AUDITORÍA A LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL SGC

Fecha del Informe: 10 de diciembre del 2025
Nombre Auditor: Crhistian Augusto Amador León
No. Informe: OCI-39-2025

1. OBJETIVO Y ALCANCE.

Evaluar el Sistema de Gestión de la Seguridad de la Información operante en el SGC, conforme con los lineamientos del Modelo de Seguridad y Privacidad de la información (Resolución 0500 de 2021 junto con sus actualizaciones y anexos).

La presente auditoría abarcó lo corrido de la vigencia del 2025, y tuvo lugar del 15 de octubre al 30 de noviembre de 2025. Se validaron las actividades propuestas en el plan de mejoramiento resultante de la auditoría en la vigencia 2024 y a la actualización de los lineamientos propuestos por el MinTIC frente al MSPI en el año 2025.

2. CRITERIOS DE AUDITORÍA / SEGUIMIENTO.

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones.
- Ley 1581 de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Decreto 1083 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 648 de 2017. Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.
- Resolución 0500 de 2021 “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”
- Resolución 746 de 2022 “Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021”
- Resolución 2277 de 2025 “Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia”
- Política General de Seguridad de la Información del SGC
- Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos establecidos por MinTIC frente a la implementación del MSPI (Documento Maestro Lineamientos MSPI 2025).
- Norma ISO: IEC 27001:2022

3. METODOLOGÍA

La Oficina de Control Interno (OCI) remitió el memorando con radicado No. 2025-130-005519-3 del 14 de octubre de 2025, correspondiente al plan de auditoría, mediante el cual se solicitó información al Grupo de Trabajo de Gestión de Plataformas de Tecnologías de la sobre los avances o la implementación de las acciones de mejora derivadas de la auditoría realizada en la vigencia 2024, así como el cumplimiento de la normativa relacionada con el Modelo de Seguridad y Privacidad de la Información (MSPI) emitida por el MinTIC.

En este contexto, y en cumplimiento de los requerimientos establecidos en la Resolución 500 de 2021, sus anexos y la Resolución 2277 de 2025 que modificó el anexo 1 de la Resolución 500 de 2021, correspondiente al Documento Maestro de Lineamientos del MSPI 2025, se solicitó la remisión de actos administrativos, políticas, planes, procedimientos, matrices de riesgo, evidencias de ejecución y seguimiento, y demás documentación asociada. Esta solicitud también fue remitida mediante correo electrónico del 27 de octubre de 2025.

Posteriormente, el Grupo de Trabajo Gestión de Plataforma de Tecnologías de Información dio respuesta a la solicitud mediante correo electrónico del 29 de octubre de 2025, a través del cual remitió la información requerida y compartió la ruta del repositorio de información alojado en Google Drive, donde se almacenaron los soportes documentales y evidencias relacionadas con los lineamientos establecidos por el MinTIC y avances o implementación de las acciones de mejora como resultado de la auditoría realizada en la vigencia 2024 . Esta entrega permitió a la Oficina de Control Interno avanzar en el proceso de revisión y verificación del cumplimiento de los criterios establecidos en la normativa vigente.

El informe preliminar fue enviado por esta oficina a la Dirección Técnica de Gestión de la Información y a la Coordinación de Gestión de Plataforma de Tecnologías de Información mediante radicado No. 2025-130-006622-3 del 24 de noviembre de 2025. Las observaciones a este informe preliminar fueron remitidas bajo radicado No. 2025-700-006801-3 del 28 de noviembre de 2025; las observaciones fueron tenidas en cuenta en lo pertinente para la elaboración del presente informe final.

En atención al desarrollo de la auditoría, el día 9 de diciembre de 2025 se llevó a cabo la reunión de cierre, en la cual se socializaron los hallazgos y observaciones contenidos en el Informe Final de Evaluación al Modelo de Seguridad y Privacidad de la Información - MSPI. Durante este espacio se presentaron los resultados obtenidos y se expusieron las respuestas a las observaciones remitidas por el proceso frente al informe preliminar.

4. ANÁLISIS REALIZADO

La revisión de las evidencias y de la documentación observada se llevó a cabo mediante una muestra selectiva de auditoría aplicada a registros y soportes, con el propósito de

evaluar el Sistema de Gestión de Seguridad de la Información operante en el SGC. Esta evaluación se realizó en cumplimiento de los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI), establecidos en la Resolución 0500 de 2021, junto con sus actualizaciones y anexos.

Es importante señalar que se verificó el estado actual de cumplimiento y nivel de implementación de las fases que componen el MSPI, conforme a lo estipulado en el Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información del MinTIC, versión 5 del 21 de abril de 2025.

A continuación, se describen las fases que estructuran el modelo:

- **Diagnóstico:** *"Esta fase permite a las entidades determinar el estado actual de implementación de la seguridad y privacidad de la información. Para ello, se debe aplicar el Instrumento de Evaluación del MSPI, mediante el cual se identifican los controles implementados, se mide el nivel de madurez del modelo y se obtienen los insumos necesarios para la fase de planificación."*

- **Fase 1 - Planificación:** *"Tiene como propósito la elaboración del Plan de Seguridad y Privacidad de la Información, con el fin de definir el tiempo, los recursos y el presupuesto requeridos para desarrollar las actividades asociadas a la implementación del MSPI."*

- **Fase 2 - Operación:** *"Corresponde a la implementación de los procesos de seguridad de la información, tales como la gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. Esta fase fomenta la cultura de seguridad, la definición de criterios de cumplimiento y la adopción de mecanismos de control para procesos y servicios externos relevantes, asegurando su alineación con el Sistema de Gestión de Seguridad de la Información (SGSI)."*

- **Fase 3 - Evaluación del Desempeño:** *"En esta fase se evalúa la efectividad de las acciones implementadas, a través de los indicadores definidos durante la ejecución del modelo. Además, se analiza la interacción del MSPI con el Modelo Integrado de Planeación y Gestión (MIPG) y con los requerimientos de la Ley 1581 de 2012 (Protección de Datos Personales) y la Ley 1712 de 2014 (Transparencia y Acceso a la Información Pública)."*

- **Fase 4 - Mejoramiento Continuo:** *"En esta etapa se consolidan los resultados obtenidos durante la evaluación del desempeño y se formula el Plan de Mejoramiento Continuo de Seguridad y Privacidad de la Información, orientado a mitigar las debilidades identificadas y fortalecer la eficacia del modelo."*

En el desarrollo de esta auditoría al cumplimiento sobre la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en el Servicio Geológico Colombiano, se aplicó una metodología basada en la revisión documental aportada por el área responsable y en el análisis de los soportes suministrados.

4.1. Anexo 1 (Resolución 500 de 2021 y/o 2277 de 2025) – Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información

4.1.1. Fase de Diagnóstico

La fase de diagnóstico permite a las entidades identificar el estado actual de la implementación del MSPI mediante el instrumento de evaluación, con el cual se determinan los controles aplicados y el nivel de madurez alcanzado. Este autodiagnóstico se realiza antes de la fase de planificación y se debe actualizar tras la evaluación de desempeño del proceso, de manera que se reflejen los cambios en la madurez del modelo. El resultado final de esta actualización constituye un insumo clave para la fase de mejoramiento continuo. De acuerdo con el Anexo 1, esta fase incluye:

Lineamiento	Propósito	Salida
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.	Identificar el nivel de madurez de Seguridad y Privacidad de la información en el que se encuentra la entidad, como punto de partida para la implementación del MSPI.	Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación del MSPI en toda la entidad y sus acciones de mejora.

Con base en el instrumento de autodiagnóstico entregado por el Grupo de Trabajo de Gestión de Plataformas de Tecnologías de la Información, se evidenció que este se encuentra elaborado; no obstante, durante su revisión se identificaron varios aspectos que requieren ajuste. En consecuencia, se determinaron los siguientes hallazgos que hacen necesario definir e implementar un plan de mejoramiento:

HALLAZGO 1. Desalineación entre el instrumento de autodiagnóstico utilizado y el formato oficial del MSPI. Al realizar la revisión del archivo "*1.Instrumento Evaluación_MSPI_SGC_2025.xlsx*" remitido por el proceso y compararla con el archivo "Instrumento de autodiagnóstico MSPI" descargado del portal de Gobierno Digital del MinTIC, se evidenció que, aunque ambos comparten la lógica general del autodiagnóstico, no corresponden al mismo formato. En forma adicional:

- El archivo entregado por el proceso indica en su hoja denominada "Portada" el ejercicio como "Evaluación de efectividad de controles – ISO 27001:2013 Anexo A", pese a que el MSPI y su documento maestro establecen lineamientos basados en la ISO/IEC 27001:2022, lo que constituye una referencia normativa desactualizada.
- El instrumento oficial organiza los controles en hojas diferenciadas por dominios (Organizacionales, Personas, Físicos, Tecnológicos, NIST, Cláusulas), con una estructura de columnas que incluye, entre otros, control, Rol, Tipo de control, Propiedades de seguridad, Conceptos de ciberseguridad, Capacidades operativas y Dominio de seguridad, mientras que el archivo utilizado por la entidad agrupa los controles principalmente en hojas denominadas Administrativas, Técnicas y Ciber, incorpora hojas propias como PHVA y Madurez, omitiendo algunos campos de clasificación presentes en el formato oficial.

Esta situación se aparta del criterio establecido en el Documento Maestro Lineamientos MSPI 2025 para la fase de Diagnóstico, que señala que, para la identificación del estado de implementación del MSPI, “se debe utilizar la herramienta de autodiagnóstico del MSPI” y que la salida consiste en el “Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación del MSPI en toda la entidad, y sus acciones de mejora”

Recomendación: Adoptar y documentar el uso de la versión oficial vigente del instrumento de autodiagnóstico MSPI publicada por el MinTIC, asegurando que el autodiagnóstico de la entidad se diligencie directamente sobre dicho formato (manteniendo su estructura de hojas y campos), sin modificar la estructura base del instrumento oficial, de manera que se garantice la plena alineación con el criterio definido en el Documento Maestro y se facilite la validación externa del diagnóstico.

HALLAZGO 2. Incompletitud en el diligenciamiento del instrumento de autodiagnóstico MSPI: Al realizar la revisión documental del instrumento de autodiagnóstico, se evidenció que, aunque este contiene el registro de controles y el cálculo del nivel de madurez, las brechas y sus acciones de mejora se encuentran consignadas de manera parcial, presentándose controles sin acción asociada o recomendaciones generales que no responden a la brecha identificada. Esta situación incumple el criterio establecido en el Documento Maestro Lineamientos MSPI, el cual exige que la herramienta diligenciada identifique de forma completa las brechas en la implementación del MSPI y sus acciones de mejora, limitando la utilidad del diagnóstico como insumo para la fase de Planificación:
Caso 1. Existen brechas sin registrar o están registradas de forma parcial en algunos dominios (ej. controles administrativos y técnicos), sin que todas cuenten con una descripción clara o completa.
Caso 2. Las recomendaciones (acciones de mejora) no están plenamente desarrolladas en parte de los controles; en varios casos se detallan las recomendaciones, pero no se tiene identificada la brecha a abordar.
Caso 3. Se identifican controles sin acción de mejora asociada, aun cuando el instrumento marca la existencia de brecha o cumplimiento parcial.
Caso 4. En algunos dominios del instrumento (ej. ciberseguridad), la evidencia documentada es insuficiente o no se encuentra relacionada con la brecha consignada, generando vacíos en el entendimiento del estado real del control.

Recomendación: Completar el diligenciamiento del instrumento oficial de autodiagnóstico MSPI asegurando que:

- Cada brecha registrada cuente con una descripción clara y coherente.
- Todas las brechas tengan acciones de mejora específicas, verificables y acordes con la necesidad del control evaluado.
- Se incluya evidencia adecuada y directamente relacionada con el estado reportado para cada control.

Esto permitirá que el instrumento cumpla plenamente con la salida definida por el Documento Maestro y pueda ser utilizado como insumo válido para la fase de Planificación del MSPI.

4.1.2. Fase 1: Planificación

En esta fase, la Entidad debe tomar como insumo los resultados del diagnóstico anterior y elaborar el Plan de Seguridad y Privacidad de la Información (MSPI), el cual permitirá planear el tiempo, recursos y presupuesto de las actividades a desarrollar.

Los documentos clave que deben generarse son:
- Alcance del MSPI.
- Acto administrativo que asigne funciones de seguridad y privacidad.
- Acto administrativo de adopción de la Política de Seguridad y Privacidad (con número de resolución).
- Documento de roles y responsabilidades en seguridad y privacidad.
- Procedimiento y metodología de inventario y clasificación de la información e infraestructura crítica.
- Política de gestión de riesgos de la entidad con lineamientos para riesgos de seguridad y privacidad.
- Plan de tratamiento de riesgos de seguridad de la información.
- Declaración de aplicabilidad.
- Manual de políticas de seguridad de la información.
- Plan de cambio, cultura y apropiación.

4.1.2.1. Comprensión de la organización y de su contexto

Lineamiento	Propósito	Salida
Determinar los elementos externos e internos que son relevantes con las actividades que realiza la entidad en el desarrollo de su misión y que podrían influir en las capacidades para lograr los objetivos del modelo, alineado con los objetivos estratégicos de la entidad, teniendo en cuenta procesos necesarios y sus interacciones.	Conocer en detalle las características de la entidad y su entorno con el fin de implementar el Modelo de Seguridad y Privacidad adaptado a las condiciones específicas de cada entidad.	Documento obligatorio: Contexto de la entidad (Política de Planeación Institucional).

Durante la verificación del documento “2. Contexto SGC 2025.xlsx” se verificó que el proceso entregó la información requerida para este lineamiento, incluyendo un análisis general del entorno institucional y una matriz que aborda oportunidades y amenazas desde perspectivas tecnológicas, ambientales, económicas y sociales, evidenciando un esfuerzo por caracterizar elementos del contexto organizacional como punto de partida para la implementación del MSPI.

En la verificación realizada se identificaron brechas importantes con la completitud y alineación normativa del contexto descrito, frente a los elementos internos y externos definidos en el Documento Maestro MSPI 2025 y su anexo de "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas". Estos aspectos se sintetizan en el siguiente hallazgo:

HALLAZGO 3. Incompletitud en la identificación del contexto interno y externo requerido para el MSPI: Al revisar el archivo "*2.Contexto SGC 2025.xlsx*" remitido por el proceso, se evidenció que, si bien el documento incluye un análisis general de factores institucionales y contiene una matriz de oportunidades y amenazas con elementos tecnológicos, ambientales, económicos y sociales, este análisis no desarrolla de manera completa ni alineada los factores del contexto interno y externo exigidos por el Documento Maestro MSPI 2025:

- En relación con el contexto externo, el anexo *"Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas"* del Documento Maestro de Lineamientos establece que deben identificarse elementos como: clientes y proveedores, normatividad aplicable, dependencias operativas, factores culturales, cantidad de ciudadanos atendidos digitalmente, ecosistema digital, interconexiones con terceros y riesgos del entorno asociados a seguridad de la información. Sin embargo, el documento entregado no incorpora estos elementos de forma explícita, limitándose a clasificar oportunidades y amenazas sin vincularlas con los procesos, activos de información o servicios digitales de la entidad.
- Respecto al contexto interno, el anexo mencionado indica que deben analizarse aspectos como recursos económicos, tecnológicos y jurídicos; flujos de información; talento humano; cultura organizacional en materia de seguridad digital y procesos críticos, los cuales no se describen ni desarrollan adecuadamente en el documento revisado.

Recomendación: Ampliar el documento de contexto incorporando de forma explícita todos los factores internos y externos definidos en la sección 7.1.1 del Documento Maestro MSPI 2025 junto con el anexo *"Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas"*, asegurando su relación con la seguridad de la información, los procesos críticos, los activos digitales, la ciudadanía atendida y las dependencias tecnológicas. Adicionalmente, vincular los elementos identificados con la forma en que condicionan o influyen en la implementación del MSPI, de modo que el contexto cumpla su propósito de orientar adecuadamente la fase de planificación. Así mismo, se debe tener en cuenta lo definido en el Documento Maestro de Lineamientos, en el capítulo 3.1.1. Contexto interno y externo de la entidad pública, del Anexo "Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas", para asegurar la completitud y trazabilidad del análisis.

Con respecto al hallazgo mencionado, el proceso indicó en la **respuesta al Informe Preliminar que: "***El documento entregado sí incorpora los elementos definidos en el MSPI, incluyendo factores internos, externos, tecnológicos, normativos, de seguridad y riesgos del entorno. Estos fueron integrados mediante la matriz DOFA construida*

específicamente con base en los lineamientos del modelo. Reconocemos que algunos elementos pueden ampliarse, lo cual realizaremos; sin embargo, dado que el documento contiene los insumos requeridos del MSPI, solicitamos que este punto sea reclasificado como observación".

Respuesta OCI al comentario del informe preliminar: El Anexo "*Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas*" establece que, para el contexto externo, deben considerarse elementos como clientes y proveedores; normativas aplicables; dependencias económicas; entorno cultural; cantidad de ciudadanos atendidos digitalmente; factores sociales, económicos y ambientales; y sistemas con interconexión operativa externa. De igual manera, para el contexto interno, el documento exige analizar recursos económicos, tecnológicos, físicos y jurídicos; flujos de información; talento humano y contratistas; cultura organizacional; procesos críticos; y políticas institucionales. Ninguno de estos factores aparece descrito de forma explícita, ni vinculada a la seguridad de la información en el documento entregado "*2.Contexto SGC 2025*", el cual presenta el análisis DOFA general sin relacionarlo con los activos de información, los servicios digitales, los riesgos del entorno ni las dependencias tecnológicas. Teniendo en cuenta lo anterior, se mantiene el hallazgo.

4.1.2.2. Necesidades y expectativas de los interesados

Lineamiento	Propósito	Salida
Se deben identificar las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información, así como sus necesidades y expectativas. Esta identificación debe incluir los requisitos legales, reglamentarios y contractuales, e integrarse adecuadamente al SGSI.	Conocer las necesidades y expectativas que se tiene respecto a la implementación del modelo de seguridad y privacidad de la información para identificar las acciones y actividades necesarias para satisfacerlas.	Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional). Análisis de partes interesadas en seguridad de la información.

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información el archivo denominado "3. Compendio Partes Interesadas_SGC.pdf" identificando lo siguiente:

OBSERVACIÓN 1. Restricción del alcance institucional y deficiencias en la estructura documental: Al revisar el archivo "3.Compendio Partes Interesadas_SGC.pdf" remitido por el proceso, se evidenció que, si bien el documento identifica partes interesadas internas y externas y describe algunas de sus necesidades y expectativas, el análisis presentado no se ajusta plenamente al lineamiento 7.1.2 del Documento Maestro MSPI 2025. El compendio establece en su alcance que aplica únicamente a las áreas, procesos y activos de información del SGC que interactúan con la DGI, lo cual restringe la cobertura institucional requerida, dado que el MSPI exige identificar a todas las partes

interesadas que puedan influir o verse afectadas por la seguridad y privacidad de la información a nivel entidad, y no únicamente a aquellas vinculadas con una dependencia específica.

Adicionalmente, aunque el archivo presenta una tabla de control de versiones, este no cumple con la estructura documental institucional, al no contar con encabezado oficial, código de documento, responsables de revisión y aprobación ni fechas de vigencia, elementos necesarios para la formalización documental del MSPI.

Recomendación: Ampliar el compendio de partes interesadas para incluir a todas las dependencias, procesos, terceros y actores institucionales relacionados con la seguridad y privacidad de la información, sin limitar su alcance a las áreas que interactúan con la DGI. Asimismo, ajustar la estructura documental del archivo conforme a la normatividad interna, incorporando encabezado institucional, código de documento y responsables de revisión y aprobación.

4.1.2.3. Definición del alcance del MSPI

Lineamiento	Propósito	Salida
Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad. Esta definición debe especificar a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo. Se recomienda iniciar con los procesos misionales, dado su impacto estratégico y su nivel de exposición a riesgos de seguridad y privacidad de la información.	Identificar qué activos de información, software, hardware, roles, sistemas de información, áreas seguras (generada o utilizada en los procesos de la entidad) será protegida mediante la adopción del MSPI.	Alcance del MSPI, (Este alcance puede estar integrado al Manual del Sistema Integrado de Gestión, o en el documento del Modelo de Planeación y Gestión).

En la revisión del documento “Política General de Seguridad de la Información 2025”, señalado como soporte del alcance del MSPI, se verificó que el proceso cuenta con una política estructurada que incorpora directrices generales de seguridad y privacidad, incluyendo una sección denominada “Alcance”. Esto evidencia un avance en la consolidación del marco documental del MSPI; sin embargo, el análisis técnico identificó que dicho documento no desarrolla los elementos específicos requeridos para la definición del alcance del MSPI, lo cual se detalla en el siguiente hallazgo:

HALLAZGO 4. Ausencia de la definición del alcance del MSPI conforme al lineamiento establecido: Al revisar el documento "*Política General de Seguridad de la Información 2025*" indicado como evidencia del alcance del MSPI, se evidenció que este no desarrolla lo solicitado en el lineamiento correspondiente a la "Definición del alcance del MSPI", el cual establece expresamente que debe:

> *"Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad, especificando a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo."*

De igual forma, el propósito del lineamiento señala que se debe:

> *"Identificar qué activos de información, software, hardware, roles, sistemas de información y áreas seguras (…) serán protegidos mediante la adopción del MSPI."*

La evidencia indicada contiene un apartado denominado "Alcance"; sin embargo, este describe únicamente el alcance de la política de seguridad de la información, y no determina los límites, alcance ni aplicabilidad del MSPI, ni especifica los procesos, recursos humanos, financieros, técnicos o tecnológicos a los que se aplicará el modelo, tal como lo exige el lineamiento. Tampoco identifica los activos de información, roles, software, hardware, sistemas de información o áreas seguras que serán protegidos mediante la adopción del MSPI. Si bien la Política General de Seguridad y Privacidad de la Información hace parte de los lineamientos del MSPI y está definida en el numeral 7.2.2 "Política de seguridad y privacidad de la información", este documento no reemplaza la obligación descrita en el lineamiento de definir el alcance del MSPI, dado que dicho lineamiento establece que la política debe construirse con base en la definición previa del alcance, la cual constituye una de sus entradas. Por lo anterior, aunque la política es un componente del MSPI, no corresponde al documento requerido como salida del lineamiento de definición del alcance del MSPI.

Recomendación: Elaborar un documento institucional que contenga de manera explícita la definición del alcance del MSPI, determinando los límites, alcance y aplicabilidad del modelo, y especificando los procesos, recursos humanos, financieros, técnicos y tecnológicos a los cuales se aplicará su implementación, así como los activos de información, software, hardware, roles, sistemas de información y áreas seguras que serán protegidos mediante su adopción. Este documento podrá integrarse al Manual del Sistema Integrado de Gestión o al Modelo de Planeación y Gestión, conforme a la salida definida del lineamiento.

Con respecto al hallazgo mencionado, el proceso indicó en la **respuesta al Informe Preliminar que: "***El alcance del Sistema de Gestión de Seguridad de la Información se encuentra definido y adoptado institucionalmente dentro de la Política General de Seguridad de la Información. Es importante precisar que este apartado describe el alcance del sistema, no el de la política. Si se requiere mayor explicitud, podemos ajustarlo, pero solicitamos que este punto se trate como observación, toda vez que el alcance existe".*

Respuesta al comentario por parte de la OCI: El lineamiento correspondiente a la Definición del Alcance del MSPI establece expresamente que la entidad debe:

> *"Determinar con claridad los límites, el alcance y la aplicabilidad del MSPI en el marco del modelo de operación por procesos de la entidad, especificando a qué procesos, recursos humanos, financieros, técnicos y tecnológicos se aplicará la implementación del modelo."*

Asimismo, el propósito del lineamiento señala que se debe:

> *"Identificar qué activos de información, software, hardware, roles, sistemas de información y áreas seguras (…) serán protegidos mediante la adopción del MSPI."*

Estas exigencias corresponden a una salida específica del lineamiento, la cual debe estar documentada y ser verificable como producto independiente, tal como se establece en la estructura del propio modelo. Adicionalmente, el lineamiento 7.2.2 – Política de seguridad y privacidad de la información señala que la definición del alcance del MSPI constituye una entrada para la formulación de la política. Esto implica necesariamente que:

- el alcance debe existir previamente,
- debe estar documentado,
- y no puede estar contenido dentro de la política, puesto que la política se construye con base en dicho alcance.

En ese sentido, la "Política General de Seguridad de la Información 2025" aporta una descripción general del alcance de la política, pero no desarrolla los elementos exigidos para la definición del alcance del MSPI, tales como procesos cubiertos, recursos aplicables, activos de información, sistemas de información, roles asociados o áreas seguras. Por lo anterior, se mantiene el Hallazgo.

4.1.2.4. Liderazgo y Compromiso

Lineamiento	Propósito	Salida
Las entidades deben asignar, mediante acto administrativo, al comité institucional de gestión y desempeño (o su equivalente) las funciones relacionadas con la seguridad y privacidad de la información, asegurando la adopción, implementación y mejora continua del MSPI. En este comité debe incluirse como miembro permanente al responsable de seguridad de la información, con el fin de garantizar su implementación efectiva y el cumplimiento de acciones claves como: • Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.	Garantizar el liderazgo y el compromiso del comité institucional de gestión y desempeño o quien haga sus veces para conseguir los objetivos definidos para la implementación del MSPI.	Evidencia en el acto administrativo que soporta la conformación del comité de gestión y desempeño o quien haga sus veces, señalando las funciones de seguridad y privacidad de la información.

• Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad. • Comunicar en la entidad la importancia del MSPI. • Planear y disponer de los recursos necesarios (presupuesto, personal, tiempo etc.) para la adopción del MSPI. • Asegurar que el MSPI consiga los resultados previstos. • Realizar revisiones periódicas de la adopción del MSPI (al menos dos veces por año y en las que el Nominador deberá estar presente).		

Durante la revisión del documento “5. Resolución No. 093 de 2018 Comité Institucional de Gestión y Desempeño”, remitido como soporte del lineamiento de Liderazgo y Compromiso, se verificó que el proceso cuenta con un acto administrativo vigente que formaliza la creación y funciones generales del comité, lo cual constituye un insumo base para la estructura de gobernanza requerida por el MSPI.

No obstante, el análisis permitió identificar que dicho acto no incorpora las funciones específicas ni la composición exigida para el liderazgo del MSPI, lo cual se detalla en el siguiente hallazgo:

HALLAZGO 5. Ausencia de asignación explícita de funciones del MSPI y de inclusión del responsable de seguridad en el Comité Institucional de Gestión y Desempeño: Al revisar el documento “Resolución No. 093 de 2018 - Comité Institucional de Gestión y Desempeño”, remitido por el proceso como evidencia del cumplimiento del lineamiento 7.2.1. Liderazgo y Compromiso, se evidenció que este acto administrativo no asigna las funciones específicas relacionadas con la seguridad y privacidad de la información requeridas por el lineamiento, ni incluye como miembro permanente al responsable de seguridad de la información, tal como lo establece el Modelo de Seguridad y Privacidad de la Información – MSPI.

El lineamiento dispone que las entidades deben asignar mediante acto administrativo al Comité Institucional de Gestión y Desempeño las funciones relacionadas con la seguridad y privacidad de la información, incluyendo acciones como: establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad; garantizar la adopción de los requisitos del MSPI; comunicar su importancia; planear y disponer recursos; asegurar los resultados previstos y realizar revisiones periódicas de adopción del modelo al menos dos veces por año con presencia del nominador. Adicionalmente, el lineamiento establece que el responsable de seguridad de la información debe ser miembro permanente del comité.

La Resolución No. 093 de 2018 únicamente incluye en el artículo 3, literal 6, la función de “asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia

de seguridad digital y de la información", pero no asigna ninguna de las funciones específicas establecidas para el MSPI. Asimismo, en la conformación del comité, el responsable de seguridad de la información no figura como integrante, incumpliendo el requisito explícito del lineamiento.

Recomendación: Expedir un acto administrativo actualizado que incluya explícitamente todas las funciones relacionadas con la adopción, implementación y mejora continua del MSPI, conforme al lineamiento 7.2.1., incorporando acciones como establecer y publicar políticas de seguridad y privacidad, garantizar el cumplimiento de los requisitos del MSPI, comunicar su importancia, planear y disponer recursos, asegurar los resultados previstos y realizar revisiones periódicas del modelo. Este acto deberá incluir como miembro permanente al responsable de seguridad de la información y referenciar de manera explícita el MSPI, garantizando su articulación institucional.

Con respecto al hallazgo mencionado, el proceso indicó en la **respuesta al Informe Preliminar** que: *Las funciones del Comité Institucional relacionadas con seguridad de la información están documentadas en la Política General de Seguridad de la Información, aprobada por el propio Comité. Allí se incluyen las responsabilidades asociadas al SGSI y su seguimiento. Por lo anterior, solicitamos que este punto sea tratado como observación documental.*

Respuesta OCI sobre el comentario del proceso: El lineamiento exige expresamente que las funciones del MSPI sean asignadas mediante acto administrativo al Comité Institucional de Gestión y Desempeño (CIGD), señalando de forma textual que el Comité debe asumir, entre otras, las siguientes responsabilidades:

- Establecer y publicar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Garantizar la adopción de los requisitos del MSPI en los procesos de la entidad.
- Comunicar la importancia del MSPI.
- Planear y disponer recursos (presupuesto, personal y tiempo) para su adopción.
- Asegurar que el modelo logre los resultados previstos.
- Realizar revisiones periódicas de adopción del MSPI al menos dos veces al año, con presencia del nominador.
- Incluir como miembro permanente al responsable de seguridad de la información.

Estos elementos son obligatorios y deben quedar asignados de forma explícita y formal en un acto administrativo vigente. Al revisar la Resolución 093 de 2018, evidenciada por el proceso como prueba de cumplimiento, se observa que:

- Únicamente incorpora en el artículo 3, literal 6, la función genérica de "*asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información";*
- No incluye ninguna de las funciones específicas exigidas por el lineamiento 7.2.1 del MSPI;
- No incorpora al responsable de seguridad de la información como miembro permanente del CIGD.

Adicionalmente se aclara que:

- La Política General no sustituye ni cumple el requisito del lineamiento, ya que el Modelo exige que las funciones del MSPI estén asignadas en acto administrativo, no en una política.
- Las responsabilidades del Comité no pueden derivarse de un documento que el mismo Comité aprueba, sino que deben ser establecidas por un acto formal que defina sus competencias en materia de seguridad y privacidad de la información.
- La inclusión del responsable de seguridad de la información como miembro permanente tampoco puede derivarse de una política, sino que requiere formalización en acto administrativo, conforme lo exige el lineamiento.
  Por lo anterior, se mantiene el Hallazgo.

4.1.2.5. Política de seguridad y privacidad de la información

Lineamiento	Propósito	Salida
Se debe establecer en la política de seguridad y privacidad de la información los lineamientos y compromisos que se adoptaran para asegurar la confidencialidad, integridad y disponibilidad de la información, para ello debe tener en cuenta: • Misión de la entidad. • Normatividad vigente la cual se debe contar para el funcionamiento de la entidad. • Establecer compromiso del cumplimiento de los requisitos relacionados con la seguridad y privacidad de la información, así como también el de la mejora continua que permita la reevaluación y actualización periódica de las medidas de seguridad para adaptarlas a la constante evolución de los riesgos y sistemas de protección. El personal calificado de la entidad supervisará, revisará y auditará la seguridad de la información. una vez el MSPI sea adoptado. • Estar alineada con el contexto de la entidad, así como la identificación de las áreas que hacen parte de la implementación de seguridad de la información.	La política establece la base respecto al comportamiento personal y profesional de los funcionarios, contratistas o terceros sobre la información obtenida, generada o procesada por la entidad. Orientar y apoyar por parte de la alta dirección de la entidad a través del comité de gestión institucional, la gestión de la seguridad de la información de acuerdo con la misión de la entidad, normatividad y reglamentación pertinente	Acto administrativo o acta de aprobación del Comité Institucional de Gestión y Desempeño con la adopción de la Política de seguridad y privacidad de la información

Lineamiento	Propósito	Salida
• Se deben asignar los roles y responsabilidades que se identifiquen. • Ser incluidos y aprobados los temas de seguridad de la información y seguridad digital en el comité gestión y desempeño institucional. Ser comunicada al interior de la entidad y a los interesados que aplique.		

Se indicó por parte del GT Gestión de Plataforma de Tecnologías de Información frente al requerimiento de “Acto administrativo con la adopción de la Política de seguridad y privacidad de la información” que “La política de seguridad de la información publicada se encuentra firmada”.
De la revisión a la Política General de Seguridad de la Información 2025, se evidenció que el documento cumple con los requisitos establecidos en el lineamiento 7.2.2. del Modelo de Seguridad y Privacidad de la Información – MSPI. La política desarrolla los lineamientos y compromisos orientados a asegurar la confidencialidad, integridad y disponibilidad de la información; incorpora la misión institucional y la normatividad vigente aplicable; define compromisos relacionados con el cumplimiento de los requisitos de seguridad y privacidad de la información, así como con la mejora continua; y establece roles y responsabilidades asociados a la gestión de la seguridad de la información. Adicionalmente, en la sección de Alcance se identifica que la política aplica a todas las dependencias del SGC involucradas en el tratamiento, uso y protección de la información digital. Finalmente, en la parte final del documento se evidencia su aprobación por parte del Comité Institucional de Gestión y Desempeño y la firma de la Alta Dirección, lo cual satisface la salida definida para este lineamiento.

4.1.2.6. Roles y responsabilidades

Lineamiento	Propósito	Salidas
Articular roles y responsabilidades con las áreas de la entidad para la adopción del MSPI, asegurando el monitoreo, reporte y aprobación ante el comité institucional. Los líderes de proceso deberán gestionar los riesgos de seguridad y privacidad de la información. Designar un responsable del MSPI con un equipo de apoyo, dependiente de un área estratégica distinta a la de Tecnología. Si no existe el cargo, deberá delegarse por acto administrativo e integrarse con voz y voto al comité de gestión institucional de	Es fundamental que los funcionarios y contratistas conozcan sus responsabilidades, comprendan el impacto de sus acciones en la seguridad de la información y entiendan cómo contribuyen a la implementación efectiva del MSPI.	Roles y responsabilidades en seguridad de la información de las diferentes áreas o procesos de la entidad. Definición del rol de: responsable de seguridad de la información, indicando sus

Lineamiento	Propósito	Salidas
gestión y desempeño y con voz al comité de control interno. Si no hay personal de planta, varias entidades podrán compartir un responsable de seguridad mediante contrato de servicios, justificando la falta de recursos, conforme al artículo 5 de la Resolución 500 sobre Estrategia de Seguridad Digital.		funciones y responsabilidades

Durante la revisión del archivo "*7. Matriz Roles Responsabilidades v2.0.xlsx*", remitido como soporte del lineamiento de Roles y Responsabilidades, se verificó que el proceso cuenta con una matriz estructurada que asigna funciones relacionadas con la operación y administración de servicios tecnológicos, e incluye una descripción general del rol del oficial de seguridad digital. Este insumo evidencia un avance inicial en la formalización de responsabilidades asociadas a la seguridad de la información.

No obstante, el análisis permitió identificar que la matriz no incorpora algunos roles requeridos para la implementación del MSPI ni desarrolla la articulación con todas las áreas misionales, de apoyo y estratégicas, lo cual se detalla en la siguiente observación**:**

OBSERVACIÓN 2. Incompletitud en la definición institucional de roles y responsabilidades para la implementación del MSPI
Al revisar el archivo "7.Matriz Roles Responsabilidades v2.0", se evidenció que, si bien el documento asigna roles y responsabilidades asociados a la prestación y administración de servicios tecnológicos (como Internet, redes LAN/WAN, VPN, correo electrónico, plataformas de almacenamiento, sistemas Geocientíficos, servidores virtuales y sistemas de videoconferencia), y describe de manera general el rol del oficial de seguridad digital, dicha matriz no desarrolla de forma completa el lineamiento 7.2.3. Roles y responsabilidades requeridos para la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI.

El lineamiento establece que las entidades deben articular roles y responsabilidades con todas las áreas de la entidad, designar un responsable del MSPI dependiente de un área estratégica distinta a Tecnología, asegurar el monitoreo, reporte y aprobación ante el comité institucional, e incluir funciones para la gestión de riesgos por parte de los líderes de proceso. Sin embargo, la matriz revisada se encuentra orientada principalmente a la operación y soporte de servicios de TI, sin incluir la participación de líderes de proceso misionales, de apoyo y estratégicos, ni reflejar las responsabilidades institucionales asociadas a la adopción, implementación y seguimiento del MSPI.

Recomendación: Ajustar y complementar la matriz institucional de roles y responsabilidades, de manera que:

- Incluya a todas las áreas y procesos de la entidad, estableciendo claramente sus responsabilidades frente a la implementación, gestión y seguimiento del MSPI.

- Identifique y documente formalmente al responsable del MSPI, sus funciones y su dependencia jerárquica conforme al lineamiento (área estratégica distinta a Tecnología).
- Integre explícitamente las responsabilidades de monitoreo, reporte y aprobación ante el Comité Institucional de Gestión y Desempeño.
- Asigne responsabilidades claras a los líderes de proceso respecto a la gestión de riesgos de seguridad y privacidad de la información.

4.1.2.7. Identificación de activos de información e infraestructura critica cibernética

Lineamiento	Propósito	Salidas
Las entidades deben definir y aplicar un proceso de identificación y clasificación de los activos de información, que permita: • Identificar los activos de información que agregan valor al proceso y requieren protección, según el alcance y los procesos cubiertos por el MSPI. • Clasificar los activos de información de acuerdo con los tres principios de seguridad de la información: Integridad, confidencialidad y disponibilidad para garantizar que la información recibe los niveles de protección adecuados. • Actualizar el inventario y la clasificación de los activos por los propietarios y custodios de los activos de forma periódica o toda vez que exista un cambio en el proceso. • Identificar los activos de información con información personal en el inventario de activos de información. • Realizar la identificación y el inventario de infraestructura crítica y servicios esenciales de la entidad.	Estructurar una metodología que permita identificar y clasificar los activos de información	Procedimiento de inventario y clasificación de activos de información2, del Modelo de Información. Documento metodológico de inventario y clasificación de la información. Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados.

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información los archivos denominados “9.FGGCAMR003formatoInvActivos.xlsx”, “2025_Activos_Inf_GT Plataforma TI.xlsx”, “*2025_Activos_Inf_Reformulado_Bucaramanga.xlsx*” y

"2025_Activos_Inf_Reformulado_Divulgación y Sistemas de Información.xlsx". Adicionalmente, se informó como Procedimiento de inventario y clasificación de la información lo correspondiente a "PR-GGC-003-Identificación, Clasificación y Etiquetado de Activos de Información Digitales". Una vez revisados los respectivos archivos se identificó lo siguiente:

Del análisis del procedimiento PR-GGC-003 y de los inventarios de activos de información remitidos, se evidenció que la entidad cuenta con una metodología formal, plantillas institucionales unificadas y registros correspondientes a la vigencia 2025, en los cuales se identifican y clasifican activos, se documentan propietarios y custodios, se gestionan categorías de datos personales y se incluye la variable de infraestructura crítica cibernética.

Estos avances reflejan que el SGC ha venido implementando de manera estructurada el proceso de identificación y clasificación de activos, en concordancia con el lineamiento del MSPI. No obstante, se identifica como oportunidad de mejora la consolidación de un inventario institucional que permita verificar de manera integral la cobertura total de los procesos incluidos en el alcance del MSPI.

Recomendación: Continuar fortaleciendo la aplicación homogénea de la metodología en todas las dependencias, consolidando un inventario institucional y armonizando los criterios de clasificación de datos personales e infraestructura crítica cibernética, con el fin de robustecer la gestión integral de los activos de información en el marco del MSPI.

4.1.2.8. Valoración de los riesgos de seguridad de la información

Lineamiento	Propósito	Salidas
Las entidades deben definir y aplicar un proceso de valoración de riesgos de la seguridad y privacidad de la información, que permita: • Identificar los riesgos que causen la pérdida de confidencialidad, integridad, disponibilidad, privacidad de la información, así como la continuidad de la operación de la entidad dentro del alcance del MSPI. • Identificar los propietarios de los riesgos. • Definir criterios para valorar las consecuencias de la materialización de los riesgos, y la probabilidad de su ocurrencia. • Determinar el apetito de riesgos definido por la entidad. • Establecer criterios de aceptación de los riesgos. • Valorar los riesgos que afecten la confidencialidad, integridad y disponibilidad de la información dentro del alcance del MSPI. • Determinar los niveles de riesgo.	Estructurar una metodología que permita identificar y clasificar los activos de información	Procedimiento y metodología de gestión de riesgos institucional incluyendo el capítulo de seguridad y privacidad de la información aprobado por el comité institucional de gestión y desempeño. Instrumento para la identificación y valoración de los riesgos de seguridad y

Lineamiento	Propósito	Salidas
• Realizar la comparación entre los resultados del análisis y los criterios de los riesgos establecidos en este mismo numeral. • Priorización de los riesgos analizados para su tratamiento. • Se debe asegurar que las valoraciones repetidas de los riesgos de seguridad y privacidad de la información produzcan resultados consistentes, válidos y comparables. • Se recomienda realizar una evaluación de riesgos específica frente a amenazas avanzadas persistentes (APT) y vulnerabilidades emergentes, con el fin de ajustar las estrategias de seguridad a los ataques de alta sofisticación. • Se deben considerar los nuevos riesgos asociados a los dominios incluidos en la ISO/IEC 27001:2022, tales como amenazas avanzadas, entornos de nube, y riesgos en la cadena de suministro digital.		privacidad de la información.

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información los archivos denominados “11.MNPSG004Manualparalagestionderiesgos SGCv5.pdf” y “12.MR Seguridad de la Información.xlsx”. Una vez revisados los respectivos archivos se identificó lo siguiente:

En relación con el lineamiento 7.3.2. Valoración de los riesgos de seguridad de la información, se evidencia que se cumple con las disposiciones establecidas en el Documento Maestro del MSPI, al contar con una metodología institucional formalizada en el Manual MN-PSG-004 y con un instrumento específico para la identificación, valoración y tratamiento de riesgos de seguridad y privacidad de la información (matriz “MR Seguridad de la Información”). Dicho instrumento permite identificar activos, amenazas, vulnerabilidades y propietarios del riesgo, así como realizar valoraciones inherentes y residuales, determinar niveles de riesgo y establecer acciones de tratamiento en coherencia con los criterios y tablas adoptados por la entidad.

No obstante, se identifica un aspecto susceptible de mejora orientado a fortalecer la trazabilidad del componente de riesgos del MSPI. Si bien la matriz contempla riesgos que afectan la confidencialidad, integridad, disponibilidad y continuidad, no se distingue de manera explícita cuando un riesgo corresponde a la privacidad de la información, obligación expresamente señalada en el Lineamiento 7.3.2 y desarrollada en el Anexo del Modelo Nacional de Gestión de Riesgos de Seguridad de la Información.

Recomendación: Incorporar un campo o indicador que permita identificar y monitorear los riesgos asociados al tratamiento de datos personales, en concordancia con la Ley 1581 de 2012 y las disposiciones del MSPI.

4.1.2.9. Plan de tratamiento de los riesgos de seguridad de la información

Lineamiento	Propósito	Salidas
Las entidades deben definir y aplicar un proceso de tratamiento de riesgos de la seguridad de la información, que permita: • Seleccionar las opciones (controles) pertinentes y apropiadas para el tratamiento de riesgos. • Elaborar una declaración de aplicabilidad que contenga: los controles adoptados por la entidad, su estado de implementación y la justificación de posible exclusión de acuerdo con los riesgos identificados y las capacidades técnicas y humanas con las que cuenta. • Definir un plan de tratamiento de riesgos que contenga, fechas, acciones de tratamientos de riesgos a tratar y responsables con el objetivo de realizar trazabilidad. • Los dueños de los riesgos que deben ser los dueños de los procesos afectados por estos riesgos, o las personas designadas por ellos. Deben realizar la aprobación formal del plan de tratamiento de riesgos y la aprobación debe llevarse a la revisión por dirección en el Comité Institucional y de Desempeño, o quien haga sus veces.	Estructurar una metodología que permita definir las acciones que debe seguir la entidad para poder gestionar los riesgos de seguridad y privacidad de la información	Plan de tratamiento de riesgos, aprobado por los dueños de los riesgos y el comité institucional de gestión y desempeño (Decreto 612 de 2018 Publicación antes de 31 de enero de cada vigencia). La aceptación de los riesgos residuales e indicación en que parte se deben aceptar. Declaración de aplicabilidad, aceptada y aprobadas en el comité institucional de gestión y desempeño.

Durante la revisión de los documentos "*15. Declaración de Aplicabilidad SGC V.1.0.pdf*" y "*Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2025*", remitidos como soporte del lineamiento de tratamiento de riesgos, se verificó que el proceso cuenta con instrumentos elaborados para documentar los controles adoptados y las acciones de tratamiento. Esto evidencia un avance en la gestión institucional del riesgo de seguridad de la información y en la estructuración de insumos necesarios para el MSPI.

No obstante, en la verificación realizada se identificaron brechas frente a los requisitos establecidos en el Documento Maestro MSPI 2025, en lo relacionado con la actualización

normativa y la aprobación institucional exigida para la Declaración de Aplicabilidad, lo cual se detalla a continuación en el hallazgo:

HALLAZGO 6. Declaración de Aplicabilidad no actualizada ni aprobada por el CIGD. De acuerdo con el Lineamiento 7.3.3. Plan de tratamiento de los riesgos de seguridad de la información del Documento Maestro del MSPI (Resolución 2277 de 2025), las entidades deben elaborar y mantener una Declaración de Aplicabilidad (DoA) que incluya los controles adoptados, su estado de implementación y la justificación de las exclusiones. Esta DoA debe encontrarse alineada con los controles establecidos en la versión vigente de la norma ISO/IEC 27001:2022 y contar con la aprobación formal del Comité Institucional de Gestión y Desempeño (CIGD), conforme a lo señalado en las salidas requeridas del lineamiento.

Durante la revisión de la evidencia suministrada por el Grupo de Trabajo Gestión de Plataformas de Tecnologías de la Información, se observó que el documento *"15.Declaración de Aplicabilidad SGC V.1.0.pdf"* se encuentra elaborado con base en la versión ISO/IEC 27001:2013, la cual fue sustituida normativamente por la versión ISO/IEC 27001:2022, que reorganiza y actualiza los controles de seguridad en cuatro dominios e introduce controles adicionales como inteligencia de amenazas, seguridad en la nube, seguimiento continuo, configuración segura, entre otros. Asimismo, en el documento remitido no se evidencia aprobación formal del CIGD, en forma de acta, constancia, firma, radicado o referencia institucional que indique su adopción en dicho comité, tal como lo exige el lineamiento para efectos de formalización y trazabilidad del MSPI.

La ausencia de actualización a la versión vigente de la norma, así como la falta de evidencia de aprobación por parte del CIGD, puede generar brechas en la implementación del MSPI, al no garantizar que los controles seleccionados correspondan a los requisitos actuales de seguridad de la información y a que el instrumento cuente con el respaldo institucional requerido para su aplicación y seguimiento.

Recomendación: Se recomienda actualizar la Declaración de Aplicabilidad conforme a los controles establecidos en la ISO/IEC 27001:2022, incorporando el estado de implementación y la justificación de exclusiones de acuerdo con los riesgos identificados, y posteriormente gestionar su aprobación formal ante el Comité Institucional de Gestión y Desempeño (CIGD). Esta aprobación debe quedar documentada mediante acta, radicado o constancia oficial, con el fin de garantizar la trazabilidad, validez y alineación del plan de tratamiento del MSPI con la normativa vigente.

Con respecto al hallazgo mencionado, el proceso indicó en la **respuesta al Informe Preliminar *que:*** *La Declaración de Aplicabilidad basada en la ISO/IEC 27001:2022 se encuentra en construcción. Ya se cuenta con el formato conforme a la versión vigente de la norma; actualmente se está adelantando el mapeo detallado de los controles frente a su implementación en el SGC. Dado que la adopción normativa de la Resolución 2277 de 2025 es reciente, solicitamos que el tema sea tratado como observación, toda vez que el proceso ya fue iniciado y se encuentra avanzando.*

Respuesta al comentario por parte de la OCI: Se precisa que la elaboración de una Declaración de Aplicabilidad (DoA) basada en la ISO/IEC 27001:2022 constituye una salida obligatoria del lineamiento 7.3.3 del MSPI y no un ajuste documental en curso. La evidencia remitida corresponde a una DoA elaborada bajo la versión ISO/IEC 27001:2013, cuya vigencia internacional finalizó en octubre de 2025, de acuerdo con el período de transición definido por ISO para la adopción de la versión 27001:2022. Por tanto, la actualización del instrumento no es opcional ni puede considerarse como un proceso *"en avance"*, sino un requisito formal del modelo que debe encontrarse vigente. Por lo anterior, se mantiene el hallazgo.

4.1.2.10. Recursos

Lineamiento	Propósito	Salidas
Las entidades deben asegurar los recursos financieros, humanos y técnicos necesarios para adoptar, implementar y mantener el MSPI como un proceso transversal conforme al alcance definido.	Determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del MSPI.	Incluir dentro de los proyectos de inversión de la entidad aquellas actividades relacionadas con la adopción de MSPI de acuerdo con el alcance establecido (esto involucra también al personal de seguridad de la información a contratar para el desarrollo de las actividades del SGSI). Actualización del PETI de acuerdo con los recursos necesarios para realizar la gestión adecuada de los riesgos de seguridad de la información identificados y el plan de seguridad y privacidad de la información.

Durante la revisión del MGA "Fortalecimiento TIC SGC 26 Abr 2024" y del PETI 2023 - 2026, remitidos como soporte del lineamiento de Recursos, se verificó que la entidad cuenta con instrumentos de planeación institucional formalizados y en ejecución, los cuales incluyen iniciativas orientadas al fortalecimiento tecnológico.

No obstante, la verificación realizada permitió identificar que dichos instrumentos no incorporan de manera explícita los requerimientos, recursos ni actividades vinculadas a la implementación integral del MSPI. En consecuencia, se establece la siguiente observación:

OBSERVACIÓN 3. Oportunidades de mejora en la incorporación de los requerimientos del MSPI en la planeación institucional de recursos tecnológicos, humanos y financieros. El Lineamiento 7.4.1 – Recursos del Modelo de Seguridad y Privacidad de la Información (MSPI), previsto en la Resolución 2277 de 2025, establece

que las entidades deben garantizar los recursos financieros, humanos y técnicos necesarios para la adopción, implementación, mantenimiento y mejora continua del MSPI, como un proceso transversal.
Para ello, el lineamiento establece como salidas obligatorias:

- Incluir dentro de los proyectos de inversión las actividades relacionadas con la adopción del MSPI, incluyendo los recursos humanos asociados (como personal de seguridad de la información).
- Actualizar el Plan Estratégico de Tecnologías de la Información – PETI de acuerdo con los recursos necesarios para la gestión adecuada de los riesgos de seguridad de la información identificados, y para la ejecución del Plan de Seguridad y Privacidad de la Información.

Durante la revisión del MGA “Fortalecimiento TIC SGC 26 Abr 2024”, se evidenció que el proyecto de inversión 2199067 – Servicios tecnológicos incluye actividades orientadas al fortalecimiento de la infraestructura de seguridad informática, tales como la actualización de la seguridad perimetral, NAC, EndPoint Trellix, seguridad de aplicaciones y vulnerabilidades (SIEM), seguridad del dato (WAF, DAM, FAM), gestión de identidad y prevención de fuga de información (DLP). Estas iniciativas se encuentran alineadas con las capacidades técnicas requeridas para la implementación del MSPI y contribuyen al cumplimiento del Lineamiento 7.4.1.

No obstante, aunque las actividades del proyecto son coherentes con las necesidades del MSPI, aún se identifica oportunidad de mejora para fortalecer la trazabilidad explícita entre dichas inversiones, los riesgos priorizados del MSPI, el Plan de Seguridad y Privacidad de la Información y la programación contenida en el PETI.

Recomendación: Ajustar la documentación estratégica para reflejar de manera diferenciada y verificable:

- la relación entre los riesgos priorizados del MSPI y las inversiones en seguridad,
- los recursos humanos asociados (como el responsable de seguridad de la información),
- y la alineación directa de estas iniciativas con el PETI y el Plan de Seguridad y Privacidad de la Información.

4.1.2.11. Competencia, toma de conciencia y comunicación

Lineamiento	Propósito	Salidas
Las entidades deben definir un plan de comunicación, capacitación, sensibilización y concientización para: • Asegurar que las personas cuenten con los conocimientos, educación y formación o experiencia adecuada para la implementación y gestión del modelo de seguridad y privacidad de la información.	Garantizar una correcta comunicación, sensibilización y concientización con respecto a la seguridad y privacidad de la información, en la que todos los funcionarios conozcan la política, su rol en el MSPI y las implicaciones de no aplicar las reglas de seguridad y privacidad.	Plan de cambio, cultura, apropiación, capacitación y sensibilización de Seguridad y Privacidad de la Información y seguridad digital. Este se puede incluir en el Plan Institucional de Capacitaciones - PIC.

Lineamiento	Propósito	Salidas
• Involucrar al 100% de los colaboradores de la entidad en la implementación y gestión del MSPI. • Concientizar a los colaboradores y partes interesadas en la importancia de la protección de la información. • Identificar las necesidades de comunicaciones internas y externas relacionadas con la seguridad y privacidad de la información. Se deberá definir qué será comunicado, cuándo, a quién, quién debe comunicar y finalmente definir los procesos para lograrlo. • Tener un enfoque práctico en la respuesta a incidentes, especialmente en técnicas de phishing, ingeniería social y ciberhigiene, para fortalecer la capacidad de respuesta ante ataques dirigidos. • Cuando proceda, tomar las acciones para adquirir y/o fortalecer la competencia de los responsables del MSPI. • Evaluar la eficacia de las acciones de concientización y sensibilización realizadas.		Plan de comunicaciones del modelo de seguridad y privacidad de la información

Durante la revisión del “Programa de Sensibilización en Seguridad de la Información 2025” y del “Plan de Comunicaciones del Modelo de Seguridad y Privacidad de la Información - SGC”, remitidos como soporte del lineamiento de competencia, toma de conciencia y comunicación, se verificó que la entidad cuenta con documentos que incluyen acciones de sensibilización y actividades generales de comunicación en materia de seguridad de la información; sin embargo, el análisis permitió identificar que dichos documentos no desarrollan de manera integral los componentes requeridos por el lineamiento ni se encuentran formalizados, situación que se detalla en el siguiente hallazgo:

HALLAZGO 7. Insuficiencia en la formalización y alineación del plan de comunicación, capacitación y sensibilización del MSPI. El Lineamiento 7.4.2 del MSPI exige que la entidad cuente con un plan formal de comunicación, capacitación, sensibilización y concientización que involucre al 100 % de los colaboradores, fortalezca las competencias del responsable del MSPI, incorpore prácticas de respuesta a incidentes (phishing, ingeniería social), identifique necesidades de comunicación internas y externas, y establezca mecanismos para evaluar la eficacia de las acciones. La evidencia

entregada correspondiente a Programa de Sensibilización en Seguridad de la Información 2025 y Plan de Comunicaciones del MSPI–SGC, si bien abordan actividades de sensibilización y comunicaciones, no cumplen de manera integral con lo requerido por el lineamiento, debido a que:

- No incorpora un plan estructurado de capacitación ni fortalecimiento de competencias del responsable del MSPI.
- No define mecanismos formales de evaluación de eficacia.
- No desarrolla necesidades de comunicación específicas del MSPI ni actividades prácticas de respuesta a incidentes.
- No está formalizada como documentación institucional (sin control de cambios, aprobación, revisión ni adopción).

Recomendación: formalizar y reestructurar el Programa de Sensibilización y el Plan de Comunicaciones para alinearlos al Lineamiento 7.4.2, incorporando:

- Un plan de capacitación completo, incluyendo competencias del responsable del MSPI y ejercicios prácticos (phishing, ingeniería social, ciberhigiene).
- Identificación de necesidades de comunicación del MSPI y definición de qué se comunica, cuándo, cómo y a quién.
- Mecanismos e indicadores de evaluación de eficacia.
- Aprobación (firmas), control de cambios y estructura formal del del documento.

Con respecto al hallazgo mencionado, el proceso indicó en la **respuesta al Informe Preliminar** que: **"***El Plan de Sensibilización en Seguridad de la Información existe y se ejecuta. Respecto al componente de capacitación, es importante precisar que la formulación, programación, ejecución y reporte del Plan Institucional de Capacitación (PIC) es responsabilidad del Equipo de Talento Humano, conforme a la normativa vigente. En ese sentido, solicitamos que la verificación de evidencias frente al PIC sea remitida directamente a dicha dependencia. En caso de que no se hayan ejecutado actividades específicas de seguridad de la información durante 2025, sugerimos que este aspecto sea articulado con Talento Humano para su incorporación en el PIC 2026. Por lo anterior, este punto debe ser tratado como observación, dado que la responsabilidad institucional no recae en el proceso líder del MSPI".*

Respuesta al comentario por parte de la OCI: El Lineamiento 7.4.2 del MSPI asigna a la entidad la responsabilidad institucional de contar con un plan formal de comunicación, capacitación, sensibilización y concientización del MSPI, el cual debe incluir el fortalecimiento de competencias del responsable del modelo, actividades prácticas de respuesta a incidentes, identificación de necesidades de comunicación y mecanismos de evaluación de eficacia. Si bien la administración del PIC recae en Talento Humano, el lineamiento exige que el plan del MSPI identifique, documente y articule dichas necesidades, de modo que luego puedan ser gestionadas para su incorporación formal. Esta articulación es un componente esencial del cumplimiento del lineamiento, así como la formalización documental (control de cambios, versión, aprobación). En este sentido, el hallazgo se mantiene, pero se reconoce la importancia de trabajar conjuntamente con Talento Humano para incorporar en el PIC 2026, los componentes de capacitación, sensibilización y fortalecimiento del MSPI conforme a lo requerido por el modelo.

4.1.3. Fase 2: Operación

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:

- Actualización del inventario de información.
- Actualización de la matriz de riesgos de seguridad de la información.
- Plan de implementación de controles de seguridad.
- Actualización de la gestión de eventos e incidentes de seguridad de la información.
- Actualización de la gestión de vulnerabilidades.
- Evidencia de la implementación de los controles de seguridad de la información.

4.1.3.1. Control y planeación operacional

Lineamiento	Propósito	Salidas
Las entidades deben realizar la planificación e implementación de las acciones determinadas en el plan de tratamiento de riesgos y el plan de Seguridad y Privacidad de la Información, esta información debe estar documentada para cada proceso según lo planificado, los planes de tratamiento deben ser definidos y aprobados por los líderes de proceso, Los proyectos o controles de seguridad que no pueden implementarse en el corto plazo o mediano plazo se deben escalar al comité institucional de gestión y desempeño para toma de decisiones y asignación de recursos. Las acciones que la entidad considere relevantes deben ser aprobadas por el comité institucional de gestión y desempeño. De igual manera, deben reforzar los mecanismos de monitoreo continuo, incluyendo la implementación de sistemas de alerta temprana que permitan a las entidades detectar y responder a incidentes en tiempo real,	Implementar los planes y controles para lograr los objetivos del MSPI	Plan de seguridad y privacidad de la información que defina la implementación de controles de seguridad y privacidad de la información y contenga como mínimo: controles, actividades, fechas, responsable de implementación y presupuesto. Evidencia de la implementación de los controles de seguridad y privacidad de la información.

Lineamiento	Propósito	Salidas
garantizando la resiliencia frente a ciberataques.		

Durante la revisión del documento “19.Plan Implementación Controles_SGC_2025.pdf” y de la carpeta con evidencias de controles lógicos, remitidos como soporte del lineamiento de control y planeación operacional, se verificó que el proceso cuenta con un plan que incorpora actividades, responsables y fechas, así como con evidencia de la implementación de diversos controles de seguridad. No obstante, el análisis permitió identificar que el plan no presenta la formalización, trazabilidad ni articulación requeridas por el lineamiento, lo cual se describe en el siguiente hallazgo:

HALLAZGO 8: Ausencia de trazabilidad, formalización y articulación del plan de implementación de controles del MSPI. El Lineamiento 8.1 del MSPI establece que las entidades deben planificar y ejecutar las acciones definidas en el plan de tratamiento de riesgos y en el plan de seguridad y privacidad, y que estos planes deben estar documentados para cada proceso, aprobados por los líderes de proceso, y cuando corresponda deben ser elevados al Comité Institucional de Gestión y Desempeño (CIGD) para toma de decisiones y asignación de recursos. Asimismo, la planeación debe garantizar trazabilidad entre los controles implementados, los riesgos priorizados del MSPI y el Plan de Seguridad y Privacidad de la Información. El documento “Plan de Implementación de Controles SGC 2025” (19.Plan Implementación Controles_SGC_2025.pdf) contiene actividades, fechas y responsables; sin embargo, no evidencia:

- aprobación por parte de los líderes de proceso,
- aprobación o elevación al CIGD,
- trazabilidad entre los controles y los riesgos del Plan de Tratamiento del MSPI,
- identificación de controles no implementables a ser escalados al CIGD,

En cuanto a la evidencia de implementación de controles, se aportó evidencia que demuestra la implementación efectiva de controles de seguridad y aunque cumple, se recomienda relacionar cada evidencia con el control del plan, para mejorar la trazabilidad y facilitar auditorías futuras.

Recomendación

- Formalizar y aprobar el Plan de Implementación de Controles mediante validación de los líderes de proceso y elevación al CIGD, conforme al Lineamiento 8.1.
- Establecer trazabilidad explícita entre cada control y los riesgos priorizados del MSPI, incluyendo su correspondencia con el Plan de Seguridad y Privacidad de la Información.
- Identificar y documentar los controles que no puedan implementarse en el corto o mediano plazo y escalarlos al CIGD para su priorización y asignación de recursos.
- Aprobación (firmas), control de cambios y estructura formal del del documento.

4.1.3.2. Plan de tratamiento de riesgos

Lineamiento	Propósito	Salidas
La entidad debe realizar evaluaciones de riesgos de seguridad de la información a intervalos planificados o cuando se propongan u ocurran cambios significativos. La entidad debe conservar información documentada de los resultados de las evaluaciones de riesgos de seguridad de la información. La entidad debe implementar el plan de tratamiento de riesgos de seguridad de la información. La entidad debe conservar información documentada de los resultados del tratamiento de riesgos de seguridad de la información.	Establecer un proceso formal de identificación, evaluación y tratamiento de los riesgos de seguridad de la información	Matriz de riesgos de seguridad de la información. Planes de tratamiento de los riesgos de seguridad e la información.

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información los archivo denominado “MR Gestión Tecnología Información Comunicaciones Seguridad.xlsx”. Una vez revisado el respectivo archivos se identificó que la entidad cumple con el Lineamiento 8.2 del Documento Maestro del MSPI, dado que cuenta con una matriz de riesgos de seguridad de la información y con planes de tratamiento incorporados dentro del mismo instrumento, en los que se identifican riesgos, controles, responsables, acciones y periodos de ejecución. La estructura de la matriz permite evidenciar la identificación, evaluación y definición de tratamiento de los riesgos, cumpliendo así con las salidas requeridas por el lineamiento (matriz de riesgos y plan de tratamiento).

No obstante, como oportunidad de mejora, se recomienda:

- Incorporar en la matriz campos de “Fecha de evaluación”, “Versión / corte” y “Periodicidad de revisión”, con el fin de evidenciar formalmente la realización de evaluaciones de riesgos a intervalos planificados, tal como lo exige el MSPI.
- Agregar columnas de “Estado del tratamiento” (no iniciado / en ejecución / cerrado) y “Resultado del tratamiento”, de manera que el instrumento permita demostrar no solo la planificación, sino también la ejecución y cierre de las acciones definidas para el tratamiento de los riesgos.

4.1.3.3. Definición de indicadores de gestión

Lineamiento	Propósito	Salida
La entidad debe definir indicadores que le permitan medir la evolución y avance en el nivel de madurez de la seguridad de la información.	Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información	Indicadores de gestión de seguridad de la información

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información el archivo denominado "*21 y 22 Ficha de Indicadores SIG SI 2025_v1.xlsx*". Una vez revisado el respectivo archivo se identificó lo siguiente:
Se cumple con el lineamiento de definición de indicadores de gestión, dado que se evidencian fichas técnicas de indicadores conforme a lo establecido en el Documento Maestro del MSPI, incluyendo fórmula, línea base, valores medidos, análisis, responsables, frecuencia y representación gráfica, de acuerdo con lo observado en el archivo "*Ficha de Indicadores SIG SI 2025_v1.pdf*"
Los indicadores permiten medir el nivel de avance del MSPI y la efectividad de acciones de sensibilización, cumpliendo con la salida requerida: indicadores de gestión de seguridad de la información.

Como oportunidad de mejora, se sugiere ampliar el conjunto de indicadores para abarcar otros componentes de la gestión del MSPI y fortalecer la medición integral del modelo.

4.1.4. Fase 3: Evaluación de desempeño

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.

4.1.4.1. Seguimiento, medición, análisis y evaluación

Lineamiento	Propósito	Salida
Las entidades deben conocer sus avances en la implementación del modelo de Gobierno Digital, estableciendo tiempos y recursos para su monitoreo y reporte ante el Comité de Gestión y Desempeño, conforme al MIPG Es importante incluir dentro del plan de auditorías los temas	Evaluar el desempeño de seguridad de la información y la eficacia del MSPI.	Hoja de vida de indicadores, los cuales deben incluirse en el tablero de control del plan de acción, tal como lo ordena el Decreto 612 de 2018. Informe con la evaluación y medición de la efectividad de la implementación de los

Lineamiento	Propósito	Salida
relacionados con seguridad digital como lo establece el MIPG. Los mecanismos utilizados para medir, analizar, monitorizar, evaluar y realizar seguimiento a la eficacia del Sistema deben ser comparables y reproducibles. Deberán incluir retroalimentación periódica que recoja la percepción de seguridad y las vulnerabilidades encontradas por los usuarios en cada entidad.		controles definidos en el plan de tratamiento de riesgos.

Durante la revisión del archivo "Ficha de Indicadores SIG SI 2025_v1.xlsx" y del documento "23.Informe_Evaluacion_Efectividad_Controles_SGC_2025.pdf", remitidos como evidencia del lineamiento de seguimiento, medición y evaluación, se verificó que el proceso cuenta con fichas de indicadores y con un informe que presenta resultados generales sobre la efectividad de los controles. Estos insumos muestran avances en la medición del desempeño del MSPI y en la evaluación de acciones implementadas; sin embargo, el análisis realizado permitió identificar que la información entregada no cumple plenamente con los requisitos de trazabilidad, formalización y reporte establecidos por el MSPI y el Decreto 612 de 2018, situación que se detalla en el siguiente hallazgo:

HALLAZGO 9: Debilidades en la trazabilidad y formalización del seguimiento e indicadores de seguridad. Durante la revisión del archivo correspondiente a la Hoja de vida de indicadores y del Informe de evaluación de la efectividad de los controles, se identificó lo siguiente:

- Aunque se entregaron fichas de indicadores en el archivo Excel, no se evidencia su incorporación en el tablero de control del Plan de Acción, como lo exige el Decreto 612 de 2018 y el lineamiento 9.1 del MSPI.
  El lineamiento establece que la hoja de vida de indicadores debe estar incluida en el tablero de control del Plan de Acción, garantizando trazabilidad, periodicidad y reporte ante el Comité de Gestión y Desempeño.
- Aunque el Informe de Evaluación de la Efectividad de los Controles sí presenta resultados globales por categorías, no se evidencia la evaluación detallada de todos los controles del plan de tratamiento de riesgos, ni muestra la validación o aprobación del Comité Institucional de Gestión y Desempeño. Adicionalmente, el documento no se encuentra aprobado ni firmado, lo que resta validez formal al reporte.

Recomendación: Incorporar formalmente los indicadores en el tablero de control del Plan de Acción, garantizar su trazabilidad y reporte institucional, y complementar el informe de controles con la evaluación detallada, firma y aprobación por parte del Comité.

4.1.4.2. Revisión por la dirección

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

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información el archivos denominados "*25 y 26.25-01-30 Acta N°1 Comité Institucional de Gestión y Desempeño.pdf*", "*Presentación comité extraordinario 10072025-2.pptx*", "*Presentación Comité Institucional de Gestión y Desempeño - Enero 2025.pptx*" y *"Presentación Comité Institucional de Gestión y Desempeño V3 - Ene 2025.pptx"*. Una vez revisados los respectivos archivos se identificó lo siguiente:

Durante la revisión del acta del Comité Institucional de Gestión y Desempeño y de las presentaciones remitidas como evidencia de la revisión por la dirección, se verificó que la entidad cuenta con registros de sesiones en las que se abordan temas asociados a seguridad y privacidad de la información, así como con material de soporte utilizado en dichas reuniones; sin embargo, el análisis realizado evidenció que la documentación no demuestra la revisión formal del Manual del MSPI ni la aprobación correspondiente por parte de la Alta Dirección, conforme a lo establecido en el lineamiento, lo cual se detalla en el siguiente hallazgo:

OBSERVACIÓN 4: Falta de revisión y aprobación del Manual de Seguridad y Privacidad por parte del Comité. No se evidencia que el Manual del Modelo de Seguridad y Privacidad haya sido tratado o revisado durante la sesión reportada. Además, aunque la Alta Dirección aparece listada entre los asistentes del comité, el acta no cuenta con su firma, quedando suscrita únicamente por funcionarios operativos. Esto impide validar formalmente la participación directiva y la aprobación de los temas estratégicos analizados.

Recomendación: Se sugiere que la Alta Dirección firme las actas y documentos derivados de la revisión, y que se incluya explícitamente la revisión del Manual dentro del orden del día, asegurando respaldo formal y trazabilidad institucional.

4.2. Anexo 2 (Resolución 746 de 2022) - Gestión de Proveedores

4.2.1. Planificación de las relaciones con Proveedores

Para gestionar adecuadamente la seguridad de la información en las relaciones con proveedores, las entidades estatales deben establecer un plan de relación con

proveedores que documente la decisión adoptada por el nivel directivo de adquirir un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.

Lineamiento	Propósito	Salidas
Establecer un plan de relación con proveedores que documente la decisión adoptada por el nivel directivo de adquirir un producto o servicio relacionado con activos de información, así como las consideraciones de seguridad de la información relacionadas con esta contratación.	Gestionar con la debida diligencia la seguridad de la información dentro del proceso de planeación de la relación con los proveedores de productos o servicios de seguridad de la información.	Plan de evaluación y tratamiento de riesgos de seguridad de la información asociados al producto o servicio que se contrate Plan de relación con proveedores.

Se entregó por parte del GT Gestión de Plataforma de Tecnologías de Información el archivos denominados *"1_Plan-Gestion-Proveedores2025.pdf"* y *"2.PRTEC_acuerdosconproveedoresconaccesoaactivosdeinformacin.V1-2.pdf"*. Una vez revisados los respectivos archivos se identificó lo siguiente:

OBSERVACIÓN 5: Debilidades del Plan de Relación con Proveedores frente a los requisitos del MSPI. Frente a los requisitos establecidos en el Lineamiento 2 del documento Relación con Proveedores de Seguridad Digital, se identifican debilidades en la planificación de las relaciones con proveedores de servicios y productos TI, dado que la documentación remitida no incorpora todos los elementos mínimos que exige el lineamiento para estructurar adecuadamente este proceso. Si bien existen documentos que abordan aspectos generales del análisis de riesgos y del proceso contractual, no se encuentra un Plan de Relación con Proveedores alineado a los elementos obligatorios definidos en el lineamiento, específicamente:

- No se documentan las especificaciones mínimas del servicio (alcance, audiencia, tipo y naturaleza) para cada adquisición,
- No se identifican los activos relevantes y sus propietarios,
- No se incluye la clasificación de la información involucrada,
- No se documentan requisitos legales y regulatorios específicos,
- No se articula un análisis de riesgos específico por cada contratación,
- No existe evidencia de la "decisión de gestión documentada",

El Plan 2025 es general y estratégico, pero presenta debilidades con las actividades, entradas y salidas que el lineamiento exige para cada producto o servicio TI adquirido.

Recomendación: Ajustar el Plan de Gestión con Proveedores o el procedimiento institucional vigente, de manera que incluya expresamente los elementos exigidos por el Lineamiento 2 del documento Relación con Proveedores de Seguridad Digital, y asegurar que dichos elementos se apliquen cuando se gestione cada contratación. En particular, incorporar las especificaciones mínimas del servicio, la identificación de activos y propietarios, la clasificación de la información involucrada, los requisitos legales y

regulatorios aplicables, el análisis de riesgos específico para la relación contractual, y la decisión de gestión documentada del nivel directivo.

4.2.2. Proceso de terminación de la relación con el proveedor

La finalidad en todos los casos es proteger la confidencialidad, integridad y disponibilidad de la información, por ello, dar por terminado el relacionamiento contractual debe ser transparente y preciso para la organización, evitando traumatismo y materialización de eventos adversos en el proceso durante el cierre y entrega a un nuevo proveedor o a la entidad, para todos los casos, es imperante que el servicio o producto siempre esté funcional según corresponda, para así evitar impactos operacionales, legales o económicos. Es preciso tener presente los tiempos, documentos y elementos requeridos para el cierre del contrato, con base en lo establecido en los términos contractuales y la normatividad vigente.

Lineamiento	Propósito	Salidas
Planificar el cierre contractual con los proveedores de productos o servicios de seguridad de la información.	Gestionar con la debida diligencia y de manera segura la terminación de la relación con el proveedor de productos o servicios de seguridad de la información garantizando la continuidad de la operación.	Acta de finalización del contrato avalada y firmada por el supervisor, en el cual certifica el cierre de la relación contractual. Informe aprendidas de lecciones durante el tiempo del servicio y en el cierre del contrato.

OBSERVACIÓN 6. Debilidades entre las lecciones aprendidas y los contratos de seguridad digital liquidados. Aunque la entidad cumple con lo solicitado en el lineamiento al entregar dos actas de liquidación debidamente firmadas que certifican el cierre contractual, así como una matriz de lecciones aprendidas, se evidencia que las lecciones documentadas no están asociadas directamente a los contratos de seguridad digital liquidados, sino que corresponden a una matriz general de proyectos. Esta situación, si bien no afecta el cumplimiento formal del requerimiento, limita la trazabilidad entre el proceso de terminación del contrato y los aprendizajes obtenidos del servicio específico.

Recomendación: Asociar explícitamente las lecciones aprendidas a cada contrato de seguridad digital liquidado, incluyendo número de contrato, proveedor y servicio prestado, de manera que exista una trazabilidad clara entre el proceso de terminación contractual y los aprendizajes obtenidos. Esto facilitará la retroalimentación en futuros procesos y fortalecerá la gestión del cierre contractual conforme al lineamiento.

4.3. Validación de las actividades propuestas en el plan de mejoramiento resultante de la auditoría en la vigencia 2024

Con base en los soportes y evidencias remitidos por el GT Gestión de Plataforma de Tecnologías de Información, se realizó la revisión del avance de las actividades incluidas en el Plan de Mejoramiento correspondiente a la vigencia 2024. Para cada hallazgo u observación, se verificó la descripción, la acción propuesta y las evidencias entregadas, evaluando su grado de implementación conforme a los criterios definidos. Este análisis permitió identificar avances, y dar como cumplidas algunas de las acciones establecidas.

A partir de esta verificación, se consolidó el estado actual de cada actividad, en la cual se relacionan los resultados del análisis efectuado y la clasificación final del cumplimiento. El cuadro siguiente presenta de manera resumida dicha validación, permitiendo visualizar el avance real de las acciones:

DESCRIPCIÓN	DESCRIPCIÓN ACCIÓN	ANÁLISIS	ESTADO
Control 6.1.1: Designación del rol Oficial de Seguridad de la Información Conforme con la Matriz de Roles y Responsabilidades, actualmente el SGC no cuenta con un responsable formal de la seguridad de la información (OSI) conforme se establece en el ítem 6.5 “Cumplimiento de la política”, la cual indica: “La Alta Dirección garantizará que el personal del SGC, directamente relacionado con el establecimiento, implementación y mejora continua del Sistema Integrado de Gestión de Seguridad de la Información, cuente con las competencias, formación y capacitación necesarias para desempeñar las funciones y responsabilidades asignadas en dicho sistema, con el fin de asegurar el cumplimiento de sus objetivos”. Por otra parte, tampoco se cuenta con un Oficial de Protección de Datos Personales (OPDP).	Designar formalmente el rol de Oficial de Seguridad de la Información en la Dirección de Gestión de Información (DGI) mediante la un acto administrativo, ejemplo: resolución, garantizando que dicha designación sea aprobada por la Alta Dirección y comunicada a todas las áreas pertinentes antes de finalizar el año 2025.	Se identifica el memorando con radicado SGC-3-2025-001432 del 10 de abril de 2025, mediante el cual la Secretaría General designa, a partir de la fecha, al Director Técnico de Gestión de Información como Oficial de Seguridad de la Información en el SGC. No obstante, es necesario adjuntar como soporte la resolución interna mencionada en el memorando que formaliza dicha designación, así como la evidencia de la comunicación emitida a todas las áreas, en coherencia con la acción definida y la meta establecida. La fecha de terminación de la acción está prevista para diciembre de 2025, por lo que su estado se mantiene en proceso, a la espera de la entrega de los soportes requeridos por parte del proceso correspondiente, con el fin de proceder a la validación y cierre de la acción.	En proceso
Control 6.1.2: Definición de Matriz de Roles y Perfiles Actualmente el SGC, no cuenta con una Matriz de Roles y Perfiles que permita definir, gestionar y controlar los accesos de los usuarios a los sistemas de	Definir y documentar la Matriz de Roles y Perfiles para gestionar y controlar los accesos de los usuarios a los sistemas de información del SGC, asegurando su implementación en todas las áreas antes de finalizar el año 2025.	Dentro del soporte suministrado se evidencian avances significativos en la definición, documentación e implementación parcial de la Matriz de Roles y Perfiles, enfocados en el cumplimiento del producto	En proceso

DESCRIPCIÓN	DESCRIPCIÓN ACCIÓN	ANÁLISIS	ESTADO
información. La ausencia de esta herramienta representa un riesgo significativo para la seguridad de la información, ya que no se garantiza la segregación de funciones, el principio de mínimo privilegio ni el acceso adecuado según las responsabilidades asignadas.		esperado en cuanto a su estructura y control de accesos. No obstante, se requiere complementar con la evidencia de socialización e implementación integral en todas las áreas del SGC, en coherencia con la descripción de la acción propuesta. En este sentido, la acción se mantiene en estado "En Proceso" hasta contar con los soportes mencionados, momento en el cual podrá efectuarse la validación final y proceder con el cierre de la acción. La fecha de terminación de la acción está prevista para diciembre de 2025, por lo que su estado se mantiene en proceso, a la espera de la entrega de los soportes requeridos por parte del proceso correspondiente, con el fin de realizar la validación final y cierre de la acción.	
Control 10.1.1 y 10.1.2: Procedimiento Gestión de Llaves En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política sobre el uso de Controles Criptográficos. Sin embargo, esta carece de información detallada en los siguientes puntos: • No se especifican procedimientos claros sobre la evaluación periódica y la actualización de las herramientas criptográficas utilizadas. • No se establecen lineamientos para la selección de algoritmos robustos, como AES-256 o RSA-2048, ni los escenarios específicos en los que deben emplearse. • No se incluyen parámetros para identificar y eliminar algoritmos considerados inseguros (por ejemplo, DES o MD5),	Establecer un procedimiento formal en Isolucion para la gestión del ciclo de vida de las llaves criptográficas, que incluya su generación, distribución, almacenamiento, uso, renovación, revocación y destrucción, incorporando directrices claras para la selección de algoritmos robustos y la eliminación de algoritmos obsoletos.	Dentro del soporte suministrado se evidencia el cumplimiento de la acción, dado que se cuenta con el procedimiento PR-TEC-001 "Gestión del Ciclo de Vida de Llaves Criptográficas, Versión 01", el cual fue elaborado, revisado, aprobado y se encuentra formalizado en el sistema Isolución, conforme a la meta establecida. El documento presenta los lineamientos técnicos y operativos para la gestión del ciclo de vida de las llaves criptográficas, desde su generación hasta su destrucción, incorporando directrices relacionadas con la utilización de algoritmos robustos y la eliminación de algoritmos obsoletos. En este sentido, la acción se considera cumplida. La validación de la publicación se realizó en Isolución, donde se verificó que el documento fue aprobado el 29 de agosto de 2025.	Cerrada

DESCRIPCIÓN	DESCRIPCIÓN ACCIÓN	ANÁLISIS	ESTADO
comprometiendo la confidencialidad, integridad y autenticidad de la información cifrada.			
Control 11.2.9: Escritorio y pantalla limpia de información En el Manual de Políticas Específicas de Gestión 'de Seguridad de la Información (versión 2020) está documentada la Política de escritorio limpio y pantalla limpia, establece "…el Grupo de Tecnologías de Información debe aplicar políticas a los equipos para restringir el almacenamiento de información en el escritorio de los equipos de cómputo suministrados por el SGC…". Sin embargo, durante una sesión virtual realizada el 11 de diciembre de 2024, esta Oficina constató que, en la práctica, se está almacenando información no solo en los escritorios de los equipos, sino también en la carpeta de "Descargas". Además, desde esa ubicación se intentaba acceder a la información relacionada con la presente auditoría. Esto sugiere que los repositorios institucionales, que cuentan con mecanismos de seguridad como copias de seguridad, no están siendo utilizados adecuadamente.	El control relacionado con la política de pantalla limpia y escritorio limpio no incluye la gestión del disco duro fijo de los equipos de cómputo. Por lo tanto, se fomentará el uso de repositorios institucionales seguros y revisar de manera periódicas para verificar el cumplimiento de dicha política. Además, estas medidas serán complementadas con sesiones de sensibilización dirigidas a los usuarios, con el objetivo de promover una cultura de seguridad de la información. Acciones:1.En el nivel del antivirus Trellix, se configurará una política para bloquear la ejecución del archivo ejecutable del utilitario, asegurando que no pueda ser ejecutado en los equipos protegidos. Tener en cuenta que en los OVS hay equipos a los que no se les puede aplicar dicha política porque por su función de monitoreo no se pueden bloquear.(para que no aplique la política se revisarán las excepciones) 2.Revisar y ajustar 6.5.1. Política de escritorio limpio y pantalla limpia - Pantalla Limpia: Directriz que asegura que las pantallas de los equipos estén protegidas contra el acceso no autorizado o visualización indebida. 3.Sensibilizar a los usuarios frente a la política una vez modificada. 4.Realizar revisiones periódicas para verificar el cumplimiento de la política mediante el análisis de los reportes generados por el antivirus o el OSC, asegurando que se detecten y gestionen posibles incumplimientos de manera oportuna.	Dentro de los soportes suministrados se evidencian avances en la implementación de las medidas correctivas, incluyendo la configuración de controles técnicos, la actualización del documento normativo y la revisión por parte de las áreas competentes. No obstante, dado que la nueva versión de la política aún no se encuentra formalizada ni se ha realizado la sensibilización a los usuarios, la acción se mantiene en estado "En Proceso" hasta completar dichas actividades, conforme a la descripción de la acción definida. La fecha de terminación de la acción está prevista para diciembre de 2025, por lo que su estado se mantiene en proceso, a la espera de la entrega de los soportes requeridos por parte del proceso correspondiente, con el fin de proceder a la validación y cierre de la acción.	En proceso
Control 13.1.1, 13.1.2 y 13.1.3: Controles de seguridad en redes En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política de Gestión de la	1. Acceso a switch core por VPN Actividad: Revisar y corregir las configuraciones de VPN y firewall para restringir el acceso no autorizado a los switches core por SSH, implementando controles de acceso adecuados y validando su efectividad mediante pruebas y monitoreo.	Dentro del soporte suministrado se evidencian avances relevantes en la ejecución de las actividades descritas en la acción, específicamente en la corrección de configuraciones de VPN y firewall para restringir accesos no autorizados, así como en la segmentación de la red en la sede	En proceso

DESCRIPCIÓN	DESCRIPCIÓN ACCIÓN	ANÁLISIS	ESTADO
Seguridad en las Redes, la cual establece que “El SGC, a través del Grupo designado, únicamente proporcionará a los funcionarios, contratistas y proveedores acceso a los servicios para los que específicamente se les haya autorizado, controlando las conexiones de red y los equipos o servicios de red que deben estar definidos según los roles y perfiles aprobados por el SGC.” No obstante, durante una sesión virtual realizada el 11 de diciembre de 2024, esta Oficina constató que, aunque se está realizando la segregación de redes mediante VLANs para las sedes de Bogotá, sin embargo, se encuentra pendiente la migración de los usuarios a dicha VLAN para la sede de Cali. Por otra parte, se identificó una brecha en la aplicación de controles de seguridad, ya que es posible acceder al switch core mediante una conexión VPN de usuarios. Esto indica que no existen restricciones de acceso adecuadas entre las VLANs, poniendo en riesgo la segregación y el control de accesos internos. Es fundamental que los recursos de administración solo sean accesibles desde VLANs de administración específicas para garantizar una mayor seguridad y control.	Desarrollo: Análisis y ajuste de configuraciones: Identificar y corregir las reglas de firewall y perfiles de VPN para restringir el acceso solo a servicios autorizados. Implementación de controles de acceso: Aplicar listas de control de acceso (ACLs) y políticas de restricción para bloquear conexiones no deseadas. Pruebas y monitoreo: Validar la efectividad de las medidas implementadas mediante pruebas de acceso y monitoreo continuo de logs de conexión. 2. Segmentación de la VLAN de usuarios en la sede Cali Actividad: Coordinar e implementar la segmentación de la VLAN de usuarios en la sede Cali, asegurando la segregación de la VLAN de servidores, realizando pruebas de validación y documentando la evidencia del proceso. Desarrollo: Coordinación con el equipo local: Planificar la ejecución con el soporte en sitio y minimizar el impacto en los usuarios. Configuración y pruebas: Implementar la segmentación en los switches y realizar pruebas de conectividad y seguridad. Documentación y validación: Registrar la configuración aplicada y generar evidencia del correcto funcionamiento de la segmentación.	Cali para separar la VLAN de servidores y de usuarios. Sin embargo, los informes entregados no incluyen información sobre quién elaboró o aprobó los documentos, ni registran fechas de emisión, control de cambios o validación formal de los resultados, lo que impide garantizar la integridad, trazabilidad y veracidad de la información contenida. Por lo anterior, no es posible confirmar el cumplimiento total de la acción, manteniéndose en estado “En Proceso”, a la espera de que el proceso remita los informes con la debida validación, fechas, aprobaciones formales Y/o soporte adicionales, que permitan verificar la efectividad de las medidas implementadas, para proceder con la validación y cierre de la acción. La fecha de terminación de la acción está prevista para diciembre de 2025, por lo que su estado se mantiene en proceso, a la espera de la entrega de los soportes requeridos.	
Control 15.1: Análisis de riesgos con proveedores En el Manual de Políticas Específicas de Gestión de Seguridad de la Información (versión 2020) se encuentra documentada la Política de Relación con los Proveedores, establece que “El SGC a través del grupo designado debe dar a conocer las políticas de SGSI y de protección de datos	Establecer un instructivo que se formalizara en Isolucion que asegure la realización de análisis de riesgos de seguridad y la formalización de acuerdos con los proveedores antes del inicio de las actividades, definiendo los criterios de acceso a los activos de información. (Revisar si se puede incluir en los estudios previos)	Dentro del soporte suministrado se evidencia el cumplimiento de la acción, toda vez que se cuenta con el procedimiento PR-TEC-002 “Análisis de riesgos y acuerdos con proveedores con acceso a activos de información”, Versión 1, formalizado en Isolución, el cual dispone las actividades requeridas para realizar el análisis de riesgos previo al inicio de las actividades con proveedores, documentar los	Cerrada

DESCRIPCIÓN	DESCRIPCIÓN ACCIÓN	ANÁLISIS	ESTADO
personales, y debe formalizar los acuerdos con los proveedores antes del inicio de las actividades. El jefe inmediato o supervisor de contrato apoyado por el Responsable de Seguridad de Información realizará análisis de riesgo de seguridad para establecer los criterios de acceso a los activos de información a los cuales tiene acceso terceras partes y definir los planes o acciones de tratamiento para prevenir la materialización de los riesgos identificados.” Sin embargo, conforme la sesión realizada el día 11 de diciembre, está actividad no se está llevando a cabo por ninguno de los dos responsables.		resultados en los estudios previos, incorporar cláusulas contractuales de seguridad y verificar su implementación antes del inicio del servicio; en consecuencia, la acción se encuentra Cumplida. La validación de la publicación se realizó en Isolución, donde se verificó que el documento fue aprobado el 29 de agosto de 2025.	

5. CONCLUSIONES

- El MSPI en el SGC presenta un nivel de implementación parcial, con avances en la definición de metodologías, controles y matrices de riesgos; sin embargo, persisten brechas relevantes que impiden la alineación completa con los lineamientos del MinTIC versión 2025.
- Las fases de Diagnóstico y Planificación muestran debilidades estructurales, especialmente en el alcance del MSPI, identificación del contexto, partes interesadas y uso de herramientas oficiales, lo que afecta la calidad de los insumos para las fases posteriores.
- La gobernanza del modelo no está formalizada, debido a la ausencia de un acto administrativo actualizado que asigne funciones al Comité Institucional de Gestión y Desempeño e incorpore al Responsable de Seguridad de la Información como miembro permanente.
- La gestión de activos y riesgos evidencia avances, pero requiere mayor integración, actualización de la Declaración de Aplicabilidad y mejor identificación de riesgos asociados a la privacidad.
- La entidad ha incorporado recursos técnicos alineados con el MSPI; sin embargo, aún se requiere fortalecer la trazabilidad de estos recursos frente a los riesgos priorizados, los componentes humanos y la alineación con el PETI, a fin de asegurar una gestión integral conforme al Lineamiento 7.4.1.
- El seguimiento y evaluación del desempeño del MSPI presenta debilidades, pues los indicadores no están incorporados en el tablero institucional del Plan de Acción y el informe de efectividad no presenta evaluación detallada ni aprobación del Comité Institucional de Gestión y Desempeño.

Finalmente, se presenta un cuadro resumen que sintetiza los hallazgos, observaciones y recomendaciones para cada una de las fases para facilitar su comprensión.

Fase	Hallazgos	Observaciones	Recomendaciones
Diagnóstico	2	0	2
Fase 1. Planificación	5	3	9
Fase 2. Operación	1	0	2
Fase 3. Evaluación del Desempeño:	1	1	2
Anexo 2. Gestión de Proveedores	0	2	2
Total	9	6	17

Auditor: Crhistian Augusto Amador León – Contratista - Oficina de Control Interno
Aprobó: Erika Marcela Huari Mateus - Jefe Oficina de Control Interno