Bogotá D.C., 22 de octubre de 2025 **CI-20251021-1295**

MEMORANDO

PARA: **LUIS FELIPE LOTA**
Director
Presidente del Comité Institucional de Coordinación de Control Interno

LILIANA MORALES
Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
Miembro del Comité Institucional de Coordinación de Control Interno

DE: **ANDREA REYES SAAVEDRA**
Jefe de Oficina de Control Interno

ASUNTO: Informe Final de Auditoría de cumplimiento "Grado de Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca".

Respetados Ingenieros

La Oficina de Control Interno entre los meses de septiembre[1] y octubre[2] de 2025, realizó la auditoría de cumplimiento "Grado de Implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca".

Las conclusiones de la auditoría realizada se presentan en el capítulo 7 del informe que se anexa a la presente comunicación. Es importante precisar que, en el desarrollo de dicha auditoría, no se emitieron hallazgos, sino observaciones y recomendaciones orientadas exclusivamente a generar oportunidades de mejora en los procesos.

[1] Se adelantó la etapa de planeación y ejecución
[2] Se culmino etapa de ejecución, se adelantó emisión de informe preliminar, cierre de auditoría y emisión de informe final.

En atención a lo anterior, se solicita analizar las circunstancias evidenciadas durante la auditoría, con el propósito de evaluar la necesidad de adoptar o fortalecer puntos de control, así como de implementar las acciones y recomendaciones formuladas. Lo anterior, para que sean revisadas por el Líder del Proceso y/o Líderes de los procesos y puedan ser consideradas por la Entidad, en aras de promover la mejora continua y el fortalecimiento institucional.

Finalmente, agradecemos el apoyo brindado en el desarrollo de la auditoría y confiamos en que los resultados obtenidos contribuyan al fortalecimiento continuo del Sistema de Control Interno en la Región Metropolitana Bogotá–Cundinamarca.

Cordialmente,

ANDREA REYES SAAVEDRA
Jefe de Oficina de Control Interno

Nota: Para este periodo no se suscribió con firma electrónica por cuanto se está adelantando actualmente el proceso contractual, de acuerdo con correo electrónico del día 5 de agosto de 2025 por parte de la Jefatura de la Oficina de Tecnologías de la Información y las Comunicaciones.

C.C.: Jennifer Bermúdez Dussán-Subdirectora de Gestión Corporativa- miembro del Comité Institucional de Coordinación de Control Interno / Diego Díaz del Castillo Fernández - Subdirector de Gestión de Proyectos - miembro del Comité Institucional de Coordinación de Control Interno / Gisela Paola Labrador Araújo -Subdirectora de Gestión Metropolitana y Regional- miembro del Comité Institucional de Coordinación de Control Interno / Luz Dary Garzón Guevara - Jefe Oficina de Control Disciplinario Interno - miembro del Comité Institucional de Coordinación de Control Interno / Luis Alberto Colorado Aldana - Jefe de Oficina Asesora de Planeación Institucional - miembro del Comité Institucional de Coordinación de Control Interno / Laura Lucia Cárdenas Hincapié- Jefe de la Oficina Jurídica (e) - miembro del Comité Institucional de Coordinación de Control Interno- y Asesora de la Dirección/ Angela Marcela Cárdenas Mora- Jefe de Oficina Asesora de Comunicaciones y Participación Ciudadana - miembro del Comité Institucional de Coordinación de Control Interno. Lo anterior para su conocimiento y fines pertinentes/

ROL	NOMBRES Y APELLIDOS	CARGO/ROL	FIRMA
Elaboró	Crhistian Augusto Amador León	Contratista	CRHISTIAN AMADOR

Oficina de Control Interno

INFORME DE AUDITORÍA DE CUMPLIMIENTO

Grado de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca

Vigencia 2025

Octubre de 2025

Contenido

1. Objetivo

Evaluar el avance en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca.

2. Alcance

Evaluar la gestión realizada en la implementación del Modelo de Seguridad y Privacidad de la información, por parte de la Región Metropolitana Bogotá-Cundinamarca durante el periodo comprendido entre el 1 de enero de 2024 y el 15 de septiembre de 2025.

3. Criterios Normativos

Los criterios de la verificación se encuentran sustentados, en la siguiente normatividad externa e interna sobre la materia:

- 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 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- 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 de Seguridad y Privacidad de la Información de la Región Metropolitana de Bogotá - Cundinamarca.
- Guía para la Administración del Riesgo y el Diseño de Controles en entidades públicas Versión 6 emitida por el Departamento Administrativo de la Función

Pública.

- Guía para la Gestión Integral del Riesgo en entidades públicas Versión 7 emitida por el Departamento Administrativo de la Función Pública.
- Guías establecidas por el MinTIC frente a la implementación del MSPI (Documento Maestro Lineamientos MSPI 2025)
- Norma ISO: IEC 27001:2022

Y la demás normatividad interna y externa aplicable con el fin de lograr el objetivo y alcance de la presente auditoría.

4. Metodología [1]

En el marco del presente seguimiento, se realizaron entre otras las siguientes actividades:

- Análisis de los criterios normativos aplicables para la Región Metropolitana Bogotá-Cundinamarca de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones MinTIC y la norma NTC ISO/27001:2022.
- Con memorando radicado No.CI-20250918-1169 del 18 septiembre de 2025, remitido a través de correo electrónico del 18 de septiembre de 2025, se notifica, solicita información y se comunican los criterios normativos a la Oficina de Tecnologías de la Información y las Comunicaciones, para la ejecución de la auditoría interna de cumplimiento al grado de implementación del modelo de seguridad y privacidad de la información – MSPI en la Región Metropolitana Bogotá-Cundinamarca.
- El día 22 de septiembre de 2025 se llevó a cabo la reunión de apertura de la Auditoría Interna de Cumplimiento al grado de implementación del modelo de seguridad y privacidad de la información – MSPI en la Región Metropolitana Bogotá-Cundinamarca, con la participación de la Oficina de Tecnologías de la Información y las Comunicaciones. Durante la reunión se comunicaron el objetivo, el alcance, el marco normativo aplicable y las fechas previstas para la realización de la auditoría.
- Mediante memorando con radicado No.CI-20250923-1192 del 25 septiembre de 2025 remitido a través de correo electrónico a la Oficina de Control Interno, la Oficina de Tecnologías de la Información y las Comunicaciones dio respuesta a la solicitud de información documental solicitada y se almacenaron en el SharePoint los soportes respectivos.

[1] Las actividades que se enuncian en el siguiente numeral se encuentran soportadas en los papeles de trabajo de la auditoría, los cuales reposan en el archivo de gestión de la OCI de acuerdo con el tiempo señalado en la TRD vigente

- Mediante correo electrónico del 14 de octubre se socializo a la Oficina de Tecnologías de la Información y las comunicaciones el informe preliminar de la presente auditoría de gestión, con el fin de garantizar el derecho a la contradicción por parte del líder del proceso.
- El día 17 de octubre de 2025, la Oficina de Tecnologías de la Información y las comunicaciones remitió respuesta correspondiente a la socialización del informe preliminar de la presente auditoría en la cual se manifestó mediante memorando CI-20251017-1286 que *"(…) se acatan en su totalidad las once (11) observaciones formuladas, comprendiendo su importancia para el fortalecimiento institucional y la adecuada implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)"*
- El día 22 de octubre de 2025 la Oficina de Control Interno realizó cierre de la auditoría a través de la Plataforma Microsoft Teams en donde se contó con la participación de la líder del proceso y la Oficina Asesora de Planeación Institucional.

5. Desarrollo del Informe

Sobre el particular es importante señalar que, se verificó el estado actual de cumplimiento de las fases que componen el Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a lo establecido 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.

Para el desarrollo de la Auditoría Interna de Cumplimiento sobre la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca, se aplicó una metodología basada en la revisión documental aportada por el área responsable y el análisis de los soportes suministrados.

El análisis comprendió el periodo del 1 de enero de 2024 al 15 de septiembre de 2025 y se complementó con la verificación de los soportes documentales, orientados a identificar riesgos, validar los controles establecidos y verificar el cumplimiento de la normativa y metas programadas.

5.1. 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. Teniendo en cuenta lo anterior se identificó lo siguiente:

Lineamiento: Identificar a través de la herramienta de autodiagnóstico (instrumento de evaluación MSPI) el estado actual de la entidad respecto a la Seguridad y Privacidad de la Información.

Propósito: 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.

Salida: Documento de la herramienta de autodiagnóstico diligenciada, identificando las brechas en la implementación del MSPI en toda la entidad y sus acciones de mejora.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución

de la auditoría: A través del No.12A

Respuesta: *La entidad realiza el autodiagnóstico frente a los expuesto por MSPI de la vigencia 2025, se deja documento en el repositorio.*

Observación y/o análisis realizado por la Oficina de Control Interno:

La Entidad entregó el autodiagnóstico MSPI 2025 en formato Excel, que incluye el resultado de la evaluación de efectividad de controles y el avance de las cláusulas del modelo de operación (PHVA).

No obstante, se evidenciaron inconsistencias y vacíos de diligenciamiento que afectan la completitud del instrumento y su utilidad como insumo para la planificación:

- En la hoja "Levantamiento de Información", las columnas "Nombre del Documento Entregado" y "Observaciones" no se encuentran diligenciadas, lo cual impide conocer el estado real de los documentos que soportan cada control y limita la verificación del cumplimiento.
- En las hojas de dominios (Organizacionales, Personas, Físicos y Tecnológicos) se evidencian avances en los campos de "Evidencia" y "Nivel de Cumplimiento", sin embargo:
    - La columna "Brecha" se encuentra vacía en ciertos casos, ya que se observó solo el diligenciamiento en los casos aislados.
    - La columna "Recomendación" no se encuentra diligenciada.
    - No se presenta consolidado de brechas ni plan de acciones de mejora derivado del autodiagnóstico (con responsables, plazos y prioridades).

En consecuencia, aunque la herramienta permite identificar el estado de madurez y aporta información preliminar sobre el avance institucional, no cumple plenamente con la salida exigida por el lineamiento, que requiere la identificación de brechas y acciones de mejora como base para la planificación.

Esta situación limita la capacidad de la Entidad para planificar adecuadamente la siguiente fase de implementación del MSPI y fortalecer su nivel de madurez en seguridad y privacidad de la información.

Recomendación de la Oficina de Control Interno:

Completar los campos faltantes en la hoja "Levantamiento de Información", registrando el nombre del documento soporte y observaciones que evidencien su existencia o ausencia, asegurando trazabilidad documental.

Diligenciar las columnas “Brecha” y “Recomendación” en cada dominio, identificando claramente los aspectos no cumplidos o parcialmente implementados y las acciones necesarias para su cierre.

Consolidar las brechas y acciones de mejora, definiendo responsables, plazos, prioridad e indicador de avance, que sirva como insumo directo para el Plan de Implementación MSPI.

Alinear los resultados del autodiagnóstico con el Plan de Implementación, priorizando los dominios con menor nivel de madurez y estableciendo acciones de mejora progresivas conforme con lo definido en los lineamientos del MinTIC.

Este documento debe consolidar la información de toda la entidad y servir como insumo para la planificación y el mejoramiento continuo.

5.2. Fase de Planeación

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.

5.2.1. Necesidades y expectativas de los interesados

Lineamiento: 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.

Propósito: 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.

Salidas: - Compendio de necesidades y expectativas de las partes interesada. (Política de Planeación Institucional).
- Análisis de partes interesadas en seguridad de la información.

Observación y/o análisis realizado por la Oficina de Control Interno:

Debilidad en la identificación y análisis de las necesidades y expectativas de las partes interesadas en materia de seguridad y privacidad de la información

Durante la verificación, se identificó que no se ha adelantado el proceso de identificación y análisis de las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información. No se han elaborado documentos que permitan reconocer las necesidades, expectativas o requisitos legales, reglamentarios y contractuales asociados al MSPI.

La ausencia de este análisis impide conocer los actores clave, sus intereses, y los requerimientos que deberían integrarse al sistema de gestión de seguridad y privacidad de la información.

Esta situación limita la capacidad institucional para alinear las acciones del MSPI con el contexto interno y externo de la entidad, y afecta la planificación de estrategias de seguridad acordes a las expectativas de las partes interesadas.

Recomendaciones de la Oficina de Control Interno

Realizar la identificación y análisis de las partes interesadas internas y externas que inciden en la gestión de la seguridad y privacidad de la información.

Documentar las necesidades, expectativas y requisitos de cada parte interesada, incluyendo aspectos legales, reglamentarios, contractuales y técnicos.

Integrar el análisis realizado al Plan de Implementación del MSPI, garantizando su coherencia con el contexto y misión de la entidad.

Socializar y actualizar periódicamente el análisis, considerando cambios en el entorno institucional, proveedores, contratistas o disposiciones normativas.

5.2.2. Definición del alcance del MSPI

Lineamiento: 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.

Propósito: 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.

Salida: 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).

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No. 1B

Respuesta: *La Oficina de TIC, atendiendo al principio de progresividad, se encuentra en proceso de documentación del Plan de Implementación del MSPI para la vigencia 2025-2026. Dicha evidencia se puede observar en el repositorio que fue compartido.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Debilidades en la formulación del alcance del MSPI en el Plan de Implementación 2025.

En el documento denominado “Plan de Implementación del MSPI 2025” se establece un alcance amplio que incluye todos los procesos misionales, estratégicos y de apoyo, así como sistemas de información, activos físicos y digitales, funcionarios, contratistas y terceros

Sin embargo, se identifican las siguientes debilidades:

- No se presenta una delimitación clara ni una aplicabilidad específica del MSPI frente al modelo de operación por procesos de la entidad.
- No se identifica los procesos priorizados ni su nivel de exposición a riesgos de seguridad y privacidad.

- No se incorporan las entradas recomendadas, tales como el modelo de procesos, el catálogo de servicios tecnológicos, el presupuesto disponible o el contexto organizacional.
- No se detallan los activos de información, software, hardware, roles y áreas seguras que serán protegidos bajo el MSPI.
- El documento carece de formalización y control documental, ya que no presenta número de versión, fecha de emisión, control de cambios, firmas de aprobación ni trazabilidad del proceso de validación por parte del Comité Institucional de Gestión y Desempeño.

La ausencia de una definición precisa y delimitada puede generar ambigüedades en la implementación del MSPI, dificultando la trazabilidad de los procesos cubiertos, la asignación de responsabilidades y la identificación de brechas específicas en seguridad y privacidad de la información.

Recomendaciones de la Oficina de Control Interno

- Ajustar y complementar el alcance del MSPI definiendo de manera específica:
    - Los límites y la aplicabilidad del modelo frente al mapa de procesos institucional.
    - Los procesos priorizados, con base en su nivel de exposición a riesgos.
    - Los activos de información, roles, sistemas y áreas seguras que se encuentran dentro del alcance.
- Incorporar como insumos documentales el modelo de procesos, modelo organizacional, catálogo de servicios tecnológicos, presupuesto y contexto de la entidad, conforme al lineamiento 7.1.3.
- Formalizar el documento mediante control de versiones, fecha de emisión, control de cambios y firma de aprobación de la Jefatura de la Oficina TIC y Comité de Gestión y Desempeño Institucional.
- Publicar la versión aprobada en un repositorio institucional, garantizando que esté disponible y actualizada para consulta de las partes interesadas.
- Mantener trazabilidad documental en el proceso de actualización del Plan de Implementación del MSPI, documentando los cambios y versiones posteriores en el pie de control del archivo.

Este ajuste garantizará la coherencia con los lineamientos establecidos y facilitará la gestión, monitoreo y mejora continua del modelo.

5.2.3. Liderazgo y Compromiso

Lineamiento: 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 sus funciones.

Propósito: 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.

Salida: 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.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.1C

Respuesta: *Las funciones de Comité de Seguridad de la Información son ejercidas por el Comité de Gestión y Desempeño Institucional, conforme a la Resolución No. 332 del 9 de septiembre de 2024.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Falta de designación expresa del responsable de seguridad de la información como miembro permanente del Comité Institucional de Gestión y Desempeño.

En la Resolución No.332 del 9 de septiembre de 2024, se crea formalmente el Comité Institucional de Gestión y Desempeño y se asignan funciones relativas a la implementación de políticas en materia de seguridad digital y de la información (Art. 17, numeral 6). Asimismo, se incluye como integrante al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), quien lidera las políticas de Gobierno Digital y Seguridad Digital.

No obstante, el acto administrativo no designa expresamente al "responsable de seguridad de la información" como miembro permanente del Comité, como lo establece el lineamiento del MSPI.

Aunque el jefe de OTIC podría ejercer dicho rol en la práctica, su falta de designación formal constituye una debilidad normativa y de trazabilidad en el cumplimiento del lineamiento, al no existir evidencia documental que acredite su nombramiento como responsable directo del MSPI ante el Comité.

Recomendación

Se recomienda ajustar la Resolución 332 o emitir un acto administrativo complementario que:

- Designe explícitamente al responsable de seguridad de la información – Oficial de Seguridad- o al Jefe de la OTIC en tal calidad como miembro permanente del Comité Institucional de Gestión y Desempeño, conforme al lineamiento MinTIC.
- Refuerce la trazabilidad del liderazgo y la responsabilidad institucional en la adopción, implementación y mejora continua del modelo.

5.2.4. Política de seguridad y privacidad de la información

Lineamiento: 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,

Propósito: 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.

Salida: 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

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No. 1A

Respuesta: *Política de seguridad y privacidad de la información vigente y aprobada. La Entidad cuenta con la Política de Seguridad Digital, Privacidad de la Información y Datos Personales, formalizada mediante la Resolución No. 065 del 4 de marzo de 2025, publicada en el portal institucional.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Se identificó política de Seguridad y privacidad de la Información en donde se evidencia que:

- La política fue adoptada mediante resolución y aprobada (sesión 31 de enero de 2025)

- Se establece explícitamente la gestión integral de riesgos y controles para preservar estos principios
- Se define revisión periódica (mínimo anual) o cuando se requiera por riesgos o cambios normativos
- Se ordena la divulgación interna y hacia la ciudadanía a través de la página web institucional
- Así mismo en el documento de la política se identifican antecedentes, objetivos, alcance, compromisos, roles, controles y responsables

Lo anterior, cumpliendo con la salida esperada (acto administrativo y política).

5.2.5. Roles y responsabilidades

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

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

Propósito: 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.

Salidas:

- 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 funciones y responsabilidades

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No. 1F

Respuesta: *La matriz fue elaborada y se encuentra en el repositorio institucional.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Debilidad en la formalización e integración de los roles y responsabilidades del

MSPI

La matriz de roles y responsabilidades evidencia avances en la definición de funciones y asignación de tareas, coherentes con los lineamientos generales del MSPI.

Sin embargo, presenta debilidades en cuanto a la formalización de la dependencia organizacional del responsable del MSPI, la acreditación de su participación con voz y voto en los comités institucionales, y la inclusión explícita de los líderes de proceso en la gestión de riesgos de seguridad y privacidad.

Asimismo, el documento no cuenta con fecha, versión, control de cambios ni firmas de aprobación, lo que afecta la trazabilidad documental, la validez formal y la garantía de vigencia del instrumento.

Tampoco se evidencia la inclusión de actores institucionales clave (Oficina Jurídica, Talento Humano, Oficial de Datos Personales) que forman parte de los roles previstos en los lineamientos del MinTIC (“Lineamientos de Roles y Responsabilidades”).

Recomendaciones de la Oficina de Control Interno:

Formalizar la matriz de roles y responsabilidades incluyendo la fecha de elaboración, número de versión, control de cambios, firmas de aprobación y validación por parte de la alta dirección o Comité Institucional.

Emitir un acto administrativo complementario para dejar constancia formal de la designación del responsable del MSPI, en donde su participación deberá ser con voz y voto en el Comité Institucional y con voz en el Comité de Control Interno.

Actualizar la matriz para incorporar a los líderes de los procesos como responsables directos de la gestión de riesgos de seguridad y privacidad tales como Oficina Jurídica, Talento Humano y Oficial de Protección de Datos Personales.

Anexar la matriz como documento de referencia dentro del Plan de Implementación del MSPI o el Manual de Seguridad y Privacidad de la Información, garantizando su trazabilidad.

5.2.6. Identificación de activos de información e infraestructura critica cibernética

Lineamiento: 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.

Propósito: Estructurar una metodología que permita identificar y clasificar los activos de información

Salidas:

- Procedimiento de inventario y clasificación de activos de información, del Modelo de Seguridad y Privacidad de la Información.
- Documento metodológico de inventario y clasificación de la información.
- Inventario de activos de información de cada proceso incluido en el alcance debidamente identificados, clasificados y valorados.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.3A y 3B.

Respuesta: ***a.*** *La Entidad, en aplicación del principio de progresividad, se encuentra actualmente adelantando la elaboración del inventario de activos de información, el cual constituye la base para la gestión integral de seguridad y privacidad.*

b. *La RMBC aún no cuenta con la clasificación formal de la información bajo los criterios de confidencialidad, integridad y disponibilidad, dado que este proceso depende directamente de la finalización del inventario de activos de información. Una vez culminado este, se procederá a su clasificación conforme a los lineamientos del MSPI*

Observación y/o análisis realizado por la Oficina de Control Interno:

Ausencia de inventario consolidado y clasificación formal de los activos de información e infraestructura crítica cibernética.

La entidad se encuentra en fase inicial de implementación del proceso de identificación y clasificación de activos de información, sin contar aún con un inventario consolidado ni con la clasificación de los activos bajo los criterios de confidencialidad, integridad y

disponibilidad.

Tampoco se evidencia la inclusión de los activos que contienen información personal ni la identificación de infraestructura crítica cibernética, de acuerdo con lo establecido en los lineamientos del MinTIC 2025.

La falta de un inventario completo y clasificado limita la capacidad institucional para priorizar controles, identificar activos críticos, proteger la información sensible y gestionar adecuadamente los riesgos de seguridad y privacidad de la información. Asimismo, impide cumplir con las fases obligatorias de identificación, clasificación, revisión y aprobación definidas en los lineamientos nacionales del MSPI

Recomendaciones de la Oficina de Control Interno:

Formalizar y consolidar el inventario de activos de información incluyendo todos los tipos definidos por el MinTIC: información, hardware, software, servicios, talento humano, instalaciones e infraestructura crítica cibernética.

Validar y aprobar la matriz de activos por parte de los propietarios y custodios de cada proceso, así como por el Comité Institucional de Gestión y Desempeño, según lo dispuesto en el Decreto 1083 de 2015 modificado por el Decreto 1499 de 2017.

Desarrollar y documentar la metodología de clasificación, aplicando los criterios de confidencialidad, integridad y disponibilidad y los niveles de impacto alto, medio o bajo, según el documento MinTIC 2025

Identificar los activos con información personal y sensible, garantizando su tratamiento conforme a la Ley 1581 de 2012, la Ley 1712 de 2014 y el Decreto 103 de 2015.

Definir la periodicidad de actualización del inventario y las condiciones que deben motivar una revisión (nuevos sistemas, cambios organizacionales o tecnológicos).

Etiquetar los activos según su nivel de clasificación y publicar la información aplicable en los medios institucionales, asegurando la anonimización de los datos que lo requieran.

Asegurar trazabilidad documental del inventario mediante control de versiones, fecha, firma de aprobación y registro de actualizaciones.

5.2.7. Valoración de los riesgos de seguridad de la información

Lineamiento: 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.
- 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.

Propósito: Estructurar una metodología que permita identificar y clasificar los activos de información

Salidas:

- 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 privacidad de la información.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.2A.

Respuesta: *Actualmente, la Entidad se encuentra adelantando el levantamiento de la matriz de activos de información, insumo necesario para la identificación, tratamiento y evaluación de los riesgos asociados.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Ausencia de metodología y proceso formal de valoración de los riesgos de seguridad y privacidad de la información

La entidad no ha desarrollado ni implementado el proceso de valoración de riesgos de seguridad y privacidad de la información**.** Actualmente se encuentra en una fase preparatoria orientada al levantamiento del inventario de activos, sin que existan metodologías, instrumentos o matrices que permitan identificar, valorar o priorizar riesgos asociados a la confidencialidad, integridad, disponibilidad o privacidad de la información.

Esta situación contraviene los numerales 3.1.8 al 3.1.13 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del MinTIC, que establecen la obligación de definir criterios de valoración, determinar el apetito y la aceptación del riesgo, y garantizar resultados consistentes, válidos y comparables en el tiempo

La ausencia de este proceso impide identificar amenazas y vulnerabilidades, asignar propietarios de riesgo, priorizar controles y evaluar su efectividad, afectando la capacidad institucional para gestionar adecuadamente los riesgos digitales y de seguridad de la información.

Recomendación de la Oficina de Control Interno:

Teniendo en cuenta que actualmente la entidad no cuenta con un instrumento o metodología para la gestión de riesgos se recomienda:

Documentar una metodología que contemple las etapas de identificación, análisis, evaluación y tratamiento, según lo dispuesto en el numeral 3.1.10 del Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, incluyendo criterios claros de probabilidad, impacto y niveles de riesgo, definidos en una matriz o escala aprobada por el Comité de Gestión y Desempeño Institucional e incorporar el concepto de riesgo inherente, riesgo residual y riesgo aceptado, garantizando que las valoraciones sean consistentes y comparables en el tiempo.

Incluir un capítulo específico sobre seguridad y privacidad de la información, conforme al numeral 3.1.3 del Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas emitido por el MinTIC.

Adicionalmente, se defina el compromiso de la alta dirección con la gestión integral de riesgos digitales y su alineación con el MIPG y el MSPI.

Designar formalmente los dueños de cada riesgo (normalmente los líderes de proceso o los custodios de los activos) y asegurar que estos sean responsables del seguimiento de los controles asociados

Una vez concluido el inventario de activos, aplicar la metodología de valoración sobre cada activo identificado, considerando los criterios de confidencialidad, integridad y disponibilidad, asegurando que los activos críticos cuenten con controles específicos y estén priorizados para su tratamiento.

Definir el apetito de riesgo institucional, diferenciando entre los niveles aceptables y los que deben ser mitigados.

Desarrollar una matriz de riesgos de seguridad y privacidad que incluya entre otras, la descripción del riesgo, el activo afectado, la amenaza y vulnerabilidad, el nivel de riesgo (inherente, residual), el responsable del control, el estado del tratamiento. Esta matriz debería revisarse al menos una vez por año o cada vez que ocurran cambios significativos en los procesos o activos.

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

Lineamiento: 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.

Propósito: 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.

Salidas:

- 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.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.2C y 2D.

Respuesta: ***2C.*** *La RMBC cuenta con un Plan de Tratamiento de Riesgos, publicado en la página web institucional. Dicho plan se puede consultar en la siguiente ruta: https://regionmetropolitana.gov.co/sites/default/files/archivos/miscelanea/2025-02-03/5870_plan-de-tratamiento-de-riesgos.pdf*

2D. *Declaración de aplicabilidad (SoA) - Controles implementados (Vigencias 2024 y 2025). La Entidad no cuenta aún con este documento. Actualmente se encuentra en proceso de construcción, en aplicación del principio de progresividad que orienta la implementación del MSPI en la RMBC.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Falta de formalización, control documental y Declaración de Aplicabilidad (SoA) en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información presenta un desarrollo metodológico alineado con el lineamiento del MSPI y con el marco ISO/IEC 27001; sin embargo, no se evidencia la adopción formal por parte del Comité Institucional de Gestión y Desempeño, ni la Declaración de Aplicabilidad (SoA) que relacione los controles adoptados y su estado de implementación.

Adicionalmente, el documento no cuenta con control de cambios, versión, fecha de emisión ni firmas de aprobación, lo que impide establecer su trazabilidad, vigencia y validación oficial por las instancias competentes.

Tampoco se identifican registros de aceptación formal de los riesgos residuales por parte de los dueños de proceso.

Recomendación de la Oficina de Control Interno:

Incluir control documental (fecha, número de versión, control de cambios y firmas de aprobación) conforme a las directrices del Sistema de Gestión Documental Institucional, garantizando trazabilidad y validez del plan.

Formalizar la aprobación del Plan de Tratamiento de Riesgos mediante acta o resolución del Comité Institucional de Gestión y Desempeño, con registro de la fecha y firmas de aprobación.

Finalizar y aprobar la Declaración de Aplicabilidad (SoA), documentando los controles implementados, su estado, y las exclusiones justificadas conforme a los riesgos identificados.

Documentar la aceptación de riesgos residuales por parte de los dueños de riesgo o líderes de proceso, garantizando trazabilidad y coherencia con la política de gestión de riesgos.

Mantener el plan actualizado y publicado antes del 31 de enero de cada vigencia, integrándolo al marco del MSPI y del MIPG[2].

5.2.9. Competencia, toma de conciencia y comunicación

Lineamiento: 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.
- 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.

[2] Lo anterior, tiene soporte en el memorando interno No. CI-20250304-321 y en la respuesta emitida por la Oficina Asesora de Planeación Institucional mediante memorando No. CI-20250815-992 en atención de la solicitud realizada por la Oficina de Control Interno mediante memorando No. CI-20250811-971 del día 11 de agosto de 2025 (auditoría al Sistema de Control Interno vigencia 2025).

- 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.

Propósito: 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.

Salidas:

- 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.
- Plan de comunicaciones del modelo de seguridad y privacidad de la información

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No. 5A y 5B.

Respuesta: ***A.*** *El día 26 de septiembre la oficina adelantará la sensibilización en la política de seguridad y privacidad de la información, esta capacitación se encuentra agendada desde el 9 de septiembre. Dicha evidencia se encuentra en el repositorio.*

B. *Dentro del proceso contratación en obligaciones generales los contratos cuentan con la cláusula 9 que especifica "guardar la debida confidencialidad y reserva sobre la información y documentos que por razón de este contrato llegare a conocer", se dejan evidencia de lo propio en el repositorio.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Falta de formalización del plan institucional de capacitación y comunicación en seguridad y privacidad de la información, y cláusulas contractuales con alcance limitado

Se evidencia una acción puntual de sensibilización en la política de seguridad y privacidad y la existencia de una cláusula general de confidencialidad en los contratos.

No obstante, la entidad no cuenta con un plan formal de capacitación, comunicación y concientización aprobado e integrado al Plan Institucional de Capacitación (PIC), ni con un Plan de Comunicaciones que articule las estrategias internas y externas sobre seguridad de la información.

Adicionalmente, la cláusula contractual identificada solo aborda la confidencialidad de forma genérica, sin incorporar obligaciones específicas relacionadas con la

implementación y gestión del MSPI, ni compromisos en materia de protección de datos personales o seguridad digital.

Recomendación de la Oficina de Control Interno:

Diseñar y aprobar un Plan de Capacitación, Sensibilización y Comunicación sobre seguridad y privacidad de la información, articulado con el PIC y con seguimiento semestral.

Definir un Plan de Comunicaciones del Modelo de Seguridad y Privacidad de la Información, identificando mensajes clave, públicos objetivo, responsables, medios y frecuencia.

Ampliar las cláusulas contractuales, incorporando compromisos explícitos relacionados con la seguridad de la información, privacidad y cumplimiento del MSPI, incluyendo sanciones o responsabilidades por incumplimiento y que se establezca un formato de acuerdo de confidencialidad.

Implementar acciones periódicas de sensibilización, que incluyan simulacros o capacitaciones sobre temas prácticos como phishing e ingeniería social.

Establecer indicadores de cobertura y efectividad, midiendo el impacto y alcance de las acciones de concientización, garantizando que el 100% del personal y contratistas reciba formación básica sobre la política, roles y responsabilidades en seguridad y privacidad de la información.

5.2.10. Información documentada

Lineamiento: El modelo de seguridad y privacidad de la información de la entidad debe incluir:

- Información documentada de los lineamientos establecidos.
- Documentos que la entidad considere necesarios para la eficacia del SGSI.
- Reglas claras para crear y actualizar documentos: identificación, formato, soporte, y control de versiones.
- La información documentada debe estar disponible y ser adecuada para su uso, donde y cuando se necesite además de estar adecuadamente protegida

Propósito: Mantener una documentación adecuada para que pueda ser consultada en cualquier momento por las partes interesadas y le permita conocer los detalles del sistema de gestión de seguridad de la información.

Salidas:

- Políticas, manuales, procesos procedimientos guías, entre otros.
- Inventario de activos, matriz de riesgos, planes de tratamiento, declaración de aplicabilidad, proceso de gestión de eventos, vulnerabilidades.

Requerimiento: Aplica con el requerimiento de documentos solicitados para la implementación del MSPI en la entidad.

Observación y/o análisis realizado por la Oficina de Control Interno:

Ausencia de información documentada y control formal de los instrumentos del Modelo de Seguridad y Privacidad de la Información

Durante la verificación se evidenció que la entidad no ha entregado ni formalizado varios de los documentos requeridos como salidas del lineamiento, tales como procedimientos, guías, inventario de activos, matriz de riesgos, proceso de gestión de vulnerabilidades y declaración de aplicabilidad.

Adicionalmente, los documentos disponibles no cuentan con control de cambios, numeración de versión, fechas ni firmas de aprobación, lo que impide establecer su trazabilidad y vigencia.

La carencia de esta documentación limita la operatividad y eficacia del modelo, así como la posibilidad de consulta y verificación por las partes interesadas.

Recomendación de la Oficina de Control Interno:

Elaborar y formalizar la documentación exigida en el marco del MSPI, incluyendo políticas, manuales, metodologías, procedimientos, inventarios, matriz de riesgos, plan de tratamiento, declaración de aplicabilidad y procesos de incidentes y vulnerabilidades.

Implementar un esquema de control documental que contemple numeración de versión, fecha de emisión, control de cambios, responsables y firmas de aprobación.

Centralizar la información documentada del MSPI en un repositorio institucional seguro, accesible y administrado bajo criterios de integridad, disponibilidad y confidencialidad.

Alinear la documentación del MSPI con el sistema de gestión documental institucional, asegurando consistencia con las políticas de calidad, seguridad y transparencia de la entidad.

Nota: Se indicó por parte del proceso que: *"La entidad cuenta según autodiagnóstico, con un puntaje de 42 puntos, y se encuentra en una etapa de planificación"*

5.3. Capítulo: Fases no evaluadas: Operación, Evaluación del Desempeño y Mejora Continua

De acuerdo con la información suministrada por el proceso, la entidad se encuentra actualmente en etapa de planificación, con un puntaje de autodiagnóstico de 42 puntos, lo que evidencia un nivel inicial de madurez en la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI).

Por tal motivo, no se revisaron las Fases 3 (Evaluación del desempeño) y 4 (Mejora continua) del modelo, ya que estas fases dependen de la culminación de los componentes planificados en la Fase 1 (diagnóstico y planeación).

En cuanto a la fase 2 (Operación), teniendo en cuenta que es la fase subsiguiente en el proceso de implementación del MSPI se realiza un análisis de los documentos resultantes de la fase 1 que deben actualizarse, de acuerdo con 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.

No obstante, se formulan observaciones preventivas y recomendaciones orientativas que deben considerarse al iniciar la ejecución y seguimiento de las siguientes fases, conforme a los lineamientos del Documento Maestro del MSPI 2025, los Lineamientos de Gestión de Incidentes, y los Lineamientos de Indicadores de Gestión de Seguridad de la Información del MinTIC

5.3.1. Fase 2 – Operación

Tras concluir la fase de Planeación, es necesario que la Entidad inicie la implementación de los procesos de seguridad de la información que incluye la gestión de activos, gestión de riesgos de la operación, gestión de incidentes, identificación de vulnerabilidades, tratamiento y evaluación de controles.

Los documentos clave que deben generarse 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.

La fase de Operación contempla las siguientes etapas:

- Control y planeación operacional.
- Plan de Tratamiento de Riesgos.
- Definición de indicadores de gestión

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No. 3A y 3B relacionados con la Gestión de activos

Respuesta: *La Entidad, en aplicación del principio de progresividad, se encuentra actualmente adelantando la elaboración del inventario de activos de información, el cual constituye la base para la gestión integral de seguridad y privacidad.*

La RMBC aún no cuenta con la clasificación formal de la información bajo los criterios de confidencialidad, integridad y disponibilidad, dado que este proceso depende directamente de la finalización del inventario de activos de información. Una vez culminado este, se procederá a su clasificación conforme a los lineamientos del MSPI.

Observación y/o análisis realizado por la Oficina de Control Interno:

Debilidades en la gestión del Sistema de Seguridad de la Información derivadas de la inexistencia de un inventario formal y actualizado de activos de información, base fundamental para la gestión de riesgos, el tratamiento de incidentes y la trazabilidad de controles de seguridad y privacidad.

El registro de activos de información constituye la piedra angular sobre el cual se deben implementar:

- Matriz de riesgos de seguridad de la información
- Planes de tratamiento de los riesgos de seguridad de la información

Recomendación de la Oficina de Control Interno:

Teniendo en cuenta que la fase de operación es inmediatamente subsiguiente a la fase de planeación y con base en el numeral 8 del Documento Maestro del MSPI 2025, la entidad deberá, en el corto plazo:

- Elaborar y adoptar mediante acto administrativo el registro de activos de información de acuerdo con los lineamientos establecidos y en cumplimiento del Decreto No. 1081 de 2015, Decreto Único Reglamentarlo del Sector Presidencia de la República, que consagra en su Artículo 2.1.1.5.1 los instrumentos para la gestión de la Información pública, disponiendo que “El sujeto obligado debe actualizar el Registro de Activos de Información de acuerdo con los

procedimientos y lineamientos definidos en su Programa de Gestión Documental". Y en consonancia con el anterior precepto, el artículo 2.1.1.5.2 ibidem señala que "el Registro de Activos de Información, el índice de Información Clasificada y Reservada, el Esquema de Publicación de Información y el Programa de Gestión Documental, deben ser adoptados y actualizados por medio de acto administrativo".

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.2A relacionado con la Gestión del riesgo y particularmente con la matriz de riesgos de seguridad y privacidad de la información.

Respuesta: *Matriz de riesgos de seguridad y privacidad de la información (Vigencias 2024 y 2025 Actualmente, la Entidad se encuentra adelantando el levantamiento de la matriz de activos de información, insumo necesario para la identificación, tratamiento y evaluación de los riesgos asociados.*

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.2B y 2C relacionado con la Gestión del riesgo y particularmente con la matriz de vulnerabilidades y plan de tratamiento asociado.

Respuesta: *Matriz de vulnerabilidades y plan de tratamiento asociado (Vigencias 2024 y 2025). La Entidad tiene identificadas vulnerabilidades relacionadas con ataques cibernéticos a través de la red de comunicaciones de la RMBC. Dichos hallazgos se encuentran documentados en el repositorio institucional, junto con el plan de tratamiento asociado. (compréndase como el conjunto de herramientas comunicativas de la RMBC). Dicho documento se encuentra en el repositorio.*

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.10A relacionado con la Gestión de incidentes y particularmente con el reporte de incidentes de seguridad de la información.

Respuesta: *La oficina adelanta a través de microsoft defender, los incidentes reportados, a la fecha y 6 meses hacia atrás, también saca el reporte de manera mensual. Dicho documento se encuentra en el repositorio.*

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.2D relacionado con la Gestión del riesgo y particularmente con la Declaración de aplicabilidad (SoA) – Controles implementados.

Respuesta: *La Entidad no cuenta aún con este documento. Actualmente se encuentra en proceso de construcción, en aplicación del principio de progresividad que orienta la implementación del MSPI en la RMBC.*

Observación y/o análisis realizado por la Oficina de Control Interno:

Nuevamente, teniendo en cuenta que la fase de operación es inmediatamente subsiguiente a la fase de planeación y con base en el numeral 8 del Documento Maestro, resulta importante que la Entidad obtenga avances relevantes en la construcción de la documentación de acuerdo con las siguientes recomendaciones.

Recomendación de la Oficina de Control Interno:

- Implementar la matriz de riesgos de SPI que contenga como mínimo la identificación de los riesgos, los controles y las actividades necesarias para el tratamiento.
- Estructurar el plan de tratamiento de riesgos de SPI evidenciando la implementación de los controles de seguridad y privacidad de la información, las evaluaciones a los riesgos a intervalos planificados o cuando se propongan u ocurran cambios significativos
- Adoptar procedimientos formales de gestión de incidentes, conforme al documento “Lineamientos de Gestión de Incidentes de Seguridad de la Información y Seguridad Digital” (2025), incluyendo:
  - Creación y formalización del Equipo de Respuesta a Incidentes.
  - Elaboración del Plan de Respuesta a Incidentes, con fases de detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.
  - Registro y reporte oportuno de incidentes al COLCERT/CSIRT Gobierno, según la Resolución 500 de 2021.
- Establecer controles operativos para acceso lógico, continuidad, protección de infraestructura y monitoreo de vulnerabilidades.
- Implementar los controles definidos en la Declaración de Aplicabilidad (SoA) y asegurar su trazabilidad frente a los riesgos priorizados.

Requerimiento realizado por la Oficina de Control Interno en etapa de ejecución de la auditoría: A través del No.1G relacionado con Gobierno y Estrategia 2024-2025 y en particular la matriz de indicadores de gestión.

Respuesta: *La Entidad cuenta con la documentación de indicadores de gestión, alineados al MSPI. No obstante, atendiendo al principio de gradualidad, su medición y aplicación práctica iniciará en la vigencia 2026.si por. (sic) Dicho documento se encuentra en el repositorio.*

Recomendación de la Oficina de Control Interno:

Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información.

5.3.2. Fase 3 – Evaluación del Desempeño

Conforme al numeral 9 del MSPI 2025 y los Lineamientos de Indicadores de Gestión de Seguridad de la Información, la entidad deberá:

- Definir e implementar indicadores de gestión y cumplimiento que midan:
  - Efectividad de los controles de seguridad.
  - Cumplimiento del plan de sensibilización y políticas de seguridad.
  - Cobertura del SGSI sobre los activos de información.
  - Eficiencia en el tratamiento de incidentes y monitoreo de vulnerabilidades.
- Asegurar que los resultados de la medición sean analizados por el Comité Institucional de Gestión y Desempeño y comunicados a la alta dirección.

5.3.3. Fase 4 – Mejora Continua

De acuerdo con el numeral 10 del Documento Maestro del MSPI, se deberá:

- Implementar un plan de mejora del modelo, basado en los hallazgos de auditoría, resultados de indicadores y lecciones aprendidas de incidentes.
- Establecer acciones correctivas y preventivas documentadas, asignando responsables y plazos de ejecución.
- Mantener un ciclo PHVA (Planear – Hacer – Verificar – Actuar) en la gestión de seguridad, garantizando la sostenibilidad del modelo.
- Evaluar la pertinencia de actualizar políticas, controles y procedimientos de acuerdo con los cambios tecnológicos o normativos.

Si bien las fases de Operación, Evaluación y Mejora no fueron objeto de revisión durante la presente auditoría, se considera necesario que la entidad planifique y documente desde ahora las estrategias, recursos y cronogramas para su implementación, asegurando coherencia con los documentos del MinTIC y el MSPI 2025.

Su ejecución permitirá pasar del cumplimiento inicial a una gestión efectiva, medible y sostenible de la seguridad y privacidad de la información.

5.4. Lineamientos de seguridad de la información para el uso de servicios en la nube

Frente a la solicitud efectuada por la Oficina de Control Interno relacionada con:

a) Políticas de uso aceptable de equipos y servicios TI,

b) Procedimientos de gestión de cambios, parches y vulnerabilidades

c) Procedimientos de respaldo y recuperación con evidencias de pruebas realizadas

El proceso manifestó lo siguiente:

a. *"La RMBC no cuenta aún con procedimientos formalizados para la gestión de copias de respaldo de la información. Es importante precisar que la Entidad tiene contratados servicios de nube privada y nube pública, a través de los cuales se ejecutan los sistemas desarrollados a la fecha, y son estos los que garantizan actualmente el respaldo y disponibilidad de la información.*

Adicionalmente, esta Oficina ha dispuesto respaldos locales en los equipos de cómputo de los funcionarios y en los servidores de desarrollo, como medida complementaria de protección. En aplicación del principio de progresividad, para la vigencia 2026 se proyecta la formalización del Plan de Respaldo y Recuperación de Información, el cual incluirá periodicidad de copias, mecanismos de resguardo, almacenamiento seguro y procedimientos de restauración."

b. *"La RMBC no cuenta con un procedimiento formalizado para la gestión de cambios, aplicación de parches y vulnerabilidades. En lo que respecta a la gestión de cambios, se precisa que la única aplicación desarrollada a la fecha es la página web institucional. Para cualquier modificación en esta plataforma, se implementa el procedimiento de Request For Change (RFC), que permite documentar la solicitud, evaluar el impacto, autorizar su ejecución y dar trazabilidad al cambio realizado. En cuanto a la gestión de vulnerabilidades, se tiene documentada una primera matriz de vulnerabilidades y plan de tratamiento asociado, disponible en el repositorio institucional, la cual se ha venido alimentando con los hallazgos derivados de las pruebas de seguridad y rendimiento realizadas sobre la página web. Por último, en materia de gestión de parches, los equipos y sistemas desplegados en nube privada y nube pública reciben actualizaciones periódicas de seguridad aplicadas directamente por los fabricantes, mientras se define un procedimiento interno que permita documentar, registrar y dar trazabilidad a esta actividad."*

c. La entidad opera actualmente con una infraestructura en la nube lo que permite

que sus repositorios estén en servidores de AZURE principalmente o en contratación de proveedores SAAS como lo es Microsoft a través de SharePoint, frente a Azure, se deja la evidencia en el repositorio de los backups generados.

Observación y/o análisis realizado por la Oficina de Control Interno:

Si bien la entidad informó que actualmente los sistemas operan sobre una infraestructura en la nube (Azure y Microsoft SharePoint) y que los proveedores garantizan los respaldos y actualizaciones de seguridad, se evidencia que no existen procedimientos formalizados que definan la gestión institucional de copias de respaldo, restauración, aplicación de parches, ni tratamiento de vulnerabilidades, conforme a lo establecido en los Lineamientos de seguridad de la información para el uso de servicios en la nube.

Dicho lineamiento establece que, aun cuando los servicios sean provistos por terceros, la responsabilidad de la seguridad de la información es compartida, y corresponde al cliente (en este cao la RMBC) implementar controles y políticas internas que aseguren la protección, disponibilidad y recuperación de los datos, la gestión de vulnerabilidades, y la supervisión de los proveedores en relación con los acuerdos de nivel de servicio (ANS)

La ausencia de documentación formal del Plan de Respaldo y Recuperación, del Procedimiento de Gestión de Cambios y del Procedimiento de Gestión de Vulnerabilidades, limita la trazabilidad y supervisión institucional sobre los servicios en la nube, y dificulta evidenciar el cumplimiento de los principios de responsabilidad compartida, continuidad del negocio, y protección de la información definidos por el MinTIC.

Recomendación de la Oficina de Control Interno:

- Formalizar el Plan de Respaldo y Recuperación de Información, estableciendo:
  - Periodicidad de copias y mecanismos de almacenamiento seguro.
  - Procedimientos de restauración y validación de efectividad mediante pruebas periódicas.
  - Roles, responsables y medidas de seguridad aplicables a servicios en la nube y respaldos locales.
- Documentar el Procedimiento de Gestión de Cambios, Parches y Vulnerabilidades, garantizando:

- Registro, análisis y trazabilidad de los cambios implementados en aplicaciones y servicios cloud.
- Evaluación de impacto y aprobación previa.
- Registro de vulnerabilidades detectadas, y plan de tratamiento asociado.

- Definir mecanismos de supervisión a proveedores cloud, asegurando que:

  - Los acuerdos de nivel de servicio (ANS) incluyan compromisos sobre respaldo, seguridad y restauración.
  - Se cuente con evidencia documental de las actualizaciones y parches aplicados.
  - Se evalúe periódicamente la efectividad de los controles de seguridad implementados por el proveedor.

6. Cumplimiento de las Normas Internacionales de Auditoría, limitaciones, conflictos de interés y fortalezas evidenciadas.

Para la realización de este seguimiento, se aplicaron las Normas de Auditoría Generalmente Aceptadas en Colombia, teniendo en cuenta que las pruebas realizadas se efectuaron mediante muestreo selectivo, por consiguiente, no se cubrió la verificación de la efectividad de todas las medidas de control del proceso.

Aunado a lo anterior, se precisa que, durante el desarrollo, no se presentaron limitaciones, así como tampoco, se dio lugar a la presentación de conflicto de intereses que pudieran afectar o impedir su desarrollo y resultado.

Se precisa además que, debido a las limitaciones de cualquier estructura de Control Interno, pueden ocurrir errores e irregularidades que no hayan sido detectadas bajo la planeación y realización de la presente auditoría, es así como la Región Metropolitana Bogotá – Cundinamarca y las dependencias que la integran, son las responsables de establecer y mantener un adecuado Sistema de Control Interno y prevenir posibles irregularidades, de acuerdo con lo establecido en el Modelo Integrado de Planeación y Gestión -MIPG-.

De acuerdo con la entrada de funcionamiento de la Región Metropolitana Bogotá-Cundinamarca, las competencias de las dependencias se han venido asumiendo de manera gradual conforme a las capacidades de índole técnica y financiera de cada una de ellas, en consonancia con lo establecido en la Ley 2199 de 2022 articulo 5 numeral 6, en su artículo 9 y 10; y lo consagrado en el Acuerdo Regional 001 de 2022 en su artículo 4.

Se indica además que se tuvo en cuenta lo señalado en el concepto emitido por el Departamento Administrativo de la Función Pública No. 20256000283531 de fecha 27/06/2025 del que destacamos:

> *"(…) Ahora bien, en cuanto al principio de gradualidad, el numeral 6 del artículo 5 de la Ley 2199 de 2022 establece: "6. Gradualidad. La Región Metropolitana Bogotá – Cundinamarca se desarrollará bajo el principio de gradualidad, en los términos en que se adopten las decisiones y actos necesarios por parte de las autoridades de las entidades territoriales integrantes."*
>
> *En este sentido, el principio de gradualidad debe analizarse a la luz de la situación jurídica para la cual se plantea y en este caso, es para la implementación y operación de la RMBC; en tal sentido, se logra entender que la gradualidad se genera a razón del avance, un proceso en el cual entidades territoriales con interés de asociarse deben o deberán, adoptar los actos administrativos y decisiones correspondientes, tales como su adhesión formal, la expedición de estatutos, la conformación de su estructura organizacional, la definición de competencias, entre otros. (SIC)*
>
> *(…) 2. De manera que, en concepto de este Departamento Administrativo, la RMBC se ubica dentro del orden territorial, con un régimen especial que exige la adopción de medidas institucionales progresivas, conforme al principio de gradualidad previsto en la Ley 2199 de 2022. (…)" (Negrilla fuera del texto)*

Actualmente la Entidad bajo el principio de gradualidad, antes mencionado, se encuentra en proceso de implementación o construcción del mapa de riesgos[3].

A la fecha del seguimiento la Región Metropolitana Bogotá -Cundinamarca, no cuenta con planes de mejoramiento resultantes de auditorías internas – Plan de Mejoramiento por Procesos- PMP y/o externas- Plan de Mejoramiento Institucional- PMI, sobre la materia de la presente auditoría.

[3]Lo anterior, tiene además soporte en la respuesta emitida por la Oficina Asesora de Planeación Institucional mediante memorando No. CI-20250815-992 en atención de la solicitud realizada por la Oficina de Control Interno mediante memorando No. CI-20250811-971 del día 11 de agosto de 2025. (auditoría al Sistema de Control Interno vigencia 2025).

7. Conclusiones: Observaciones y/o Recomendaciones

Una vez adelantadas las etapas de planeación y ejecución de la auditoría, se precisa que, teniendo en cuenta que la entidad se encuentra actualmente en la fase de Planeación del Modelo de Seguridad y Privacidad de la Información (MSPI) y que su implementación es de carácter gradual y progresivo, no se formularon hallazgos de auditoría.

No obstante, en el desarrollo de la auditoría se identificaron situaciones y aspectos susceptibles de fortalecimiento, frente a los cuales se formularon las observaciones y recomendaciones orientadas a apoyar la adecuada implementación y madurez del modelo.

En este sentido, es pertinente precisar que:

I. Las observaciones, son banderas rojas para el proceso, que buscan que la Entidad analice dichas circunstancias evidenciadas en la auditoría, con el fin de evaluar la necesidad de adoptar y/o fortalecer puntos de control y/o implementar acciones; sin embargo, se aclara que estas no están llamadas a establecerse Plan de Mejoramiento[4] y;

II. Las recomendaciones no están llamadas a establecer Plan de Mejoramiento, pero se invita a que sean evaluadas por el Líder del Proceso con el fin de ser tenidas en cuenta en la Entidad para generar oportunidades de mejora al proceso.

Se precisa que mediante memorando CI-20251017-1286 el día 17 de octubre de 2025, la Oficina de Tecnologías de la Información y las comunicaciones remitió respuesta del informe preliminar de la presente auditoría en la cual se manifestó: *"(…) se acatan en su totalidad las once (11) observaciones formuladas, comprendiendo su importancia para el fortalecimiento institucional y la adecuada implementación del Modelo de Seguridad y Privacidad de la Información (MSPI)"* en ese sentido a continuación se señalan los resultados del ejercicio de evaluación independiente:

OBSERVACIONES Y RECOMENDACIONES

Observación No. 1 Respecto de la Fase de Diagnostico:

Se evidenciaron inconsistencias y vacíos de diligenciamiento que afectan la completitud del instrumento y su utilidad como insumo para la planificación:

[4] Se plantea como observación, teniendo en cuenta el principio de gradualidad de que trata el articulo 5 numeral 6, articulo 9 y 10 de la ley 2199 de 2022 y el Acuerdo Regional 001 de 2022 articulo 4, con el fin de generar oportunidades de mejora al proceso.

- En la hoja “Levantamiento de Información”, las columnas “Nombre del Documento Entregado” y “Observaciones” no se encuentran diligenciadas, lo cual impide conocer el estado real de los documentos que soportan cada control y limita la verificación del cumplimiento.
- En las hojas de dominios (Organizacionales, Personas, Físicos y Tecnológicos) se evidencian avances en los campos de “Evidencia” y “Nivel de Cumplimiento”, sin embargo:
    - La columna “Brecha” se encuentra vacía en ciertos casos, ya que se observó solo el diligenciamiento en los casos aislados.
    - La columna “Recomendación” no se encuentra diligenciada.
    - No se presenta consolidado de brechas ni plan de acciones de mejora derivado del autodiagnóstico (con responsables, plazos y prioridades).

En consecuencia, aunque la herramienta permite identificar el estado de madurez y aporta información preliminar sobre el avance institucional, no cumple plenamente con la salida exigida por el lineamiento, que requiere la identificación de brechas y acciones de mejora como base para la planificación.

Esta situación limita la capacidad de la Entidad para planificar adecuadamente la siguiente fase de implementación del MSPI y fortalecer su nivel de madurez en seguridad y privacidad de la información.

Recomendación de la Oficina de Control Interno:

Completar los campos faltantes en la hoja “Levantamiento de Información”, registrando el nombre del documento soporte y observaciones que evidencien su existencia o ausencia, asegurando trazabilidad documental.

Diligenciar las columnas “Brecha” y “Recomendación” en cada dominio, identificando claramente los aspectos no cumplidos o parcialmente implementados y las acciones necesarias para su cierre.

Consolidar las brechas y acciones de mejora, definiendo responsables, plazos, prioridad e indicador de avance, que sirva como insumo directo para el Plan de Implementación MSPI.

Alinear los resultados del autodiagnóstico con el Plan de Implementación, priorizando los dominios con menor nivel de madurez y estableciendo acciones de mejora progresivas conforme con lo definido en los lineamientos del MinTIC.

Este documento debe consolidar la información de toda la entidad y servir como insumo para la planificación y el mejoramiento continuo.

FASE DE PLANEACIÓN.

Observación No. 2: Debilidad en la identificación y análisis de las necesidades y expectativas de las partes interesadas en materia de seguridad y privacidad de la información.

se identificó que no se ha adelantado el proceso de identificación y análisis de las partes interesadas internas y externas que puedan influir o verse afectadas por la seguridad y privacidad de la información. No se han elaborado documentos que permitan reconocer las necesidades, expectativas o requisitos legales, reglamentarios y contractuales asociados al MSPI.

La ausencia de este análisis impide conocer los actores clave, sus intereses, y los requerimientos que deberían integrarse al sistema de gestión de seguridad y privacidad de la información.

Esta situación limita la capacidad institucional para alinear las acciones del MSPI con el contexto interno y externo de la entidad, y afecta la planificación de estrategias de seguridad acordes a las expectativas de las partes interesadas.

Recomendaciones de la Oficina de Control Interno

Realizar la identificación y análisis de las partes interesadas internas y externas que inciden en la gestión de la seguridad y privacidad de la información.

Documentar las necesidades, expectativas y requisitos de cada parte interesada, incluyendo aspectos legales, reglamentarios, contractuales y técnicos.

Integrar el análisis realizado al Plan de Implementación del MSPI, garantizando su coherencia con el contexto y misión de la entidad.

Socializar y actualizar periódicamente el análisis, considerando cambios en el entorno institucional, proveedores, contratistas o disposiciones normativas.

Observación No. 3: Debilidades en la formulación del alcance del MSPI en el Plan de Implementación 2025.

En el documento denominado “Plan de Implementación del MSPI 2025” se establece un alcance amplio que incluye todos los procesos misionales, estratégicos y de apoyo, así como sistemas de información, activos físicos y digitales, funcionarios, contratistas y terceros

Sin embargo, se identifican las siguientes debilidades:

- No se presenta una delimitación clara ni una aplicabilidad específica del MSPI frente al modelo de operación por procesos de la entidad.
- No se identifica los procesos priorizados ni su nivel de exposición a riesgos de seguridad y privacidad.
- No se incorporan las entradas recomendadas, tales como el modelo de procesos, el catálogo de servicios tecnológicos, el presupuesto disponible o el contexto organizacional.
- No se detallan los activos de información, software, hardware, roles y áreas seguras que serán protegidos bajo el MSPI.
- El documento carece de formalización y control documental, ya que no presenta número de versión, fecha de emisión, control de cambios, firmas de aprobación ni trazabilidad del proceso de validación por parte del Comité Institucional de Gestión y Desempeño.

La ausencia de una definición precisa y delimitada puede generar ambigüedades en la implementación del MSPI, dificultando la trazabilidad de los procesos cubiertos, la asignación de responsabilidades y la identificación de brechas específicas en seguridad y privacidad de la información.

Recomendaciones de la Oficina de Control Interno

- Ajustar y complementar el alcance del MSPI definiendo de manera específica:
    - Los límites y la aplicabilidad del modelo frente al mapa de procesos institucional.
    - Los procesos priorizados, con base en su nivel de exposición a riesgos.
    - Los activos de información, roles, sistemas y áreas seguras que se encuentran dentro del alcance.
- Incorporar como insumos documentales el modelo de procesos, modelo organizacional, catálogo de servicios tecnológicos, presupuesto y contexto de la entidad, conforme al lineamiento 7.1.3.
- Formalizar el documento mediante control de versiones, fecha de emisión, control de cambios y firma de aprobación de la Jefatura de la Oficina TIC y Comité de Gestión y Desempeño Institucional.
- Publicar la versión aprobada en un repositorio institucional, garantizando que esté disponible y actualizada para consulta de las partes interesadas.
- Mantener trazabilidad documental en el proceso de actualización del Plan de Implementación del MSPI, documentando los cambios y versiones posteriores en el pie de control del archivo.

Observación No. 4: Falta de designación expresa del responsable de seguridad de la información como miembro permanente del Comité Institucional de Gestión y Desempeño.

En la Resolución No.332 del 9 de septiembre de 2024, se crea formalmente el Comité Institucional de Gestión y Desempeño y se asignan funciones relativas a la implementación de políticas en materia de seguridad digital y de la información (Art. 17, numeral 6). Asimismo, se incluye como integrante al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC), quien lidera las políticas de Gobierno Digital y Seguridad Digital.

No obstante, el acto administrativo no designa expresamente al "responsable de seguridad de la información" como miembro permanente del Comité, como lo establece el lineamiento del MSPI.

Aunque el jefe de OTIC podría ejercer dicho rol en la práctica, su falta de designación formal constituye una debilidad normativa y de trazabilidad en el cumplimiento del lineamiento, al no existir evidencia documental que acredite su nombramiento como responsable directo del MSPI ante el Comité.

Recomendación

Se recomienda ajustar la Resolución 332 o emitir un acto administrativo complementario que:

- Designe explícitamente al responsable de seguridad de la información – Oficial de Seguridad- o al Jefe de la OTIC en tal calidad como miembro permanente del Comité Institucional de Gestión y Desempeño, conforme al lineamiento MinTIC.
- Refuerce la trazabilidad del liderazgo y la responsabilidad institucional en la adopción, implementación y mejora continua del modelo.

Observación No. 5: Debilidad en la formalización e integración de los roles y responsabilidades del MSPI

La matriz de roles y responsabilidades evidencia avances en la definición de funciones y asignación de tareas, coherentes con los lineamientos generales del MSPI.

Sin embargo, presenta debilidades en cuanto a la formalización de la dependencia organizacional del responsable del MSPI, la acreditación de su participación con voz y voto en los comités institucionales, y la inclusión explícita de los líderes de proceso en la gestión de riesgos de seguridad y privacidad.

Asimismo, el documento no cuenta con fecha, versión, control de cambios ni firmas de aprobación, lo que afecta la trazabilidad documental, la validez formal y la garantía de vigencia del instrumento.

Tampoco se evidencia la inclusión de actores institucionales clave (Oficina Jurídica, Talento Humano, Oficial de Datos Personales) que forman parte de los roles previstos en los lineamientos del MinTIC ("Lineamientos de Roles y Responsabilidades").

Recomendaciones de la Oficina de Control Interno:

Formalizar la matriz de roles y responsabilidades incluyendo la fecha de elaboración, número de versión, control de cambios, firmas de aprobación y validación por parte de la alta dirección o Comité Institucional.

Emitir un acto administrativo complementario para dejar constancia formal de la designación del responsable del MSPI, en donde su participación deberá ser con voz y voto en el Comité Institucional y con voz en el Comité de Control Interno.

Actualizar la matriz para incorporar a los líderes de los procesos como responsables directos de la gestión de riesgos de seguridad y privacidad tales como Oficina Jurídica, Talento Humano y Oficial de Protección de Datos Personales.

Anexar la matriz como documento de referencia dentro del Plan de Implementación del MSPI o el Manual de Seguridad y Privacidad de la Información, garantizando su trazabilidad.

Observación No. 6: Ausencia de inventario consolidado y clasificación formal de los activos de información e infraestructura crítica cibernética.

La entidad se encuentra en fase inicial de implementación del proceso de identificación y clasificación de activos de información, sin contar aún con un inventario consolidado ni con la clasificación de los activos bajo los criterios de confidencialidad, integridad y disponibilidad.

Tampoco se evidencia la inclusión de los activos que contienen información personal ni la identificación de infraestructura crítica cibernética, de acuerdo con lo establecido en los lineamientos del MinTIC 2025.

La falta de un inventario completo y clasificado limita la capacidad institucional para priorizar controles, identificar activos críticos, proteger la información sensible y gestionar adecuadamente los riesgos de seguridad y privacidad de la información. Asimismo, impide cumplir con las fases obligatorias de identificación, clasificación, revisión y aprobación definidas en los lineamientos nacionales del MSPI

Recomendaciones de la Oficina de Control Interno:

Formalizar y consolidar el inventario de activos de información incluyendo todos los tipos definidos por el MinTIC: información, hardware, software, servicios, talento humano, instalaciones e infraestructura crítica cibernética.

Validar y aprobar la matriz de activos por parte de los propietarios y custodios de cada proceso, así como por el Comité Institucional de Gestión y Desempeño, según lo dispuesto en el Decreto 1083 de 2015 modificado por el Decreto 1499 de 2017.

Desarrollar y documentar la metodología de clasificación, aplicando los criterios de confidencialidad, integridad y disponibilidad y los niveles de impacto alto, medio o bajo, según el documento MinTIC 2025

Identificar los activos con información personal y sensible, garantizando su tratamiento conforme a la Ley 1581 de 2012, la Ley 1712 de 2014 y el Decreto 103 de 2015.

Definir la periodicidad de actualización del inventario y las condiciones que deben motivar una revisión (nuevos sistemas, cambios organizacionales o tecnológicos).

Etiquetar los activos según su nivel de clasificación y publicar la información aplicable en los medios institucionales, asegurando la anonimización de los datos que lo requieran.

Asegurar trazabilidad documental del inventario mediante control de versiones, fecha, firma de aprobación y registro de actualizaciones.

Observación No. 7: Ausencia de metodología y proceso formal de valoración de los riesgos de seguridad y privacidad de la información

La entidad no ha desarrollado ni implementado el proceso de valoración de riesgos de seguridad y privacidad de la información**.** Actualmente se encuentra en una fase preparatoria orientada al levantamiento del inventario de activos, sin que existan metodologías, instrumentos o matrices que permitan identificar, valorar o priorizar riesgos asociados a la confidencialidad, integridad, disponibilidad o privacidad de la información.

Esta situación contraviene los numerales 3.1.8 al 3.1.13 del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas del MinTIC, que establecen la obligación de definir criterios de valoración, determinar el apetito y la aceptación del riesgo, y garantizar resultados consistentes, válidos y comparables en el tiempo

La ausencia de este proceso impide identificar amenazas y vulnerabilidades, asignar propietarios de riesgo, priorizar controles y evaluar su efectividad, afectando la capacidad institucional para gestionar adecuadamente los riesgos digitales y de seguridad de la información.

Recomendación de la Oficina de Control Interno:

Teniendo en cuenta que actualmente la entidad no cuenta con un instrumento o metodología para la gestión de riesgos se recomienda:

Documentar una metodología que contemple las etapas de identificación, análisis, evaluación y tratamiento, según lo dispuesto en el numeral 3.1.10 del Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas, incluyendo criterios claros de probabilidad, impacto y niveles de riesgo, definidos en una matriz o escala aprobada por el Comité de Gestión y Desempeño Institucional e incorporar el concepto de riesgo inherente, riesgo residual y riesgo aceptado, garantizando que las valoraciones sean consistentes y comparables en el tiempo.

Incluir un capítulo específico sobre seguridad y privacidad de la información, conforme al numeral 3.1.3 del Lineamientos del Modelo Nacional de Gestión de Riesgo de Seguridad de la Información en Entidades Públicas emitido por el MinTIC. Adicionalmente, se defina el compromiso de la alta dirección con la gestión integral de riesgos digitales y su alineación con el MIPG y el MSPI.

Designar formalmente los dueños de cada riesgo (normalmente los líderes de proceso o los custodios de los activos) y asegurar que estos sean responsables del seguimiento de los controles asociados

Una vez concluido el inventario de activos, aplicar la metodología de valoración sobre cada activo identificado, considerando los criterios de confidencialidad, integridad y disponibilidad, asegurando que los activos críticos cuenten con controles específicos y estén priorizados para su tratamiento.

Definir el apetito de riesgo institucional, diferenciando entre los niveles aceptables y los que deben ser mitigados.

Desarrollar una matriz de riesgos de seguridad y privacidad que incluya entre otras, la descripción del riesgo, el activo afectado, la amenaza y vulnerabilidad, el nivel de riesgo (inherente, residual), el responsable del control, el estado del tratamiento. Esta matriz debería revisarse al menos una vez por año o cada vez que ocurran cambios significativos en los procesos o activos.

Observación No. 8: Falta de formalización, control documental y Declaración de Aplicabilidad (SoA) en el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información presenta un desarrollo metodológico alineado con el lineamiento del MSPI y con el marco ISO/IEC 27001; sin embargo, no se evidencia la adopción formal por parte del Comité Institucional de Gestión y Desempeño, ni la Declaración de Aplicabilidad (SoA) que relacione los controles adoptados y su estado de implementación.

Adicionalmente, el documento no cuenta con control de cambios, versión, fecha de emisión ni firmas de aprobación, lo que impide establecer su trazabilidad, vigencia y validación oficial por las instancias competentes.

Tampoco se identifican registros de aceptación formal de los riesgos residuales por parte de los dueños de proceso.

Recomendación de la Oficina de Control Interno:

Incluir control documental (fecha, número de versión, control de cambios y firmas de aprobación) conforme a las directrices del Sistema de Gestión Documental Institucional, garantizando trazabilidad y validez del plan.

Formalizar la aprobación del Plan de Tratamiento de Riesgos mediante acta o resolución del Comité Institucional de Gestión y Desempeño, con registro de la fecha y firmas de aprobación.

Finalizar y aprobar la Declaración de Aplicabilidad (SoA), documentando los controles implementados, su estado, y las exclusiones justificadas conforme a los riesgos identificados.

Documentar la aceptación de riesgos residuales por parte de los dueños de riesgo o líderes de proceso, garantizando trazabilidad y coherencia con la política de gestión de riesgos.

Mantener el plan actualizado y publicado antes del 31 de enero de cada vigencia, integrándolo al marco del MSPI y del MIPG.

Observación No. 9: Falta de formalización del plan institucional de capacitación y comunicación en seguridad y privacidad de la información, y cláusulas contractuales con alcance limitado

Se evidencia una acción puntual de sensibilización en la política de seguridad y

privacidad y la existencia de una cláusula general de confidencialidad en los contratos.

No obstante, la entidad no cuenta con un plan formal de capacitación, comunicación y concientización aprobado e integrado al Plan Institucional de Capacitación (PIC), ni con un Plan de Comunicaciones que articule las estrategias internas y externas sobre seguridad de la información.

Adicionalmente, la cláusula contractual identificada solo aborda la confidencialidad de forma genérica, sin incorporar obligaciones específicas relacionadas con la implementación y gestión del MSPI, ni compromisos en materia de protección de datos personales o seguridad digital.

Recomendación de la Oficina de Control Interno:

Diseñar y aprobar un Plan de Capacitación, Sensibilización y Comunicación sobre seguridad y privacidad de la información, articulado con el PIC y con seguimiento semestral.

Definir un Plan de Comunicaciones del Modelo de Seguridad y Privacidad de la Información, identificando mensajes clave, públicos objetivo, responsables, medios y frecuencia.

Ampliar las cláusulas contractuales, incorporando compromisos explícitos relacionados con la seguridad de la información, privacidad y cumplimiento del MSPI, incluyendo sanciones o responsabilidades por incumplimiento y que se establezca un formato de acuerdo de confidencialidad.

Implementar acciones periódicas de sensibilización, que incluyan simulacros o capacitaciones sobre temas prácticos como phishing e ingeniería social.

Establecer indicadores de cobertura y efectividad, midiendo el impacto y alcance de las acciones de concientización, garantizando que el 100% del personal y contratistas reciba formación básica sobre la política, roles y responsabilidades en seguridad y privacidad de la información.

Observación No. 10: Ausencia de información documentada y control formal de los instrumentos del Modelo de Seguridad y Privacidad de la Información

Durante la verificación se evidenció que la entidad no ha entregado ni formalizado varios de los documentos requeridos como salidas del lineamiento, tales como procedimientos, guías, inventario de activos, matriz de riesgos, proceso de gestión de vulnerabilidades y declaración de aplicabilidad.

Adicionalmente, los documentos disponibles no cuentan con control de cambios, numeración de versión, fechas ni firmas de aprobación, lo que impide establecer su trazabilidad y vigencia.

La carencia de esta documentación limita la operatividad y eficacia del modelo, así como la posibilidad de consulta y verificación por las partes interesadas.

Recomendación de la Oficina de Control Interno:

Elaborar y formalizar la documentación exigida en el marco del MSPI, incluyendo políticas, manuales, metodologías, procedimientos, inventarios, matriz de riesgos, plan de tratamiento, declaración de aplicabilidad y procesos de incidentes y vulnerabilidades.

Implementar un esquema de control documental que contemple numeración de versión, fecha de emisión, control de cambios, responsables y firmas de aprobación.

Centralizar la información documentada del MSPI en un repositorio institucional seguro, accesible y administrado bajo criterios de integridad, disponibilidad y confidencialidad.

Alinear la documentación del MSPI con el sistema de gestión documental institucional, asegurando consistencia con las políticas de calidad, seguridad y transparencia de la entidad.

FASE OPERACIÓN.

Observación No. 11: Debilidades en la gestión del Sistema de Seguridad de la Información derivadas de la inexistencia de un inventario formal y actualizado de activos de información, base fundamental para la gestión de riesgos, el tratamiento de incidentes y la trazabilidad de controles de seguridad y privacidad.

El registro de activos de información constituye la piedra angular sobre el cual se deben implementar:

- Matriz de riesgos de seguridad de la información
- Planes de tratamiento de los riesgos de seguridad de la información

Recomendación de la Oficina de Control Interno:

Teniendo en cuenta que la fase de operación es inmediatamente subsiguiente a la fase de planeación y con base en el numeral 8 del Documento Maestro del MSPI 2025, la entidad deberá, en el corto plazo:

- Elaborar y adoptar mediante acto administrativo el registro de activos de información de acuerdo con los lineamientos establecidos y en cumplimiento del Decreto No. 1081 de 2015, Decreto Único Reglamentarlo del Sector Presidencia de la República, que consagra en su Artículo 2.1.1.5.1 los instrumentos para la gestión de la Información pública, disponiendo que "El sujeto obligado debe actualizar el Registro de Activos de Información de acuerdo con los procedimientos y lineamientos definidos en su Programa de Gestión Documental". Y en consonancia con el anterior precepto, el artículo 2.1.1.5.2 ibidem señala que "el Registro de Activos de Información, el índice de Información Clasificada y Reservada, el Esquema de Publicación de Información y el Programa de Gestión Documental, deben ser adoptados y actualizados por medio de acto administrativo".
- Implementar la matriz de riesgos de SPI que contenga como mínimo la identificación de los riesgos, los controles y las actividades necesarias para el tratamiento.
- Estructurar el plan de tratamiento de riesgos de SPI evidenciando la implementación de los controles de seguridad y privacidad de la información, las evaluaciones a los riesgos a intervalos planificados o cuando se propongan u ocurran cambios significativos
- Adoptar procedimientos formales de gestión de incidentes, conforme al documento "Lineamientos de Gestión de Incidentes de Seguridad de la Información y Seguridad Digital" (2025), incluyendo:
  - Creación y formalización del Equipo de Respuesta a Incidentes.
  - Elaboración del Plan de Respuesta a Incidentes, con fases de detección, análisis, contención, erradicación, recuperación y lecciones aprendidas.
  - Registro y reporte oportuno de incidentes al COLCERT/CSIRT Gobierno, según la Resolución 500 de 2021.
- Establecer controles operativos para acceso lógico, continuidad, protección de infraestructura y monitoreo de vulnerabilidades.
- Implementar los controles definidos en la Declaración de Aplicabilidad (SoA) y asegurar su trazabilidad frente a los riesgos priorizados.

- Establecer indicadores para medir la gestión y madurez de la entidad en la implementación del modelo de seguridad y privacidad de la información.

Realizó Verificación y Elaboró el informe:

Crhistian Augusto Amador León
Auditor Líder

Revisó y aprobó:

Andrea Reyes Saavedra
Jefe Oficina de Control Interno