RESOLUCIÓN NÚMERO 323207 DE 2023

"“ Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□"

EL(LA) SECRETARIA DE DESPACHO DE LA SECRETARÍA DISTRITAL DE MOVILIDAD- SDM, en ejercicio de sus facultades legales y en especial las establecidas en el literal b del artículo 108 del Acuerdo Distrital 257 de 2006, los numerales 14 y 20 del artículo 4 del Decreto Distrital 672 de 2018, y

CONSIDERANDO

Que de conformidad con lo establecido en los artículos 17 y 18 de la Ley 1581 de 2012 "Por la cual se dictan disposiciones generales para la protección de datos personales", dentro de los Deberes de los Responsables del Tratamiento de datos personales, entre otros, se encuentran; conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular e informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.

Que el artículo 2.2.17.5.6 del Decreto Nacional Único Reglamentario 1078 de 2015 *"Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".* establece que; "*Los actores que traten información en el marco del presente título deberán contar con una estrategia de seguridad y privacidad de la información, seguridad digital y continuidad de la prestación del servicio en la cual, deberán hacer periódicamente una evaluación del riesgo de seguridad digital. que incluya una identificación de las mejoras a implementar en su Sistema de Administración del Riesgo Operativo. Para lo anterior, deben contar con normas. políticas. procedimientos. recursos técnicos, administrativos y humanos necesarios para gestionar efectivamente el riesgo. En ese sentido, deben adoptar los lineamientos para la gestión de la seguridad de la información y seguridad digital que emita el Ministerio de Tecnologías de la Información y las Comunicaciones*."

Que el artículo 2.2.22.2.1 del Decreto Nacional 1499 de 2017 "Por medio del cual se modifica el Decreto número 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015", establece las Políticas de Gestión y Desempeño Institucional, donde señala que las políticas de Desarrollo Administrativo de que trata la Ley 489 de 1998, formuladas por el Departamento Administrativo de la Función Pública y los demás líderes, se denominarán Políticas de Gestión y Desempeño Institucional.

Que los numerales 11 y 12 del artículo 2.2.22.2.1 ídem establece dentro de las Políticas de Gestión y Desempeño Institucional las de Gobierno Digital, antes Gobierno en Línea, y la de Seguridad Digital.

Que de acuerdo con el parágrafo del artículo 2.2.22.2.1 y el artículo 2.2.22.3.1. ibídem a través del cual se actualizó el Modelo Integrado de Planeación y Gestión - MIPG, las Políticas de Gestión y Desempeño Institucional se regirán por las normas que las regulan o reglamentan y se implementarán a través de planes, programas, proyectos, metodologías y estrategias.

RESOLUCIÓN NÚMERO 323207 DE 2023

"“ Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□”

Que el Decreto Nacional 1008 de 2018 “Por medio del cual se establecen lineamientos generales de la Política de Gobierno Digital”, tiene como objeto “ establecer los lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital”.

Que el capítulo 1 sección 2 artículo 2.2.9.1.1.3. ídem, incluye la Seguridad de la Información entre los principios de la Política de Gobierno Digital, en armonía con lo establecido en el artículo 2.2.9.1.2.1 del mismo Decreto, en el que define la seguridad de la información como habilitador transversal de la Política de Gobierno Digital el cual junto con los demás habilitadores permiten el desarrollo de los componentes y logros incluidos en dicha política.

Que de conformidad con lo establecido en el artículo 2.2.9.1.3.4. del Decreto Nacional 767 del 16 de mayo de 2022 “Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el Capítulo 1 del Título 9 de la Parte 2 del Libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones', el responsable de liderar la implementación de la Política de Gobierno Digital es el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, quien debe presentar avances y gestión de su implementación.

Que el Decreto Nacional 338 de 2022 *“Por el cual se adiciona el Título 21 a la Parte 2 del libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones”* dispuso un marco para la gobernanza de la seguridad digital del país, con el fin de implementar y aplicar modelos de gestión de riesgos de seguridad y un modelo nacional de atención a incidentes y la creación de un equipo de respuesta a incidentes de seguridad.

Que el CONPES 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital, mediante la cual crea las condiciones para que las múltiples partes interesadas gestionen el riesgo de seguridad digital en sus actividades socioeconómicas y se genere confianza en el uso del entorno digital, siendo uno de los principales aportes de esta política el desarrollo de estrategias que establecieron un marco institucional para la seguridad digital con un enfoque de gestión de riesgos, es decir, con una visión preventiva antes que reactiva ante las posibles amenazas en seguridad digital.

Que de conformidad con lo dispuesto en el artículo 4 del Decreto Distrital 672 de *2018 “Por medio del cual se modifica la estructura organizacional de la Secretaría Distrital de Movilidad y se dictan otras disposiciones”,* la Secretaría Distrital de Movilidad tiene entre otras, las siguientes funciones: *“(...) 14. Dirigir la formulación, ejecución, seguimiento y evaluación de resultados de políticas, planes, programas y proyectos para gestión de tecnologías de la información y las comunicaciones y administración de los sistemas de información de la Secretaría Distrital de Movilidad y el sector movilidad. (...) 20. Establecer las políticas y lineamientos para el adecuado y oportuno funcionamiento de la Secretaría, en busca de generar eficiencia en los procesos, procedimientos y eficacia en la prestación de los servicios de la entidad. (...)”.*

RESOLUCIÓN NÚMERO 323207 DE 2023

"" Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad"

Que mediante Decreto Distrital 221 del 06 de junio de 2023 *"Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital, se deroga el Decreto Distrital 807 de 2019 y se dictan otras disposiciones"*, se adoptó el Modelo Integrado de Planeación y Gestión – MIPG, como marco de referencia para el ajuste del diseño, la implementación y la mejora continua del Sistema Integrado de Gestión Distrital - SIGD, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Distrito Capital para adecuar la institucionalidad del sistema y de las instancias correspondientes con el modelo nacional.

Que el artículo 4 ídem señala que el Sistema de Gestión Distrital que propone el Modelo Integrado de Planeación y Gestión – MIPG, se complementa y articula con otros sistemas, modelos y estrategias que establecen lineamientos y directrices en materia de gestión y desempeño para las entidades públicas, tales como el Sistema de Seguridad de la Información- SGSI,

Que el artículo 15 Ibídem, señala que los Comités Institucionales de Gestión y Desempeño son los encargados de orientar la implementación y seguimiento del Sistema de Gestión y la operación del MIPG, articulando todas las áreas de la entidad, recursos, herramientas, estrategias y políticas de gestión y desempeño institucional, de acuerdo con la normatividad vigente en la materia.

Que mediante Resolución SDM No. 236 del 13 de diciembre de 2018 se adoptó el Manual Específico de Funciones y Competencias Laborales de los Empleos Públicos de la Planta de Personal de la SDM, estableciendo funciones esenciales relacionadas con seguridad de la información para el Profesional Especializado Código 222 Grado 219 área funcional Oficina de Tecnologías de la Información y las Comunicaciones.

Que la Secretaría Distrital de Movilidad, a través de la Resolución 344237 del 23 de diciembre de 2022, creó el Comité Institucional de Gestión y Desempeño de la Entidad.

Que en el artículo 3 ídem, se definen los responsables del Sistema Integrado de Gestión, señalando que la responsabilidad de la implementación, desarrollo, control y mejora del Sistema Integrado de Gestión y su marco de referencia Modelo Integrado de Planeación y Gestión - MIPG, en la Secretaría Distrital de Movilidad, se encuentra a cargo de los siguientes funcionarios: Secretario Distrital de Movilidad, líderes de proceso (Despacho, Subsecretarías, Oficinas Asesoras, Oficinas, Direcciones, Subdirecciones), jefe de la Oficina Asesora de Planeación Institucional, las y los servidores públicos que tienen a su cargo cada plan, programa, proyecto o estrategia y la jefatura de la Oficina de Control Interno.

Que en el Modelo Integrado de Planeación y Gestión – MIPG adoptado mediante manual, se establece en la Política de Seguridad digital que para garantizar que la seguridad de la información sea gestionada correctamente se implementa el Sistema de Gestión de Seguridad de la Información y en este se definen responsabilidades y autoridades para el sistema; entre las autoridades definidas están: Jefe de la Oficina de Tecnologías de la Información, Oficial de seguridad de la información, Director de Talento Humano, Director de Contratación, líderes de los procesos, administradores de las plataformas tecnológicas, Jefe Oficina de Control Interno, servidores públicos, contratistas y terceros.

RESOLUCIÓN NÚMERO 323207 DE 2023

"“ Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□"

Que en el numeral 3.3.8.1. del Manual del Modelo Integrado de Planeación y Gestión – MIPG de la Secretaría Distrital de Movilidad - PE01-M01 -versión 15.0 se establece que; "*Las actividades de liderazgo y compromiso con respecto al Sistema Gestión de Seguridad de la Información son llevadas a cabo por la alta dirección, desempeñando un papel fundamental en el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejora del Sistema. Por lo anterior, la Alta Dirección, en cabeza de la Secretaria (o) Distrital de Movilidad y por medio del Comité Institucional de Gestión y Desempeño - CIGD, realiza el seguimiento al SGSI conforme a los requisitos definidos por la norma ISO/IEC 27001 en su versión vigente."*

Que en el numeral 5.21 del Manual de Políticas Específicas de Seguridad de la Información - PA04-M01, relacionado con la Política de Acuerdos de Confidencialidad, se establece que; *"Todo el funcionariado, contratistas y demás terceros deben firmar el acuerdo de confidencialidad de acuerdo con el formato PA04-M01-F02 "Acuerdo de confidencialidad de la SDM" y este deberá ser parte integral de los contratos utilizando términos legalmente ejecutables y contemplando factores como responsabilidades y acciones de los firmantes para evitar la divulgación de información no autorizada(...)"*

Que en la Guía de Gestión de Incidentes de Seguridad de la Información - PA04-G01, se establecen los canales de comunicación autorizados por la entidad para el reporte de cualquier evento o incidente de seguridad de la información.

Que en la implementación del Sistema de Gestión de Seguridad de la Información, es preciso establecer los roles y responsabilidades de Seguridad de la Información, así como las políticas adicionales del Sistema de Gestión de conformidad con la norma NTC-ISO-IEC 27001.

Que con el fin de promover en las personas naturales y jurídicas vinculadas contractualmente con la SDM el cumplimiento de las políticas y lineamientos de seguridad de la información adoptadas; se incluyeron cláusulas de obligaciones contractuales en materia de seguridad de la información. aplicables al contrato estatal, desde el proceso de selección, hasta la ejecución del contrato y su liquidación.

Que en consideración de lo anteriormente expuesto, y la intención implementar buenas prácticas asociadas a la seguridad de la información, con la finalidad de la defensa, la protección y la gestión de la información como uno de los activos más importantes de la Entidad, y en consecuencia adoptar el Sistema de Gestión de Seguridad de la Información, definir los roles y responsabilidades en materia de seguridad de la información para la Entidad.

Que, en mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO – OBJETO. Adoptar el Sistema de Gestión de Seguridad de la Información. - SGSI- para la Secretaría Distrital de Movilidad, bajo el estándar de la NTC-ISO-IEC 27001 y demás disposiciones reglamentarias y concordantes.

RESOLUCIÓN NÚMERO 323207 DE 2023

"“ Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□”

ARTICULO SEGUNDO. Ámbito de Aplicación. Las disposiciones de la presente resolución aplican para todos los procesos de la Entidad y serán de obligatorio cumplimiento teniendo en cuenta los roles y responsabilidades de que trata el artículo 5 de la presente Resolución.

ARTÍCULO TERCERO. Propósito del Sistema. El Sistema de Gestión de Seguridad de la Información – SGSI - permitirá a la entidad identificar y minimizar los riesgos a los cuales se expone la información, ayudar al uso eficiente de los recursos, establecer una cultura de seguridad de la información y garantizar el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes, en el marco de la estrategia del Gobierno Digital o la que haga sus veces y el Modelo de Seguridad y Privacidad de la Información formulados por el Ministerio de Tecnología de Información y Comunicaciones.

ARTÍCULO CUARTO. Oficial de Seguridad de la Información. Asignar el rol de "Oficial de Seguridad de la Información", en el marco de la implementación y ejecución del Sistema de Gestión de Seguridad de la Información, en la SDM; al **PROFESIONAL ESPECIALIZADO DE LA OTIC, CÓDIGO 222, GRADO 19**.

ARTÍCULO QUINTO. Roles y Responsabilidades de Seguridad de la Información: Se definen los siguientes roles y responsabilidades específicas frente a la seguridad de la información en la Secretaría Distrital de Movilidad:

1. Comité Institucional de Gestión y Desempeño

a) Aprobar la Política de Seguridad de la Información.
b) Asignar los recursos disponibles para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
c) Revisar el estado, adecuación y eficacia del Sistema de Gestión de Seguridad de la Información.

2. Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones:

a) Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información de la entidad y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información.
b) Liderar la implementación y divulgación de las políticas y procedimientos de tecnología y el uso de los servicios tecnológicos en toda la entidad de acuerdo con las mejores prácticas y lineamientos de la Alta Dirección y directrices del Gobierno.
c) Administrar el portafolio de servicios de tecnología y sistemas de información que presta la Secretaría Distrital de Movilidad y establecer los acuerdos de niveles de servicio con las dependencias de la entidad.
d) Proponer las estrategias y lineamientos de la continuidad de las operaciones de los sistemas de información de la entidad, a fin de evitar las interrupciones de la operación y de salvaguardar la información almacenada.
e) Liderar la implementación y actualización de los procedimientos de seguridad de la información que apliquen para la plataforma de tecnologías de información administrada por esta oficina.

RESOLUCIÓN NÚMERO 323207 DE 2023

"" Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□"

3. Jefe de la Oficina de Control Interno

a) Validar mediante el proceso de auditoría la aplicación y cumplimiento de las políticas de Seguridad de la Información, la aplicación de controles sobre los activos de información y los requerimientos del Sistema de Gestión de Seguridad de la Información.
b) Proporcionar una evidencia objetiva al Oficial de Seguridad de la Información y al Comité Institucional de Gestión de Desempeño, sobre la eficacia con la que la entidad evalúa y gestiona sus riesgos de seguridad de la información, incluida la forma en la que funcionan y son aplicados los controles para mitigar los riesgos.
c) Verificar la aplicación de las recomendaciones relacionadas con controles de seguridad identificadas en los informes de auditoría interna para determinar si los procesos han ejecutado los planes de acción adecuadamente.

4. Director de Talento Humano

a) Realizar la gestión de vinculación, capacitación y desvinculación del personal de planta dando cumplimiento a los controles de normatividad vigente y procedimientos internos relacionados con seguridad de la información.
b) Aplicar el formato de Acuerdo de Confidencialidad a todos los servidores públicos y funcionarios que ejerzan funciones en la secretaría.
c) Incluir en los programas de inducción y de reinducción los temas de seguridad de la información definidos por el Oficial de Seguridad de la Información, asegurando que los funcionarios conozcan sus responsabilidades, así como las implicaciones por el uso indebido de activos de información o de otros recursos informáticos, haciendo énfasis en las consecuencias jurídicas que puede acarrear al servidor público.
d) Incluir en el plan de capacitaciones anual temas de seguridad de la información conforme a las necesidades definidas por la Oficina de Tecnologías de la Información y las Comunicaciones.

5. Director de Contratación

a) Incluir en las obligaciones generales contractuales de personas jurídicas y naturales, las responsabilidades en materia de seguridad de la información definidas por el Jefe de Oficina de Tecnologías de la Información y las Comunicaciones con el fin de garantizar el conocimiento y cumplimiento de las políticas de seguridad de la información de la entidad.

6. Oficial de Seguridad de la Información: El Oficial de Seguridad de la Información de la Secretaría Distrital de Movilidad, tendrá a su cargo las siguientes funciones:

a) Liderar y garantizar la implementación, mantenimiento y mejora del Sistema de Gestión de seguridad de la Información-SGSI.
b) Ejercer seguimiento y control del Sistema de Gestión de Seguridad de la Información-SGSI, aplicando los correctivos y ajustes necesarios para el logro de los objetivos, de conformidad con el formato PA04-P01-F02 de gestión SGSI, informando a la alta dirección sobre el desempeño del sistema.
c) Documentar los procedimientos de seguridad de la información y someterlos a decisión de la Alta Dirección, realizando su posterior implementación y seguimiento.

RESOLUCIÓN NÚMERO 323207 DE 2023

"" Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad"

d) Desarrollar, mantener y comunicar las políticas, estándares y guías de seguridad de la información de la Entidad.
e) Realizar el análisis de riesgos de seguridad de la información y el plan para la mitigación de estos.
f) Gestionar la actualización de los activos de información conforme a las dinámicas de la Entidad y coordinar la publicación respectiva conforme lo señala la Ley de Transparencia y Acceso a la Información Pública.
g) Gestionar los eventos e incidentes de seguridad de la información de acuerdo con las mejores prácticas existentes.
h) Servir como punto de apoyo a la Oficina de Tecnologías de la Información y las Comunicaciones, respecto a cambios en plataformas tecnológicas para brindar conceptos en aspectos de seguridad de la información.
i) Atender las auditorías internas, externas y revisiones de entes de control, proporcionando la información correspondiente a seguridad de la información.
j) Documentar la actualización, el seguimiento, medición, análisis y evaluación del desempeño de la seguridad de la información y eficacia del SGSI.
k) Definir e implementar la estrategia de concientización y sensibilización en Seguridad de la Información para los funcionarios, contratistas y terceros.
l) Verificar el cumplimiento de la legislación y normatividad de seguridad de la información aplicable a la entidad.
m) Revisar que se conserve la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento

n) Exigir al Encargado del Tratamiento de datos personales, en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.

7. Líderes de los Procesos

a) Participar en la identificación de los proyectos y planes de mejoramiento de seguridad de la información asociados a la gestión de riesgo sobre la información de su proceso.
b) Reportar al Oficial de Seguridad de la Información el desempeño de la gestión de seguridad de la información y los planes y proyectos asociados de su proceso.
c) Hacer seguimiento de las acciones preventivas o correctivas del proceso a su cargo.
d) Identificar y valorar los activos de información y la información más importante del proceso a su cargo en términos de confidencialidad, privacidad, integridad y disponibilidad.
e) Realizar y mantener actualizada la clasificación de los activos de información y la información del proceso de acuerdo con el esquema de clasificación definido por la Entidad.
f) Revisar y asegurar que los privilegios de acceso a los activos de información de su proceso o área son los adecuados.
g) Asignar el etiquetado pertinente a los activos de información y la información del proceso, conforme a los lineamientos dados por la Entidad.
h) Participar en la identificación y evaluación de los riesgos de seguridad de la información del proceso y sus activos de información asociados, así mismo proponer planes para su tratamiento (controles de seguridad de la información).
i) Asegurar la implementación, operación y mantenimiento de los controles de seguridad de la información aplicados a los activos de información y la información del proceso.

RESOLUCIÓN NÚMERO 323207 DE 2023

"" Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□"

j) Establecer los mecanismos para asegurar la participación y capacitación de los servidores y contratistas de su proceso en las sensibilizaciones programadas por la Oficina de Tecnologías de la Información y las Comunicaciones con relación a temas de seguridad de la información.

8. Administradores de las Plataformas Tecnológicas y Sistemas de Información

a) Gestionar todas las solicitudes de creación, cancelación y modificación de usuarios y sus respectivos perfiles para los equipos y aplicaciones.
b) Mantener actualizada una lista de todos los usuarios con permisos de acceso a los equipos y sistemas de información bajo su responsabilidad.
c) Cumplir con los requerimientos de seguridad de la información establecidos para la operación y administración de los sistemas de información y recursos de tecnología.
d) Analizar e informar por los medios establecidos en la Guía de Gestión de Incidentes de Seguridad de la Información al Oficial de Seguridad de la Información, cualquier evento que atente contra la seguridad de la información.
e) Mantenerse actualizado y capacitado con respecto a nuevas amenazas, posibles ataques y riesgos que pueden afectar los equipos y/o sistemas de información bajo su responsabilidad.
f) Implementar y velar por una adecuada operación de los lineamientos (Normas y estándares), mecanismos, herramientas y procedimientos de seguridad en la plataforma tecnológica que soporta los procesos.
g) Gestionar, administrar y monitorear los controles de seguridad implementados en redes de comunicaciones, servicios y sistemas de información y en generar en la plataforma TI de la entidad.
h) Gestionar, administrar, identificar, implementar y aplicar las configuraciones de la base de reglas de seguridad, de perfiles y opciones de seguridad.
i) Gestionar y monitorear de forma centralizada las configuraciones de dispositivos y los registros. Así mismo, identificar mecanismos para la autorización, autenticación y administración de dispositivos.

9. Servidores Públicos, contratistas y proveedores

a) Conocer y cumplir las políticas, procedimientos, guías, instructivos y demás controles de seguridad de la información.
b) Conocer y cumplir los requisitos legales , contractuales y regulatorios que debe aplicar la Entidad, de acuerdo con su misión.
c) Utilizar los activos de la información, sólo para el cumplimiento de sus funciones y obligaciones.
d) Participar activamente en las charlas, talleres y capacitaciones sobre seguridad de la información, impartidas por la Oficina de Tecnologías de la Información y las Comunicaciones.
e) Reportar los incidentes o eventos de seguridad de la información detectados, de acuerdo con lo establecido en la Guía de Gestión de Incidentes de Seguridad de la Información.
f) Responder por la seguridad de la información que tiene bajo su custodia.
g) No deshabilitar los controles de seguridad en su estación de trabajo, ni buscar opciones para evitar su cumplimiento (firewall, antivirus, cifrado, entre otros).

RESOLUCIÓN NÚMERO 323207 DE 2023

"" Por medio de la cual se adopta el Sistema de Gestión de Seguridad de la Información y se establecen roles y responsabilidades de Seguridad de la Información para la Secretaría Distrital de Movilidad□"

h) Proteger las cuentas de acceso, privilegios y contraseñas asociadas, evitando compartirlas con otros usuarios.
i) Utilizar los controles de seguridad física determinados por la Entidad para salvaguardar la seguridad de la información.
j) Colaborar en las investigaciones de eventos y/o incidentes de seguridad que se presenten y estén relacionadas con la actividad de sus usuarios individuales.

ARTÍCULO SEXTO. Socialización. La Oficina de Tecnologías de la Información y las Comunicaciones publicará el presente acto administrativo en la intranet y en la página web de la entidad.

ARTÍCULO SÉPTIMO. Vigencias La presente Resolución rige a partir de su publicación.

COMUNÍQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C. a los treinta y un día(s) del mes de Octubre de 2023.

Deyanira Consuelo Avila Moreno
Secretaria de Despacho
Firma mecánica generada en 31-10-2023 06:39 PM

Aprobó: Vladimiro Alberto Estrada Moncayo-Subsecretaría de Gestión Corporativa
Aprobó: Leydy Yohana Pineda Afanador-Oficina de Tecnologías de la Información y las Comunicaciones
Aprobó: Natalia Catalina Cogollo Uyaban-Dirección de Normatividad y Conceptos
Aprobó: Paulo Andres Rincon Garay-Subsecretaría de Gestión Jurídica
Elaboró: Roger Alfonso Gonzalez Herrera
Revisó: Jason Nova Salgado, Abogado Normatividad y Conceptos
Elaboró: Oficina de Tecnologías de la Información y las Comunicaciones