MEMORANDO

Bogotá D.C, 2025-10-28 16:51:15.196372

PARA: IVONNE ADRIANA MARTÍNEZ ZAPATA
Directora General (E)

DE: GILBERTO ANTONIO SUAREZ FAJARDO
Asesor, Control Interno

ASUNTO: Informe final auditoría MSPI 2025

En cumplimiento al Plan Anual de Auditoría 2025 V3, en lo referente al Modelo de Seguridad y Privacidad de la Información MSPI – 2025, se remite el informe final correspondiente. Teniendo en cuenta que durante el ejercicio de auditoría se identificaron tres (3) no conformidades y una (1) observación, se solicita implementar y suscribir un plan de mejoramiento, que, según el cronograma, debe ser remitido a la Oficina de Control Interno el 7 de noviembre de 2025.

Cordialmente,

Documento 20251010025223 firmado electrónicamente por:	
GILBERTO ANTONIO SUAREZ FAJARDO	Asesor Control Interno Fecha firma: 28-10-2025 16:51:15
Revisó:	JOHANN RICARDO PACHON RUIZ - Contratista - Control Interno
629bbc320ec179578aa2cc709dafae6e877bfeead5da7367f91259f496a9a25a Codigo de Verificación CV: eecf6	

Anexos: 1 folios

1. INFORMACIÓN GENERAL

FECHA DEL INFORME: 28/10/2025 - ***Final***
PROCESO/DEPENDENCIA AUDITADA: Gestión Tecnológica/Subdirección de Inteligencia y Gestión de Tecnologías de la Información
NOMBRE Y CARGO DEL RESPONSABLE DEL PROCESO / DEPENDENCIA AUDITADA: Ivonne Adriana Martínez Zapata/ Subdirectora de Inteligencia y Gestión de Tecnologías de la Información
AUDITOR LÍDER: Jesús Albeiro Rizo Gallardo
EQUIPO AUDITOR: N/A

2. OBJETIVOS Y ALCANCE DE LA EVALUACIÓN Y AUDITORÍA

Objetivo de la Auditoría:
Evaluar los avances en la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI), de acuerdo con los lineamientos impartidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) y la normatividad interna aplicable.

Alcance de la Auditoría:
La auditoría se orienta hacia el proceso Gestión Tecnológica y evaluará los controles relacionados con la seguridad y privacidad de la información, durante el 1 de agosto del 2024 al 31 de agosto del 2025.

Criterios de Auditoría:

- Normatividad interna aplicable.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas versión 7 del 2025, DAFP.
- Resolución nro. 02277 de junio del 2025. Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia. MinTIC.
- Anexo 1. Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información, versión 5 del 2025, MinTIC y guías relacionadas.
- Decreto 767 de 2022. Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Resolución nro. 746 de 2022 de MinTIC. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución número 500 de 2021.
- Norma ISO 27001:2022. Técnicas de seguridad: Sistemas de gestión de la seguridad de la información. Requisitos.
- Guía para la administración del riesgo y el diseño de control en entidades públicas, versión 6 del 2022, DAFP.
- Resolución nro. 500 de 2021 de MinTIC. Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
- Implementación de la Estrategia del MSPI de las Entidades Distritales - Alta Consejería Distrital de TIC de agosto 3 de 2017.

- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- ISO 9001:2015. Sistemas de gestión de la calidad – Requisitos.
- Anexo 4. Lineamientos para la Gestión de Riesgos de Seguridad Digital en Entidades Públicas, Ministerio de Tecnologías de la Información y las Comunicaciones.
- Anexo 5. Matriz Riesgos de Seguridad de la Información, DAFP.

3. RESULTADOS DE LA AUDITORÍA

Descripción de Hallazgo: marque con una X según corresponda: No Conformidad (NC); Observación (OBS)

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
1		X	Planificación – Numeral 2.2: se observó que el Manual de Políticas de Seguridad y Privacidad de la Información, versión 6 del 04/04/2025, no tiene el acta de aprobación por parte de la Alta Dirección; lineamiento del numeral 9.3. Revisión por la dirección del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; ocasionado por una posible falta de control de los documentos del Sistema de Gestión de Seguridad de la Información (SGSI); lo que resta autoridad institucional y obligatoriedad al manual, exponiendo a la entidad al debilitamiento de la gobernanza de seguridad de la información.
2		X	Planificación – Numeral 2.4: gestionar la designación de un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de Tecnología; de conformidad con el Anexo 1 de la Resolución 02277 de junio de 2025, numeral 7.2.3. Roles y responsabilidades.
3		X	Planificación - Numeral 2.7: no se evidenciaron los documentos de Metodología de gestión de riesgos; de Análisis y evaluación de riesgos y de Declaración de aplicabilidad; revisados y aprobados por la Alta Dirección; solicitados en el numeral 7.3.2. Valoración de los riesgos de seguridad de la información y 7.3.3. Plan de tratamiento de los riesgos de seguridad de la información del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; ocasionado posiblemente por fallas en el proceso de control documental; lo que expone a la entidad a inefectividad en el SGSI, a amenazas no mitigadas y a sanciones por incumplimiento de lineamientos obligatorios del MSPI del MinTIC, afectando la reputación institucional.
4	X		Planificación – Numeral 2.6: ausencia de avance en la gestión con la Subdirección de Gestión Corporativa para adquirir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), que cumpla con la normatividad archivística del Archivo General de la Nación y esta se integre a los lineamientos del MSPI.

Total, Hallazgos: No conformidades: **3** y Observaciones: **1**.

NOTAS:
Las observaciones son aspectos que eventualmente pueden llegar a ser una No Conformidad.
Las no conformidades son incumplimiento de requisitos.

4. DESARROLLO DE LA AUDITORÍA

La Política de Gobierno Digital es el instrumento del orden nacional que propende por la transformación digital pública, hace parte del Modelo Integrado de Planeación y Gestión Institucional (MIPG) y se debe integrar con las políticas de gestión y desempeño institucional del Instituto Distrital de Turismo (IDT), conforme a los lineamientos del Decreto nro. 338 de 2022 y las Resoluciones nro. 500 de 2021 y 2277 de 2025 emanadas del MinTIC.

De conformidad con el Plan Anual de Auditorías 2025 versión 3, publicado en la página web, el Instituto Distrital de Turismo (IDT) programó la ejecución de la Auditoría gestión tecnológica - MSPI (Modelo de Seguridad y Privacidad de la Información), cuyo desarrollo se centra en la recopilación y el análisis de las evidencias para determinar el cumplimiento de los criterios establecidos y el grado de avance en la implementación.

Por lo anterior, se realizaron las siguientes actividades:

- El 19/sept/2025 se realizó la reunión virtual de apertura a la auditoría del MSPI, donde se socializó el plan de auditoría a la Subdirección de Inteligencia y Gestión de Tecnologías de Información (SIGTI), responsable del proceso Gestión Tecnológica.

- El 23/sept/2025, la Asesoría de Control Interno (ACI) realizó, vía correo electrónico, la primera solicitud de información relacionada con los avances en la implementación del modelo.

- La SIGTI, mediante memorando nro. 20254000022053 del 25/sept/2025, allegó la información solicitada con las evidencias correspondientes.

- El 26/sept/2025, la Asesoría de Control Interno (ACI) realizó, vía correo electrónico, la segunda solicitud de información relacionada con la normatividad interna aplicada al modelo.

- La SIGTI, mediante memorando nro. 20254000022453 del 29/sept/2025, allegó la información solicitada con las evidencias correspondientes.

- El 30/sept/2025, la Asesoría de Control Interno (ACI) realizó visita al centro de datos y al centro de cableado, y solicitó información relacionada con el control de acceso al cuarto de datos y del diagrama de la infraestructura tecnológica de TI.

- La SIGTI, mediante memorando nro. 20254000022543 del 30/sept/2025, allegó la información solicitada con las evidencias correspondientes.

- El 20/oct/2025, se realizó la reunión virtual de cierre con la líder del proceso y se envió el informe preliminar a la SIGTI con radicado número 20251010024133.

- El 24/oct/2025, se recibieron las observaciones por parte de la SIGTI al informe preliminar, mediante radicado número 20254000024443 del 23/oct/2025.

Finalmente, se llevó a cabo la revisión de las evidencias en cuanto a su completitud y coherencia, acorde con lo solicitado por esta oficina, las cuales fueron dispuestas por el proceso en repositorios de almacenamiento de Google; adicionalmente, se hicieron consultas aclarativas con personal de la SIGTI y se inspeccionaron y validaron los documentos publicados en la página web y en la intranet. Los resultados obtenidos fueron plasmados en papeles de trabajo que facilitaron determinar el estado de avance del MSPI en la entidad, durante la vigencia 2025.

4.1 Resultado de la evaluación del MSPI 2025

Una vez realizado el seguimiento a cada una de las fases y validado el cumplimiento de los entregables (productos), se obtuvo un avance del **92,22%** en la implementación del MSPI en el IDT, durante la vigencia 2025 (hasta el alcance de la auditoría); quedando por ejecutar el 7,78%.

Se observa también que de las 19 actividades a ejecutar del MSPI, la SIGTI dio cumplimiento a 15, cumplió parcialmente 1 y no cumplió 3. Ver tabla.

Tabla Nro. 1. Avance implementación MSPI 2025

NRO.	FASE MSPI	MSPI	CUMPLE	META	% ESPERADO	% FINAL EJECUTADO	% PENDIENTE POR EJECUTAR	ACTIVIDADES MSPI	CUMPLIÓ	CUMPLIÓ PARCIAL	NO CUMPLIÓ
1	Diagnóstico	1.1	Si	20%	6,667	6,667	0,000	1	1	0	0
		1.2	Si		6,667	6,667	0,000	2	1	0	0
		1.3	Si		6,667	6,667	0,000	3	1	0	0
2	Planificación	2.1	Cumple	20%	2,222	2,222	0,000	4	1	0	0
		2.2	No		2,222	0,000	2,222	5	0	0	1
		2.3	Cumple		2,222	2,222	0,000	6	1	0	0
		2.4	No		2,222	0,000	2,222	7	0	0	1
		2.5	Si		2,222	2,222	0,000	8	1	0	0
		2.6	Parcial		2,222	1,111	1,111	9	0	1	0
		2.7	No		2,222	0,000	2,222	10	0	0	1
		2.8	Si		2,222	2,222	0,000	11	1	0	0
		2.9	Si		2,222	2,222	0,000	12	1	0	0
3	Implementación	3.1	Si	20%	5,000	5,000	0,000	13	1	0	0
		3.2	Si		5,000	5,000	0,000	14	1	0	0
		3.3	Si		5,000	5,000	0,000	15	1	0	0
		3.4	Si		5,000	5,000	0,000	16	1	0	0
4	Evaluación de desempeño	4.1	Si	20%	10,00	10,00	0,00	17	1	0	0
		4.2	Si		10,00	10,00	0,00	18	1	0	0
5	Mejora continua	5.1	Si	20%	20,00	20,00	0,00	19	1	0	0
RESULTADO MSPI				**100%**	**100**	**92,22**	**7,78**	**19**	**15**	**1**	**3**

Fuente: IDT – Elaboración ACI

En cuanto al avance del MSPI por cada una de las fases, se observó que la fase de diagnóstico, implementación, evaluación de desempeño y mejora continua, dieron cumplimiento al 100% de las actividades; mientras que la fase de planificación tiene pendiente por ejecutar el 7,78%, debido a la ausencia de la metodología de gestión de riesgos; del análisis y evaluación de riesgos y de la declaración de aplicabilidad; del acta de aprobación del manual de políticas de seguridad y privacidad de la información; de la designación de un responsable del MSPI no dependiente de la SIGTI, y por el poco avance en la gestión para adquirir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) integrada con el MSPI. Ver tabla.

Tabla Nro. 2. Avance implementación MSPI 2025 por fase

FASE MSPI	META %	% FINAL EJECUTADO	% PENDIENTE POR EJECUTAR
Diagnóstico	20	20,00	0,00
Planificación	20	12,22	7,78
Implementación	20	20,00	0,00
Evaluación de desempeñ	20	20,00	0,00
Mejora continua	20	20,00	0,00
TOTAL	**100**	**92,22**	**7,78**

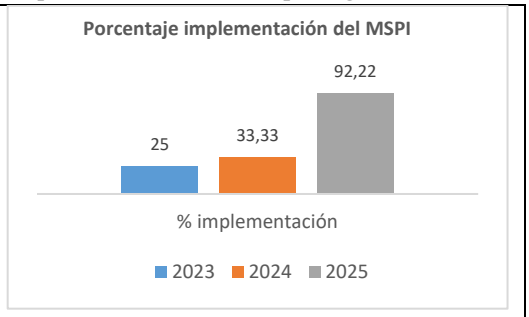
Fuente: IDT – Elaboración ACI

4.2 Comparativo de las implementaciones de MSPI

Con el fin de conocer el avance en la implementación del MSPI, durante las vigencias 2023, 2024 y 2025, se muestra en la tabla los porcentajes alcanzados; junto con la variación alcanzada entre un periodo y otro, destacándose que entre la vigencia 2024 y la 2025 hubo un aumento del 176,69%, pasando del 33,33% al 92,22%. Ver gráfica.

Gráfica Nro. 1. Avance en la implementación del MSPI por vigencia

Vigencia	% implementación	% variación
2023	25	-
2024	33,33	33,32
2025	92,22	176,69



Fuente: IDT – Elaboración ACI

5. HALLAZGOS DE AUDITORÍA

La SIGTI envió las observaciones al informe preliminar mediante radicado número 20254000024443 del 23/oct/2025, como se muestra a continuación.

5.1 Observaciones de la SIGTI al informe preliminar

- **No conformidad Nro. 1:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
1		X	Planificación – Numeral 2.2: se observó que el Manual de Políticas de Seguridad y Privacidad de la Información, versión 6 del 04/04/2025, no tiene el acta de aprobación por parte de la Alta Dirección; lineamiento del numeral 9.3. Revisión por la dirección del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; ocasionado por una posible falta de control de los documentos del Sistema de Gestión de Seguridad de la Información (SGSI); lo que resta autoridad institucional y obligatoriedad al manual, exponiendo a la entidad al debilitamiento de la gobernanza de seguridad de la información.

Respuesta SIGTI:

En atención a lo señalado, se precisa que mediante acta No. 6 del 28 de noviembre de 2024, se realiza la aprobación de la política de seguridad y privacidad de la información, dando así cumplimiento a los que estipula el numeral 7.2.2. Política de seguridad y privacidad de la información, del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información de 2025 (Documento que se cita en el criterio de la auditoría) y se comparte pantallazo.

Entradas recomendadas	Salidas
• Comprensión de la organización y de su contexto. • Necesidades y expectativas de los interesados. • Definición del alcance del MSPI. • Requerimientos normativos y buenas prácticas de seguridad y privacidad de la información.	• Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información

Asi mismo se precisa que el GT-M04 Manual de Políticas de Seguridad y Privacidad de la Información V6 tiene un flujo de aprobación de acuerdo con lo definido por el proceso del Sistema Integrado de Gestión, en el documento, SIG-I01 Instructivo para Elaborar Documentos (https://intranet.idt.gov.co/sites/default/files/2023-08/SIG-I01%20Instructivo%20elaboracion%20documentos%20SIG%20V6%2031072023.pdf) que se Requieran Incorporar al Sistema Integrado de Gestión, donde se estipula lo siguiente:

4.5. DEFINICIÓN DE ROLES PARA REVISAR Y APROBAR LOS DIFERENTES DOCUMENTOS

Aplicable a **políticas, manuales, procedimientos, programas y planes, instructivos y guías.**

Nivel del Proceso	Quien Aprueba	Quien Aprueba por parte de la Subdirección de Planeación
Todos los procesos	Líder del Proceso	Subdirector(a) de Planeación

Tabla No. 3. Contenido por tipo de documento

Contenido mínimo	Políticas	Manuales	Programas y planes	Procedimientos	Instructivos
Encabezado	x	x	x	x	x
Control de cambios				x	
Aprobación de líderes	x	x	x	x	x
Pie de pagina	x	x	x	x	x
Tabla de contenido		x	x		
Introducción		x	x		
Objetivo				x	x
Alcance				x	x
Definiciones	x	x	x	x	x
Consideraciones generales		x	x		x
Desarrollo del documento	x	x	x	x	x

Por lo sustentado anteriormente, se considera que el cumplimiento es parcial toda vez que se cumple con lo establecido en los lineamientos institucionales y se cuenta con la aprobación de la política de seguridad y privacidad de la información.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, se aclara que la no conformidad nro. 1 hace referencia específica y puntual a la inobservancia del acta de aprobación del Manual de Políticas de Seguridad y Privacidad de la Información, por parte de la Alta Dirección; tal como se estipula en el Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones, numeral 9.3. Revisión por la dirección, versión 5 del 21/04/2025; donde, adicionalmente a la política de seguridad y privacidad, el manual requiere también la revisión y aprobación por parte de la Alta Dirección.

9.3. Revisión por la dirección

Lineamiento:	La Política y el Manual de Seguridad y Privacidad deben ser revisados y aprobados por el Comité de Gestión y Desempeño o por decisión del nominador, considerando los cambios en las necesidades de las partes interesadas.
Propósito:	Revisar el MSPI de la entidad, por parte de la alta dirección (comité Institucional de Gestión y Desempeño), en los intervalos planificados, que permita determinar su conveniencia, adecuación y eficacia.

Entradas recomendadas	Salidas
• Los documentos de alto nivel del MSPI deberán ser aprobados, incluyendo los actos administrativos que se necesiten para constituirlos al interior de la entidad.	• Revisión a la implementación. • Acta y documento de Revisión por la Dirección. • Compromisos de la Revisión por la Dirección.

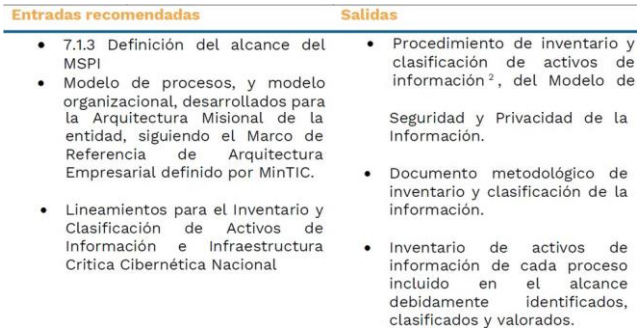
- **En consecuencia, se mantiene la No Conformidad Nro. 1.**

- **No Conformidad Nro. 2:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
2		X	Planificación - Numeral 2.5: no se evidenció la validación de la metodología para identificación, clasificación y valoración de activos de información por parte del comité de seguridad de la información o quien haga sus veces; estipulado en el numeral 7.3.1. Identificación de activos de información e infraestructura critica cibernética del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; ni el inventario de activos de IPv6, como lo indica la Guía de Gestión de Activos de Información; ocasionado posiblemente por debilidades en la supervisión de los documentos que hacen parte del SGSI y por la falta de actualización y adecuación del inventario de activos del IPv6; lo que puede ocasionar riesgos operacionales y de ciberseguridad altos, y de activos de información desprotegidos que no tienen controles de seguridad asignados o priorizados.

Respuesta SIGTI:

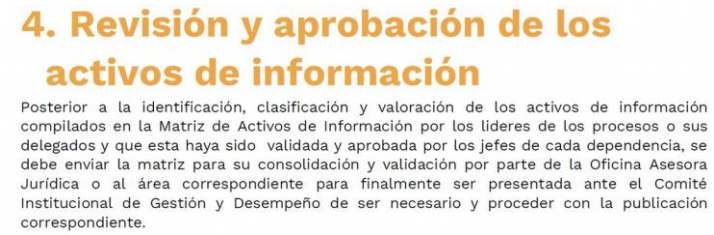
Referente a esta no conformidad solicitamos aclaración del numeral que establece la obligatoriedad de la aprobación metodológica para la identificación de inventarios de activos de información mediante comité, dado que una vez revisado el numeral 7.3.1 establece lo siguiente:



Entradas recomendadas	Salidas
• 7.1.3 Definición del alcance del MSPI • Modelo de procesos, y modelo organizacional, desarrollados para la Arquitectura Misional de la entidad, siguiendo el Marco de Referencia de Arquitectura Empresarial definido por MinTIC. • Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional	• Procedimiento de inventario y clasificación de activos de información [2], del Modelo de Seguridad y Privacidad de la Información. • Documento metodológico de inventario y clasificación de la información. • Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados.

No obstante, se precisa que la metodología fue definida mediante el documento aprobado y publicado en el sistema integrado de gestión - mapa de procesos de la intranet, GT-I06 Guía para la gestión de activos de información V2 (https://intranet.idt.gov.co/sites/default/files/2025-07/GT-I06%20Guia%20para%20la%20Gestion%20de%20Activos%20Informaci%C3%B3n%20%20V2%2015072025.pdf).

Así mismo, en atención a lo que indica el documento Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional de 2025, en su numeral 4. Se realiza la aprobación de los activos para la vigencia del alcance de la auditoría, mediante acta No. 6 del 28 de noviembre de 2024 en su numeral 10.



4. Revisión y aprobación de los activos de información

Posterior a la identificación, clasificación y valoración de los activos de información compilados en la Matriz de Activos de Información por los lideres de los procesos o sus delegados y que esta haya sido validada y aprobada por los jefes de cada dependencia, se debe enviar la matriz para su consolidación y validación por parte de la Oficina Asesora Jurídica o al área correspondiente para finalmente ser presentada ante el Comité Institucional de Gestión y Desempeño de ser necesario y proceder con la publicación correspondiente.

De otro lado en la normativa vigente del MSPI, no se cuenta con la guía mencionada donde se precise el requerimiento del inventario de activos de IPv6, por lo que se solicita la aclaración de este requisito y se precisa que la entidad gestiona sus activos de información teniendo en cuenta los diferentes tipos, donde se incluyen los componentes de red y hardware independiente de su tecnología.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, se verificó en la intranet la publicación de la guía para la gestión de activos de información, versión 2 del 15/07/2025 y el Acta nro. 06 del 28/11/2024 del Comité Institucional de Gestión y Desempeño, relacionado con la presentación y aprobación de los activos de información. Adicionalmente, la Resolución nro. 02277 de 03/jun/2025, "por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia", no exige la obligatoriedad de la aprobación metodológica para la identificación de inventarios de activos de información mediante comité; ni la elaboración del inventario de activos de IPv6, ya que estos hacen parte de la infraestructura de hardware y software que posee la entidad.

Tal como lo indica la Nota del documento MinTIC, "Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Critica Cibernética Nacional", versión 5 del 21/04/2025, numeral

4; el IDT debe estar atento a la actualización de los lineamientos generados, lo que será de obligatorio cumplimiento:

Nota: De conformidad con la implementación del presente lineamiento es importante tener en cuenta que, una vez se publique la metodología para la identificación de infraestructuras criticas cibernéticas establecida en el Decreto 1078 de 2015, adicionado por el Decreto 338 de 2022, se actualizarán los lineamientos generados en el presente documento para realizar la identificación de activos vinculados a las infraestructuras criticas cibernéticas, la cual será de obligatorio cumplimiento para entidades del sector público.

- **En consecuencia, se desvirtúa el hallazgo por dar cumplimiento a lo requerido por el MSPI.**

- **No conformidad Nro. 3:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
3		X	Planificación - Numeral 2.7: no se evidenciaron los documentos de Metodología de gestión de riesgos; de Análisis y evaluación de riesgos y de Declaración de aplicabilidad; revisados y aprobados por la Alta Dirección; solicitados en el numeral 7.3.2. Valoración de los riesgos de seguridad de la información y 7.3.3. Plan de tratamiento de los riesgos de seguridad de la información del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; ocasionado posiblemente por fallas en el proceso de control documental; lo que expone a la entidad a inefectividad en el SGSI, a amenazas no mitigadas y a sanciones por incumplimiento de lineamientos obligatorios del MSPI del MinTIC, afectando la reputación institucional.

Respuesta SIGTI:

En atención al hallazgo, se precisa que el IDT adopta la metodología definida desde el Departamento Administrativo de la Función Pública y por medio de la Subdirección de Planeación como segunda línea de defensa se lidera la gestión de los riesgos, lo que conlleva a que todos los procesos nos alineamos según las orientaciones de esta dependencia.

En comunicación con el área nos notifica que en la metodología de la función pública no menciona el requerimiento de aprobación por el comité institucional de gestión y desempeño, en consecuencia a que es un lineamiento que automáticamente se adopta.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, y teniendo en cuenta que La Política de Gobierno Digital (PGD), es el instrumento gubernamental del orden nacional que propende por la transformación digital pública, que busca fortalecer la relación Ciudadano - Estado, mejorando la prestación de servicios por parte de las entidades, y generando confianza en las instituciones que conforman la administración pública; a través del uso y aprovechamiento de las TIC. La PGD hace parte del Modelo Integrado de Planeación y Gestión (MIPG) y se integra con las políticas de gestión y desempeño institucional.

El MSPI imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e

implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital. Para que las entidades públicas incorporen la seguridad de la información en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y, en general, en todos los activos de información, con el fin de preservar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Por lo expuesto en la página web de MinTIC, donde se destaca que el MSPI está alineado con el Marco de Referencia de Arquitectura TI y la Guía de MIPG para la Administración del Riesgo y el Diseño Controles en entidades Públicas; se requiere en cumplimiento de lo emanado por dicho ministerio y en concordancia con la Política de Gobierno Digital, la elaboración de los documentos: Metodología de gestión de riesgos, Análisis y evaluación de riesgos; Declaración de aplicabilidad; documentos revisados y aprobados por la Alta Dirección; tal como lo exigen los numerales 7.3.2. y 7.3.3. del Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC, versión 5 del 21/04/2025, dirigida a las entidades del Estado.

Cabe anotar que la entidad en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión 4, hace referencia en el numeral 9 a la metodología, pero se requiere que esta se desarrolle de forma más extendida en un documento diferente. La adopción automática de una metodología externa no exime la responsabilidad de documentar su aplicación específica, ni de contar con trazabilidad institucional. Aunque la metodología provenga de Función Pública, debe adaptarse y formalizarse en el contexto del Sistema de Gestión de Seguridad de la Información (SGSI) del IDT.

- **Por lo anteriormente expuesto, se mantiene la no conformidad Nro. 3.**

- **No Conformidad Nro. 4:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
4		X	Planificación - Numeral 2.8: no se evidenció el Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, descrito en la guía nro. 14 del MinTIC, versión 1, aprobado por la Alta Dirección; y en el numeral 7.4.2. Competencia, toma de conciencia y comunicación del Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC; por una posible desconexión entre la planeación y la ejecución del SGSI, lo que eventualmente puede conllevar al personal de la entidad a operar con un conocimiento desactualizado o insuficiente de las políticas de seguridad y privacidad, aumentando significativamente la probabilidad de incidentes causados por errores humanos.

Respuesta SIGTI:

El Plan de Capacitación, que para la entidades públicas corresponde al Plan de Capacitación Institucional, fue aprobado mediante acta No 01 del 29 de enero de 2025 (https://intranet.idt.gov.co/sites/default/files/2025-03/Acta%20No.01%20Comite%20MIPG%2029012025.pdf) y se encuentra publicado en el link de transparencia de la sede electrónica de la entidad (https://www.idt.gov.co/plan-institucional-de-capacitacion), en el cual se establece el cronograma de actividades de capacitación correspondiente al MSPI.

Por lo anterior se solicita desestimar el hallazgo, toda vez que no se da un incumplimiento a un requisito.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, se verificó en la página web la publicación del Plan Institucional de Capacitación - PIC 2025, que incluye temáticas relacionadas con Gobierno y Seguridad Digital; y la aprobación de dicho plan mediante el Comité Institucional de Gestión y Desempeño, Acta Nro. 01 del 29 de enero de 2025.

- **En consecuencia, se desvirtúa el hallazgo por dar cumplimiento a lo requerido por el MSPI.**

- **Observación Nro. 5:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
5	X		Planificación – Numeral 2.1 y 2.3: inobservancia de las firmas correspondientes de la o las personas que elaboraron, revisaron y aprobaron las políticas, manuales, guías y procedimientos relacionados con la seguridad de la información; de conformidad con la norma ISO 9001:2015, numeral 7.5 Información documentada.

Respuesta SIGTI:

La entidad define mediante el documento SIG-I01 Instructivo para Elaborar Documentos que se Requieran Incorporar al Sistema Integrado de Gestión, las características y estructura de los diferentes documentos del Sistema Integrado de Gestión - SIG, en donde establece los mecanismos de aprobación, revisión y publicación, adicional el SIG establece los formatos respectivos para los diferentes tipos de documentos.

No obstante, se considera que la observación se encuentra fuera del alcance de la presente auditoría y por ende de los requisitos establecidos en el Modelo de Seguridad y Privacidad de la información, y como se indica en la observación hace parte de la Norma ISO 9001:2015, la cual se atiende mediante el Sistema Integrado de Gestión liderado por otro proceso.

Por lo anterior, se solicita desestimar la observación realizada.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, la entidad cuenta con el documento SIG-I01 Instructivo para Elaborar Documentos, el cual establece la estructura, características, y los mecanismos de revisión, aprobación y publicación de los documentos que hacen parte del Sistema Integrado de Gestión (SIG). Esto incluye los documentos relacionados con la seguridad de la información, cuyo control documental está liderado por otro proceso que regula la gestión documental.

- **En consecuencia, la observación se desvirtúa. Pasa de No cumple a Cumple**.

- **Observación Nro. 6:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
6	X		Planificación – Numeral 2.4: gestionar la designación de un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de Tecnología; de conformidad con el Anexo 1 de la Resolución 02277 de junio de 2025, numeral 7.2.3. Roles y responsabilidades.

Aunque no se recibió observación alguna por parte del proceso que argumentará el incumplimiento del hallazgo nro. 6, esta oficina cita a continuación los lineamientos del numeral 7.2.3. Roles y responsabilidades, del Anexo 1 de la Resolución 02277 de junio de 2025:

- Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional. Los líderes de proceso deberán gestionar los riesgos de seguridad y privacidad de la información.

- Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño y con voz al comité de control interno.

- Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital.

Durante el análisis, se evidenció que la entidad cuenta con un profesional especializado que entre sus funciones establece el desarrollo de actividades para la implementación del MSPI, con el apoyo de un contratista con obligaciones específicas para implementar el MSPI en su proceso de mejora continua y cumplimiento normativo, quienes no dependen de un área estratégica distinta a la de Tecnologías de Información (TI); situación que no da cumplimiento total al numeral 7.2.3.

- **En consecuencia, la observación se convierte en una No Conformidad.**

- **Observación nro. 7:**

No.	HALLAZGO		DESCRIPCIÓN DEL HALLAZGO
	OBS	NC	
7	X		Planificación – Numeral 2.6: ausencia de avance en la gestión con la Subdirección de Gestión Corporativa para adquirir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), que cumpla con la normatividad archivística del Archivo General de la Nación y esta se integre a los lineamientos del MSPI.

Respuesta SIGTI:

La observación se encuentra fuera del alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), dado que no corresponde a un requisito ni a una obligación propia de este modelo, sino que hace

parte de la normatividad archivística asociada a la implementación de un Sistema de Gestión Documental Electrónico de Archivo (SGDEA), tal como se menciona en la redacción de la observación.

Al respecto, es importante precisar que si bien la observación no hace parte del alcance de la auditoría ni de las responsabilidades de la Subdirección, la entidad se encuentra actualmente en proceso de implementación del sistema ORFEO, mediante el cual, y a través de un enfoque de mejora continua, se avanza en la adopción e implementación progresiva del SGDEA en el IDT y al cual el proceso de gestión tecnológica aprovisionó la infraestructura de TI requerida para soportar este sistema de información.

Por lo anterior, se solicita desestimar la observación realizada.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, el MSPI exige la gestión segura, trazable y controlada de la información, lo que incluye la gestión documental electrónica como componente esencial. La normatividad del Archivo General de la Nación (AGN), Ley 594 de 2000 (artículo 19. Soporte documental) y Decreto 1080 de 2015 (Artículo 2.8.2.5.8. Instrumentos archivísticos para la gestión documental), establece requisitos que deben integrarse al MSPI, especialmente en lo relativo a la protección, disponibilidad y autenticidad de la información.

Ahora, aunque la implementación del SGDEA sea liderada por otra área, la SIGTI tiene responsabilidad en la planificación y articulación de los sistemas de información que impactan la seguridad documental; tal como se está haciendo actualmente con la implementación del sistema ORFEO. Cabe resaltar que el MSPI no se limita a sistemas tecnológicos, sino que abarca la gestión integral de riesgos, controles y procesos asociados a la información. Así las cosas, la gestión documental electrónica constituye un componente transversal del MSPI, conforme a la normatividad del AGN.

- **En consecuencia, se mantiene la observación.**

- **Tabla Nro. 5. Seguimiento ACI - Fase Planificación - Numeral 2.1:**

Respuesta SIGTI:

*Por último, la observación referida en la **Tabla Nro. 5. Seguimiento ACI - Fase Planificación** Numeral 2.1 respecto a las políticas a incluir en los documentos del MSPI para la Entidad relacionados, se establece:*

Frente a la observación se precisa de la Política de Seguridad y privacidad de la información, como documento de alto nivel se derivan dos manuales donde se disponen lineamientos o políticas específicas para la gestión de gobierno de seguridad de la información y de otro lado lo relacionado con la operación y controles técnicos de los servicios de TI (GT-M03 Manual de Políticas para la Administración y uso de las Tecnologías de la Información y la Comunicación (TIC) V7 y GT-M04 Manual de Políticas de Seguridad y Privacidad de la Información). Lo que conlleva a una adecuada articulación y complemento entre el MSPI y el Modelo de Gestión de Gobierno de TI - MGGTI, atendiendo la implementación de las políticas de Gobierno y Seguridad Digital aplicables para el IDT.

En ese sentido, las políticas sugeridas en la observación fueron consideradas y desarrolladas dentro de estos dos documentos.

Por lo anterior, se solicita desestimar la observación realizada de CUMPLIMIENTO PARCIAL y pasar a estado CUMPLE.

Análisis Control Interno:

De acuerdo con la respuesta y consideraciones del proceso Gestión Tecnológica, vale la pena aclarar que lo indicado en el numeral 2.1 de la Tabla Nro. 5. Seguimiento ACI - Fase Planificación, hace parte de la recomendación que pretende complementar las políticas específicas existentes en la entidad; para lo cual, se sugirió verificar de una lista, aquellas que aún no tiene implementadas la entidad y que le podrían aplicar; por consiguiente, no hace parte de la calificación del porcentaje del numeral 2.1; razón por la cual se definió la observación nro. 5.

- **En consecuencia, la observación se mantiene.**

5.2 Evaluación del avance del MSPI

Para cada una de las fases se realizó el seguimiento basado en la respuesta a cada uno de los requerimientos de información, a las evidencias enviadas por la SIGTI y a las observaciones realizadas al informe preliminar; lo que permitió determinar los hallazgos del caso, registrados en las siguientes matrices por etapa, junto con el estado de avance de implementación del MSPI.

5.2.1 Evaluación del avance del MSPI - Fase de DIAGNÓSTICO

Aunque la SIGTI dio cumplimiento a los entregables de la fase de Diagnóstico, es importante implementar de manera sostenida el escaneo de vulnerabilidades, con el fin de anticipar y reducir riesgos que puedan comprometer la seguridad de la información. Este proceso debe estar respaldado por un plan técnico que establezca con claridad la frecuencia, los puntos de control, los procedimientos de ejecución y las medidas correctivas asociadas. Ver tabla.

Tabla Nro. 3. Seguimiento ACI - Fase Diagnóstico

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
DIAGNÓSTICO	1.1 Diligenciamiento de la herramienta.	Actividad hace parte del plan de mejoramiento y se diligencia a principio de año, la cual fue presentada en abril de 2025.	Se evidenció archivo Excel con el diligenciamiento de la herramienta, fecha de evaluación del 15-julio-2024. No se observa el diligenciamiento a principio del año 2025 y/o la presentación en abril.	**CUMPLE**
	1.2 Diligenciamiento de la herramienta e Identificación del nivel de madurez de la Entidad.	Por medio de la herramienta de autodiagnóstico se evidencia un nivel de madurez del 81%,	Se evidenció el acta de comité institucional de gestión y desempeño nro. 6 del 28 de noviembre de 2024, *numeral 11. Socialización avances implementación MSPI*, donde se indica que el porcentaje de avance de la matriz autodiagnóstico, generada por MINTIC, es del 67%, lo que no tiene correspondencia con lo reportado por el proceso Gestión Tecnológica (81%).	**CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
	1.3 Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Esta actividad hace parte del plan de mejoramiento. Se realiza el análisis de vulnerabilidades de los servicios externos por parte de Colsert y en la infraestructura OnPremise por medio de una herramienta de uso opensource. La información se encuentra encriptada por temas de seguridad.	Se evidenciaron 2 archivos pdf, así: 1. *PC_Informe Vulnerabilidades OnPremise_protected*, realizado por la Subdirección de Inteligencia y Gestión de Tecnologías de Información a la red de servidores de la entidad, con una herramienta de código libre. El reporte del scan de vulnerabilidades es del 18-agosto-2025. 2. *PC_WAS_SCAN_PORTALES_IDT_protected (1)*, enviado por CSIRT Gobierno, con el informe técnico de los escaneos web. El reporte del scan de vulnerabilidades es del 1-junio-2025. Aunque durante el primer semestre de 2025 se reportaron incidentes de seguridad como la indisponibilidad del servicio del canal principal de internet, indisponibilidad del portal Bogotá Aprende y correos maliciosos; estos fueron debidamente controlados, superados y documentados. En general, no se presentaron incidentes graves o muy graves, ni hubo materialización de riesgos. Se recomienda continuar con la ejecución permanente del scan de vulnerabilidades para prevenir eventuales fallas o incidentes de seguridad de la información, a través del diseño de un plan de escaneo de vulnerabilidades que permita programar la periodicidad, dónde, cuándo, cómo realizarlo y las acciones de mitigación o correctivas aplicadas.	**CUMPLE**

Fuente: IDT – Elaboración ACI

5.2.2 Evaluación del avance del MSPI - Fase de PLANIFICACIÓN

Dentro de los entregables de esta fase, algunos no se recibieron o están incompletos, como se resume a continuación:

- Aunque se observó en la intranet la publicación del Manual de Políticas de Seguridad y Privacidad de la Información, versión 6 del 04/04/2025, no se evidencia el acta de aprobación por parte de la alta dirección.

- Aunque se evidenció avances en temas de seguridad de la información como asignación de roles y responsabilidades de la política de gobierno digital y seguridad digital; aprobación de la política de seguridad y privacidad de la información; aprobación actualización del PETI; presentación y aprobación activos de información, y socialización de los avances en la implementación del MSPI; se debe designar un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de la SIGTI, en cumplimiento de la Resolución 2277 de 2025, Anexo 1 – MinTIC.

- No hubo avances en la gestión para adquirir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) conforme al Archivo General de la Nación y alineado con el MSPI.

- Aunque se evidenció la publicación del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se requiere elaborar de forma independiente el documento con la metodología de gestión de riesgos. Adicionalmente, no se evidenció el documento con el análisis y evaluación de riesgos ni el documento con la declaración de aplicabilidad, revisados y aprobados por la Alta Dirección.

Tabla Nro. 4. Seguimiento ACI - Fase Planificación

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	**Estado**
PLANIFICACIÓN	2.1 Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Esta actividad hace parte del plan de mejoramiento. El 28 de noviembre de 2024 fue publicada en el sistema integrado de gestión la GT-PO1 Política de Seguridad y Privacidad de la Información V1, la cual fue aprobada por el comité institucional de gestión y desempeño el día 26 de noviembre de 2024 y por la subdirectora de la SIGTI y la Subdirectora de Planeación.	Se evidenció el documento de la Política de seguridad y privacidad de la información, que contiene también algunas políticas específicas de seguridad, versión 1 del 28/11/2024; publicada en la página web y en la intranet de la entidad; aprobada por el Comité Institucional de Gestión y Desempeño, Acta nro. 06 del 28/11/2024. Se recomienda que el documento esté validado con las firmas correspondientes de la o las personas que lo elaboraron, revisaron y aprobaron; esto teniendo en cuenta que la firma; manuscrita, electrónica o digital, no es solo un requisito formal; es un elemento esencial para garantizar la validez, autenticidad y responsabilidad sobre los documentos institucionales. La norma ISO 9001:2015 no menciona explícitamente la "firma" de documentos institucionales; en el numeral 7.5 Información documentada, establece los requisitos para crear, actualizar y controlar la información documentada dentro del Sistema de Gestión de Calidad. Aunque no exige la firma como tal, sí contempla elementos que suelen implicarla en la práctica institucional. ***(Acorde con la subsanación de la SIGTI al informe preliminar, se pasa de Cumple parcial a CUMPLE).*** Por otra parte, si la entidad lo considera, las políticas específicas de seguridad podrían incluirse en un documento independiente de la política general de seguridad y privacidad de la información. Con el fin de complementar las políticas específicas, se recomienda verificar dentro de la siguiente lista aquellas que aún no tiene implementadas la entidad y que le apliquen. Se sugiere que incluyan el objetivo y las directrices a seguir: • Política de correo corporativo • Política para el uso de recursos tecnológicos • Política de control de acceso (usuario y contraseña) a sistemas de información • Política de copias de seguridad • Política de estaciones de trabajo • Política de red corporativa y wireless • Política de uso de Internet • Política de uso de sistemas de información • Política de seguridad física y del entorno del centro de datos • Política de acceso remoto • Política de servidor de archivos • Política de administración de base de datos • Política de pistas de auditoría • Política de transmisión y publicación de información • Política de teletrabajo y trabajo en casa • Política de derechos de autor y legalidad de software • Política de uso de impresoras y servicios de impresión • Política de seguridad de los recursos humanos • Política de gestión de página web • Política de gestión de comunicaciones y operaciones • Política de control de acceso a los recursos informáticos • Política de adquisición, desarrollo y mantenimiento de sistemas de información • Política de gestión de incidentes de seguridad de la información • Política de gestión de vulnerabilidades técnicas • Política de gestión de continuidad del negocio • Política para la gestión de activos de información • Política de cumplimiento de la normatividad vigente • Política para la gestión de dispositivos móviles • Política de seguridad en la nube	**CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	**Estado**
			• Política de uso de controles criptográficos • Política de gestión de contraseñas • Política de desarrollo seguro de software	
	2.2 Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Esta actividad hace parte del plan de mejoramiento. El documento es aprobado y publicado en el sistema integrado de gestión el 04 de abril de 2025, GT-M04 Manual de Políticas de Seguridad y Privacidad de la Información V6.	Aunque se observó en la intranet la publicación del Manual de Políticas de Seguridad y Privacidad de la Información, versión 6 del 04/04/2025, no se evidencia el acta de aprobación por parte de la alta dirección. Se recomienda que el documento esté validado con las firmas correspondientes de la o las personas que lo elaboraron, revisaron y aprobaron; esto teniendo en cuenta que la firma; manuscrita, electrónica o digital, no es solo un requisito formal; es un elemento esencial para garantizar la validez, autenticidad y responsabilidad sobre los documentos institucionales.	**NO CUMPLE**
	2.3 Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	En el proceso de mejora continua se han actualizado y definido los siguientes documentos, los cuales se encuentran aprobados y publicados en el sistema integrado de gestión. 1. Política de Seguridad y privacidad de la información (GT-P01): En este se define los principios, alcance, objetivos, roles y responsabilidades, políticas. 2. Manual de Políticas de Seguridad y Privacidad de la Información (GT-M04): En este se definen las políticas específicas organizacionales, de personas, controles físicos y tecnológicos. 3. Manual de Políticas para la Administración y uso de las Tecnologías de la Información y la Comunicación (TIC) V7 (GT-M03). 4. Guía para la gestión de activos de información (GT-I06). 5. Procedimiento Gestión de Cambios (GT-P17). 6. Procedimiento para Gestión de Incidentes de Seguridad de la Información (GT-P13) 7. GT-P07 Procedimiento para la Ejecución de Mantenimiento Preventivo y Correctivo de Equipos. 8. GT-P04 Procedimiento para Crear Backup de la Información V7 9. GT-P03 Procedimiento de Requerimiento de Soporte de Tecnología V5. 10. GT-P02 Procedimiento de Recuperación de Información V6. 11. GT-P01 Procedimiento Para la Administración de los Servidores de Tecnología de la Entidad V10. 12. GT-I06 Guía para la gestión de activos de información V2. 13. GT-F23 Formato de solicitud Gestión de Cambios. 14. GT-F14 Formato Inventario de activos de información. 15. GT-F22 Bitacora control de acceso a cuartos de datos	Se evidenció en la intranet la publicación de los documentos mencionados, como políticas, manuales, guías y procedimientos. Se recomienda que los documentos estén validados con las firmas correspondientes de la o las personas que lo elaboraron, revisaron y aprobaron; esto teniendo en cuenta que la firma; manuscrita, electrónica o digital, no es solo un requisito formal; es un elemento esencial para garantizar la validez, autenticidad y responsabilidad sobre los documentos institucionales. Se resalta que el documento CARACTERIZACIÓN DE PROCESOS, versión 4 del 17/10/2023, es el único que cumple con el registro de los nombres y firmas de las personas que lo elaboraron, revisaron y aprobaron. ***(Acorde con la subsanación de la SIGTI al informe preliminar, se pasa de Cumple parcial a CUMPLE).***	**CUMPLE**
	2.4 Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y	Esta actividad hace parte del plan de mejoramiento. La actividad fue realizada, en el marco del comité institucional de gestión y desempeño realizado el 28 de noviembre se incluyó como uno de los puntos de la agenda la designación de roles y responsabilidades para la SIGTI en la implementación de la política de Gobierno Digital y Seguridad Digital.	Se evidenció Comité Institucional de Gestión y Desempeño, Acta nro. 06 del 28/11/2024, que incluye temas de seguridad de la información aprobados, como: 7. Asignación de roles y responsabilidades de la política de gobierno digital y seguridad digital. 8. Aprobación de la política de seguridad y privacidad de la información. 9. Aprobación actualización del PETI.	**NO CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	**Estado**
	aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.		10. Presentación y aprobación activos de información. 11. Socialización de los avances en la implementación del MSPI. En cuanto al equipo de seguridad de la información en la entidad, se evidenció: • En el acta del comité institucional de gestión y desempeño nro. 6 del 28 de noviembre de 2024, numeral 7, la designación de la Subdirectora de Inteligencia y Gestión de Tecnologías de la Información (SIGTI) como responsable en el proceso de liderazgo en la implementación de las políticas de Seguridad Digital y Gobierno Digital establecidas por el Modelo Integrado de Planeación y Gestión. • Según memorando radicado nro. 20254000022453 del 29-09-2025, la SIGTI cuenta con un profesional especializado que entre sus funciones establece el desarrollo de actividades para la implementación del MSPI. • Apoyo de un contratista con obligaciones específicas para implementar el MSPI en su proceso de mejora continua y cumplimiento normativo. Por consiguiente, es claro que los integrantes del equipo de seguridad hacen parte del área de TI; por lo que se recomienda, de conformidad con el Anexo 1 de la Resolución 02277 de junio de 2025, *numeral 7.2.3. Roles y responsabilidades*, designar un responsable del MSPI con un equipo de apoyo dependiente de un área estratégica distinta a la de Tecnología; si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de gestión y desempeño y con voz al comité de control interno. Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital. ***(Acorde con la revisión de la OCI al informe preliminar, no se da cumplimiento total al requisito; y pasa de Cumple parcial a NO CUMPLE).***	
	2.5 Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento de caracterización de activos de información y datos personales Inventario de activos de IPv6.	Esta actividad hace parte del plan de mejoramiento. Mediante mesas de trabajo se realiza la actualización de los activos de información del IDT y son aprobados mediante el comité institucional el 28 de noviembre de 2024. En la vigencia 2025 se adelantaron las mesas de trabajo para la actualización de los activos de información.	Se evidenció Comité Institucional de Gestión y Desempeño, Acta nro. 06 del 28/11/2024, numeral 10, relacionado con la presentación y aprobación de los activos de información. Se evidenció documento de gestión de activos de información 2024 que incluye una metodología con 6 pasos a seguir: Identificación, Clasificación, Valoración, Legalidad, Aprobación y Actualización. No se evidenció la validación de la metodología por parte del comité de seguridad de la información o quien haga sus veces ***(Acorde con la subsanación de la SIGTI al informe preliminar, se da cumplimiento al requisito; y pasa de No cumple a CUMPLE).*** Se evidenció matrices por dependencias con la identificación, valoración y clasificación de los activos de información, para el año 2024 y 2025. Se evidenció en la intranet la publicación de la Guía para la gestión de activos de información, versión 2 del 15/07/2025. No se evidenció el inventario de activos de IPv6. ***(Acorde con la subsanación de la SIGTI al informe preliminar, se da cumplimiento al requisito; y pasa de No cumple a CUMPLE).***	**CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
	2.6 Documento de Integración del MSPI, con el sistema de gestión documental de la entidad.	Esta actividad hace parte del plan de mejoramiento. El Manual de políticas de seguridad y privacidad de la información, es actualizado y publicado en el sistema integrado de gestión, en el cual se establecen e integra los lineamientos para la protección de registros de acuerdo con lo definido en las tablas de retención, así como el borrado seguro y registros electrónicos, entre otros.	Se evidenció en la intranet la publicación del Manual de Políticas de Seguridad y Privacidad de la Información, versión 6 del 04/04/2025. Se recomienda que el documento esté validado con las firmas correspondientes de la o las personas que lo elaboraron, revisaron y aprobaron; esto teniendo en cuenta que la firma; manuscrita, electrónica o digital, no es solo un requisito formal; es un elemento esencial para garantizar la validez, autenticidad y responsabilidad sobre los documentos institucionales. No se reportaron avances en la recomendación del informe de auditoría 2024, sobre la gestión con la Subdirección de Gestión Corporativa para adquirir un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), que cumpla con la normatividad archivística del Archivo General de la Nación y esta se integre a los lineamientos del MSPI.	**CUMPLE PARCIAL**
	2.7 Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	El plan de tratamiento de riesgos es aprobado y publicado en el SIG el 29 de enero de 2025 y se realiza la actualización de los riesgos de seguridad en el primer cuatrimestre del año en conjunto con la subdirección de planeación. El aplicativo de riesgos ya cuenta con certificado SSL (https://riesgos.idt.gov.co/)	Se evidenció en la intranet la publicación del Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión 4 del 29/01/2025; aprobado en el Comité Institucional de Gestión y Desempeño, Acta nro. 01 del 29 de enero de 2025. Se recomienda que el documento esté validado con las firmas correspondientes de la o las personas que lo elaboraron, revisaron y aprobaron; esto teniendo en cuenta que la firma; manuscrita, electrónica o digital, no es solo un requisito formal; es un elemento esencial para garantizar la validez, autenticidad y responsabilidad sobre los documentos institucionales. Se evidenció documento (Acta) con la revisión y seguimiento primer cuatrimestre al mapa de riesgos de los procesos Gestión Tecnológica, fecha: 15 de abril de 2025; donde la SIGTI identifica 5 nuevos riesgos de seguridad digital (RT-00096, RT-00097, RT-00098, RT-00099 y RT-00100), basado en los criterios de disponibilidad, integridad y confidencialidad de la información estipulados en la ISO/IEC 27001:2022. Se evidenció en Google Drive la documentación de cada uno de los controles, observando que para el riesgo RT-00099, el documento *Bitácora control de accesos a centro de datos, versión 1 del 18/06/2024*, no tiene el código que permita su identificación en el sistema de gestión documental. No se evidencian los documentos: • Documento con la metodología de gestión de riesgos: aunque en el Plan de tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión 4, se hace referencia en el numeral 9 a la metodología, se requiere que esta se desarrolle de forma más extendida en un documento aparte. • Documento con el análisis y evaluación de riesgos. • Documento con la declaración de aplicabilidad. • Documentos revisados y aprobados por la Alta Dirección. En visita realizada por la Oficina de Control interno al Centro de Datos y al Centro de Cableado, el 30 de septiembre del 2025, se evidenció: • La aplicación del formato de control de acceso, con el registro a la entrada y salida. • Autenticación biométrica con huella. • De la solicitud de los accesos al centro de datos ocurridos en junio, julio y agosto del 2025, la SIGTI	**NO CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	**Estado**
			allegó (según memorando radicado nro. 20254000022543 del 30-09-2025), 2 documentos sin la identificación correspondiente al código GT-F22; adicionalmente, sólo se observan 2 visitas en junio y ninguna realizada en julio y agosto, ni por personal de la SIGTI para monitorear el funcionamiento y la operatividad de los dispositivos allí instalados. • No hay un correcto diligenciamiento de los formatos, ya que se observan días y fechas sin el año; y algunos sin fecha solo la hora, tanto en el ingreso como la salida. Adicionalmente, un registro no tiene firma de salida; situaciones que afectan la trazabilidad y responsabilidad en caso de un incidente. • Algunos registros no tienen el número de identificación del visitante. • La aplicación del control GT-F22 sólo aplica para el acceso al centro de datos, no para el centro de cableado. • Los extintores de incendio, tanto a la entrada del centro de datos como del centro de cableado, tienen fecha activa de funcionamiento, ya que vencen en enero de 2026. • En el centro de datos; que hospeda el aire acondicionado, UPS, el dominio, SICapital, la LAN, firewall, racks, switches y demarcadores para canal principal y canal secundario; se encontraron elementos como cajas de cartón, un balde, un descansa pies, monitores, torres de computador y switches para dar de baja; así como, residuos de cables, papeles, plástico y resaltadores en el piso, junto con exceso de polvo; lo que evidencia falta de organización, limpieza y orden. • En el centro de cableado se observó 2 estantes con cajas, papeles, teclado y mouse, un escáner, 2 sillas, torres de computador para dar de baja y cartuchos de impresora; residuos de basura como cables, papeles y cajas, así como exceso de polvo; lo que evidencia falta de organización, limpieza y orden. • Así las cosas, se recomienda que el centro de datos y el centro de cableado ofrezcan mejores condiciones de orden y aseo, que eventualmente puedan evitar la disponibilidad de equipos y/o servicios informáticos, generando un posible riesgo de seguridad. Por otra parte, se debe evaluar la pertinencia de que elementos como sillas, estantes, torres, monitores que estén para dar de baja y tóneres de impresoras, entre otros, se almacenen en el sitio destinado por el área administrativa para tal fin. Las actividades de limpieza deben ser realizadas por personal autorizado, bajo el acompañamiento, supervisión y control de la SIGTI.	
	2.8 Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Para la vigencia 2025 se incluyó dentro del PIC las socializaciones de seguridad de la información.	Se evidenció la publicación en la página web del Plan Institucional de Capacitación 2025, que incluye en los Lineamientos de la política de Talento Humano – MIPG, numerales 11 y 12, temáticas relacionadas con Gobierno y Seguridad Digital respectivamente. La SIGTI allegó la programación de inducción y reinducción – Charlas formativas para el 2025, para los meses de mayo, septiembre y diciembre. No se evidenció el Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, descrito en la guía nro. 14 del MinTIC, versión 1; que sugiere para su construcción 4 fases: Diseño, Desarrollo, Implementación y Mejoramiento. Su objetivo es establecer lineamientos para la construcción y mantenimiento del plan de capacitación, sensibilización y comunicación de la seguridad de la información. Este plan debe ser aprobado por la Alta Dirección. ***(Acorde con la subsanación de la SIGTI al informe***	**CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
			preliminar, se da cumplimiento al requisito; y pasa de No cumple a CUMPLE).	
	2.9 Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	La entidad cuenta con IPv6 y se realizó la migración de manera satisfactoria en el año 2022	Se evidenció documento con la Implementación del protocolo IPv6 de diciembre de 2022.	**CUMPLE**

Fuente: IDT – Elaboración ACI

5.2.3 Evaluación del avance del MSPI - Fase de IMPLEMENTACIÓN

Aunque la SIGTI dio cumplimiento a los entregables de la fase de Implementación, se recomienda incluir en la etiqueta del nombre, publicada en la página web, los riesgos de seguridad de la información; así: Matriz de Riesgos de Gestión, Corrupción y Seguridad de la información. Ver tabla.

Tabla Nro. 5. Seguimiento ACI - Fase Implementación

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
IMPLEMENTACIÓN	3.1 Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Se presentó el avance del MSPI al comité institucional de gestión y desempeño el 28 de noviembre. Se aprueba y publica el plan de Seguridad y Privacidad de la información el 29 de enero de 2025.	Se evidenció el Plan de Seguridad y Privacidad de la Información aprobado por la Alta Dirección.	**CUMPLE**
	3.2 Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	El seguimiento a los riegos del IDT se realiza de manera cuatrimestral, por medio de la plataforma https://riesgos.idt.gov.co/. Actualmente se realizó el primer reporte de los riesgos que se actualizaron en el primer cuatrimestre, correspondiente a los riesgos RT-00096, RT-00097, RT-00098, RT-00099, RT-00100 y RC00072.	Se evidenció el reporte de seguimiento de los controles asociados a los riesgos de seguridad digital: RT-00096, RT-00097, RT-00098, RT-00099 y RT-00100. En el aplicativo https://riesgos.idt.gov.co/, se evidenció el registro y control de los riesgos de seguridad de la información, bajo la responsabilidad del proceso Gestión Tecnológica. Se recomienda incluir en la etiqueta del nombre, publicada en la página web, los riesgos de seguridad de la información; así: **Matriz de Riesgos de Gestión, Corrupción y Seguridad de la información**, actualmente aparece como:  Lo anterior, en cumplimiento de la Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional).	**CUMPLE**
	3.3 Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Son actualizados los indicadores del MSPI, en donde se definen dos adicionales correspondiente a la implementación de controles y gestión de activos de información.	Se evidenció la hoja de vida, el seguimiento y análisis de los siguientes indicadores: 1. Soporte técnico que se brinda para el correcto funcionamiento de los servicios tecnológicos de la Entidad. 2. Número de activos de información reportados por los procesos, clasificados y valorados. 3. Número de charlas y/o socializaciones realizadas. 4. Número de controles implementados para el MSPI. 5. Soporte técnico que se brinda para el correcto funcionamiento de los módulos de SI CAPITAL.	**CUMPLE**
	3.4 Documento con las estrategias del plan de	La entidad cuenta con IPv6 y se realizó la migración de manera satisfactoria en el año	Se evidenció documento con la Implementación del protocolo IPv6	**CUMPLE**

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
	implementación de IPv6 en la entidad, aprobado por la Oficina de TI.	2022	de diciembre de 2022, que contiene las estrategias del plan de implementación de IPv6 en el IDT.	

Fuente: IDT – Elaboración ACI

5.2.4 Evaluación del avance del MSPI - Fase de EVALUACIÓN DE DESEMPEÑO

La SIGTI dio cumplimiento a los entregables relacionados con la socialización de los avances en la implementación del MSPI y el plan de trabajo con las actividades programadas y los entregables correspondientes, acorde con la implementación del modelo. Ver tabla.

Tabla Nro. 6. Seguimiento ACI - Fase Evaluación de desempeño

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
EVALUACIÓN DE DESEMPEÑO	4.1 Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección.	En noviembre de 2024 se expone al comité institucional de gestión y desempeño el avance del MSPI. La SIGTI cuenta con un plan de trabajo de seguimiento a la implementación del MSPI, al cual se le hace seguimiento de manera mensual.	Se evidencia Comité Institucional de Gestión y Desempeño, Acta nro. 06 del 28 de noviembre de 2024, que registra en el numeral 11 la socialización de los avances en la implementación MSPI, junto con la presentación de apoyo que detalla dicho avance. Adicionalmente, se evidenció el plan de trabajo con las actividades programadas y los entregables correspondientes, acorde con la implementación del modelo.	**CUMPLE**
	4.2 Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Esta actividad fue analizada con la Oficina de Control Interno y se dejo en principio en el plan de mejoramiento, sin embargo luego fue eliminada en razón a que corresponde a la auditoria interna realizada por dicha oficina. Se cuenta con el plan de auditoría de oficina de control interno para la vigencia 2025, en donde se encuentran la auditoria al MSPI	Se evidencia en la página web (https://www.idt.gov.co/plan-anual-de-auditorias), la publicación del Plan Anual de Auditorías PAA - 2025 versión 3, que registra con el número 41 la Auditoría gestión tecnológica - MSPI (Modelo de Seguridad y Privacidad de la Información). Dicha versión 3 del PAA - 2025 fue aprobada por el Comité Institucional de Coordinación de Control Interno, mediante Acta de Reunión nro. 3, del 29 de agosto de 2025, numeral 4. MODIFICACIÓN AL PLAN ANUAL DE AUDITORÍA INTERNA V2.	**CUMPLE**

Fuente: IDT – Elaboración ACI

5.2.5 Evaluación del avance del MSPI - Fase de MEJORA CONTINUA

En esta fase se constató la publicación de los planes de mejoramiento, junto con el seguimiento a las acciones definidas, todas cerradas a septiembre de 2025. Ver tabla.

Tabla Nro. 7. Seguimiento ACI - Fase Mejora continua

FASE	ENTREGABLE	REPORTE SIGTI 2025	SEGUIMIENTO ACI 2025	
			Observaciones	Estado
MEJORA CONTINUA	5.1 Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Se cuenta con el plan de mejoramiento definido de acuerdo con los resultados de la auditoría interna realizada por la oficina de control interno. Este plan constituye el seguimiento por parte de la SIGTI y de la Oficina de Control Interno.	Se evidencia en la página web la publicación de los planes de mejoramiento con el seguimiento a las acciones propuestas, todas cerradas a septiembre de 2025. https://www.idt.gov.co/planes-de-mejoramiento-vigentes-exigidos-por-entes-de-control-internos-o-externos	**CUMPLE**

Fuente: IDT – Elaboración ACI

5.3 Plan de mejoramiento

Con corte a septiembre de 2025, el proceso Gestión Tecnológica, bajo la responsabilidad de la Subdirección de Inteligencia y Gestión de Tecnologías de la Información, reporta la totalidad de las acciones cerradas; por consiguiente, no tiene planes de mejoramiento sujetos de seguimiento por parte de la Asesoría de Control Interno.

6. CONCLUSIONES DE AUDITORÍA

1. Evaluado el avance del Modelo de Seguridad y Privacidad de la Información en el Instituto Distrital de Turismo, se obtuvo como resultado el 92,22% en la implementación; quedando pendiente por ejecutar el 7,78% de la fase de planificación.

2. Como resultado del ejercicio de auditoría se obtuvieron cuatro (4) hallazgos, distribuidos en tres (3) No conformidades y una (1) Observación.

3. Los avances en la implementación del MSPI han sido progresivos, teniendo en cuenta que en el 2023 fue del 25%, en el 2024 del 33,33% y en el 2025 del 92,22%; lo que demuestra la tendencia a lograr la ejecución total del modelo.

4. El capítulo 5 del informe detalla en las matrices por cada fase del MSPI, el seguimiento realizado por la Asesoría de Control Interno que permitió determinar los hallazgos respectivos.

FORTALEZAS Y BUENAS PRÁCTICAS:

1. Se destaca por parte de la Subdirección de Inteligencia y Gestión de Tecnologías de la Información, la diligencia y oportunidad de las respuestas a los requerimientos de información realizados por la Asesoría de Control Interno, lo que permitió dar cumplimiento al cronograma del plan de auditoría.

2. Se destaca la gestión realizada por el equipo de la Subdirección de Inteligencia y Gestión de Tecnologías de la Información, que permitió alcanzar el 90% en la implementación del MSPI. Adicionalmente, la disposición del equipo del proceso para aclarar las inquietudes y dudas manifestadas en sesiones de socialización; así como durante la visita al centro de datos y centro de cableado.

RECOMENDACIONES:

1. Actualizar el MSPI con los lineamientos de la Resolución nro. 02277 de 03/jun/2025, “por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”; con el fin de fortalecer la estrategia de seguridad digital en la entidad.

2. Institucionalizar el escaneo permanente de vulnerabilidades como parte del sistema de gestión de seguridad de la información, mediante un plan que especifique la periodicidad, los responsables,

los entornos de aplicación, los protocolos de ejecución y las acciones correctivas o de mejora continua que se deriven del análisis realizado.

3. Programar sesiones de organización, limpieza y aseo en el centro de datos y centro de cableado, con el fin de evitar eventuales incidentes de seguridad de la información, ocasionados por elementos ajenos a estos espacios.

4. Dar estricta aplicación al control de acceso al centro de datos y centro de cableado, realizado con el formato GT-F22, ya que se evidenció días y fechas sin el año; algunos sin fecha solo la hora, tanto en el ingreso como la salida; un registro sin firma de salida y algunos registros no tienen el número de identificación del visitante; situaciones que eventualmente pueden afectar la trazabilidad y responsabilidad en caso de un incidente de seguridad.

5. Ampliar las políticas específicas de seguridad con el fin de cubrir más activos de información, con la inclusión del objetivo y los criterios de aplicación.

6. Gestionar la pertenencia del oficial de seguridad de la información a una dependencia diferente de la Subdirección de Inteligencia y Gestión de Tecnologías de la Información, como la Alta Dirección o la Oficina de Planeación.

7. Atender las sugerencias y observaciones indicadas en las matrices de seguimiento de cada una de las fases de implementación del MSPI, capítulo 5; relacionadas con la completitud y entrega de los documentos faltantes y la validación de las firmas de las personas que lo elaboraron, revisaron y aprobaron.

Auditor Líder	**Asesor Control Interno**
	
Nombre: Jesús Albeiro Rizo Gallardo	**Nombre:** Gilberto Antonio Suárez Fajardo