CLIENTE: SECRETARIA DISTRITAL DE MOVILIDAD

Nº CLIENTE: SG-118

ALCANCE DE LA ORGANIZACIÓN: El Sistema de Gestión de Seguridad 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 y las Comunicaciones como habilitador de la Política de Gobierno Digital y Seguridad Digital, establece dentro de su alcance la aplicación de 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 transito

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.

NOMBRE COMPLETO Y VERSIÓN VIGENTE DE LA DECLARACIÓN DE APLICABILIDAD: Matriz de Aplicabilidad: Código PA04-P01-F03 Declaración de aplicabilidad Versión 1.0

TIPO DE AUDITORIA: Segundo Seguimiento

FECHA(S) DE LA AUDITORÍA: 13/11/2025 - 19/06/2017

NORMA DE REFERENCIA: ISO/IEC 27001:2022

AUDITOR LÍDER: Ing. Elsa Marlen Baracaldo

AUDITOR(ES): Ing. Diana Murillo

---

1 OBJETIVOS:

El propósito de la evaluación es evaluar la implementación, incluida la eficacia del sistema de gestión de seguridad de la información de **SECRETARIA DISTRITAL DE MOVILIDAD**

2 ALCANCE DE LA AUDITORIA:

El alcance de la evaluación es el sistema de gestión de seguridad de la información de **SECRETARIA DISTRITAL DE MOVILIDAD**

3 PROCESOS AUDITADOS:

- Direccionamiento Estratégico
- Gestion tics
- Inteligencia para la movilidad
- Gestión administrativa
- Seguridad Vial
- Control y evaluación de la gestión
- Gestión Financiera
- Gestión Jurídica
- Gestión TICS
- Gestión de talento humano
- Comunicaciones y Cultura para la movilidad

4 RESUMEN DE AUDITORÍA

Antes de la Auditoría de Certificación, **SECRETARIA DISTRITAL DE MOVILIDAD**, facilitó su Alcance del SGSI, Políticas y objetivos de seguridad de la información, Proceso de evaluación y tratamiento de riesgos, Declaración de aplicabilidad, Plan de tratamiento del riesgo, Informe de evaluación de riesgos, Uso aceptable de los activos, Política de control de acceso, Procedimientos operativos para gestión de TI, Principios de ingeniería para sistema seguro, Política de seguridad para proveedores, Procedimiento para gestión de incidentes, Procedimientos de la continuidad del negocio, Requisitos legales, normativos y contractuales, Ultima revisión Gerencial y Último informe de auditoría interna para que fuesen revisados. El Auditor Líder realizó el Análisis del Sistema de Gestión Documental y envió a la organización los hallazgos encontrados durante este Análisis.

La Auditoría se llevó a cabo en un lugar y se han mantenido conversaciones con miembros de todos los Procesos. El alcance original de la Auditoría fue revisado y se ha considerado apropiado para las actividades que se están llevando a cabo.

La documentación interna y procedimientos que han sido mostrados, en la mayoría de los casos cumplen coherentemente los requisitos acordados como se determina mediante evidencias revisadas y entrevistas realizadas.

En la reunión de Cierre, la Dirección fue informada de la eficacia del sistema de gestión conforme la norma de referencia es adecuada y por tanto SI se ha recomendado la certificación.

5 REUNIÓN DE APERTURA

Antes del comienzo de la Auditoría, se mantuvo una reunión de apertura que fue sostenida entre las siguientes personas:

5.1 Representando a Cliente:

Julieth Rojas Betancour - jefe Oficina Asesora de Planeación
Edgar Eduardo Romero Bohórquez jefe OTIC
Jasvleidy Fajardo Rozo - Profesional Especializado OTIC
Jorge Luis Vargas Contratista OTIC
Rafael Unda - Director de Inteligencia para la Movilidad
Ilba Milady Vargas - subdirectora Administrativa
José Segundo Lopez Valderrama - jefe de Oficina de Seguridad Vial
Alba Enidia Villamil Muñoz - jefe Oficina de Control Interno
Sandra Velásquez - Contratista OTIC
Jose David Robayo - subdirector Financiero
Paulo Andrés Rincón Garay - Subsecretario de Gestión Jurídica
Hernán Sebastián Cortes - Director de Gestión de Cobro
Natalia Cogollo - Directora de Normatividad y Conceptos
María Jimena Yáñez - Directora de Contratación
Maria Teresa Rodriguez Leal - Directora de Talento Humano

5.2 Representando a Global:

Ing. Elsa Marlen Baracaldo Huertas (Auditora líder)
Ing. Diana Murillo

El Auditor Líder se presentó y explicó el Proceso de Auditoría.

El Auditor Líder confirmó que desearía establecer, mediante evidencias objetivas, que ha sido seguido el Sistema de gestión documental. Esto conllevaría a realizar preguntas de prueba y

registrar las respuestas dadas. Además mencionó que la Auditoría se llevaría a cabo por muestreo y que sería al azar y no de modo estadístico, aunque si se descubre una No Conformidad, se aumentará el muestreo para establecer el impacto de la No Conformidad. Se explicaron los conceptos de No conformidad mayor y menor

Se confirmó que para evitar situaciones que pongan en riesgo la seguridad y salud en el trabajo del equipo auditor, estos estarán acompañados por personal de la organización, y serán vigilados para salvaguardar su seguridad, además que en caso de emergencia seguirán las instrucciones de su acompañante.

Los criterios utilizados en la auditoría (Norma **ISO/IEC 27001:2022**, procesos y documentación del cliente) han servido como referencia para determinar la conformidad de su sistema de gestión.

El Auditor Líder confirma que toda la información obtenida durante el transcurso de la Auditoría es confidencial entre ambas partes a excepción de la información que puede ser requerida por la Entidad Nacional de Acreditación (ONAC) o mediante requerimiento legal realizado por los organismos de control o judiciales en cuyo caso el suministro de información será notificado a la organización .

Se confirmó la conveniencia del Programa de Auditoría previamente emitido. Se determinó que SI será necesaria la utilización de guías en el proceso de auditoría. El alcance de la Auditoría fue confirmado como, ***El Sistema de Gestión de Seguridad 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 y las Comunicaciones como habilitador de la Política de Gobierno Digital y Seguridad Digital, establece dentro de su alcance la aplicación de 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 transitoDe 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.***

6 AUDITORÍA

6.1 Análisis de riesgos de seguridad de información de la organización

El análisis de riesgos de seguridad de información de la organización es consistente en el contexto del negocio, y las interrelaciones con otras funciones de negocios, tales como recursos humanos, desarrollo, producción, operaciones, administración, TI, finanzas, entre otros.

6.2 Tiempo empleado y lugares visitados

La auditoría in situ duro 5,50 días siendo visitado 1 lugar/es. La distribución del tiempo empleado en la evaluación es la siguiente:

0,10 días	Análisis del Sistema Documental y elaboración del Programa.
0 días	Etapa 1.
5,50 días	Etapa 2. (Incluye Análisis de Riesgo)
0,10 días	Informe.
0,10 días	Administración

La Auditoría se llevó a cabo en las siguientes fechas y sitios **(forma Presencial o Remota indicar el %)**:

N°	Fecha	Sitio
1	13/11/2025	Presencial 100 % Calle 13 # 37 - 35, Bogotá D.C.
2	14/11/2025	Presencial 100 % Calle 13 # 37 - 35, Bogotá D.C.
3	18/11/2025	Presencial 100 % Calle 13 # 37 - 35, Bogotá D.C.
4	19/11/2025	Presencial 100 % Calle 13 # 37 - 35, Bogotá D.C.
5		
6		

Si es evaluación multisitio se debe documentar qué procesos fueron auditados en cada sitio visitado:

N°	Sitio	Procesos evaluados
N.A.	N.A.	N.A.

Los resultados detectados en esta auditoría están basados en los hallazgos y evidencias descritos en el check-list utilizado para su realización. Tras el análisis de todos ellos se han detectado 0 NCN's menores.

6.3 No Conformidades identificadas

No se identificaron no conformidades durante el ejercicio de auditoria

6.4 Grado de Confianza asignado a las Auditorías Internas

Las auditorías internas son realizadas según el plan de auditoría que asegura que todos los elementos del sistema son auditados con regularidad.

Los auditores son subcontratados a una entidad externa

Las calificaciones del auditor, datos principales e informes de auditoría dan un Medio grado de confianza en los resultados de la auditoría.

¿Desviaciones del plan de auditoria? **SI** ☐ **NO** ☒
En caso de afirmativo por favor justifique: Haga clic aquí para escribir texto.

¿Existen cuestiones no resueltas? **SI** ☐ **NO** ☒
En caso de afirmativo por favor justifique: Haga clic aquí para escribir texto.

El cliente está controlando de manera eficiente el uso de los documentos y marca de certificación **SI** ☒ **NO** ☐
Justificación: Se evidencia la aplicación del logo de certificación como se encuentra en el Manual de Imagen Corporativo

Verificación de la eficacia de las acciones correctivas tomadas con relación a no conformidades identificadas previamente, si aplica **SI** ☒ **No Aplica** ☐
Se evidencio el cierre eficaz de los planes de acción de las no conformidades anteriores

¿Se declara conformidad y eficacia del sistema **SI** ☒ **NO** ☐

de gestión respecto a la capacidad del sistema de gestión para cumplir los requisitos legales aplicables y lograr los resultados esperados?

Resumen de evidencia:
Haga clic aquí para escribir texto.

¿Se declara conformidad respecto a la auditoría interna y proceso de revisión por la dirección? **SI** ☐ **NO** ☐
Resumen de evidencia:

- Haga clic aquí para escribir texto.

¿Han sido cumplidos los objetivos de la auditoria? **SI** ☒ **NO** ☐
En caso de respuesta negativa por favor justifique la respuesta:
Haga clic aquí para escribir texto.

¿Es una evaluación de seguimiento? **SI** ☒ **NO** ☐
En caso de afirmativo indique la comparación con los resultados de auditorías de certificación previas:
No se presentaron hallazgos de no conformidad durante el ejercicio de auditoria respecto a las dos no conformidades evidenciadas de la auditoria anterior

¿La organización realiza la evaluación del tratamiento de quejas? **SI** ☒ **NO** ☐
Justifique la respuesta
S La entidad cuenta con metodología para la gestión de quejas, realiza tratamiento de PQR a través del sistema Bogotá Te Escucha, Atención al Ciudadano y de la SDM con la Mesa de Servicio y por radicación en físico.

¿Se genera progreso de las actividades planificadas dirigidas a la mejora continua? **SI** ☒ **NO** ☐
Justifique la respuesta
se evidencia en la ejecución de planes de acción derivados de auditorías internas y externas, la revisión periódica de indicadores de seguridad de la información, la implementación de acciones

correctivas frente a hallazgos, y la actualización de procedimientos conforme a cambios normativos o tecnológicos.

¿Se da continuidad en el control operacional por parte de la organización? **SI ☒** **NO ☐**

Justifique la respuesta

En el SGSI de la Secretaría de Movilidad de Bogotá, la continuidad del control operacional se evidencia cuando la entidad mantiene procedimientos documentados, registros periódicos, indicadores de desempeño y responsables asignados para cada control, asegurando su ejecución y mejora continua; sin embargo, en auditoría suele identificarse como oportunidad de mejora la necesidad de fortalecer la trazabilidad y la documentación de dichas actividades, de modo que se demuestre de forma clara y auditable que los controles no solo están definidos, sino que se aplican y revisan de manera constante en el tiempo.

¿Se realizó revisión de cambios que afectan el sistema de gestión de la organización? **SI ☐** **NO ☒**

Justifique la respuesta

No se han presentado cambios al SGSI

7 REUNIÓN DE CLAUSURA

La Reunión de Clausura fue presenciada por el siguiente personal:

7.1 Representando a Cliente:

Julieth Rojas Betancour - jefe Oficina Asesora de Planeación
Edgar Eduardo Romero Bohórquez jefe OTIC
Jasvleidy Fajardo Rozo - Profesional Especializado OTIC
Jorge Luis Vargas Contratista OTIC
Rafael Unda - Director de Inteligencia para la Movilidad
Ilba Milady Vargas - subdirectora Administrativa
Jose Segundo López Valderrama - jefe de Oficina de Seguridad Vial
Alba Enidia Villamil Muñoz - jefe Oficina de Control Interno
Sandra Velásquez - Contratista OTIC
José David Robayo - subdirector Financiero
Paulo Andrés Rincón Garay - Subsecretario de Gestión Jurídica
Hernán Sebastián Cortes - Director de Gestión de Cobro
Natalia Cogollo - directora de Normatividad y Conceptos
María Jimena Yáñez - Directora de Contratación

Maria Teresa Rodriguez Leal - Directora de Talento Humano

7.2 Representando a Global:

Ing. Elsa Marlen Baracaldo Huertas (Auditora líder)
Ing. Diana Murillo

Recomendación:

El equipo auditor recomienda **Mantener la certificación**
Justificación: Se evidencia que la Secretaría Distrital de Movilidad 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

El Alcance de la Certificación ha sido confirmado como: "El Sistema de Gestión de Seguridad 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 y las Comunicaciones como habilitador de la Política de Gobierno Digital y Seguridad Digital, establece dentro de su alcance la aplicación de 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 de apoyo cuyo objetivo contemple la implementación de controles de seguridad de la información de manera transversal para la Secretaría Distrital de Movilidad".

Fue explicado el procedimiento de cómo responder al informe.

El Auditor Líder volvió a confirmar la confidencialidad.

El Auditor Líder señaló el hecho de que como una Auditoría se lleva a cabo por muestreo era posible que existiesen no conformidades en distintos procesos no encontradas. El Cliente ha sido informado de que unas Auditorías Internas efectivas son fundamentales para el futuro del Sistema de Gestión.

El Auditor Líder ha agradecido a la organización la cooperación y hospitalidad mostrada durante el proceso de Auditoría global.

8 NOTAS GENERALES

Se debe hacer notar que se levantará una NCN Mayor si cualquiera de las NCN levantadas durante la auditoría no ha sido cerrada para la próxima visita que realizará el Auditor Líder.

Por consiguiente, es importante que la acción correctiva haya sido llevada a cabo e implantada eficazmente antes de la próxima visita.

Los cambios en la ubicación o en la plantilla (Director y representantes de gestión) deberían ser informados a Global Colombia Certificación tan pronto como sean prácticos después de que haya tenido lugar el cambio.

9 FORTALEZAS REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI

1. Compromiso visible y sostenido de la Alta Dirección

La alta dirección demuestra liderazgo proporcionando recursos, definiendo roles claros y respaldando activamente las políticas de seguridad. Esto fortalece la gobernanza y asegura que el SGSI esté alineado con los objetivos estratégicos del negocio.

2. Personal concienciado y comprometido con la seguridad

La cultura organizacional promueve que todos los empleados comprendan su rol en la protección de la información. Esto reduce errores humanos, incrementa la responsabilidad individual y mejora la detección temprana de riesgos.

3. Gestión eficiente y documentada del SGSI

El SGSI se opera siguiendo procesos claros y medibles: análisis de riesgos actualizado, auditorías internas, revisiones periódicas, mejora continua y control de documentos. Esta buena gestión garantiza un sistema robusto, trazable y preparado para cumplir y mantener la certificación.

4. Buenas practicas

La entidad adopta las buenas prácticas establecidas en la **ISO 27001:2022**, reafirmando su compromiso con la **protección de la información** y estableciendo **bases sólidas para la gestión eficaz y continua de los riesgos de seguridad de la información**.

5. Equipo auditado

Se destaca la capacidad técnica, conocimiento y disposición del equipo auditado, quienes demostraron dominio sobre los procesos bajo su responsabilidad y comprensión y lineamientos del Sistema de Gestión de Seguridad de la Información (SGSI).

6. Prácticas de vulnerabilidades

Se destacan las prácticas de análisis de vulnerabilidades en el ciclo de desarrollo de software, mediante el uso de herramientas como FortiDevSec y la aplicación de los lineamientos del marco OWASP, orientados a la identificación y mitigación temprana de riesgos de seguridad en el código fuente.

Las prácticas de análisis de vulnerabilidades técnicas realizadas mediante la herramienta Tenable, las cuales están orientadas a la identificación, evaluación y mitigación temprana de riesgos de seguridad en los diferentes componentes tecnológicos de la infraestructura institucional. Estas actividades permiten detectar configuraciones inseguras, brechas en sistemas operativos, aplicaciones, dispositivos de red y servidores, contribuyendo a fortalecer la postura de ciberseguridad y a mantener un entorno tecnológico más resiliente y alineado con los principios del SGSI

10 OPORTUNIDADES DE MEJORA REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI

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.

2. Fortalecer de manera continua las actividades de sensibilización en seguridad de la información, manteniendo un enfoque constante en la concientización del personal sobre las amenazas y buenas prácticas de ciberseguridad. Asimismo, promover la identificación

activa y la participación del personal en la mejora y eficiencia del Sistema de Gestión de Seguridad de la Información (SGSI). Dentro de estas actividades de sensibilización de seguridad de la información es importante incluir temas como cuales son los tipos de incidentes y/o eventos de seguridad de la información.

3. Se sugiere implementar mecanismos de doble factor de autenticación (2FA) tanto para el acceso al correo electrónico corporativo como para las conexiones a la red mediante VPN, con el fin de reforzar los controles de acceso y mitigar riesgos asociados a la suplantación de identidad o uso no autorizado de credenciales.

4. La autenticación de doble factor agrega una capa adicional de seguridad al requerir, además de la contraseña, un segundo elemento de validación (por ejemplo, un código temporal, token físico o aplicación de autenticación). Esta medida contribuye significativamente a la protección de la información confidencial, reduce la probabilidad de accesos indebidos y fortalece la postura general de ciberseguridad de la entidad.

5. Desde el proceso de Talento Humano se sugiere actualizar y fortalecer las actividades de inducción y reinducción incorporando contenidos actualizados sobre seguridad de la información y ciberseguridad, con el fin de reforzar la concientización del personal frente a las amenazas digitales y el adecuado manejo de la información institucional.

11 NO APLICABILIDAD Y JUSTIFICACIONES

Punto de la Norma	**Justificación**
N.A.	N.A.

Espacio exclusivo para la Dirección Técnica

¿la información plasmada está acorde a lo evaluado por el auditor Líder?

SI __X__ NO ____

Fecha de Realización del Informe	19/11/2025
Realizado Por	Ing. Marlen Baracaldo
Cargo	Auditora Líder

Este documento es Valido sin Firma y ha sido revisado y emitido por el Auditor Líder indicado en el mismo.