Fecha de Emisión del Informe: 25-09-2024

Sistema auditado:	**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 y Control Interno.
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 – Jefe OTIC
Equipo auditor y Rol desempeñado:	Juan Pablo Peralta – Auditor Líder Diana Patricia Murillo – Equipo Auditor
Fechas de Ejecución de la auditora:	Fecha de Apertura: 05-09-2024 Fecha de Cierre: 25-09-2024

Objetivo de la auditoría	Verificar que el Sistema de gestión de seguridad de la información -SGSI- Se mantiene de manera eficaz, eficiente y efectiva para satisfacer los requisitos conforme a los requisitos del estándar ISO/IEC 27001:2022. • Determinar la conformidad del sistema de gestión con los requisitos del estándar de sistema de gestión. • Evaluar la capacidad del sistema de gestión para asegurar el cumplimiento de los requisitos. legales y reglamentarios aplicables al alcance del sistema de gestión y a la norma de requisitos de gestión. • Determinar la eficaz implementación y mantenimiento del sistema de gestión • Identificar oportunidades de mejora en el sistema de gestión.
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 publico • 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:	ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements
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 dos (2) no conformidades y cuatro (4) oportunidades de mejora:

Resultados	Cantidad
No conformidad	**2**
Oportunidad de mejora	**4**
Total	**6**

DESARROLLO DE LA AUDITORÍA

En el desarrollo de la auditoría se realizó el seguimiento a los requisitos para establecer, implementar, mantener y mejorar continuamente el sistema de gestión de seguridad de la información, durante el periodo 2024. Para ello, se aplicaron métodos de auditoría según la norma ISO 19011:2018 mediante la realización de entrevistas, completar listas de verificación, revisión de documentos y observación del trabajo realizado, con la participación del auditado.

RESULTADOS DE LA AUDITORÍA

No conformidad No 01

El formato utilizado para registrar los cambios no considera la opción para la descripción de actividades de *rollback*.

Durante la revisión del formato *PA04-PR04-F01 RFC para componentes de infraestructura tecnológica, comunicaciones y sistemas de información*, no se evidencia un apartado para contemplar las acciones de marcha atrás o plan de “retirada del cambio” (rollback) en caso de un incorrecto funcionamiento tras su implementación, como consta en el documento *PA04-M01 Manual de políticas específicas de seguridad de la información*, lo anterior contraviene el control *A.8.32 Gestión del cambio*, al no adoptar e implementar apropiadamente el lineamiento de la política.

No conformidad No 02

Falta de actualización del Sistema Operativo en algunos Servidores.

En el marco de la auditoría realizada conforme a la norma ISO 27001:2022, se ha identificado no conformidad en relación con el control *A.8.19 Instalación de software en sistemas operativos*. Se realizó la validación del inventario de los servidores de propiedad de la SDM, mediante una toma de muestra de seis (6) servidores de cuarenta y un (41) servidores, evidenciando que estos seis (6) equipos cuentan con versiones de Windows 2003, 2008 y 2012, las cuales ya han finalizado el soporte de Microsoft.

El responsable comenta que existen sistemas de información heredados que no admiten las actualizaciones; no obstante, no se evidencia la aplicación de aceptación de riesgos con el análisis adecuado que permita establecer medidas complementarias de control.

Oportunidad de Mejora No 01

De acuerdo con lo manifestado en el documento *Guía para la Gestión de Riesgos*, el numeral 5 detalla la identificación y valoración de los riesgos para la seguridad de la información, se valida en el formato de inventario de activos de información del proceso Gestión TICS los activos con criticidad “critica” el campo del “Riesgo Asociado” derivado del mapa de riesgos de dicho proceso, encontrando que este no está identificado. Por lo anterior se recomienda actualizar en el inventario de activos de información el ID del riesgo asociado, según la criticidad del activo de información.

Oportunidad de Mejora No 02

El documento *PA04-M01 Manual de Políticas específicas de seguridad de la información*, numeral 5.6 brinda lineamientos para el bloqueo de las estaciones de trabajo cuando los usuarios se retiren del puesto, se validó sobre el cumplimiento y se identificaron usuarios que no están aplicando esta política, por lo tanto, se recomienda fortalecer los controles para evitar e impedir que otras personas puedan usar el escritorio y acceda a los datos en el momento en que los equipos queden desatendidos.

Oportunidad de Mejora No 03

Conforme con la Norma ISO/IEC 27001:2022, control *A.7.10 Medios de almacenamiento* y teniendo en cuenta que el operador Alpopular se encarga del almacenamiento, custodia de las cintas, trasporte y restauración de *backup* de la SDM, se recomienda realizar visitas en sitio para verificar el lugar donde se están almacenando dichas cintas de backup. Esta verificación permite asegurar que se cumplan con las medidas de seguridad física para proteger los respaldos, que son esenciales para la recuperación en caso de perdida, daño o ataques a la infraestructura.

Oportunidad de Mejora No 04

De acuerdo con lo dispuesto en el documento *PA04-M01 Manual de políticas específicas de seguridad de la información, numeral 5.40 Política de Gestión de Incidentes de Seguridad de la información* y el documento *PA04-G01 Guía de gestión de incidentes*, y teniendo en cuenta que todos los funcionarios y contratistas pueden reportar posibles eventos y/o incidentes de correos sospechosos, se sugiere ajustar las respuestas que se dan al usuario de tal manera que se incluyan recomendaciones claves sobre cómo actuar frente a posibles intentos de *phishing* o correos fraudulentos, por ejemplo: validar el remitente, no hacer clic en enlaces ni descargar adjuntos de correos desconocidos, no compartir información personal o financiera, entre otros.

CONCLUSIONES DE LA AUDITORÍA

Fortalezas

- La Secretaría Distrital de Movilidad cuenta con un modelo de empresarial por procesos que ha permitido orientar sus necesidades, aplicando de manera estructurada los lineamientos del Modelo Integrado de Planeación y Gestión.
- Se cuenta con una plataforma estratégica consolidada por medio del Sistema Integrado de Gestión que permite el seguimiento y cumplimiento de las metas definidas.
- El compromiso de la alta dirección en asegurar la disponibilidad de los recursos necesarios para el SGSI, brindando un conjunto de plataformas tecnológicas de información y comunicaciones modernas, además de facilitar la adopción de procesos tercerizados que facilitan la gestión.
- La entidad cuenta con un equipo de profesionales con las competencias suficientes para la ejecución eficaz de los roles definidos en el SGSI.
- En relación con el inventario de activos de información, la entidad realiza la identificación, clasificación, valoración, aprobación y la publicación de estos; lo anterior permite el cumplimiento de la Ley 1712 del 2014, Artículo 13, Registro de Activos de Información.
- La entidad identifica y actualiza los requisitos legales y regulatorios aplicables a la seguridad de la información incluyendo las leyes, regulaciones específicas y las normas internacionales como la norma ISOIIEC 27001:2022.
- Las políticas y procedimientos evidenciados se encuentran documentados de manera clara y comprensible.

Conclusiones

- Con el ejercicio de auditoría se evidencia que el SGSI se mantiene de manera eficaz, eficiente y efectiva satisfaciendo de manera apropiada los requisitos del estándar ISO/IEC 27001:2022, reforzando su compromiso con la protección de la información y estableciendo

bases solidas para la gestión de los riesgos de seguridad de la información de manera continua.

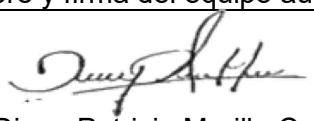
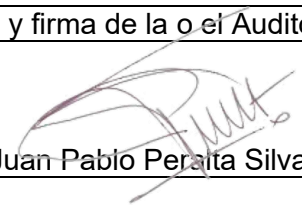
- La entidad demuestra un enfoque continuo y proactivo para la protección de la información mediante la aplicabilidad de los acuerdos de confidencialidad que son esenciales para establecer limites sobre el manejo, acceso y divulgación de la información. Sin embargo, para mantener y maximizar su efectividad es importante que su cumplimiento sea monitoreado y revisado periódicamente.

Recomendaciones

- La adopción e implementación de los nuevos controles requiere de especial atención, en particular el control de inteligencia de amenazas se soporta en la contratación de los servicios SOC, no obstante, al momento de la auditoría el respectivo contrato de servicios se encuentra finalizado. Por lo anterior se recomienda agilizar el nuevo proceso de contratación actual y planificar apropiadamente la vigencia de los contratos para realizar oportunamente el proceso de renovación.
- Realizar una evaluación de riesgos especifica de los servidores que han finalizado el soporte de Windows y basándose en los resultados, considerar medidas adicionales como por ejemplo el monitoreo continuo y el aislamiento en la red de estos servidores para mitigar riesgos, lo anterior a fin de reducir la exposición a ciberataques y fortalecer la infraestructura tecnológica.
- Continuar fortaleciendo las sensibilizaciones en seguridad de la información manteniendo un enfoque constante en la toma de conciencia del personal sobre las amenazas y buenas prácticas en ciberseguridad.

ANEXOS

PV01-IN03-F02 Lista de Verificación 27001 V2.0 (05sep2024).xlsx

Nombre y firma del equipo auditor:	Nombre y firma de la o el Auditor Líder
 Diana Patricia Murillo Calderón	 Juan Pablo Peralta Silva