Fecha de Emisión del Informe: 05-08-2026

Sistema auditado:	**SGSI - NTC ISO/IEC 27001:2022**
Proceso(s) auditado(s):	• Inteligencia para la Movilidad • Gestión de Trámites y Servicios a la Ciudadanía • Gestión de Tránsito y Control de Tránsito y Transporte • Control Disciplinario • Gestión de TICS • Comunicaciones y Cultura para la Movilidad • Seguridad Vial • Planeación de Transporte e Infraestructura • Direccionamiento Estratégico • Talento Humano • Ingeniería de Tránsito • Gestión Social • Gestión Contravencional y Transporte Público • Gestión Financiera • Gestión Jurídica • Gestión Administrativa • Control Interno
Dependencia(s) auditada(s):	• Gestión del Talento Humano • Inteligencia para la Movilidad Gestión de TICS-OTIC (Seguridad de la Información) • Gestión de Trámites y Servicios a la Ciudadanía • Gestión de Tránsito y Control de Tránsito y Transporte • Control Disciplinario • Ingeniería de Tránsito • Gestión Social • Gestión Contravencional y Transporte Público • Gestión Financiera • Seguridad Vial • Planeación de Transporte e Infraestructura • Gestión de TICS-OTIC (Seguridad de la Información) • Gestión Administrativa • Operador Tecnológico • Gestión Jurídica • Control Interno • Direccionamiento Estratégico-OAPI • Comunicaciones y Cultura para la Movilidad

Nombre y cargo del responsable del proceso / dependencia auditada:	Edgar Eduardo Romero Bohorquez - OTIC Seguridad de la Información
Equipo auditor y Rol desempeñado:	Oscar Alberto Barragán León - Auditor Líder Sergio Eduardo Reyes Trillos - Auditor
Fechas de Ejecución de la auditora:	Fecha de Apertura: 22-07-2026 Fecha de Cierre: 05-08-2026

Objetivo de la auditoría	Evaluar la conformidad, implementación y eficacia del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de Movilidad - SDM, respecto a los requisitos de la norma ISO/IEC 27001:2022 y controles del Anexo A, asociados. Determinar la capacidad para asegurar el cumplimiento en la Entidad de los objetivos del SGSI, los requisitos legales, reglamentarios y contractuales, y los controles relacionados.
Alcance de la auditoría:	La auditoría se aplica a la seguridad sobre 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 lo 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:	Los criterios de auditoría son los requisitos de la norma y los procesos establecidos, así como la documentación del sistema de gestión de la Entidad. El objetivo de la auditoría es confirmar el cumplimiento del sistema de gestión SGSI con los criterios de auditoría, para determinar la capacidad del sistema de gestión y garantizar que la organización cumpla con los requisitos legales y de otro tipo, pero no es una auditoría de cumplimiento con la legislación. Además, el objetivo es determinar si la efectividad del sistema de gestión permite alcanzar los objetivos establecidos e identificar áreas para una mejora potencial.
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.

Nota: Los pies de página y el ejemplo planteado, son elementos orientadores al momento de elaborar el respectivo informe, por favor no los incluya en la emisión del informe.

RESUMEN EJECUTIVO[1]

Resultados	Cantidad
No conformidad	01
Oportunidad de mejora	03
Total	04

DESARROLLO DE LA AUDITORÍA[2]

OBJETIVO DE LA AUDITORÍA

Evaluar la conformidad, implementación y eficacia del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de Movilidad - SDM, respecto a los requisitos de la norma ISO/IEC 27001:2022 y controles del Anexo A, asociados. Determinar la capacidad para asegurar el cumplimiento en la Entidad de los objetivos del SGSI, los requisitos legales, reglamentarios y contractuales, y los controles relacionados.

DESCRIPCIÓN DE LA COMPAÑÍA AUDITADA Y SUS ACTIVIDADES

DETALLES DE LA ENTIDAD.

La Secretaría Distrital de Movilidad formula e implementa políticas y estrategias para una movilidad segura, sostenible, inclusiva y accesible, que contribuyan al bienestar y la calidad de vida de la ciudadanía, promoviendo la cultura ciudadana, la protección de la vida, el espacio público para la movilidad y el uso eficiente de medios de transporte en Bogotá y la región, con una gestión de trámites y servicios integral y transparente, y un equipo humano que genera confianza en la ciudadanía y en la Entidad.

OBJETIVOS ESTRATÉGICOS

1. Proteger vidas en el espacio público para la movilidad, a través de la formulación e implementación de proyectos e intervenciones, así como el fomento de la cultura ciudadana.

[1] Describa en un párrafo no mayor a 6 líneas el resultado de la auditoría realizada.

[2] Relación clara y dimensionada de las conclusiones y recomendaciones derivadas de las pruebas o procedimientos de auditoría desarrollados. En este espacio, registre la metodología (Reunión de Apertura, Entrevistas, Encuestas etc.), muestra, limitaciones y en si los aspectos revisados.

2. Prestar trámites y servicios confiables, eficientes, oportunos y de calidad, mediante el uso de tecnologías y seguridad de la información y las comunicaciones, innovación, gestión del conocimiento, promoción de la participación incidente y formación ciudadana.
3. Fortalecer el uso de medios de transporte sostenibles y alternativos mediante políticas de movilidad amigables con el ambiente y con un enfoque diferencial e incluyente.
4. Consolidar un equipo humano calificado, comprometido e íntegro fomentando su bienestar, la lucha contra la corrupción, la protección de recursos públicos y el cumplimiento normativo.
5. Mejorar la calidad de vida y bienestar de la ciudadanía a través de políticas, programas y acciones de gestión, innovación, control en vía, prestación de servicios y optimización de la infraestructura para la Movilidad en Bogotá – Región.

La plataforma estratégica fue adoptada mediante Resolución 759884 del 11 de diciembre de 2024 y rige a partir del 01 de enero de 2025.

SISTEMAS DE GESTIÓN

Los sistemas de gestión Secretaría Distrital de Movilidad conforman un conjunto integral bajo el Modelo Integrado de Planeación y Gestión (MIPG). Estos sistemas están diseñados para garantizar la mejora continua y el fortalecimiento del desempeño institucional de la entidad.

El Sistema Integrado de Gestión de la Secretaría de Movilidad está compuesto por siete sistemas de gestión (Sistema de Gestión Ambiental, Antisoborno, de Calidad, de Continuidad del Negocio, Empresa Familiarmente Responsable, de Seguridad de la Información y de Seguridad y Salud en el Trabajo) que trabajan de manera coordinada para optimizar procesos, promover la transparencia y asegurar el cumplimiento de las normativas vigentes.

Entre los sistemas destacados se encuentran el Sistema de Gestión de Calidad, el Sistema de Gestión Ambiental, y el Sistema de Seguridad y Salud en el Trabajo, que contribuyen a una administración pública eficiente y orientada a resultados.

El compromiso de la Secretaría con la mejora continua impulsa la actualización constante de estos sistemas, garantizando un servicio público de alta calidad que responde a las necesidades de la ciudadanía.

Esta estructura integral fortalece la cultura organizacional, fomenta la responsabilidad institucional y permite una gestión transparente y efectiva en todas las áreas.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información SGSI de la Secretaría Distrital de Movilidad está definido como un enfoque sistemático para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información de la Organización y lograr sus objetivos y/o servicios.

Tiene definido como objetivo general proteger y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de la Secretaría Distrital de Movilidad, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la Entidad.

Como objetivos específicos ha definido:

- Gestionar los activos de información, salvaguardándolos ante cualquier incidente que pueda provocar su destrucción, divulgación, indisponibilidad o uso no compartido.
- Gestionar los riesgos de seguridad de la información aplicando los controles necesarios para cada situación, garantizando la sostenibilidad de las operaciones.
- Fortalecer la cultura de seguridad de la información, brindando concientización y sensibilización permanente a cada colaborador, para enfrentar proactiva y reactivamente las amenazas a las que se exponen en el manejo diario de la información propia y de terceros.
- Establecer mecanismos que permitan mantener la seguridad de la información durante una interrupción de la infraestructura tecnológica que soporta la operación de los servicios ofrecidos por la Entidad.
- Gestionar los eventos e incidentes de seguridad de la información, fortaleciendo la capacidad de la Secretaría Distrital de Movilidad para hacer frente a las amenazas y ataques informáticos.

Permitiendo a la Entidad entre otros aspectos:

- Analizar los riesgos, identificar las amenazas, vulnerabilidades e impactos sobre los activos de información de la Secretaría Distrital de Movilidad.
- Reducir los riesgos que pueden producir pérdidas o afectar la integridad, confidencialidad y disponibilidad de nuestra información.
- Garantizar la continuidad del servicio tras un incidente de seguridad de seguridad de la información de alto impacto.

ALCANCE DE LA AUDITORÍA

La auditoría se aplica a la seguridad sobre 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 lo 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.

ÁREAS EXCLUIDAS DE LA AUDITORÍA

No se evidencian áreas excluidas dentro del alcance del SGSI. La Declaración de Aplicabilidad Código: PA04-P01-F03, versión de actualización 3, vigente desde el 16/07/2025, mantiene la aplicabilidad de los controles definidos para la operación.

OBJETIVOS DE AUDITORIA

Objetivos de la auditoría, donde metodológicamente puede 1) confirmar el cumplimiento del sistema de gestión del cliente con los criterios de auditoría, 2) determinar la capacidad del sistema de gestión para garantizar que la organización cumple con los requisitos legales, regulatorios y contractuales aplicables, y 3) lograr los objetivos especificados, ya que el sistema de gestión puede identificar áreas de mejora potencial, incluida la revisión de la administración y las auditorías - Se cumplieron.

PROCEDIMIENTO DE AUDITORÍA

EXENCIÓN DE RESPONSABILIDAD

La auditoría se basa en un proceso de muestreo de la información disponible y, en consecuencia, siempre habrá un elemento de incertidumbre presente en la evidencia de auditoría, que puede reflejarse en los hallazgos de la auditoría. Quienes dependen o actúan sobre los resultados y conclusiones de la auditoría deben tener en cuenta esta incertidumbre.

PARTICIPANTES EN LA REUNIÓN DE CIERRE Y DE APERTURA

Participan en las reuniones de apertura y cierre los responsables de los procesos auditados: Inteligencia para la Movilidad, Gestión de Trámites y Servicios a la Ciudadanía, Gestión de Tránsito Y Control de Tránsito y Transporte, Control Disciplinario, Gestión de TICS, Comunicaciones y Cultura para la Movilidad, Seguridad Vial, Planeación de Transporte e Infraestructura, Direccionamiento Estratégico, Talento Humano, Ingenieria de Tránsito, Gestión Social, Gestión Contravencional y Transporte Público, Gestión Financiera, Gestión Jurídica, Gestión Administrativa y Control Interno. La participación evidencia continuidad del equipo clave frente a la auditoría anterior y adecuada representación de los procesos vinculados al SGSI.

DESCRIPCIÓN DEL MUESTREO Y ESTADÍSTICAS DE MUESTREO

Se realizó muestreo sobre los procesos incluidos en el alcance del SGSI y los numerales definidos en el plan de auditoría. La revisión consideró evidencia documental, entrevistas y registros asociados a operación, desarrollo, soporte, gestión de accesos, riesgos, continuidad y prestación del servicio.

RESULTADOS DE LA AUDITORÍA

Matriz de cumplimiento - ISO/IEC 27001:2022

Elemento de la norma	Grado de cumplimiento	Verificación en la próxima auditoría
Entendimiento de la organización y su contexto (4.1)		SI
Entendimiento de las necesidades y expectativas de las partes interesadas (4.2)		SI
Determinación del alcance del sistema de gestión de la seguridad de la información (4.3)		SI
Sistema de gestión de la seguridad de la información (4.4)		SI
Liderazgo (5)		SI
Medidas dirigidas a riesgos y oportunidades (6.1)		SI
Objetivos de seguridad de la información, y planeación para alcanzarlos (6.2)		SI
Recursos (7.1)		SI
Competencia (7.2)		SI
Conciencia (7.3)		SI
Comunicación (7.4)		SI
Información documentada (7.5)		SI
Planeación operacional y control (8.1)		SI
Evaluación del riesgo de la seguridad de la información (8.2)		SI
Tratamiento de riesgos de la seguridad de la información(8.3)		SI
Vigilancia, medición, análisis y evaluación (9.1)		SI
Auditoría interna (9.2)		SI
Revisión por la dirección (9.3)		SI
No conformidades y acciones correctivas (10.2)		SI
Mejora continua (10.1)		SI

Se cumplen de manera adecuada tanto los requisitos de la norma como el expediente de gestión. Se reconocen determinadas deficiencias pendientes que son resueltas durante el proceso.

Se cumplen tanto los requisitos de la norma y expediente de gestión. No siempre se reconocen/eliminan deficiencias encontradas durante el proceso; o se encuentran bajo requisitos de la norma sin beneficio para la empresa. El auditor puede hacer excepciones

No se cumplen de manera adecuada tanto los requisitos de la norma como el expediente de gestión. El auditor opta por la excepción o no conformidad de acuerdo a su extensión e impacto en la funcionalidad del sistema

CONSOLIDADO DE HALLAZGOS DE AUDITORÍA (NC - OM).
NC: No Conformidad
OM: Oportunidad de Mejora

No Conformidad (NC).

NC 1 - Deficiencias en la seguridad física del cableado y servicios eléctricos

- Numerales / controles afectados: A.7.12 seguridad del cableado.
- Declaración del hallazgo: La organización no está asegurando que el cableado de energía y de telecomunicaciones esté protegido de manera adecuada contra interceptación, interferencia o daños físicos, ni está garantizando instalaciones eléctricas seguras en las áreas de trabajo.

Evidencia objetiva:

1. Sala de juntas Jiménez: Se observan cables de red colgando sin canalización, sujetos con abrazaderas plásticas, y múltiples puntos eléctricos/de red sin tapas de protección.
2. Cuarto de control: Cableado fuera de la línea de protección, cables cortados y encintados, uniones de cable UTP realizadas con soldadura (degradando la señal) y cables con blindaje dañado.
3. Puestos de trabajo (QT80, JM63, JM59): Equipos operando con extensiones eléctricas y adaptadores tipo "T" sobre la superficie de trabajo, anulando la conexión a tierra física.
4. Sala de juntas mezanine: Cámaras de seguridad con instalaciones eléctricas deficientes (cinta aislante) y cables apretados contra la tubería eléctrica.

Oportunidad de Mejora (OM).

OM 1 - Precisión en la apreciación de riesgos (Identificación de amenazas)

- Numerales / Controles afectados: 6.1.2 Evaluación de riesgos de seguridad de la información.
- Descripción: Al revisar la matriz de riesgos del aplicativo "Observatorio" respecto a la pérdida de disponibilidad, se evidenció que se incluyó la "Falta de mantenimiento" catalogada como una amenaza.
- Recomendación: Se recomienda reevaluar la taxonomía de riesgos del sistema. El mantenimiento de plataformas es un proceso interno controlado; por ende, su omisión constituye una "vulnerabilidad" o una "falla operativa", no una amenaza probabilística de origen externo o incontrolable.

OM 2 - Protección de la información de autenticación (Credenciales en navegador)

- Numerales / Controles afectados: A.5.18 Información de autenticación, A.8.1 Dispositivos de punto final.
- Descripción: Durante las entrevistas y revisiones de campo, se identificó la práctica de guardar contraseñas de acceso a los sistemas de información corporativos directamente en el gestor de credenciales nativo del navegador web de los puestos de trabajo.
- Recomendación: Se sugiere fortalecer los controles técnicos mediante la implementación de políticas de dominio (GPO) que deshabiliten la opción de guardar contraseñas en los navegadores web institucionales. Como medida complementaria, se recomienda reforzar la Toma de Conciencia (7.3) sobre los riesgos de esta práctica o proveer un gestor de contraseñas corporativo centralizado y seguro.

VERIFICACIÓN DE OPORTUNIDAD DE MEJORA DESDE LA AUDITORÍA PREVIA

OM 3 - A.5.3 Rol del Oficial de Seguridad
En el marco de la presente auditoría, se realizó la evaluación a la oportunidad de mejora (OM) generada durante la Auditoría etapa II ISO/IEC 27001:2022, segundo seguimiento, noviembre de 2025, con el propósito de verificar el grado de avance, cumplimiento y efectividad de las acciones definidas, así como la existencia de evidencias que respalden su ejecución y contribuyan a la mitigación de los riesgos asociados. Para tal efecto, se analizó la coherencia entre los hallazgos identificados, las acciones formuladas, los responsables asignados, los plazos establecidos y los mecanismos de seguimiento implementados.

- 1 OM: A.5.3 Rol del Oficial de Seguridad

Se identifica la oportunidad de fortalecer la independencia y claridad del rol del responsable del MSPI. Se recomienda designar un Oficial de Seguridad o responsable del MSPI que dependa de un área estratégica distinta a la de Tecnología, con el fin de evitar conflictos de interés y garantizar una adecuada segregación de funciones en la gestión de la seguridad y privacidad de la información.

En caso de no existir el cargo dentro de la estructura organizacional, este deberá ser delegado mediante acto administrativo, asegurando su participación formal con voz y voto en el Comité Institucional de Gestión y Desempeño, y con voz en el Comité de Control Interno, para asegurar su intervención efectiva en la toma de decisiones relacionadas con el MSPI.

En relación con la oportunidad de mejora asociada, se evaluó el avance formulado por la dependencia responsable la Oficina TIC, evidenciando el envío de comunicaciones (25 de febrero y 24 de julio de 2026) a la Oficina Asesora de Planeación Institucional y a la Dirección de Talento Humano y por parte del Jefe de Oficina de Tecnologías de la Información y las Comunicaciones, en la cual realiza solicitud de revisión independencia funcional del oficial de seguridad de la información, y Alcance al Memorando No. 202612000034663 – Solicitud revisión independencia funcional del oficial de seguridad de la información, respectivamente, resaltando entre otros apartes :

En concordancia con los lineamientos actualizados del Modelo de Seguridad y Privacidad de la Información (MSPI), adoptados mediante la Resolución 2277 de 2025 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, la cual armoniza el modelo con la norma internacional ISO/IEC 27001:2022 con el propósito de fortalecer la gestión integral de la seguridad y la privacidad de la información en las entidades públicas, se identifica la pertinencia de fortalecer la independencia funcional del rol del Oficial de Seguridad de la Información, con el fin de garantizar una adecuada segregación entre las funciones asociadas a la implementación, administración y operación de los controles tecnológicos y la funciones de supervisión, evaluación, seguimiento y reporte del cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) y del MSPI.

Así mismo, la norma ISO/IEC 27001:2022, en su cláusula 5.3 y en el control A.5.3, establece que las responsabilidades y autoridades deben estar claramente definidas y que la segregación de deberes es un mecanismo esencial para prevenir conflictos de interés y reducir riesgos operacionales. En coherencia con ello, el MSPI actualizado exige una estructura de gobernanza que garantice liderazgo, asignación clara de responsabilidades y capacidad efectiva de reporte a la alta dirección.

Por ello la Oficina TIC, solicita evaluar y redefinir la ubicación organizacional del Oficial de Seguridad de la Información, con el fin de establecer una dependencia funcional de nivel estratégico, separada de la operación tecnológica, que asegure la independencia, imparcialidad y eficacia en la supervisión y control del Sistema de Gestión de Seguridad de la Información (SGSI), lo cual constituye un avance frente a la situación inicialmente identificada.

No obstante, la cobertura y ejecución integral de la acción no presenta respuesta completa a las solicitudes realizadas y no se cuenta aún con evidencia de actualización formal ni con soporte que permita verificar la validación de los controles requeridos.

En consecuencia, aunque se reconocen avances en la atención del hallazgo, estos no resultan suficientes para dar cumplimiento total a la acción formulada ni para mitigar de manera integral el riesgo identificado, motivo por el cual el resultado de la evaluación de la OM es Parcialmente cumple (50) y el hallazgo permanece abierto, a la espera de la ejecución completa de las acciones y del seguimiento correspondiente.

CONCLUSIONES DE LA AUDITORÍA

CONCLUSIONES Y RECOMENDACIONES

Como resultado de la auditoría para evaluar la conformidad, implementación y eficacia del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de Movilidad - SDM, respecto a los requisitos de la norma ISO/IEC 27001:2022 y controles del Anexo A, asociados, se concluye que la entidad cuenta con una adecuada gestión de la seguridad de la información, reflejada en una estructura de gobernanza definida, controles técnicos operativos activos y compromiso de la alta dirección con el control interno y la protección de la información.

De igual forma en la capacidad para asegurar el cumplimiento en la Entidad de los objetivos del SGSI, los requisitos legales, reglamentarios y contractuales, y los controles relacionados, la auditoría evidenció que el SGSI se encuentra implementado con un Alto nivel de madurez. Existe consolidación del sistema, con énfasis en la adopción de los requisitos de la norma y la totalidad de los 93 controles del Anexo A requeridos, incluyendo los nuevos once controles en su versión ISO 27001:2022, sin embargo, se observaron debilidades que limitan su consolidación, en particular, se identifican brechas en el control A.7.12 Seguridad del cableado contra interceptación, interferencia o daños físicos, así como en garantizar instalaciones eléctricas seguras en las áreas de trabajo, por lo que se recomienda implementar planes de tratamiento tendientes a remediar las causas generadores del riesgo, incluyendo campañas de sensibilización y seguimiento continuo a los planes definidos.

Las pruebas de recorrido a los centros de datos - datacenter, centros de procesamiento de la información y centros de cableado, evidencian que existen controles físicos en funcionamiento, sin embargo, la protección de la infraestructura tecnológica en alguno de ellos no es homogénea ni integral frente a los riesgos actuales del entorno físico y ambiental (Ej: centro de cableado 1 piso 2). Estas debilidades representan riesgo para la continuidad de los servicios tecnológicos y la disponibilidad de la información institucional, por lo que se recomienda atención prioritaria.

En la revisión a los controles A.5.18 Información de autenticación y A.8.1 Dispositivos de punto final se observó la práctica de guardar contraseñas de acceso a los sistemas de información corporativos directamente en el gestor de credenciales nativo del navegador web de los puestos de trabajo, por lo que se recomienda fortalecer los controles mediante la implementación de políticas de dominio (GPO) que deshabiliten la opción de guardar contraseñas en los navegadores web institucionales. Como medida complementaria, se recomienda reforzar la Toma de Conciencia (7.3) sobre los riesgos de esta práctica o proveer un gestor de contraseñas corporativo centralizado y seguro.

En lo relacionado con la consolidación del control centralizado sobre equipos de usuario final, actualización e instalación de software (controles A.5.22 seguridad de la información en la relación con proveedores, A.8.19 Instalación de software en sistemas operativos), se observaron algunas inconsistencias, como el equipo de cómputo asignado al contratista externo, Ingeniero Ubolmester, operando con el sistema operativo Windows en estado inactivo, sin licencia válida. Se recomienda priorizar su implementación para fortalecer la seguridad, el monitoreo, la actualización y restricción de software no autorizado y protección de endpoints.

Se evidencia gestión de proveedores y aceptación de términos de servicios en la nube o cloud. No obstante, se recomienda fortalecer la trazabilidad del seguimiento periódico sobre la seguridad, protección de datos, actualizaciones y parches, así como conexiones a la red y servicios de la Secretaria Distrital de Movilidad SDM, que considere los dispositivos, equipos y sistemas de los proveedores críticos, especialmente aquellos que soportan servicios en la nube, operador tecnológico, comunicaciones, autenticación, almacenamiento, disponibilidad y operación de la plataforma, dejando evidencia de revisión, riesgos asociados y cambios relevantes.

El equipo auditor recomienda mantener la certificación en razón que se evidencia que la Secretaría Distrital de Movilidad SDM adopta e implementa el Sistema de Gestión de Seguridad de la Información alineado con la norma ISO/IEC 27001:2022 y los requisitos estatutarios, reglamentarios y contractuales pertinentes al enfoque de la entidad.

ANEXOS

Nota[3]

Nombre y firma del equipo auditor:	Nombre y Firma de la o el Auditor Líder
 Oscar Alberto Barragán León - Auditor Líder  Sergio Eduardo Reyes Trillos - Auditor	 Oscar Alberto Barragán León - Auditor Líder

[3] **Los informes en desarrollo de las auditorías deben ser:**

a) **Precisos** (Diga lo que tiene que decir. Es conveniente ser exacto (puntual) en cada frase y en el informe completo. Su redacción debe ser sencilla, clara, ordenada, coherente y en orden de importancia).
b) **Concisos** (La redacción debe ser breve, pero sin omitir lo relevante, la brevedad permite mayor impacto. Se debe buscar la forma de redactar los hallazgos en forma concreta, pero sin dejar de decir lo que se tiene que decir sobre la condición (situación detectada); asimismo, se debe incluir la fuente de criterio, el criterio de auditoría).
c) **Objetivo** (Todas las No Conformidades deben reflejar una situación real, manejada con criterios técnicos, analíticos e imparciales).
d) **Soportado** (Las afirmaciones, conceptos, opiniones y hallazgos, deben estar respaldadas con evidencia válida, suficiente, pertinente y competente).
e) **Oportuno** (Debe cumplir los términos de elaboración, consolidación, entrega, comunicación y publicidad).