BOGOTÁ | SECRETARÍA DE INTEGRACIÓN SOCIAL

RESOLUCIÓN N. ° 1414 DE 30 DE JUNIO 2022

"Por la cual se adopta la Política General de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social y se dictan otras disposiciones"

LA SECRETARIA DISTRITAL DE INTEGRACIÓN SOCIAL

En uso de sus facultades legales y reglamentarias, en especial de las establecidas en los literales h) y j) del artículo 4°, del Decreto Distrital 607 de 2007, y

CONSIDERANDO:

Que en el artículo 15 de la Constitución Política de Colombia se establece que *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas. (...)".*

Que el artículo 74 de la Carta Política preceptúa que *"Todas las personas tienen derecho a acceder a los documentos públicos salvo los casos que establezca la Ley. El secreto profesional es inviolable.".*

Que la Ley 1273 de 2009 modifica el Código Penal, crea un nuevo bien jurídico tutelado denominado *"de la protección de la información y de los datos",* y establece normas para preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que mediante la Ley 1581 de 2012 se expidió el Régimen General de Protección de Datos Personales, el cual, de conformidad con su artículo 1, tiene por objeto *"(...) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.".*

Que la norma internacional ISO/IEC 27001:2013 (Icontec, 2013) - Tecnología de la Información - Técnicas de Seguridad - Sistemas de Gestión de Seguridad de la Información - Requisitos, especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.

Que la norma internacional ISO-IEC 27002:2013 (Icontec, 2015) - Tecnología de la Información - Técnicas de Seguridad, relaciona el código de práctica para controles de seguridad de la información.

Que la Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional, tiene por objeto adoptar disposiciones tendientes a prevenir los actos de corrupción, a reforzar la articulación y coordinación de las entidades del Estado y a recuperar los daños ocasionados por dichos actos con el fin de asegurar promover la cultura de la legalidad e integridad y recuperar la confianza ciudadana y el respeto por lo público.

Que el artículo 133 de la Ley 1753 de 2015 *"Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "Todos por un nuevo país"*, establece la integración de todos los componentes del Sistema de Gestión de Calidad con el Sistema de Control Interno en un solo Sistema de Gestión a implementar en todas las entidades públicas del nivel nacional y territorial.

Que el Decreto Nacional 1078 de *2015 "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*, definió la estrategia de seguridad y privacidad de la información, estableciendo que la misma no se limita a este sólo aspecto, sino que comprende la seguridad digital y los requerimientos necesarios para garantizar la continuidad en la prestación de los servicios digitales, en los siguientes términos:

> ***"ARTÍCULO 2.2.17.5.6. Seguridad de la información y Seguridad Digital.*** *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 mediante Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital, se establece un marco institucional claro y preciso en torno a la seguridad digital.

Que en cumplimiento de Ley la 1753 de 2015, se expidió el Decreto Nacional 1499 de 2017 *"Por medio del cual se modifica el Decreto 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*", el cual sentó las bases del nuevo Sistema Integrado de Gestión, estableció el Modelo Integrado de Planeación y de Gestión para implementar dicho sistema, e hizo énfasis en que dentro de las políticas de gestión y de desempeño institucional se encuentran, según el artículo 2.2.22.2.1 del Decreto Nacional 1083 de 2015, numerales 11 y 12, las Políticas de Gobierno Digital y de Seguridad Digital, con las cuales debe alinearse la Política de Seguridad y Privacidad de la Información de la Secretaría Distrital de Integración Social.

Que la temática de seguridad de la información está claramente ligada a otros sistemas de gestión con los cuales se articula en los términos de ese mismo Decreto Nacional, a saber:

> *"ARTÍCULO 2.2.22.1.5. Articulación y complementariedad con otros sistemas de gestión. El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de*

Seguridad de la Información".

Que mediante el Decreto Nacional 1008 de 2018, que modificó el Decreto 1078 de 2015, antes mencionado, se establecen *"(...) 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 la Guía No. 5 de Gestión y Clasificación de Activos de Información del Ministerio de Tecnologías de la Información y las Comunicaciones, relaciona los lineamientos básicos que deben ser utilizados por los responsables de la seguridad de la información, para poner en marcha la gestión y clasificación de activos de información que son manejados por cada entidad del Estado, con el fin de determinar que activos posee la Entidad, cómo deben ser utilizados, los roles y responsabilidades que tiene los funcionarios sobre los mismos, reconociendo adicionalmente el nivel de clasificación de la información que a cada activo debe dársele.

Que la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (Departamento Administrativo de la Función Pública, 2018), unifica los lineamientos en los aspectos comunes de las metodologías para la administración de todo tipo de riesgos y fortalece el enfoque preventivo con el fin de facilitar a las entidades la identificación y tratamiento de cada uno de ellos.

Que mediante Documento CONPES 3995 de 2020 - Política Nacional de Confianza y Seguridad Digital, se establecen medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.

Que el fundamento normativo interno para la adopción de los nuevos lineamientos de las políticas de seguridad de la información está dado por las siguientes disposiciones del Decreto Distrital 607 de 2007 *"Por el cual se determina el Objeto, la Estructura Organizacional y Funciones de la Secretaría Distrital de Integración Social":*

- El artículo 14 que establece que la Dirección de Análisis y Diseño Estratégico tiene entre otras las siguientes funciones: *"(...) e) Coordinar implementación, mantenimiento y seguimiento del Sistema Integrado de Gestión en la Entidad, f) Diseñar y proponer las políticas para el adecuado funcionamiento de los Sistemas de Información de la Entidad (...) p) Orientar la formulación y desarrollo de las políticas tanto de los sistemas de información como del desarrollo informático de la Secretaría, en busca del uso de tecnologías que hagan más eficiente la utilización de los recursos físicos, humanos y financieros de la Entidad (...)".*

- El artículo 16 que dispone, entre otras funciones de la Subdirección de Investigación e Información, las siguientes: *"(...) h) Proponer, aplicar y desarrollar las políticas tanto de los sistemas de información como del desarrollo informático de la Secretaría, realizando el procesamiento y control de estos, y asistir en lo pertinente a las entidades adscritas (...) ñ) Desarrollar procedimientos y crear planes de contingencia para los sistemas de información (...)".*

Que la Resolución 5569 del 11 de Diciembre de 2018 de la Comisión de Regulación de Comunicaciones *"Por la cual se modifica el artículo 5.1.2.3 del Capítulo 1 del Título V de la Resolución CRC 5050 de 2016 en materia de gestión de seguridad en redes de telecomunicaciones y se dictan otras disposiciones",* consagra en el artículo 1º de definiciones, el término "Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. (De acuerdo con lo dispuesto en el estándar ISO/IEC 27000:2016). Así mismo en el artículo 2º Gestión de Seguridad en Redes de Telecomunicaciones, subnumeral 5.1.2.3.1. Políticas de seguridad de la información, define las categorías de los incidentes, así: a) Denegación de servicio, b) Acceso no autorizado, c) Malware (software malintencionado), d) Abuso y e) Recopilación de información de sistema.

Que la Directiva Presidencial 03 del 15 de marzo de 2021, por la cual se expiden "*Lineamientos para el uso de servicios en la nube, inteligencia artificial, seguridad digital y gestión de datos"* en su numeral 3 *"Seguridad Digital"* precisa directrices con el fin de fortalecer las capacidades y la funcionalidad de las Entidades en términos de ciberseguridad y resiliencia corporativa.

Que la Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social está dirigida entre otros aspectos al cumplimiento de los planes institucionales que establece la Resolución 612 de 2018, tales como el Plan Estratégico de Tecnologías de la Información (PETI), Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información y Plan de Seguridad y Privacidad de la Información.

Que el artículo 8° del Decreto Distrital 807 de 2019 *"Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital y se dictan otras disposiciones",* establece la creación de los Comités Instituciones de Gestión y Desempeño, definiendo la institucionalidad para la implementación del Modelo Integrado de Plantación y de Gestión (MIPG) como *"(...) el conjunto de instancias que de manera coordinada establecen las reglas, condiciones, políticas y metodologías que facilitan la implementación, evaluación y seguimiento del modelo".*

Que en cumplimiento del mencionado Decreto Distrital, mediante la Resolución No. 0355 de 2019, modificada por la Resolución No. 00652 de 2020 se crea el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Integración Social, como la instancia encargada de orientar, articular y ejecutar las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento

del Modelo Integrado de Planeación y Gestión.

Que para realizar por parte de los usuarios un buen uso de los activos de información, la Secretaría Distrital de Integración Social, requiere la definición e implementación de una política de seguridad digital y un compendio de políticas detalladas que indiquen lineamientos frente a la seguridad y privacidad de la información.

Que esta Secretaría expidió la Resolución No. 0083 de 2021 "*Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social*" la cual es necesario derogar de acuerdo con la normatividad anteriormente mencionada.

En mérito de lo expuesto,

RESUELVE:

CAPITULO I

DISPOSICIONES GENERALES

ARTÍCULO 1.-OBJETO. La presente Resolución tiene por objeto establecer la Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social en el marco de su misión y entendiendo la importancia de una adecuada gestión de la información, en la cual se compromete a realizar las acciones pertinentes y de carácter obligatorio para conservar la integridad, confidencialidad, disponibilidad y privacidad de sus activos de información institucional, en procura de la mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI.

Esta política permite la gestión integral de riesgos e incidentes, fortalece la cultura de seguridad en los colaboradores y propende por la continuidad del negocio. Lo anterior, enmarcado en el cumplimiento de los requisitos legales, regulatorios y en concordancia con la misión y visión de la Entidad.

ARTÍCULO 2.-ÁMBITO DE APLICACIÓN. La Política de Seguridad y Privacidad de la Información y Seguridad Digital aplica a todos los niveles y unidades operativas de la Secretaría Distrital de Integración Social, a todos sus funcionarios, contratistas, proveedores, operadores, entes de control y demás terceros que debido al cumplimiento de sus funciones y las de la Secretaría, compartan, utilicen, recolecten, procesen, intercambien o consulten su información de forma interna o externa, independientemente de su ubicación. De igual forma, esta política aplica a toda la información creada, procesada o utilizada por la Entidad, sin importar el medio, formato, presentación o lugar en la cual se encuentre.

ARTÍCULO 3.- CONCEPTO. La presente Política es la declaración de alto nivel que describe la posición de la Secretaría Distrital de Integración Social frente a la Seguridad y Privacidad de la Información y Seguridad Digital.

ARTÍCULO 4.- DEFINICIONES. Para efectos de la interpretación e implementación de la Política de Seguridad y Privacidad de la Información y Seguridad Digital, se tendrán como marco de referencia las siguientes definiciones:

Activo de información: Es todo aquel recurso tangible o intangible que tenga valor o importancia para la organización, de acuerdo con la tipificación definida.
Adaptabilidad: Permite identificar y rastrear toda operación llevada a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados.

Archivos: Conjunto de datos o instrucciones que se almacenan en el Disco Duro y/o cualquier otro medio de almacenamiento con un nombre que los identifica.

Autenticidad: Consiste en garantizar que las personas, entidades o procesos sean lo que dicen ser ante un activo de información.

Autorización: Es el otorgamiento de permiso a una persona, entidad o proceso, para acceder a un activo de información.

Backup: Copiar y resguarda la información para protegerla de posibles riesgos.

Confiabilidad: La información debe ser la apropiada para la administración de la entidad y el cumplimiento de sus obligaciones.

Confidencialidad: Consiste en garantizar que el activo de información no esté disponible o sea divulgado por personas, entidades o procesos NO autorizados.

Contraseña: Contraseña, password o clave de acceso es una combinación de letras, números y signos, que conoce y debe teclear el usuario para obtener acceso a un programa o partes de un programa determinado, un terminal u ordenador personal, un punto en la red, etc.

Cuenta de Correo: Servicio en línea que provee un espacio para la recepción, envío y almacenamiento de mensajes de correo electrónico en Internet.

Cuenta de Usuario: Es el identificador que utiliza un Sistema de Información en la autenticación de un usuario.

Custodios de la información: se denominan así al personal o departamento que proporciona servicios informáticos de todo tipo en cualquier área de MOVIL SERVICIOS, Los custodios no necesitan conocer la información para la realización de su trabajo, solamente procesarla, gestionar su almacenamiento y hacerla accesible.

Crítico: Estado en el cual la pérdida de capacidad de procesamiento pueda llegar a tener consecuencias negativas significativas, desde los siguientes puntos de vista: continuidad del negocio, operacional y de integridad del personal.

Disponibilidad: Consiste en garantizar que el activo de información este accesible y utilizable en el momento oportuno que se requiera bajo la demanda de personas, entidades o procesos.

Dueño: Es la persona responsable de una aplicación que utiliza sistemas de información para proporcionar servicios que apoyan una o varias unidades de negocio. Es el responsable por velar que se implementen controles que disminuyan el riesgo de la información a su cargo. Es también la persona que tiene la potestad de autorizar el acceso a la información.

Eficiencia: Criterio de calidad en que el procesamiento y suministro de la información, que debe contar con la capacidad de lograr ese efecto con el mínimo de recursos posibles o en el menor tiempo posible.

Equipos de cómputo: Dispositivo electrónico que se emplea para procesar datos. También pueden ser considerados como equipos de cómputo los equipos que prestan servicios de almacenamiento y procesamiento desde la nube.

Evidencia Digital: Es un tipo de evidencia física que puede tomar muchas formas como son:

- Registros de aplicaciones, sistema operacional, comunicaciones (logs de transacciones, logs de seguridad, logs de intentos de login fallidos, etc.)
- Imágenes o graficas
- Documentos en todos los formatos
- Correo electrónico archivos digitales
- Información financiera y de transacciones
- Archivos de cache, cookies
- Archivos eliminados
- Archivos de intercambio

Firewall: Es un filtro o cortafuegos (hardware o software) que controla todas las comunicaciones que pasan de una red a otra y en función de lo que sean permite o deniega su paso.

Hardware: Partes físicas de un sistema de procesamiento de datos.

Incidente: Se define como un acceso, intento de acceso, uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos; o cualquier otro acto que implique una violación a la Política

Información: conjunto organizado de datos procesados, que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje.

Integridad: Consiste en asegurar o salvaguardar que el activo de información cuente con las propiedades de: exactitud, precisión, consistencia, confiablidad y totalidad.

Integridad de datos: Proteger y garantizar la exactitud e integridad de la información en el momento de su ingreso a los sistemas y la identificación de cualquier alteración de la información.

Log: Archivo que registra movimientos y actividades de un determinado programa, utilizado como mecanismo de control y estadística.

Medios de almacenamiento externo: Medio utilizado para el almacenamiento de información, que puede conectarse o introducirse y retirarse del Hardware por varias interfaces como puertos usb, unidad de cinta, unidades de disco, etc.

Nivel de seguridad estándar: Nivel de seguridad que restringe a los usuarios la ejecución de algunos comandos o el acceso a algunos archivos basados en permisos y en niveles de acceso. Este nivel de seguridad requiere de auditoría del sistema. Esto incluye la creación de un registro de auditoría para cada evento que ocurre en el sistema.

No-Repudiación: Consiste en asegurar que el activo de información NO sea negado bajo un evento o transacción demandado por personas, entidades o procesos.

Parche de Seguridad: Conjunto de instrucciones de corrección para un software en especial, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento, en el código original de este.

Periféricos: Dispositivo electrónico físico que se conecta o acopla a una computadora, pero no forma parte del núcleo básico

Recursos Tecnológicos: Elementos de tecnología que pueden ser hardware y/o software, tales como equipos de cómputo, servidores, impresoras, teléfonos, programas y/o aplicativos de software, dispositivos USB, entre otros.

Red: Nombre dado al conjunto de equipos de cómputo y de telecomunicaciones, interconectados entre sí al interior de la organización, para permitir a los usuarios acceso a los recursos tecnológicos.

Riesgo Informático: Es una combinación de la posibilidad de que una amenaza contra un activo de información ocurra aprovechando una vulnerabilidad y/o falla en un control, y la severidad del impacto adverso resultante. Reduciendo la amenaza o la vulnerabilidad reduce el riesgo. Dentro de esta definición se incluye el software y hardware.

Terceros: Se entiende por tercero a toda persona, jurídica o natural, como proveedores, temporales contratistas o consultores, que provean servicios o productos a la compañía.

Software: Es el conjunto de instrucciones mediante las cuales el Hardware puede realizarlas tareas ordenadas por el usuario. Está integrado por los programas, sistemas operativos y utilidades.

Software ilegal: Es el Software que se adquiere y se instala sin el consentimiento de la empresa que lo desarrolla o sin licencia de uso.

Trazabilidad: Asegurar que en todo momento se podrá determinar quién accedió a qué activo de información (servicio, datos, etc.), qué hizo y en qué momento lo hizo.

ARTÍCULO 5.-COMPONENTES DE LA POLÍTICA. La Política de Seguridad y Privacidad de la Información y Seguridad Digital está conformada por estándares técnicos y generales de seguridad de la información, procesos y procedimientos, estructura organizacional y mecanismos de verificación y control para garantizar que los riesgos de seguridad de la información y los riesgos de ciberseguridad sean conocidos, asumidos, gestionados y mitigados de forma documentada, sistemática, estructurada, repetible, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

ARTÍCULO 6.- ENUNCIADO GENERAL DE LA POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL. Las dependencias del Nivel Central, las Subdirecciones Locales, Comisarías de Familia y en general, todas las Unidades Operativas de la Secretaría Distrital de Integración Social protegen, preservan y administran la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de toda la información que gestiona la Entidad, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales, previniendo incidentes y dando cumplimiento a los requisitos legales y reglamentarios, propendiendo además por el acceso, uso efectivo y apropiación de las Tecnologías de la Información y las Comunicaciones -TIC.

Por lo anterior, se debe asegurar la divulgación e implementación de esta política, manuales, procedimientos, guías e instructivos relacionados, garantizando el seguimiento y mejora de estos en todos los procesos de la Entidad.

ARTÍCULO 7.- OBJETIVOS. La Política de Seguridad y Privacidad de la información y de Seguridad Digital en la Secretaría Distrital de Integración Social tiene los siguientes objetivos:

a. Identificar, clasificar, valorar y mantener actualizados los activos de información de la Entidad.
b. Gestionar los riesgos de Seguridad y Privacidad de la información que afecten la confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucional.
c. Gestionar los incidentes y eventos de seguridad y privacidad que pongan en riesgo la confidencialidad, disponibilidad, integridad y privacidad de los activos de información de la Entidad, de manera oportuna, con el fin de minimizar su impacto y propagación.
d. Promover e implementar estrategias para establecer una cultura y apropiación en temas de Seguridad y Privacidad de la información en todos los colaboradores de la entidad.
e. Establecer, implementar y mejorar el plan de continuidad del negocio para la Secretaría Distrital de Integración Social en cuanto a los procesos y/o actividades críticas de la entidad.
f. Garantizar a través de la implementación del Modelo de Seguridad y Privacidad de la Información la continuidad de los servicios de la Entidad.
g. Fomentar el uso y apropiación de las TIC en la Secretaría de Integración Social, contribuyendo en las políticas de seguridad y privacidad en los procesos de gestión, administrativos y formativos de la Entidad.
h. Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la Entidad.

Para realizar una medición acorde con la efectividad, eficacia y eficiencia de la Seguridad de la Información en la Entidad, se deben aplicar los indicadores relacionados en la Guía de Indicadores de Gestión de la Información emitida por el Ministerio de las TIC.

ARTÍCULO 8.- PRINCIPIOS. La Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social, tiene los siguientes principios:

a. **Socialización.** Las responsabilidades frente a la seguridad y privacidad de la información deben ser definidas, compartidas y publicadas a los funcionarios, contratistas, proveedores, operadores, entes de control y aquellas personas o terceros involucrados debido al cumplimiento de sus funciones y las de la Secretaría.
b. **Identificación de riesgos de seguridad y privacidad de la información y seguridad digital**. Los líderes de cada proceso deberán identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta la confidencialidad, integridad y disponibilidad de la información. Para ello, la Entidad adopta la metodología de riesgos del Departamento Administrativo de la Función Pública.
c. **Gestión de riesgos de seguridad y privacidad de la información y seguridad digital**. La Secretaría Distrital de Integración Social mediante la mesa de servicios, debe realizar la gestión de incidentes, eventos y debilidades de seguridad, para lograr el mejoramiento continuo de su modelo

de seguridad y privacidad de la información.

ARTÍCULO 9.- RESPONSABLES. La definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social así como sus lineamientos específicos, tiene como responsables las siguientes instancias:

a. La Subdirección de Investigación e Información, quién será la encargada de establecer y elaborar los lineamientos complementarios de seguridad y privacidad de la información para la Entidad.
b. El Comité Institucional de Gestión y Desempeño, en representación de la Alta Dirección, quién tiene la responsabilidad de asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.
c. El personal encargado de la seguridad de la información, adscrito a la Subdirección de Investigación e Información, que implementará y velará por el mantenimiento del Modelo de Seguridad y Privacidad de la Información de la Entidad.
d. Los funcionarios, contratistas, proveedores, operadores, entes de control y terceros, quienes deberán cumplir la Política de Seguridad y Privacidad de la Información y Seguridad Digital y sus lineamientos específicos.

ARTÍCULO 10.- COMPROMISO DE LA ALTA DIRECCIÓN. La Secretaría Distrital de Integración Social, por intermedio de Subsecretaría, Direcciones, Subdirecciones y Oficinas Asesoras se comprometen y responsabilizan con la asignación y comunicación de las funciones, obligaciones y responsabilidades de todos los colaboradores en materia de seguridad y privacidad de la información, apalancando así el establecimiento, implementación, operación, seguimiento, mantenimiento y mejora continua del SGSI.

ARTÍCULO 11.- REVISIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN. La Política de Seguridad y Privacidad de la Información, como elemento estructural del Sistema de Gestión de Seguridad de la Información, y demás documentación relacionada, será revisada anualmente o cuando la Entidad lo considere necesario, en los escenarios de posibles cambios de entorno interno, externo y/o cuando sea solicitado por la normativa colombiana. Este proceso será liderado por el Oficial de Seguridad de la Información o quien haga sus veces y será aprobados por el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Integración Social.

CAPITULO II

LINEAMIENTOS ESPECIFÍCOS QUE SOPORTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO 12. DEFINICIÓN DE LINEAMIENTOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. La Subdirección de Investigación e Información nombrará al Oficial de Seguridad de la Información quien elaborará los lineamientos específicos para el manejo y mejora continua del Modelo de Seguridad y Privacidad de la Información -MSPI. Todos los lineamientos descritos en este capítulo están reglamentados de manera detallada y clara en la Declaración de Aplicabilidad y en los lineamientos específicos de seguridad y privacidad de la información y seguridad digital.

PARÁGRAFO. - A los líderes de proceso les corresponderá definir, documentar, mantener, actualizar y mejorar permanentemente los procedimientos relacionados con sus procesos, incluyendo aquellas actividades que sean consideradas como controles de Seguridad de la información dentro de dichos procedimientos, así como implementar, apoyar y soportar el Modelo de Seguridad y Privacidad de la Información -MSPI.

ARTÍCULO 13.- LINEAMIENTOS ESPECÍFICOS. Como complemento fundamental a la Política de Seguridad y Privacidad de la Información y Seguridad Digital en la Secretaría Distrital de Integración Social, se establecen los siguientes lineamientos específicos que a su vez, darán soporte al Modelo de Seguridad y Privacidad de la Información - MSPI:.

a. **Organización de seguridad de la información:** la Subdirección de Investigación e Información establecerá el marco de referencia de gestión para la implementación y operación de la seguridad de la información en la Secretaria Distrital de Integración Social – SDIS, propendiendo por proteger, preservar y administrar la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de la información que circula en los respectivos mapas de procesos del Sistema de Gestión, mediante una gestión integral de activos y riesgos, con la implementación de controles físicos y digitales, previniendo así eventos o incidentes y dando cumplimiento a los requisitos legales y reglamentarios, propendiendo de esta manera por el acceso, uso efectivo y apropiación de las TIC.

   La Subdirección de Investigación e Información documentará, implementará y propondrá mejoras continuas a los procesos, políticas, manuales, procedimientos, guías y otros tipos documentales que contemplen lineamientos de Seguridad y Privacidad de la Información; realizará acompañamiento a las diferentes dependencias de la Entidad en temas inherentes a la

protección de activos de información y gestionará y apoyará en la elaboración de conceptos sobre estos mismos temas, que solicite la Entidad.

b. **Gestión de proyectos**: La Dirección de Análisis y Diseño Estratégico establecerá los lineamientos específicos para que los proyectos o iniciativas de la SDIS incluyan los lineamientos relacionados con la seguridad de la información, identificación y tratamiento de los riesgos de seguridad de la información en todas las fases de los proyectos institucionales, de acuerdo con la metodología establecida por la SDIS, en armonía con lo señalado por el Ministerio de Tecnologías de la Información y las Comunicaciones, definiendo los roles, responsabilidades y procedimientos necesarios para la gestión de estos.

c. **Dispositivos móviles y BYOD:** la Subdirección de Investigación e información establecerá las medidas de seguridad frente a la confidencialidad, integridad, privacidad y disponibilidad de los activos de información que son accedidos, modificados, generados, transmitidos y/o eliminados desde dispositivos móviles institucionales y dispositivos personales (BYOD). Sin perjuicio de lo anterior, los dispositivos de cómputo asignados a los servidores públicos que aplican en modalidad de teletrabajo deberán contar con los siguientes controles como mínimo: sistema de autenticación, uso de software de antivirus suministrado por la Entidad, restricción de privilegios administrativos para los usuarios y uso de software licenciado suministrado por la Entidad. Para los dispositivos móviles autorizados que no son propiedad de la entidad, tales como tabletas, celulares o computadores portátiles, se deberá implementar la exigencia de requerimientos técnicos mínimos y de medidas de seguridad para gestionar los riesgos introducidos por el uso de dispositivos móviles y así asegurar que no se comprometa la información de la Entidad.

d. **Teletrabajo, trabajo en casa o trabajo remoto:** la Subdirección de Investigación e Información, junto con la Subdirección de Gestión y Desarrollo del Talento Humano, personal de planta, contratistas y con los supervisores de contratos, desarrollarán y establecerán los respectivos protocolos de monitoreo sobre las actividades desempeñadas en su trabajo, en estas modalidades, para minimizar el riesgo de afectación sobre la integridad, disponibilidad, privacidad y confidencialidad de los activos de información a los cuales tiene acceso durante el teletrabajo o trabajo en casa o trabajo remoto, lo anterior según aplique de acuerdo con la relación contractual o laboral de que se trate.

e. **Talento humano:** La Subdirección de Gestión, Desarrollo del Talento Humano y la Subdirección de Contratación, desarrollarán las acciones necesarias para que los colaboradores y terceros tomen conciencia y comprendan sus responsabilidades frente a la seguridad de la información, así como para su cumplimiento y protección de los intereses de la organización, durante su permanencia y en la terminación de la relación laboral o contractual que desarrollen.

f. Gestión de activos de información: La información, los sistemas, los servicios y los equipos (estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, servidores, aplicaciones, teléfonos, entre otros) de la Secretaria Distrital de Integración Social – SDIS, son activos de la Entidad que se facilitan a los funcionarios y contratistas para cumplir estrictamente con los propósitos institucionales, de acuerdo con la respectiva relación laboral o contractual según sea el caso; en este sentido, todos los activos de la Secretaria Distrital de Integración Social – SDIS, previa asignación a un responsable deben estar inventariados y clasificados de acuerdo con los requerimientos y los criterios para la clasificación de activos de la información. La Subdirección de Investigación e Información implementara los procedimientos frente a la identificación, uso, administración y responsabilidad asociados a los activos de información, estableciendo así las responsabilidades de protección apropiadas para minimizar los riesgos de seguridad digital.

g. Control de acceso: La Subdirección de Investigación e Información establecerá quién, cómo y cuándo puede acceder a los activos de la Secretaría Distrital de Integración Social y registrar dichos accesos, preservando los principios de seguridad de la información para los activos de información, que son accedidos y/o se encuentran bajo responsabilidad de los funcionarios, contratistas o terceros, debido a su cargo y/o responsabilidades. Por tal motivo, establecerá los controles que permitan gestionar de manera segura los accesos a las redes, áreas de procesamiento, plataformas tecnológicas, sistemas de información, datos e información, contra accesos no autorizados, a través de mecanismos de control de acceso lógico definidos por los propietarios de los activos, definiendo los controles de acceso, derechos y restricciones de acceso.

h. Política de Criptografía: La Subdirección de Investigación e Información propenderá por el uso apropiado y eficaz de la criptografía en procura de la protección de los activos de información sensibles de la Entidad mediante la implementación de herramientas que permitan el cifrado y garanticen la confidencialidad, integridad y disponibilidad de la información, transferencia a través de correo electrónico y otros mecanismos de transferencia de información a nivel interno y externo. Las llaves criptográficas de la Entidad deberán estar resguardadas por los responsables y custodios de la información. La administración de llaves criptográficas y certificados digitales estarán a cargo de la Subdirección de Investigación e Información.

i. Seguridad física y del entorno: La Subdirección de Investigación e Información, la Subdirección Administrativa y Financiera y la Subdirección de Plantas Físicas, definirán los lineamientos para prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización, disminuyendo el riesgo de acceso físico no autorizado, el daño y la interferencia a la información en las instalaciones de procesamiento de información de la Entidad, así como la pérdida, daño, robo o compromiso de activos y la interrupción de las operaciones de la Entidad. La Subdirección de Investigación e Información es la responsable de las medidas de seguridad física en donde se

resguardan los datos de la Entidad, tales como datacenter y centros de cableado estructurado.

j. Seguridad en las operaciones: La Subdirección de Investigación e Información definirá los lineamientos para establecer operaciones correctas y seguras en las instalaciones de procesamiento de información en la Secretaría de Integración Social, así mismo mantendrá documentados, formalizados, actualizados y divulgados los procedimientos relacionados con la operación y administración de los servicios y componentes tecnológicos que garanticen la disponibilidad, integridad, confidencialidad y privacidad de la información, tales como: copias de respaldo, mantenimiento de equipos, gestión de cambios, gestión de capacidad, gestión de eventos, entre otros. También velará por la eficiencia de los controles asociados a los recursos tecnológicos y para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de prueba y producción sean controlados y debidamente autorizados. De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad, e implementará mecanismos de contingencias, recuperación ante desastres y continuidad del negocio, con el fin de propender por la disponibilidad de los servicios de Tecnologías de la Información en el marco de la operación.

k. Seguridad de las comunicaciones: La Subdirección de Investigación e Información gestionará la protección de la información que transita en las redes de comunicaciones y sus instalaciones de procesamiento de información, manteniendo la seguridad de la información transferida de manera interna y con cualquier entidad externa; se establecerán mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios tecnológicos que soportan la operación de esta; así mismo, establecerá los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se envía a través de dichas redes de datos.

l. Adquisición, desarrollo seguro y mantenimiento de sistemas: La Subdirección de Investigación e Información establecerá las condiciones para que el desarrollo y mantenimiento de sistemas de información realizado tanto internamente como por proveedores externos, cumpla con buenas prácticas para el desarrollo seguro, además de establecer los criterios de seguridad que deben ser considerados en todas sus etapas, garantizando que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, así como con la aplicación de metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la institución.

m. Relaciones con los proveedores: La Subdirección de Investigación e Información y la Subdirección de Contratación definirán los requisitos de seguridad y privacidad de la información y seguridad digital para mitigar los riesgos asociados con el acceso de proveedores a los activos de la Secretaría Distrital de Integración Social, estableciendo los mecanismos de control con los

proveedores con el objetivo de asegurar que la información o servicios a los que tengan acceso, mantengan los controles de seguridad permitidos para su acceso o gestión. Adicionalmente, para todos los acuerdos, convenios, contratos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se solicitará la firma de acuerdos de confidencialidad sobre el manejo de la información, los cuales harán parte integral de los contratos o documentos que formalicen la relación contractual.

n. Gestión de incidentes de seguridad de la información: La Subdirección de Investigación e Información, por intermedio del Oficial de Seguridad de la Información, gestionará los incidentes de seguridad y privacidad de la información y seguridad digital al interior de la Secretaría Distrital de Integración Social, asegurando un enfoque coherente y eficaz incluida la comunicación sobre eventos de seguridad y debilidades. El procedimiento de gestión de incidentes debe contener los lineamientos mínimos tales como:

- Responsabilidades y procedimientos.
- Reporte de eventos de seguridad de la información.
- Reporte de debilidades de seguridad de la información.
- Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
- Respuesta a incidentes de seguridad de la información.
- Aprendizaje obtenido de los incidentes de seguridad de la información.
- Recolección de evidencia.

o. Seguridad de la información en la gestión de continuidad de negocio: La Subdirección de Investigación e Información, la Subdirección Administrativa y Financiera y la Subdirección de Plantas Físicas garantizarán la seguridad de la información en los sistemas de gestión de la continuidad de negocio de la Entidad, asegurando la disponibilidad de instalaciones de procesamiento de información y la continuidad tecnológica y operacional de las instalaciones de procesamiento de información.

ARTÍCULO 14.- VERIFICACIÓN DEL CUMPLIMIENTO: La Subdirección de Investigación e Información y la Oficina de Control Interno propenderán por el cumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con la seguridad de la información, garantizando que su implementación y operación este acorde con las políticas y procedimientos organizacionales.

El cumplimiento normativo que incluye esta política abarca normativa y requisitos contractuales, derechos de propiedad intelectual, protección de registros, privacidad y protección de información de datos personales, reglamentación de controles criptográficos, revisión independiente de la seguridad de la información, cumplimiento con las políticas y normas de seguridad y toda la revisión del cumplimiento técnico.

Las responsabilidades de ejecutar este lineamiento, cumplirlo a cabalidad y sin excepciones son para todos los funcionarios, contratistas y visitantes de la Secretaría de Integración Social

ARTÍCULO 15.- INSTRUMENTOS DE LA POLITICA. En la Secretaría Distrital de Integración Social se deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlos, en la página web de la entidad, a más tardar el 31 de enero de cada año, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011. Los instrumentos de gestión de esta política son los siguientes:

15.1. Lineamiento o Política de Administración de Riesgos. Es el instrumento a través del cual se establecen las directrices para la administración de riesgos en la Secretaría Distrital de Integración Social - SDIS, a través de la armonización de los lineamientos y la normativa vigente en la materia, con el fin de garantizar la adecuada identificación y tratamiento de los riesgos asociados a los procesos de la entidad, en cumplimiento de la misión institucional y objetivos estratégicos.

El lineamiento o Política de Administración de Riesgos de la Secretaría Distrital de Integración Social abarca el manejo de los riesgos asociados a los procesos definidos por la entidad, incluyendo los correspondientes a seguridad de la información, seguridad digital, en los siguientes términos:

- Riesgo de seguridad de la información: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño parcial o total en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.

- Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas. Este riesgo se encuentra inmerso en los riesgos de seguridad de la información.

15.2. El Modelo de Seguridad y Privacidad de la Información – MSPI. Es el instrumento a través del cual el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC, establece los lineamientos que deben seguir las entidades públicas en cumplimiento de la política de gobierno digital en su habilitador transversal "Seguridad de la información", con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

La Secretaría Distrital de Integración Social reconoce la importancia y el valor de los activos (en especial de la información) tanto para el funcionamiento al interior de la entidad como de cara a los ciudadanos y así mismo reconoce que deben protegerse de los posibles riesgos a los que puedan verse expuestos.

A fin de garantizar los principios de integridad, confidencialidad, disponibilidad y mitigar los posibles riesgos que puedan afectar a los activos, la Secretaría Distrital de Integración Social ha decidido implementar un Sistema de Gestión de Seguridad y Privacidad de la Información, de acuerdo con la normatividad vigente, estableciendo directrices en el marco de la transformación digital que permita maximizar la efectividad en los procesos y minimizar la exposición al riesgo derivado del uso de tecnologías de la información y las comunicaciones.

15.3. El Plan Estratégico de Tecnologías de la Información describe las iniciativas, estrategias y proyectos de Tecnologías de Información que se propone alcanzar Ia Subdirección de Investigación e Información para el periodo 2021 – 2024, con la finalidad de apoyar el cumplimiento de los objetivos misionales de Ia Secretaría Distrital de Integración Social, define estrategias, actividades, proyectos e iniciativas de tecnología que Ia Secretaría Distrital de Integración Social demanda para el cumplimiento del Plan Estratégico Institucional, fundamentados en un modelo de Tl estructurado en Ia Política de Gobierno Digital y el modelo de gestión IT4+, que soporten adecuadamente los procesos de Ia Entidad para el periodo mencionado.

PARÁGRAFO 1. El desarrollo en detalle de los lineamientos específicos descritos en el artículo 12 de la presente Resolución, se realizará a través de la instrumentalización del Manual de Seguridad y Privacidad de la Información y Seguridad Digital, a cargo del Oficial de Seguridad de la Información o quién haga sus veces.

PARÁGRAFO 2. El desarrollo y seguimiento a los instrumentos descritos en el artículo 15 de la presente Resolución, se llevará a cabo sin perjuicio de los demás instrumentos de gestión de la Política SPI que surjan con posterioridad a su expedición.

ARTÍCULO 16.- DEBERES GENERALES PARA EL CUMPLIMIENTO. La Entidad protegerá la información generada, procesada, transmitida y/o resguardada por los procesos y procedimientos en la prestación de los servicios estratégicos, misionales y operacionales, así como los activos de información que hacen parte de estos, con el fin de minimizar impactos negativos a la entidad; para ello, es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad y/o en custodia.

- La Entidad protegerá su información de las amenazas internas y/o externas por parte del personal custodio, responsable, usuario de esta y/o personas ajenas a la Entidad.

- La Entidad protegerá las instalaciones de procesamiento de datos e información y la infraestructura tecnológica que soporta sus procesos de soporte, misionales y estratégicos.

- La Entidad implementará controles de acceso a la información, sistemas y recursos de red.

- La Entidad verificará que la seguridad sea una pieza integral del ciclo de vida de los sistemas de información.

- La Entidad revisará a través de una adecuada gestión los eventos y/o incidentes de seguridad las debilidades asociadas con los sistemas de información, logrando una mejora efectiva de su modelo de seguridad y privacidad de la información.

- La Entidad verificará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas. El incumplimiento a la Política de Seguridad y Privacidad de la Información traerá consigo las consecuencias legales que apliquen de acuerdo con la normativa aplicable, incluyendo lo establecido en las normas que corresponden al Gobierno Nacional y territorial en cuanto a Seguridad, Privacidad de la Información y Gobierno Digital se refiere.

Todos los funcionarios, contratistas, proveedores, operadores, entes de control y los terceros que tengan alguna relación con la entidad, deben cumplir la Política de Seguridad y Privacidad de la Información y Seguridad Digital y sus lineamientos específicos.

El incumplimiento de la Política de Seguridad y Privacidad de la Información y Seguridad Digital en la Secretaría Distrital de Integración Social y de sus lineamientos específicos, así como la violación a los procedimientos que soporten la presente Política, generará responsabilidad civil, penal y disciplinaria, cuando por acción u omisión de sus lineamientos se cause un perjuicio a la entidad, a los ciudadanos o a terceros.

ARTÍCULO 17.- PUBLICACIÓN. La presente resolución deberá ser publicada en el enlace de Transparencia de la página web de esta Entidad, en cumplimiento a lo dispuesto en la Ley 1712 de 2014 y el Decreto Nacional 103 de 2015, compilado en el Decreto 1081 de 2015.

ARTÍCULO 18.-COMUNICACIÓN. Comunicar el contenido del presente acto administrativo a cada una de las dependencias de esta Secretaría, para su conocimiento y fines pertinentes.

"Por la cual se adopta la Política General de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social y se dictan otras disposiciones"

ARTÍCULO 19.- VIGENCIA Y DEROGATORIA. La presente Resolución rige a partir de la fecha de su expedición, o hasta que sea derogada por disposiciones que le sean contrarias.

PUBLÍQUESE, COMUNÍQUESE Y CUMPLASE

Dado en Bogotá, D.C., a los treinta 30 días del mes de junio de 2022.

MARGARITA BARRAQUER SOURDIS
Secretaria Distrital de Integración Social

Elaboró: Edna Rocio Univio Amaya – Apoyo Seguridad de la Información
Revisó: Jaime Guerrero Clavijo – Oficial Seguridad de la Información
Andrea Vega Rodríguez- Abogada Oficina Asesora Jurídica

Aprobó: Franky González Daza – Subdirector de Investigación e Información
Oscar David Garzón Alfaro - Subdirector de Diseño, Evaluación y Sistematización
Alexandra Rivera Pardo- Directora de Análisis y Diseño Estratégico
Andrés Pachón Torres - Jefe Oficina Asesora
Carlos Javier Muñoz Sánchez- Asesor Despacho

REGISTRO DE FIRMAS ELECTRONICAS

30062022 RESOLUCION PSISD VF OAJ-2

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

Id Acuerdo: 20220630-113417-16b455-74014409 Creación: 2022-06-30 11:34:17

Estado: Finalizado Finalización: 2022-06-30 18:22:12

Escanee el código para verificación

Aprobación: Aprobó

Franky González Daza
79602435
fgonzalezd@sdis.gov.co
Subdirector de Investigación e Información
Subdirección de Investigación e Información

Revisión: Revisó

Andrea Vega Rodríguez
52516635
avegar@sdis.gov.co
Profesional Especializada Grado 23
Secretaría Distrital de Integración Social

Revisión: Revisó

jaime guerrero clavijo
80894038
jguerreroc@sdis.gov.co
oficial de seguridad de la informacion
sdis

Elaboración: Elaboró

Edna Rocio Univio Amaya
1026251584
eunivio@sdis.gov.co
Profesional Seguridad Dígital
Subdirección de Investigación e Información

REGISTRO DE FIRMAS ELECTRONICAS

30062022 RESOLUCION PSISD VF OAJ-2

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20220630-113417-16b455-74014409 Creación: 2022-06-30 11:34:17

Estado: Finalizado Finalización: 2022-06-30 18:22:12

Escanee el código para verificación

Aprobación: Aprobó

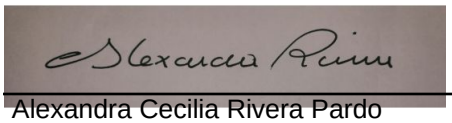
CARLOS JAVIER MUÑOZ SANCHEZ

cjmunozs@sdis.gov.co
ASESOR

Aprobación: Aprobó

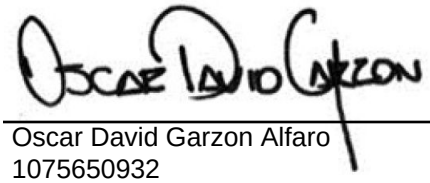
Andrés Felipe Pachón
80.871.878
apachon@sdis.gov.co
Jefe de la Oficina Asesora Jurídica
Secretaría Distrital de Integración Social

Aprobación: Aprobó



Alexandra Cecilia Rivera Pardo
39577611
arivera@sdis.gov.co
Director
SDIS

Aprobación: Aprobó



Oscar David Garzon Alfaro
1075650932
ogarzona@sdis.gov.co
Subdirector
Integracion Social

REGISTRO DE FIRMAS ELECTRONICAS

30062022 RESOLUCION PSISD VF OAJ-2

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20220630-113417-16b455-74014409
Creación: 2022-06-30 11:34:17
Estado: Finalizado
Finalización: 2022-06-30 18:22:12

Escanee el código para verificación

Aprobación: Aprobó

mbarraquer@sdis.gov.co

REPORTE DE TRAZABILIDAD

30062022 RESOLUCION PSISD VF OAJ-2

SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

gestionado por: azsign.com.co

Id Acuerdo: 20220630-113417-16b455-74014409 Creación: 2022-06-30 11:34:17

Estado: Finalizado Finalización: 2022-06-30 18:22:12

Escanee el código para verificación

TRAMITE	PARTICIPANTE	ESTADO	ENVIO, LECTURA Y RESPUESTA
Elaboración	Edna Rocio Univio Amaya eunivio@sdis.gov.co Profesional Seguridad Dígital Subdirección de Investigación e Información	Aprobado	Env.: 2022-06-30 11:34:18 Lec.: 2022-06-30 11:35:18 Res.: 2022-06-30 11:35:43 IP Res.: 186.86.52.23
Revisión	jaime guerrero clavijo jguerreroc@sdis.gov.co oficial de seguridad de la informacion sdis	Aprobado	Env.: 2022-06-30 11:35:43 Lec.: 2022-06-30 11:37:42 Res.: 2022-06-30 11:38:05 IP Res.: 191.95.60.11
Revisión	Andrea Vega Rodríguez avegar@sdis.gov.co Profesional Especializada Grado 23 Secretaría Distrital de Integración Social	Aprobado	Env.: 2022-06-30 11:38:05 Lec.: 2022-06-30 11:46:36 Res.: 2022-06-30 11:46:48 IP Res.: 190.156.72.248
Aprobación	Franky González Daza fgonzalezd@sdis.gov.co Subdirector de Investigación e Información Subdirección de Investigación e Información	Aprobado	Env.: 2022-06-30 11:46:48 Lec.: 2022-06-30 12:20:47 Res.: 2022-06-30 12:21:26 IP Res.: 186.155.7.19
Aprobación	Oscar David Garzon Alfaro ogarzona@sdis.gov.co Subdirector Integracion Social	Aprobado	Env.: 2022-06-30 12:21:26 Lec.: 2022-06-30 13:10:06 Res.: 2022-06-30 13:10:36 IP Res.: 186.155.7.19
Aprobación	Alexandra Cecilia Rivera Pardo arivera@sdis.gov.co Director SDIS	Aprobado	Env.: 2022-06-30 13:10:36 Lec.: 2022-06-30 13:19:57 Res.: 2022-06-30 13:20:16 IP Res.: 186.155.7.19
Aprobación	Andrés Felipe Pachón apachon@sdis.gov.co Jefe de la Oficina Asesora Jurídica Secretaría Distrital de Integración Social	Aprobado	Env.: 2022-06-30 13:20:16 Lec.: 2022-06-30 13:38:16 Res.: 2022-06-30 13:39:04 IP Res.: 190.25.70.120
Aprobación	CARLOS JAVIER MUÑOZ SANCHEZ cjmunozs@sdis.gov.co ASESOR	Aprobado	Env.: 2022-06-30 13:39:04 Lec.: 2022-06-30 14:33:57 Res.: 2022-06-30 14:34:55 IP Res.: 186.155.7.19
Aprobación	MARGARITA BARRAQUER SOURDIS mbarraquer@sdis.gov.co	Aprobado	Env.: 2022-06-30 14:34:55 Lec.: 2022-06-30 18:22:03 Res.: 2022-06-30 18:22:12 IP Res.: 186.155.7.19