Al contestar por favor cite este número
Radicado N° 202601300020453

COMUNICACIÓN INTERNA

Bogotá D.C, Viernes, 18 de Septiembre de 2026

PARA: Liliana Morales
Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - Miembro del Comité Institucional de Coordinación de Control Interno.
Luis Felipe Lota
Director y Presidente del Comité Institucional de Coordinación de Control Interno.
Luis Alberto Colorado Aldana
Jefe de la Oficina de Asesora de Planeación Institucional - Miembro del Comité Institucional de Coordinación de Control Interno.
Ángela Marcela Cárdenas Mora
Jefe de la Oficina Asesora de Comunicaciones y Participación Ciudadana - Miembro del Comité Institucional de Coordinación de Control Interno.
Luz Dary Garzón Guevara
Jefe de la Oficina de Control Disciplinario Interno - Miembro del Comité Institucional de Coordinación de Control Interno.
Gotardo Antonio Yáñez Álvarez
Jefe Oficina Jurídica - Miembro del Comité Institucional de Coordinación de Control Interno.
Henry David Ortiz Saavedra
Subdirector de Gestión Corporativa - Miembro del Comité Institucional de Coordinación de Control Interno.
Gisela Paola Ladrador Araújo
Subdirectora de Planeación Metropolitana y Regional - Miembro del Comité Institucional de Coordinación de Control Interno.
Luis Eduardo Gutiérrez Diaz
Subdirector de Gestión de Proyectos - Miembro del Comité Institucional de Coordinación de Control Interno.

ASUNTO: Informe de la Auditoría de Cumplimiento *"Modelo de Seguridad y Privacidad de la Información (MSPI), gestión de riesgos de seguridad de la información y riesgos asociados a las tecnologías de la información".*

En cumplimiento de lo establecido en la Plan Anual de Auditoría de la vigencia 2026, la Oficina de Control Interno realizó durante los meses de agosto y septiembre de 2026, la auditoría de cumplimiento denominada *"Modelo de Seguridad y Privacidad de la Información (MSPI), gestión de riesgos de seguridad de la información y riesgos asociados a las tecnologías de la información".*

Las conclusiones de la verificación se describen en el numeral 8 del informe que se anexa a la presente comunicación.

Agradecemos el apoyo brindado en el marco de la auditoría y esperamos que los resultados contribuyan a continuar fortaleciendo el Sistema de Control Interno en la Región Metropolitana Bogotá-Cundinamarca.

Finalmente precisamos que (i) Teniendo en cuenta que el sistema de correspondencia SIGMA se encuentra en etapa de desarrollo de acuerdo con la respuesta remitida a la Oficina de Control Interno mediante radicado No. 202604000013383 del 15 de julio de 2026[1], por la Subdirección de Gestión Corporativa[2] se remite al líder del proceso, a fin de que pueda conocer en primera instancia de los resultados y pueda analizar las conclusiones del informe y en informados a los Miembros del Comité Institucional de Coordinación de Control Interno; y,

(ii) Asimismo, el memorando y el informe serán enviados por correo electrónico con el fin de dar cumplimiento a lo dispuesto en el parágrafo No. 1 del artículo 2.2.21.4.7. del Decreto 1083 de 2015[3] y Resolución Regional No. 112 de 2025 *"Por medio de la cual se crea, integra y se establece el reglamento de funcionamiento del Comité Institucional de Coordinación de Control Interno de la Región Metropolitana Bogotá – Cundinamarca"*. Lo anterior, teniendo en cuenta que el Sistema de Correspondencia - SIGMA de la Región Metropolitana Bogotá–Cundinamarca no permite asignar varios usuarios como destinatarios principales, dado que actualmente se encuentra en desarrollo.

Cordialmente,

REYES SAAVEDRA AURORA ANDREA
Firmado digitalmente por REYES SAAVEDRA AURORA ANDREA
Fecha: 2026.09.18 11:43:42 -05'00'

Aurora Andrea Reyes Saavedra
Jefe Oficina de Control Interno
OFICINA DE CONTROL INTERNO

Proyectó: Crhistian Augusto Amador León - OFICINA DE CONTROL INTERNO
Anexo: Documento 1 PDF – Informe Final de auditoría.

[1] Respuesta a las solicitudes elevadas por la Oficina de Control Interno mediante radicados Nos. 202601300012433 y 202601300013033.

[2] Emitido a través del Sistema de Gestión Documental SIGMA.

[3] *"(….) PARÁGRAFO 1. Los informes de auditoría, seguimiento y evaluaciones* ***tendrán como destinatario principal el representante legal de la entidad y el Comité Institucional de Coordinación de Control Interno y/o Comité de Auditoría y/o Junta Directiva****, y deberán ser remitidos al nominador cuando este lo requiera".* (Negrilla fuera del texto).

Oficina de Control Interno

INFORME DE AUDITORÍA DE CUMPLIMIENTO

Modelo de Seguridad y Privacidad de la Información (MSPI), gestión de riesgos de seguridad de la información y riesgos asociados a las tecnologías de la información

Vigencia 2026

Septiembre de 2026

Contenido

1. Objetivo

Evaluar la implementación y operación del Modelo de Seguridad y Privacidad de la Información – MSPI en la Región Metropolitana Bogotá-Cundinamarca, así como la gestión de los riesgos y controles asociados a la seguridad de la información y tecnologías de la información, de acuerdo con los lineamientos y criterios aplicables, el diseño y operación de los controles, y el avance frente a las observaciones y recomendaciones formuladas en la auditoría de la vigencia 2025.

2. Alcance

Evaluar la gestión realizada en la implementación y operación del Modelo de Seguridad y Privacidad de la Información - MSPI en la Región Metropolitana Bogotá-Cundinamarca durante el periodo comprendido entre el 16 de septiembre de 2025 y el 31 de julio de 2026.

La evaluación comprendió las fases de Diagnóstico, Planificación, Operación, Evaluación del Desempeño y Mejora Continua del MSPI; la gestión de los riesgos y controles asociados a la seguridad de la información y tecnologías de la información, incluyendo la revisión de su diseño y operación; y el seguimiento al avance de las once (11) observaciones y recomendaciones formuladas en la auditoría de la vigencia 2025.

3. Criterios Normativos

Los criterios de la auditoría se encuentran sustentados en la siguiente normatividad externa e interna, así como en los lineamientos técnicos aplicables en materia de seguridad y privacidad de la información:

- Ley 87 de 1993, por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015, Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 648 de 2017, por el cual se modifica y adiciona el Decreto 1083 de 2015.
- Resolución 500 de 2021 del Ministerio de Tecnologías de la Información y las

Comunicaciones, por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el Modelo de Seguridad y Privacidad de la Información como habilitador de la Política de Gobierno Digital.

- Resolución 746 de 2022 del Ministerio de Tecnologías de la Información y las Comunicaciones, 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 500 de 2021.
- Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.
- Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información – MSPI, expedido por el Ministerio de Tecnologías de la Información y las Comunicaciones.
- Norma ISO/IEC 27001:2022, Sistemas de gestión de seguridad de la información.
- Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7, expedida por el Departamento Administrativo de la Función Pública, como criterio técnico y metodológico para la evaluación de la gestión de riesgos y el diseño de controles.
- Política de Seguridad Digital, Privacidad de la Información y Datos Personales de la Región Metropolitana Bogotá-Cundinamarca, y demás documentos internos relacionados con la implementación y operación del MSPI.
- Política para la Gestión Integral de Riesgos de la Región Metropolitana Bogotá-Cundinamarca – PL-DES-001, adoptada mediante la Resolución 448 del 22 de diciembre de 2025, como marco institucional para la gestión de riesgos.

Así como las demás disposiciones internas y externas aplicables, consideradas para el cumplimiento del objetivo y alcance de la presente auditoría.

4. Metodología [1]

Para el desarrollo de la auditoría se aplicaron procedimientos de revisión documental, análisis de la información y verificación de los soportes suministrados por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC, con el propósito de obtener evidencia suficiente para evaluar los aspectos definidos en el objetivo y alcance de la auditoría.

La auditoría fue notificada mediante memorando con radicado 202601300015223 del 3

[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

de agosto de 2026, a través del cual la Oficina de Control Interno comunicó el inicio del ejercicio auditor y efectuó la correspondiente solicitud de información. Posteriormente, el 6 de agosto de 2026 se llevó a cabo la reunión de apertura, en la cual se socializaron el objetivo, alcance, criterios, metodología, cronograma y demás aspectos relacionados con el desarrollo de la auditoría.

En atención al requerimiento efectuado, la OTIC remitió respuesta mediante comunicación interna con radicado 202601600016113 del 11 de agosto de 2026, junto con los documentos y soportes dispuestos para atender los diferentes requerimientos de información. A partir de esta documentación se realizó la revisión y análisis correspondiente.

La evaluación se desarrolló considerando los siguientes componentes:

1. Implementación y operación del MSPI: se verificó el cumplimiento de los lineamientos aplicables a las fases de Diagnóstico, Planificación, Operación, Evaluación del Desempeño y Mejora Continua, contrastando los requerimientos establecidos con la documentación y evidencias suministradas.
2. Seguimiento a la auditoría de la vigencia 2025: se verificó el avance frente a las once (11) observaciones y recomendaciones formuladas en la auditoría anterior, determinando para cada una si la situación se encontraba superada, parcialmente superada o persistía, de acuerdo con las acciones adelantadas y los soportes disponibles.
3. Gestión de riesgos y controles de TI: se revisaron los riesgos relacionados con pérdida de información, interrupción de servicios tecnológicos, daño a la infraestructura tecnológica y gestión de accesos privilegiados, considerando su identificación y valoración, así como el diseño y, cuando correspondía, la operación de los controles establecidos. Para este análisis se tomó como referente técnico y metodológico la Guía para la Gestión Integral del Riesgo en Entidades Públicas – Versión 7 del Departamento Administrativo de la Función Pública.

Los resultados de las verificaciones realizadas fueron documentados en los respectivos papeles de trabajo, a partir de los cuales se determinaron las situaciones y recomendaciones presentadas en este informe.

El 7 de septiembre de 2026, la Oficina de Control Interno remitió mediante correo electrónico el informe preliminar de resultados al proceso auditado, para su conocimiento, revisión y presentación de comentarios u observaciones. El 10 de septiembre de 2026, la OTIC remitió, por el mismo medio, sus observaciones frente a los resultados presentados, las cuales fueron analizadas por la Oficina de Control Interno junto con los argumentos y soportes correspondientes.

Como parte del análisis de las observaciones recibidas, el 14 de septiembre de 2026 se realizó una mesa de trabajo entre la Oficina de Control Interno y la OTIC, en la cual se abordaron y aclararon aspectos relacionados con las observaciones formuladas al informe preliminar y se efectuaron verificaciones adicionales sobre los soportes asociados a algunos de los aspectos evaluados. Los resultados de este análisis y de las verificaciones realizadas fueron considerados para la elaboración del informe final.

Finalmente, se desarrolló el 18 de septiembre de 2026, mediante Microsoft Teams, la reunión de cierre de la auditoría, en la cual la Oficina de Control Interno socializó al proceso auditado los resultados finales del ejercicio.

5. Desarrollo del Informe

5.1. Fase de Diagnóstico

La fase de diagnóstico permite establecer el estado actual de implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, mediante la aplicación de la herramienta de autodiagnóstico, a partir de la cual se identifican los controles implementados, el nivel de madurez alcanzado y las brechas existentes. Este ejercicio constituye el punto de partida para orientar la planificación del modelo y, a partir de su actualización posterior a la evaluación del desempeño, permite identificar los avances alcanzados y los aspectos que deben ser fortalecidos como parte del mejoramiento continuo.

Para la vigencia 2026, la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC presentó la Herramienta de Autodiagnóstico del MSPI, mediante la cual evaluó el estado de implementación de los controles e identificó brechas asociadas a los diferentes componentes del modelo. Asimismo, se evidenció que la Entidad cuenta con el Plan Estratégico de Seguridad y Privacidad de la Información – PESI, código PN-TIC-001, versión 2, aprobado por el Comité Institucional de Gestión y Desempeño el 26 de junio de 2026, en el cual se establecieron actividades y un cronograma para avanzar en la implementación del MSPI.

La revisión permitió establecer que la Entidad avanzó frente a la situación evidenciada en la auditoría de 2025, toda vez que actualmente dispone de un nuevo autodiagnóstico, registra las brechas identificadas y cuenta con instrumentos para conocer el estado de implementación y orientar las actividades previstas para la vigencia 2026.

No obstante, en la revisión de la Herramienta de Autodiagnóstico del MSPI se identificaron algunos aspectos que requieren ajuste para asegurar la consistencia y trazabilidad de la información registrada. En particular, se evidenció que la portada del instrumento registra como fecha “jun-26”, mientras que otras hojas presentan la fecha “6 de septiembre de 2026”, posterior al periodo objeto de auditoría.

Asimismo, se identificaron casos en los que la calificación asignada no guarda total correspondencia con la información registrada en el mismo instrumento. Como se observa en la siguiente imagen, el control A.7.13 – Mantenimiento de equipos presenta un nivel de cumplimiento de 100, mientras que en la misma fila se registra como brecha la necesidad de establecer y conservar registros de mantenimiento preventivo y correctivo de los equipos de cómputo e infraestructura tecnológica bajo responsabilidad de la Entidad. En consecuencia, se considera necesario revisar la consistencia entre la calificación asignada y la brecha identificada, teniendo en cuenta que esta última evidencia un aspecto pendiente de fortalecimiento relacionado con el propio control.

Adicionalmente, algunos controles fueron calificados con un nivel de cumplimiento del 100 % utilizando como soporte el M-TIC-004 – Manual de Políticas Complementarias de Seguridad y Privacidad de la Información, documento que al 31 de julio de 2026, fecha de corte de la auditoría, se encontraba en proceso de revisión y aprobación.

Estas situaciones no desconocen la realización del autodiagnóstico ni los avances alcanzados por la Entidad; sin embargo, evidencian la necesidad de revisar la correspondencia entre las calificaciones asignadas, las brechas identificadas y los soportes utilizados para sustentar la evaluación.

Ejemplo de inconsistencia identificada en la Herramienta de Autodiagnóstico del MSPI

COLOMBIA POTENCIA DE LA VIDA — Controles Físicos

ENTIDAD EVALUADA	RMBC
FECHAS DE	6/09/2026
CONTACTO	Jefe OTIC
ELABORADO POR	Liliana Morales

ID.ITEM	CONTROL	ROL	DESCRIPCIÓN	PRUEBA	EVIDENCIA	BRECHA	NIVEL DE CUMPLIMIENTO ANEXO A ISO 27001	RECOMENDACIÓN
F.1.13	A 7.13	Responsable recursos físicos	Mantenimiento de equipos	Se deben considerar las siguientes pautas para el mantenimiento del equipo: a) mantener el equipo de acuerdo con la frecuencia de servicio recomendada por el proveedor y especificaciones; b) implementación y seguimiento de un programa de mantenimiento por parte de la organización; c) solo personal de mantenimiento autorizado que realice reparaciones y mantenimiento en el equipo; d) mantener registros de todas las fallas sospechadas o reales, y de todo mantenimiento preventivo y correctivo; e) implementar controles apropiados cuando el equipo está programado para mantenimiento, teniendo en cuenta si este mantenimiento es realizado por personal en el sitio o externo a la organización; someter al personal de mantenimiento a un adecuado acuerdo de confidencialidad; f) supervisar al personal de mantenimiento al realizar el mantenimiento en el sitio; g) autorizar y controlar el acceso para el mantenimiento remoto) aplicar medidas de seguridad para activos fuera de las instalaciones (ver 7.9) si el equipo que contiene información es sacado de las instalaciones para mantenimiento; i) cumplir con todos los requisitos de mantenimiento impuestos por el seguro; j) antes de volver a poner en funcionamiento el equipo después del mantenimiento, inspeccionarlo para asegurarse de que el equipo no ha sido manipulado y funciona correctamente;	RMBC ejecuta el mantenimiento preventivo y correctivo de la infraestructura tecnológica mediante el P-TIC-001 Gestionar la arquitectura de tecnología - proceso habilitación del cambio, complementado con el Plan de Mantenimiento de TI, el cual permite programar, controlar y hacer seguimiento a las actividades de mantenimiento de la infraestructura tecnológica. Las actividades son ejecutadas por personal autorizado de la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) o por proveedores especializados cuando se requiere soporte externo, dejando trazabilidad de las actividades realizadas y el registro de las actividades programadas en Microsoft Lists. Cuando el mantenimiento implica intervención de terceros, este se realiza bajo supervisión de la Entidad y conforme a los acuerdos contractuales y de confidencialidad aplicables. Evidencias P-TIC-001 Gestionar la arquitectura de tecnología - proceso habilitación del cambio.	Establecer y conservar registros de mantenimiento preventivo y correctivo de los equipos de cómputo e infraestructura tecnológica bajo responsabilidad de la Entidad, como evidencia del adecuado soporte a los servicios de tecnología.	100	N/A

ESCALA DE EVALUACIÓN | LEVANTAMIENTO DE INFO. | ÁREAS INVOLUCRADAS | CLÁUSULAS | ORGANIZACIONALES | PERSONAS | FÍSICOS | TECNOLÓGICOS | NIST

Por otra parte, se verificó que el autodiagnóstico contiene brechas asociadas a los controles evaluados, lo que representa un avance frente a la vigencia anterior. Sin

embargo, con la información revisada no fue posible verificar que todas las brechas identificadas contaran con una acción de cierre claramente definida, acompañada de responsable, fecha estimada de cumplimiento y un mecanismo que permita realizar seguimiento a su avance. En consecuencia, si bien la Entidad cuenta con la identificación de las brechas, se requiere fortalecer la forma en que estas se convierten en acciones concretas y verificables para su cierre.

De igual manera, se verificó que la Entidad dispone de instrumentos que permiten conocer el estado de implementación del modelo y orientar las actividades previstas para su fortalecimiento. El PESI presenta el estado general del MSPI, el autodiagnóstico permite identificar su nivel de madurez y las brechas existentes, y el cronograma de implementación contiene las actividades previstas para la vigencia 2026.

En conclusión, la fase de diagnóstico evidencia avances frente a la vigencia anterior, principalmente por la actualización y utilización del autodiagnóstico y la aprobación del PESI. No obstante, se requiere fortalecer la consistencia de la información registrada en el autodiagnóstico y asegurar que las brechas identificadas cuenten con acciones claramente definidas que permitan realizar seguimiento hasta su cierre.

5.2. Fase de Planeación

La fase de planeación establece las condiciones necesarias para la implementación del MSPI, a partir del conocimiento del contexto de la Entidad, las necesidades y expectativas de las partes interesadas, la definición del alcance, los roles y responsabilidades, la gestión de los activos y riesgos de seguridad de la información, así como los demás elementos necesarios para orientar la implementación y operación del modelo.

Para la evaluación de esta fase, la Oficina de Control Interno revisó la información y los soportes suministrados por la OTIC, cuyos resultados se presentan a continuación.

1.2.1. Necesidades y expectativas de las partes interesadas

El MSPI establece la necesidad de identificar las partes interesadas internas y externas, así como sus necesidades, expectativas y requisitos aplicables, de manera que sean consideradas en la planificación del modelo.

Para este aspecto, la OTIC remitió la G-TIC-005 – Guía para la Construcción y Actualización del Contexto Estratégico de TI, versión 1 del 26 de junio de 2026. En la revisión se evidenció que el documento desarrolla el contexto interno y externo e incorpora un apartado específico de Partes Interesadas, en el cual se identifican actores internos y externos y se relacionan sus necesidades o expectativas y los requisitos aplicables al Sistema de Gestión de Seguridad de la Información – SGSI.

Asimismo, la guía establece que las partes interesadas, sus necesidades, expectativas y requisitos deben revisarse como mínimo una vez al año o cuando se presenten cambios normativos, institucionales, tecnológicos, organizacionales o del entorno que puedan afectar el SGSI.

En consecuencia, se evidenció el cumplimiento del lineamiento evaluado, así como la atención de la situación identificada en la Observación No. 2 de la auditoría de 2025, cuyo resultado será presentado en el apartado de seguimiento correspondiente.

1.2.2. Definición del alcance del MSPI

El MSPI establece que la Entidad debe definir los límites y la aplicabilidad del modelo, determinando los procesos y recursos tecnológicos que estarán comprendidos dentro de su implementación.

Para este aspecto, la OTIC informó que el alcance se encuentra definido en el M-TIC-004 – Manual de Políticas Complementarias de Seguridad y Privacidad de la Información. Asimismo, se verificó que el PESI V2 contiene una definición de alcance que comprende sistemas de información, redes, datos, áreas de la Entidad y terceros relacionados, evidenciando una mayor delimitación de la cobertura del modelo frente a lo observado en la vigencia anterior.

No obstante, al 31 de julio de 2026, el M-TIC-004, señalado por la OTIC como el documento en el cual se establece el alcance del MSPI, se encontraba en proceso de revisión por la Oficina Asesora de Planeación, previo a su presentación y aprobación ante el Comité Institucional de Gestión y Desempeño. Por lo anterior, aunque se evidenció la definición del alcance, su formalización mediante el instrumento señalado por la OTIC no había finalizado al corte de la auditoría.

En consecuencia, este aspecto se considera parcialmente cumplido y mantiene relación con la Observación No. 3 de la auditoría de 2025, cuyo estado será presentado en el apartado de seguimiento correspondiente.

1.2.3. Liderazgo y compromiso

El MSPI establece que la Alta Dirección debe demostrar liderazgo y compromiso frente a la seguridad y privacidad de la información, promoviendo su incorporación en la gestión institucional y respaldando las acciones necesarias para la implementación del modelo.

En la revisión se evidenció que la Entidad cuenta con la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales, adoptada mediante la Resolución No. 065 del 4 de marzo de 2025, en la cual se establecen compromisos relacionados

con la protección de la información y se asigna a la Alta Dirección la responsabilidad de proporcionar los recursos necesarios y liderar el cumplimiento de la política.

Asimismo, se evidenciaron acciones para su divulgación, entre ellas la socialización realizada a funcionarios y contratistas de la Entidad, así como avances institucionales asociados a la aprobación y desarrollo de instrumentos para la implementación del MSPI.

En consecuencia, se evidenció el liderazgo y compromiso institucional frente a la implementación del MSPI, por lo que este aspecto se considera cumplido.

1.2.4. Política de Seguridad y Privacidad de la Información

El MSPI establece que la Entidad debe contar con una política que defina los lineamientos y compromisos para proteger la confidencialidad, integridad y disponibilidad de la información, formalmente aprobada y comunicada a quienes corresponda.

Se verificó que la Región Metropolitana Bogotá-Cundinamarca cuenta con la Política de Seguridad Digital, Privacidad de la Información y de Datos Personales, adoptada mediante la Resolución No. 065 del 4 de marzo de 2025. La política establece su ámbito de aplicación, lineamientos para la gestión de riesgos de seguridad digital, revisión periódica y mecanismos para su comunicación.

Asimismo, se evidenció la divulgación de la política mediante jornada de socialización realizada el 26 de septiembre de 2025. En consecuencia, se evidenció la existencia, adopción y divulgación de la política, por lo que este aspecto se considera cumplido.

1.2.5. Roles y responsabilidades

El MSPI establece que la Entidad debe definir y formalizar los roles y responsabilidades necesarios para su implementación, incluyendo la asignación de responsabilidades a las diferentes áreas y la designación del responsable del modelo, de acuerdo con los lineamientos establecidos.

Frente al requerimiento realizado por la Oficina de Control Interno, la OTIC informó que los roles y responsabilidades se encontraban definidos en el numeral 8.1.2 “Roles y responsabilidades” del Manual de Políticas Complementarias de Seguridad y Privacidad de la Información – M-TIC-004, documento que al momento de la respuesta se encontraba en revisión por la Oficina Asesora de Planeación, previo a su presentación y aprobación ante el Comité Institucional de Gestión y Desempeño.

La revisión realizada permitió evidenciar avances en la definición de responsabilidades.

El M-TIC-004 asigna funciones a la OTIC, líderes de proceso, dependencias de apoyo, servidores públicos, contratistas, proveedores y demás usuarios autorizados, e incorpora una matriz RACI para actividades relacionadas con el MSPI, como el autodiagnóstico, la identificación y clasificación de activos, la valoración de riesgos, la implementación de controles, la gestión de incidentes y vulnerabilidades y el seguimiento a las acciones de mejora.

No obstante, al 31 de julio de 2026 no se acreditó la definición y formalización del rol de Responsable de Seguridad de la Información, con sus respectivas funciones y responsabilidades. Adicionalmente, el M-TIC-004, mediante el cual la OTIC venía desarrollando la definición general de roles y responsabilidades frente al MSPI, se encontraba en proceso de revisión y aprobación. En consecuencia, aunque se evidenciaron avances, el requisito específico no se encontraba cumplido al cierre del periodo evaluado, por lo que el criterio se calificó como NO CUMPLE.

La versión posteriormente formalizada del M-TIC-004, con fecha 31 de agosto de 2026, evidencia que la Entidad continuó avanzando en este aspecto; sin embargo, al ser posterior al periodo auditado, no modifica el resultado de la evaluación al 31 de julio de 2026.

1.2.6. Identificación y clasificación de activos de información

La Entidad cuenta con la Metodología y Registro de Activos de Información F-TIC-004, mediante la cual se establecen lineamientos para la identificación, clasificación y valoración de los activos de información. Asimismo, se evidenció el levantamiento de un inventario que contenía 135 activos de información, en el cual se registraron aspectos como el proceso y dependencia responsable, nombre y descripción del activo, tipo, medio de conservación y formato.

Durante la auditoría, la OTIC informó que el inventario se encontraba en proceso de actualización, revisión y validación metodológica por parte de la Oficina Asesora de Planeación, situación que se corroboró mediante correo del 28 de julio de 2026, a través del cual se remitió el Registro de Activos de Información para su revisión y validación.

Frente a lo señalado en el informe preliminar respecto de la clasificación y valoración individual de los activos, la OTIC precisó que el archivo suministrado inicialmente correspondía al Registro de Activos de Información destinado a divulgación y que la valoración detallada se encontraba contenida en una matriz interna. Durante las validaciones efectuadas con posterioridad al informe preliminar, la OTIC presentó dicha matriz a la auditoría, manteniendo restringida la visualización de la información que por razones de seguridad no debía ser expuesta, lo que permitió verificar la existencia del instrumento interno asociado a los 135 activos de información y su estructura para la clasificación y valoración de estos.

No obstante, al 31 de julio de 2026, el proceso de gestión de activos de información aún no había culminado. Al respecto, el PESI V2, aprobado el 26 de junio de 2026, incluyó dentro de su cronograma la actividad “Inventario de Activos + Metodología” para el segundo trimestre de 2026. De igual manera, el cronograma presentado en el Acta CIGD No. 002 del 26 de junio de 2026 para el levantamiento de activos contempló como etapa final la “Presentación y acta de aprobación final del inventario de activos”, bajo responsabilidad del CIGD y la Oficina TIC. Como actuación posterior al periodo evaluado, durante la etapa de validación del informe preliminar se informó y verificó que el inventario fue presentado y aprobado por el Comité Institucional de Gestión y Desempeño el 8 de septiembre de 2026; esta actuación evidencia la culminación posterior del proceso, sin modificar la situación existente al corte de la auditoría (31 de julio de 2026).

En consecuencia, se evidenció un avance importante frente a la vigencia anterior, representado en la definición de la metodología, el levantamiento de los 135 activos de información y la existencia de un instrumento interno para su clasificación y valoración. Sin embargo, al 31 de julio de 2026 el inventario aún se encontraba en proceso de revisión y validación y no había culminado la etapa de aprobación final prevista institucionalmente, la cual se materializó posteriormente, el 8 de septiembre de 2026. Esta situación guarda relación con la Observación No. 6 de la auditoría de 2025, cuyo avance se analiza posteriormente en el presente informe.

1.2.7. Valoración de los riesgos de seguridad de la información

Para la gestión de los riesgos de seguridad de la información, la Entidad informó que cuenta con la Política para la Gestión Integral del Riesgo – PL-DES-001, adoptada mediante la Resolución No. 448 del 22 de diciembre de 2025, en la cual se establecen los lineamientos para la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos, incluyendo los asociados a la seguridad de la información. Asimismo, señaló que para su identificación y valoración se utiliza el formato institucional F-DES-020 – Matriz de Riesgos Institucional.

Adicionalmente, se verificó el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PN-TIC-002, versión 2 del 26 de junio de 2026, el cual establece que la gestión de estos riesgos se realizará de manera articulada con la metodología institucional y contempla la identificación de los riesgos asociados a los activos de información, su análisis y valoración.

Al 31 de julio de 2026, la matriz específica de riesgos de seguridad de la información aún no se encontraba elaborada y aplicada. Esta situación fue informada por la OTIC durante la auditoría y guarda correspondencia con el cronograma institucional definido para su implementación, según el cual las actividades relacionadas con la identificación y evaluación de estos riesgos, incluyendo las mesas de trabajo, el levantamiento de la matriz, su validación y la valoración de los riesgos, se desarrollarían durante el segundo

semestre de 2026. Asimismo, el PESI V2, aprobado el 26 de junio de 2026, contempla la elaboración de la Matriz de Riesgos de Seguridad de la Información durante el tercer y cuarto trimestre de 2026.

En este sentido, se reconoce que al cierre del periodo evaluado la Entidad contaba con una política, una metodología, un instrumento y una planeación definida para adelantar la gestión de los riesgos de seguridad de la información. No obstante, el numeral 7.3.2 del Documento Maestro de Lineamientos del MSPI establece que las entidades deben definir y aplicar un proceso de valoración que permita, entre otros aspectos, identificar y valorar los riesgos que puedan afectar la confidencialidad, integridad, disponibilidad y privacidad de la información, determinar sus niveles y priorizarlos para su tratamiento.

Por lo anterior, al 31 de julio de 2026 se encontraba definida y programada la implementación del proceso de valoración de riesgos de seguridad de la información, pero aún no se había culminado su aplicación para identificar y valorar de manera específica los riesgos asociados a los activos de información. La programación de estas actividades para el segundo semestre de 2026 permite establecer el estado de implementación previsto por la Entidad, sin que ello acredite por sí mismo la aplicación del proceso exigido por el MSPI al cierre del periodo evaluado.

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

La gestión de los riesgos de seguridad de la información requiere que, una vez identificados y valorados los riesgos, la Entidad defina las medidas para su tratamiento, determine el riesgo residual y, cuando corresponda, formalice su aceptación. Asimismo, debe establecer los controles aplicables y realizar seguimiento a la ejecución y efectividad de las medidas definidas.

Frente a estos aspectos, la OTIC remitió el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PN-TIC-002, versión 2, del 26 de junio de 2026, documento que establece las etapas para la identificación, análisis, valoración, tratamiento, monitoreo y evaluación de los riesgos de seguridad de la información. El Plan incorpora además un cronograma para su implementación y articula la gestión de estos riesgos con la metodología institucional de administración del riesgo.

Como se indicó en el numeral anterior, al 31 de julio de 2026 aún no se había culminado la aplicación del proceso de valoración específica de los riesgos de seguridad de la información. En consecuencia, las etapas posteriores asociadas con la determinación del riesgo residual, su aceptación cuando correspondiera y la definición y seguimiento de tratamientos específicos se encontraban igualmente pendientes de desarrollo. De acuerdo con la información suministrada por la OTIC en etapa de socialización del informe, estas actividades se encontraban programadas para ejecutarse durante el segundo semestre de 2026.

En relación con la Declaración de Aplicabilidad – SoA, se evidenció un borrador estructurado con base en los controles de ISO/IEC 27002:2022, en el cual se identifican controles, razones para su selección y evidencias o estado de aplicación. Al cierre del periodo evaluado este instrumento se encontraba en construcción y revisión. Asimismo, el PESI V2, aprobado el 26 de junio de 2026, contempló la elaboración de la Matriz de Riesgos de Seguridad de la Información durante el tercer y cuarto trimestre de 2026 y la Declaración de Aplicabilidad – SoA, en calidad de borrador, para el cuarto trimestre de la vigencia.

En este sentido, se evidenció que la Entidad formalizó el PN-TIC-002 y definió las actividades y el cronograma para desarrollar el proceso de tratamiento de los riesgos de seguridad de la información, así como avances en la construcción de la Declaración de Aplicabilidad. No obstante, al 31 de julio de 2026, la aplicación del proceso de tratamiento aún dependía de culminar previamente la identificación y valoración específica de los riesgos de seguridad de la información. Por lo anterior, al cierre del periodo evaluado permanecían pendientes etapas posteriores como la determinación del riesgo residual, su aceptación cuando correspondiera, la consolidación de la Declaración de Aplicabilidad y el seguimiento de los tratamientos definidos.

1.2.9. Competencia, toma de conciencia y comunicación

La Oficina de Control Interno verificó el Plan de Sensibilización y Comunicación en Seguridad de la Información 2026 – PN-TIC-004, versión 1, aprobado el 26 de junio de 2026, mediante el cual la Entidad estableció las actividades orientadas a fortalecer la cultura de seguridad de la información en servidores públicos, contratistas y colaboradores. El plan define los temas a desarrollar, público objetivo, canales de comunicación, responsables y programación de las actividades, e incorpora acciones relacionadas con prevención de phishing y malware, manejo adecuado de la información, uso seguro de contraseñas y autenticación multifactor, entre otras.

Asimismo, se verificó el expediente virtual 2026160299500002E dispuesto en SIGMA para conservar los soportes de ejecución del plan. Para el periodo objeto de auditoría se evidenciaron actividades desarrolladas durante los meses de abril, mayo, junio y julio de 2026, con soportes asociados a las convocatorias, presentaciones y registros de asistencia. Lo anterior permitió evidenciar que las actividades previstas no se limitaron a su planificación, sino que presentaron ejecución durante el periodo evaluado.

De igual manera, se evidenció que el componente de comunicación se encuentra incorporado en el mismo plan, mediante la definición de canales como charlas presenciales o virtuales, correos institucionales, boletines de seguridad digital, piezas gráficas e intranet, por lo cual no se considera necesaria la existencia de un Plan de Comunicaciones independiente.

En consecuencia, se evidenció que la Entidad cuenta con mecanismos formalizados y en ejecución para la sensibilización y comunicación en seguridad de la información, orientados al fortalecimiento de conocimientos y buenas prácticas de los servidores públicos, contratistas y colaboradores.

1.2.10. Información documentada

El MSPI establece que la Entidad debe contar con la información documentada necesaria para soportar la implementación y operación del modelo, asegurando su identificación, actualización, disponibilidad y adecuado control documental. Entre sus principales salidas se encuentran políticas, manuales, procedimientos, inventario de activos, matriz de riesgos, planes de tratamiento, Declaración de Aplicabilidad y demás instrumentos relacionados con la seguridad de la información.

La revisión realizada permitió evidenciar un fortalecimiento frente a la vigencia 2025. La Entidad cuenta con diferentes instrumentos asociados al MSPI formalizados, codificados y versionados, y mantiene la documentación relacionada con el modelo organizada y disponible a través del Banco de Documentos institucional.

Frente a los productos que al 31 de julio de 2026 aún se encontraban en proceso de elaboración o consolidación, como la matriz específica de riesgos de seguridad de la información y la Declaración de Aplicabilidad – SoA, se verificó que estos hacían parte del proceso de implementación del MSPI y contaban con actividades programadas para etapas posteriores de la vigencia. Su estado de desarrollo se analiza en los numerales correspondientes del presente informe y no constituye, por sí mismo, una deficiencia en los mecanismos de identificación, formalización, versionamiento y control de la información documentada.

En consecuencia, se evidenció que la Entidad fortaleció los mecanismos para la elaboración, formalización, organización y disponibilidad de la documentación asociada al MSPI, por lo que el criterio se califica como CUMPLE. Esta situación se encuentra relacionada con la Observación No. 10 de la auditoría de 2025, cuyo seguimiento se desarrolla posteriormente en el presente informe.

5.3. Fase de Operación

De acuerdo con el Documento Maestro de Lineamientos del MSPI, una vez finalizada la fase de planeación se debe avanzar en la implementación de los procesos de seguridad de la información relacionados, entre otros aspectos, con la gestión de activos, riesgos, incidentes, vulnerabilidades, tratamiento y evaluación de controles. En esta fase, además de contar con los documentos que orientan su ejecución, la Entidad debe disponer de evidencias que permitan verificar la implementación de los controles

de seguridad y privacidad de la información.

Para evaluar el avance de la Región Metropolitana Bogotá–Cundinamarca en esta fase, la Oficina de Control Interno revisó los procedimientos y lineamientos operativos remitidos por la OTIC, así como los soportes relacionados con la gestión de incidentes, vulnerabilidades, respaldos y recuperación, control de accesos, protección de la infraestructura tecnológica, gestión documental y relación con proveedores y terceros.

Como resultado general, se evidenciaron avances frente a la vigencia 2025, principalmente por la formalización de documentos y la disponibilidad de mecanismos para atender diferentes aspectos de la seguridad de la información. No obstante, la revisión también permitió establecer que algunos componentes aún no se encontraban completamente implementados o no contaban con evidencia suficiente que permitiera verificar su operación durante el periodo auditado.

5.3.1. Lineamientos y procedimientos para la operación del MSPI

Lineamiento

La Entidad debe contar con lineamientos y procedimientos que orienten la operación de los controles de seguridad y privacidad de la información y permitan gestionar, entre otros aspectos, los incidentes de seguridad, las copias de respaldo y recuperación, los cambios, las vulnerabilidades, los accesos e identidades y la continuidad de los servicios tecnológicos.

El Documento Maestro establece que en esta fase se deben implementar los procesos de seguridad de la información y mantener evidencia de la implementación de los controles definidos. Asimismo, señala que las acciones establecidas en el Plan de Tratamiento de Riesgos y en el Plan de Seguridad y Privacidad de la Información deben ser implementadas y documentadas.

Requerimiento realizado por la Oficina de Control Interno

Se solicitaron los procedimientos o lineamientos documentados relacionados con la gestión de incidentes de seguridad de la información, copias de respaldo y recuperación, gestión de cambios, gestión de vulnerabilidades, control de accesos y gestión de identidades y continuidad de la operación de los servicios de tecnologías de la información.

Respuesta de la OTIC

La OTIC remitió la documentación disponible en la carpeta 1.3.a, relacionada con los componentes solicitados.

Análisis de la Oficina de Control Interno

De acuerdo con la revisión realizada, se evidenció que la Entidad avanzó en la documentación de diferentes aspectos necesarios para la operación del MSPI. Entre los soportes revisados se identificaron documentos relacionados con la gestión de incidentes de seguridad, administración de usuarios y accesos, gestión de cambios, copias de respaldo y recuperación y gestión de servicios tecnológicos.

Entre estos documentos se encuentra el Manual de Gestión de Incidentes de Seguridad y Privacidad de la Información M-TIC-001, versión 1 del 16 de abril de 2026, que establece actividades para la detección, análisis, contención, erradicación, recuperación, cierre y seguimiento posterior de los incidentes de seguridad.

Igualmente, se evidenció la Guía de Solicitud para Creación y Cierre de Usuario G-TIC-001, versión 1 del 23 de diciembre de 2025, como instrumento para orientar la administración de usuarios y accesos. También se identificaron instrumentos para la gestión de servicios tecnológicos, entre ellos la Guía Acuerdo de Niveles de Servicios y Catálogo de Servicios de TI G-TIC-002, que establece lineamientos para el registro, seguimiento y control de incidentes y requerimientos relacionados con los servicios de TI.

En materia de respaldos, se evidenció el Manual de Apoyo en el Servicio de Backup y Borrado Seguro, versión 1 del 17 de julio de 2026, el cual incluye lineamientos relacionados con almacenamiento, programación y respaldo de la información institucional.

No obstante, no se acreditó con el mismo nivel de suficiencia la formalización de lineamientos para la totalidad de los componentes evaluados, particularmente en materia de gestión de vulnerabilidades y continuidad de la operación. Estos aspectos se analizan de manera específica en los numerales siguientes, junto con las evidencias disponibles para verificar la aplicación de los controles durante el periodo auditado.

En consecuencia, aunque la Entidad cuenta con documentación formal para varios de los componentes requeridos para la operación del MSPI, no se acreditó de manera integral la totalidad de los lineamientos solicitados, por lo que este aspecto se determinó como CUMPLE PARCIALMENTE.

5.3.2. Gestión de incidentes, vulnerabilidades y respaldos

En el marco de la fase de operación del MSPI, la Oficina de Control Interno verificó la gestión realizada por la Entidad frente a los incidentes de seguridad de la información, la identificación y tratamiento de vulnerabilidades y la recuperación de la información a partir de las copias de respaldo.

En relación con la gestión de incidentes, la OTIC remitió el registro consolidado generado a través de la mesa de servicios GLPI para el periodo comprendido entre el 15 de septiembre de 2025 y el 31 de julio de 2026. El archivo contiene 133 registros asociados a categorías de seguridad y permite identificar información como estado, prioridad, ANS y fecha de apertura, evidenciando que la Entidad cuenta con un mecanismo para registrar y realizar seguimiento operativo a los casos reportados.

Asimismo, se evidenció que la Entidad cuenta con el Manual de Gestión de Incidentes de Seguridad y Privacidad de la Información M-TIC-001, versión 1 del 16 de abril de 2026, en el cual se establecen las actividades para la gestión de los incidentes de seguridad.

Frente a lo señalado en el informe preliminar respecto de la trazabilidad de los incidentes, la OTIC precisó que la información inicialmente suministrada correspondía al tablero de seguimiento que consolida información proveniente de GLPI y que el detalle de la gestión de cada caso se conserva directamente en dicha herramienta.

En atención a esta precisión, durante la etapa de observaciones al informe preliminar se realizó una validación directa en GLPI sobre una muestra de casos registrados durante el periodo evaluado. En dicha revisión se evidenció información relacionada con la apertura, clasificación, análisis, atención, solución y cierre de los casos, así como las actuaciones realizadas y la documentación asociada a su gestión.

En particular, para uno de los incidentes revisados se verificó la existencia de un informe de seguridad digital en el cual se documentó el análisis técnico realizado y las medidas adoptadas para la atención del evento, incluyendo verificaciones mediante herramientas de seguridad, revisión de los equipos involucrados y acciones preventivas posteriores. Asimismo, en otros casos revisados se evidenció el análisis efectuado para determinar la naturaleza del evento y su correspondiente atención y cierre.

Por lo anterior, la validación complementaria permitió verificar la trazabilidad de la gestión de los incidentes de seguridad de la información en los casos revisados y superar la limitación de evidencia identificada durante la ejecución inicial de la auditoría. En consecuencia, este aspecto se califica como CUMPLE.

Respecto de la gestión de vulnerabilidades, de acuerdo con los lineamientos del MSPI, durante la fase de operación la Entidad debe implementar los procesos de seguridad de la información, incluida la gestión de vulnerabilidades, de manera que estas puedan ser identificadas y se definan las acciones correspondientes para su tratamiento.

Al 31 de julio de 2026 no se evidenciaron análisis de vulnerabilidades realizados sobre las plataformas tecnológicas ni acciones de tratamiento derivadas de sus resultados. No obstante, se verificó que la Entidad había adelantado acciones para fortalecer este componente y, al cierre del periodo evaluado, ya se encontraba firmado el contrato

CO1.PCCNTR.9705440, cuyo objeto corresponde a la adquisición de una herramienta de análisis de vulnerabilidades para las plataformas tecnológicas de la Región Metropolitana Bogotá–Cundinamarca. El contrato fue aprobado por la Entidad el 31 de julio de 2026 y su ejecución inició posteriormente, el 6 de agosto de 2026.

Frente a la observación presentada al informe preliminar, se verificó igualmente que el PESI versión 2, aprobado por el Comité Institucional de Gestión y Desempeño el 26 de junio de 2026, contempló la actividad de gestión de vulnerabilidades para el periodo comprendido entre el 1 de abril y el 30 de diciembre de 2026. Por tanto, al cierre del periodo auditado la actividad se encontraba dentro del cronograma institucional definido por la Entidad y presentaba avances relacionados con la contratación de la herramienta requerida para su ejecución.

En este sentido, si bien al 31 de julio de 2026 aún no se habían realizado los análisis técnicos de vulnerabilidades sobre las plataformas tecnológicas ni se habían definido acciones de tratamiento derivadas de sus resultados, se evidenció que la Entidad había iniciado las actuaciones para la implementación de este componente y que su ejecución se encontraba programada dentro de la vigencia, conforme con el cronograma establecido en el PESI. En consecuencia, considerando conjuntamente el estado de implementación evidenciado al corte y las actividades que aún se encontraban pendientes de ejecución, este aspecto se determina como CUMPLE PARCIALMENTE. La culminación de las actividades programadas y los resultados obtenidos podrán ser verificados en posteriores ejercicios de seguimiento.

Finalmente, frente a las pruebas de restauración de respaldos, la OTIC informó inicialmente que durante el periodo auditado no se presentaron eventos que requirieran la restauración de información. Posteriormente, como resultado de las validaciones efectuadas frente al informe preliminar, se acreditó la realización de una prueba formal de restauración de la base de datos de SIGMA el 24 de junio de 2026, mediante la cual, de acuerdo con la información y evidencia suministrada, se validó la integridad de los respaldos y la correcta recuperación de la base de datos, obteniendo un resultado satisfactorio.

En consecuencia, se evidenció la ejecución satisfactoria de una prueba de restauración durante el periodo evaluado. No obstante, al revisar el M-TIC-003 – Manual de apoyo en el servicio de backup y borrado seguro, si bien este contempla lineamientos para la gestión de respaldos, recuperación y restauración de la información, no se identificó una periodicidad definida para la realización de pruebas de restauración que permita establecer su ejecución regular. Al respecto, el control A.8.13 – Respaldo de información del Documento Maestro de Lineamientos del MSPI establece que las copias de respaldo deben ponerse a prueba regularmente de acuerdo con la política de copias de respaldo definida por la Entidad. Por lo anterior, aunque se acreditó la realización de una prueba de restauración con resultado satisfactorio, permanece pendiente fortalecer los lineamientos internos para establecer la regularidad con la cual deben efectuarse

estas pruebas, por lo que este aspecto se califica como CUMPLE PARCIALMENTE.

5.3.3. Control de accesos y protección de la infraestructura tecnológica

En el marco de la fase de operación del MSPI, la Oficina de Control Interno verificó los mecanismos establecidos por la Entidad para la administración de usuarios y accesos, así como los controles dispuestos para la protección física y tecnológica de la infraestructura.

En relación con el control de accesos y gestión de identidades, la OTIC informó que la administración de usuarios se realiza de acuerdo con la Guía de Solicitud para Creación y Cierre de Usuario G-TIC-001, versión 1, y que las matrices de perfiles, roles y privilegios son administradas de manera independiente por cada sistema de información, teniendo en cuenta el nivel de reserva de la información.

La revisión de la G-TIC-001 permitió evidenciar que la Entidad cuenta con lineamientos para la solicitud, aprobación, creación, modificación, suspensión y cierre de cuentas de usuario. Asimismo, el documento establece criterios para la asignación de perfiles de acuerdo con las funciones y niveles de acceso requeridos, así como la aplicación del principio de mínimo privilegio, orientado a evitar la asignación de permisos superiores a los necesarios para el desarrollo de las funciones.

De acuerdo con la información suministrada y los documentos revisados, se evidenció que la Entidad cuenta con lineamientos formalizados para la administración de usuarios y accesos, incluyendo controles sobre la asignación de perfiles y privilegios. Por lo anterior, frente al criterio y alcance de la verificación realizada, este aspecto se calificó como CUMPLE.

Frente a la protección de la infraestructura tecnológica, la OTIC informó que dispone de mecanismos físicos y tecnológicos soportados mediante diferentes servicios y contratos vigentes. En materia física, señaló la existencia de mecanismos de vigilancia y control de acceso a las instalaciones; mientras que, en el componente tecnológico, informó sobre servicios orientados a la protección de la infraestructura, redes y seguridad perimetral.

Dentro de los soportes revisados se evidenció el contrato CO1.PCCNTR.9450108, cuyo objeto comprende la adquisición de sistemas de aseguramiento perimetral, networking, WaaP y acceso a red, con sus respectivos equipos, implementación y soporte técnico. El contrato fue aprobado por la Entidad el 15 de abril de 2026 y corresponde a mecanismos orientados a fortalecer la protección y operación de la infraestructura tecnológica de la Entidad.

De acuerdo con los soportes suministrados, se evidenció que la Entidad dispone de

mecanismos físicos y tecnológicos orientados a proteger su infraestructura, sistemas y redes. En consecuencia, frente al criterio y alcance de la verificación realizada, este aspecto se calificó como CUMPLE.

5.3.4. Gestión documental y seguridad en las relaciones con proveedores y terceros

En relación con la gestión, conservación y disposición de la información digital, la OTIC informó que estos aspectos se gestionan de manera articulada con Gestión Documental, mediante el Manual para la Gestión y Control de los Documentos M-ECM-001, la Guía para la conformación de Expedientes Electrónicos – SharePoint G-DOC-001 y el Procedimiento para la Gestión de Expedientes Electrónicos P-DOC-001.

La revisión permitió evidenciar que la Entidad cuenta con lineamientos para la conformación, organización, conservación y disposición de documentos y expedientes electrónicos, articulados con las Tablas de Retención Documental y demás instrumentos archivísticos. Por lo anterior, este aspecto se calificó como CUMPLE.

Respecto de la seguridad de la información en las relaciones con proveedores y terceros, el Documento Maestro del MSPI establece que la Entidad debe gestionar los riesgos asociados al acceso de terceros a la información, sistemas e infraestructura y establecer los controles correspondientes, incluyendo, según aplique, requisitos de confidencialidad, protección de datos personales, gestión de incidentes, accesos y responsabilidades, los cuales deben reflejarse en las relaciones contractuales.

La OTIC informó en etapa de socialización del informe preliminar que este componente se soportaba en diferentes instrumentos institucionales y que durante la vigencia 2026 adelantó, en articulación con la Oficina Jurídica, acciones orientadas a fortalecer los requisitos de seguridad de la información aplicables a las relaciones contractuales.

Frente a lo señalado en el informe preliminar, durante la etapa de observaciones se verificó que el 1 de julio de 2026 la OTIC remitió a la Oficina Jurídica una solicitud para revisar y fortalecer las cláusulas contractuales relacionadas con seguridad y privacidad de la información y que el 21 de julio de 2026 recibió respuesta de dicha Oficina, mediante la cual se incorporó una cláusula específica para su utilización en los instrumentos contractuales correspondientes. En consecuencia, al cierre del periodo evaluado ya se encontraba definido y avalado un requisito contractual específico en materia de seguridad de la información, por lo que se ajusta lo señalado en el informe preliminar respecto de que estas gestiones aún se encontraban en desarrollo.

Asimismo, durante la validación se indicó que, con posterioridad a la definición de la cláusula y hasta el cierre del periodo evaluado, no se presentaron nuevos instrumentos contractuales en los cuales fuera posible verificar su aplicación. Por lo anterior, la ausencia de evidencia de incorporación material de la cláusula en nuevos contratos no

se considera, por sí sola, una situación de incumplimiento durante el periodo evaluado.

No obstante, los lineamientos del MSPI para las relaciones con proveedores comprenden, además de la definición de requisitos contractuales, la identificación y gestión de los riesgos de seguridad asociados a estas relaciones y la aplicación de los controles correspondientes. Si bien se evidenció un avance concreto mediante la definición y aval de la cláusula de seguridad de la información, al 31 de julio de 2026 este componente se encontraba en proceso de implementación integral, de acuerdo también con las actividades previstas por la Entidad en el PESI para etapas posteriores de la vigencia. Por lo anterior, considerando las medidas implementadas y los elementos que aún se encontraban pendientes de desarrollo, este aspecto se califica como CUMPLE PARCIALMENTE.

5.4. Fase de Evaluación del Desempeño

El Documento Maestro del MSPI establece que la Entidad debe realizar seguimiento, medición, análisis y evaluación que permitan conocer el avance y desempeño del modelo, así como efectuar su revisión periódica por parte de la alta dirección.

5.4.1. Seguimiento, medición y evaluación del MSPI

La OTIC aportó la hoja de vida del indicador asociado al Plan de Sensibilización del SGSI, mediante el cual se mide el porcentaje de ejecución de las actividades programadas. El indicador cuenta con fórmula, fuentes de información, responsables y periodicidad anual.

Asimismo, se evidenciaron otros mecanismos de seguimiento, entre ellos el cronograma de implementación contenido en el PESI, los tableros de seguimiento a incidentes de seguridad y cumplimiento de ANS y la presentación de avances del MSPI ante el Comité Institucional de Gestión y Desempeño.

No obstante, el indicador formal aportado se concentra en el componente de sensibilización y no permite por sí solo medir de manera integral la evolución, desempeño y nivel de madurez del MSPI. Por lo anterior, el componente de indicadores se calificó como CUMPLE PARCIALMENTE.

Frente al seguimiento a la implementación, se evidenció que la Entidad cuenta con un cronograma definido en el PESI y realizó seguimiento a sus avances durante el periodo evaluado. En la sesión del CIGD del 26 de junio de 2026 se presentaron avances relacionados con las diferentes fases del MSPI, infraestructura tecnológica, vulnerabilidades, gestión de riesgos y sensibilización.

En consecuencia, aunque el informe consolidado de seguimiento estaba previsto para el último trimestre de 2026, se evidenciaron mecanismos y actividades de seguimiento

durante el periodo auditado, por lo que este aspecto se calificó como CUMPLE.

5.4.2. Revisión del MSPI por la Dirección

Se evidenció que el 26 de junio de 2026 el Comité Institucional de Gestión y Desempeño revisó aspectos relacionados con la implementación del MSPI, incluyendo el Plan de Sensibilización y Comunicación de Seguridad de la Información, el PESI y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Durante la sesión se presentaron el cronograma de implementación y avances en diferentes componentes del modelo, y los instrumentos señalados fueron posteriormente aprobados de manera unánime por los miembros del Comité.

Por lo anterior, se evidenció la participación de la alta dirección en la revisión y seguimiento de la implementación del MSPI, por lo que este aspecto se calificó como CUMPLE.

5.5. Fase de Mejora Continua

El Documento Maestro del MSPI establece que la Entidad debe desarrollar acciones orientadas a corregir las situaciones identificadas y fortalecer continuamente la seguridad y privacidad de la información, teniendo en cuenta los resultados del seguimiento, las evaluaciones y las oportunidades de mejora identificadas.

Durante la auditoría se evidenció que la Entidad adelantó acciones para fortalecer el MSPI, entre ellas la actualización del Plan Estratégico de Seguridad y Privacidad de la Información – PESI, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y el Plan de Sensibilización y Comunicación de Seguridad de la Información, los cuales fueron presentados y aprobados por el Comité Institucional de Gestión y Desempeño el 26 de junio de 2026.

Asimismo, se evidenciaron acciones relacionadas con el fortalecimiento de la infraestructura de seguridad, la gestión de vulnerabilidades, la sensibilización en seguridad de la información y la actualización de instrumentos asociados a la implementación del modelo. En el CIGD se reportaron, entre otros, avances en seguridad perimetral, networking, WAF, control de acceso, monitoreo de conectividad y adquisición de una herramienta para la gestión de vulnerabilidades.

Adicionalmente, el PESI contempla la mejora continua como parte de su implementación y establece que, a partir de los resultados de las actividades de sensibilización, el análisis de incidentes y la identificación de nuevos riesgos, se deberán definir acciones para fortalecer la seguridad de la información.

En este sentido, se evidenciaron acciones orientadas al fortalecimiento y mejora continua del MSPI, cuyo avance y efectividad deberán continuar siendo objeto de seguimiento conforme avance la implementación del modelo.

5.6. Seguimiento a las observaciones y recomendaciones de la auditoría MSPI 2025

Como parte de la presente auditoría se realizó seguimiento a las once (11) observaciones formuladas en la auditoría al Modelo de Seguridad y Privacidad de la Información – MSPI de la vigencia 2025, con el propósito de establecer el estado de las situaciones identificadas y verificar las acciones adelantadas por la Entidad durante el periodo evaluado. Para determinar su estado se contrastaron las condiciones identificadas en 2025 con los documentos y soportes suministrados por la OTIC y con los resultados de las pruebas realizadas durante la presente auditoría.

No.	Observación 2025	Resultado del seguimiento 2026
1	Fase de Diagnóstico Se evidenciaron inconsistencias y vacíos de diligenciamiento en el autodiagnóstico MSPI 2025 que afectaban la completitud del instrumento y su utilidad como insumo para la planificación. En las hojas de dominios Organizacionales, Personas, Físicos y Tecnológicos se identificaron campos sin diligenciar y no se presentó un consolidado de brechas ni un plan de acciones de mejora derivado del autodiagnóstico.	**Parcialmente Superada** Se evidenció que la Entidad actualizó y utilizó el Autodiagnóstico MSPI como instrumento para identificar el estado de implementación del modelo y las brechas existentes. No obstante, durante la revisión se identificaron inconsistencias en las fechas registradas y en la correspondencia entre algunas calificaciones y las brechas identificadas, así como aspectos por fortalecer en la relación de estas con las acciones de mejora correspondientes. Por lo anterior, si bien se atendieron parcialmente las situaciones identificadas en 2025, la condición no se encontraba subsanada en su totalidad al cierre del periodo evaluado.
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 evidenció que no se había adelantado la identificación y análisis de las partes	**Superada** Se evidenció que la Entidad formalizó la G-TIC-005 – Guía para la Construcción y Actualización del Contexto Estratégico de TI, versión 1 del 26 de junio de 2026, la cual incorpora la identificación de

No.	Observación 2025	Resultado del seguimiento 2026
	interesadas internas y externas que pudieran influir o verse afectadas por la seguridad y privacidad de la información, ni se contaba con documentos que permitieran reconocer sus necesidades, expectativas o requisitos legales, reglamentarios y contractuales asociados al MSPI.	partes interesadas internas y externas, sus necesidades o expectativas y los requisitos aplicables al SGSI, así como su revisión periódica. En consecuencia, se evidenció que la condición identificada en 2025 fue atendida.
3	Debilidades en la formulación del alcance del MSPI en el Plan de Implementación 2025 Se evidenció que, aunque el Plan de Implementación establecía un alcance amplio, no presentaba una delimitación clara de la aplicabilidad del MSPI frente al modelo de operación por procesos, no identificaba los procesos priorizados según su exposición a riesgos y no detallaba los activos, sistemas, roles y áreas seguras incluidos en el alcance. Asimismo, el documento presentaba debilidades de formalización y control documental.	**Parcialmente Superada** Se evidenció una mayor definición del alcance del MSPI mediante su incorporación en el PESI V2 y su desarrollo en el M-TIC-004, permitiendo precisar la cobertura del modelo frente a lo observado en 2025. No obstante, al 31 de julio de 2026 el M-TIC-004 se encontraba en proceso de revisión y aprobación y no había culminado la formalización de los elementos definidos para el alcance del modelo. Por lo anterior, aunque se evidenciaron avances sustanciales frente a la condición identificada en 2025, esta no se encontraba subsanada en su totalidad al cierre del periodo evaluado.
4	Falta de designación expresa del responsable de seguridad de la información como miembro permanente del Comité Institucional de Gestión y Desempeño Se evidenció que, aunque la Resolución No. 332 del 9 de septiembre de 2024 incluyó al Jefe de la OTIC como integrante del Comité, no lo designó expresamente como responsable de seguridad de la información, ni se evidenció otro documento que acreditara formalmente dicha designación.	**Persiste** Durante 2026 la OTIC adelantó gestiones orientadas a formalizar la designación del responsable de seguridad de la información, entre ellas la consulta realizada a la Oficina Asesora de Planeación mediante memorando No. 202601600012363 del 30 de junio de 2026. Sin embargo, al 31 de julio de 2026 no se había formalizado dicha designación, por lo que la condición identificada en 2025 permanecía al cierre del periodo evaluado.
5	Debilidad en la formalización e integración de los roles y responsabilidades del MSPI Se evidenciaron debilidades relacionadas con la dependencia organizacional del responsable del MSPI, su participación en los comités institucionales y la inclusión de	**Parcialmente Superada** Se evidenció que la Entidad avanzó en la definición e integración de los roles y responsabilidades asociados al MSPI mediante el M-TIC-004, el cual incorpora responsabilidades para la OTIC, líderes

No.	Observación 2025	Resultado del seguimiento 2026
	los líderes de proceso y otros actores institucionales en la gestión de la seguridad y privacidad de la información. Asimismo, la matriz revisada no contaba con fecha, versión, control de cambios ni firmas de aprobación.	de proceso, dependencias de apoyo, servidores públicos, contratistas, proveedores y demás usuarios autorizados, así como una matriz RACI para diferentes actividades relacionadas con la implementación del modelo. No obstante, al 31 de julio de 2026 dicho documento se encontraba en proceso de revisión y aprobación, por lo que la formalización de estos roles y responsabilidades no había culminado al cierre del periodo evaluado. En consecuencia, la condición identificada en 2025 se considera parcialmente superada.
6	Ausencia de inventario consolidado y clasificación formal de los activos de información e infraestructura crítica cibernética Se evidenció que la Entidad se encontraba en una fase inicial del proceso de identificación y clasificación de activos, sin contar con un inventario consolidado ni con la clasificación bajo los criterios de confidencialidad, integridad y disponibilidad. Tampoco se evidenció la inclusión de activos con información personal ni la identificación de infraestructura crítica cibernética.	**Parcialmente Superada** Se evidenció que la Entidad formalizó la metodología F-TIC-004 para la identificación, clasificación y valoración de activos de información y adelantó el levantamiento de un inventario que contiene 135 activos. Frente a la clasificación y valoración de estos, durante las validaciones efectuadas con posterioridad al informe preliminar, la OTIC presentó a la auditoría la matriz interna utilizada para su gestión, lo que permitió verificar la existencia del instrumento para la clasificación y valoración de los activos. No obstante, al 31 de julio de 2026, el proceso de gestión de activos de información aún no había culminado, toda vez que el inventario se encontraba en proceso de revisión y validación y estaba pendiente la etapa de aprobación final prevista institucionalmente. Por lo anterior, si bien se evidenciaron avances sustanciales frente a la condición identificada en 2025, esta no se encontraba subsanada en su totalidad al cierre del periodo evaluado.

No.	Observación 2025	Resultado del seguimiento 2026
7	Ausencia de metodología y proceso formal de valoración de los riesgos de seguridad y privacidad de la información Se evidenció que la Entidad no había desarrollado ni implementado el proceso de valoración de riesgos de seguridad y privacidad de la información y se encontraba en una fase preparatoria orientada al levantamiento del inventario de activos, sin contar con metodologías, instrumentos o matrices que permitieran identificar, valorar o priorizar los riesgos asociados.	**Parcialmente Superada** Se evidenció que la Entidad formalizó la Política para la Gestión Integral del Riesgo – PL-DES-001, adoptada mediante Resolución No. 448 de 2025, dispone del formato F-DES-020 – Matriz de Riesgos Institucional para documentar la identificación y valoración de riesgos y cuenta con el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PN-TIC-002, mediante el cual se definieron las actividades para desarrollar la gestión específica de los riesgos de seguridad de la información. No obstante, al 31 de julio de 2026 aún no se había culminado la aplicación del proceso para identificar y valorar específicamente los riesgos de seguridad de la información asociados a los activos de información. La elaboración de la matriz específica se encontraba programada para desarrollarse durante el segundo semestre de 2026. Por lo anterior, si bien se evidenciaron avances en la definición de lineamientos e instrumentos para la gestión de estos riesgos, permanecía pendiente la aplicación del proceso específico de valoración, por lo que la condición identificada en 2025 no se encontraba subsanada en su totalidad al cierre del periodo evaluado.
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 Se evidenció que el Plan de Tratamiento presentaba un desarrollo metodológico; sin embargo, no se acreditó su adopción formal por el Comité Institucional de Gestión y Desempeño ni se contaba con una Declaración de Aplicabilidad – SoA. Adicionalmente, el documento no contaba	**Parcialmente Superada** Se evidenció la formalización del PN-TIC-002 – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, versión 2 del 26 de junio de 2026, el cual cuenta con control documental y registra su aprobación por el Comité Institucional de Gestión y Desempeño. Con ello, se atendieron los aspectos identificados en 2025 relacionados con la formalización,

No.	Observación 2025	Resultado del seguimiento 2026
	con control de cambios, versión, fecha de emisión ni firmas de aprobación y tampoco se identificaron registros de aceptación formal de los riesgos residuales.	aprobación y control documental del Plan. No obstante, al 31 de julio de 2026, la Declaración de Aplicabilidad – SoA aún se encontraba en proceso de construcción y revisión y, dado que no se había culminado la valoración específica de los riesgos de seguridad de la información, permanecían pendientes las etapas posteriores relacionadas con la determinación del riesgo residual, su aceptación cuando correspondiera y la relación entre los riesgos identificados, los controles y su tratamiento. Por lo anterior, si bien se atendieron algunos de los aspectos que dieron origen a la observación de 2025, la condición no se encontraba subsanada en su totalidad al cierre del periodo evaluado, por lo que se considera parcialmente superada.
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 evidenció una acción puntual de sensibilización y la existencia de una cláusula general de confidencialidad en los contratos; sin embargo, la Entidad no contaba con un plan formal de capacitación, comunicación y concientización aprobado e integrado al PIC, ni con un Plan de Comunicaciones. Adicionalmente, la cláusula contractual abordaba la confidencialidad de manera general, sin incorporar obligaciones específicas relacionadas con la implementación y gestión del MSPI, protección de datos personales o seguridad digital.	**Parcialmente Superada** Se evidenció la formalización del Plan de Sensibilización y Comunicación en Seguridad de la Información 2026, así como la ejecución de actividades de sensibilización y comunicación durante el periodo evaluado. Frente al componente contractual, se verificó que durante julio de 2026 la OTIC adelantó actuaciones con la Oficina Jurídica orientadas al fortalecimiento de los requisitos de seguridad y privacidad aplicables a proveedores y terceros, como resultado de las cuales se definió y aprobó una cláusula de seguridad de la información para su utilización institucional. No obstante, durante el periodo evaluado no se contó con nuevos instrumentos contractuales posteriores a su aprobación que permitieran verificar su aplicación.

No.	Observación 2025	Resultado del seguimiento 2026
		Por lo anterior, se evidenciaron avances sustanciales frente a los componentes que dieron origen a la observación de 2025; sin embargo, al cierre del periodo evaluado no era posible verificar la aplicación de la cláusula aprobada en nuevas relaciones contractuales, por lo que la observación se considera parcialmente superada.
10	Ausencia de información documentada y control formal de los instrumentos del Modelo de Seguridad y Privacidad de la Información Se evidenció que no habían sido entregados ni formalizados varios documentos requeridos para la implementación del MSPI, entre ellos procedimientos, guías, inventario de activos, matriz de riesgos, proceso de gestión de vulnerabilidades y Declaración de Aplicabilidad. Adicionalmente, los documentos disponibles presentaban debilidades relacionadas con control de cambios, versión, fechas y firmas de aprobación.	**Superada** Se evidenció un fortalecimiento en la gestión de la información documentada del MSPI mediante la elaboración y formalización de políticas, planes, metodologías, manuales, procedimientos, guías y formatos que cuentan con elementos de control documental y se encuentran organizados y disponibles en el Banco de Documentos institucional. Frente a la situación identificada en 2025, se verificó que la Entidad contaba al cierre del periodo evaluado con mecanismos para la identificación, formalización, versionamiento y organización de la documentación asociada al MSPI, superando las debilidades de control documental evidenciadas en dicha vigencia. Los instrumentos que al 31 de julio de 2026 se encontraban en proceso de elaboración o consolidación, como la matriz específica de riesgos de seguridad de la información y la Declaración de Aplicabilidad – SoA, corresponden a productos asociados al proceso de implementación del modelo y su estado se evalúa en los numerales específicos del presente informe, sin que ello constituya, por sí mismo, una deficiencia en la gestión y control de la información documentada.

No.	Observación 2025	Resultado del seguimiento 2026
		Por lo anterior, la observación se considera SUPERADA.
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 Se evidenció que la inexistencia de un inventario formal y actualizado de activos limitaba el desarrollo de componentes posteriores de la Fase de Operación, entre ellos la matriz de riesgos de seguridad de la información y los planes para su tratamiento.	**Parcialmente Superada** Se evidenció un cambio sustancial frente a la situación identificada en 2025. La Entidad formalizó la metodología para la identificación, clasificación y valoración de activos de información y adelantó el levantamiento de un inventario que contiene 135 activos. Asimismo, cuenta con instrumentos para la gestión de riesgos y con el PN-TIC-002 – Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información. Frente a la clasificación y valoración de los activos, durante las validaciones efectuadas con posterioridad al informe preliminar se verificó la existencia de la matriz interna utilizada para su gestión. No obstante, al 31 de julio de 2026, el proceso de gestión de activos aún se encontraba en revisión y validación y no había culminado la aplicación del proceso específico de identificación y valoración de los riesgos de seguridad de la información asociados a dichos activos. Por lo anterior, aunque se atendieron aspectos relevantes de la condición identificada en 2025, aún no había culminado el desarrollo de los componentes posteriores asociados a la valoración específica de riesgos de seguridad de la información, por lo que la observación se considera parcialmente superada.

Como resultado del seguimiento realizado a las once (11) observaciones de la auditoría MSPI 2025, se estableció que dos (2) se encuentran superadas, ocho (8) parcialmente superadas y una (1) persiste.

En términos generales, se evidenció un fortalecimiento en la implementación del MSPI

frente a la vigencia anterior, principalmente en la identificación de partes interesadas, definición del alcance y responsabilidades, levantamiento del inventario de activos, formalización de la metodología para la gestión de riesgos, elaboración de planes y procedimientos, sensibilización y documentación asociada al modelo.

No obstante, al 31 de julio de 2026 permanecían aspectos por completar relacionados principalmente con la designación formal del responsable de seguridad de la información, culminación del proceso de gestión de activos de información, aplicación de la valoración específica de riesgos de seguridad de la información, finalización de la Declaración de Aplicabilidad – SoA, gestión de vulnerabilidades y aplicación de los requisitos de seguridad definidos para proveedores y terceros.

En consecuencia, se requiere continuar con las acciones necesarias para atender integralmente las situaciones que se encuentran parcialmente superadas o que persisten, y verificar su avance y cierre en los seguimientos posteriores por parte de la Oficina de Control Interno.

5.7. Gestión de riesgos y controles asociados a las tecnologías de la información

Como parte de la auditoría se evaluó la gestión de los riesgos institucionales asociados a las tecnologías de la información, con el propósito de verificar su identificación, valoración, tratamiento y los controles establecidos por la Entidad.

Para esta evaluación se tomó como referencia la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del Departamento Administrativo de la Función Pública – DAFP, teniendo en cuenta la tipología definida para cada riesgo y los criterios particulares establecidos en dicha metodología para su análisis y valoración.

La revisión comprendió cuatro (4) riesgos registrados en la Matriz de Riesgos Institucional: dos (2) clasificados como riesgos de Gestión, uno (1) como riesgo Fiscal y uno (1) como riesgo de Integridad-Corrupción. En cada caso se revisó la formulación y valoración del riesgo, el diseño y clasificación de los controles, el riesgo residual y el tratamiento definido.

A partir de lo anterior, se obtuvieron los siguientes resultados:

5.7.1. Riesgo asociado a la pérdida de información

En la Matriz de Riesgos Institucional se identificó el siguiente riesgo de Gestión:

"Posibilidad de afectación reputacional por la pérdida de la información en bases

de datos de la Región Metropolitana Bogotá – Cundinamarca (RMBC), a causa de la insuficiencia en los mecanismos de respaldo y recuperación."

La revisión realizada, de acuerdo con la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP, permitió establecer que el riesgo se encuentra identificado y valorado y cuenta con un control relacionado con la ejecución programada de copias de respaldo y la utilización de la copia inmediatamente anterior cuando se presenten fallas en la recuperación.

No obstante, se evidenció que dicho control fue clasificado en la matriz como Preventivo – Manual, mientras que la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP, en el numeral 3.9 "Tipologías de Controles" (pág. 64), incluye expresamente las copias de seguridad (backup) dentro de los mecanismos asociados a controles correctivos y precisa que, aunque estos requieren acciones previas que garanticen su utilización al momento de materializarse el riesgo, no pueden clasificarse como preventivos, dado que ello generaría una sobrevaloración del control.

En consecuencia, aunque el riesgo se encuentra identificado y valorado y cuenta con un control definido, se evidenció una diferencia en la clasificación del control frente a lo establecido en la Guía DAFP V7, por lo que **se recomienda** revisar su tipología y el efecto que el ajuste correspondiente pueda tener sobre la valoración del riesgo residual.

5.7.2. Riesgo asociado a la interrupción de los servicios tecnológicos

En la Matriz de Riesgos Institucional se identificó el siguiente riesgo de Gestión:

"Posibilidad de afectación reputacional por la interrupción de los servicios tecnológicos que soporta los sistemas de información de OTIC, a causa de fallas en la infraestructura tecnológica, comprometiendo la disponibilidad de la información institucional."

La Entidad valoró el riesgo con Probabilidad Baja (40 %) e Impacto Leve (20 %) y estableció como control que el Profesional de Infraestructura monitoree continuamente la infraestructura tecnológica para detectar fallas o degradaciones del servicio y, cuando identifique un evento, registre el caso correspondiente en GLPI.

Al revisar el diseño del control frente a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP, se evidenció que este contiene los elementos básicos para su aplicación; sin embargo, la Entidad lo clasificó como Preventivo – Manual. Por la forma como se encuentra descrito, el control funciona principalmente como Detectivo – Manual, dado que el monitoreo se realiza continuamente durante la operación de la infraestructura para identificar fallas o degradaciones del servicio y, una vez detectado un evento, generar el registro correspondiente en GLPI. Al respecto, tanto

la Guía DAFP V7, en el numeral 3.9 “Tipologías de Controles” (pág. 64), como la Política para la Gestión Integral del Riesgo – PL-DES-001 de la Entidad, en el numeral 6.1.7 (pág. 10), establecen que el control detectivo es aquel que se acciona durante la ejecución del proceso.

Esta diferencia resulta relevante para la valoración del control, teniendo en cuenta que tanto la Guía DAFP V7 como la Política para la Gestión Integral del Riesgo – PL-DES-001 de la Entidad asignan una ponderación de 25 % al control Preventivo y 15 % al Detectivo, por lo que corresponde determinar el efecto que un eventual ajuste en la clasificación pueda tener sobre la valoración del riesgo residual.

En consecuencia, aunque el riesgo se encuentra identificado y valorado y cuenta con control, riesgo residual y tratamiento definidos, **se recomienda** revisar la clasificación del control como Preventivo frente a su funcionamiento principalmente Detectivo y determinar, dentro del instrumento institucional utilizado para la gestión de riesgos, el efecto que el ajuste correspondiente pueda tener sobre la valoración del riesgo residual.

5.7.3. Riesgo asociado al daño de la infraestructura tecnológica

En la Matriz de Riesgos Institucional se identificó el siguiente riesgo Fiscal:

> *“Posibilidad de efecto dañoso sobre el recurso público por daño en equipos tecnológicos a causa de omisión en la ejecución del plan de mantenimiento preventivo.”*

La revisión realizada con base en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP permitió establecer que la formulación del riesgo identifica el posible efecto dañoso sobre los recursos públicos y la causa asociada a la omisión en la ejecución del mantenimiento preventivo. La Entidad valoró el riesgo con Probabilidad Media (60%) e Impacto Leve (20%) y estableció como tratamiento Reducir (mitigar).

Como control se estableció que el Profesional de Infraestructura supervise el plan de mantenimiento preventivo, verificando que los equipos cuenten con hoja de vida y que sus mantenimientos estén incluidos en la planeación. Sin embargo, se evidenció que el control no cubre completamente la causa identificada, debido a que esta corresponde a la omisión en la ejecución del mantenimiento, mientras que el control se concentra principalmente en verificar su planeación, sin establecer claramente la verificación de que los mantenimientos programados efectivamente se realicen de manera oportuna.

En consecuencia, aunque el riesgo fiscal se encuentra identificado y valorado y cuenta con control, riesgo residual, tratamiento y plan de acción, el diseño del control debe fortalecerse para que permita verificar de manera directa el cumplimiento del

mantenimiento preventivo programado. Por lo anterior, **se recomienda** fortalecer el control para que, además de verificar la inclusión de los equipos y mantenimientos en la planeación, contemple la verificación de que los mantenimientos programados se realicen de manera efectiva y oportuna, así como las acciones a seguir cuando se presenten incumplimientos.

5.7.4. Riesgo asociado a los accesos privilegiados y manipulación de la información

En la Matriz de Riesgos Institucional se identificó el siguiente riesgo de Integridad-Corrupción:

> *"Posibilidad de pérdida reputacional por actos de corrupción en la gestión de accesos privilegiados, a causa de debido a la manipulación, alteración o eliminación de la información contenida en los sistemas de información, en beneficio propio o de terceros."*

La Entidad valoró el riesgo con Probabilidad Baja (40 %) e Impacto Moderado (60 %) y estableció como control el monitoreo de las herramientas utilizadas para administrar los permisos, a cargo de los profesionales de cada dominio, señalando que, cuando se identifique una inconsistencia, se realizará el bloqueo inmediato de los permisos.

Al revisar su formulación y el diseño del control frente a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP, se evidenciaron aspectos por fortalecer. La causa definida como "manipulación, alteración o eliminación de la información" describe principalmente la conducta mediante la cual podría materializarse el riesgo, pero no permite identificar con claridad la debilidad que podría facilitar su ocurrencia, relacionada, por ejemplo, con la asignación, revisión o monitoreo de los accesos privilegiados.

Asimismo, aunque el control establece responsable, actividad, frecuencia, actuación frente a inconsistencias y evidencia, su descripción no precisa suficientemente qué se verifica sobre los accesos privilegiados. Adicionalmente, fue clasificado por la Entidad como Preventivo – Manual; sin embargo, de acuerdo con la forma como se encuentra descrito, el monitoreo está orientado a identificar inconsistencias en los permisos y actuar posteriormente mediante su bloqueo. Al respecto, tanto la Guía DAFP V7, en el numeral 3.9 "Tipologías de Controles" (pág. 64), como la Política para la Gestión Integral del Riesgo – PL-DES-001 de la Entidad, en el numeral 6.1.7 (pág. 10), establecen que la tipología del control se determina de acuerdo con el momento en que este se activa frente al desarrollo del proceso. En consecuencia, se recomienda revisar la clasificación asignada al control y determinar el efecto que un eventual ajuste pueda tener sobre la valoración del riesgo residual.

En consecuencia, aunque el riesgo se encuentra identificado bajo una tipología de

Integridad-Corrupción acorde con el escenario planteado y cuenta con valoración, control, riesgo residual, tratamiento y plan de acción, **se recomienda** revisar su formulación para identificar con mayor claridad la causa que podría permitir la materialización del riesgo; fortalecer la descripción del control precisando qué aspectos se verifican sobre los accesos privilegiados; y revisar su clasificación de acuerdo con el momento en que este se activa, así como el efecto que los ajustes realizados puedan tener sobre la valoración del riesgo residual.

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

Para la realización de esta auditoría, se aplicaron las Normas de Auditoría generalmente aceptadas en Colombia. Se precisa que, durante su desarrollo, no se presentaron limitaciones que impidieran la ejecución de la auditoría, así como tampoco se presentaron conflictos de interés que pudieran afectar o impedir su desarrollo y resultado.

Se precisa además que, debido a las limitaciones inherentes de cualquier estructura de Control Interno, pueden ocurrir errores e irregularidades que no hayan sido detectados durante la planeación y realización de la presente auditoría. En este sentido, la Región Metropolitana Bogotá – Cundinamarca y las dependencias que la integran son 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.

A la fecha de la auditoría, la Región Metropolitana Bogotá – Cundinamarca no contaba con Planes de Mejoramiento por Procesos – PMP ni Planes de Mejoramiento Institucional – PMI relacionados con el objeto de la presente auditoría. No obstante, como parte del alcance del presente trabajo se efectuó seguimiento a las once (11) observaciones y recomendaciones formuladas en la auditoría del MSPI de la vigencia 2025, las cuales no dieron lugar a la formulación de un plan de mejoramiento.

7. Análisis de las observaciones al informe preliminar

Una vez realizado el análisis de la respuesta remitida por la Oficina de Tecnologías de la Información y las Comunicaciones – OTIC mediante correo electrónico del 10 de septiembre de 2026, respecto del informe preliminar, así como de las aclaraciones y soportes revisados durante la mesa de trabajo realizada el 14 de septiembre de 2026, la Oficina de Control Interno efectuó los ajustes que se consideraron procedentes para la elaboración del informe final.

A continuación, se presentan los cambios efectuados frente a las observaciones

comunicadas en el informe preliminar:

Informe preliminar	Informe final	Conclusión
Observación No. 1. Formalización de roles y responsabilidades para la implementación del MSPI. Al 31 de julio de 2026 no se acreditó la definición y formalización del rol de Responsable de Seguridad de la Información, con sus respectivas funciones y responsabilidades. Si bien la Entidad adelantó acciones para estructurar los roles asociados al MSPI e incorporó una matriz RACI en el Manual de Políticas Complementarias de Seguridad y Privacidad de la Información – M-TIC-004, dicho documento se encontraba en proceso de revisión y aprobación al cierre del periodo evaluado. Esta situación evidencia que, a la fecha de corte de la auditoría, permanecía pendiente la formalización de un elemento requerido para establecer claramente la responsabilidad sobre la coordinación y seguimiento de la	**Observación No. 1.** Formalización del Responsable de Seguridad de la Información *(Ver en párrafos siguientes)*	**Se ajusta.** Analizada la respuesta de la OTIC, se precisa el alcance de la observación, teniendo en cuenta que la situación identificada no corresponde a una ausencia general de roles y responsabilidades frente al MSPI, sino específicamente a que, al 31 de julio de 2026, se encontraba pendiente la formalización del Responsable de Seguridad de la Información. La información posterior al periodo evaluado se considera como una acción adelantada por la Entidad, sin modificar la situación existente a la fecha de corte.

implementación y operación del MSPI.		
Observación No. 2. Valoración y tratamiento de los riesgos de seguridad de la información Al 31 de julio de 2026 no se había culminado la aplicación del proceso específico de valoración de riesgos de seguridad de la información asociados a los activos de la Entidad. Aunque se cuenta con la Política para la Gestión Integral del Riesgo – PL-DES-001, el formato institucional F-DES-020 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PN-TIC-002, no se evidenció diligenciada la matriz específica de riesgos de seguridad de la información. Como consecuencia, al cierre del periodo evaluado tampoco se encontraba completada la aplicación del tratamiento de estos riesgos, la determinación y aceptación de los riesgos residuales cuando correspondiera, la consolidación de la	**Observación No. 2**. Valoración y tratamiento de los riesgos de seguridad de la información *(Ver en párrafos siguientes)*	**Se ajusta.** Se acogen parcialmente las precisiones y soportes presentados por la OTIC, particularmente frente a la gestión de activos de información. No obstante, se mantiene la observación debido a que, al 31 de julio de 2026, no se había culminado la aplicación del proceso específico de identificación y valoración de los riesgos de seguridad de la información y, en consecuencia, las etapas posteriores asociadas a su tratamiento se encontraban pendientes de desarrollo integral. En próximos seguimientos se verificará su implementación.

Declaración de Aplicabilidad – SoA ni el seguimiento a las medidas de tratamiento.		
Observación No. 3. Implementación de componentes operativos de seguridad de la información. Durante la evaluación de la fase de Operación se evidenció que la Entidad cuenta con procedimientos, lineamientos y mecanismos para diferentes componentes de seguridad de la información; sin embargo, al 31 de julio de 2026 permanecían aspectos relevantes pendientes de implementación o de acreditación de su funcionamiento. En particular, no se evidenció la realización de análisis de vulnerabilidades sobre las plataformas tecnológicas ni las acciones de tratamiento derivadas de sus resultados; tampoco se acreditó la realización de pruebas de restauración que permitieran verificar la recuperación efectiva de la información a partir de las copias de respaldo.	N/A	**Se retira.** Como resultado del análisis de la respuesta de la OTIC y de las verificaciones adicionales efectuadas, se evidenciaron elementos que modificaron las condiciones consideradas inicialmente para la formulación de la observación. En particular, se verificaron soportes relacionados con las pruebas de restauración y se realizaron verificaciones adicionales frente a la gestión de proveedores. Respecto de la gestión de vulnerabilidades, el resultado correspondiente se mantiene dentro de la evaluación del MSPI y del seguimiento a las observaciones de la vigencia 2025, por lo cual no se considera procedente mantener una observación adicional independiente sobre este aspecto.

Adicionalmente, no se acreditó la incorporación sistemática de los requisitos específicos de seguridad y privacidad de la información aplicables a proveedores y terceros en las relaciones contractuales correspondientes. Estas situaciones evidencian la necesidad de culminar la implementación de controles operativos necesarios para fortalecer la protección de la información y verificar que los mecanismos establecidos funcionen de acuerdo con lo previsto.		
Recomendaciones. Se formularon cinco (5) recomendaciones relacionadas con el autodiagnóstico del MSPI, la gestión de incidentes de seguridad de la información y los controles asociados a los riesgos de TI evaluados.	Se formulan seis (6) recomendaciones. Se mantienen las relacionadas con el autodiagnóstico, la gestión de incidentes y el fortalecimiento de los controles de los riesgos fiscal y de Integridad-Corrupción; se ajusta la recomendación relacionada con la clasificación y valoración de los controles asociados a los riesgos de pérdida de información e interrupción de los servicios tecnológicos, y	**Se ajustan.** Como resultado del análisis de las observaciones presentadas por la OTIC y de las verificaciones adicionales efectuadas, se precisó el alcance de las recomendaciones formuladas en el informe preliminar. En particular, se ajustó la recomendación asociada a la clasificación y valoración de los controles de riesgos de TI, eliminando la referencia a la conservación de evidencias sobre su ejecución y seguimiento, y se incorporó una recomendación relacionada con la periodicidad de las pruebas de restauración de

	se incorpora una recomendación orientada a fortalecer la realización periódica de pruebas de restauración de respaldos.	respaldos, teniendo en cuenta los soportes verificados durante la etapa de análisis del informe preliminar.

8. Conclusiones: Hallazgos[2], Observaciones[3] y/o Recomendaciones[4]

Como resultado de la auditoría realizada a la implementación y operación del Modelo de Seguridad y Privacidad de la Información – MSPI, se evidenció que la Región Metropolitana Bogotá – Cundinamarca ha adelantado acciones para su implementación, contando con documentos, instrumentos y actividades asociadas a las diferentes fases del modelo.

No obstante, la evaluación permitió identificar aspectos que requieren fortalecimiento, principalmente relacionados con la formalización de algunos elementos del MSPI, la gestión de activos y riesgos de seguridad de la información, la definición y seguimiento de controles y la culminación de actividades previstas para la implementación del modelo.

Respecto del seguimiento a la auditoría de la vigencia 2025, de las once (11) observaciones y recomendaciones evaluadas, se determinó que dos (2) se encuentran superadas, ocho (8) parcialmente superadas y una (1) persiste, evidenciándose que varias de las acciones adelantadas atendieron parcialmente las situaciones identificadas, aunque permanecen aspectos pendientes de completar o formalizar.

Adicionalmente, la revisión de los cuatro (4) riesgos asociados a tecnologías de la información registrados en la Matriz de Riesgos Institucional permitió identificar aspectos por fortalecer en la formulación y diseño de algunos controles, así como en su clasificación, de acuerdo con la metodología establecida en la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP.

A partir de los resultados obtenidos, se presentan a continuación las conclusiones, hallazgos, observaciones y/o recomendaciones derivadas de la auditoría, según

[2] Los hallazgos están llamados a elaborar Plan de Mejoramiento.
[3] Las observaciones, son banderas rojas para el proceso, que buscan que la Entidad analice dichas circunstancias evidenciadas en el seguimiento, con el fin de evaluar la necesidad de adoptar y/o fortalecer puntos de control y/o implementar acciones.
[4] 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

corresponda.

Conclusiones

i. La evaluación evidenció que la Región Metropolitana Bogotá – Cundinamarca ha avanzado en la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, mediante la definición y actualización de documentos, instrumentos y actividades correspondientes a sus diferentes fases. No obstante, al 31 de julio de 2026 permanecían elementos pendientes de culminar, formalizar o implementar, por lo que la implementación del modelo aún no se encontraba completada integralmente.

ii. En la fase de Diagnóstico y Planificación se evidenciaron elementos implementados relacionados con la identificación de partes interesadas, definición del alcance, política, metodología para la gestión de riesgos, identificación e inventario de activos de información y actividades de sensibilización y comunicación. Sin embargo, permanecían aspectos por completar, principalmente en la formalización de roles y responsabilidades, la culminación del proceso de gestión de activos de información y la valoración específica de los riesgos de seguridad de la información.

iii. En relación con la gestión de riesgos de seguridad de la información, al 31 de julio de 2026 no se evidenció culminada y aplicada la valoración específica de estos riesgos. En consecuencia, tampoco se encontraba consolidado integralmente su tratamiento, la aceptación de los riesgos residuales, la Declaración de Aplicabilidad y el seguimiento correspondiente, elementos necesarios para completar esta fase del MSPI.

iv. En la fase de Operación se evidenció la existencia y aplicación de diferentes medidas relacionadas con la gestión de la seguridad de la información. No obstante, permanecían aspectos por fortalecer o completar en algunos de los componentes evaluados, de acuerdo con los resultados presentados en el numeral 5.3 del presente informe.

v. En las fases de Evaluación del Desempeño y Mejora Continua se evidenciaron mecanismos para realizar seguimiento al avance del MSPI, entre ellos herramientas de medición y espacios de seguimiento institucional. No obstante, algunos elementos requerían fortalecimiento para acompañar la culminación de la implementación del modelo.

vi. Frente al seguimiento de las once (11) observaciones y recomendaciones formuladas en la auditoría del MSPI de la vigencia 2025, se determinó que dos (2) se encuentran superadas, ocho (8) parcialmente superadas y una (1) persiste. Lo anterior evidencia que se adelantaron acciones frente a las situaciones identificadas en la vigencia anterior, aunque permanecen aspectos pendientes de

completar o formalizar.

vii. En la revisión de los cuatro (4) riesgos asociados a tecnologías de la información registrados en la Matriz de Riesgos Institucional, se evidenció que estos cuentan con identificación, valoración y controles definidos. No obstante, se identificaron aspectos por fortalecer relacionados con la formulación y el diseño de algunos controles, así como con su clasificación, conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP y la Política para la Gestión Integral del Riesgo – PL-DES-001 de la Entidad.

viii. En términos generales, los resultados de la auditoría evidencian que la Entidad cuenta con una base documental y operativa para continuar la implementación del MSPI; sin embargo, resulta necesario culminar y formalizar los elementos pendientes y fortalecer los controles identificados, con el propósito de consolidar la implementación y operación del modelo.

Hallazgos y Observaciones

En desarrollo de la presente auditoría, y de acuerdo con el objetivo, alcance, criterios y resultados obtenidos, no se configuraron hallazgos que den lugar a la formulación de Plan de Mejoramiento. No obstante, se identificaron las siguientes observaciones, las cuales constituyen situaciones que requieren análisis y atención por parte del proceso:

Observación No. 1. Formalización del Responsable de Seguridad de la Información

Al 31 de julio de 2026 no se encontraba formalizada la designación del Responsable de Seguridad de la Información, con sus respectivas funciones y responsabilidades. Si bien la Entidad contaba con responsables asignados para diferentes actividades asociadas a la implementación del MSPI y adelantaba acciones para formalizar este rol específico, al cierre del periodo evaluado dicha formalización se encontraba pendiente.

Esta situación evidencia que, a la fecha de corte de la auditoría, permanecía pendiente la formalización del responsable encargado de coordinar y hacer seguimiento a la implementación y operación del MSPI.

Observación No. 2. Valoración y tratamiento de los riesgos de seguridad de la información

Al 31 de julio de 2026 no se había culminado la aplicación del proceso específico de identificación y valoración de los riesgos de seguridad de la información asociados a los activos de la Entidad. Si bien la Entidad contaba con la Política para la Gestión Integral del Riesgo – PL-DES-001, el formato institucional F-DES-020 y el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información – PN-TIC-002, la elaboración y aplicación de la matriz específica de riesgos de seguridad de la información se

encontraba en desarrollo, de acuerdo con la programación institucional definida para el segundo semestre de 2026.

En consecuencia, al cierre del periodo evaluado aún no se habían desarrollado integralmente las etapas posteriores asociadas a la determinación del riesgo residual, su aceptación cuando correspondiera, la definición y aplicación del tratamiento y el seguimiento a las medidas establecidas. Asimismo, la Declaración de Aplicabilidad – SoA se encontraba en proceso de construcción y su elaboración estaba prevista institucionalmente para el cuarto trimestre de 2026.

Si bien la programación establecida evidencia que la Entidad había definido una ruta para continuar la implementación de estos componentes durante el segundo semestre de 2026, al 31 de julio de 2026 aún no se había culminado la aplicación del proceso específico de valoración de los riesgos de seguridad de la información requerido por el MSPI.

Recomendaciones

1. Revisar y ajustar la Herramienta de Autodiagnóstico del MSPI, procurando que exista consistencia entre las fechas registradas, las calificaciones asignadas, las brechas identificadas y los soportes utilizados; asimismo, establecer para las brechas identificadas acciones claramente definidas, con responsable, fecha prevista y mecanismo de seguimiento hasta su cierre.
2. Revisar la clasificación y valoración de los controles asociados a los riesgos de pérdida de información e interrupción de los servicios tecnológicos, teniendo en cuenta el momento en que actúa cada control conforme a la Guía para la Gestión Integral del Riesgo en Entidades Públicas – versión 7 del DAFP y la Política para la Gestión Integral del Riesgo – PL-DES-001 de la Entidad, y ajustar, cuando corresponda, la valoración del riesgo residual.
3. Fortalecer el control definido para el riesgo fiscal asociado al daño de equipos tecnológicos, de manera que, además de verificar la inclusión de los equipos y mantenimientos en la planeación, contemple la verificación de que los mantenimientos programados se realicen efectiva y oportunamente, así como las acciones a seguir frente a incumplimientos.
4. Revisar la formulación y el control del riesgo de Integridad-Corrupción asociado a accesos privilegiados, procurando que la causa identifique claramente la condición que puede facilitar la materialización del riesgo; precisar qué aspectos se verifican mediante el control y revisar su clasificación de acuerdo con el momento en que actúa, evaluando el efecto de los ajustes sobre el riesgo residual.
5. Fortalecer las pruebas de restauración de respaldos, definiendo una periodicidad para su realización y conservando los soportes de su ejecución y resultados, con

el fin de verificar regularmente la recuperación efectiva de la información a partir de las copias de respaldo.

Realizó verificación y elaboró el informe:

Crhistian Augusto Amador León
Auditor Líder

Revisó y aprobó:

Andrea Reyes Saavedra
Jefe Oficina de Control Interno