Fecha de Emisión del Informe: 21-07-2025

Sistema auditado:	Sistema de Gestión de Seguridad de la Información - SGSI
Proceso(s) auditado(s):	Direccionamiento Estratégico, Comunicaciones y Cultura para la Movilidad, Seguridad Vial, Inteligencia para la Movilidad, Control y Evaluación de la Gestión, Control Disciplinario, Planeación de Transporte e Infraestructura, Ingeniería de Tránsito, Gestión Social, Gestión de Tránsito y Control de Tránsito y Transporte, Gestión de Trámites y Servicios para los Ciudadanos, Gestión Contravencional y Transporte Público, , Gestión Administrativa, Gestión Financiera, Gestión Jurídica, Gestión del Talento Humano y Gestión de TICS.
Dependencia(s) auditada(s):	Sede Calle 13 #37-35, Bogotá – virtual y presencial
Nombre y cargo del responsable del proceso / dependencia auditada:	Edgar Eduardo Romero Bohórquez Oficina de Tecnologías de la Información y las Comunicaciones – OTIC
Equipo auditor y Rol desempeñado:	Clara Patricia Muñoz Jiménez. Auditor Líder Leonardo Sierra Rodríguez. Equipo Auditor
Fechas de Ejecución de la auditora:	Fecha de Apertura: 14-07-2025 Fecha de Cierre: 17-07-2025

Objetivo de la auditoría	Determinar la conformidad del Sistema de Gestión de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad, con los requisitos y controles aplicables de la Norma ISO/IEC 27001:2022. Determinar la capacidad para asegurar el cumplimiento de los requisitos legales, reglamentarios y contractuales aplicables. Determinar la eficacia para asegurar que los objetivos específicos son razonablemente logrados y para identificar cuando aplique áreas de mejora potenciales.
Alcance de la auditoría:	"El Sistema de Gestión de la Información de la Secretaría Distrital de Movilidad, alineado al Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información que sea creada, procesada, transmitida o resguardada dentro de su sede principal por las partes interesadas y que a su vez hagan parte de los procesos misionales de la Entidad, como son: Planeación de transporte e infraestructura, Gestión social, Gestión de trámites y servicios para la ciudadanía, Gestión contravencional y transporte público, Gestión de tránsito y control de tránsito y transporte, Ingeniería de tránsito. De este mismo modo y siguiendo el enfoque del Sistema Integrado de Gestión, se contará con aquellos procesos estratégicos, de apoyo o de evaluación, cuyo objetivo contemple la implementación de controles de seguridad de la información de manera transversal para la Secretaría Distrital de Movilidad".

Criterios de la auditoría:	Norma ISO/IEC 27001:2022 Seguridad de la Información, ciberseguridad y protección de la privacidad. Sistemas de gestión de seguridad de la información. Requisitos.
Declaración del Auditor o Equipo Auditor:	En el desarrollo de la presente auditoría, el auditor o equipo de auditoría no fue sujeto de presiones indebidas, no presentó ningún tipo de impedimento que afectara su objetividad, actuó con el debido cuidado profesional y bajo los principios éticos y reglas de conducta del estatuto de auditoría.

RESUMEN EJECUTIVO

La auditoría tuvo un enfoque sistemático de recopilación, análisis y síntesis de la documentación revisada, entrevistas realizadas y evidencias identificadas, dando como resultado la identificación de una (1) oportunidad de mejora:

La auditoría interna de gestión se llevó a cabo con un enfoque sistemático orientado a la recopilación, análisis y síntesis de la documentación revisada, las entrevistas realizadas y las evidencias obtenidas. Como resultado, se identificó cero (0) no conformidad y una (1) oportunidad de mejora.

Tabla 1. Resultados de la Auditoría Interna

Resultados	Cantidad
No conformidad	0
Oportunidad de mejora	1
Total	**1**

DESARROLLO DE LA AUDITORÍA

Durante el desarrollo de la auditoría interna de gestión, se realizó el seguimiento al cumplimiento de los requisitos necesarios para establecer, implementar, mantener y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información (SGSI) en el periodo 2024. Para ello, se aplicaron métodos de auditoría conforme a la norma ISO 19011:2018, que incluyeron entrevistas, verificación mediante listas de chequeo, revisión documental y observación directa de las actividades, con la participación activa de los auditados, de acuerdo con el Plan de Auditoría PV01-IN03-F01 v2 del 07-07-2025.

El propósito fue evaluar el grado de conformidad del Sistema de Gestión de Seguridad de la Información - SGSI con los requisitos establecidos, así como su eficacia para alcanzar los objetivos de seguridad de la información de la Entidad y su mejora continua.

Tabla 2. Sesiones de auditoría interna ISO/IEC 27001:2022

Item	Reunión/Proceso	Criterios de Auditoría	Fecha- Hora
S00	Inicio de la auditoría interna	Presentación del Plan de Auditoría	Jul14/2025 8:30-9:00am
S01	Gestión TICS-OTIC	5,5.1,5.2,6.2, A5.4	Jul14/2025 9:00-10:30am
S02	Gestión del Talento Humano	5.3, 7.2, 7.3, A6, A5.2, A5.3	Jul14/2025 10:30-12:00m
S03	[*] 11 Procesos	6, 6.1.1, 6.1.2,6.1.3, 7.3	Jul14/2025 1:00-3:00pm
S04	Gestión TICS-OTIC	8, 8.1, 8.2, 8.3	Jul14/2025 3:00-5:00pm
S05	Gestión Administrativa	A5.9, A5.10, A5.11, A5.12, A5.13	Jul15/2025 8:00-10:00am
S06	Gestión TICS y Jurídica	6.3, 9.1, A5.31, A5.32, A5.33, A5.34, A5.35, A5.36	Jul15/2025 10:00-12:00m
S07	Gestión TICS y Control Interno	9.2, 9.3, 10.1, 10.2	Jul15/2025 1:00-3:00pm
S08	Gestión TICS y Direccionamiento Estratégico	4, 4.1, 4.2, 4.3, 4.4, 7.1	Jul15/2025 3:00-5:00pm
S09	Gestión TICS y Comunicaciones	7.4, 7.5, A5.1	Jul16/2025 8:00-10:00am
S10	Gestión TICS y Operador Tecn.	A5.3, A5.6, A5.7,A5.8, A8.1	Jul16/2025 10:00-12:00m
S11	Gestión TICS y Operador Tecnológico	A5.15, A5.16, A5.17, A5.18, A8.2, A8.3, A8.14, A8.15, A8.17, A8.18, A8.24	Jul16/2025 1:00-3:00pm
S12	Gestión TICS y Operador Tecnológico	A5.37, A8.6, A8.7, A8.8, A8.9, A8.10	Jul16/2025 3:00-5:00pm
S13	Gestión TICS y G. Administrativa	A7.1, A7.2, A7.3, A7.4, A7.5, A7.6, A7.7, A7.8, A7.9, A7.10, A7.11, A7.12, A7.13, A7.14.	Jul17/2025 8:00-10:00am
S14	Gestión TICS y Operador Tecnológico	A5.14, A8.11, A8.12, A8.13, A8.14, A8.15, A8.16, A8.17, A.8.19, A8.20, A8.21, A8.22, A8.23.	Jul17/2025 10:00-12:00m
S15	Gestión TICS y Operador Tecnológico	A.8.25, A8.26, A8.27, A8.28, A8.29, A8.30, A8.31, A8.32, A8.33, A8.34, A5.29, A5.30, A8.14	Jul17/2025 1:00-3:00pm
S16	Gestión TICS y Operador Tecnológico	A5.19, A5.20, A5.21, A5.22, A5.23, A5.24, A5.25, A5.26, A5.27, A5.28	Jul17/2025 3:00-5:00pm
S17	Cierre de la auditoría interna	Presentación de Resultados	Jul23/2025 2:00-3:00pm

[*] Seguridad Vial, Inteligencia para la Movilidad, Planeación de Transporte e Infraestructura, Ingeniería de Tránsito, Gestión Social, Gestión de Tránsito y Control de Tránsito y Transporte, Gestión de Trámites y Servicios para los Ciudadanos, Gestión Contravencional y Transporte Público, Control Disciplinario, Gestión Financiera y Gestión de TICS.

RESULTADOS DE LA AUDITORÍA

Oportunidad de Mejora No.1

Falta alineación del Sistema de Gestión de Seguridad de la Información - SGSI y la nueva versión del Modelo de Seguridad y Privacidad de la Información del MSPI de la Secretaría Distrital de Movilidad

Durante la auditoría interna realizada al Sistema de Gestión de Seguridad de la Información (SGSI) de la Secretaría Distrital de Movilidad -SDM, se evidenció que el sistema no se encuentra totalmente alineado con el Modelo de Seguridad y Privacidad de la Información -MSPI actualizado por el Ministerio de Tecnologías de la Información y las Comunicaciones -MinTIC, mediante la Resolución 02277 del 3 de junio de 2025, que sustituye al modelo contenido en el Anexo 1 de la Resolución 500 de 2021.

Esta situación evidencia que la Entidad se encuentra en proceso de incorporación de los requisitos actualizados de una parte interesada MinTIC, específicamente los de carácter reglamentario y obligatorio, dentro de su sistema de gestión. En consecuencia, se requiere realizar la alineación de los instrumentos SGSI y MSPI gestionando adecuadamente los requisitos externos que afectan la determinación del alcance del sistema de gestión de seguridad de la información (Numeral 4.3 y control A5.31).

En este contexto, y considerando que el Modelo de Seguridad y Privacidad de la Información - MSPI continúa siendo un habilitador clave para asegurar la confidencialidad, integridad, disponibilidad y privacidad de la información en el sector público, se recomienda actualizar oportunamente la información documentada del Sistema de Gestión de Seguridad de la Información - SGSI, de acuerdo con el impacto derivado de la expedición de la Resolución 02277 de 2025. Esta resolución adopta y actualiza el Anexo A del MSPI, alineándolo con los requisitos establecidos en la norma ISO/IEC 27001:2022. (Numeral 7.5.2).

CONCLUSIONES DE LA AUDITORÍA

Fortalezas

Compromiso de la alta dirección

La alta dirección evidencia un compromiso sólido y continuo con la seguridad de la información, garantizando la asignación adecuada de recursos, promoviendo una cultura organizacional orientada a la protección de la información y participando activamente en la toma de decisiones estratégicas. (Numerales 5.1, 5.2 y 5.3)

Políticas y procedimientos bien documentados

Se han desarrollado y mantenido políticas y procedimientos detallados y bien documentados que cubren todos los aspectos relevantes de la gestión del sistema de gestión de seguridad de la información - SGSI. (Numeral 5.2 y 7.5).

Cultura organizacional fortalecida a través de programas de capacitación y concienciación en seguridad de la información

Se implementan programas efectivos de capacitación y concienciación en seguridad de la información dirigidos a todo el personal y contratistas, garantizando que comprendan claramente sus roles y responsabilidades en la protección de la información. (Numerales 7.2 y 7.3).

Gestión de Seguridad de la información en la relación con Proveedores

Durante la auditoría interna, se evidenció que la Secretaría Distrital de Movilidad - SDM ha establecido y mantiene un proceso robusto para la gestión de relaciones con proveedores que acceden o procesan información relevante para el Sistema de Gestión de Seguridad de la Información - SGSI. (Numerales 8.1, 8.2 y 8.3).

Conclusiones

- A partir del ejercicio de auditoría, se evidencia que el Sistema de Gestión de Seguridad de la Información - SGSI es un sistema maduro y se mantiene implementado de forma eficaz, eficiente y efectivo, cumpliendo adecuadamente con los requisitos establecidos y controles aplicados bajo la norma ISO/IEC 27001:2022. Este desempeño refuerza el compromiso institucional con la protección de la información y consolida una base sólida para la gestión continua y tratamiento de los riesgos asociados a la seguridad de la información, ciberseguridad y protección de la privacidad.

- La Entidad evidencia un enfoque proactivo y sostenido hacia la protección de la información, a través de la implementación de acuerdos de confidencialidad y seguridad, que establecen límites claros respecto al acceso, manejo y divulgación de la información. Estos acuerdos constituyen un elemento fundamental del Sistema de Gestión de Seguridad de la Información SGSI. No obstante, para asegurar su vigencia y efectividad, se recomienda establecer y mantener los mecanismos formales de monitoreo y revisión periódica que garanticen su cumplimiento continuo.

- La Cultura organizacional fortalecida a través de programas de capacitación y concienciación en seguridad de la información no solo reside en impartir conocimientos técnicos, sino en lograr que todo el personal, contratistas y proveedores comprendan y asuman activamente sus responsabilidades frente a la protección de la información. Esto contribuye a minimizar los riesgos humanos, aumentar el cumplimiento normativo y asegurar una respuesta oportuna y adecuada ante incidentes de seguridad. Esta práctica responde a los requisitos 7.2 y 7.3 de la norma ISO/IEC 27001:2022, garantizando la competencia y conciencia del recurso humano como un pilar fundamental del Sistema de Gestión de Seguridad de la Información (SGSI).

- Fortalecer los indicadores clave de desempeño del Sistema de Gestión de Seguridad de la Información SGSI para alcanzar un nivel óptimo de seguridad. La identificación y tratamiento sistemático de oportunidades de mejora permitirá a la Secretaria Distrital de Movilidad - SDM robustecer su postura de seguridad, reducir riesgos, y asegurar el cumplimiento sostenido con los estándares y regulaciones aplicables. Estos esfuerzos contribuirán no solo a la protección de los activos de información, sino también al incremento de la confianza de las partes interesadas y a una mayor resiliencia institucional.

Recomendaciones

- Se recomienda formalizar la independencia funcional y organizacional de los roles de Oficial de Seguridad de la Información y de Oficial de Protección de Datos Personales, adscribiéndolos a un área transversal y estratégica como la Oficina Asesora de Planeación Institucional, donde se integran el Modelo Integrado de Planeación y Gestión (MIPG) y el Sistema Integrado de Gestión (SIG). Esta ubicación estratégica permite garantizar su autonomía frente a las áreas operativas y de tecnología, evitando posibles conflictos de interés y fortaleciendo su capacidad para supervisar, asesorar y escalar riesgos de seguridad y privacidad de la información con objetividad e imparcialidad. Además, al integrarse al núcleo de gobernanza institucional, estos roles pueden alinear sus acciones con la planeación estratégica, la gestión del riesgo, la mejora continua y el cumplimiento normativo, conforme a los numerales 5.3 (Roles y responsabilidades organizacionales) y 6.1.3 (Tratamiento de riesgos de seguridad de la información) de la norma ISO/IEC 27001:2022.

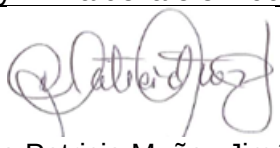
  Esta medida también permite una mejor articulación con las políticas públicas en materia de protección de datos y ciberseguridad, fortaleciendo la cultura institucional de protección de la información y asegurando la trazabilidad y eficacia del SGSI y del Programa de Gestión de Datos Personales.

- La adopción e implementación de los nuevos controles, en particular al relacionado con la inteligencia de amenazas, el cual depende directamente de la contratación de servicios especializados de un Centro de Operaciones de Seguridad (SOC). Durante la auditoría se evidenció la generación del documento Anexo Técnico asociado a estos servicios. Se evidencia la necesidad de agilizar el proceso de contratación actualmente en curso y establecer una planificación adecuada que garantice la seguridad y continuidad del servicio de la Secretaría Distrital de Movilidad.

- Continuar fortaleciendo las actividades de sensibilización y generación de capacidades en seguridad de la información, asegurando un enfoque continuo en la concienciación del personal sobre amenazas actuales, buenas prácticas en ciberseguridad y medidas de protección de la privacidad. Estas acciones contribuyen significativamente al desarrollo de una cultura institucional orientada a la seguridad, al cumplimiento de los requisitos del SGSI y a la reducción de riesgos derivados del factor humano.

ANEXOS

- PV01-IN03-F02 Lista de Verificación Sesión 1 Jul14_2025
- PV01-IN03-F02 Lista de Verificación Sesión 2 Jul14_2025
- PV01-IN03-F02 Lista de Verificación Sesión 3 Jul14_2025
- PV01-IN03-F02 Lista de Verificación Sesión 4 Jul14_2025
- PV01-IN03-F02 Lista de Verificación Sesión 5 Jul15_2025
- PV01-IN03-F02 Lista de Verificación Sesión 6 Jul15_2025
- PV01-IN03-F02 Lista de Verificación Sesión 7 Jul15_2025
- PV01-IN03-F02 Lista de Verificación Sesión 8 Jul15_2025
- PV01-IN03-F02 Lista de Verificación Sesión 9 Jul16_2025
- PV01-IN03-F02 Lista de Verificación Sesión 10 Jul16_2025
- PV01-IN03-F02 Lista de Verificación Sesión 11 Jul16_2025
- PV01-IN03-F02 Lista de Verificación Sesión 12 Jul16_2025
- PV01-IN03-F02 Lista de Verificación Sesión 13 Jul17_2025
- PV01-IN03-F02 Lista de Verificación Sesión 14 Jul17_2025
- PV01-IN03-F02 Lista de Verificación Sesión 15 Jul17_2025
- PV01-IN03-F02 Lista de Verificación Sesión 16 Jul17_2025

Nombre y firma del equipo auditor:	Nombre y Firma de la o el Auditor Líder
 Leonardo Sierra Rodríguez	 Clara Patricia Muñoz Jiménez