1581 de 2012 y las demás que la complementen, modifiquen o sustituyan; así mismo, se deberá regir a la Política de Tratamiento de Datos Personales de la ART, sus procedimientos y formatos, establecidos.*

Resolución 000423 Art 4 Responsabilidades Generales de las Dependencias que hacen Tratamiento de datos personales numeral 3. *Antes de la creación de nuevas bases de datos, someter a consideración del Oficial de Protección de Datos Personales su necesidad y seguir sus lineamientos frente a la recolección, almacenamiento, uso, circulación o supervisión de datos y, en general, lo dispuesto en el Programa Integral de Gestión de Datos Personales sobre el particular.*

Situación evidenciada

Se observa que en la TRD del Proceso de Fortalecimiento en la serie documental 320.031 PROCESOS DE FORTALECIMIENTO DE CAPACIDADES contiene como tipología documental Actas y Registros de Asistencia identificados con Tipo de soporte: Papel-PDF/A. Al realizar la verificación del manejo documental se observan actas en el repositorio MARTE (digital en PDF), sin embargo, no se tienen los registros de asistencia digital de las mesas realizadas en territorio y se informa que dichos documentos se quedan en físico en las Regionales, aunque hacen parte de la TRD de la Subdirección y deberían conservarse y custodiarse en la misma. En el caso de la lista de asistencia revisada no es correspondiente con el formato aprobado en SIGART (FM-ART-12). En la matriz de activos de información, además, se reporta como repositorio un enlace de la vigencia 2024.

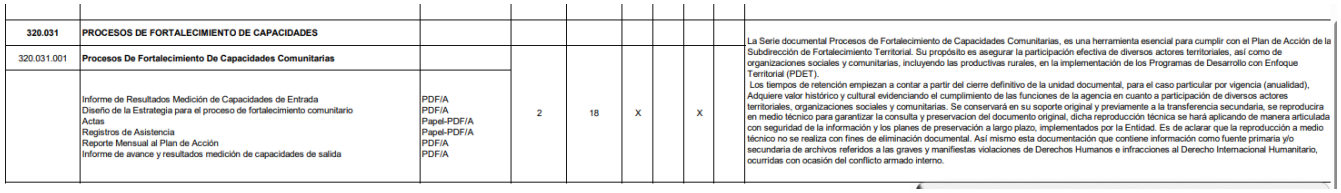
Se presenta un registro de asistencia como ejemplo de una mesa comunitaria realizada en 2025 observando que no tiene el aviso de privacidad (está cortado) y contiene datos personales; al revisar el inventario de activos se observa que los listados de asistencia se clasificaron como *Información Pública*, en un nivel de criticidad y CID *medio*, como *datos públicos* y se trata de datos sensibles, con una finalidad de recolección de *asistencia* pero que se usan para bases de datos y que debe documentarse el aviso de privacidad según la columna AJ de la matriz de inventarios, lo cual no se está cumpliendo; adicionalmente se observa en la clasificación sin fundamento jurídico o legal de excepción para tratarlo como público y no como sensible / reservado. Frente a las bases de datos se informa que no se han puesto a consideración del Oficial de Protección de datos y por ende no se ha reportado a la SIC.



Registro de Activos de Información												Esquema de Publicación de Informac			
Proceso (Mapa de Procesos)	Dependencia	Nombre o título de la categoría de información	Activos: Nombre o título de la informacion	Descripción de la información	Marca	Plataforma	Tipo de Activo	Idioma	Medio de Conservación y/o soporte	Formato	Información Pública o disponible	Lugar de consulta	Frecuencia de actualización	Fecha de generación de la información	Rol del propietario información
Fortalecimiento de Capacidades	Subdireccion de Fortalecimiento Territorial	Procesos	Proceso de Fortalecimiento Capacidades	Actas, Listados de asistencia y/o anexos evidencia del proceso de fortalecimiento de capacidades	No Aplica	No Aplica	Información	Español	Físico/Electrónico	PDF	Publicada	\\Marte\dpgi_sft\24\320.27 PROCESOS	Trimestral	No Aplica	SFT

Índice de Información Clasificada y Reservada.							Principio de seguridad de la información afectado			Clasificación del Activo de Información (ISO 27001)	Datos Personales (Ley 1581 de 2012)				
Clasificación de la Información: Pública, Clasificada, Reservada	Objetivo legítimo de la excepción	Fundamento constitucional o legal.	Fundamento jurídico de la excepcion.	Excepción total o parcial	Fecha de la calificación	Plazo de la clasificación o reserva	Confidencialidad	Integridad	Disponibilidad	Criticidad del Activo	¿ Contiene datos personales ?	¿ Contiene Datos personales de niños, niñas o adolescentes ?	Tipo de Datos Personales	Finalidad de la Recolección de los Datos Personale	Existe la Autorización para el Tratamiento de los Dat Personale
Información Pública	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	No Aplica	Medio	Medio	Medio	Medio	SI	NO	Dato público	Asistencia	SI

Fuente: Matriz de Activos de Información ART 2025



320.031	PROCESOS DE FORTALECIMIENTO DE CAPACIDADES						La Serie documental Procesos de Fortalecimiento de Capacidades Comunitarias, es una herramienta esencial para cumplir con el Plan de Acción de la Subdirección de Fortalecimiento Territorial. Su propósito es asegurar la participación efectiva de diversos actores territoriales, así como de organizaciones sociales y comunitarias, incluyendo las productivas rurales, en la implementación de los Programas de Desarrollo con Enfoque Territorial (PDET). Los tiempos de retención empiezan a contar a partir del cierre definitivo de la unidad documental, para el caso particular por vigencia (anualidad), Adquiere valor histórico y cultural evidenciando el cumplimiento de las funciones de la agencia en cuanto a participación de diversos actores territoriales, organizaciones sociales y comunitarias. Se conservará en su soporte original y previamente a la transferencia secundaria, se reproducira en medio técnico para garantizar la consulta y preservacion del documento original, dicha reproducción técnica se hará aplicando de manera articulada con seguridad de la información y los planes de preservación a largo plazo, implementados por la Entidad. Es de aclarar que la reproducción a medio técnico no se realiza con fines de eliminación documental. Así mismo esta documentación que contiene información como fuente primaria y/o secundaria de archivos referidos a las graves y manifiestas violaciones de Derechos Humanos e infracciones al Derecho Internacional Humanitario, ocurridas con ocasión del conflicto armado interno.
320.031.001	Procesos De Fortalecimiento De Capacidades Comunitarias						
	Informe de Resultados Medición de Capacidades de Entrada Diseño de la Estrategia para el proceso de fortalecimiento comunitario Actas Registros de Asistencia Reporte Mensual al Plan de Acción Informe de avance y resultados medición de capacidades de salida	PDF/A PDF/A Papel-PDF/A Papel-PDF/A PDF/A PDF/A	2	18	X		X

Fuente: \\Marte\dpgi_sft\24\320.27 PROCESOS

Causas: Desconocimiento de parte de las regionales del uso de documentos oficiales que se deben descargar del repositorio SIGART; Falta de seguimiento y revisión de los registros por parte de la Subdirección y desconocimiento de la custodia de acuerdo con las TRD, así como del manejo documental de acuerdo a los lineamientos de Gestión Documental de la ART.

Consecuencia(s): Inadecuada conservación de los documentos, archivos desactualizados y con documentos no clasificados debidamente en la matriz de activos de información y por ende con tratamiento de datos sin autorización expresa, acceso sin restricciones y sin análisis de riesgos y controles de SI.

Recomendación: Es importante que se apliquen los lineamientos frente a la protección de datos y la gestión documental con el fin de que las dependencias responsables identifiquen la adecuada clasificación y evaluación tanto en la matriz de activos de información, como en la matriz de riesgos en la cual se deben describir los controles pertinentes.

Observación 8

De acuerdo a los resultados de la evaluación aplicada a los funcionarios de la Subdirección de Fortalecimiento en la cual participaron 4 servidores públicos, se encontró un bajo nivel de conocimiento acerca del SGSI, toda vez que, de los 38 ítems de la encuesta, en promedio de obtuvo un porcentaje de conocimiento del 44% y se tiene desconocimiento total frente a:

- Quien es el oficial de Protección de Datos de la ART
- El responsable del manejo de bases de datos y protección de los mismos para salvaguardar la confidencialidad en la dependencia
- Si se pone a consideración del Oficial de Protección de datos nuevas bases de datos o se reportan a este las bases que maneje la Dependencia
- Medidas de seguridad cuando el contratista trabaje de forma remota para proteger la información
- Si se tienen diseñadas e implementas medidas para la protección contra amenazas físicas y ambientales

Respecto a la protección de datos todos afirman tener poco conocimiento; De manera general se menciona por algunos de los participantes que: no hay un protocolo de manejo de datos sensibles en la implementación del Plan de Fortalecimiento de Capacidades, *se recogen datos sensibles en las actividades de implementación del Plan de Fortalecimiento de Capacidades pero no se manejan por Marte sino que circulan indistintamente por One Drive, y WhatsApp*; Respecto a la identificación y reporte de riesgos y/o controles relacionados con el tratamiento de datos personales se menciona que se han identificado y se tratan de manera informal.

Recomendación: es indispensable generar un mayor conocimiento y sensibilización en el área sobre los temas relativos a la SI, teniendo en cuenta que se requiere para el fortalecimiento y efectividad del sistema y con ello se sugiere que mensualmente se realicen las capacitaciones de generalidades del SGSI a los funcionarios y contratistas que ingresan a la entidad de acuerdo a la información remitida por el GIT de TH y por el GIT de Contratación, y/o que se disponga de un módulo virtual y el acceso se requiera de manera obligatoria para todos los servidores públicos y expedir certificado para conservar en la HV o en el expediente contractual.

Proceso de Gestión de Proyectos

De los 25 aspectos evaluados con el papel de trabajo de acuerdo a los ítems de la ISO 27001:2025 definidos en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información, activos de información y Política de Protección de Datos personales, se observa cumplimiento en 12 ítems, 6 no cumplen y 6 cumplen parcialmente, un ítem referido a la información sensible y si se firman acuerdos de confidencialidad clasificado como No Aplica.

Se observa conformidad en ítems relacionados con cómo se aplican las reglas de control de acceso a los sistemas de información, aplicativos de la ART y activos de información de la dependencia; la dependencia se asegura que los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finalice la relación contractual o laboral, se cumple lo estipulado en la política de no almacenamiento de información personal y Política de pantalla limpia de los que están presentes en la reunión; protección de registros.

Se definieron los lineamientos y controles de seguridad durante el ciclo de vida de los proyectos; para el manejo de los proyectos y convenios/contratos se definieron lineamientos en la guía de gestión documental de convenio que indica como se debe conservar la información y hacer el cargue en el repositorio (DRIVE) y se tienen dos check list para seguimiento. Se crean drives y se definen los roles y accesos para el manejo de la información tanto precontractual como de ejecución y seguimiento- Supervisor, Coordinador Regional y si aplica, una persona de FCP. Esto queda consignado en los anexos técnicos y se aplica lo establecido en el Manual de gestión documental del FCP y el FUID. Adicionalmente para el manejo se hacen reuniones de trasferencia metodológica que incluyen el tema documental. Se hacen capacitaciones relativas a la gestión documental para el cargue de información si es con el municipio o con ART y allí se carga la información con accesos definidos y esa información es la que se descarga por el funcionario de la ART.

Hallazgo 2

Criterios: ISO/CEI 27001:2022 Numerales 4.2a Comprender las necesidades y expectativas de las partes interesadas, 5.1 Liderazgo y compromiso, 6.1 Acciones para abordar riesgos y oportunidades, 7.2 Competencia. Anexo A 6,3 Concientización, educación y capacitación en seguridad de la información -Control: El personal de la organización y las partes interesadas relevantes deben recibir la conciencia, educación y capacitación adecuadas en seguridad de la información y actualizaciones periódicas de la política de seguridad de la información de la organización, las políticas y los procedimientos específicos del tema, según sea relevante para su función laboral. 7.5 Información documentada, 8.3 Tratamiento de riesgos de seguridad de la información; Anexo A numerales: ANEXO A 5.2 Roles y responsabilidades de seguridad de la información -Control: Los roles y responsabilidades de seguridad de la información;

5.9 Inventario de información y otros activos asociados, 5.33 Protección de registros, 5.34 Privacidad y protección de la información de identificación personal (PII) Control -La organización deberá identificar y cumplir los requisitos relacionados con la preservación de la privacidad y la protección de la información. Anexo A 5.9 Inventario de información y otros activos asociados. Control: Se debe desarrollar y mantener un inventario de información y otros activos asociados, incluidos los propietarios. ANEXO A 5.10 Uso aceptable de la información y otros activos asociados. ANEXO A 5.15 Control de acceso. Las reglas para controlar el acceso físico y lógico a la información y otros activos asociados se establecerán e implementarán en función de los requisitos de seguridad de la información y del negocio. 5.2 Roles y responsabilidades de seguridad de la información

MI-TI-01. V5 Manual de Políticas de Seguridad de la Información. 13. CUMPLIMIENTO (analiza los requisitos legales aplicables a…la protección de datos personales). 6.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN

MI-TI-03.V2. Manual de Políticas y Procedimientos para la Protección de Datos Personales D. LISTADO DE BASES DE DATOS, TRATAMIENTO Y FINALIDAD - 9. Base de datos con el registro de asistentes a las sesiones institucionales y las mesas de impulso. Su finalidad es el control y soporte documental de las sesiones institucionales y mesas impulso llevadas a cabo en el marco de la estrategia Nación-Territorio, a través de ayudas de memoria y lista de asistencia de quienes participan en la sesión.

GU-TI-02.V2 Guía de Gestión y Clasificación de Activos de Información. Todos los activos de información identificados deben etiquetarse de acuerdo con los criterios de confidencialidad, integridad y

disponibilidad. Toda información que contenga datos personales deberá sujetarse a las disposiciones legales contenidas en la Ley 1581 de 2012 y las demás que la complementen, modifiquen o sustituyan; así mismo, se deberá regir a la Política de Tratamiento de Datos Personales de la ART, sus procedimientos y formatos, establecidos.

Resolución 000423 Art 4 Responsabilidades Generales de las Dependencias que hacen Tratamiento de datos personales numeral 3. Antes de la creación de nuevas bases de datos, someter a consideración del Oficial de Protección de Datos Personales su necesidad y seguir sus lineamientos frente a la recolección, almacenamiento, uso, circulación o supervisión de datos y, en general, lo dispuesto en el Programa Integral de Gestión de Datos Personales sobre el particular.

Situaciones evidenciadas

- Respecto a los Activos de Información, la Subdirección de infraestructura no ha revisado, actualizado ni reportado los activos de información de la vigencia 2025 y por ende no se ha actualizado la matriz de riesgos de seguridad de la información. Dado que no se ha evaluado y actualizado el Inventario de Activos de información, no se tiene identificada la existencia de información sensible que necesite la firma de acuerdos de confidencialidad para ello y que se encuentren etiquetados con base en los lineamientos establecidos por el GIT de Servicios Administrativos de acuerdo con su clasificación. Se identificó un activo desactualizado referido a informes de seguimiento.
- La información relevante del ejercicio de las funciones de la dependencia se tiene a cargo de un funcionario en un disco extraíble a cargo de la custodia. La información no está alojada en los repositorios oficiales en cumplimiento de las políticas de Seguridad de la Información y el Disco Duro extraíble no fue reportado como activo de información con el fin de darle un nivel de seguridad. No obstante, lo anterior se han definido reglas de acceso y custodios de información, sin embargo, no se da con ello cumplimiento a los controles del anexo técnico de la norma.
- Frente a las bases de datos, no se observa conocimiento de los delegados y recopilación de la información, no se han puesto a consideración del Oficial de Protección de datos y por ende no se han reportado a la SIC. Se observa que se asignaron las responsabilidades relacionadas con el sistema para informar situaciones relacionadas con el mismo y para cumplir lo establecido en MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN y Protección de datos personales a dos funcionarios, no obstante, se evidencia que de acuerdo a sus funciones y/o carga laboral el conocimiento y manejo de la información asociada a temas de SI se encuentra en otro funcionario no asignado.
- No es evidente cómo desde la Subdirección se garantiza que el SGSI logre los resultados previstos o apoya las sensibilizaciones en Seguridad y privacidad de la Información para que contribuyan a la eficacia del sistema dado que de parte de los delegados no se observa claridad frente a temas asociados a las políticas indagadas.

Causas: Desconocimiento de parte de los funcionarios de los activos de información y controles y conservación de los mismos. Falta de seguimiento y revisión de los registros por parte de la Subdirección y desconocimiento de la custodia de acuerdo con las TRD, así como del manejo documental de acuerdo a los lineamientos de Gestión Documental de la ART.

Consecuencia(s): Inadecuada conservación de los documentos, archivos desactualizados y con documentos no clasificados debidamente en la matriz de activos de información y por ende con tratamiento de datos sin autorización expresa, acceso sin restricciones y sin análisis de riesgos y controles de SI.

Recomendación: Es importante que se apliquen los lineamientos frente a la protección de datos y de la gestión documental con el fin de que los responsables identifiquen la adecuada clasificación y evaluación

tanto en la matriz de activos de información, como en la matriz de riesgos en la cual se deben describir los controles pertinentes.

Observación 9:

No hubo participación significativa en el diligenciamiento del formulario de evaluación (solo 2 personas) y a partir de los resultados de la evaluación aplicada a los funcionarios de la Subdirección de Infraestructura se encontró un conocimiento medio acerca del SGSI, toda vez que, de los 40 ítems de la encuesta, en promedio de obtuvo un porcentaje de conocimiento del 49% y se evidencian debilidades de conocimientos generales frente a:

Política de Seguridad de la Información y sus responsabilidades y contribución a la mejora del SGSI; reportes de incidentes; participación en las inducciones o sensibilizaciones del SGSI; responsabilidades establecidas en acuerdos contractuales; validez de responsabilidades y deberes de seguridad de la información después de la terminación del contrato; acceso a información sensible y/o datos semiprivados; sanciones disciplinarias por incumplimiento o violación a las Políticas de Seguridad de la Información; reconocimiento del oficial de Protección de Datos de la ART y del responsable del manejo y protección de bases de datos en la dependencia; política de protección de datos, de control de accesos, de seguridad de los equipos de cómputo y de establecimiento, uso y protección de claves; bases de datos manejadas en la dependencia; actividades recopilatorias de datos de grupos de interés de la ART; mecanismos para la protección de datos personales; generación de documentos para recopilación de información; identificación de riesgos y/o controles relacionados con el tratamiento de datos personales y procedimientos en caso de incidentes; medidas de seguridad de la información en trabajo remoto; control de información documentada, medidas para la protección contra amenazas físicas y ambientales; activos de información de la dependencia y su responsable y los riesgos asociados; lineamientos de clasificación de la información; y consumo de bebidas o alimentos en los puestos de trabajo.

Respecto a la protección de datos la mitad de los servidores demuestra manejo suficiente, y la otra mitad afirma tener poco conocimiento; Existen incoherencias entre ambas partes, al confirmar y negar la designación de un delegado de seguridad de la información que comunica y retroalimenta la información en cuestión.

Recomendación: es indispensable generar un mayor conocimiento y sensibilización en el área sobre los temas relativos a la SI, teniendo en cuenta que se requiere para el fortalecimiento y efectividad del sistema y con ello se sugiere que mensualmente se realicen las capacitaciones de generalidades del SGSI a los funcionarios y contratistas que ingresan a la entidad de acuerdo a la información remitida por el GIT de TH y por el GIT de Contratación, y/o que se disponga de un módulo virtual y el acceso se requiera de manera obligatoria para todos los servidores públicos y expedir certificado para conservar en la HV o en el expediente contractual.

Proceso Contratación

De los 25 aspectos evaluados con el papel de trabajo de acuerdo a los ítems de la ISO 27001:2025 definidos en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información, activos de información y Política de Protección de Datos personales, se observa cumplimiento en 21 ítems, 0 en no cumple y 1 cumplen parcialmente, 3 ítem clasificados como No Aplica referidos a la información sensible y si se firman acuerdos de confidencialidad.

Se observa conformidad en ítems relacionados con cómo se aplican las reglas de control de acceso a los sistemas de información, aplicativos de la ART y activos de información de la dependencia; la dependencia se asegura que los funcionarios y contratistas hacen la devolución de los activos de

información asignados a su cargo una vez finaliza la relación contractual o laboral, se cumple lo estipulado en la política de no almacenamiento de información personal y Política de pantalla limpia de los que están presentes en la reunión; protección de registros.

Observación 10:

De acuerdo a los resultados de la evaluación aplicada a los funcionarios del GIT de Contratación en la cual participaron **5** servidores públicos, se encontró un nivel medio-alto sobre el conocimiento del SGSI, toda vez que, de los 40 ítems de la encuesta, en promedio de obtuvo un porcentaje de conocimiento del **74**% y se encontraron debilidades por desconocimiento de los siguientes temas:

Reporte de incidentes; designación del delegado de seguridad de la información, del oficial de Protección de Datos de la ART y del responsable del manejo y protección de bases de datos, actividades de datos de grupos de interés; mecanismos de protección e identificación de riesgos frente a datos personales; generación de documentos para recopilación de información; medidas para la protección contra amenazas físicas y ambientales; políticas de control de accesos y de establecimiento, uso y protección de claves; activos de información de la dependencia, sus riesgos y su responsable de seguridad asignado; y consumo de bebidas o alimentos en los puestos de trabajo.

Respecto a la protección de datos la mayoría afirman tener conocimiento en cuanto al nombramiento de un servidor público como enlace y apoyo al Oficial de Protección de Datos; Se conoce claramente la política de establecimiento, uso y protección de claves; se desconoce por la mayoría sobre el consumo de bebidas o alimentos en los puestos de trabajo.

Recomendación: es indispensable generar un mayor conocimiento y sensibilización en el área sobre los temas relativos a la SI, teniendo en cuenta que se requiere para el fortalecimiento y efectividad del sistema y con ello se sugiere que mensualmente se realicen las capacitaciones de generalidades del SGSI a los funcionarios y contratistas que ingresan a la entidad de acuerdo a la información remitida por el GIT de TH y por el GIT de Contratación, y/o que se disponga de un módulo virtual y el acceso se requiera de manera obligatoria para todos los servidores públicos y expedir certificado para conservar en la HV o en el expediente contractual.

Proceso Gestión del Talento Humano

De los 23 aspectos evaluados con el papel de trabajo de acuerdo a los ítems de la ISO 27001:2025 definidos en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información, activos de información y Política de Protección de Datos personales, se observa cumplimiento en 15 ítems, 4 no cumplen y 4 cumplen parcialmente. Con lo anterior, el 33% de los requerimientos no se cumplen a cabalidad.

Se observa conformidad en ítems relacionados con cómo se aplican las reglas de control de acceso a los sistemas de información, aplicativos de la ART y activos de información de la dependencia; la dependencia se asegura que los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finaliza la relación contractual o laboral, se cumple lo estipulado en la política de no almacenamiento de información personal y Política de pantalla limpia de los que están presentes en la reunión; protección de registros.

Se llevaron a cabo los controles de verificación de antecedentes de todos los candidatos que ingresaron a la ART en la vigencia, aunque se sugiere que el formato se codifique e incluya en los documentos estandarizados del Proceso de GTH en SIGART.

Se actualizo la Matriz de Activos de Información y se remitió a la OTI el 15 de julio del 2025.

Se asignaron las responsabilidades sobre el manejo y acceso a la información y delegado para informar situaciones relacionadas con el SGSI y para cumplir lo establecido en MANUAL DE POLÍTICAS DE

SEGURIDAD DE LA INFORMACIÓN, así como delegado para el tema de Protección de datos personales.

Se realizaron Capacitaciones a los delegados de SI y Capacitación de Resolución de Protección de datos personales, sin embargo, en este caso se cambió la delegada y no se evidencia capacitación formal de socialización de responsabilidades como delegada de la SI; No obstante, la funcionaria ha participado en capacitaciones en temas de SI.

Observación 11:

De acuerdo a los resultados de la evaluación aplicada a los funcionarios del GIT de Talento Humano en la cual participaron **4** servidores públicos sobre el SGSI se encontró un alto nivel de conocimiento, toda vez que, de los 40 ítems de la encuesta, en promedio de obtuvo un porcentaje de conocimiento del 84% sin embargo se encontraron situaciones desconocimiento total frente a:

Mecanismos aplicados para la protección de datos personales de partes interesadas; consideración o reporte de nuevas o actuales bases de datos de la dependencia al Oficial de Protección de Datos; identificación o reporte de riesgos y/o controles relacionados con el tratamiento de datos personales; medidas de seguridad de la información en trabajo remoto; y consumo de bebidas o alimentos en los puestos de trabajo.

Recomendación: Es indispensable mantener y mejorar el conocimiento y sensibilización en el área sobre los temas relativos a la SI, para el fortalecimiento y efectividad del sistema dado que no se ha evaluado la efectividad de dichas acciones; se sugiere que desde la OTI mensualmente se realicen las capacitaciones de generalidades del SGSI a los funcionarios que ingresan a la entidad de acuerdo a la información remitida por el GIT de TH, y/o que se disponga de un módulo virtual y el acceso se requiera de manera obligatoria para todos los servidores públicos y expedir certificado para conservar en la HV .

Observación 12:

Se observa una especial falta de conocimiento en el reporte de bases de datos de la dependencia al Oficial de Protección de Datos y en general en todo lo relacionado a tratamiento de datos personales y en cuanto a la actualización de activos de información, considerando que, en la actualización de Activos de información de TH hace falta la inclusión de correos de COPASST, Comité de Convivencia Laboral y de Comisión de personal de acuerdo con la TRD y, que algunos activos clasificados como Información Pública Clasificada con datos semiprivados sobre los mismos se registra que no aplica para la columna de autorización de tratamiento de datos; para el caso del activo "Historias Laborales" que contiene datos sensibles, no se requiere firma de acuerdos de confidencialidad específicos para el manejo de este activo y no está determinado el responsable o custodio del mismo (se refiere GIT TH en la mayoría de los activos). Igualmente, sobre la información recopilada de los funcionarios, se elaboran bases de datos con información de los mismos y en la matriz de activos se determinó que no aplica la autorización de tratamiento de datos personales por lo cual no se solicita. Si bien se ha tratado el tema y se adelantó una reunión entre la OTI y el GIT de TH para analizar el manejo de bases de datos a cargo e identificación de riesgos, en la matriz de riesgos no se tienen identificados riesgos / controles asociados a los activos de información calificados con nivel Alto.

Recomendación: Actualizar la Matriz de Activos de Información y requerir el apoyo y asesoría del Oficial de Protección de Datos para ajustar lo pertinente y hacer el reporte de las bases de datos de acuerdo con los criterios definidos para tal fin en la ART.

Observación 13:

Se encuentran en el repositorio MARTE carpetas de los funcionarios que han finalizado su relación laboral en TH. De acuerdo a los lineamientos de la OTI y de Gestión documental no deberían encontrarse alojadas allí carpetas de back up.

Se observan formatos de acuerdos de confidencialidad firmados por funcionarios sin firma de jefe inmediato, conservados en historias laborales de funcionarios que, aunque no hacen parte de la TRD de GTH se resguardan en las Historias Laborales.

Para la transferencia o intercambio de información, no se firman acuerdos de confidencialidad, para controlar la eliminación, divulgación o transferencia para el caso de reportes o atención de solicitudes de información de la Registraduría Nacional, siendo pertinente incluso implementar el formato FM-TI-02.V4 Acuerdo Intercambio de Información.

Recomendación: Se sugiere revisar si es pertinente incluir el formato de acuerdos de confidencialidad en la TRD del GIT TH o quien debería custodiarlos porque el formato es de la OTI; se deben actualizar los acuerdos firmados y conservados en los expedientes de Hojas de Vida de los Funcionarios que actualmente se encuentran con formatos en versiones anteriores dado que la versión actual es la numero 4, y no tienen firmas de jefes inmediatos.

Proceso Gestión Administrativa

De los 37 aspectos evaluados con el papel de trabajo de acuerdo a los ítems de la ISO 27001:2025 definidos en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información, activos de información y Política de Protección de Datos personales, se observa cumplimiento en 32 ítems, 2 no cumplen y 2 cumplen parcialmente y uno No Aplica. Con lo anterior, el 86% de los requerimientos se cumplen a cabalidad.

De manera general, se observa conformidad en ítems relacionados con cómo se aplican las reglas de control de acceso a los sistemas de información, aplicativos de la ART y activos de información de la dependencia; se tiene documentado e implementado un plan de tratamiento de riesgos de seguridad de la información; la dependencia se asegura que los funcionarios y contratistas hacen la devolución de los activos de información asignados a su cargo una vez finaliza la relación contractual o laboral.

Se actualizo la Matriz de Activos de Información y se remitió a la OTI en julio del 2025.

Se asignaron las responsabilidades sobre el manejo y acceso a la información y delegado para informar situaciones relacionadas con el SGSI y para cumplir lo establecido en MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN, así como delegado para el tema de Protección de datos personales.

Hallazgo 3

Criterios: ISO 27001:2022 Numeral 6.1.1 Generalidades MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN 6.4. GESTIÓN DE ACTIVOS DE INFORMACIÓN. ANEXO A 5.10 Uso aceptable de la información y otros activos asociados, ANEXO A 5.13 Etiquetado de información, Anexo A -5.9 Inventario de información y otros activos asociados

Situación evidenciada: La información no está actualizada en la matriz de activos de información en cuanto a los links de ubicación. En algunos activos se refieren carpetas de 2023 en la actualización de la vigencia 2025. La información se conserva el GIT Administrativa en un repositorio Onedrive sin embargo para el caso de la muestra tomada en la prueba de auditoría, validando por ej. la serie documental correspondiente a Actas de Comité de Bienes, se menciona en la Matriz que el lugar de consulta es en MARTE y no se encuentran registros en la carpeta de Marte, no correspondiendo esto a lo señalado en la matriz de activos de información:

Activos: Nombre o título de la informacion	Medio de Conservación y/o soporte	Formato	Lugar de consulta
Actas Comité Evaluación de Bienes	Físico	Físico	Archivo de Gestion Servicios Administrativos\\marte.honos.col\GIT_AD_2023\240.2 ACTAS\240.2.7 Com_Bie
Actas de Eliminacion Documental	Físico/Electrónico	Físico	Archivo de Gestion Servicios Administrativos \\marte.honos.col\GIT_AD_2023\240.2 ACTAS\240.2.25 Elim_Doc
Actas de Toma Física de Inventario	Físico/Electrónico	Físico	Archivo de Gestion Servicios Administrativos - \\marte.honos.col\GIT_AD_2023\240.2 ACTAS\240.2.41 To_Fis
Historiales de vehiculos	Físico	Físico	Archivo de Gestion Servicios Administrativos- \\marte.honos.col\GIT_AD_2023\240.16 HIS_VEHI
Control de Correspondencia	Físico/Electrónico	WORD/PDF/EXCEL/JPG/SHAPE Y OTROS	\\marte.honos.col\GIT_AD_2023\240.20 INS_CONT
Registro de Préstamos Documentales	Físico/Electrónico	Digital	\\marte.honos.col\GIT_AD_2023\240.20 INS_CONT\240.20.158 Pres_Doc

Fuente: Matriz de Activos de Información ART 2025

Adicionalmente, se evidenció que no se tiene clasificada de manera adecuada dentro de la matriz de activos de información, la clasificación de biométricos (tipo de dato - tipo de activo y manejo o clasificación)

Causas: Desconocimiento de parte de los funcionarios de los activos de información y controles y conservación de los mismos. Falta de seguimiento y revisión de los registros por parte de la Subdirección y desconocimiento de la custodia de acuerdo con las TRD, así como del manejo documental de acuerdo a los lineamientos de Gestión Documental de la ART.
Consecuencia(s): Inadecuada conservación de los documentos, archivos desactualizados y con documentos no clasificados debidamente en la matriz de activos de información y por ende con tratamiento de datos sin autorización expresa, acceso sin restricciones y sin análisis de riesgos y controles de SI.
Recomendación: Es importante que se apliquen los lineamientos frente a la adecuada clasificación y evaluación tanto en la matriz de activos de información, como en la matriz de riesgos en la cual se deben describir los controles pertinentes (para el caso de los biométricos).

Observación 14:
Debilidades en la implementación de controles del Anexo Técnico 7.2 Entrada física - 7.3 Asegurar oficinas, salas e instalaciones -7.4 Monitoreo de seguridad física, 5.15 Control de acceso físico y lógico a la información y otros activos asociados *se establecerán e implementarán en función de los requisitos de seguridad de la información*, 5.33 Protección de registros y numeral 7.5.3 Control de la información documentada de la ISO 27001:2022.

Se tiene un circuito cerrado de tv para proteger las áreas sensibles, entre las que se incluyen las que almacenen información, sin embargo, se detectaron 2 cosas por mejorar, la primera es que el área donde se encuentran los expedientes de los contratos no tiene una cámara exclusiva a ésta área (ésta área es

quien debe solicitarla) y la segunda es que la hora que refleja el circuito de tv estaba al momento de la inspección 4 minutos adelantada, se debe determinar la responsabilidad de esta verificación y por consiguiente sincronización periódica. Adicionalmente, durante la inspección realizada, se encuentra el computador de procesamiento de registros biométrico sin bloqueo de sesión con lo cual se puede vulnerar la seguridad de la información y se incumplen las políticas de SI así como los controles establecidos y/o generar materialización de riesgos.

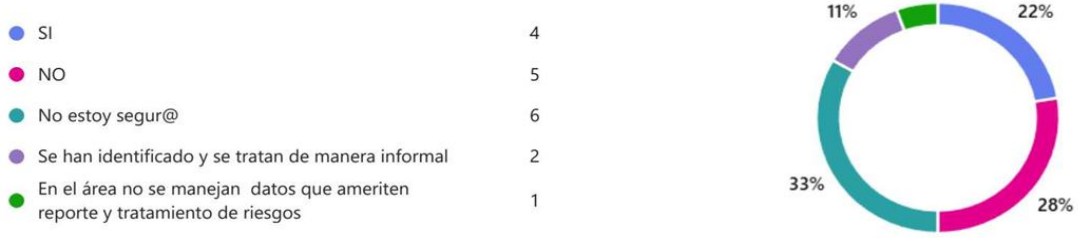
Recomendación: Se sugiere implementar los correctivos necesarios para evitar que se repitan las situaciones expuestas dado que podrían afectar lo referido en los Controles *Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada*

Protección de Datos Personales

De los 22 aspectos evaluados con el papel de trabajo de acuerdo a lo definido en el plan de Auditoria sobre el cumplimento de políticas de Seguridad de la información y Política de Protección de Datos personales, se observa cumplimiento en 14 ítems evaluados, 1 no cumple, 1 cumple parcialmente y 6 No Aplica o No se han presentado. Con lo anterior, el 88% de los requerimientos se cumplen a cabalidad.

En la encuesta de evaluación a los funcionarios de las dependencias se observa un nivel medio de conocimiento de temas asociados al manejo de bases de datos y protección de datos en las dependencias vislumbrado en lo siguiente:

27. En su área o dependencia, se han identificado y reportado riesgos y/o controles relacionados con el tratamiento de datos personales?



Pregunta	SI	NO / No estoy seguro	Nivel de conocimiento
Según sus responsabilidades, debe acceder a información sensible y/o datos semiprivados?	11	7	61%
Los funcionarios y contratistas de su dependencia, cuentan con acuerdos de confidencialidad firmados	16	2	89%
Conoce quien es el oficial de Protección de Datos de la ART	8	10	44%
Conoce la política de protección de datos y sus lineamientos	13	5	72%
Conoce Cuáles son las bases de datos que se manejan en su dependencia	11	7	61%
Conoce en que actividades de su proceso se recopilan datos de grupos de interés de la ART	13	5	72%
Conoce los mecanismos se aplican para la protección de datos personales de partes interesadas	11	7	61%

Conoce el responsable del manejo de bases de datos y protección de los mismos para salvaguardar la confidencialidad en la dependencia	8	10	44%
Conoce Como se generan y conservan los documentos que recopilen información de las partes interesadas y grupos de interés	12	6	67%
Se pone a consideración del Oficial de Protección de datos nuevas bases de datos o se reportan a este las bases que maneje la Dependencia	5	13	28%
Conoce si se han identificado y reportado riesgos y/o controles relacionados con el tratamiento de datos personales	6	12	33%

Fuente: Resumen cuestionario FORMS – Elaboración propia – Papeles de trabajo equipo auditor

Observación 15:
No se ha presentado informe anual sobre el Programa de gestión protección de datos personales en el marco de Comité institucional de gestión y desempeño y no se han actualizado la política de tratamiento de datos personales y el Manual de protección de datos y con ello, la estructura documental del Programa integral de gestión de datos personales.
Recomendación: verificar con la matriz de activos de información, la coherencia e implementación de la política de protección de datos en las dependencias de la ART sobre la clasificación adecuada de los activos, manejo de datos sensibles o privados, aplicación de Autorización de tratamiento de Datos personales y firma de acuerdos de confidencialidad especialmente para información sensible o acuerdos de intercambio de información, así como la generación de bases de datos no reportadas por las dependencias o no asesoradas por el Oficial de protección de datos personales. Adicionalmente, se sugiere fomentar el conocimiento acerca del Manual y Política de Protección de datos personales, roles y responsabilidades y bases de datos.

Numeral 8. Operación
Se hizo la revisión de la implementación de los siguientes numerales con los delegados del proceso de Tecnologías de la Información
8. Operación
8.1 planificación y control operacional
8.2 valoración de riesgos de seguridad de la información
8.3 tratamiento de riesgos de seguridad de la información (Controles tecnológicos relacionados con el anexo A Numeral 8 de la ISO/IEC 27002:222 y dominios de la ISO:27002)

Este numeral se evalúa con un 97% de cumplimiento, de los 37 ítems evaluados con el papel de trabajo, se evidencia cumplimiento de 36 y uno evaluado con No Cumple. De manera general se observa conformidad en el cumplimiento de los requisitos establecidos y revisados para este numeral, controles del anexo técnico y políticas; como debilidad se encuentra lo siguiente:

Observación 16:
En cuanto a si se monitorea, revisa, evalúa y gestionan periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios, se encontró que no se han realizado auditorías y/o revisiones de cumplimiento de requisitos y políticas de seguridad a los proveedores críticos de la Entidad; Se diseño formato Código: FM-TI-16 de Revisión de Políticas Proveedores para el seguimiento a proveedores, sin embargo en 2025 no se evidencia aplicación.
Recomendación: Dar aplicación del formato y realizar la evaluación a proveedores de la vigencia 2025

Numeral 9. Evaluación del desempeño

Se hizo la revisión de la implementación de 12 ítems con los delegados del proceso de Tecnologías de la Información. Frente a los requisitos de este numeral se evalúa con un cumplimiento del 100% con dos recomendaciones respecto a los indicadores revisados, destacando lo siguiente:

Para la medición del SGSI se tienen 4 indicadores del proceso de TI los cuales están alineados a los objetivos del sistema, son medidos periódicamente, se observa ejecución y seguimiento así como presentación de resultados en Comité de Gestión y Desempeño. De la revisión realizada se sugirió lo siguiente:

- Respecto a la Eficacia de capacitaciones: se observa que se mide frente a la apropiación de conocimiento en cada jornada realizada, sin embargo, se considera que para mayor efectividad se tenga un mayor cubrimiento frente al universo y participación teniendo en cuenta que el resultado con corte a junio se tenían 231 participantes que no significa que sea el número de personas capacitadas dado que algunos funcionarios participaron en las diferentes jornadas realizadas. Por lo tanto, se sugiere implementar nuevas estrategias para fomentar un mayor nivel de conocimiento y apropiación del sistema.
- El Indicador Plan Tratamiento de Riesgos se considera importante revisar dado que no mide el nivel de ejecución del plan, se enfocó al cumplimiento en cortes trimestrales y no hay coherencia entre la formula del indicador, la medición y los resultados.

En cuanto a la Revisión por la Dirección se observa cumplimiento sin embargo se sugiere que se documente en acta en caso de que no exista retroalimentación, ni observaciones o acciones de mejora, que los miembros del Comité no tienen ninguna observación ni sugerencia o retroalimentación.

Numeral 10. Mejora.

Se hizo la revisión de la implementación de los siguientes numerales con la evaluación de la implementación de 12 ítems de la Lista de Chequeo, aplicada a los delegados del proceso de Tecnologías de la Información, encontrando conformidad del 75% con 9 de los 12 ítems evaluados como “Cumple”, sobre los cuales se destaca que:

Existe un procedimiento de gestión del cambio, las mejoras del sistema se basan de hallazgos de auditorías, cambios externos e internos que puedan afectar el SGSI, se actualizo la Política el SIG-ART y el Manual de Políticas de SI, se actualizaron los indicadores del SGSI, se actualizo la matriz de activos de la información y se está actualizando la matriz de riesgos, se documentan las acciones sobre los incidentes reportados y analizados.

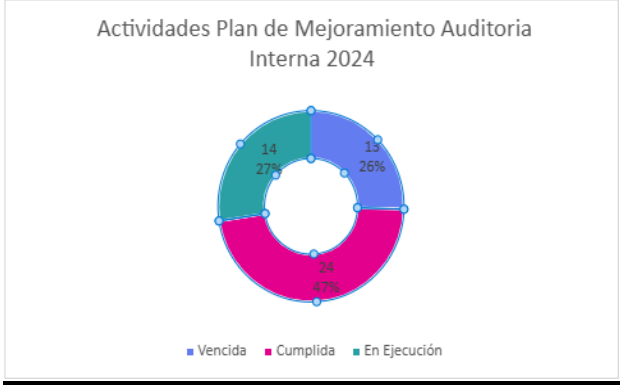
Observación 17:

Se observó en la revisión de ejecución del Plan de Mejoramiento documentado por la OTI sobre la auditoria interna vigencia 2024, que existen debilidades en los análisis de causas realizados de algunas de las acciones no ejecutadas; No se revisó a modo de autocontrol, la eficacia y efectividad de las acciones correctivas tomadas con el fin de identificar previo a la ejecución de la presente auditoría, las actividades vencidas o pendientes de ejecución, así como las evidencias que soportan las acciones ejecutadas sobre lo cual se observó que en algunos casos no corresponden a lo determinado en el plan. Producto de la auditoría interna vigencia 2024 la cual arrojo 16 oportunidades de mejora (H/O), se establecieron 51 actividades en el Plan de Mejoramiento todas para ejecutar dentro de la vigencia 2025. Se evidencia un nivel bajo de ejecución con un 47% de cumplimiento, actividades vencidas, actividades sin soporte real de ejecución o soportes no ajustados a lo determinado en el Plan. Al respecto, es evidente la ausencia de seguimientos preventivos que hubieran permitido la toma de acciones de manera oportuna. A continuación, se expone al detalle lo evidenciado:

CÓDIGO HALLAZGO	DESCRIPCIÓN ACTIVIDAD	ESTADO	OBSERVACIONES REV AUDITORIA 2025
O01AISI24	Actualizar la información histórica del SGSI en el repositorio destinado para tal fin en el SharePoint	Vencida	Efectivamente se observa que se tienen las actas suscritas con los responsables de las áreas en el repositorio sin embargo no se tienen actas de seguimiento como se determinó en el plan de mejoramiento donde se documente el seguimiento a la información del repositorio.
O01AISI24	Velar por el estricto cumplimiento de la Política establecida en el "MI-TI-01 Manual de políticas de seguridad de la información.pdf"	Vencida	Esta actividad no es coherente con acción de mejora y con el producto (meta). Se observa que no hay un análisis de causas de fondo y además es diferente lo que se documentó en esta actividad de esta acción de mejora con lo que se encuentra en el formato de análisis de causas donde dice que la actividad era controles establecidos en el manual de políticas debidamente aplicados y el entregable eran 10 actas de seguimiento y se presentan solo 3 actas que no corresponden a lo mencionado que hacen referencia a 3 actas de aceptación de riesgos firmadas con los responsables
O02AISI24	1. Desarrollar material de consulta que será puesto a disposición de los contratistas.	Vencida	No se evidencia que se haya dispuesto específicamente un espacio (por ej. En Intranet) con la información sobre el sistema y que esto sea comunicado a los contratistas ART y FCP
O02AISI24	6. Envío de cumplimiento de consulta del material propuesto por parte de los contratistas.	En Ejecución	No se presentan evidencias contundentes que permitan soportar la ejecución de actividades y que se subsano lo observado; de acuerdo a la actividad "Envío de cumplimiento de consulta del material propuesto por parte de los contratistas." y acción de mejora propuesta "Proporcionar el material de consulta de las generalidades y los Sistemas de Gestión de la Entidad a los contratistas de ART y FCP." No es claro por ende el producto "11 Reportes" dado que no da cuenta de la efectividad de las acciones con el fin de subsanar lo observado frente a que No se encuentra cubierto el 100% de los contratistas en la participación de las capacitaciones, inducciones o socializaciones.
O03AISI24	3. Socializar el protocolo de comunicaciones.	Vencida	Pendiente evidencia
O04AISI24	1. Incluir dentro del plan de sensibilización y capacitación en Seguridad de la Información de la vigencia 2025 las evaluaciones de efectividad.	Cumplida	Aunque la actividad se encuentra cumplida, No se considera efectiva dado que no se asegura desde la entidad que todos los funcionarios y contratistas que llegan a la entidad reciben la información y se hace el cierre el brechas. Se sugiere que se lidere desde la OTI con los listados de asistencia de TH y de contratos y que se haga mensualmente
O06AISI24	Aplicar la lista de chequeo de forma semestral según el cronograma establecido	Vencida	PENDIENTE EVIDENCIA
O07AISI24	1. Incluir dentro del informe de revisión por la dirección 2024 que se presenta en el 2025 el plan de mejoramiento de la Auditoría al SGSI 2023 y los avances del mismo.	Vencida	Se observa que la unidad de medida se determino como "plan de Mejoramiento actualizado", no obstante la actividad se refiere a la inclusión en el informe de revisión por la dirección" lo cual se observa cumplido. Adicionalmente, la acción de m ejora indica "Realizar reporte semestral al Comité Institucional de Gestión y Desempeño de los planes e mejoramiento y avance de los mismos. " correspondiendo esto a una actividad y no a un acción de mejora
O08AISI24	Revisar de forma exhaustiva el inventario de activos de información de cada uno de los procesos de la entidad	Vencida	Solamente se presenta como evidencia 1 acta de socialización de Matriz de Riesgos de la SAM. No se cumplió en la fecha determinada y se evalúa con avances considerando que la acción de mejora y actividad se refiere a Revisar de forma exhaustiva el inventario de activos de información de cada uno de los procesos de la entidad" y se determinó como meta 5 por lo que se mantiene en ejecución y se debe replantear la fecha de cumplimiento ajustándose a la revisión de la matriz de activos de información de todas las dependencias con

			el fin de fortalecer el levantamiento y actualización de activos especialmente porque se observaron situaciones similares en esta auditoria en los procesos evaluados.
O08AISI24	Brindar capacitación con ejercicios prácticos en cuanto a la actividad de actualización de inventario de activos de información a los delegados de seguridad de la información	Vencida	No se presentan evidencias de capacitación en actualización de inventario de activos de información
O9AISI24	1. Realizar revisión de los roles dentro del proceso y generar una matriz de control de acceso a la carpeta de MARTE por parte del equipo de Financiamiento.	Cumplida	Se observa un reporte como evidencia que enlista los funcionarios de la Subdirección y los accesos a Marte sin embargo no es posible identificar en el mismo si se concedieron a modo de consulta o edición
O9AISI24	2. Elaborar protocolo de control de acceso a las carpetas de la Subdirección de Financiamiento.	Vencida	No se evidencia cumplimiento de esta actividad por lo cual se debe replantear fecha de cumplimiento
O9AISI24	3. Realizar una revisión semestral del control de acceso de las carpetas de acuerdo con el protocolo establecido.	En Ejecución	No se evidencia cumplimiento de esta actividad por lo cual se debe replantear fecha de cumplimiento
H13AISI24	Designar al Oficial de Protección de Datos Personales	En Ejecución	No se evidencia ejecutada la acción de mejora y actividad referida a la resolución actualizada
O14AISI24	Actualizar la resolución de designación de oficial de datos personales	En Ejecución	Si bien la actividad se describe como Actualizar la resolución de designación de oficial de datos personales y no se determinó con base en lo descrito en el hallazgo "El reporte de información en el RNBD ante la SIC se está ejecutando con un usuario y contraseña de un usuario que ya no trabaja en la ART", frente al hallazgo se evidencio que se asignó un nuevo usuario a cargo de (Coordinador Git Financiera), por lo que se sugiere ajustar la actividad toda vez que como se describe no se cumple
O14AISI24	Designar al Oficial de Protección de Datos Personales	En Ejecución	Si bien la actividad se describe como Actualizar la resolución de designación de oficial de datos personales y no se determinó con base en lo descrito en el hallazgo "El reporte de información en el RNBD ante la SIC se está ejecutando con un usuario y contraseña de un usuario que ya no trabaja en la ART", frente al hallazgo se evidencio que se asignó un nuevo usuario a cargo de (Coordinador Git Financiera), por lo que se sugiere ajustar la actividad toda vez que como se describe no se cumple
H15AISI24	Designar al Oficial de Protección de Datos Personales	En Ejecución	Evidencias no coherentes a la acción de mejora y a la unidad de medida
H16AISI24	1.Actualizar la Política y el Manual de Políticas de Protección de Datos Personales	En Ejecución	El manual y la policita aun no están actualizadas sin embargo se tiene documento en borrador
H16AISI24	2. Designar al Oficial de Protección de Datos Personales	En Ejecución	Evidencias no coherentes a la acción de mejora y a la unidad de medida

Fuente: Archivo Excel al Plan de Mejoramiento Seguimiento dic – Papeles de trabajo equipo auditor



Fuente: Archivo Excel al Plan de Mejoramiento Seguimiento dic – elaboración propia

Recomendación: Revisar y reformular las acciones de acuerdo a lo mencionado en las observaciones del seguimiento, así como dar cumplimiento a las mismas.

8. OPORTUNIDADES DE MEJORAMIENTO

A continuación, se relacionan los HALLAZGOS identificados con la letra “H” y las OBSERVACIONES identificadas con la letra “O”

N°	TIPO	DESCRIPCIÓN
1	H	**Debilidades en activos de información y bases de datos Proceso de Fortalecimiento** Se observa que en la TRD del Proceso de Fortalecimiento en la serie documental 320.031 PROCESOS DE FORTALECIMIENTO DE CAPACIDADES contiene como tipología documental Actas y Registros de Asistencia identificados con Tipo de soporte: Papel-PDF/A. Al realizar la verificación del manejo documental se observan actas en el repositorio MARTE (digital en PDF), sin embargo, no se tienen los registros de asistencia digital de las mesas realizadas en territorio y se informa que dichos documentos se quedan en físico en las Regionales, aunque hacen parte de la TRD de la Subdirección y deberían conservarse y custodiarse en la misma. En el caso de la lista de asistencia revisada no es correspondiente con el formato aprobado en SIGART (FM-ART-12). En la matriz de activos de información, además, se reporta como repositorio un enlace de la vigencia 2024. Se presenta un registro de asistencia como ejemplo de una mesa comunitaria realizada en 2025 observando que no tiene el aviso de privacidad (está cortado) y contiene datos personales; al revisar el inventario de activos se observa que los listados de asistencia se clasificaron como *Información Pública*, en un nivel de criticidad y CID *medio*, como *datos públicos* y se trata de datos sensibles, con una finalidad de recolección de *asistencia* pero que se usan para bases de datos y que debe documentarse el aviso de privacidad según la columna AJ de la matriz de inventarios, lo cual no se está cumpliendo; adicionalmente se observa en la clasificación sin fundamento jurídico o legal de excepción para tratarlo como público y no como sensible / reservado. Frente a las bases de datos se informa que no se han puesto a consideración del Oficial de Protección de datos y por ende no se ha reportado a la SIC. Responsable: Proceso de Fortalecimiento – Subdirección de Fortalecimiento

2	**H**	**Debilidades en activos de información y bases de datos Proceso de Gestión de Proyectos** Respecto a los Activos de Información, la Subdirección de infraestructura no ha revisado, actualizado ni reportado los activos de información de la vigencia 2025 y por ende no se ha actualizado la matriz de riesgos de seguridad de la información. Dado que no se ha evaluado y actualizado el Inventario de Activos de información, no se tiene identificada la existencia de información sensible que necesite la firma de acuerdos de confidencialidad para ello y que se encuentren etiquetados con base en los lineamientos establecidos por el GIT de Servicios Administrativos de acuerdo con su clasificación. Se identificó un activo desactualizado referido a informes de seguimiento. La información relevante del ejercicio de las funciones de la dependencia se tiene a cargo de un funcionario en un disco extraíble a cargo de la custodia. La información no está alojada en los repositorios oficiales en cumplimiento de las políticas de Seguridad de la Información y el Disco Duro extraíble no fue reportado como activo de información con el fin de darle un nivel de seguridad. No obstante, lo anterior se han definido reglas de acceso y custodios de información, sin embargo, no se da con ello cumplimiento a los controles del anexo técnico de la norma. Frente a las bases de datos, no se observa conocimiento de los delegados y recopilación de la información, no se han puesto a consideración del Oficial de Protección de datos y por ende no se han reportado a la SIC. Se observa que se asignaron las responsabilidades relacionadas con el sistema para informar situaciones relacionadas con el mismo y para cumplir lo establecido en MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN y Protección de datos personales a dos funcionarios, no obstante, se evidencia que de acuerdo a sus funciones y/o carga laboral el conocimiento y manejo de la información asociada a temas de SI se encuentra en otro funcionario no asignado. No es evidente cómo desde la Subdirección se garantiza que el SGSI logre los resultados previstos o apoya las sensibilizaciones en Seguridad y privacidad de la Información para que contribuyan a la eficacia del sistema dado que de parte de los delegados no se observa claridad frente a temas asociados a las políticas indagadas. Responsable: Proceso de Gestión de Proyectos -Subdirección de Infraestructura
3	**H**	**Debilidades en activos de información y bases de datos Proceso de Gestión Administrativa** La información no está actualizada en la matriz de activos de información en cuanto a los links de ubicación. En algunos activos se refieren carpetas de 2023 en la actualización de la vigencia 2025. La información se conserva el GIT Administrativa en un repositorio Onedrive sin embargo para el caso de la muestra tomada en la prueba de auditoría, validando por ej. la serie documental correspondiente a Actas de Comité de Bienes, se menciona en la Matriz que el lugar de consulta es en MARTE y no se encuentran registros en la carpeta de Marte, no correspondiendo esto a lo señalado en la matriz de activos de información. Responsable: Proceso de Gestión Administrativa – GIT Servicios Administrativos

4	**O**	**Numeral 6. Planificación. Plan de implementación de inteligencia de amenazas** Respecto a la definición del plan de implementación de inteligencia de amenazas que debe tener como fin proteger la seguridad de la información y los datos y el seguimiento a su ejecución, se determinó como “NO CUMPLE”, dado que se presentó en su lugar un Plan de mantenimiento de Servicios Tecnológicos. Según lo revisado, se hacen seguimientos, se ha trabajado con el equipo del SOC y COLCER para evaluar tendencias y adaptar la infraestructura a partir de los análisis de vulnerabilidades que se generan además a través del contrato con Datasec; Sin embargo, el procedimiento de PD-TI-10 GESTIÓN DE VULNERABILIDADES TÉCNICAS, menciona la elaboración de Plan de tratamiento de vulnerabilidades técnicas y el documento presentado no cumple con lo mencionado tanto en el Manual como en el procedimiento y no identifica si se definieron los *controles, lineamientos y documentación necesaria para realizar una adecuada identificación de amenazas que permitan recopilar procesar, identificación y analizar ciber amenazas que puedan poner en riesgo la seguridad de la información de la Entidad.* Responsable: Proceso Tecnologías de la Información - OTI
5	**O**	**Numeral 6. Planificación. Procedimiento PD-TI-05.V5 Incidentes de seguridad de la Información** Se tiene procedimiento PD-TI-05.V5 Incidentes de seguridad de la Información de marzo del 2024, en el cual se menciona en condiciones generales la utilización del formato FM-TI-20 Formato de Gestión Incidentes de Seguridad, el cual no se encuentra en uso toda vez que los reportes se hacen a través de la mesa de ayuda y se genera un Excel. En los registros de las actividades del procedimiento, no se encuentra relacionado el formato mencionado, uso o aplicación; por otra parte, una vez revisado algunos de los casos reportados como incidentes en la vigencia 2025 (en su mayoría por disponibilidad de la información y varios por situaciones externas), para los mismos, no se ejecutan las actividades establecidas en el procedimiento. Responsable: Proceso Tecnologías de la Información - OTI
6	**O**	**Numeral 6. Planificación. Plan de continuidad del negocio** En la verificación sobre si la ART cuenta con un plan para mantener la seguridad de la información en un nivel adecuado durante interrupciones o se tiene un Plan de continuidad del negocio con los requisitos de continuidad de las TIC, se presenta un documento de 2024 sin embargo no es claro si debe actualizarse cada año y cómo se incluyen las actividades realizadas y presentadas en el Documento Plan de Pruebas 2025, considerando que el mismo, no hace parte de los documentos formales del proceso en SIGART; se tiene un informe de plan de pruebas de julio de 2025 pero no se observa el documento que contenga los requisitos del MinTic para la continuidad del negocio. Responsable: Proceso Tecnologías de la Información - OTI

7	**O**	**Numeral 6. Planificación. Gestión de incidentes y riesgos de ciberseguridad** Respecto a la articulación de gestión de incidentes y riesgos de ciberseguridad con la inteligencia de amenazas con el fin de prevenir incidentes de alto impacto para la Entidad, a través del SOC se reportan eventos de seguridad de la información asociados al tema de ciberseguridad, a medida que se reciben se van gestionando; se tiene informe de pruebas de julio de 2025 y se tiene boletín de seguridad de URL maliciosas remitido por FORTINET, sin embargo, no se tiene articulado a nivel de procedimiento y, si bien se ejecutan actividades y se tiene un control, no se tienen documentadas las actividades; Se tiene en un archivo Excel el cual debería hacer parte del procedimiento y se realizan reuniones de seguimiento sobre los casos incluidos en MDS pero no se incluyen todos y no se reportan para efectos del indicador de incidentes, dado que son eventos que se gestionan por el procedimiento de gestión de vulnerabilidades. Responsable: Proceso Tecnologías de la Información - OTI
8	**O**	**Numeral 6. Planificación. Transferencia o intercambio de información** Para la transferencia o intercambio de información , se verificó si se firman acuerdos de confidencialidad, no divulgación o transferencia. Se tiene Documento técnico de entendimiento con las entidades CGR y MinVivienda, en ambos se observa periodicidad y tipo de información a transferir con clasificación; se observan acuerdos de confidencialidad con CGR (actualizado en sep/2024) y con MinVivienda un convenio (documento técnico) firmado en 2023, sin embargo se observó que no se tiene acuerdo de confidencialidad con MINVIVIENDA de acuerdo a lo establecido en el Manual de Políticas de SI numerales 8, 35 y 42. Responsable: Proceso Tecnologías de la Información - OTI
9	**O**	**Numeral 7.3. Toma de Conciencia** Si bien se han tomado acciones para adquirir la competencia necesaria o conocimiento de funcionarios a través de las jornadas de capacitación y a los contratistas en el SGSI incluso incluyendo en las minutas obligaciones generales o especificas relacionadas con la seguridad de la información y se exige la firma de acuerdos de confidencialidad los cuales reposan en los expedientes, no se ha evaluado la efectividad de dichas acciones para la toma de conciencia toda vez que no existe la obligatoriedad de presentar un soporte de participación en actividades y, aunque se remiten mensualmente los listados de parte del GIT Contratos de los contratistas que ingresan, no se identifica si el 100% adquirieron el conocimiento. Se evidenciaron debilidades de conocimientos generales del SGSI en los resultados de la encuesta de evaluación aplicada a los funcionarios y contratistas de los procesos evaluados que presentaron bajo nivel de conocimiento en los temas indagados referidos en el presente informe como Observaciones puntuales en los procesos evaluados (Observaciones 8, 9,10 y 11 consolidadas en esta observación para que se tomen las acciones tanto para funcionarios como para contratistas). Responsables: Procesos Gestión de TH, Contratación, Gestión de Proyectos, Administrativa, Tecnologías de la Información, Fortalecimiento de Capacitades.

10	**O**	**Numeral 7.4. Comunicación** Dentro de la revisión de registros de auditoría, se encontró que la política de S.I se encuentra disponible para las partes interesadas y se comunicó dentro de la entidad, sin embargo, al revisar el enlace en la página web donde se comunica la política, se observó que no se encuentra actualizada la publicación de políticas en el link de transparencia. Se sugiere actualizar la información y el nombre el menú/link https://www.renovacionterritorio.gov.co/#/es/acerca-de-la-entidad/Proteccion-de-datos-personales Adicionalmente, la política del SGSI actualizada, fue aprobada en Comité de Gestión y Desempeño y el documento que se encuentra publicado en el repositorio SIGART no tiene la firma establecida del Director General. Responsable: Proceso Tecnologías de la Información - OTI
11	**O**	**Debilidades en manejo de bases de datos Proceso de Gestión de Talento Humano** Se observan debilidades de conocimiento en el reporte de bases de datos de la dependencia al Oficial de Protección de Datos y en general en todo lo relacionado a tratamiento de datos personales y en cuanto a la actualización de activos de información, considerando que, en la actualización de Activos de información de TH hace falta la inclusión de correos de COPASST, Comité de Convivencia Laboral y de Comisión de personal de acuerdo con la TRD y, que algunos activos clasificados como Información Pública Clasificada con datos semiprivados sobre los mismos se registra que no aplica para la columna de autorización de tratamiento de datos; para el caso del activo "Historias Laborales" que contiene datos sensibles, no se requiere firma de acuerdos de confidencialidad específicos para el manejo de este activo y no está determinado el responsable o custodio del mismo (se refiere GIT TH en la mayoría de los activos). Igualmente, sobre la información recopilada de los funcionarios, se elaboran bases de datos con información de los mismos y en la matriz de activos se determinó que no aplica la autorización de tratamiento de datos personales por lo cual no se solicita. Si bien se ha tratado el tema y se adelantó una reunión entre la OTI y el GIT de TH para analizar el manejo de bases de datos a cargo e identificación de riesgos, en la matriz de riesgos no se tienen identificados riesgos / controles asociados a los activos de información calificados con nivel Alto. Responsable: Proceso Gestión de Talento Humano – GIT TH

12	**O**	**Debilidades en activos de información del Proceso de Gestión de Talento Humano** Se encuentran en el repositorio MARTE carpetas de los funcionarios que han finalizado su relación laboral en TH. De acuerdo a los lineamientos de la OTI y de Gestión documental no deberían encontrarse alojadas allí carpetas de back up. Se observan formatos de acuerdos de confidencialidad firmados por funcionarios sin firma de jefe inmediato, conservados en historias laborales de funcionarios que, aunque no hacen parte de la TRD de GTH se resguardan en las Historias Laborales. Para la transferencia o intercambio de información, no se firman acuerdos de confidencialidad, para controlar la eliminación, divulgación o transferencia para el caso de reportes o atención de solicitudes de información de la Registraduría Nacional, siendo pertinente incluso implementar el formato FM-TI-02.V4 Acuerdo Intercambio de Información. Responsable: Proceso Gestión de Talento Humano – GIT TH
13	**O**	**Debilidades en el numeral 7.5.3 Control de la información documentada del Proceso de Gestión Administrativa** Se tiene un circuito cerrado de tv para proteger las áreas sensibles, entre las que se incluyen las que almacenen información, sin embargo, se detectaron 2 cosas por mejorar, la primera es que el área donde se encuentran los expedientes de los contratos no tiene una cámara exclusiva a ésta área (ésta área es quien debe solicitarla) y la segunda es que la hora que refleja el circuito de tv estaba al momento de la inspección 4 minutos adelantada, se debe determinar la responsabilidad de esta verificación y por consiguiente sincronización periódica. Adicionalmente, durante la inspección realizada, se encuentra el computador de procesamiento de registros biométrico sin bloqueo de sesión con lo cual se puede vulnerar la seguridad de la información y se incumplen las políticas de SI así como los controles establecidos y/o generar materialización de riesgos. Responsable: Proceso Gestión Administrativa – GIT Servicios Administrativos
14	**O**	**Programa de Protección de datos personales** Se observó que no se ha presentado informe anual sobre el Programa de gestión protección de datos personales en el marco de Comité institucional de gestión y desempeño y se encuentra pendiente la actualización de la política de tratamiento de datos personales y el Manual de protección de datos y con ello, la estructura documental del Programa integral de gestión de datos personales. Responsable: OTI – Secretaría General
15	**O**	**Numeral 8. Operación. Seguimiento a Proveedores** En cuanto a si se monitorea, revisa, evalúa y gestionan periódicamente los cambios en las prácticas de seguridad de la información del proveedor y la prestación de servicios, se encontró que no se han realizado auditorías y/o revisiones de cumplimiento de requisitos y políticas de seguridad a los proveedores críticos de la Entidad; Se diseño formato Código: FM-TI-16 de Revisión de Políticas Proveedores para el seguimiento a proveedores, sin embargo en 2025 no se evidencia aplicación. Responsable: Proceso Tecnologías de la Información OTI

16	**O**	**Numeral 10. Ejecución Plan de Mejoramiento** Se observó en la revisión de ejecución del Plan de Mejoramiento documentado por la OTI sobre la auditoria interna vigencia 2024, que existen debilidades en los análisis de causas realizados de algunas de las acciones no ejecutadas; No se revisó a modo de autocontrol, la eficacia y efectividad de las acciones correctivas tomadas con el fin de identificar previo a la ejecución de la presente auditoría, las actividades vencidas o pendientes de ejecución, así como las evidencias que soportan las acciones ejecutadas sobre lo cual se observó que en algunos casos no corresponden a lo determinado en el plan. Producto de la auditoría interna vigencia 2024 la cual arrojo 16 oportunidades de mejora (H/O), se establecieron 51 actividades en el Plan de Mejoramiento todas para ejecutar dentro de la vigencia 2025. Se evidencia un nivel bajo de ejecución con un 47% de cumplimiento, actividades vencidas, actividades sin soporte real de ejecución o soportes no ajustados a lo determinado en el Plan. Al respecto, es evidente la ausencia de seguimientos preventivos que hubieran permitido la toma de acciones de manera oportuna Responsable: Proceso Tecnologías de la Información OTI

9. RECOMENDACIONES

1. Es importante que se apliquen los lineamientos frente a la protección de datos y la gestión documental con el fin de que las dependencias responsables identifiquen la adecuada clasificación y evaluación tanto en la matriz de activos de información, como en la matriz de riesgos en la cual se deben describir los controles pertinentes.
2. Es importante que se apliquen los lineamientos frente a la adecuada clasificación y evaluación tanto en la matriz de activos de información, como en la matriz de riesgos en la cual se deben describir los controles pertinentes (para el caso de los biométricos y los demás procesos con observaciones similares).
3. Se sugiere documentar un plan de implementación de amenazas a partir de los seguimientos y resultados de análisis realizados con los contratistas SOC y DATASEC que cumpla con la finalidad y objetivos de acuerdo al procedimiento, manual y la norma.
4. Revisar y ajustar el procedimiento PD-TI-05.V5 Incidentes de seguridad de la Información y adaptar o especificar en qué casos aplica y si se requiere determinar un nivel de impacto o evaluación de los incidentes incluirlo en las políticas del procedimiento. El conocimiento obtenido de los incidentes de seguridad de la información debe utilizarse para fortalecer y mejorar los controles de seguridad de la información, lo cual debe estar debidamente documentado.
5. Revisar y adaptar los documentos asociados al Plan de continuidad de manera que permita observarse el cumplimiento de requisitos normativos.
6. considerando que no es clara la articulación de los procedimientos de gestión de incidentes y gestión de vulnerabilidades, se sugiere que se definan las situaciones analizadas y categorizadas de vulnerabilidades y amenazas que harán parte de los reportes de indicadores y para evaluar y prevenir incidentes de alto impacto.
7. Suscribir acuerdo de confidencialidad con MinVivienda con el fin de dar cumplimiento a los lineamientos establecidos en el Manual de Políticas de SI V5 numeral 8 Transferencia o intercambio de información, numeral 35 Seguridad de las Comunicaciones y numeral 42. Política de Control de Accesos; Revisar si en las demás áreas de acuerdo a lo revisado en la presente auditoría, existen acuerdos o intercambios de información no formalizados o que requieran la actualización de acuerdos de confidencialidad.

8. Con el fin de brindar la competencia necesaria de los contratistas, así como la apropiación de conceptos y toma de conciencia en ejercicio de las actividades relacionadas con la seguridad de la información, es importante asegurar que el 100% de los mismos reciben la capacitación, inducción o sensibilización, por lo que se considera necesario establecer en los procedimientos que al inicio de la ejecución contractual o cómo mínimo con la entrega del primer informe, cada contratista y supervisor evidencie la sensibilización sobre el SGSI. Adicionalmente, teniendo en cuenta que desde los GIT de Talento Humano y Contratación se disponen mensualmente de los listados de funcionarios y contratistas que ingresan a la entidad, se realicen las respectivas socializaciones al momento de su ingreso. Para el caso de los funcionarios de planta, es necesario asegurar que el 100% de los mismos participen de una jornada de inducción o reinducción y se tenga los registros en sus expedientes de HV.

Es indispensable generar un mayor conocimiento y sensibilización en el área sobre los temas relativos a la SI, teniendo en cuenta que se requiere para el fortalecimiento y efectividad del sistema y con ello se sugiere que mensualmente se realicen las capacitaciones de generalidades del SGSI a los funcionarios y contratistas que ingresan a la entidad de acuerdo a la información remitida por el GIT de TH y por el GIT de Contratación, y/o que se disponga de un módulo virtual y el acceso se requiera de manera obligatoria para todos los servidores públicos y expedir certificado para conservar en la HV o en el expediente contractual.

9. Se sugiere actualizar la información y el nombre el menú/link https://www.renovacionterritorio.gov.co/#/es/acerca-de-la-entidad/Proteccion-de-datos-personales en el cual reposan las políticas del SGSI y corregir lo observado acerca del documento de Política general del SGSI publicado en SIGART sin firma.

10. Se sugiere revisar si es pertinente incluir el formato de acuerdos de confidencialidad en la TRD del GIT TH o quien debería custodiarlos porque el formato es de la OTI; se deben actualizar los acuerdos firmados y conservados en los expedientes de Hojas de Vida de los Funcionarios que actualmente se encuentran con formatos en versiones anteriores dado que la versión actual es la numero 4, y no tienen firmas de jefes inmediatos.

11. Se sugiere implementar los correctivos necesarios para evitar que se repitan las situaciones expuestas sobre el circuito de tv dado que podrían afectar lo referido en los Controles *Los registros deben protegerse contra pérdida, destrucción, falsificación, acceso no autorizado y publicación no autorizada*

12. Avanzar con la inclusión en el Protocolo de Comunicaciones respecto a la comunicación externa, cómo se deben abordar los casos específicos de seguridad de la información que afecten a las partes interesadas o grupos de valor de la entidad, y la comunicación en caso de que se materialicen riesgos de seguridad de la información o incidentes. En la actualización que se está realizando a la matriz de riesgos y plan de manejo, es necesario revisar de fondo y de forma la matriz de inventarios de activos de información de acuerdo con las funciones de las áreas y registros de la TRD así como la aplicación de lineamientos de datos personales y bases de datos.

13. Verificar con la matriz de activos de información, la coherencia e implementación de la política de protección de datos en las dependencias de la ART sobre la clasificación adecuada de los activos, manejo de datos sensibles o privados, aplicación de Autorización de tratamiento de Datos personales y firma de acuerdos de confidencialidad especialmente para información sensible o acuerdos de intercambio de información, así como la generación de bases de datos no reportadas por las dependencias o no asesoradas por el Oficial de protección de datos personales. Adicionalmente, se sugiere fomentar el conocimiento acerca del Manual y Política de Protección de datos personales, roles y responsabilidades y bases de datos.

14. Generar las acciones necesarias para avanzar en la implementación de la Política de Privacidad y protección de datos personales y dar cumplimiento a lo establecido en la Normatividad, realizar capacitaciones y actividades de sensibilización con el fin de fortalecer el conocimiento y seguimiento a la implementación de la política en las dependencias e informar a la Alta Dirección de manera periódica los avances o resultados.

15. Dar aplicación del formato Código: FM-TI-16 de Revisión de Políticas Proveedores y realizar la evaluación a proveedores de la vigencia 2025

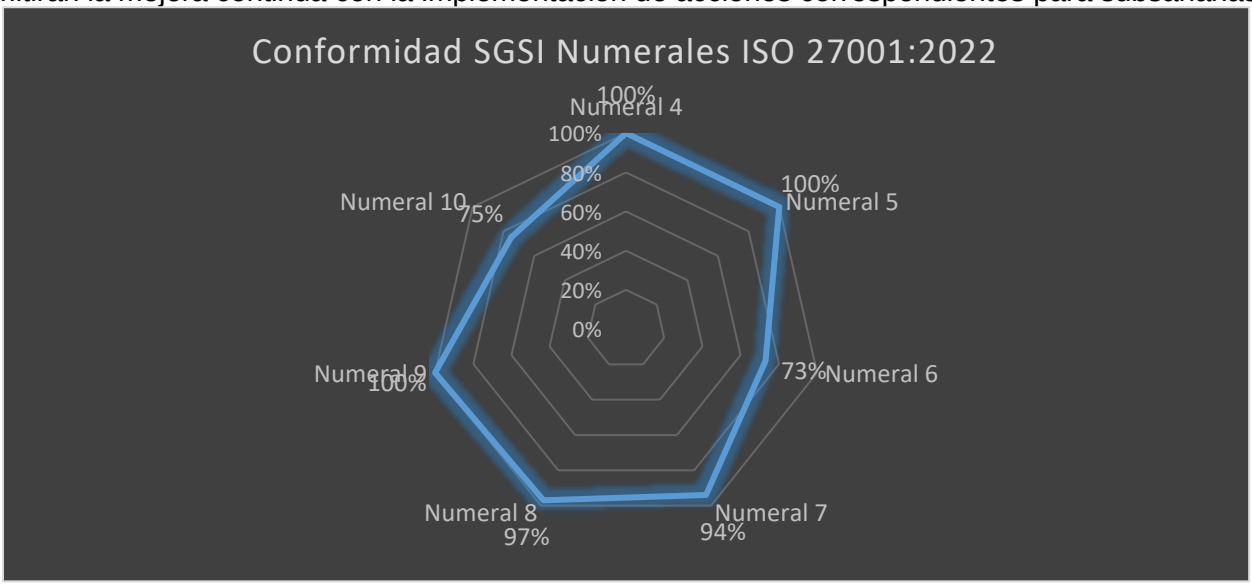
16. Se sugiere abordar una metodología de evaluación o verificación que garantice que las comunicaciones internas en temas de seguridad de la información están siendo efectivas y documentar la revisión periódica de las políticas, así como el cumplimiento de las mismas a partir de monitoreos que pueden realizarse con el apoyo del equipo de seguridad de la ART.

17. Se recomienda que el GIT Servicios administrativos en conjunto con la Oficina de Tecnología de la Información revise e indague detalladamente con las dependencias de la ART sobre la producción documental de tal manera que se asegure razonablemente que la tipificación es adecuada (Pública, clasificada y reservada) y si es consistente con las TRD y la ejecución real de actividades y funciones a cargo. Esto permite a su vez identificar la información que para el caso específico de las misionales, se produce en el accionar de las mismas y cual tiene como fuente externa pero que se requiere para dar cuenta de la gestión por ejemplo en el caso de requerimientos de entes de control y su manejo.
Se sugiere revisar el tema de accesos en las áreas misionales de acuerdo con la actualización de los activos de información y clasificación de los mismos en los repositorios de MARTE y OneDrive.

18. Revisar y reformular las acciones del Plan de mejoramiento producto de la auditoría de la vigencia 2024 de acuerdo a lo mencionado en las observaciones del seguimiento, así como dar cumplimiento a las mismas con el fin de verificar efectividad y cerrarlas en lo posible en el primer semestre del 2026.

10. CONCLUSIONES

De acuerdo con los objetivos de la auditoría, se evaluó la conformidad del Sistema de Seguridad de la Información sobre los requisitos de la norma NTC/ISO 27001:2022, encontrando un nivel de cumplimiento del 91% con algunas oportunidades de mejora descritas en el numeral 8 del presente informe, las cuales permitirán la mejora continua con la implementación de acciones correspondientes para subsanarlas.

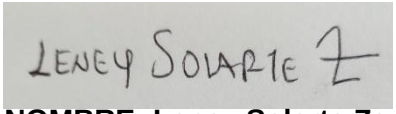
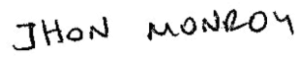
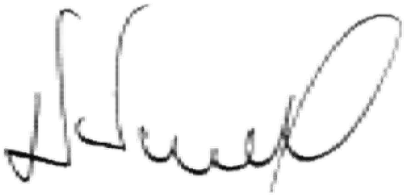


Fuente: elaboración propia

En cuanto a la evaluación de la gestión de la información y eficacia de los controles implementados en las dependencias y los procesos de la ART para garantizar que los activos de información estén adecuadamente protegidos de acuerdo a los criterios de seguridad de la información (disponibilidad, confidencialidad, integridad), se determinaron las observaciones y hallazgos referidas al tema y se vislumbra la necesidad de revisar los activos de información, bases de datos y protección de datos personales, se resalta que los procesos evaluados han establecido controles y roles para evitar la materialización de los riesgos relacionados a la información a su cargo.

En la verificación de la implementación de Políticas de Seguridad de la información en los procesos de la ART, según los temas a cargo de los procesos evaluados, se revisó el conocimiento y aplicación de las políticas del manual MI-TI-01.V3 siendo importante continuar con las sensibilizaciones y lograr el 100% de conocimiento, aplicación y toma de conciencia frente a las responsabilidades y apropiación del sistema por parte de cada uno de los involucrados en el mismo.

11. FIRMAS RESPONSABLES

Equipo Auditor:  **NOMBRE: Marisol Gutierrez Hernandez** **CARGO: Auditor Líder**  **NOMBRE: Leney Solarte Zambrano** **CARGO: Auditor**  **NOMBRE: Jhon Alexander Monroy Trigos** **CARGO: Experto Técnico**	**Vo. Bo**  **NOMBRE: MARLON SALOMON CONTRERAS TURBAY** **CARGO:** Coordinador GIT de Control Interno
FECHA DE INFORME:	**07-01-2026**