ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-51990
Fecha: 26/12/2025 11:23:09 AM
Destino: 100-DESPACHO

MEMORANDO

Para: CESAR ANDRES RESTREPO FLOREZ
DESPACHO SECRETARIO DE SEGURIDAD

De: OFICINA DE CONTROL INTERNO

Asunto: INFORME DE SEGUIMIENTO A LA IMPLEMENTACIÓN DE LA POLÍTICA DE GOBIERNO Y SEGURIDAD DIGITAL - 2025

Respetado Doctor Restrepo:

En el marco de las funciones establecidas en la Ley 87 de 1993, el Decreto 648 de 2017 y de conformidad con lo dispuesto en el Plan Anual de Auditoría de la presente vigencia, la Oficina de Control Interno se permite comunicar el resultado del ejercicio de seguimiento a la implementación de la Política de Gobierno y Seguridad Digital en la Secretaría Distrital de Seguridad, Convivencia y Justicia.

Como resultado del seguimiento efectuado, se identificó una (1) oportunidad de mejora lo cual queda a discrecionalidad del proceso de gestión de tecnologías de la información la formulación del plan de mejoramiento.

Cómo conclusión el ejercicio de seguimiento se indica que la Secretaría presenta un avance en la implementación de la política de gobierno y seguridad digital, consolidando un marco normativo y procedimental y alcanzando un incremento en el índice de gobierno digital. Fue evidenciada la adopción de documentos oficiales en el sistema integrado de gestión y la aplicación efectiva de controles administrativos, físicos, tecnológicos y de personal, lo que refleja un nivel de madurez favorable y sostenido en la gestión de seguridad y privacidad de la información.

No obstante lo mencionado, se identificaron situaciones principalmente con el diligenciamiento del instrumento del modelo de seguridad y privacidad de la información - MSPI, especialmente en la identificación de brechas, actividades faltantes y evidencias de soporte. Fortalecer este componente permitirá reflejar con mayor precisión el estado real de cumplimiento y facilitar la toma de decisiones, asegurando la mejora continua y la efectividad del modelo la cantidad.

Finalmente, es preciso informar que el documento será publicado en la sección de transparencia de la entidad, a través del siguiente enlace: https://scj.gov.co/transparencia/planeacion-presupuesto-ingresos/informes-control-interno

Cordialmente,

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

ALCALDÍA MAYOR DE BOGOTÁ
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA
AL RESPONDER CITAR EL NR.
Nro. Rad: 3-2025-51990
Fecha: 26/12/2025 11:23:09 AM
Destino: 100-DESPACHO

KAROL ANDREA PARRAGA HACHE
JEFE DE OFICINA CONTROL INTERNO

c.c.e.: IVAN HERSAYN PINILLA HERRERA-DIRECCION DE TECNOLOGIAS Y SISTEMAS DE LA INFORMACION

Anexos: -1

Elaboró: DIEGO ALEXANDER URAZAN FRANCO
Revisó: DIEGO ALEXANDER URAZAN FRANCO-OFICINA DE CONTROL INTERNO -
Aprobó: KAROL ANDREA PARRAGA HACHE

Av. Calle 26 # 57- 83
Torre 7 Tel: 3779595
Código Postal: 111321
www.scj.gov.co

Informe de seguimiento a La Implementación de la Política de Gobierno y Seguridad Digital.

2025

Oficina de Control Interno

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

Tabla de contenido

1. OBJETIVO 3
1.1 OBJETIVOS ESPECÍFICOS 3
2. ALCANCE 3
3. CRITERIOS DE AUDITORIA 3
4. METODOLOGIA 3
5. SEGUIMIENTO DE AUDITORIA 4
5.1 Estado actual de la entidad según reporte del MinTIC en la plataforma de Gobierno Digital: 4
5.1.1 Gobernanza: 5
5.1.2 Habilitadores 5
5.1.2.1 Arquitectura 5
5.1.2.2 Cultura y apropiación 6
5.1.2.3 Seguridad y Privacidad de la Información 7
5.1.2.4 Servicios ciudadanos digitales 7
5.1.3 Líneas de acción 7
5.1.3.1 Servicios y procesos inteligentes 7
5.1.3.2 Decisiones basadas en datos 7
5.1.3.3 Estado abierto 8
5.1.4 Iniciativas dinamizadoras 8
5.1.4.1 Proyectos de transformación digital 8
5.1.4.2 Estrategias de Ciudades y Territorios Inteligentes 8
5.2 Seguridad Digital: 9
5.3 Modelo de seguridad y privacidad de la información - MSPI 9
5.3.1 Diagnóstico: 10
5.3.2 Planificación: 40
5.3.3 Implementación: 43
5.3.4 Evaluación del desempeño: 45
5.3.5 Mejoramiento continuo: 46
5.3.6 Calificación frente a mejores prácticas en ciberseguridad (NIST) 47
6. CONCLUSIONES 50

1. OBJETIVO

Evaluar el grado de implementación y efectividad de las medidas establecidas en el Decreto 767 de 2022 y en la Política de Seguridad Digital, con el propósito de determinar el nivel de madurez y gestión institucional en materia de ciberseguridad.

1.1 OBJETIVOS ESPECÍFICOS

- Verificar el cumplimiento de los lineamientos establecidos en el Decreto 767 de 2022 y en la Política de Seguridad Digital, con el fin de identificar brechas y riesgos asociados a la gestión de ciberseguridad en la Entidad.

- Determinar el grado de madurez de la seguridad digital en el marco del Modelo de Seguridad y Privacidad de la Información – MSPI, analizando el avance de los dominios y controles aplicables y su contribución al fortalecimiento de la gestión institucional en ciberseguridad.

2. ALCANCE

El alcance del presente seguimiento comprende la evaluación de la gestión institucional en materia de seguridad digital y ciberseguridad correspondiente a la vigencia 2025. Lo anterior en cumplimiento a lo establecido en el Decreto 767 de 2022, la Política de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información – MSPI actualizado en la presente vigencia con el propósito de identificar avances, brechas y oportunidades de mejora en la protección de los activos de información y en la respuesta frente a amenazas cibernéticas.

3. CRITERIOS DE AUDITORIA

- ✓ Ley 1581 de 2012
- ✓ Decreto 767 de 2022 - MINTIC
- ✓ Resolución 2277 de 2025 – MINTIC

4. METODOLOGIA

Sobre el presente informe de seguimiento se aplicaron las siguientes técnicas de auditoría:

- ✓ Cotejo y contraste de información.
- ✓ Validación en Portal MIPG.
- ✓ Revisión de soportes y evidencias documentales.
- ✓ Entrevistas.

5. SEGUIMIENTO DE AUDITORIA

5.1 Estado actual de la entidad según reporte del MinTIC en la plataforma de Gobierno Digital:

Como parte del ejercicio de seguimiento al cumplimiento de la Política de Gobierno Digital y Seguridad Digital, se procede a validar el estado actual de la entidad con base en la información disponible en la página oficial del Ministerio de Tecnologías de la Información y las Comunicaciones. Esta información corresponde a los datos reportados por la entidad en los mecanismos definidos por el MinTIC y constituye la fuente oficial para la medición del avance en la implementación de la política.

El análisis de este estado actual permite contar con una referencia objetiva y estandarizada, que sirve como punto de partida para el seguimiento, la identificación de avances y la determinación de posibles desviaciones frente a los lineamientos establecidos en el Manual de Gobierno Digital.

De acuerdo con la funcionalidad "Puntaje y hoja de ruta para entidades del orden territorial", disponible en la página oficial de Gobierno Digital del MinTIC, se procedió a consultar la información correspondiente a la entidad.

Con base en el puntaje obtenido y en la hoja de ruta asociada, a continuación, se presentan los resultados que la entidad tiene cargados en la plataforma del MinTIC, los cuales constituyen la referencia oficial para el análisis del estado actual y el seguimiento al cumplimiento de los lineamientos establecidos.

En primera medida se reporta el índice de gobierno digital de la siguiente manera:

Imagen N° 1 Índice Gobierno Digital – Fuente: https://gobiernodigital.mintic.gov.co/portal/Mediciones/

De acuerdo con la información reportada en el tablero interactivo de Gobierno Digital del MinTIC, la Secretaría Distrital de Seguridad, Convivencia y Justicia alcanzó en la vigencia 2024 un Índice de Gobierno Digital de 87,4, evidenciando una mejora frente al resultado obtenido en 2023 (83,9), lo que representa

un incremento de 3,5 puntos.

Este avance se sustenta principalmente en el fortalecimiento de subíndices asociados a Innovación Pública Digital, Arquitectura Empresarial y Estrategias de Ciudades y Territorios Inteligentes, lo que refleja una evolución positiva en la adopción de prácticas de transformación digital, planeación tecnológica y desarrollo de soluciones innovadoras alineadas con la Política de Gobierno Digital.

No obstante, el análisis del tablero también permite identificar oportunidades de mejora en los componentes de Servicios y Procesos Inteligentes, que presentan una disminución frente a la vigencia anterior, así como en Servicios Ciudadanos Digitales, cuyo puntaje se mantiene en 0,0. Estos resultados evidencian la necesidad de priorizar acciones orientadas a la digitalización de trámites y servicios, con énfasis en la experiencia del ciudadano.

En conjunto, el puntaje de 87,4 ubica a la entidad en un nivel alto de implementación de la Política de Gobierno Digital, al tiempo que define retos claros para consolidar los avances alcanzados y fortalecer los componentes aún rezagados.

Ahora bien, para los elementos la política, la entidad presenta al siguiente avance:

5.1.1 Gobernanza:

Las instancias de la Entidad a través de las cuales se toman decisiones sobre la implementación de la Política de Gobierno Digital: Comité de Gestión y Desempeño Institucional, Dirección de Tecnologías y Sistemas de la Información, Oficina Asesora de Planeación, Mesa Técnica de Gobierno Digital, Mesa Técnica de relacionamiento con la ciudadanía. Se generó el espacio virtual de participación ciudadana, a través del Botón Participa, en la sección Consulta Ciudadana a través del cual se invita a participar en la Encuesta Ciudadana, una herramienta clave para conocer las opiniones, necesidades y propuestas sobre el PETI, permitiendo a los Grupos de valor e interés que participen en la toma de decisiones sobre la implementación de la Política de Gobierno Digital en la Entidad: Academia, Ciudadanía, Sector privado y Sociedad civil.

5.1.2 Habilitadores

5.1.2.1 Arquitectura

En lo que respecta a los lineamientos respecto al habilitador Arquitectura, se cuenta con el proceso denominado “Gestión de Tecnologías de la Información”, formalizado a través del Sistema Integrado de Gestión el cual tiene definidos los indicadores de gestión del proceso. Se cuenta con el procedimiento de Gestión de Proyectos de TI a través del cual se determina el alcance y se priorizan los proyectos, basado en la metodología para gestión de proyectos con componentes de TI. Adicionalmente, se cuenta con el catálogo de servicios tecnológicos, el proceso de adopción de IPv6 que fue realizado desde la vigencia 2021, y se utilizan los Acuerdos Marco de Precios (AMP) o Instrumentos de Agregación de demanda (IAD) disponibles en la Tienda Virtual del Estado Colombiano (TVEC).

Por otra parte, la Entidad formuló el proyecto PETI P07 denominado “Adopción e implementación del Marco de Referencia de Arquitectura Empresarial”, el cual está proyectada su ejecución para el periodo

2024-2028. Al respecto, durante la vigencia 2025 se tiene:

Se avanzó en la documentación del Modelo de Arquitectura Empresarial - MAE para el proceso Gestión de Tecnologías de la Información:

- Documentar el Proceso de AE.
- Documentar el Dominio de Arquitectura Institucional.
- Documentar el Dominio de Arquitectura de Información.
- Documentar el Dominio de Arquitectura de Sistemas de Información.
- Documentar el Dominio de Arquitectura de Tecnología.
- Documentar el Dominio de Arquitectura de Seguridad.
- Documentar el proceso de Uso y Apropiación de la Práctica de AE.

Se avanzó en la documentación del Modelo de Gestión y Gobierno de TI - MGGTI para el proceso Gestión de Tecnologías de la Información:

- Documentar el Dominio de Estrategia de TI.
- Documentar el Dominio de Gobierno de TI.
- Documentar el Dominio de Gestión de Información.
- Documentar el Dominio de Gestión de Sistemas de Información.
- Documentar el Dominio de Gestión de Servicios de TI.
- Documentar el Dominio de Gestión de Seguridad.
- Documentar el Dominio de Uso y Apropiación de TI.

Se inició la documentación del Modelo de Gestión de Proyectos de TI - MGPTI, para el proceso Gestión de Tecnologías de la Información:

- Documentar el Dominio Contexto Estratégico.
- Documentar el Dominio de Planeación.
- Documentar el Dominio de Ejecución y Control.
- Documentar el Dominio de Cierre.

5.1.2.2 Cultura y apropiación

La Entidad para 2025, dentro de la estrategia de uso y apropiación ha realizado charlas y sensibilizaciones dirigidas a servidores y contratistas en temáticas de la Política de Gobierno Digital, Innovación Pública Digital, Seguridad y Privacidad de la Información, Datos Abiertos y demás sistemas y servicios de

tecnologías dispuestos por la Dirección de Tecnologías y Sistemas de la Información.

5.1.2.3 Seguridad y Privacidad de la Información

La Secretaría ha formulado para la vigencia 2025 y se encuentran en ejecución el Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información MSPI, los cuales fueron aprobados por el Comité Institucional de Gestión y Desempeño.

5.1.2.4 Servicios ciudadanos digitales

La Entidad cuenta con el catálogo de servicios ciudadanos digitales el cual se encuentra resumido en la siguiente tabla, y disponibles a través del enlace:

https://scj.gov.co/es/transparencia/tramites-y-servicios/servicios

5.1.3 Líneas de acción

5.1.3.1 Servicios y procesos inteligentes

En lo que corresponde a servicios y procesos inteligentes, la Entidad cuenta con un (1) único trámite registrado en el SUIT, correspondiente a "Autorización para ingreso como visitante a la Cárcel Distrital de Varones y Anexo de Mujeres". Para dicho trámite, durante la vigencia 2025 la Dirección de Tecnologías y Sistemas de la Información realizó el desarrollo del sistema para agendamiento de visitas de Cárcel Distrital, dispuesto dentro de la sección de Servicios Ciudadanos Digitales https://scd.scj.gov.co/servicio_inscripcion/verifica a través del cual se apalanca la estrategia de racionalización de trámites de la Entidad.

5.1.3.2 Decisiones basadas en datos

A través de la Oficina de Análisis de Información y Estudios Estratégicos, mediante el proceso C-GI-01 gestión y análisis de la información y el procedimiento PD-GI5 generación de documentos de análisis, los cuales se tienen con el propósito de establecer los parámetros y actividades requeridas para la elaboración de documentos o investigaciones, a través del análisis de información cuantitativa y cualitativa, para de generar recomendaciones y/o posibles estrategias en temas de Seguridad, Convivencia y Acceso a la Justicia que sirvan como insumo para la toma de decisiones de las instancias correspondientes.

Como complemento a lo anterior, se tienen implementados tableros de control básicos usando las herramientas de Oracle Analytics Cloud, disponibles en el siguiente enlace https://scj.gov.co/es/oficina-oaiee/estadisticas-mapas y otros tableros desarrollados en Power BI, dispuestos únicamente a los usuarios internos que requieren el acceso a éstos. Adicionalmente, se implementó el Observatorio de Seguridad, Convivencia y Justicia de Bogotá (OSCJ) como una herramienta que recopila, analiza y difunde información pertinente y oportuna sobre seguridad, convivencia y acceso a la justicia en Bogotá, para la generación de conocimiento que contribuya a la toma de decisiones para el diseño de política pública, el cual está

dispuesto en el siguiente enlace: https://oaiee.scj.gov.co/ObservatorioSCJ.html

5.1.3.3 Estado abierto

Para la presente vigencia, se realizó la actualización del Plan de Apertura de Datos Abiertos. Para este caso la entidad reporta que tiene publicados en el portal de datos abiertos Bogotá 19 conjuntos a saber:

1) **Esquema de publicación**
2) **Índice de Información Reservada y Clasificada**
3) **Registro Activos de Información**
4) **Cuadrantes de Policía**
5) **Cárcel**
6) **Sistema de Responsabilidad Penal para Adolescentes**
7) **Unidad de Reacción Inmediata**
8) **Centro de Atención a Víctimas**
9) **Sala de Atención al Usuario**
10) **Casa de Justicia**
11) **Centro de Traslado por Protección**
12) **Comando de Acción Inmediata**
13) **Estación de Policía**
14) **Centro de Comando, Control, Comunicaciones y Cómputo de Bogotá**
15) **Comando Operativo de Seguridad Ciudadana**
16) **Delito de Alto Impacto**
17) **Incidente Reportado**
18) **Medida Correctiva**
19) **Incidentes Tramitados en el C4**

5.1.4 Iniciativas dinamizadoras

5.1.4.1 Proyectos de transformación digital

Con respecto a las iniciativas dinamizadoras de la Política de Gobierno Digital, la Entidad formuló y se encuentra en ejecución los trece (13) Proyectos de TI definidos en el PETI, los cuales fueron aprobados por el Comité de Gestión y Desempeño Institucional, a través de los cuales se habilitan y mejoran los trámites y servicios digitales a través de los cuales se le prestan los servicios a los ciudadanos, así como se habilitan y mejoran los procesos internos de la Entidad, permitiendo fortalecer la toma de decisiones basada en datos a partir del aumento en el uso y aprovechamiento de la información.

Trimestralmente se han reportado los avances en los proyectos PETI a todo el equipo directivo de la Entidad.

5.1.4.2 Estrategias de Ciudades y Territorios Inteligentes

La Entidad ha avanzado en el desarrollo de un documento que defina la Estrategia de Ciudades y Territorios Inteligentes, desde las competencias de la Secretaría Distrital de Seguridad, Convivencia y Justicia, y alineado con la Política Pública Bogotá Territorio Inteligente. Al respecto, a la fecha la Dirección de Tecnologías y Sistemas de la Información se encuentra consolidando la información para realizar el registro de las iniciativas de conectividad pública y social en el Distrito Capital, en el marco de la circular no. 003 de 2025 emitida por la Consejería Distrital de TICs. Al respecto, la iniciativa de conectividad pública y social

desde la SDSCJ se viene estructurando para ofrecer el servicio en la Oficina de Atención al Ciudadano del primer piso de nivel central, y en las 16 casas de justicia. Se tiene proyectado realizar el registro de las iniciativas en diciembre de 2025, para iniciar la implementación en la vigencia 2026.

5.2 Seguridad Digital:

En lo que corresponde a los avances en la Política de Seguridad Digital por parte de la Entidad, en el mes de enero de 2025 se realizó la actualización del Plan de Seguridad y Privacidad de la Información, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Modelo de Seguridad y Privacidad de la Información - MSPI, en lo que corresponde a la vigencia 2025. Dichos planes fueron socializados en la Mesa Técnica de Seguridad Digital, posteriormente aprobados por el Comité Institucional de Gestión y Desempeño y publicado en el Portal MIPG y en el sitio web de la Entidad el 30 de enero de 2025, en cumplimiento del Decreto 612 de 2018. Igualmente, el Modelo fue aprobado por el Comité Institucional de Gestión y Desempeño y publicado en el Portal web en el mes de julio de 2025. Respecto al Plan de seguridad y privacidad de la información, desde la DTSI se han realizado la ejecución de las actividades programadas en el Plan, mencionando ejecución de gestiones de cambios de la plataforma tecnológica y los sistemas de información, atención de casos través de la consola System Center Service Manager correspondientes a creación de usuarios VPN, activación usuario plataforma SIGA, acceso a sitios Web y autorización de instalación de software, entre otros. Se ha realizado la correspondiente gestión de incidentes y vulnerabilidades a la infraestructura TI catalogados como de riesgo bajo o medio, registrados en la plataforma System Center Service Manager sobre información por correo electrónico institucional tipo, SPAM y tipo PHISHING, intentos accesos fallidos, tráfico IP sospechoso, intento ataques inyección SSL, entre otros.

Respecto al Plan de Tratamiento de riesgos de seguridad de la información, desde la DTSI se han realizado la ejecución de las actividades programadas del Plan, actualización de activos de Información de los procesos de la Entidad, socialización de gestión de riesgos de seguridad de la información, seguimiento a controles de riesgos de seguridad de la información y entrega de los informes cuatrimestrales de riesgos de seguridad de la información.

5.3 Modelo de seguridad y privacidad de la información- MSPI

Para la presente vigencia, la Oficina de Control Interno adelantó y enfatizó el seguimiento a la implementación y fortalecimiento del Modelo de Seguridad y Privacidad de la Información – MSPI, en atención a las disposiciones vigentes emitidas por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC. Este ejercicio se desarrolló con base en los lineamientos actualizados establecidos en la Resolución 2277 de 2025, cuya entrada en vigencia se dio el 3 de junio de 2024, mediante la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se fortalecen los criterios asociados a la gestión de la seguridad digital y la protección de la información en las entidades públicas.

El seguimiento tuvo como propósito verificar el avance y la efectividad de las acciones implementadas por la entidad para dar cumplimiento a los requerimientos normativos y técnicos aplicables al MSPI. En este sentido, el análisis se orientó a determinar el nivel de madurez institucional del modelo, a partir de la revisión de la aplicación práctica de lo establecido en el Documento Maestro del Modelo de Seguridad y

Privacidad de la Información, versión 5, emitido en la presente vigencia, el cual se estructura en cinco fases para su implementación y mejora continua.

- Diagnóstico.
- Planificación.
- Operación / implementación.
- Evaluación del desempeño.
- Mejoramiento continuo.

El modelo de manera gráfica se expresa así:

Imagen N° 2 Modelo MSPI – Fuente: https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/portal/Estrategias/MSPI/.

Ahora bien, respecto a cada una de las fases se validó lo siguiente:

5.3.1 Diagnóstico:

El documento maestro indica para esta fase como lineamiento; "Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) el estado actual de la entidad respecto a la Seguridad y Privacidad de la Información." Ante esto, y con base en la información suministrada por la DTSI, el instrumento actualizado presenta los siguientes datos:

No.	Evaluación de Efectividad de controles			
	DOMINIO	Calificación Actual	Calificación Objetivo	Nivel de Madurez
A.5	CONTROLES ORGANIZACIONALES	85	100	OPTIMIZADO
A.6	CONTROLES DE PERSONAS	95	100	OPTIMIZADO
A.7	CONTROLES FÍSICOS	86	100	OPTIMIZADO
A.8	CONTROLES TECNOLÓGICOS	82	100	OPTIMIZADO
PROMEDIO EVALUACIÓN DE CONTROLES		87	100	OPTIMIZADO

Imagen N° 3 Evaluación efectividad de controles - ISO 27001:2022 ANEXO A– Fuente: Instrumento MSPI remitido por la DTSI

De acuerdo con los resultados obtenidos en la evaluación de efectividad de controles del Modelo de Seguridad y Privacidad de la Información – MSPI, la entidad alcanza un nivel de madurez global optimizado, con una calificación promedio de 87 frente a una meta de cumplimiento del 100 . Este resultado evidencia un grado de consolidación en la gestión de la seguridad de la información, reflejando la aplicación sistemática y consistente de los controles definidos por el modelo, así como un enfoque orientado a la mejora continua.

En el análisis por dominios, los controles organizacionales registran una calificación de 85, lo cual refleja que la entidad cuenta con lineamientos, políticas y procedimientos formalizados y aplicados de manera adecuada, aunque con oportunidades de fortalecimiento para cerrar brechas frente al nivel objetivo. En cuanto a los controles de personas, se obtiene una calificación de 95, evidenciando avances significativos en la gestión del talento humano, la apropiación de la cultura de seguridad de la información y la sensibilización del personal frente a sus responsabilidades.

Respecto a los controles físicos, estos alcanzan una calificación de 86, lo que indica una gestión e implementación de medidas para la protección de los activos de información y de la infraestructura que los soporta. Finalmente, los controles tecnológicos presentan una calificación de 82, manteniéndose en un nivel optimizado, lo que demuestra la existencia de controles técnicos implementados y operativos, aunque con oportunidades de ajuste y fortalecimiento para asegurar su alineación permanente con los riesgos y las mejores prácticas en seguridad de la información.

Complementariamente, respecto al avance de cláusulas del modelo de operación (PHVA):

AÑO	COMPONENTE (PHVA)	CLAUSULAS	% de Avance Actual	% Avance Esperado
2025	Planificación	Contexto de la organización	8%	14%
		Liderazgo	11%	14%
		Planificación	8%	14%
		Soporte	10%	14%
	Implementación	Operación	14%	16%
	Evaluación de Desempeño	Evaluación del desempeño	9%	14%
	Mejora Continua	Mejora	8%	14%
TOTAL			70%	100%

Imagen N° 4 AVANCE CLÁUSULAS DEL MODELO DE OPERACIÓN (PHVA)– Fuente: Instrumento MSPI remitido por la DTSI

Con base en la revisión del avance del sistema de gestión durante la vigencia 2025, se evidencia un cumplimiento global del 70 frente al 100 esperado, lo cual refleja progresos importantes en la implementación de los componentes del ciclo PHVA, aunque aún persisten brechas que requieren atención para alcanzar el nivel objetivo.

En el componente de planificación, los avances se ubican entre el 8 y el 11 frente a un 14 esperado, evidenciando que los aspectos relacionados con contexto, liderazgo, planificación y soporte se encuentran en proceso de consolidación. En cuanto a la implementación, la cláusula de operación alcanza un 14 frente a un 16 esperado, lo que muestra un desarrollo significativo en la ejecución de los procesos definidos.

Por su parte, la evaluación del desempeño presenta un avance del 9 frente al 14 esperado, y el componente de mejora continua registra un 8 frente al mismo valor de referencia, lo que indica la necesidad de fortalecer las actividades de seguimiento, análisis y mejora para lograr el cumplimiento integral del sistema de gestión.

El instrumento del modelo contempla un levantamiento de información conformado por 42 ítems. Se procedió a validar la información compartida por la DTSI, obteniendo los siguientes resultados:

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
1	Tipo de entidad (Nacional, Territorial y categoría)	La entidad responde dentro del instrumento es de Orden Territorial tipo A	Si
2	Misión	La entidad remite Vinculo de la página web en donde se encuentra la misión la visión y las funciones https://scj.gov.co/es/transparencia/informacion-entidad/mision-vision-funciones	Si
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su	La entidad no relaciona información asociada al análisis de contexto dentro de los instrumentos del Modelo de Seguridad y Privacidad de la Información – MSPI.	No

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
	capacidad para lograr los resultados previstos en el MSPI.		
4	Mapa de Procesos	Se remite vínculo al mapa de procesos de la entidad. https://scj.gov.co/sites/default/files/mapa_procesos_sdscj_2023.jpeg	Si
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces	Se identifica organigrama en el siguiente vinculo: https://scj.gov.co/es/secretaria/organigrama	Si
6	Políticas de seguridad de la información formalizada y firmada	La entidad remite vínculo a la política de seguridad de la información así: https://scj.gov.co/transparencia/obligacion-reporte-informacion/politica-seguridad	Si
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.	Dentro del instrumento del MSPI se incluye un vínculo al organigrama institucional; no obstante, no se evidencia información específica relacionada con la definición de roles y responsabilidades en materia de seguridad de la información, ni la asignación de recursos para su gestión. De igual manera, no se identifican mecanismos documentados para la comunicación y socialización de dichos roles y responsabilidades al interior de la entidad.	No
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.	Se evidenció que, adicional al documento relacionado con la transición del direccionamiento IP de IPv4 a IPv6, la entidad remitió como soporte el acta de aprobación y validación correspondiente a las sedes de la entidad. Dicho documento acredita la revisión y validación del resultado de la autoevaluación de la gestión de la seguridad y privacidad de la información y de la infraestructura de red de comunicaciones por parte de la instancia competente.	Si
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
12	Procedimientos de control documental del MSPI	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
13	Metodología de Gestión de riesgos	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado. No obstante la entidad cuenta con la política de administración de riesgos en el cual se incluye la tipología de riesgos de seguridad la información, por lo indicada se recomienda al proceso responsable complementar el diligenciamiento del instrumento MSPI.	Si
14	Riesgos identificados y valorados de acuerdo a la metodología.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado. Sin embargo la entidad identificados riesgos relacionados con seguridad de la información con sus correspondientes controles por tanto este ítem	Si

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
		se está cumpliendo. Ante lo anterior se recomienda diligenciar el instrumento MSPI Y asociar los soportes relacionados.	
15	Planes de tratamiento de los riesgos	n el marco del seguimiento realizado, se identificó que para el ítem relacionado con los planes de tratamiento de los riesgos no se registra información ni soportes en el instrumento MSPI que permitan evidenciar formalmente su cumplimiento. Sin embargo, se verificó que la entidad cuenta con una Política de Administración del Riesgo que contempla los riesgos de seguridad de la información y define lineamientos para su tratamiento. En consecuencia, el ítem se considera cumplido; no obstante, se recomienda fortalecer el diligenciamiento del instrumento MSPI y la incorporación de evidencias que respalden de manera formal la gestión y tratamiento de los riesgos de seguridad de la información.	Si
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información	Para el ítem relacionado con la existencia de formatos de acuerdos contractuales con contratistas que establezcan responsabilidades en materia de seguridad de la información, se evidenció que en el instrumento MSPI no se registra respuesta ni se incorporan soportes que permitan verificar formalmente su cumplimiento. No obstante, en el desarrollo del seguimiento se identificó que los contratos de prestación de servicios suscritos por la entidad incluyen cláusulas asociadas a la seguridad de la información y a la confidencialidad, lo cual permite establecer responsabilidades claras para las partes. En consecuencia, el ítem se considera cumplido; sin embargo, se recomienda fortalecer el diligenciamiento del instrumento MSPI y asociar las evidencias correspondientes que respalden de manera formal este requisito.	Si
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.	Para este criterio se identificó que en el instrumento MSPI no se registra respuesta ni se adjuntan soportes que evidencien formalmente su cumplimiento. Sin embargo, durante la vigencia 2025 la Dirección de Tecnologías y Sistemas de la Información realizó charlas y capacitaciones en seguridad y privacidad de la información, lo que evidencia la ejecución de acciones asociadas al plan. En consecuencia, el criterio se considera en cumplimiento; no obstante, se recomienda fortalecer el diligenciamiento del MSPI y el aporte de evidencias que respalden dichas actividades.	Si
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado. No obstante, para la vigencia 2025 se identificó que la Dirección de Tecnologías y Sistemas de la Información, en conjunto con la Dirección de Recursos Físicos y Gestión Documental, adelantó la actualización de los activos de información para todos los procesos de la entidad, lo cual permite concluir que el criterio se encuentra cumplido. Se recomienda reflejar esta gestión y sus evidencias en el instrumento MSPI, con el fin de garantizar la trazabilidad y consistencia de la información registrada.	Si
21	Inventario de áreas de procesamiento de información y telecomunicaciones	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
22	Diagrama de red de alto nivel o arquitectura de TI	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
23	Inclusión de la seguridad de la información en la gestión de proyectos	Para el criterio relacionado con la inclusión de la seguridad de la información en la gestión de proyectos, se verificó que el procedimiento de Gestión de Proyectos de TI incorpora, como política de operación, la consideración de los riesgos de seguridad de la información identificados y documentados desde la etapa de planeación, específicamente en el acta de inicio o constitución de los proyectos. Esto evidencia que, en la práctica, la entidad contempla la seguridad de la información como un componente transversal dentro de la gestión de proyectos tecnológicos, dando cumplimiento al criterio evaluado. No obstante, al revisar el instrumento MSPI, se identificó que la información correspondiente a este criterio no se encuentra diligenciada, ni se evidencian soportes o documentos asociados que permitan reflejar de manera explícita dicha gestión dentro del instrumento. En consecuencia, se recomienda actualizar el MSPI, incorporando la información y evidencias pertinentes, con el fin de asegurar la trazabilidad y consistencia entre la operación del control y su registro formal.	Si
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
25	Formato de acuerdo de transferencia de información	Como resultado del seguimiento efectuado, se evidenció que para el ítem relacionado con el formato de acuerdo de transferencia de información el proceso responsable remitió la URL del portal MSPI como soporte. Sin embargo, en la validación realizada no se identificaron lineamientos, formatos ni disposiciones específicas asociadas a la transferencia de información. Por lo anterior, no es posible confirmar el cumplimiento del ítem evaluado. En consecuencia, se recomienda definir y formalizar los lineamientos y formatos correspondientes para la transferencia de información, así como incorporarlos en el instrumento MSPI con sus respectivos soportes, a fin de garantizar la trazabilidad y verificación del control.	No
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.	Derivado del análisis realizado en el presente seguimiento, se observó que para el ítem correspondiente al reporte de eventos e incidentes de seguridad de la información de los últimos doce meses no se evidencian registros ni soportes cargados en el instrumento MSPI. No obstante, se verificó que durante la vigencia 2025 la Dirección de Tecnologías y Sistemas de la Información cuenta con reportes de incidentes de seguridad de la información producto de las actividades de gestión adelantadas. En consecuencia, el ítem se considera cumplido; sin perjuicio de lo anterior, se recomienda fortalecer el diligenciamiento del instrumento MSPI mediante la incorporación de las acciones, actividades y evidencias desarrolladas a nivel institucional, con el fin de asegurar la trazabilidad y el adecuado seguimiento de la gestión de incidentes de seguridad de la información.	Si
28	Plan de continuidad de la Entidad aprobado	Para el ítem relacionado con la existencia del Plan de Continuidad de la Entidad aprobado de manera oficial en el Sistema Integrado de Gestión, se verificó que la entidad cuenta con el documento PL-DE-02 “Plan de Continuidad de Negocio”, en su segunda versión, debidamente formalizado. En consecuencia, el ítem se considera cumplido. No obstante, se evidenció que dentro del instrumento MSPI no se registra información ni se asocian evidencias relacionadas con este plan, por lo cual se recomienda realizar la correspondiente actualización del instrumento, incorporando el documento y sus soportes, con el fin de garantizar la trazabilidad y coherencia de la información reportada.	SI
29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información	Como resultado del seguimiento efectuado, se identificó que para el ítem relacionado con el inventario de obligaciones legales, estatutarias, reglamentarias y normativas en materia de seguridad de la información no se evidencia diligenciamiento ni soportes asociados en el instrumento MSPI. Sin embargo, se verificó que en el Sistema Integrado de Gestión la entidad dispone de la Política de Seguridad de la Información y del Manual de Seguridad y Privacidad de la Información, documentos que incorporan los principales lineamientos normativos aplicables. En este sentido, el ítem se	SI

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
		considera cumplido; no obstante, se recomienda actualizar el instrumento MSPI incluyendo el inventario correspondiente y las evidencias de soporte, a fin de garantizar la trazabilidad y coherencia de la información reportada.	
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad	En relación con este ítem, en el instrumento MSPI no se evidencia el diligenciamiento ni el reporte de información asociada al listado de auditorías en materia de seguridad de la información. No obstante, durante la vigencia evaluada, la Oficina de Control Interno adelantó actividades de seguimiento a la implementación de la política de Gobierno y Seguridad Digital, las cuales guardan relación directa con este aspecto. En consecuencia, el ítem se considera cumplido; sin perjuicio de lo anterior, se recomienda actualizar el instrumento MSPI e incorporar de manera formal la información y los soportes correspondientes a las auditorías y seguimientos realizados.	SI
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno Digital	en el instrumento MSPI se referencia el vínculo al Sistema Integrado de Gestión (portal institucional), en el cual, principalmente dentro del proceso de Gestión de Tecnologías de la Información, se encuentra disponible documentación asociada a seguridad de la información y al Modelo de Seguridad y Privacidad de la Información del MinTIC y a Gobierno Digital, entre la que se destacan la Política de Seguridad de la Información y el Manual de Seguridad y Privacidad de la Información. En consecuencia, este ítem se considera cumplido.	Si
32	Indicadores y métricas de seguridad de la información definidos.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
33	Declaración de aplicabilidad	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos	En relación con este criterio, la aceptación de los riesgos residuales por parte de los dueños de los riesgos se encuentra abordada mediante la Política y la Guía de Administración del Riesgo, particularmente en el capítulo asociado a seguridad de la información, donde se define el tratamiento aplicable a los riesgos identificados. En este sentido, a nivel institucional el tema de seguridad de la información se encuentra incorporado y gestionado, por lo cual el ítem se considera cumplido. No obstante, se recomienda actualizar y diligenciar el instrumento MSPI, incorporando de manera explícita la gestión realizada y los soportes correspondientes frente a este aspecto.	Si
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN		
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
36	Avance en la ejecución del plan de tratamiento de riesgos	En cuanto a este criterio, no se evidencia el registro ni el reporte de información en el instrumento MSPI. Sin embargo, de acuerdo con lo establecido en la Política y la Guía de Administración de Riesgos, así como en el documento PL-GT-03 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, la entidad cuenta con los lineamientos y acciones orientadas a la ejecución del tratamiento de riesgos. En consecuencia, el ítem se considera cumplido; no obstante, se recomienda actualizar el instrumento MSPI e incorporar la información y evidencias que den cuenta del avance en su ejecución.	Si
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO		

N°	Lista de información a solicitar	Comentario OCI 2025	Nivel de cumplimiento
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.	Cómo se indicó, en el instrumento MSPI no se evidencia el diligenciamiento ni el reporte de información asociada al listado de auditorías en materia de seguridad de la información. No obstante, durante la vigencia evaluada, a través del Plan Anual de Auditoria PAA la Oficina de Control Interno adelantó actividades de seguimiento a la implementación de la política de Gobierno y Seguridad Digital, las cuales guardan relación directa con este aspecto. En consecuencia, el ítem se considera cumplido; sin perjuicio de lo anterior, se recomienda actualizar el instrumento MSPI e incorporar de manera formal la información y los soportes correspondientes a las auditorías y seguimientos realizados.	Si
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.	En relación con este criterio, la aceptación de los riesgos residuales por parte de los dueños de los riesgos se encuentra abordada mediante la Política y la Guía de Administración del Riesgo, particularmente en el capítulo asociado a seguridad de la información, donde se define el tratamiento aplicable a los riesgos identificados. En este sentido, a nivel institucional el tema de seguridad de la información se encuentra incorporado y gestionado, por lo cual el ítem se considera cumplido. No obstante, se recomienda actualizar y diligenciar el instrumento MSPI, incorporando de manera explícita la gestión realizada y los soportes correspondientes frente a este aspecto.	Si
	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA		
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.	Dentro del instrumento MSPI no se evidencia el registro de respuestas ni la incorporación de soportes que respalden el cumplimiento del criterio evaluado.	No
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.	Cómo se indicó, en el instrumento MSPI no se evidencia el diligenciamiento ni el reporte de información asociada al listado de auditorías en materia de seguridad de la información. No obstante, durante la vigencia evaluada, a través del Plan Anual de Auditoria PAA la Oficina de Control Interno adelantó actividades de seguimiento a la implementación de la política de Gobierno y Seguridad Digital, las cuales guardan relación directa con este aspecto. En consecuencia, el ítem se considera cumplido; sin perjuicio de lo anterior, se recomienda actualizar el instrumento MSPI e incorporar de manera formal la información y los soportes correspondientes a las auditorías y seguimientos realizados.	Si

Tabla N° 1 Hoja levantamiento de información – Fuente: Instrumento MSPI remitido por la DTSI.

Del análisis integral del levantamiento de información asociado a los 42 ítems que conforman el instrumento del Modelo de Seguridad y Privacidad de la Información – MSPI, se observa que la entidad presenta avances en su nivel de diligenciamiento y documentación. En este sentido, se identifican ítems que cuentan con información completa y soportes adecuados que permiten concluir su cumplimiento; otros que, aun cuando no se encuentran formalmente diligenciados en el instrumento, evidencian desarrollos y prácticas institucionales que permiten considerarlos cumplidos desde el punto de vista operativo; y, finalmente, ítems para los cuales no se registra información ni evidencias que respalden su cumplimiento.

Lo anterior evidencia que, si bien la entidad ha adelantado acciones relevantes en materia de seguridad y privacidad de la información, estas no se encuentran plenamente reflejadas ni sistematizadas en el instrumento MSPI. En consecuencia, se recomienda de manera general fortalecer el proceso de

levantamiento de información, actualizar y diligenciar de forma integral el instrumento, y asociar los soportes correspondientes para cada ítem, con el fin de garantizar la trazabilidad, coherencia y consistencia entre la gestión institucional desarrollada y la información reportada, así como facilitar el seguimiento, la evaluación y la mejora continua del modelo.

A continuación, se presenta el resultado del seguimiento de los controles de seguridad y privacidad de la información contemplados en el instrumento MSPI, con el fin de medir el nivel de madurez del modelo.

La evaluación se organiza en cuatro dominios según ISO 27001:2022 Anexo A: organizacionales, personas, físicos y tecnológicos. La OCI presenta los resultados por cada dominio, principalmente con lo registrado en el instrumento MSPI así:

Dominio controles organizacionales:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.1	A 5.1	Políticas de seguridad de la información	100	La entidad cuenta con la Política y Manual de Seguridad de la Información debidamente aprobada y publicada en el SIG.
AD.1.2	A 5.2	Roles y responsabilidades de seguridad de la información	100	Se evidenció que la entidad cuenta con roles y responsabilidades formalmente establecidos y oficializados en el Sistema Integrado de Gestión. En particular, mediante la Resolución 0098 de marzo de 2021 se modificó el Comité de Gestión Institucional; adicionalmente, el Manual de Seguridad y Privacidad de la Información define los roles y responsabilidades en materia de seguridad de la información, y los procedimientos PD-GT-02 Gestión de Cambios de TIC y PD-GT-03 Gestión de Incidentes de Seguridad de la Información establecen responsabilidades específicas asociadas a dichos procesos. Por otra parte con respecto al tema de roles y responsabilidades, con la actualización de la documentación del modelo, específicamente lo establecido en el documento maestro del MSPI en el numeral 7.2.3 Roles y responsabilidades, se define designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Así mismo, se indica que, en caso de no existir el cargo, este deberá ser delegado mediante acto administrativo y contar con participación con voz y voto en el Comité Institucional de Gestión y Desempeño, y con voz en el Comité de Control Interno. En este contexto, se evidencia que, si bien la entidad ha venido gestionando el MSPI a través de la DTSI, resulta necesario evaluar y ajustar la asignación formal de responsabilidades conforme a lo dispuesto en el modelo actualizado, con el fin de fortalecer la gobernanza, la independencia funcional y el cumplimiento integral de este criterio.

ID. Ítem	Control	Descripción	Nivel de cumplimiento o anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.3	A 5.3	Segregación de funciones	100	Se evidenció que la entidad ha establecido lineamientos formales para la separación de deberes en materia de seguridad de la información. En particular, el Manual de Seguridad de la Información define los parámetros de segregación de funciones; adicionalmente, en los sistemas de información se asignan perfiles de acceso conforme a las funciones de cada usuario, con controles de autorización para el escalamiento de permisos. Este esquema se encuentra soportado por el procedimiento PD-GT-08 Gestión y Administración de Usuarios y el uso del formato F-GT-285 para la solicitud y aprobación de accesos.
AD.1.4	A 5.4	Responsabilidades de la dirección	80	Para el ítem relacionado con las responsabilidades de la dirección en materia de seguridad de la información, se evidenció que la entidad cuenta con políticas, manuales y resoluciones formalmente adoptadas que demuestran el apoyo de la alta dirección a la gestión de la seguridad y privacidad de la información. En particular, se dispone del Manual de Políticas de Seguridad y Privacidad de la Información, la política general adoptada mediante resolución, el plan de sensibilización en seguridad digital y los lineamientos incorporados en los contratos y condiciones de vinculación del personal, lo que permite asegurar que empleados y contratistas conocen sus roles, responsabilidades y obligaciones antes de acceder a la información y a los activos de la entidad. Así mismo, se identificó que la entidad promueve la toma de conciencia y el fortalecimiento de competencias en seguridad de la información mediante acciones de sensibilización y capacitación periódicas, y cuenta con canales formales para el reporte de incidentes o incumplimientos, tales como la Mesa de Servicio y el procedimiento de gestión de incidentes de seguridad de la información. Adicionalmente, la existencia de la Mesa Técnica de Gobierno y Seguridad Digital permite la socialización, seguimiento y análisis de temas y resultados asociados a este componente, fortaleciendo la gestión institucional en la materia. La entidad reporta una calificación de 80; no obstante, en el instrumento evaluado no se identifica el detalle de actividades o temas pendientes que expliquen la brecha frente al cumplimiento total del 100 . Por lo anterior, se recomienda identificar y documentar de manera explícita los temas faltantes, así como las acciones necesarias para su cierre, con el fin de orientar la gestión hacia el logro del cumplimiento integral del aspecto evaluado.
AD.1.5	A 5.5	Contacto con las autoridades	100	Se establece que la entidad da cumplimiento al criterio relacionado con el contacto con las autoridades en materia de seguridad de la información. Conforme a lo definido en el Manual de Seguridad de la Información, en su numeral 7.2.3 “Contacto con las Autoridades”, se encuentran formalizados los lineamientos que determinan cuándo y quién debe efectuar el contacto con las autoridades competentes, así como los escenarios en los cuales resulta necesario realizar dichos reportes.
AD.1.6	A 5.6	Contacto con grupos de interés especial	100	Se identifica que la entidad cumple con el criterio asociado al contacto con grupos de interés especial en seguridad de la información. De acuerdo con lo establecido en el Manual de Seguridad y Privacidad de la Información, en su numeral 7.2.4 “Contacto con los Grupos de Interés Especial”, se encuentran definidos los mecanismos y contactos con actores y entidades especializadas en la materia, tales como MinTIC, CSIRT Gobierno, colCERT y otros referentes del sector.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.7	A 5.7	Inteligencia de amenazas	20	De acuerdo con lo informado por el proceso responsable, se evidencia que la entidad se encuentra adelantando la implementación de actividades orientadas a la recolección y análisis de información proveniente de distintos actores en materia de seguridad de la información y ciberseguridad, con el propósito de fortalecer la inteligencia de amenazas y generar conciencia sobre el entorno de riesgos que pueden afectar a la organización. Así mismo, de acuerdo con la calificación otorgada de 20 puntos y al evidenciarse la ausencia de datos en el campo de brechas del instrumento, se recomienda complementar la información consignada, con el fin de identificar y precisar las actividades faltantes o pendientes, y así definir de manera clara las acciones necesarias que permitan avanzar hacia el cumplimiento integral del criterio evaluado.
AD.1.8	A 5.8	Seguridad de la información en la gestión de proyectos	80	Se verificó que los lineamientos y disposiciones correspondientes se encuentran establecidos en la documentación vigente del Sistema Integrado de Gestión, lo cual confirma lo reportado por el área responsable y permite concluir que el aspecto evaluado se encuentra en cumplimiento. No obstante, si bien el instrumento refleja una calificación de 80 , no se evidencia el diligenciamiento del campo de brechas, lo cual impide identificar de manera clara las actividades, acciones o elementos pendientes para alcanzar el cumplimiento total. En consecuencia, se recomienda complementar la información registrada en dicho campo, detallando las gestiones que adelanta la entidad y las acciones requeridas para avanzar hacia el cumplimiento del 100 de este criterio.
AD.1.9	A 5.9	Inventario de información y otros activos asociados	100	Se constató que la entidad ha identificado y documentado su información y los activos asociados, así como su importancia en términos de seguridad de la información, en concordancia con los lineamientos establecidos. Para tal fin, dispone de documentos formales y vigentes en el SIG. Adicional, se identificó que para la vigencia 2025 la actualización del inventario de activos de información, a cargo de la Dirección de Tecnologías y Sistemas de la Información y la Dirección de Recursos Físicos y Gestión Documental, se encuentra en proceso, lo cual permitirá mantener la información actualizada y fortalecer la gestión de los activos en el marco del Sistema de Seguridad de la Información.
AD.1.10	A 5.10	Uso aceptable de la información y otros activos asociados	80	Se verificó que la entidad ha definido y formalizado los lineamientos relacionados con este aspecto a través del Manual de Seguridad de la Información, en cuyo numeral 7.4.3 se establecen los parámetros para el uso aceptable de los activos de información. De acuerdo con la información reportada en el instrumento, este criterio obtuvo una calificación de 80, lo que evidencia un nivel de cumplimiento satisfactorio en cuanto a la existencia de políticas y lineamientos formales. No obstante, no se identificó información detallada en el campo de brechas que permita precisar los aspectos o actividades pendientes para alcanzar el cumplimiento total. En este sentido, se recomienda complementar dicho campo, identificando de manera explícita los elementos faltantes o por fortalecer, con el fin de establecer las acciones requeridas que permitan avanzar hacia un cumplimiento del criterio.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.11	A 5.11	Devolución de Activos	100	La mesa de servicios realiza el borrado seguro de la información en los equipos de cómputo, garantizando la protección de datos y el cumplimiento de los procedimientos establecidos. De acuerdo con lo sustentado por la entidad, se relaciona el formato F-GT-540 “Acta de Entrega Elementos Tecnológicos”; sin embargo, al ser este validado en el Sistema Integrado de Gestión, fue eliminado. Por lo tanto, como recomendación, se requiere que la respuesta sea actualizada para reflejar los lineamientos y documentación vigentes.
AD.1.12	A 5.12	Clasificación de la información	100	La entidad indica que los parámetros para la clasificación de información se encuentran establecidos en el Manual de Seguridad de la Información (numeral 7.4.5). Se dispone del formato F-GD-1081_v1 “Registro de Activos de Información e Índice de Información Clasificada y Reservada”, donde se clasifica la información como Pública, Clasificada o Reservada, así como su criticidad según su naturaleza y relevancia. Adicionalmente, se cuenta con la guía G-FD-1 “Gestión de Activos de Información” para el diligenciamiento de los activos de información. Durante el seguimiento se estableció que, para la vigencia 2025, la Dirección de Tecnologías y Sistemas de la Información, en acompañamiento con la Dirección de Recursos Físicos y Gestión Documental, se encuentra culminando el proceso de actualización de activos de información para todos los procesos, asegurando que la información esté alineada con los lineamientos y documentación vigente.
AD.1.13	A 5.13	Etiquetado de la información	80	El etiquetado de la información está liderado a través de la Dirección de Recursos Físicos y Gestión Documental, siguiendo las tablas de retención documental vigentes y los lineamientos del procedimiento PG-FD-1 “Programa de Gestión Documental”, así como lo establecido en los ítems 6.1.6 y 6.1.7 de la guía G-FD-1 “Gestión de Activos de Información”. Sin embargo, en el seguimiento se identificó que en el campo de brechas no se diligencia información, por lo que con la calificación de 80 no queda claro cuáles son las actividades necesarias para cumplir al 100 el criterio. Como recomendación, se sugiere realizar el diligenciamiento correspondiente e identificar las acciones, actividades y gestiones a ejecutar por la Entidad para lograr la completa implementación del etiquetado de la información. De igual manera, se sugiere tener en cuenta los resultados presentados por la OCI en el informe de auditoría al proceso de gestión documental realizado en la presente vigencia.
AD.1.14	A 5.14	Transferencia de información	80	Los parámetros para la transferencia de información están establecidos en el Manual de Seguridad y Privacidad de la Información (numeral 7.4.10). La Entidad dispone del procedimiento PD-FD-2 “Administración de Archivos”, del procedimiento PD-GD-09 “Servicio de Mensajería” para la transferencia de medios físicos y archivos documentales mediante servicios externos. Sin embargo, en el seguimiento se identificó que en el campo de brechas no se diligencia información, por lo que con la calificación de 80 no queda claro cuáles son las actividades necesarias para cumplir al 100 . Como recomendación, se sugiere realizar el diligenciamiento correspondiente e identificar las acciones, actividades y gestiones a ejecutar por la Entidad para lograr la completa implementación de la transferencia de información de manera segura y conforme a los lineamientos vigentes.
AD.1.15	A 5.15	Control de acceso	100	Según lo evidenciado en la Entidad, en el Sistema Integrado de Gestión se encuentra la Guía I-GRF-04 “Acceso a las Instalaciones de Funcionamiento de la SSCJ”, que gestiona de manera oficial el acceso a las instalaciones. Adicionalmente, se valida que la política y el Manual de Seguridad y Privacidad de la Información incluyen ámbitos relacionados con control de acceso, y en el proceso de gestión de tecnologías de la información se cuenta con el procedimiento PD-GT-8 “Gestión y Administración de Usuarios”. Sin embargo, la

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				respuesta otorgada requiere ser actualizada y complementada para reflejar todos los documentos y procedimientos oficiales existentes, incluyendo los relacionados con el control de acceso a los sistemas de información; por lo tanto, se recomienda realizar esta actividad para asegurar que la información proporcionada esté completa y alineada con los lineamientos vigentes.
AD.1.16	A 5.16	Gestión de la identidad	60	El criterio no se encuentra documentado, ni se diligencia información en el campo de brechas, así como tampoco se relaciona cuál es la gestión o respuesta que justifique la calificación de 60. Por lo tanto, se recomienda actualizar el documento correspondiente y establecer un procedimiento formal que refleje claramente la gestión de identidades, incluyendo todos los pasos y controles necesarios para cumplir con los lineamientos y garantizar el manejo adecuado de identidades de usuarios y entidades.
AD.1.17	A 5.17	Información de autenticación	80	De acuerdo con el Manual de Seguridad de la Información, ítems (Gestión de información secreta para autenticación de usuarios) y (Uso de información secreta para autenticación), se obtuvo una calificación de 80. Sin embargo, no se tiene diligenciado el campo de brechas, lo que impide establecer con claridad cuáles son los aspectos faltantes para alcanzar el cumplimiento total. Durante el seguimiento se evidenció que la entidad cuenta con controles implementados para la autenticación, principalmente mediante el uso de Directorio Activo y sus políticas aplicadas, lo que contribuye a la protección de credenciales y la gestión segura de usuarios. De acuerdo con lo mencionado se recomienda complementar la información principalmente explicando los controles actualmente implementados en el directorio activo y los sistemas de información que se conectan este así como las aplicaciones que tiene su propio ambiente de gestión de usuarios y contraseñas, teniendo como ejemplo los sistemas de información que operan en el C4.
AD.1.18	A 5.18	Derechos de acceso	100	La entidad dispone de documentación formal en el Sistema Integrado de Gestión que respalda la administración de usuarios, incluyendo el Manual de Seguridad y Privacidad de la Información (MA-GT-01), el Procedimiento PD-GT-8 “Administración de Usuarios”, el Formato F-GT-285 “Solicitud administración de Usuarios” y la matriz de roles y usuarios con la cual se controla la informacion de los sistemas de información institucionales. A través de la mesa de servicios se gestionan las solicitudes de activación y eliminación de usuarios en el Directorio Activo, configurando accesos y autorizando servicios conforme a las responsabilidades asignadas. Con base en lo anterior, se obtuvo una calificación de 100, lo que evidencia el cumplimiento del criterio.
AD.1.19	A 5.19	Seguridad de la información en las relaciones con proveedores	100	Se cuenta con documentación formal en el Sistema Integrado de Gestión que aborda la relación con proveedores, conforme al Manual de Seguridad de la Información – Ítem 7.11.1 “Relación con proveedores”. Este lineamiento establece los principios y controles para garantizar la protección de la información en los vínculos contractuales y operativos con terceros. Como acción complementaria, se recomienda al proceso responsable detallar la respuesta incorporando detalles sobre cómo se asegura la protección de la información en la relación con proveedores, incluyendo mecanismos específicos y controles aplicados. Asimismo, se sugiere asociar evidencias que respalden estas prácticas. Esto permitirá consolidar la trazabilidad y garantizar la efectividad de los lineamientos establecidos.

ID. Ítem	Control	Descripción	Nivel de cumplimiento o anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.20	A 5.20	Abordar la seguridad de la información en los acuerdos con proveedores	80	Dentro del marco del Manual de Seguridad de la Información – Ítem 7.11.2 "Tratamiento de la seguridad dentro de los acuerdos con proveedores", se establecen lineamientos para incorporar medidas de protección en los contratos y acuerdos con terceros. En la evaluación se obtuvo una calificación de 80; sin embargo, no se encuentra diligenciado el campo de brechas, lo que no permite identificar las actividades específicas necesarias para Incrementar la calificación del criterio.
AD.1.21	A 5.21	Gestión de la seguridad de la información en la cadena de suministro de las TIC	80	Se evidenció que el Manual de Seguridad de la Información – Ítem 7.11.3 "Cadena de suministro de tecnología de información y comunicación" establece lineamientos para proteger la información en los procesos relacionados con la cadena de suministro. La evaluación obtuvo una calificación de 80; sin embargo, el campo de brechas no fue diligenciado, lo que impide determinar las acciones concretas necesarias para incrementar la calificación. Se recomienda complementar la respuesta detallando cómo se garantiza la seguridad de la información en la cadena de suministro, incorporando controles aplicados, mecanismos de verificación y evidencias que respalden estas prácticas.
AD.1.22	A 5.22	Seguimiento, Revisión y Gestión de Cambios de Servicios de Proveedores	100	El Sistema Integrado de Gestión cuenta con los documentos, procedimientos y formatos aplicables para la gestión de cambios, tal vez como el Manual de Seguridad de la Información, el procedimiento PD-GT-2 "Gestión de Cambios de TIC" y el formato F-GT-278 "Gestión de Cambios". Adicionalmente, la DTSI cuenta con el repositorio en SharePoint con todos los RFC presentados, aprobados y ejecutados.
AD.1.23	A 5.23	Seguridad de la información para el uso de servicios en la nube	80	Se identificó que el proceso responsable otorgó una calificación de 80 para este criterio. Sin embargo, no se diligenció la respuesta en el instrumento ni el campo de brechas, lo que impide establecer cómo se garantiza el avance actual y cuáles son las acciones necesarias para alcanzar el 100 de cumplimiento. Esta falta de información limita la trazabilidad y dificulta la definición de medidas concretas. Ante lo expuesto, se recomienda precisar el diligenciamiento del instrumento, incorporando detalles sobre los controles aplicados para garantizar la seguridad de la información en el uso de servicios en la nube. Asimismo, es importante definir las brechas existentes y las acciones específicas para cerrarlas, incluyendo evidencias que respalden la implementación de mecanismos de protección y monitoreo. Esto permitirá consolidar la gestión y asegurar el cumplimiento integral del criterio.
AD.1.24	A 5.24	Planificación y preparación de la gestión de incidentes de seguridad de la información	80	Se verificó que el Manual de Seguridad de la Información, en el ítem "Gestión de Incidentes de Seguridad de la Información", establece los parámetros para el reporte de eventos. Además, se cuenta con el procedimiento PD-GT-6 "Gestión de Incidentes o Problemas" y los incidentes son documentados en la herramienta Service Manager de la entidad, informándose a las entidades correspondientes según su criticidad. Para esto, se propone diligenciar el campo de brechas en el instrumento, con el fin de identificar las acciones faltantes para alcanzar el total cumplimiento. Asimismo, es importante complementar la información sobre cómo se garantiza la preparación y

ID. Ítem	Control	Descripción	Nivel de cumplimiento o anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				respuesta ante incidentes, incluyendo evidencias del proceso y mecanismos de mejora continua. Esto permitirá fortalecer la trazabilidad y asegurar la efectividad del control.
AD.1.25	A 5.25	Evaluación y Decisión sobre Eventos de Seguridad de la Información	100	Se verificó que el Manual de Seguridad de la Información, en el ítem 7.12.4, establece los parámetros para la evaluación de eventos de seguridad y la toma de decisiones sobre ellos. Cada incidente se evalúa según su criticidad, conforme al procedimiento PD-GT-6 "Gestión de Incidentes o Problemas", y se le asigna el tratamiento adecuado de acuerdo con su relevancia. Todos los casos son reportados y registrados en la herramienta Service Manager habilitada para la entidad.
AD.1.26	A 5.26	Respuesta a los Incidentes de Seguridad de la Información	80	El Manual de Seguridad de la Información, en el ítem 7.12.5, establece los parámetros para la atención de incidentes de seguridad. También, La entidad cuenta con el procedimiento PD-GT-6 "Gestión de Incidentes o Problemas", donde se definen los lineamientos necesarios para la respuesta ante incidentes. Con base en lo anterior, se otorgó una calificación de 80. Para complementar los datos del instrumento se propone diligenciar el campo de brechas, con el fin de identificar las actividades faltantes para alcanzar el 100 de cumplimiento. Además, es importante complementar la información sobre cómo se garantiza la respuesta efectiva ante incidentes, incorporando evidencias del proceso y mecanismos de mejora continua.
AD.1.27	A 5.27	Aprendizaje sobre los incidentes de seguridad de la información	80	Dentro del Manual de Seguridad de la Información, en el numeral 7.12.6, establece los parámetros para el aprendizaje obtenido de los incidentes de seguridad. La entidad cuenta con el procedimiento PD-GT-6 "Gestión de Incidentes o Problemas", donde se definen los lineamientos necesarios para la atención y análisis de incidentes. Con base en lo anterior, se otorgó una calificación de 80. Se sugiere para este tema diligenciar el campo de brechas en el instrumento, con el fin de identificar las actividades faltantes para incrementar la calificación. Además, es importante complementar la información sobre cómo se garantiza el aprendizaje derivado de los incidentes, incorporando evidencias del proceso y mecanismos que permitan la mejora continua.
AD.1.28	A 5.28	Recopilación de pruebas	100	Se verificó que el Manual de Seguridad de la Información, en el numeral 7.12.7 "Recolección de evidencia", establece los parámetros para la recopilación de pruebas en el contexto de incidentes de seguridad. La entidad cuenta con el procedimiento PD-GT-6 "Gestión de Incidentes o Problemas", donde se definen los lineamientos necesarios para la atención y documentación de incidentes. Con base en estas evidencias, se otorgó una calificación de 100, lo que confirma el cumplimiento total del criterio. Se recomienda mantener la actualización periódica del procedimiento y garantizar que las evidencias recopiladas se documenten de manera completa y trazable.

ID. Ítem	Control	Descripción	Nivel de cumplimiento o anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
AD.1.29	A 5.29	Seguridad de la información durante la interrupción	40	Se observó que el proceso responsable otorgó una calificación de 40 para este criterio. Sin embargo, no se diligenció en el instrumento la respuesta ni el campo de brechas, lo que impide conocer cuáles son los aspectos que justifican la calificación y cuáles son las acciones necesarias para alcanzar el 100 de cumplimiento. Para tal fin, se recomienda diligenciar el instrumento de manera completa, incorporando el campo de brechas para identificar las actividades faltantes y definir las acciones concretas que permitan garantizar la seguridad de la información durante interrupciones. Esto facilitará una medición acorde y fortalecerá la gestión del criterio evaluado.
AD.1.30	A 5.30	Preparación de las TIC para la continuidad del negocio	80	En la sección 7.13 del Manual de Seguridad de la Información, se cuenta con información relacionado a la planificación de la continuidad de la seguridad de la información, lo que confirma la existencia del lineamiento; sin embargo, se evidenció un nivel de cumplimiento de 80 y se identificó que el campo brechas no fue diligenciado, lo que impide determinar con exactitud los elementos faltantes para alcanzar el 100 de cumplimiento y limita la trazabilidad y la validación completa de los controles asociados a la preparación de las TIC para la continuidad del negocio. Se recomienda completar de manera detallada el campo brechas, incorporando todos los aspectos relacionados con la gestión de continuidad y la seguridad de la información, con el fin de identificar los faltantes específicos, garantizar la alineación con los requisitos del Manual de Seguridad de la Información, lo anterior con el acompañamiento de la información que actualmente ha determinado la Oficina Asesora de Planeación.
AD.1.31	A 5.31	Requisitos legales, estatutarios, reglamentarios y contractuales	80	Dentro del Manual de Seguridad de la Información, específicamente en el ítem 7.14 Cumplimiento, se identificó que este criterio se está abordando, adicionalmente, la dependencia responsable otorgó una calificación de 80 sobre 100, lo que refleja un nivel aceptable de implementación. Se evidenció que en el campo brechas no se realizó el diligenciamiento correspondiente, por lo cual se recomienda a la entidad identificar las actividades y acciones faltantes que permitan cerrar las brechas existentes. Esto incluye definir responsables, establecer plazos y documentar evidencias que respalden la ejecución de dichas acciones.
AD.1.32	A 5.32	Derechos de propiedad intelectual	100	Dentro de la Política de Seguridad de la Información, en el numeral 7.14 titulado Cumplimiento, se establecen los lineamientos relacionados con los derechos de propiedad intelectual. La dependencia responsable otorgó una calificación de 100 sobre 100, lo que evidencia un cumplimiento total del criterio evaluado. Adicionalmente en el informe anual del cumplimiento de las normas derechos de autor no se reportaron situaciones críticas en referencia al cumplimiento de las normas asociadas. En este caso, se recomienda fortalecer la respuesta mediante la incorporación de evidencias que demuestren cómo se está cumpliendo este requisito, y no únicamente con lineamientos del sistema integrado de gestión.
AD.1.33	A 5.33	Protección de registros	80	En el Manual de Seguridad de la Información, específicamente en el ítem 7.8.8 “Protección de la información de registro”, se identificó que este criterio se está abordando y la dependencia responsable otorgó una calificación de 80 sobre 100, lo que refleja un nivel aceptable de implementación, aunque no se ha alcanzado el cumplimiento total.

ID. Ítem	Control	Descripción	Nivel de cumplimiento o anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				Se evidenció que en el campo brechas no se realizó el diligenciamiento correspondiente; por tanto, se recomienda a la entidad completar este aspecto con el fin de establecer los faltantes y definir la gestión necesaria para cerrar las brechas.
AD.1.34	A 5.34	Privacidad y protección de la PII	80	La entidad, en referencia a la protección de datos personales, cuenta con la PO-GCT-01 Política de Tratamiento y Protección de Datos Personales, la cual se estableció mediante la Resolución 645 de 2018. Este criterio se encuentra abordado y la dependencia responsable otorgó una calificación de 80 sobre 100, lo que refleja un nivel aceptable de implementación, aunque no se ha alcanzado el cumplimiento total. Se evidenció que en el campo brechas no se realizó el diligenciamiento correspondiente; por tanto, se recomienda complementar esta respuesta identificando claramente los aspectos faltantes y las acciones necesarias para cerrar las brechas. Adicionalmente, se sugiere tener en cuenta los resultados del informe de seguimiento emitido por la Oficina de Control Interno en la presente vigencia, en relación con el cumplimiento de la normatividad sobre protección de datos personales.
AD.1.35	A 5.35	Revisión independiente de la seguridad de la información	80	Dentro del Plan de Auditoría 2025, se identificó que este criterio se encuentra abordado y la dependencia responsable otorgó una calificación de 80 sobre 100, lo que refleja un nivel aceptable de implementación, aunque no se ha alcanzado el cumplimiento total. Por tanto, se recomienda definir cuáles son los puntos específicos que requieren atención y qué información debe ser para cumplir con este aspecto.
AD.1.36	A 5.36	Cumplimiento de políticas, normas y estándares de seguridad de la información	80	En el Manual de Seguridad de la Información, específicamente en el ítem 7.14 Cumplimiento, se identificó que este criterio se encuentra abordado y la dependencia responsable otorgó una calificación de 80 sobre 100, lo que refleja un nivel aceptable de implementación. Se evidenció que en el campo brechas no se diligenció; por tanto, se recomienda establecer cuáles son las actividades y gestiones necesarias para cumplir al 100 .
AD.1.37	A 5.37	Procedimientos operativos documentados	100	La entidad cuenta con procedimientos documentados en el Portal MIPG para todos los procesos institucionales, lo que evidencia un cumplimiento total del criterio evaluado. La dependencia responsable otorgó una calificación de 100 sobre 100, reflejando la adecuada implementación de este aspecto.

Tabla N° 2 Controles organizacionales – Fuente: Instrumento MSPI remitido por la DTSI.

Dominio controles de personas:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
P.1.1	A 6.1	Revisión de antecedentes	100	Se verificó que el procedimiento PD-GH-12 "Selección y Vinculación de Personal" y el Manual de Seguridad de la Información – ítem 7.3.1 "Selección" contemplan la revisión de antecedentes del personal como parte del proceso de selección.
P.1.2	A 6.2	Términos y condiciones de empleo	100	Respecto a este criterio, se evidencia que la entidad cuenta con el Manual de Seguridad y Privacidad de la Información – ítem 7.3.2 "Términos y condiciones del empleo" y el Formato F-GH-807 "Compromiso de Confidencialidad y no Divulgación de la Información, los cuales se aplican al momento de la vinculación del personal.
P.1.3	A 6.3	Concientización, educación y entrenamiento en seguridad de la información	100	Se validó que el Manual de Seguridad y Privacidad de la Información – ítem 7.3.4 y el Procedimiento PD-GT-13 "Procedimiento de Uso y Apropiación" establecen lineamientos para la formación, sensibilización y apropiación de la seguridad de la información por parte del personal. Si bien la entidad cuenta con estos lineamientos, durante la vigencia 2025 se han realizado procesos de capacitación y entrenamiento en seguridad de la información. Por lo tanto, se recomienda fortalecer y/o complementar la respuesta registrada en el instrumento MSPI, evidenciando las actividades desarrolladas y su impacto en la apropiación de la seguridad de la información.
P.1.4	A 6.4	Proceso disciplinario	80	Dentro del seguimiento se identificó por parte del equipo auditor que el Manual de Seguridad y Privacidad de la Información contempla el numeral 7.3.5 "Proceso disciplinario". Si bien se evidencia la existencia de lineamientos, se recomienda fortalecer la evidencia en el instrumento MSPI, registrando claramente el alcance de las actividades implementadas y las brechas identificadas, con el fin de reflejar de manera precisa la calificación actual y las acciones necesarias para alcanzar el cumplimiento total.
P.1.5	A 6.5	Responsabilidades después de la finalización o cambio de empleo	100	Se identificó que el Manual de Seguridad y Privacidad de la Información contempla el numeral 7.3.6 "Terminación o cambio de responsabilidades de empleo", estableciendo obligaciones post-empleo, incluyendo confidencialidad y devolución de activos. En la entidad, se han definido actividades claras para notificar cambios de rol o finalización de contrato, ajustar accesos a sistemas, y gestionar la entrega de credenciales, información y bienes asignados, incluyendo la generación de paz y salvo para contratistas. Durante el seguimiento se validó que estos procedimientos se aplican efectivamente, garantizando la devolución de activos, la entrega de información entre otros aspectos por medio del paz y salvo.
P.1.6	A 6.6	Acuerdos de confidencialidad o no divulgación	80	En el Manual de Seguridad y Privacidad de la Información se encuentra el numeral 7.9.7 "Acuerdos de confidencialidad o de no divulgación". La SDSCJ ha establecido el formato F-GH-807 "Compromiso de Confidencialidad y No Divulgación de la Información", que debe ser diligenciado por los funcionarios de la entidad para garantizar el cumplimiento de las normas legales y jurídicas relacionadas con la seguridad y privacidad de la información. Si bien se evidencia la existencia de lineamientos relacionados con este control, la calificación actual es de 80 y al no diligenciar el campo de brechas, no se pueden identificar claramente las actividades necesarias para alcanzar el 100. Se recomienda completar esta información en el instrumento MSPI, registrando las brechas y acciones pendientes para asegurar el cumplimiento total del criterio.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
P.1.7	A 6.7	Trabajo remoto	100	Durante el seguimiento se constató que el Manual de Seguridad y Privacidad de la Información incluye el numeral 7.2.7 "Teletrabajo", que define los lineamientos, requisitos de seguridad, uso de dispositivos, acceso remoto y protección de la información en entornos externos a la entidad. Lo anterior también se complementa con el hecho que se cuenta con personal trabajando bajo esta modalidad. Para puntualizar el tema, se recomienda incluir y adicionar dentro del instrumento MSPI las evidencias e información que respalden el cumplimiento de lo descrito en el Manual de Seguridad y Privacidad de la Información, asegurando así la trazabilidad y documentación de las prácticas implementadas en cada modalidad de trabajo remoto.
P.1.8	A 6.8	Reporte de eventos de seguridad de la información	100	En el seguimiento realizado se verificó que la entidad dispone de lineamientos claros para el reporte de eventos o incidentes de seguridad de la información, establecidos en el procedimiento PD-GT-6 "Procedimiento Gestión de Incidentes o Problemas". Adicionalmente, se validó la existencia de los reportes de incidentes gestionados durante la presente vigencia. Se indica continuar documentando y archivando los reportes de incidentes, asegurando la trazabilidad y la disponibilidad de la información para futuras revisiones, adicionalmente, es importante incluir los soportes o evidencias correspondientes, asociándolos de manera explícita al numeral del instrumento MSPI, con el fin de fortalecer lo respondido en el mismo.

Tabla N° 3 Controles de personas – Fuente: Instrumento MSPI remitido por la DTSI.

Dominio controles físicos:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
F.1.1	A 7.1	Perímetros de seguridad física	100	En el seguimiento realizado se verificó que la entidad cuenta con lineamientos para el control de los perímetros de seguridad física, establecidos en el Manual de Seguridad de la Información – ítem 7.7.1, en el instructivo I-GRF-04 "Acceso a las instalaciones de Funcionamiento de la SSCJ" y en el documento MA-GE-1 "Manual Operativo del C4". Dichos lineamientos definen los controles de acceso físico, las zonas restringidas, los mecanismos de protección perimetral y los procedimientos de vigilancia. Adicionalmente, se constató que todas las sedes de la entidad cuentan con controles implementados para el acceso del personal.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
F.1.2	A 7.2	Entrada física	80	Durante la revisión se constató que la entidad cuenta con lineamientos para la entrada física, establecidos en el Manual de Seguridad de la Información – ítem 7.7.2 "Controles de acceso físicos", en el instructivo I-GRF-04 "Acceso a las instalaciones de Funcionamiento de la SSCJ" y en el documento MA-GE-1 "Manual Operativo del C4". Dichos documentos definen los controles de acceso físico, zonas restringidas, mecanismos de protección perimetral y procedimientos de vigilancia. Como se mencionó en el anterior control, la entidad cuenta para el ingreso de personal a todas sus sedes con controles implementados para evitar el acceso no autorizado. En el instrumento MSPI se registró una calificación de 80, sin diligenciar el campo de brechas o los temas faltantes para alcanzar el cumplimiento total del control. Por lo tanto, se determina la pertinencia de fortalecer la documentación, identificando claramente las actividades y gestiones pendientes, así como los temas que deben ser atendidos para lograr el cumplimiento completo del control y actualizar el instrumento MSPI con la información correspondiente.
F.1.3	A 7.3	Aseguramiento de oficinas, salas e instalaciones	80	Se identificó que la entidad cuenta con lineamientos para el aseguramiento de oficinas e instalaciones, establecidos en el Manual de Seguridad de la Información – ítem 7.7.3 "Seguridad de oficinas, recintos e instalaciones", en el instructivo I-GRF-04 "Acceso a las instalaciones de Funcionamiento de la SSCJ" y en el documento MA-GE-1 "Manual Operativo del C4". Estos documentos definen los controles de acceso físico, zonas restringidas, mecanismos de protección perimetral y procedimientos de vigilancia. En el instrumento MSPI se registró una calificación de 80, sin diligenciar el campo de brechas o los temas faltantes para alcanzar el cumplimiento total del control. Por lo tanto, se recomienda fortalecer la documentación, identificando las actividades y gestiones pendientes, así como los aspectos que deben ser atendidos para lograr el cumplimiento completo del control y actualizar el instrumento MSPI con la información correspondiente.
F.1.4	A 7.4	Supervisión de la seguridad física	80	De acuerdo con la respuesta suministrada por la entidad en el instrumento MSPI, la entidad cuenta con un contrato con un proveedor externo para la supervisión de la seguridad física, el cual incluye servicios de vigilancia, monitoreo mediante cámaras, rondas de seguridad y control de accesos a las instalaciones, contribuyendo a la protección de los activos físicos y de la información institucional. No obstante, en el instrumento MSPI se registró una calificación de 80, sin que se haya diligenciado el campo de brechas. Por lo anterior, se indica la conveniencia de fortalecer la documentación, identificando de manera clara las actividades, controles o gestiones pendientes que impiden alcanzar el cumplimiento total del control, así como registrar dichas brechas y acciones en el instrumento MSPI para avanzar hacia una calificación del 100.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
F.1.5	A 7.5	Protección contra amenazas físicas y ambientales	80	Con base en la información reportada por la entidad en el instrumento MSPI, se evidenció que el Manual de Seguridad de la Información incluye el ítem 7.7.4 “Protección contra amenazas externas y ambientales”, en el cual se definen medidas preventivas y de mitigación frente a riesgos físicos y ambientales. Asimismo se tienen implementados elementos en operación, tales como controles de acceso, elementos para la prevención de incendios, sistemas de alarmas, contrato de vigilancia, entre otros. Sin embargo, la calificación registrada en el instrumento MSPI es de 80. En este sentido, se plantea complementar la respuesta consignada, incorporando los controles y actividades actualmente implementados, así como diligenciar y complementar las brechas o aspectos pendientes que permitan alcanzar el cumplimiento total del control y reflejar una calificación del 100.
F.1.6	A 7.6	Trabajar en áreas seguras	80	A partir del análisis de la respuesta consignada por la entidad en el instrumento MSPI, se identificó que el Manual de Seguridad de la Información incluye el ítem 7.7.5 “Trabajo en áreas seguras”, complementado por el instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ” y el documento MA-GE-1 “Manual Operativo del C4”. En estos documentos se establecen los controles de acceso físico, la definición de zonas restringidas, los mecanismos de protección perimetral y los procedimientos de vigilancia aplicables a las áreas que requieren mayores niveles de seguridad. La calificación registrada en el instrumento MSPI es de 80, en este contexto, se considera necesario detallar la respuesta registrada, detallando de manera más completa los controles y actividades que se encuentran en operación, así como diligenciar las brechas o temas pendientes que permitan avanzar hacia el cumplimiento total del control y reflejar una calificación del 100.
F.1.7	A 7.7	Escritorio despejado y pantalla despejada	100	Como resultado de la revisión efectuada, se constató que el Manual de Seguridad de la Información contempla el ítem 7.7.15 “Escritorio y pantalla limpios”, en el cual se establecen las prácticas relacionadas con el resguardo de documentos físicos, el cierre de sesiones, el bloqueo de pantallas y el manejo adecuado de los dispositivos. Adicionalmente, se validó que los equipos de cómputo conectados al directorio activo reciben de manera automática la política de bloqueo de sesión en un tiempo de 4 minutos, cuando el equipo queda desatendido. Durante el seguimiento se evidenció que estas disposiciones se aplican en la entidad, contribuyendo a la protección de la información y a la reducción de riesgos asociados al acceso no autorizado, manteniéndose una calificación de 100 en el instrumento MSPI.
F.1.8	A 7.8	Ubicación y Protección del equipo	80	En validación realizada por el equipo auditor se identificó en el Manual de Seguridad de la Información el ítem 7.7.7 titulado “Ubicación y Protección de los equipos”, en el cual se establecen directrices para la instalación segura de los equipos, la protección frente a amenazas físicas y ambientales y el control de accesos. Estos lineamientos proporcionan un marco para la adecuada protección de los activos tecnológicos de la entidad. No obstante, en el instrumento MSPI se registra una calificación de 80. Por lo anterior, se recomienda especificar la respuesta documentada, incorporando de forma detallada los controles y actividades que se encuentran actualmente en operación, así como diligenciar y complementar las brechas o aspectos pendientes necesarios para alcanzar el cumplimiento total del control y reflejar una calificación del 100.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
F.1.9	A 7.9	Seguridad de los activos fuera de las instalaciones	80	Como resultado del análisis realizado por el equipo auditor, se evidenció que el Manual de Seguridad de la Información contempla el numeral 7.7.12 “Seguridad de equipos y activos fuera de las instalaciones”, en el cual se establecen lineamientos para la protección de los activos cuando estos se encuentran fuera de las instalaciones de la entidad. Estas disposiciones buscan mitigar los riesgos asociados a la pérdida, robo o uso no autorizado de los activos de información. Sin embargo, la calificación obtenida en el instrumento MSPI es de 80, lo que evidencia la necesidad de ampliar la información registrada. En este sentido, se recomienda precisar los controles implementados y las acciones desarrolladas, así como identificar los aspectos pendientes que permitan cerrar las brechas existentes y avanzar hacia el cumplimiento total del control.
F.1.10	A 7.10	Medios de almacenamiento	80	A partir de la información analizada por el equipo auditor, se identificó que el Manual de Seguridad de la Información incorpora disposiciones relacionadas con los medios de almacenamiento mediante los numerales 7.9.5 “Acuerdos sobre transferencia de información” y 7.9.6 “Mensajería electrónica”. En estos apartados se definen lineamientos orientados a garantizar el uso adecuado, la protección y la transferencia segura de la información a través de diferentes medios. Complementario a lo descrito, la valoración de este control en el instrumento MSPI corresponde a una calificación de 80, lo que evidencia oportunidades de mejora en la descripción del control. Por ello, se sugiere ampliar la respuesta registrada, incluyendo de manera detallada los controles en operación y las acciones ejecutadas, así como señalar los aspectos pendientes que permitan cerrar las brechas existentes y avanzar hacia el cumplimiento total del control.
F.1.11	A 7.11	Servicios de apoyo	80	Con base en la revisión realizada, se evidenció que el Manual de Seguridad de la Información contempla el numeral 7.7.8 “Servicios de suministro”, en el cual se establecen lineamientos orientados a garantizar la continuidad y seguridad de los servicios de apoyo que soportan la operación de la entidad. Dichos lineamientos buscan prevenir afectaciones a la disponibilidad de los servicios y a la seguridad de la información ante fallas en los suministros. La calificación registrada en el instrumento MSPI es de 80, lo que indica la necesidad de fortalecer la información consignada. En este sentido, se propone complementar la respuesta, detallando los controles implementados, las actividades en operación y los aspectos pendientes que permitan cerrar las brechas identificadas y avanzar hacia el cumplimiento total del control.
F.1.12	A 7.12	Seguridad del cableado	80	Se identificó que el Manual de Seguridad de la Información contempla el ítem 7.7.9 “Seguridad del cableado”, en el cual se establecen lineamientos orientados a la protección del cableado eléctrico y de telecomunicaciones frente a daños, interferencias o accesos no autorizados. Estas disposiciones contribuyen a preservar la continuidad de los servicios y la integridad de la información. La calificación registrada en el instrumento MSPI es de 80, lo cual evidencia que, si bien existen lineamientos definidos, la información consignada resulta parcial. En consecuencia, es necesario ampliar la descripción del control, incorporando de manera más detallada las

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				actividades y controles que se encuentran en operación, así como los aspectos pendientes que impiden alcanzar el cumplimiento total del control.
F.1.13	A 7.13	Mantenimiento de equipos	100	En validación realizada, se evidenció que el Manual de Seguridad de la Información contempla el numeral 7.7.10 "Mantenimiento de Equipos", en el cual se establecen lineamientos para la adecuada conservación y funcionamiento de los activos tecnológicos. Durante el seguimiento se constató que la entidad cumple con los cronogramas de mantenimientos programados, lo que contribuye a garantizar la disponibilidad, integridad y seguridad de los equipos.
F.1.14	A 7.14	Eliminación segura o reutilización de equipos	100	En resultado del seguimiento realizado, se evidenció que el Manual de Seguridad de la Información contempla el numeral 7.7.13 "Disposición segura o reutilización de equipos", en el cual se establecen los lineamientos para la eliminación segura o reutilización de los equipos, garantizando la protección de la información y la correcta gestión de los activos tecnológicos.

Tabla N° 4 Controles físicos – Fuente: Instrumento MSPI remitido por la DTSI.

Dominio controles tecnológicos:

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.1	A 8.1	Dispositivos de punto final de usuario	100	La DTSI remite respuesta al instrumento MSPI, evidenciando el cumplimiento de los controles asociados a los dispositivos de punto final de usuario, conforme a lo establecido en la documentación del SIG.
T.1.2	A 8.2	Derechos de acceso privilegiado	80	La dependencia remite respuesta al instrumento MSPI, indicando la aplicación de las directrices definidas en el Manual de Seguridad de la Información, específicamente en el ítem 7.5.13 – Uso de programas utilitarios privilegiados, relacionadas con el control y uso de herramientas con privilegios elevados. No obstante, a pesar de que se asigna una calificación de 80 , se evidencia que el campo correspondiente a brechas no fue diligenciado y no se describen las actividades, acciones o gestiones pendientes que permitan llevar el cumplimiento del control al 100 . En consecuencia, se recomienda identificar y documentar los aspectos faltantes, así como definir las acciones necesarias para cerrar las brechas.

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.3	A 8.3	Restricción de acceso a la información	80	La dependencia remite respuesta al instrumento MSPI y se procede a corroborar la información con base en los documentos mencionados, evidenciando la existencia de lo establecido en el Manual de Seguridad de la Información, ítem 7.5 Control de acceso, orientado a la restricción del acceso a la información bajo el principio de mínimo privilegio. Sin embargo, pese a la calificación obtenida de 80 , se evidencia que no se diligenció el campo correspondiente a brechas o derechos, ni se detallan las acciones requeridas para avanzar hacia un mayor nivel de cumplimiento. En este sentido, se recomienda completar dicho campo, identificando claramente los aspectos pendientes y las acciones necesarias que permitan fortalecer el control y alcanzar una calificación superior. En otra medida se sugiere describir la manera de cómo se restringe el acceso a la información.
T.1.4	A 8.4	Acceso al código fuente	80	La información remitida en respuesta al instrumento MSPI permite evidenciar la existencia de los lineamientos definidos y asociados, los cuales se encuentran en el Manual de Seguridad de la Información, ítem 7.5.14 Control de acceso a códigos fuente de programas, así como del procedimiento PD-GT-17 Ciclo de Vida de Desarrollo de Software, orientados a la protección del código fuente. No obstante, pese a la calificación de 80 , se observa que no se diligenció el campo correspondiente a brechas lo cual no describe las actividades, acciones o gestiones pendientes que permitan alcanzar el cumplimiento total del control. En consecuencia, se recomienda identificar y documentar los aspectos faltantes y definir las acciones necesarias para cerrar las brechas y avanzar hacia una calificación del 100 .
T.1.5	A 8.5	Autenticación segura	80	La información remitida en respuesta al instrumento MSPI permite evidenciar la aplicación de los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.5.10 Restricción de acceso a la información, así como del procedimiento PD-GT-8 Gestión y Administración de Usuarios, en los que se definen los mecanismos de autenticación para el acceso a los recursos de red. No obstante, pese a la calificación de 80 , se recomienda fortalecer la respuesta con el fin de detallar de manera clara cómo se está logrando la autenticación segura en los sistemas de información, teniendo en cuenta que una parte significativa de estos se encuentra integrada al Directorio Activo. Lo anterior permitirá identificar posibles brechas, documentar las acciones de mejora y avanzar hacia un mayor nivel de cumplimiento del control.
T.1.6	A 8.6	Gestión de la capacidad	80	De acuerdo con la respuesta presentada en el instrumento MSPI, se evidencia la adopción de los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.8.3 Gestión de capacidad, orientados al monitoreo y la planificación de la capacidad de los recursos tecnológicos. No obstante, pese a la calificación de 80 , no se observa el diligenciamiento del campo de brechas ni la descripción de las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. Por lo anterior, se recomienda identificar y documentar los aspectos faltantes y definir acciones de mejora que permitan fortalecer este control y avanzar hacia una calificación del 100 .

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.7	A 8.7	Protección contra malware	100	Con base en la información remitida por el área responsable en el instrumento MSPI, se valida el cumplimiento de lo dispuesto en el Manual de Seguridad de la Información, ítem 7.8.5 Controles contra códigos maliciosos, evidenciando la aplicación de medidas preventivas y reactivas frente a software malicioso, lo que sustenta la calificación del 100 . Como recomendación, se sugiere complementar la respuesta detallando los controles implementados, tales como el uso de soluciones de antivirus, mecanismos de actualización y monitoreo, así como otras medidas técnicas y operativas adoptadas para la protección contra malware, con el fin de fortalecer la documentación y soporte del cumplimiento alcanzado.
T.1.8	A 8,8	Gestión de vulnerabilidades técnicas	100	De acuerdo con la respuesta consignada en el instrumento MSPI, se valida el cumplimiento de lo dispuesto en el Manual de Seguridad de la Información, ítem 7.8.12 Gestión de las vulnerabilidades técnicas, en articulación con el Plan de Gestión de Vulnerabilidades vigente, lo cual respalda la calificación del 100 . Como recomendación, se sugiere complementar la respuesta reportando de manera clara las actividades que se desarrollan o que se tienen implementadas en el marco de este criterio.
T.1.9	A 8.9	Gestión de la configuración	80	La información reportada por el área responsable en el instrumento MSPI permite evidenciar la implementación de los lineamientos definidos en el Manual de Seguridad de la Información y en los Manuales Técnicos de los Sistemas de Información, donde se documentan las configuraciones aprobadas y los procedimientos para su gestión. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describen las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. En consecuencia, se recomienda identificar y documentar los aspectos faltantes, así como definir las acciones necesarias que permitan fortalecer la gestión de la configuración.
T.1.10	A 8.10	Eliminación de información	80	La respuesta registrada en el instrumento MSPI evidencia la aplicación de los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.7.13 Disposición segura o reutilización de equipos, relacionados con los procedimientos para la eliminación segura de la información contenida en dispositivos. Sin embargo, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describen las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. En este sentido, se recomienda identificar y documentar los aspectos faltantes y definir las acciones necesarias que permitan fortalecer la eliminación segura de la información y avanzar hacia una calificación del 100 .

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.11	A 8.11	Enmascaramiento de datos	80	La información consignada en el instrumento MSPI permite evidenciar la aplicación de los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.10.13 Protección de los datos de prueba, relacionados con el uso seguro de datos en entornos no productivos, incluyendo prácticas de enmascaramiento. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describen las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. En consecuencia, se recomienda identificar y documentar los aspectos faltantes, así como definir las acciones necesarias que permitan fortalecer las prácticas de enmascaramiento de datos.
T.1.12	A 8.12	Prevención de fuga de datos	80	La DTSI, en el instrumento MSPI, indica la aplicación de las medidas establecidas en el Manual de Seguridad de la Información, ítem 7.9 Seguridad de las comunicaciones, orientadas a la protección de la información durante su transmisión y a la prevención de fugas de datos. Sin embargo, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se detallan las acciones de mejora requeridas. En este sentido, se sugiere precisar y documentar las actividades técnicas y procedimentales pendientes, así como los controles específicos que deben fortalecerse o implementarse, con el fin de cerrar las brechas identificadas y avanzar hacia el cumplimiento total del control.
T.1.13	A 8.13	Copia de seguridad de la información	80	La información reportada por la DTSI en el instrumento MSPI refleja la implementación de las directrices establecidas en el procedimiento PD-GT-11 Gestión de Infraestructura y Plataformas Tecnológicas, orientadas a la realización y administración de copias de seguridad de la información. Sin embargo, pese a la calificación de 80 , no se diligenció el campo de brechas ni se detallan las acciones pendientes para alcanzar el cumplimiento total del control. Por lo anterior, se recomienda identificar y documentar los aspectos faltantes y definir las acciones de mejora correspondientes, incluyendo de manera expresa los componentes y sistemas de información que operan en el C4, con el fin de fortalecer el cumplimiento de este criterio a nivel institucional y avanzar hacia una calificación del 100 .
T.1.14	A 8.14	Redundancia de las instalaciones de procesamiento de información	80	La DTSI, en el instrumento MSPI, señala la aplicación de los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.13.4 Disponibilidad de instalaciones de procesamiento de información, orientados a garantizar la continuidad operativa mediante esquemas de redundancia. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describen las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. En este sentido, se recomienda identificar y documentar los aspectos faltantes, así como definir las acciones técnicas y operativas requeridas para fortalecer los mecanismos de redundancia y avanzar hacia una calificación del 100 .
T.1.15	A 8.15	Registro	80	La información reportada por la DTSI en el instrumento MSPI evidencia la implementación de los lineamientos definidos en el Manual de Seguridad de la Información, ítems 7.8.7 Registro de eventos y 7.8.9 Registro del administrador y del operador, orientados a la generación, almacenamiento y revisión de los registros de actividades. Sin embargo, pese a la calificación de 80 , no se diligenció el campo de brechas ni se detallan de manera suficiente las acciones pendientes para alcanzar el cumplimiento total del control. Adicionalmente,

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				como resultado de las pruebas de efectividad realizadas a los planes de mejoramiento del proceso de gestión de emergencias, se identificó que en el componente de logs o registros de eventos persiste la misma observación previamente formulada, especialmente en el sistema de videovigilancia Securos. Por lo anterior, se recomienda reevaluar la calificación asignada, realizar un diagnóstico integral de toda la plataforma tecnológica de la entidad, incluyendo los sistemas de información que operan en el C4, y definir acciones correctivas que permitan fortalecer la gestión de registros y asegurar el cumplimiento efectivo de este control.
T.1.16	A 8.16	Actividades de seguimiento	80	La información reportada por la DTSI en el instrumento MSPI evidencia la aplicación de los lineamientos establecidos en el Manual de Seguridad de la Información, ítems 7.9.1 Controles de redes y 7.9.2 Seguridad de los servicios de red, relacionados con las actividades de monitoreo y supervisión de la infraestructura de red. No obstante, pese a la calificación de 80 , no se diligenció el campo de brechas ni se describen las acciones pendientes para alcanzar el cumplimiento total del control. Adicionalmente, de manera similar a lo observado en el control de registro de eventos, se recomienda reevaluar la calificación asignada y realizar un diagnóstico general de los mecanismos de seguimiento y monitoreo de la red en toda la plataforma tecnológica de la entidad, incluyendo los sistemas de información que operan en el C4, con el fin de fortalecer este criterio y avanzar hacia su cumplimiento integral.
T.1.17	A 8.17	Sincronización del reloj (clock)	100	La DTSI en el instrumento MSPI evidencia el cumplimiento de los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.8.10 Sincronización de relojes, orientados a mantener la coherencia temporal en los sistemas de información, lo cual sustenta la calificación del 100 . No obstante, en el marco de la revisión de las pruebas de efectividad realizadas al proceso de gestión de emergencias, se identificaron situaciones relacionadas con la sincronización de relojes en los puntos de videovigilancia. Frente a esta situación, el proceso auditado indicó que adelantará las gestiones necesarias, teniendo en cuenta que se requiere la intervención técnica correspondiente, con el fin de asegurar la consistencia temporal en todos los componentes de la plataforma tecnológica.
T.1.18	A 8.18	Uso de programas de utilidad privilegiados	80	En el marco del diligenciamiento del instrumento MSPI, la DTSI reporta la implementación de los controles establecidos en el Manual de Seguridad de la Información, ítem 7.5.13 Uso de programas utilitarios privilegiados, relacionados con el uso seguro de herramientas con privilegios elevados. No obstante, pese a la calificación de 80 , no se registraron brechas ni se detallaron las actividades, acciones o gestiones pendientes para alcanzar el cumplimiento total del control. Por lo anterior, se recomienda identificar y documentar los aspectos faltantes, así como definir las acciones técnicas y administrativas requeridas que permitan fortalecer este control y avanzar hacia una calificación del 100 .

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.19	A 8.19	Instalación de software en sistemas operativos	100	Como parte de la revisión del instrumento MSPI, se verifica la aplicación de los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.8.11 Instalación de software en sistemas operativos, orientados a garantizar la instalación controlada de software en los sistemas institucionales, lo cual respalda la calificación del 100 . Como recomendación, se sugiere fortalecer la respuesta consignada en el instrumento, incorporando de manera más detallada las acciones que actualmente se ejecutan en la entidad para el control de la instalación de software en los sistemas operativos, a fin de consolidar y evidenciar el cumplimiento total de este criterio.
T.1.20	A 8.20	Seguridad en redes	80	En el desarrollo del diligenciamiento del instrumento MSPI, la DTSI señala la aplicación de los controles definidos en el Manual de Seguridad de la Información, ítem 7.9.1 Controles de redes, orientados a la protección de la infraestructura de red y de los servicios que la utilizan. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describen las acciones pendientes para alcanzar el cumplimiento total del control. En este sentido, se considera pertinente identificar y documentar los aspectos faltantes, así como establecer las acciones técnicas y operativas necesarias que permitan fortalecer la seguridad en redes y avanzar hacia una calificación del 100 .
T.1.21	A 8.21	Seguridad de los servicios de red	80	Dentro de la información reportada en el instrumento MSPI, la DTSI da cuenta de la aplicación de los controles establecidos en el Manual de Seguridad de la Información, ítem 7.9.2 Seguridad de los servicios de red, orientados a la protección de la infraestructura de red y de los servicios que la utilizan. Sin embargo, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se precisaron las acciones necesarias para alcanzar el cumplimiento total del control. En consecuencia, se hace pertinente identificar y documentar los aspectos faltantes, así como definir las acciones técnicas y operativas que permitan fortalecer este control y avanzar hacia una calificación del 100 .
T.1.22	A 8.22	Segregación de redes	80	En el diligenciamiento del instrumento MSPI, la DTSI reporta la adopción de las medidas definidas en el Manual de Seguridad de la Información, ítem 7.9.3 Separación en las redes, orientadas a la protección de la infraestructura de red y de los servicios que la utilizan a través de esquemas de segregación. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se precisaron las acciones necesarias para alcanzar el cumplimiento total del control. En consecuencia, se hace necesario identificar y documentar los aspectos faltantes, así como establecer las acciones técnicas y operativas que permitan fortalecer la segregación de redes

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
T.1.23	A 8.23	Filtrado web	80	Como resultado de la información consignada en el instrumento MSPI, la DTSI da cuenta de la implementación de servicios de seguridad perimetral que contemplan funcionalidades de filtrado web para controlar y restringir el acceso a contenidos no autorizados o maliciosos. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se especificaron las acciones pendientes para alcanzar el cumplimiento total del control. En consecuencia, se considera necesario identificar y documentar los aspectos faltantes, así como definir las acciones técnicas y operativas que permitan fortalecer el filtrado web
T.1.24	A 8.24	Uso de criptografía	80	En la información registrada en el instrumento MSPI, la DTSI manifiesta la aplicación de los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.6.1 Uso de controles criptográficos, orientados a la protección de la información mediante el uso de mecanismos criptográficos. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se detallaron las acciones pendientes para alcanzar el cumplimiento total del control. En este contexto, se hace necesario fortalecer la respuesta consignada, indicando de manera clara en qué aspectos y componentes de la entidad se tiene implementada la criptografía, tales como comunicaciones, almacenamiento de información, sistemas de información o servicios de red.
T.1.25	A 8.25	Ciclo de vida de desarrollo seguro	80	Dentro del seguimiento efectuado al diligenciamiento del instrumento MSPI, se observa que la entidad dispone del procedimiento PD-GT-17 Ciclo de Vida de Desarrollo de Software, en el cual se establecen las etapas, responsabilidades y controles de seguridad aplicables a lo largo del proceso de desarrollo. No obstante, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se describieron las acciones necesarias para alcanzar el cumplimiento total del control. En este contexto, se considera pertinente realizar una revisión interna de los procedimientos asociados y su aplicación práctica, con el fin de identificar los elementos que aún no se encuentran plenamente implementados o documentados, y formalizar las actividades requeridas que permitan evidenciar un mayor nivel de madurez en la incorporación de la seguridad durante todo el ciclo de vida del desarrollo de software.
T.1.26	A 8.26	Requisitos de seguridad de la aplicación	80	En la revisión realizada al instrumento MSPI, se observa que la entidad ha incorporado los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.10.1 Análisis y especificación de requisitos de seguridad de la información, orientados a la definición de requisitos de seguridad para las aplicaciones. No obstante, a pesar de la calificación de 80 , no se diligenció el campo de brechas ni se detallaron las acciones necesarias para alcanzar el cumplimiento total del control. En consecuencia, se considera importante identificar y documentar los aspectos faltantes, así como definir las acciones que permitan fortalecer la gestión de los requisitos de seguridad de la información en las aplicaciones.
T.1.27	A 8.27	Arquitectura del sistema seguro y principios de ingeniería	100	Resultado del análisis del instrumento MSPI, se valida que la entidad aplica los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.10.8 Principios de construcción de los sistemas seguros, orientados al diseño de

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				arquitecturas de sistemas que integran la seguridad desde su concepción, lo cual sustenta la calificación del 100 .
T.1.28	A 8.28	Codificación segura	80	Durante la revisión del diligenciamiento del instrumento MSPI, se observa que la entidad contempla los lineamientos definidos en el Manual de Seguridad de la Información, ítem 7.10.9 Ambiente de desarrollo seguro, orientados a la adopción de prácticas de codificación segura. Sin embargo, pese a la calificación de 80 , no se diligenció el campo correspondiente a brechas ni se precisaron las acciones necesarias para alcanzar el cumplimiento total del control. En consecuencia, se requiere identificar y documentar los aspectos faltantes, así como definir las acciones que permitan fortalecer las prácticas de codificación segura.
T.1.29	A 8.29	Pruebas de seguridad en desarrollo y aceptación	80	En el proceso de revisión del instrumento MSPI, se evidencia que la entidad considera los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.10.11 Pruebas de seguridad de los sistemas, aplicables a las fases de desarrollo y aceptación. No obstante, aunque se asignó una calificación de 80 , no se evidenció el diligenciamiento del campo de brechas ni la definición clara de las actividades, acciones o gestiones pendientes que permitan alcanzar el cumplimiento total del control. En este sentido, se considera necesario identificar y documentar de manera precisa los aspectos aún no cubiertos, así como establecer las acciones concretas que fortalezcan tanto la ejecución como la adecuada documentación de las pruebas de seguridad.
T.1.30	A 8.30	Desarrollo subcontratado	80	En el análisis del instrumento MSPI, se identifica que la entidad contempla los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.10.10 Desarrollo contratado externamente, así como en el procedimiento PD-GT-17 Ciclo de Vida de Desarrollo de Software, en los que se definen controles orientados a garantizar que las pruebas de seguridad hagan parte integral de los procesos de desarrollo y aceptación. Frente a la calificación de 80 , se hace necesario precisar y documentar las brechas existentes, así como definir de manera clara las actividades, acciones o gestiones pendientes que permitan fortalecer la aplicación de los controles de seguridad en los desarrollos subcontratados.
T.1.31	A 8.31	Separación de los entornos de desarrollo, prueba y producción	80	En el marco del diligenciamiento del instrumento MSPI, se identifica que la entidad ha definido lineamientos para la separación de los entornos de desarrollo, prueba y producción, conforme a lo establecido en el Manual de Seguridad de la Información, ítem 7.8.4 Separación de los ambientes de desarrollo, y en el procedimiento interno PD-GT-17 Ciclo de Vida de desarrollo de software, pruebas y operación. Frente a la calificación de 80 , se considera pertinente fortalecer la respuesta consignada, incorporando la documentación que identifique de manera específica cuáles sistemas de información cuentan con dos o tres ambientes diferenciados. Lo anterior permitirá clarificar el nivel real de implementación, así como determinar las acciones necesarias para cerrar las brechas identificadas.
T.1.32	A 8.32	Gestión de cambios	100	La información consignada en el instrumento MSPI evidencia la aplicación de los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.8.2 Gestión de cambios, así como del procedimiento PD-GT-2 Gestión de

ID. Ítem	Control	Descripción	Nivel de cumplimiento anexo A ISO 27001 – (Calificación DTSI)	Comentario OCI
				Cambios de TIC, orientados al control, registro y aprobación de los cambios en los componentes tecnológicos.
T.1.33	A 8.33	Información de prueba	80	Se identifica que la entidad contempla los lineamientos establecidos en el Manual de Seguridad de la Información, ítem 7.10.11 Pruebas de seguridad de los sistemas, relacionados con el manejo y uso de información de prueba. Frente a la calificación de 80 , se hace necesario precisar y documentar las brechas existentes, así como definir de manera clara las actividades, acciones o gestiones pendientes que permitan fortalecer el uso seguro de la información de prueba y avanzar hacia el cumplimiento total de este control.
T.1.34	A 8.34	Protección de los sistemas de información durante las pruebas de auditoría	0	Para el control Protección de los sistemas de información durante las pruebas de auditoría no se reportó información por parte del área responsable. En consecuencia, no fue posible asignar valor a este control, razón por la cual se establece una calificación de 0 . Adicionalmente, no se diligenció el campo correspondiente a brechas ni se registraron actividades, acciones o gestiones asociadas, lo que impide evaluar el nivel de implementación y definir acciones orientadas a su cumplimiento.

Tabla N° 5 Controles tecnológicos– Fuente: Instrumento MSPI remitido por la DTSI.

De manera posterior, para la evaluación del Modelo de Seguridad y Privacidad de la Información MSPI, se analiza el avance de las cláusulas del Modelo de Operación bajo el enfoque PHVA (previamente presentadas) así:

5.3.2 Planificación:

Para la vigencia 2025, la entidad informa que ha definido y documentado los elementos fundamentales para la gestión de la seguridad y privacidad de la información, tales como la Política de Seguridad y Privacidad de la Información, el Manual de Seguridad y Privacidad de la Información, los procedimientos aplicables, los roles y responsabilidades, el inventario de activos de información y la articulación del MSPI con el Sistema de Gestión Documental. Adicionalmente, se cuenta con la identificación, valoración y tratamiento de riesgos, así como con un Plan de Comunicaciones.

El documento maestro del MSPI establece que, para el desarrollo de la fase de Planificación, se deben utilizar los resultados obtenidos en la fase de planeación y, con base en estos, elaborar el Plan de Seguridad y Privacidad de la Información. Dicho plan tiene como objetivo permitir a la entidad realizar la planeación del tiempo, los recursos y el presupuesto necesarios para la ejecución de las actividades relacionadas con la implementación, operación y fortalecimiento del MSPI.

En este sentido, la entidad cuenta oficialmente con el Plan de Seguridad y Privacidad de la Información, identificado como PL-GT-1, el cual se encuentra publicado en el SIG y hace parte del proceso de Gestión de Tecnologías de la Información. Dicho plan corresponde a la versión vigente con fecha 30 de enero de

2025 y constituye el instrumento mediante el cual se definen y articulan las actividades requeridas para la adecuada planeación y ejecución de las acciones relacionadas con el MSPI.

De manera complementaria para esta fase y con lo estipulado por el documento maestro MSPI, se indica que se deben generar los siguientes documentos a los cuales se les realiza seguimiento así:

Requerimiento	Seguimiento OCI
Alcance MSPI	El documento de implementación del MSPI construido por la DTSI, Indica dentro de su alcance lo siguiente" *El Modelo de Seguridad y Privacidad de la Información (MSPI) será aplicable a todos los procesos, sistemas de información, aplicaciones, plataformas tecnológicas, servicios, así como al personal vinculado a la Secretaría Distrital de Seguridad, Convivencia y Justicia (SDSCJ), incluyendo funcionarios, contratistas y terceros que gestionen o tengan acceso a información sensible o datos personales. Esta aplicabilidad garantiza un enfoque integral en la protección de los activos de información institucionales"* . También dentro del Manual de Seguridad y Privacidad de la Información se encuentra articulado con el alcance del Modelo de Seguridad y Privacidad de la Información MSPI, al establecer de forma expresa los lineamientos y directrices que regulan la gestión y tratamiento de la información en la entidad. Este alcance integra a funcionarios, contratistas y terceros, cubre todas las etapas del ciclo de vida de la información y contempla el cumplimiento de los principios de confidencialidad, integridad y disponibilidad, así como de los requisitos legales y normativos aplicables.
Acto administrativo con las funciones de seguridad y privacidad de la información.	En el análisis realizado a este criterio, se evidencia que la entidad ha adelantado acciones orientadas a la definición y asignación de funciones relacionadas con la seguridad y privacidad de la información, reflejadas en la matriz de roles y responsabilidades de seguridad de la información. Adicionalmente, durante la vigencia 2025, en el marco de la II sesión ordinaria del Comité Institucional de Gestión y Desempeño, como instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la adecuada implementación y seguimiento del Sistema de Gestión de Calidad SGC y del Modelo Integrado de Planeación y Gestión MIPG en la Secretaría Distrital de Seguridad, Convivencia y Justicia, se abordaron temas y se adoptaron decisiones relacionadas con el Modelo de Seguridad y Privacidad de la Información, lo cual evidencia una gestión continua a lo largo de las vigencias. Sin perjuicio de lo anterior, para este criterio el modelo exige de manera específica la existencia de un acto administrativo formal que establezca las funciones de seguridad y privacidad de la información. En la documentación revisada no se evidencia dicho acto administrativo. En consecuencia, se sugiere a la entidad elaborar y formalizar la documentación requerida, mediante la expedición del acto administrativo correspondiente, con el fin de dar cumplimiento integral a lo establecido por el modelo.
Adoptar la Política de Seguridad y Privacidad de la Información mediante acto administrativo, indicando el número de resolución o acto administrativo correspondiente.	Se constató que la entidad adoptó la Política de Seguridad y Privacidad de la Información mediante acto administrativo, a través de la Resolución número 0025 de enero de 2021, por medio de la cual se formaliza su adopción. En este sentido, se concluye que el criterio se encuentra cumplido en su totalidad, al contar con el soporte administrativo que oficializa la política y respalda su aplicación a nivel institucional.
Documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información.	Se evidencia que la entidad cuenta con el documento de roles y responsabilidades asociadas a la seguridad y privacidad de la información, a través del formato F-GT-953 versión 2 Matriz de Roles y Responsabilidades, el cual se encuentra diligenciado. En este documento se definen y asignan responsabilidades, obligaciones y funciones de acuerdo con los diferentes roles, entre los que se incluyen la Alta Dirección, la Dirección de Tecnologías y Sistemas de la Información, los líderes o responsables de proceso, el Profesional de Seguridad de la

Requerimiento	Seguimiento OCI
	Información, el Grupo de Gestión de Cambios, el Profesional de Uso y Apropiación, así como los funcionarios y contratistas, lo cual permite evidenciar la formalización de responsabilidades en materia de seguridad y privacidad de la información dentro de la entidad. Como comentario de la verificación realizada, se observa que el campo titulado “acto administrativo” no se encuentra diligenciado para ninguno de los roles, ni se evidencia un documento formal u oficial que respalde y formalice dichas asignaciones. Por lo anterior, se sugiere complementar este campo con el acto administrativo correspondiente, con el fin de fortalecer la formalización y trazabilidad de las responsabilidades definidas.
Procedimiento de inventario y clasificación de la información e infraestructura crítica.	Se verifica que la entidad cuenta con el Procedimiento de inventario y clasificación de la información e infraestructura crítica, el cual se encuentra documentado y publicado en el portal MIPG mediante la G-GD-01 Guía de Gestión de Activos de Información e Índice de Información Clasificada y Reservada, adscrita al proceso de Gestión Documental, con fecha de publicación 24 de noviembre de 2023, versión 1. Lo anterior evidencia que la entidad dispone de lineamientos formales para la identificación, clasificación y gestión de sus activos de información, en concordancia con los requerimientos del MSPI.
Metodología de inventario y clasificación de la información e infraestructura crítica.	La entidad cuenta con una metodología formal para el inventario y la clasificación de la información, así como para la identificación de la infraestructura crítica, a través del documento G-GD-01 Guía de Gestión de Activos de Información e Índice de Información Clasificada y Reservada, oficializado en el Sistema Integrado de Gestión. En particular, el numeral 7.2.1.8 Infraestructura Crítica Cibernética establece los criterios y parámetros necesarios para determinar si los activos de información pueden ser catalogados como Infraestructura Crítica Cibernética, considerando impactos sociales, económicos y ambientales. En este sentido, se concluye que la entidad dispone de las metodologías requeridas para identificar, evaluar y establecer su infraestructura crítica, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información.
Política de Gestión de Riesgos de la entidad, incluyendo lineamientos para la gestión de riesgos de seguridad y privacidad de la información y demás documentación asociada que determinan dichos lineamientos para la administración y gestión del riesgo.	Se constató que la entidad dispone de lineamientos formales para la gestión de riesgos, incluyendo aquellos asociados a la seguridad y privacidad de la información. En el portal MIPG se encuentra publicada la PO-FI-02 Política de Administración de Riesgos, del proceso de Fortalecimiento Institucional, versión 3, con fecha 07/07/2025, así como la G-FI-04 Guía de Administración de Riesgos, versión 4, con fecha 25/07/2025. Esta documentación permite evidenciar que la entidad cuenta con un marco definido para la administración y gestión del riesgo, en concordancia con los lineamientos del MSPI.
Plan de tratamiento de riesgos de seguridad de la información.	En el portal MIPG se evidencia que la entidad cuenta con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, identificado como PL-GT-3, adscrito al proceso de Gestión de Tecnologías de la Información. Dicho plan fue actualizado con fecha 30/01/2025 y constituye el instrumento mediante el cual se definen las acciones para el tratamiento de los riesgos de seguridad y privacidad de la información, en concordancia con los lineamientos establecidos por el MSPI.
Declaración de aplicabilidad.	En relación con el criterio de Declaración de Aplicabilidad, se informa que la Dirección de Tecnologías y Sistemas de la Información DTSI cuenta con un documento en estado de borrador de la Declaración de Aplicabilidad, el cual será presentado para aprobación en la próxima sesión del Comité Institucional de Gestión y Desempeño. Lo anterior evidencia gestión y avance por parte de la entidad frente a este requisito, especialmente considerando la actualización del instrumento realizada por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC en la presente vigencia. Adicionalmente, se mantiene la articulación con los controles de la ISO 27001, para los cuales la entidad ha venido generando documentación y lineamientos oficializados en el Sistema Integrado de Gestión.

Requerimiento	Seguimiento OCI
Manual de políticas de Seguridad de la Información.	La entidad cuenta oficialmente con el Manual de Seguridad y Privacidad de la Información, identificado como MA-GT-1, adscrito al proceso de Gestión de Tecnologías de la Información. Dicho manual se encuentra publicado con fecha 25/11/2024, versión 5, y establece las políticas y lineamientos generales para la gestión de la seguridad y privacidad de la información en la entidad, en concordancia con los requerimientos del MSPI.
Plan de capacitación, sensibilización y comunicación de seguridad de la información	Se observa que la Dirección de Tecnologías y Sistemas de la Información dispone de un Plan de Uso y Apropiación orientado a fortalecer la cultura organizacional en materia de seguridad y privacidad de la información. Este plan contempla, para la vigencia 2025, la ejecución de actividades de capacitación, sensibilización y divulgación a nivel institucional, las cuales se desarrollan a través de canales como el correo electrónico, la intranet, boletines informativos y presentaciones internas. En este sentido, se cuenta con soporte documental que respalda la existencia y aplicación de acciones dirigidas a promover la apropiación de los lineamientos de seguridad y privacidad de la información en la entidad.

Tabla N° 6 Documentos etapa de planificación – Fuente: Instrumento MSPI remitido por la DTSI.

5.3.3 Implementación:

El documento maestro indica que "Tras *finalizar la fase 7 de planeación del MSPI, se iniciará la implementación de los procesos de seguridad de la información: gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Se fomentará la cultura de seguridad y se definirán criterios de cumplimiento y mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el SGSI. Los documentos que se deben generar en esta fase son*"; de acuerdo con lo mencionado, se realiza seguimiento de cada uno de estos así:

- **Actualización del inventario de información:** Respecto a la actualización del inventario de información, se identifica que para la vigencia 2025 la entidad se encuentra adelantando el proceso de actualización de los activos de información. Esta actividad se desarrolla de manera articulada entre la Dirección de Tecnologías y Sistemas de la Información y la Dirección de Recursos Físicos y Gestión Documental, con el objetivo de consolidar la información y culminar el ejercicio antes del cierre de la presente vigencia.

- **Actualización de la matriz de riesgos de seguridad de la información**: Se establece que la Dirección de Tecnologías y Sistemas de la Información realiza seguimiento y actualización de la matriz de riesgos de seguridad de la información con una periodicidad cuatrimestral. Para este proceso se cuenta con un repositorio de evidencias que soporta las actualizaciones efectuadas, las cuales han sido validadas por la segunda y tercera línea de defensa, lo que permite evidenciar control, seguimiento y gestión adecuada del riesgo de seguridad de la información.

- **Plan de implementación de controles de seguridad:** En el análisis del criterio correspondiente a la fase de implementación, se identifica que la entidad cuenta con el Plan de Seguridad y Privacidad de la Información PL-GT-01, en el cual se incorporan los resultados actuales y el consolidado de los controles alineados con la Norma ISO/IEC 27001. En este documento se establece que, al finalizar la presente vigencia, se realizará la actualización del plan, así como la validación y los ajustes a la implementación de los controles, atendiendo los nuevos requisitos definidos en la Norma ISO/IEC

27001:2022. En este sentido, se reconoce la gestión adelantada por la entidad frente a la implementación y fortalecimiento de los controles de seguridad de la información, evidenciando un proceso en ejecución y alineado con los lineamientos normativos vigente.

- **Actualización de la gestión de eventos e incidentes de seguridad de la información**: fue identificado por el equipo auditor que la Dirección de Tecnologías y Sistemas de la Información cuenta con la actualización de la gestión de eventos e incidentes de seguridad de la información. Para este fin, la entidad dispone del registro y seguimiento de los eventos e incidentes a través de la herramienta Service Manager, en la cual se documentan de manera sistemática los casos presentados, permitiendo su control, trazabilidad y gestión conforme a los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información.
- **Actualización de la gestión de vulnerabilidades**: la Dirección de Tecnologías y Sistemas de la Información adelanta de manera permanente actividades de análisis sobre los servidores y servicios tecnológicos de la entidad. Estas acciones se encuentran soportadas con documentación correspondiente a los ejercicios de análisis realizados en diferentes vigencias, lo cual permite evidenciar un proceso continuo de identificación y tratamiento de vulnerabilidades. En consecuencia, se reconoce que la entidad mantiene una gestión activa frente a este tema, en alineación con los lineamientos de seguridad de la información.
- **Evidencia de la implementación de los controles de seguridad de la información**: Como resultado de la revisión efectuada a este criterio, se identifica que la entidad dispone de la información registrada en el instrumento del Modelo de Seguridad y Privacidad de la Información, así como de documentación oficializada y publicada en la página web institucional y en el portal del Sistema Integrado de Gestión MIPG. De igual manera, se cuenta con la documentación asociada a la ejecución de cada uno de los procedimientos del proceso de Gestión de Tecnologías de la Información, lo cual permite soportar la implementación de los controles de seguridad y privacidad de la información.

Posteriormente, el instrumento MSPI para esta fase se subdivide en 3 elementos así:

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001 (DTSI)	Seguimiento OCI
8.1	Planificación y control operacional	Planificar, implementar, controlar & documentar el proceso del SGSI para gestionar los riesgos (i.e. un plan de tratamiento de riesgos)	60	Una vez evaluado el criterio 8.1 Planificación y control operacional, correspondiente a la fase de implementación del MSPI, se evidencia que en el instrumento la Dirección de Tecnologías y Sistemas de la Información asignó una calificación de 60 . No obstante, durante la revisión se identificó que los campos asociados a evidencias y brechas no fueron diligenciados, lo cual impide establecer los soportes que justifican dicha calificación, así como identificar con claridad los aspectos pendientes o los controles que requieren fortalecimiento para alcanzar el cumplimiento total del criterio. En este sentido, se sugiere a la dependencia responsable complementar el diligenciamiento del instrumento, incorporando las evidencias y la información

				necesaria que permita sustentar la calificación otorgada y definir las acciones requeridas para avanzar hacia el 100 de cumplimiento.
8.2	Evaluación de riesgos de seguridad de la información	(Re)hacer la apreciación y documentar los riesgos de seguridad de la información en forma regular y ante cambios o modificaciones	100	Frente a este criterio, la entidad reporta una calificación de 100 en el instrumento MSPI; sin embargo, no se registraron evidencias que respalden dicha valoración. Teniendo en cuenta que la entidad realiza análisis y gestión de riesgos de seguridad de la información de manera periódica, con una frecuencia cuatrimestral, resulta necesario incorporar en el instrumento los soportes documentales derivados de estas actividades. Por lo anterior, se recomienda fortalecer el registro de evidencias, de manera que se garantice la trazabilidad y sustento del cumplimiento reportado para este criterio.
8.3	Tratamiento del riesgo de seguridad de la información	Implementar el plan de tratamiento de riesgos (tratar los riesgos) y documentar los resultados	100	En relación con este criterio, se evidencia que la entidad cuenta con documentación oficializada en el Sistema Integrado de Gestión MIPG, específicamente el documento PL-GT-3 Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, con fecha 30/01/2025, versión 10. No obstante, dicha información no fue reportada en el instrumento MSPI. Por lo anterior, se recomienda actualizar el instrumento incorporando la referencia y los soportes correspondientes, a fin de asegurar la trazabilidad y coherencia entre la documentación institucional y el reporte del modelo.

Tabla N° 7 Etapa de implementación – Fuente: Instrumento MSPI remitido por la DTSI.

5.3.4 Evaluación del desempeño:

Para esta fase, el documento maestro del modelo indica que:"*Una vez culminada las actividades de la fase de operación del MSPI, se evalúa la efectividad de las acciones tomadas a través de los indicadores definidos en la fase de implementación que debe incluir la correcta interacción entre el MSPI, MIPG y los requerimientos de la Ley 1581 de 2012 "Protección de datos personales", Ley 1712 de 2014 "Ley de Transparencia y Acceso a la Información Pública", Decreto 2106 de 2019 o cualquier norma que las reglamente, adicione, modifique o derogue*".

A continuacións presentan los elementos que componen esta fase:

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001 (DTSI)	Seguimiento OCI
9.1	Seguimiento, medición, análisis y evaluación	Hacer seguimiento, medir, analizar y evaluar el SGSI y los controles	60	Para este requisito se asignó una calificación de 60 en el instrumento MSPI; no obstante, no se evidenció el diligenciamiento del campo correspondiente a evidencias ni brechas. En consecuencia, no es posible identificar los soportes que sustentan dicha calificación ni los aspectos pendientes por fortalecer para alcanzar un mayor nivel de madurez. Se sugiere a la dependencia responsable complementar la información en el instrumento, incorporando las evidencias y brechas identificadas que permitan reflejar el estado real del seguimiento y evaluación del SGSI.

9.2	Auditoría interna	Planificar y llevar a cabo auditorías internas del SGSI	80	Frente a este criterio se reportó una calificación de 80; sin embargo, el instrumento no cuenta con información diligenciada en los campos de evidencias ni brechas. Esta situación limita la verificación de los soportes asociados a la planeación y ejecución de auditorías internas del SGSI, así como la identificación de oportunidades de mejora. Se recomienda completar el registro de evidencias y brechas, con el fin de respaldar la calificación otorgada y orientar las acciones necesarias para el fortalecimiento del proceso. También se sugiere complementar su diligenciamiento reportando los documentos que soportan el cumplimiento del requisito (informes de auditoría, planes de mejoramiento, actas de seguimiento) y describir los aspectos pendientes o de mejora en el campo de brechas, con el fin de fortalecer la trazabilidad y el control del proceso de auditoría interna.
9.3	Revisión por la dirección	Determinar los objetivos del SGSI de la organización y cualquier cuestión que pueda comprometer su efectividad	60	Para este requisito se asignó una calificación de 60, sin que se haya registrado información en los campos de evidencias ni brechas del instrumento MSPI. En consecuencia, no se logra establecer qué información, análisis o decisiones de la alta dirección respaldan dicha calificación, ni cuáles son los elementos faltantes para avanzar hacia el cumplimiento total del criterio. Se sugiere diligenciar los campos correspondientes, documentando los insumos, resultados y brechas asociadas a la revisión del SGSI por parte de la alta dirección.

Tabla N° 8 Etapa Evaluación de desempeño – Fuente: Instrumento MSPI remitido por la DTSI.

5.3.5 Mejoramiento continuo:

En esta fase se establecen las actividades adelantadas respecto al plan de mejoramiento continuo de seguridad y privacidad de la información el cual hace parte del modelo; a continuación se presenta el seguimiento realizado por la OCI:

NUM	DESCRIPCIÓN	REQUISITOS	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001 (DTSI)	Seguimiento OCI
10.1	Mejora continua	Mejorar continuamente el SGSI	60	Para el criterio de mejora continua se observa una calificación de 60 , sin que se encuentre diligenciado el campo de evidencias ni el de brechas en el instrumento MSPI. En este sentido, no es posible evidenciar las acciones adelantadas ni los elementos pendientes para fortalecer el SGSI. Se recomienda establecer de manera explícita las actividades que conforman las brechas identificadas y documentar las evidencias respectivas, permitiendo así determinar las acciones necesarias para alcanzar el 100 de cumplimiento.
10.2	No conformidad y acciones correctivas	Identificar, corregir y llevar a cabo acciones para prevenir la recurrencia de no conformidades, documentando las acciones	60	Respecto a este criterio, se reporta una calificación de 60 ; sin embargo, no se registró información en los campos de evidencias ni brechas. Esta situación dificulta la identificación de las acciones implementadas para el tratamiento de no conformidades y la prevención de su recurrencia. Se sugiere definir y documentar las actividades pendientes dentro de las brechas, así como diligenciar el campo de evidencias, con el propósito de establecer claramente las acciones requeridas para lograr el cumplimiento total del criterio.

Tabla N° 9 Etapa Mejoramiento continuo – Fuente: Instrumento MSPI remitido por la DTSI.

5.3.6 Calificación frente a mejores prácticas en ciberseguridad (NIST)

Respecto al componente de ciberseguridad- NIST, dentro del instrumento MSPI la entidad reporta lo siguiente:

MODELO FRAMEWORK CIBERSEGURIDAD NIST		
Etiquetas de fila	CALIFICACIÓN ENTIDAD	NIVEL IDEAL CSF
GOVERNAR	80	100
IDENTIFICAR	84	100
PROTEGER	86	100
DETECTAR	80	100
RESPONDER	80	100
RECUPERAR	81	100

Imagen N° 5 Componente Ciber - NIST – Fuente: : Instrumento MSPI remitido por la DTSI

Función	Categoría	CALIFICACIÓN	Clausula / Control ISO 27001
Governar (GV)	Contexto organizativo	60	4. Contexto de la Organización
Governar (GV)	Estrategia de gestión de riesgos	60	6.1 Acciones para tratar con los riesgos y oportunidades
Governar (GV)	Funciones, responsabilidades y autoridades	100	5.2. Funciones y responsabilidades de seguridad de la información. 5.3 Segregación de funciones. 5.5 Contacto con las autoridades
Governar (GV)	Política	100	Clausula 5.2 Política. 5.1 Políticas de seguridad de la información
Governar (GV)	Supervisión	80	8.16 Actividades de supervisión
Governar (GV)	Gestión de riesgos de la cadena de suministro en materia de seguridad cibernética	80	5.21 Gestión de seguridad de la información en la gestión de la cadena de suministro TIC
Identificar (ID)	Gestión de activos	93	5.9 Inventario de información y otros activos asociados. 5.10 Uso aceptable de la información y otros activos asociados 5.11 Devolución de activos
Identificar (ID)	Evaluación de riesgos	100	Clausula 8.2 Evaluación de riesgos de seguridad de la información.
Identificar (ID)	Mejora	60	Clausula 10.1 Mejora continua. 10.2 No conformidad y acciones correctivas
Proteger (PR)	Gestión de identidades, autenticación y control de acceso	70	8.2 Derechos de acceso privilegiado. 8.3 Restricción de acceso a la información. 8.4 Acceso al código fuente. 8.5 Autenticación segura 5.15 Control de acceso. 5.16 Gestión de identidad. 5.17 Información de autenticación. 5.18 Derechos de acceso
Proteger (PR)	Concienciación y capacitación	100	6.3 Concientización, educación y capacitación en seguridad de la información
Proteger (PR)	Seguridad de datos	80	8.11 Enmascaramiento de datos. 8.12 Prevención de filtración de datos
Proteger (PR)	Seguridad de plataformas	80	8.21 Seguridad de los servicios de red

Proteger (PR)	Resistencia de la infraestructura tecnológica	100	8.27 Arquitectura del sistema seguro y principios de ingeniería
Detectar (DE)	Monitoreo continuo	60	Clausula 9.1. Seguimiento, medición, análisis y evaluación
Detectar (DE)	Análisis de eventos adversos	100	5.25 Evaluación y Decisión sobre Eventos de Seguridad de la Información
Responder (RS)	Gestión de incidentes	80	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Responder (RS)	Análisis de incidentes	80	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Responder (RS)	Notificación y comunicación de la respuesta al incidente	80	5.26 Respuesta a incidentes de seguridad de la información
Responder (RS)	Mitigación de incidentes	80	5.26 Respuesta a incidentes de seguridad de la información
Recuperar (RC)	Ejecución del Plan de Recuperación de Incidentes	80	5.24 Planificación y preparación de la gestión de incidentes de seguridad de la información
Recuperar (RC)	Comunicación de la recuperación del incidente	80	5.26 Respuesta a incidentes de seguridad de la información
		81,97	

Tabla N° 10 Ítems Ciber - NIST – Fuente: Instrumento MSPI remitido por la DTSI.

El análisis de los resultados del componente de Ciberseguridad, alineado al marco NIST, muestra que la entidad alcanza un promedio general de 81,97, lo cual refleja un nivel de madurez adecuado en la gestión de la seguridad de la información y la ciberseguridad.

Entre los aspectos con mejor desempeño se destacan Política, Funciones y responsabilidades, Evaluación de riesgos, Concienciación y capacitación, Resistencia de la infraestructura tecnológica, Análisis de eventos adversos y Arquitectura del sistema seguro, los cuales presentan calificaciones iguales o cercanas al 100. Estos resultados evidencian que la entidad cuenta con lineamientos definidos, roles, procesos de evaluación de riesgos consolidados y capacidades técnicas para soportar la seguridad de la información.

Por otro lado, los aspectos con mayores oportunidades de mejora corresponden a Contexto organizativo, Estrategia de gestión de riesgos, Mejora continua, Monitoreo continuo y componentes asociados a la gestión de identidades, control de acceso y seguridad de datos, cuyos resultados se ubican entre 60 y 70. Estas calificaciones indican la necesidad de fortalecer la documentación de evidencias, el seguimiento sistemático, la definición de brechas y la ejecución de acciones que permitan cerrar los vacíos identificados y avanzar hacia un mayor nivel de madurez.

En conjunto, los resultados reflejan una base sólida en materia de ciberseguridad, con retos puntuales orientados principalmente al fortalecimiento del ciclo de mejora continua, el monitoreo permanente y la formalización de evidencias que respalden la implementación integral de los controles.

Una vez validada la información reportada por la DTSI en el instrumento MSPI de manera general se presenta la siguiente oportunidad de mejora:

Oportunidad de mejora N° 1: Actualización y diligenciamiento datos del instrumento del Modelo de Seguridad y Privacidad de la Información – MSPI.

En primera instancia se evidenció que, en el levantamiento de información del Modelo de Seguridad y Privacidad de la Información – MSPI, una proporción significativa de los 42 ítems evaluados no cuenta con información diligenciada ni con soportes asociados que permitan evidenciar de manera formal su cumplimiento. Adicionalmente, se identificó que, si bien la entidad ha desarrollado acciones, políticas, procedimientos y actividades relacionadas con la seguridad y privacidad de la información, estas no se encuentran sistemáticamente registradas ni documentadas dentro del instrumento, generando brechas entre la gestión institucional efectivamente realizada y la información reportada.

Como segundo aspecto relevante, en la hoja correspondiente a las cláusulas del modelo, donde se presentan las diferentes fases del MSPI, se identificó la ausencia de diligenciamiento de los campos de evidencias, brechas y recomendaciones. En dichos apartados únicamente se asignaron calificaciones, lo que limita la posibilidad de realizar un contraste objetivo entre el puntaje otorgado y los soportes que lo sustentan, especialmente en aquellos criterios con valoraciones inferiores al 100, para los cuales no se identifican los aspectos pendientes ni las acciones necesarias para alcanzar el cumplimiento total.

Posteriormente, en las hojas relacionadas con los datos de los controles del anexo A de la ISO 27001, subdivididos en controles organizacionales, personas, físicos y tecnológicos, se evidenció de manera general que el campo correspondiente a brechas no fue diligenciado en ninguno de los dominios. Esto impide identificar las situaciones, debilidades o aspectos faltantes que justifican las calificaciones asignadas. Adicionalmente, en el campo de recomendaciones no se incorporaron orientaciones que permitan fortalecer la gestión, pese a que la entidad cuenta con avances y acciones en ejecución que van más allá de la existencia de lineamientos documentales, los cuales fueron, en la mayoría de los casos, el soporte general referenciado en el instrumento.

Por lo anteriormente observado respecto al diligenciamiento de los campos de brechas, evidencias y recomendaciones, limita la consolidación de una hoja de ruta clara que permita priorizar actividades, definir responsables y orientar acciones para incrementar progresivamente el nivel de madurez del Modelo de Seguridad y Privacidad de la Información. Esta situación evita tener trazabilidad, el seguimiento y la evaluación del MSPI, y puede afectar la capacidad de la entidad para demostrar el nivel de madurez y cumplimiento frente a los lineamientos del Modelo, así como para soportar procesos de auditoría, control y mejora continua.

En el marco de lo descrito se recomienda a la DTSI fortalecer el diligenciamiento integral del instrumento MSPI, asegurando que cada ítem evaluado cuente con evidencias documentales claras, la identificación de brechas asociadas a las calificaciones otorgadas y recomendaciones concretas que definan las acciones requeridas para alcanzar el cumplimiento total. Lo anterior permitirá reflejar de manera más precisa la gestión institucional realmente desarrollada, facilitar el seguimiento, la toma de decisiones y contribuir al fortalecimiento continuo y al aumento del nivel de madurez del modelo en la entidad.

6. CONCLUSIONES

Una vez culminado el informe de seguimiento realizado a la implementación de la Política de Gobierno y Seguridad Digital en la Secretaría, se concluye que la entidad ha consolidado un marco normativo y procedimental sólido, evidenciado en la adopción y oficialización de documentos en el SIG asociados principalmente al proceso de Gestión de Tecnologías de la Información.

Respecto a la información reportada en el tablero interactivo de MINTIC, presenta un desempeño favorable y sostenido en la implementación de la Política de Gobierno Digital. El Índice de Gobierno Digital alcanza un puntaje de 87,4, ubicándose por encima del promedio del grupo par (85,3), lo que evidencia un nivel de madurez incremental.

Desde la perspectiva MSPI y sobre la cual se profundizó en el presente informe de seguimiento, se evidenció un avance en la implementación de controles administrativos, de personal, físicos y tecnológicos, reflejado en múltiples controles que alcanzan una calificación del 100 , tales como la gestión de incidentes de seguridad de la información, el trabajo remoto, el mantenimiento de equipos, la disposición segura o reutilización de activos, los perímetros de seguridad física y las prácticas de escritorio y pantalla despejada. Estos resultados demuestran que los lineamientos definidos no solo se encuentran documentados, sino que también están siendo aplicados en la operación institucional.

En materia de seguridad física, la entidad cuenta con controles implementados para el acceso a las instalaciones en todas sus sedes, contratos de vigilancia, mecanismos de control perimetral, procedimientos de monitoreo y lineamientos operativos, lo cual contribuye a la protección de los activos de información y a la continuidad de la operación. No obstante, se identificaron controles con calificación de 80, indicando la falta de diligenciamiento del campo de brechas en el instrumento MSPI, pese a que existen controles y actividades en operación, por tanto, se requiere complementación.

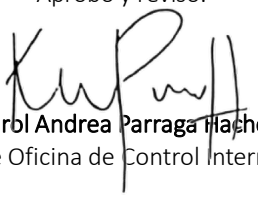
En el componente de talento humano, se evidenció que existen lineamientos definidos para selección, confidencialidad de información, procesos disciplinarios, responsabilidades post-empleo y concientización en seguridad de la información. Sin embargo, en el instrumento no se detalla las brechas ni las acciones necesarias para avanzar hacia el cumplimiento total.

Finalmente, la entidad presenta un nivel de madurez favorable en la gestión de la seguridad y privacidad de la información, con controles implementados y operando de manera efectiva. El principal aspecto de mejora identificado corresponde al fortalecimiento y detalle del diligenciamiento del instrumento MSPI, especialmente en la identificación de brechas, actividades faltantes y evidencias de soporte, con el fin de reflejar de manera más precisa el estado real de cumplimiento y facilitar la toma de decisiones para el cierre de brechas y la mejora continua del modelo.

Elaboró:

Diego Alexander Urazán Franco
Contratista Oficina de Control Interno

Aprobó y revisó:



Karol Andrea Parraga Hache
Jefe Oficina de Control Interno