CLIENTE: SECRETARÍA DISTRITAL DE MOVILIDAD

Nº CLIENTE: SG-0118

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 público, Gestión de tránsito y control de tránsito y transporte, Ingeniería de transito

NOMBRE COMPLETO Y VERSIÓN VIGENTE DE LA DECLARACIÓN DE APLICABILIDAD: PA04-P01-F03_DECLARACION_DE_APLICABILIDAD_SDM_2013.

TIPO DE AUDITORIA: Otorgamiento

FECHA(S) DE LA AUDITORÍA: 02/11/2023 - 10/11/2023

NORMA DE REFERENCIA: NTC ISO/IEC 27001:2013

AUDITOR LÍDER: Ing. Jesús David Díaz

AUDITOR(ES): Ing. Olga Henker – Ing. Sergio Ramos

---

1 OBJETIVOS:

El propósito de la evaluación es evaluar la implementación, incluida la eficacia del sistema de gestión de seguridad de la información de **la Secretaría Distrital de Movilidad.**

2 ALCANCE DE LA AUDITORIA:

El alcance de la evaluación es el sistema de gestión de seguridad de la información de **la Secretaría Distrital de Movilidad.**

3 PROCESOS AUDITADOS:

- Direccionamiento estratégico.
- Comunicaciones y cultura para la movilidad.
- Gestión TIC'S – Direccionamiento estratégico.
- Ingeniería de tránsito.
- Planeación de transporte e infraestructura.
- Gestión social.
- Inteligencia para la movilidad.
- Gestión tránsito y control de tránsito y transporte.
- Gestión de trámites y servicios para la ciudadanía.
- Gestión contravencional y transporte público.
- Gestión del talento humano.
- Gestión Jurídica.
- Gestión administrativa.
- Control y evaluación de la Gestión.
- Control disciplinario.

4 RESUMEN DE AUDITORÍA

Antes de la Auditoría de Certificación, **La Secretaría Distrital de Movilidad**, facilitó su información documentada en cuanto a Política general de seguridad de la información de la secretaria distrital de movilidad PA04 P01 v.2, Guía para la Gestión de riesgos SDM en versión 9.0, Manual de Políticas específicas de Seguridad de la información PA04 M01 versión 2.0, Acta de reunión del Comité Institucional de Gestión del Desempeño, Plan de recuperación de desastres DRP de agosto de 2023, Informe de seguimiento a las matrices de riesgo de seguridad de la información de la secretaria distrital de movilidad, Manual del modelo integrado de planeación y gestión de la secretaría distrital de movilidad PE01-M01 Versión 15.0, Matriz de Cumplimiento Legal PA05-IN02-F03 Versión 4.0, Guía de gestión de incidentes de seguridad de la información PA04-G01 versión 2.0, Manual de Arquitectura de Desarrollo Seguro para la Secretaría Distrital de Movilidad PA04-M02 versión 1.0, Declaración de aplicabilidad del SGSI PA04-P01-F03 Versión 1.0, Guía para la Gestión de accesos, Guía de Recuperación Ante Desastres informáticos PA04-G02 versión 1.0, Guía Metodológica para el Análisis de Impacto al Negocio (BIA) PA04-G03 versión 1.0, Manual para la protección de los datos personales en la Secretaría Distrital de Movilidad PA04-M03 versión 1.0, Procedimiento de firma digital PA04-PR02 Versión 3.0, Procedimiento gestión de cambios de TIC PA04-PR04 versión 2.0, Procedimiento de gestión de la información PA04-PR05 versión 3.0, Gestión de Requerimientos y Solicitudes en Materia Tecnológica PA04-PR06 Versión 2.0, Informe de auditoría de Sistemas de gestión del 27 de julio al 10 de agosto de 2023, Caracterizaciones de procesos. El Auditor Líder realizó el Análisis del Sistema Documental y envió a la empresa los hallazgos encontrados durante este Análisis.

La Auditoría se llevó a cabo de forma presencial y remota en las instalaciones de la **Secretaría Distrital de Movilidad** ubicadas en la Calle 13 # 37 – 35 en la Ciudad de **Bogotá D.C** 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 después de revisar y aprobar los planes de acción de las no conformidades evidenciadas.

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 b.
Jasvleidy Fajardo Rozo.
Roger González.
Yohana Pineda.
Javier Sarmiento.
Eliana Robayo.
Neyfi Martínez.
Vladimiro Estrada M.

5.2 Representando a Global:

Jesús David Díaz – Auditor líder.
Sergio ramos – Auditor.
Francisco Cardozo – Auditor.

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 **NTC ISO/IEC 27001:2013**, 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 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 de apoyo 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 13 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.
3 días	Etapa 1.
13 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
01	03 de noviembre de 2023	Proceso de Gestión de Tramites y servicios para la ciudadanía Calle 13 # 37 - 35, Bogotá D.C. (7,69 %)
02	09 de noviembre de 2023	Proceso de Gestión TIC´s Calle 13 # 37 - 35, Bogotá D.C. (7,69 %)
03	09 de noviembre de 2023	Procesos de Control Disciplinario, Gestión TIC´S – Direccionamiento Estratégico) Calle 13 # 37 - 35, Bogotá D.C. (7,69 %)

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

N°	Sitio	Procesos evaluados
1	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 **3 NCN's menores.**

6.3 No Conformidades identificadas

Nc m 1: Se evidenció que la Declaración de aplicabilidad contiene en varios casos (Ej. Algunos controles de A.9) explicaciones idénticas para distintos requisitos y en otros casos, se asocian conceptos que no necesariamente corresponden (Ej. A11.2.4), lo que contraviene el numeral 6.1.3 d) de la Norma ISO 27001:2013.

Nc m 2: En la oficina de la dirección de Atención al Ciudadano se observaron varias cajas desprotegidas con información pública clasificada. Si bien la entidad cuenta con archivos de gestión, estos no se encontraban bajo los controles establecidos en este tipo de área segura, lo cual incumple con el requisito del control de la norma A.11.1.4 Protección contra amenazas externas y ambientales de la Norma ISO 27001:2013.

Nc m3: No hay evidencia de la desactivación en oportunidad, del usuario CARLOS ALBERTO LARA quien cedió su contrato a la señora DIANA CATALINA REYES. Si bien hay evidencia de que a la fecha (9 de noviembre) no se encuentra activo, el directorio activo señala que la fecha límite de dicho usuario era 27 de octubre por tanto no es posible establecer la fecha de desactivación el 4 de octubre como debió haber sucedido, lo que contraviene el control A.9.2.6 de la Norma ISO 27001:2013.

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: Se realizaron ajustes con el plan de auditoría en el desarrollo del ejercicio, se realizó la revisión de todos los procesos según lo establecido en el plan de auditoría.

¿Existen cuestiones no resueltas? **SI** ☐ **NO** ☒
En caso de afirmativo por favor justifique: N.A.

El cliente está controlando de manera eficiente el uso de los documentos y marca de certificación **SI** ☐ **NO** ☐
Justificación: N.A. es una evaluación de otorgamiento

Verificación de la eficacia de las acciones correctivas tomadas con relación a no conformidades identificadas previamente, si aplica	**SI** ☒	**No Aplica** ☐

Se revisaron las evidencias de los planes de acción y registros del cierre de las No Conformidades. Se revisó la eficacia de estas acciones correctivas.

¿Se declara conformidad y eficacia del sistema de gestión respecto a la capacidad del sistema de gestión para cumplir los requisitos legales aplicables y lograr los resultados esperados?	**SI** ☒	**NO** ☐

Resumen de evidencia:
Se declara la conformidad y eficacia de la implementación del Sistema de Gestión, para el cumplimiento de los requisitos legales.

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

Resumen de evidencia:

Se declara conformidad de la auditoría interna, Durante la revisión se detallaron tres (3) hallazgos de No conformidad menores, que en el ejercicio se encontraron que estas se encontraban subsanadas. Se evidenció la revisión por la dirección es conforme con lo establecido en la norma ISO/IEC 27001:2013.

¿Han sido cumplidos los objetivos de la auditoria?	**SI** ☒	**NO** ☐

En caso de respuesta negativa por favor justifique la respuesta:
Se cumplió el objetivo de la auditoría en los tiempos establecidos.

¿Es una evaluación de seguimiento?	**SI** ☐	**NO** ☒

En caso de afirmativo indique la comparación con los resultados de auditorías de certificación previas:
N.A.

¿La organización realiza la evaluación del tratamiento de quejas?	**SI** ☐	**NO** ☐

Justifique la respuesta
N.A.

¿Se genera progreso de las actividades planificadas dirigidas a la mejora continua? Justifique la respuesta N.A. es una auditoria de otorgamiento	**SI** ☐	**NO** ☐
¿Se da continuidad en el control operacional por parte de la organización? Justifique la respuesta N.A. es una auditoria de otorgamiento	**SI** ☒	**NO** ☐
¿Se realizó revisión de cambios que afectan el sistema de gestión de la organización? Justifique la respuesta N.A. es una auditoria de otorgamiento	**SI** ☒	**NO** ☐

7 REUNIÓN DE CLAUSURA

La Reunión de Clausura fue presenciada por el siguiente personal:

7.1 Representando a Cliente:

Jasvleidy Fajardo Rozo.
Yohana Pineda Afanador.
Roger Alfonso González.
Javier Alfonso Sarmiento.
Eliana Robayo.

7.2 Representando a Global:

Ing. Olga Henker.

Recomendación:

El equipo auditor recomienda **Otorgar 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 27001:2013 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 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 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

- El esfuerzo de la alta dirección para la implementación del sistema demuestra el compromiso que se tiene para operar el sistema por parte de la entidad, lo que evidencia en corto tiempo un buen nivel de madurez.
- Se evidencia el compromiso y conocimiento por parte de la entidad, frente al sistema de gestión de seguridad de la información, lo cual ayuda a fortalecer la cultura y lograr la mejora continua del mismo.
- Resaltar los controles que se tienen establecidos durante el ciclo de vida para el desarrollo seguro de los sistemas de información misionales.
- Se evidenció que en todos los procedimientos internos de la entidad se contemplan las políticas de seguridad, adoptando las medidas y controles establecidos.
- Se identifica la propiedad de los procesos frente a los conceptos relacionados con seguridad de la información y los controles de seguridad establecidos para la mejora continua del sistema.
- El Sistema de Gestión de Seguridad de la Información (SGSI) de la entidad, demuestra que a lo largo de la implementación alcanzará un nivel de madurez significativo.

10 OBSERVACIONES - REFERENTES A LA IMPLEMENTACIÓN Y EFECTIVIDAD DE LOS REQUISITOS Y CONTROLES DEL SGSI (puede llegar a ser una no conformidad si no se da tratamiento)

- Todos los numerales deben cumplir el ciclo PHVA. Si en algún caso no se ha logrado la EJECUCIÓN (H), esto no exime de la Planeación.
- Todos los numerales son de obligatoria aplicación porque la Secretaria de Movilidad ha decidido acogerse a un referencial, a no ser que, la declaración de aplicabilidad indique lo contrario.
- Fortalecer la toma de conciencia respecto a “no permitir a visitantes deambular por las instalaciones”.
- Instanciar dentro del documento PA-04-P01 FO01 PLAN DE CUMPLIMIENTO DE OBJETIVOS, las actividades planeadas (Lo que se va hacer) para el logro de los objetivos.
- Revisar y actualizar la documentación en general del SGSI cuando se considere pertinente, durante la revisión se pudo evidenciar documento PROCEDIMIENTO DE GESTIÓN DE INVENTARIOS, INGRESOS, EGRESOS Y TRASLADOS DE ALMACÉN código PA-01-PR12 VERSION 4, con última revisión y actualización del 24-12-2021.

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

- Revisar y ajustar en la gestión de riesgos de seguridad de la información los criterios para la formulación de los planes de tratamiento con nuevos controles o con el refuerzo de los existentes y que el mismo, responda a la priorización definida y aprobada por la alta dirección, mejorar la redacción de la descripción del riesgo y controles. Así mismo, relacionar lo que denominan plan de acción al seguimiento de los controles establecidos.
- Evaluar la gestión de activos de información, frente a la relación que deben tener los criterios establecidos para la valoración del activo y formalizar la identificación de los custodios de estos.
- Fortalecer la política de BYOD (Trae tu propio dispositivo) frente a la conexión de los equipos personales a las redes de la entidad.
- Revisar la documentación relacionada con el sistema de gestión de seguridad de la Información, dado que requieren actualización (Control de cambios, procesos de comunicaciones, requisitos legales, entre otros).
- Fortalecer el diligenciamiento de los registros del Sistema de Gestión de Seguridad de la información en algunos casos se evidencia formato de solicitud de equipo y /o instalación de software contrato 2022-1815 ASIGNACION a FABIAN ROJAS CASTIBLANCO. OM El formato da por hecho que el espacio en blanco significa NO, pero las buenas prácticas de seguridad de la información instan a que existan campos diligenciados. Ej. INSTALACION DE AUTOCAD “No”.
- Fortalecer los métodos de divulgación y sensibilización del Sistema de gestión de Seguridad de la información de entidad.
- Contemplar la posibilidad de identificar las personas como activos de información, Si bien la entidad identifica sus activos es importante revisar el valor de las personas de acuerdo con su nivel de Criticidad para la entidad.
- Fortalecer la definición sobre la priorización de los riesgos de Seguridad de la información para el posterior tratamiento de los riesgos.
- Actualizar el autodiagnóstico del sistema de gestión de Seguridad de la información, como garantía de la implementación, mantenimiento y mejora continua del SGSI.
- Definir y asociar la documentación relacionada con Seguridad de la información al plan de comunicaciones y/o al documento de cronograma de comunicaciones internas y externas.

12 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	20 de noviembre de 2023.
Realizado Por	Jesús David Díaz.
Cargo	Auditor Líder.

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