



SECRETARÍA DE
INTEGRACIÓN SOCIAL



RESOLUCIÓN N.º _____ DE 2024

“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”

EL SECRETARIO 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 4º, del Decreto Distrital 607 de 2007,

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 Ley 1712 de 2014, Ley de Transparencia y del Derecho de Acceso a la Información Pública, 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 en cumplimiento de la Ley 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.

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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 Documento CONPES 3854 de 2016 - Política Nacional de Seguridad Digital, se establece un marco institucional claro y preciso en torno a la seguridad digital, complementado con el CONPES 3995 de 2020, buscando establecer medidas para desarrollar la confianza digital a través de la mejora 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 Decreto Nacional 767 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 Unico Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”* establece,

“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 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 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.

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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).*

Que 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 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 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 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*

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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 mediante el Decreto Distrital 221 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 establece el alcance de la Política de Seguridad Digital y su liderazgo en cabeza de la Alta Consejería de Tecnologías de la Información y la Comunicaciones – ACTIC, que es interlocutora en la materia con todas las entidades distritales, en los siguientes términos:

POLÍTICA	ALCANCE	LÍDER DISTRITAL
Gobierno Digital	Promover el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones -TIC, para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital y que a su vez permita optimizar la gestión de las entidades, interactuar de manera ágil y coordinada, trabajar conjuntamente en el diseño y desarrollo de políticas, normas, proyectos y servicios, y dar solución a problemáticas y necesidades de interés público.	Secretaría General - Alta Consejería de Tecnologías de la Información y la Comunicaciones - ACTIC

Que el Acuerdo Distrital 927 de 2024 “Por medio del cual se adopta el plan de desarrollo económico, social, ambiental y de obras públicas del distrito capital 2024-2027 “Bogotá Camina Segura”, establece en su artículo 16 los programas del Objetivo Estratégico “Bogotá Confía en su Gobierno”, entre ellos, el Programa 35 “Bogotá Ciudad Inteligente”, según el cual, Bogotá avanzará en el cierre de la brecha digital, y el sector público debe ser un ejemplo para ello. Con este propósito, adoptará el uso estratégico de la tecnología y los datos y la innovación para solucionar problemáticas y necesidades de interés colectivo mejorando la eficiencia en la gestión pública y la calidad de vida de la ciudadanía.

Que esta Secretaría expidió la Resolución No. 1414 de 2022 "*Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social*"

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

Que para hacer más eficiente al Comité Institucional de Gestión y Desempeño, en la Secretaría Distrital de Integración Social se expidió la Resolución No. 1074 de 2024, con el objeto de actualizar la reglamentación del Comité que estaba vigente, estableciendo en el artículo 5° dentro de sus funciones “(...) 5. *Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información*”.

Que para realizar por parte de los usuarios un buen uso de los activos de información de la Secretaría Distrital de Integración Social, se hace necesario definir e implementar la política de seguridad y privacidad de la información y seguridad digital que incluya los procedimientos relacionados con la gestión de datos de los beneficiarios que son víctimas del conflicto armado interno, la aplicación estricta del “Protocolo de gestión documental de los archivos referidos a las graves y manifiestas violaciones a los Derechos Humanos V. 2”, en cumplimiento de la Ley 1448 de 2011 y el Acuerdo 001 de 2024 del Archivo General de la Nación (AGN), Capítulo 2, título 9, para garantizar la protección, conservación y disposición final adecuada de la información sensible, con especial atención a las normas de protección de datos personales y derechos humanos.

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 y privacidad de la información y seguridad digital que indiquen lineamientos frente a la seguridad y privacidad de la información.

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.

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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 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.- COMPONENTES DE LA POLÍTICA. La Política de Seguridad y Privacidad de la Información y Seguridad Digital está conformada por estándares técnicos de seguridad aplicables en los procesos, procedimientos, estructura organizacional, mecanismos de verificación y control, infraestructura tecnológica para garantizar espacios digitales seguros, con una gestión documentada, sistemática, estructurada, eficiente y adaptable a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

ARTÍCULO 4.- DECLARACIÓN DE LA POLÍTICA. 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 5.- 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:

- Fortalecer los procesos, procedimientos, herramientas para impulsar acciones de cierre de brecha digital, generando espacios digitales seguros para la oferta de servicios confiables para los usuarios.
- Gestionar los riesgos de Seguridad y Privacidad de la información que afecten la confidencialidad, integridad, disponibilidad y privacidad de los activos de información institucional, a partir de la generación de capacidades de gestión de riesgos digitales, protección de datos personales y de aseguramiento de las infraestructuras críticas de la entidad.
- Identificar, clasificar, valorar y mantener actualizados los activos de información de la Entidad.
- Gestionar los incidentes y eventos de seguridad y privacidad que pongan en riesgo la

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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.

- 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.
- 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.
- Garantizar, a través de la implementación del Modelo de Seguridad y Privacidad de la Información, la continuidad de los servicios de la Entidad.
- Fomentar el uso y apropiación de las TIC en la Secretaría de Integración Social, contribuyendo con las políticas de seguridad y privacidad en los procesos de gestión, administrativos y formativos de la Entidad.

ARTÍCULO 6.- PRINCIPIOS. La Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social, tiene los siguientes principios:

- **Espacios digitales seguros.** 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 definidos por el líder de política nacional y los lineamientos que emita la Consejería Distrital de TIC.
- **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.
- **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.

ARTÍCULO 7.- 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:

- 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.
- 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 y privacidad de la información y seguridad digital.
- El personal encargado de la seguridad de la información, adscrito a la Subdirección de Investigación

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

e Información, que implementará y velará por el mantenimiento del Modelo de Seguridad y Privacidad de la Información de la Entidad.

- 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 8.- COMPROMISO DE LA ALTA DIRECCIÓN. La Secretaría Distrital de Integración Social, por intermedio de Subsecretaría, Direcciones, Subdirecciones y Oficinas, 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 9.- 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 ESPECÍFICOS QUE SOPORTAN EL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ARTÍCULO 10. DEFINICIÓN DE LINEAMIENTOS ESPECÍFICOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN. La Subdirección de Investigación e Información contará con un rol para la Seguridad de la Información, desde el cual se 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 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

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

Información -MSPI.

ARTÍCULO 11.- 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 Secretaría 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

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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 Secretaría 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 Secretaría 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 implementará los procedimientos necesarios para la identificación, uso, administración y protección de los activos de información, estableciendo así las responsabilidades adecuadas para minimizar los riesgos de seguridad digital.
- g. Control de acceso:** La Subdirección de Investigación e Información de la Secretaría Distrital de Integración Social (SDIS) establecerá los procedimientos para determinar quién, cómo y cuándo puede acceder a los activos de información de la SDIS, y registrar dichos accesos. Este proceso se llevará a cabo en coordinación con la Subdirección Administrativa y Financiera, que administra la gestión documental, y la Subdirección de Diseño, Evaluación y Sistematización, que se encarga del gobierno de la información. Se preservarán los principios de seguridad de la información para los activos de

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

información bajo la responsabilidad de los funcionarios, contratistas o terceros, de acuerdo con sus cargos y responsabilidades. Por tal motivo, se implementarán controles que permitan gestionar de manera segura los accesos a las redes, áreas de procesamiento, plataformas tecnológicas, sistemas de información, datos e información, protegiéndolos contra accesos no autorizados mediante mecanismos de control de acceso lógico definidos por los propietarios de los activos. Estos controles establecerán los derechos y restricciones de acceso necesarios.

- h. 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 u 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 entidad, 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 será responsable de las medidas de seguridad en datacenter y centros de cableado estructurado. La Subdirección Administrativa y Financiera gestionará los recursos y la documentación de activos, mientras que la Subdirección de Plantas Físicas diseñará, mantendrá y gestionará las barreras físicas y controles de acceso en las instalaciones.
- j. Seguridad en las operaciones:** La Subdirección de Investigación e Información definirá los lineamientos para establecer operaciones 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

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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 o quien haga sus veces, 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

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

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 12.- VERIFICACIÓN DEL CUMPLIMIENTO: La Subdirección de Investigación e Información, en su rol de primera línea de defensa, será responsable de implementar y operar las políticas y procedimientos relacionados con la seguridad de la información, asegurando que se cumplan las obligaciones legales, estatutarias, reglamentarias y contractuales. Por otra parte, la segunda línea de defensa revisa que las actividades de control y los procesos de la política implementados por la primera línea de defensa. Finalmente, la Oficina de Control Interno, como tercera línea de defensa, se encargará de evaluar la efectividad y el cumplimiento de dichas políticas y procedimientos conforme a los estándares organizacionales establecidos.

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 13.- INSTRUMENTOS DE LA POLITICA. En la Secretaría Distrital de Integración Social se deberán integrar los planes institucionales y estratégicos que articulan los esfuerzos para la gestión de la información y la garantía de espacios digitales seguros, los cuales se publicarán en la página web de la entidad, anualmente, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión,

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011.

ARTÍCULO 14.- 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 con acceso a su información.
- 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.
- La Entidad protegerá la información de las víctimas de conflicto armado, y de las víctimas atendidas en las comisarías de familia.

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 15.- 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

Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

compilado en el Decreto 1081 de 2015 y de acuerdo con la Resolución 1519 donde se establece lineamientos para la implementación de políticas de seguridad de la información en entidades públicas del territorio Colombiano.

ARTÍCULO 16.- COMUNICACIÓN. Comunicar el contenido del presente acto administrativo a cada una de las dependencias de esta Secretaría, para su conocimiento y fines pertinentes.

ARTÍCULO 17.- VIGENCIA Y DEROGATORIA. La presente Resolución rige a partir de la fecha de su expedición y deroga todas las disposiciones que le sean contrarias, en especial, la Resolución No. 1414 de 2022.

PUBLÍQUESE, COMUNIQUESE Y CÚMPLASE

Dado en Bogotá, D.C., a los _____ () días del mes de _____ de dos mil _____ (2024).

ROBERTO CARLOS ANGULO SALAZAR
Secretario Distrital de Integración Social

Elaboró: Edna Rocio Univio Amaya - Contratista

Revisó: Claudia Patricia Guerrero – Contratista

Gloria Matilde Torres Cruz – Subdirectora Administrativa y Financiera

Lina Maria Sanchez Romero - Subsecretaria de gestión institucional

Oscar David Garzon Alfaro – Subdirector de Diseño, Evaluación y Análisis Estratégico

Laura Alejandra Contreras Salazar - Jefe de Oficina Jurídica

Maria Camila Diaz Marin - Directora de Gestión Corporativa

Ines Francy Peña Medina – Gestión Documental

Aprobó:

Lina Maria Sanchez – Subsecretaria de gestión institucional

Maria Camila Diaz - Directora de Gestión Corporativa

Laura Alejandra Contreras – Jefe de Oficina Jurídica

Helena Patricia Hernandez - Directora Poblacional (E)

Ivon Carolina Camargo - Directora de Nutrición y Abastecimiento

Sandra Patricia Orozco - Directora Territorial

Juliana Sanchez Subsecretaria técnica

Roberto Angulo Salazar – Secretario de despacho

Ivan Osejo Villamil - Director de Análisis y Diseño Estratégico/ Secretario Técnica del Comité

Diana Patricia Martinez - Directora para la Inclusión y las Familias

Mauricio Sandino - Director de Transferencias

Sede Principal: Carrera 7 # 32 -12 / Ciudadela San Martín
Secretaría Distrital de Integración Social
Teléfono: 3 27 97 97
Correo electrónico institucional: integracion@sdis.gov.co





Continuación de la Resolución No. XXXX DE XX DE XXXXX 2024

“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”

