# Objetivo general

Establecer las políticas complementarias para la adecuada gestión de la seguridad y privacidad de la información, desarrollando los lineamientos específicos para el cumplimiento de los controles, propendiendo por la protección de la confidencialidad, integridad, disponibilidad, privacidad, continuidad, autenticidad, no repudio y el cumplimiento de la normativa vigente aplicable, mediante la implementación, medición y mejora continua del Sistema de Gestión de Seguridad de la Información de la Secretaria Distrital de Integración Social -SDIS-.

1. Objetivos específicos
* Identificar e implementar las tecnologías necesarias para fortalecer la función de la seguridad de la información en la entidad.
* Implementar el Sistema de Gestión de Seguridad de la Información.
* Proteger la información y los activos de la información de la entidad.
* Asegurar la identificación y gestión de los riegos a los cuales se expone los activos de información de la entidad.
* Cumplir con los principios de seguridad de la información: disponibilidad, integridad y confidencialidad de la información.
* Concientizar a los funcionarios, contratistas sobre el uso adecuado de los activos de información puestos a su disposición para la realización de las funciones y actividades diarias, garantizando la confidencialidad, la privacidad y la integridad de la información.
* Dar cumplimiento a los lineamientos establecidos en la Estrategia de Gobierno en Línea y Seguridad de la Información respecto a la Seguridad de la Información.
* Dar las pautas generales para la protección de los datos personales y sensibles, brindando herramientas que garanticen la autenticidad, confidencialidad e integridad de la información.
* Regular la recolección, tratamiento, almacenamiento, protección y administración de los datos personales legalmente obtenidos de sus funcionarios, contratistas, usuarios, proveedores, terceros y ciudadanos en general, que puedan involucrarse en virtud del desarrollo de sus actividades misionales, captados a través de los diferentes canales de

información y almacenados en bases de datos de la entidad, sujetos a tratamiento y protección de datos personales.

1. Alcance

El presente documento aplica a todos los funcionarios, contratistas, proveedores, operadores, entes de control y a los terceros que en razón del cumplimiento de sus funciones y las de la Secretaria Distrital de Integración Social - SDIS, compartan, utilicen, recolecten, procesen, intercambien o consulten información de forma interna o externa, independientemente de su ubicación.

1. Vigencia

El lineamiento rige a partir de su aprobación por el Comité Institucional de Coordinación del Sistema de Control Interno, se adopta mediante acto administrativo del líder del proceso responsable, y permanece vigente hasta una nueva actualización.

1. Marco conceptual
* Access Point: (Punto de Acceso Inalámbrico) es un dispositivo de red que interconecta equipos de comunicación inalámbricos.
* Activo: cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales, de apoyo y operativos de la Secretaria Distrital de Integración Social -SDIS-. Se pueden clasificar de la siguiente manera:
* Datos: son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la entidad.
* Aplicaciones: es todo el software que se utiliza para la gestión de la información en la entidad.
* Servicios: son los servicios internos, aquellos que en parte la entidad suministra a otra, como los externos, aquellos que la entidad suministra a clientes y usuarios.
* Tecnología: son todos los equipos utilizados para gestionar la información y las comunicaciones.
* Instalaciones: son todos los lugares en los que se alojan los sistemas de información.
* Acuerdo de confidencialidad: es un documento en los que los funcionarios, contratistas y terceros manifiestan su voluntad de mantener la confidencialidad de la información de la Secretaria Distrital de Integración Social -SDIS, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
* Almacenamiento en la nube: es un modelo de servicio en el cual la información de un equipo de cómputo se almacena, se administra, y se respalda de forma remota, permitiendo acceder a la información a través de internet.
* Aplicaciones: es todo el software que se utiliza para la gestión de la información.
* Autenticación: es el procedimiento de comprobación de identidad de un usuario al intentar acceder a un recurso tecnológico o sistema de información.
* Base de datos: es una colección de información organizada con el propósito que sea fácilmente accesible, administrada y actualizada.
* Centros de cableado: son cuartos donde se ubican los dispositivos de comunicación, tecnológicos y en gran parte los cables.
* Cifrado: es un procedimiento que utiliza un algoritmo que está escrito con letras, símbolos o números que solo puede interpretarse si se dispone de la clave para descifrarlos.
* Criptografía: es el proceso para proteger la información al transformarla en un formato seguro, con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
* Control de acceso: medios para asegurar que el acceso a los activos está autorizado y restringido en función de los requisitos de la entidad y de seguridad.
* Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información en todos los servicios de la entidad.
* Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.
* Integridad: propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada.
* Información: es el activo más importante para llevar a cabo las actividades de la entidad, por lo anterior requiere una protección adecuada, se describe a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inserción de formas textuales, gráficas, cartográficas, audiovisuales, etc. y en cualquier medio, magnético, en papel, pantallas de computadoras, audiovisual u otro.
* Disponibilidad: es una característica, cualidad o condición de la información que se encuentra a disposición de quien tiene que acceder a esta, por usuarios, procesos o aplicaciones.
* Incidente de seguridad de la información: es una ocurrencia identificada en el estado de un sistema, servicio o red, indicando una posible violación de la seguridad de la información, política o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad.
* Riesgo de información: es el proceso sistemático de identificación de fuentes, gestión y estimación de impactos, probabilidades comparando estos componentes contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información de la entidad.
* Dato sensible: es aquel dato personal de especial protección, por cuanto afecta la intimidad del titular y su tratamiento puede generar discriminación.
* Firmware: (programación en firme) es un software que opera físicamente el hardware en varios dispositivos tecnológicos.
* Malware: (software malicioso) es todo programa malicioso cuya función es causar un mal funcionamiento a un sistema informático.
* Plataforma tecnológica: es un conjunto de elementos compuestos por hardware y software que permiten el funcionamiento de aplicaciones, sistemas etc.
* Sistema de información: es el conjunto de tecnologías, procesos, aplicaciones, etc. relacionadas entre sí, permitiendo que la información esté disponible para satisfacer las necesidades de la entidad.
* Software: es un conjunto de programas y rutinas que incluye datos, procedimientos y pautas que permiten realizar diferentes tareas en un sistema de información.
* Spam: correo basura o mensaje basura a los mensajes no solicitados, son tipo publicitario, enviados de forma masiva, que perjudican de alguna o varias maneras al receptor.
* UPS: es un dispositivo conformado por elementos almacenadores de energía, para suministrar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.
* Virus informático: es un software que busca alterar el normal funcionamiento de los equipos de cómputo, sin el permiso o conocimiento del usuario.
* VPN: (Red Privada Virtual) es una tecnología de red utilizada para conectar uno o varios equipos de cómputo a una red privada a través de internet.
1. Marco normativo

El diseño e implementación del Sistema de Gestión de Seguridad de la Información -SGSI- de la Secretaria Distrital de Integración Social -SDIS se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones -MINTIC-:

* Resolución --- de 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 deroga la Resolución No. 0083 de 2021.
* Guía 2 Modelo de Seguridad y Privacidad de la Información -MSPI- V1.
* Ley 1581 de 2012 denominada “Protección de Datos Personales”.
* Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
* Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”
* Conpes 3995 de 2020, de “Política Nacional de Confianza y Seguridad Digital”.
* Conpes 3701 Lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.
* Conpes 3854 Política Nacional de Seguridad digital. Establece un marco institucional claro en torno a la seguridad digital.
* Modelo Integrado de Planeación y Gestión MIPG versión 2 – 2018.
* Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones.
* Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP, 2018) Guía que unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos.
* 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.
* ISO-IEC 27002:2013 (Icontec, 2015) Tecnología de la información. Técnicas de seguridad. Código de práctica para controles de seguridad de la información.
1. Desarrollo del Lineamiento o Política Interna

En la Resolución --- de 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 que deroga la Resolución No. 0083 de 2021”, basa su estructura en el Modelo de Seguridad y Privacidad de la Información -MSPI- el cual hace parte integral de la estrategia de Gobierno Digital mediante el desarrollo del habilitador transversal de seguridad de la información y de la cual se desprenden políticas específicas orientadas a la mejora continua y alto desempeño del Sistema de Gestión de la Entidad, en lo atinente a la seguridad y privacidad de la información y seguridad digital.

Para la Secretaria Distrital de Integración Social – SDIS, el concepto de política se alinea al concepto de lineamiento, entendiendo este como *una directriz general a mediano y largo plazo de obligatorio cumplimiento (sinónimo de política Interna).*

Los lineamientos específicos desarrollados en el presente manual guiarán el comportamiento del personal en cumplimiento de la responsabilidad asignada para la formulación e implementación de políticas públicas poblacionales orientadas al ejercicio de derechos, alineado con la protección y preservación de la colección de datos organizada para dar servicio a muchas aplicaciones al mismo tiempo, al combinar los datos de manera que parezcan estar en una sola ubicación, con el fin de preservar los principios de confidencialidad, integridad y disponibilidad de la información y se convierten en la base para la implementación de los controles, procedimientos y/o estándares.

Cada lineamiento se compondrá de la siguiente estructura:

1. Objetivo: describe la intención de la política.
2. Responsables de la ejecución política: describe quién es el responsable de dar los lineamientos y las acciones para cumplir los requisitos de la política.
3. Responsables del cumplimiento de la política: describe quién es el responsable de hacer cumplir los lineamientos y las acciones para cumplir los requisitos de la política.
4. Controles que abarcan la Norma: hace referencia a los controles de la norma, y en los cuales se dan los lineamiento y cumplimiento de esta.
5. Lineamientos: es la descripción de como la entidad da cumplimento a los controles definidos en la norma ISO 27001:2013.
	1. Política de seguridad y privacidad de la información
		1. Lineamientos

La Secretaria Distrital de Integración Social – SDIS a través de la Política de Seguridad y Privacidad de la información, busca propender que se mantengan los objetivos institucionales de la entidad, por lo tanto, la política tiene lo siguientes objetivos:

1. Promover una cultura de Seguridad al interior la Secretaria Distrital de Integración Social – SDIS con el objetivo de generar confianza en los procesos de la entidad y sus niveles de seguridad.
2. Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
3. Establecer e implementar el Modelo de seguridad y privacidad de la información a través de la socialización y prevalencia de la Política General de Seguridad y Privacidad de la Información.
4. Cumplir con los principios fundamentales de seguridad confidencialidad, integridad y disponibilidad de la información y los lineamientos y/o controles de Seguridad y Privacidad de la Información definidos por la Entidad.
5. Mejorar los procesos, procedimientos e instructivos en materia de seguridad de la información para toda la entidad.
6. Propender por el cuidado de los activos de información de la Entidad, a través de la identificación y/o actualización de los activos de información y sus riesgos asociados.
7. Fomento del uso y apropiación de las TIC en la Secretaria Distrital de Integración Social – SDIS para que contribuya en las políticas de seguridad y privacidad en los procesos de gestión, administrativos y formativos de la entidad.
8. Dar lineamientos para la implementación de mejores prácticas de seguridad que permita identificar infraestructuras críticas en la Entidad.
9. Proporcionar elementos que permiten a la Secretaria Distrital de Integración Social – SDIS contribuir a la aplicación de controles para hacer seguimiento a la eficacia y aplicación de las políticas y procedimientos.
10. Apoyar a las dependencias de la entidad para la salvaguarda de la información y demás servicios tecnológicos propios de la Secretaria Distrital de Integración Social – SDIS, con el propósito de proteger a la entidad de riesgos, ataques por virus, compromiso de los sistemas de red, los servicios y aspectos legales.
11. Establecer lineamientos y políticas de seguridad y privacidad de la información que definan las directrices formales de actuación en la Entidad.
12. Definir, gestionar y mantener roles y responsabilidades en materia de Seguridad y Privacidad de la Información que apoyen la gestión del Modelo definido en la Entidad.
13. Mantener actualizadas las políticas y procedimientos relacionados con la Seguridad y Privacidad de la Información.
14. Propender al cumplimiento de las obligaciones legales, regulatorias o contractuales de la Entidad, que se encuentren relacionadas con la Seguridad y Privacidad de la Información.
15. Dar una respuesta oportuna y adecuada en caso de materializarse un evento que pudiera afectar la disponibilidad de los recursos que son indispensables para el desarrollo de las diferentes actividades de la Entidad, personas, locaciones, tecnología, información o proveedores.
16. Propender a la seguridad de la información con el fin de mantener su integridad y la continuidad del acceso a la información ante situaciones adversas que se pudieran presentar en la Secretaria Distrital de Integración Social – SDIS.
17. Identificar, analizar, evaluar y tratar los riesgos de seguridad de la información, con el fin de prevenir o reducir su impacto sobre el normal desarrollo de las actividades de la Secretaria Distrital de Integración Social – SDIS.
18. Propender a una adecuada gestión de incidentes, eventos o debilidades de seguridad de la información, reduciendo su impacto, propagación y duración.
19. Fortalecer el conocimiento y las habilidades en seguridad y privacidad de la información en todos los funcionarios, contratistas y terceros de la Secretaria Distrital de Integración Social – SDIS.
20. Sensibilizar al personal de la entidad en el uso adecuado, la importancia y protección de los activos de información.
21. Definir, implementar, operar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información MSPI de la Secretaria Distrital de Integración Social – SDIS aumentando y manteniendo el nivel de madurez requerido por la entidad.
	1. Política organización de la seguridad de la información
		1. Objetivo

Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información en la Secretaria Distrital de Integración Social – SDIS.

* + 1. Responsable(s) de la ejecución de la política
* Dirección de Análisis y Diseño Estratégico
* Subdirección de Investigación e información -SII

* + 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A
* A.6.1.1 Roles y responsabilidades para la seguridad de la información.
* A.6.1.2 Separación de deberes.
* A.6.1.3 Contacto con las autoridades.
* A.6.1.4 Contacto con grupos de interés especial.
	+ 1. Lineamientos:

La Secretaria Distrital de Integración Social – SDIS a través del Comité de Gestión y Desempeño que representa a la Alta Dirección, debe proteger los activos de información que ha identificado y clasificado la Entidad (las partes interesadas internas y externas, la información como tal, los procesos, las tecnologías de información y la comunicación: tecnologías y personas involucradas en éstas), y de esta manera apoya la implementación del Sistema de Gestión de Seguridad de la Información - SGSI, el cual tiene como referencia para su implementación el Modelo de Seguridad y Privacidad de la Información – MSPI del MinTIC, por medio de la aprobación de las respectivas políticas, procesos, procedimientos e instructivos, orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, privacidad y a la continuidad de las operaciones de la Entidad a través de la gestión de los activos y de los riesgos de seguridad y privacidad de la información; fomentando la creación de una cultura y conciencia de seguridad en los funcionarios de la Secretaria Distrital de Integración Social – SDIS, los cuales se encuentran fundamentados en la NTC-ISO/IEC27001:2013 a través de la asignación de responsabilidades generales y específicas para llevar a cabo la gestión de dicho sistema de gestión.

Este compromiso se verá reflejado a través de:

1. Asignar el rol de Oficial de Seguridad de la Información - CISO, quien será el encargado de liderar los temas relacionados con seguridad y privacidad de la información, continuidad del negocio, protección de datos personales, entre otros.
2. Asignar el rol de Gestor de Seguridad de la Información quien se encargará de apoyar la implementación, fortalecimiento, revisión, medición y mejora continua del SGSI.
3. Asignar el rol de Gestor de Seguridad de la Información, quien se encargará de apoyar la implementación, seguimiento, medición y mejora continua de la protección de los datos y privacidad de la información institucional.
4. Asignar el rol de Gestor de Seguridad de la información, quien se encargará de apoyar la implementación, seguimiento, medición y mejora continua de la continuidad del negocio a nivel institucional.
5. Conformar un equipo de trabajo de profesionales de la Subdirección de Investigación e información -SII en conjunto con infraestructura y SGSI para la implementación, seguimiento y mejoramiento continuo de la seguridad, privacidad de la información y protección de datos personales.
6. Apoyar mediante diferentes estrategias institucionales el cumplimiento de las políticas de seguridad y privacidad de la información, para que los directivos, servidores públicos, contratistas y terceros de la Secretaria Distrital de Integración Social – SDIS las conozcan, apliquen y cumplan.
7. Definir, asignar y realizar seguimiento a las responsabilidades asociadas a temas de la seguridad y privacidad de la información, en los diferentes roles que hagan parte del Sistema de Gestión de Seguridad de la Información.

La Subdirección de Investigación e información -SII es responsable del diseño y determinación de las políticas, orientaciones estratégicas, planes, programas y proyectos de la Secretaria Distrital de Integración Social – SDIS, en relación con el MSPI; promoviendo y apoyando la implementación en la Entidad de una cultura de la gestión orientada por resultados, por lo que debe:

1. Definir y asignar las responsabilidades asociadas a la seguridad y privacidad de la información, teniendo en cuenta la segregación de funciones, separando las que se encuentren en conflicto.
2. Revisar y aprobar la política y manual de políticas de seguridad y privacidad de la información, la política y manual de protección de datos personales; garantizando su difusión y aplicación en la entidad.
3. Apoyar el cumplimiento de las políticas de seguridad y privacidad de la información y protección de datos personales, por parte de los colaboradores y proveedores para que las conozcan, apliquen y cumplan.
4. Acompañar y promover el desarrollo de estrategias de seguridad y privacidad como los planes de socialización, capacitación y apropiación de los temas relacionados con el SGSI.
5. Conocer los diagnósticos del nivel de implementación del SGSI en la entidad y tomar las decisiones que sean necesarias para apoyar su mejoramiento continuo.
6. Realizar revisiones periódicas del SGSI (por lo menos una vez al año) y según los resultados de esta revisión definir las acciones pertinentes.
7. Motivar el entendimiento, la toma de conciencia y el cumplimiento de las políticas, normas, procedimientos y estándares establecidos.
8. Evaluar en forma permanente los modelos de operación del MSPI en todas las áreas de la entidad y proponer esquemas de mejoramiento de estos, en coordinación con las diferentes dependencias de la Entidad.
9. Definir, liderar y socializar la documentación como políticas, manuales, procedimientos y guías y demás, relacionados con la Seguridad y Privacidad de la Información.
10. La Subdirección de Investigación e información -SII y la Subdirección de gestión y desarrollo de talento, serán los encargados de convocar a los directivos, funcionarios y contratistas a las sensibilizaciones, charlas, talleres y/o eventos programados como parte del plan de comunicaciones en seguridad de la información, que se realizará anualmente y proveer los recursos para su ejecución y control.
11. Conformar el equipo de trabajo para gestionar la seguridad y privacidad de la Información encargado de liderar, planear, implementar, controlar, gestionar, medir y rendir cuentas sobre la seguridad y privacidad de la información, continuidad del negocio, datos personales y el Sistema de Gestión de Seguridad de la Información - SGSI, quienes realizarán las actividades descritas a continuación:

Oficial de Seguridad de la Información -CISO: Este rol debe liderar todas las actividades de seguridad, privacidad de la información y protección de datos, cumpliendo con las siguientes tareas y actividades:

1. Realizar las actividades de planeación, ejecución y seguimiento de los proyectos relacionados con la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, Protección de Datos y Continuidad del Negocio, de acuerdo con la normatividad vigente.
2. Realizar las actividades de planeación, ejecución y seguimiento a la construcción e implementación del Plan de Continuidad del Negocio y Plan de Continuidad Tecnológico.
3. Definir y gestionar el Plan Anual de Seguridad y Privacidad de la Información.
4. Gestionar la apropiación y cumplimiento de la documentación como políticas, manuales, directrices y procedimientos del Sistema de Gestión de Seguridad de la Información y Protección de Datos Personales.
5. Gestionar y hacer seguimiento a la solución técnica de incidentes y eventos de seguridad de la información que ocurran en la Secretaria Distrital de Integración Social – SDIS, de acuerdo con los lineamientos establecidos en el Sistema de Gestión de Seguridad de la Información – SGSI.
6. Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad y privacidad de la información.
7. Definir el plan de concientización y sensibilización en Seguridad y Privacidad de la Información de la entidad y apoyar su ejecución y seguimiento.
8. Gestionar la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.
9. Evaluar el nivel de implementación y efectividad de los controles de seguridad, políticas y procedimientos que conformen el Sistema de Gestión de Seguridad de la Información – SGSI para definir o realizar mejoras a los mismos.
10. Gestionar las acciones correctivas y preventivas que se deriven de las auditorías internas y externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI.
11. Coordinar las actividades para la gestión de activos de información, riesgos de seguridad y privacidad de la información en todos los procesos la Secretaria Distrital de Integración Social – SDIS.
12. Documentar y proponer mejoras continuas a los procesos y procedimientos, políticas, guías, manuales y otros tipos documentales que conformen el Sistema de Gestión de Seguridad de la Información - SGSI y otros sistemas de Gestión de la Secretaria Distrital de Integración Social – SDIS.
13. Elaborar los informes de avance de las actividades del proyecto de implementación que exige el Modelo de Seguridad y Privacidad de la Información – MSPI, así como los del Sistema de Gestión de Seguridad de la Información.

Gestor de Seguridad de la información: Este rol se encargará de apoyar la implementación, fortalecimiento, revisión, medición y mejora continua del SGSI, cumpliendo con las siguientes tareas y actividades:

1. Apoyar las actividades de ejecución, seguimiento y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información - SGSI de acuerdo con la normatividad vigente.
2. Apoyar en la articulación del Sistema de Gestión de Seguridad de la Información con los otros Sistemas del Sistema Integrado de Gestión de la Secretaria Distrital de Integración Social – SDIS, recomendando buenas prácticas en materia de Seguridad y Privacidad de la información.
3. Documentar y proponer mejoras continuas a los procesos, procedimientos, políticas, guías, manuales, y otros tipos documentarles que conformen el Sistema de Gestión de Seguridad de la Información - SGSI y otros sistemas de gestión de la Entidad.
4. Apoyar en la definición e implementación del Plan de Continuidad del Negocio la Secretaria Distrital de Integración Social – SDIS.
5. Apoyar la ejecución y monitoreo de las actividades de sensibilización y concientización en todo lo referente a seguridad y privacidad de la Información a los colaboradores de la Secretaria Distrital de Integración Social – SDIS.
6. Apoyar en el seguimiento a las acciones de remediación que se deriven de la ejecución de las pruebas de seguridad (hacking ético y análisis de vulnerabilidades) que se realicen a los sistemas de información de la entidad.
7. Apoyar en la evaluación del nivel de implementación y efectividad de los controles de seguridad, políticas y procedimientos que conformen el Sistemas de Gestión de Seguridad de la Información – SGSI proponiendo e implementando medidas correctivas y preventivas para mitigar vulnerabilidades e incrementar el nivel de implementación y efectividad de los controles de seguridad.
8. Apoyar en la gestión de las acciones correctivas y preventivas que se deriven de las auditorías internas y externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI.
9. Apoyar las actividades para la gestión de activos de información.
10. Apoyar las actividades para la gestión de riesgos de seguridad y privacidad de los procesos de la Secretaria Distrital de Integración Social – SDIS.
11. Apoyar las actividades de ejecución, seguimiento y mejoramiento continuo en lo referente a Protección de Datos Personales, de acuerdo con la normatividad vigente.
12. Documentar y proponer mejoras continuas a los procesos, procedimientos, políticas, guías, manuales, políticas y otros tipos documentarles que contemplen lineamientos en Protección de Datos, alineados con Seguridad y Privacidad de la Información.
13. Realizar acompañamiento a las diferentes dependencias de la entidad en temas inherentes a la protección de datos, de conformidad con la normatividad vigente.
14. Apoyar en la gestión técnica de incidentes y eventos relacionados con Protección de Datos que se presente en la entidad.
15. Apoyar la ejecución y monitoreo de las actividades de sensibilización y concientización a nivel institucional en lo referente con la protección de datos y privacidad de la información.
16. Evaluar el nivel de implementación, cumplimiento y efectividad de los controles de protección de datos, de acuerdo con las políticas, manuales y procedimientos establecidos, proponiendo e implementando medidas correctivas y preventivas e incrementar el nivel de implementación y efectividad de los controles en la Secretaria Distrital de Integración Social – SDIS.
17. Apoyar en la gestión de las acciones correctivas y preventivas que se deriven de las auditorías internas y externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI y Privacidad de la información.
18. Apoyar las actividades para la gestión de activos de información y riesgos de protección de datos para todos los procesos de la Secretaria Distrital de Integración Social – SDIS.
19. Apoyar las actividades definición de ejecución, seguimiento y mejoramiento continuo de Continuidad del Negocio de acuerdo con la normatividad vigente.
20. Apoyar en la articulación del Sistema de Gestión de Seguridad de la Información con la Continuidad del Negocio de la Secretaria Distrital de Integración Social – SDIS, recomendando buenas prácticas en materia de Seguridad y Privacidad de la información.
21. Documentar y proponer mejoras continuas a los procesos, procedimientos, políticas, guías, manuales y otros tipos documentarles que conformen la Continuidad del Negocio.
22. Apoyar la ejecución y monitoreo de las actividades de sensibilización y concientización a nivel institucional en todo lo referente a Continuidad del Negocio.
23. Apoyar en el seguimiento a las actividades de mejoramiento continuo que se deriven de los resultados de la ejecución de las pruebas al Plan de Continuidad del Negocio y continuidad tecnológica.
24. Evaluar el nivel de implementación y efectividad de los controles de seguridad, políticas y procedimientos que conformen la Continuidad del Negocio proponiendo e implementando medidas correctivas y preventivas para mitigar vulnerabilidades e incrementar el nivel de implementación y efectividad de los controles de seguridad.
25. Apoyar las actividades para la identificación del BIA en los procesos de la Secretaria Distrital de Integración Social – SDIS.
26. Apoyar las actividades para la gestión de riesgos de Continuidad del Negocio de los procesos de la Secretaria Distrital de Integración Social – SDIS.

La Subdirección de Investigación e información -SII y los propietarios de sistemas son responsables de apoyar la implementación de las políticas, procedimientos, guías y demás lineamientos de seguridad y privacidad de la información de manera tecnológica, alineados al MSPI y demás funciones señaladas en el art. 8 del Decreto 249 de 2003 de la Función Pública, por lo que le corresponde:

1. Apoyar en la implementación y monitoreo de las políticas de seguridad y privacidad de la información definidas por de la Secretaria Distrital de Integración Social – SDIS.
2. Apoyar en la implementación de controles que aporten a la disponibilidad, integridad, confidencialidad y privacidad de los activos de información.
3. Apoyar la ejecución y monitoreo de las actividades de sensibilización y concientización en todo lo referente a seguridad y privacidad de la Información a los funcionarios y contratistas de la Secretaria Distrital de Integración Social – SDIS.
4. Gestionar y realizar seguimiento a las acciones de remediación que se deriven de la ejecución de las pruebas de seguridad (hacking ético y análisis de vulnerabilidades) que se realicen a los sistemas de información de la entidad.
5. Apoyar en la evaluación del nivel de implementación y efectividad de los controles de seguridad, políticas y procedimientos que conformen el Sistema de Gestión de Seguridad de la Información – SGSI, proponiendo e implementando medidas correctivas y preventivas para mitigar vulnerabilidades e incrementar el nivel de implementación y efectividad de los controles de seguridad.
6. Apoyar en la gestión de las acciones correctivas y preventivas que se deriven de las auditorías internas y externas que se realicen al Sistema de Gestión de Seguridad de la Información – SGSI.
7. Apoyar las actividades para la gestión de activos de información, riesgos de seguridad y privacidad de los procesos de la Secretaria Distrital de Integración Social – SDIS.
8. Gestionar los requerimientos de gestión de accesos, gestión de usuarios en todos los aplicativos y sistemas de información de la Secretaria Distrital de Integración Social – SDIS.
9. Apoyar en la definición y revisión de los lineamientos para la adquisición y desarrollo de sistemas de información teniendo en cuenta las buenas prácticas de desarrollo seguro.
10. Apoyar en la definición y revisión de los lineamientos para la adquisición, afinamiento y actualización de las plataformas de seguridad y privacidad de la Secretaria Distrital de Integración Social – SDIS.
11. Gestionar la tercerización de los bienes y servicios tecnológicos requeridos para soportar la prestación de los servicios críticos de la Secretaria Distrital de Integración Social – SDIS.
12. Atender y gestionar oportunamente los incidentes de seguridad de la información, así como realizar la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados.
13. Dar cumplimiento a las responsabilidades definidas en el artículo 8° del decreto 249 de 2004 de la gestión Pública, que apalancan la planeación, implementación y mejora del modelo de Seguridad y privacidad de la Entidad.
14. Definir un plan de concientización y sensibilización en los diferentes aspectos relacionados con seguridad y privacidad de la información para todos los colaboradores y terceros involucrados.
15. Realizar periódicamente la validación al cumplimiento de las políticas y lineamientos de seguridad y privacidad de la información por parte de los colaboradores.

Funcionarios, contratistas, proveedores de la Secretaria Distrital de Integración Social – SDIS son responsables de conocer, divulgar y dar cumplimiento a las Políticas de Seguridad y Privacidad de la Información, así como:

1. Implementar las Políticas de Seguridad y Privacidad de la Información de la Secretaria Distrital de Integración Social – SDIS en los procedimientos y actividades que apliquen a su trabajo, rol o función.
2. Reportar oportunamente cualquier evento e incidente de seguridad de la información que sospeche o detecte, de acuerdo con lo establecido en el procedimiento.
3. Llevar a cabo sus funciones u obligaciones, asegurando que sus acciones u omisiones no producen ningún incumplimiento al Sistema de Gestión de Seguridad de la Información.
4. Conocer y cumplir con las obligaciones y cláusulas en lo relacionado con confidencialidad y protección de datos personales.

Segregación de Funciones: Los funcionarios, contratistas y proveedores de la Secretaria Distrital de Integración Social – SDIS. que en ejercicio de sus funciones u obligaciones tengan acceso a la información, infraestructura tecnológica y/o a los sistemas de información, deben contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y privilegios establecidos sobre los activos de información y/o la información misma, con el fin de reducir y evitar el uso o modificación no autorizada sobre los activos de información de la Entidad.

Específicamente de acuerdo con los siguientes aspectos:

1. Los sistemas de información clasificados como críticos, con alta disponibilidad, deben incluir reglas de acceso que aseguren una adecuada segregación de funciones entre quien autorice, administre, opere, mantenga, audite y, en general, tenga la posibilidad de acceder a estos.
2. Los cambios o pasos a ambientes productivos solo podrán realizarse una vez sean aprobados por el área usuaria o solicitante del requerimiento a través de una gestión de cambios.
3. El nivel de súper usuario de los sistemas de información debe tener un control, que garantice una supervisión a las actividades realizadas por el administrador del sistema. Para tal efecto, se deben realizar verificaciones periódicas y aleatorias.
4. Las funciones de soporte técnico, planificación, desarrollo y operación deben estar claramente segregadas, así como distribuidos los ambientes de desarrollo, de pruebas y de producción, según corresponda.

Contacto con Autoridades: La Secretaria Distrital de Integración Social – SDIS a través de la Subdirección de Investigación e información -SII y los propietarios de sistemas o quien haga sus veces, deberá establecer y mantener una relación cercana con las entidades responsables de atender emergencias y desastres en cada territorio, zona o ubicación geográfica, así como con los grupos de interés y foros de especialistas en seguridad y privacidad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un incidente de seguridad y privacidad de la información que permita, entre otros:

1. Mejorar el conocimiento, implementar buenas prácticas y estar informado sobre la actualidad de la seguridad y privacidad de la información.
2. Recibir advertencias tempranas de alertas, avisos y parches acerca de ataques y vulnerabilidades.
3. Obtener acceso a herramientas y asesoría especializada en seguridad de la información.
4. Compartir e intercambiar información acerca de nuevas tecnologías, productos, amenazas o vulnerabilidades.
	1. Política de seguridad de la información en la gestión de proyectos.

* + 1. Objetivo:

Incluir la identificación de riesgos de seguridad de la información en la gestión de los proyectos de la Secretaria Distrital de Integración Social – SDIS de cualquier alcance.

* + 1. Responsable(s) de la ejecución de la política:
* Dirección de Análisis y diseño Estratégico
* Subdirección de Investigación e información -SII
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Líderes de procesos
* Apoyos a la supervisión de contratos.
* Todos los Funcionarios, contratistas, proveedores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.6.1.5 Seguridad de la información en la gestión de proyectos.

* + 1. Lineamientos:

La Subdirección de Investigación e información -SII y los propietarios de sistemas o quien haga sus veces como líderes de la gestión de proyectos deben establecer los lineamientos para la identificación y tratamiento de riesgos de seguridad de la información en todas las fases de los proyectos institucionales, de acuerdo con la metodología establecida por la Secretaria Distrital de Integración Social – SDIS definiendo los roles, responsabilidades y procedimientos necesarios para la gestión de estos.

* 1. Política de dispositivos móviles y trae tu propio dispositivo (BYOD)
		1. Objetivo:

Establecer 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).

* + 1. Responsable(s) de la ejecución de la política:
* Subdirección de Investigación e información -SII
* Dirección de análisis y diseño estratégico
* Dirección administrativa y financiera
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores la Secretaria Distrital de Integración Social – SDIS

* + 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.6.2.1 Política para dispositivos móviles
	+ 1. Lineamientos dispositivos móviles internos:
1. Para los dispositivos móviles asignados o autorizados tales como Tablet, celulares o computadores portátiles, se deberán implementar medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles y así asegurar que no se comprometa la información sensible la Secretaria Distrital de Integración Social – SDIS.
2. Los colaboradores que se encuentren autorizados para el uso de dispositivos móviles se comprometen a ejecutar los controles de seguridad definidos para proteger y asegurar de manera física y lógica el dispositivo, con el objeto de no poner en riesgo la información institucional.
3. Estas políticas deben ser conocidas y aplicadas por todos los colaboradores y partes interesadas que utilicen dispositivos móviles para el desarrollo de las actividades de la Entidad y su objetivo es garantizar la seguridad en uso de los dispositivos móviles de la misma.
4. Se debe llevar un registro de los dispositivos móviles autorizados para el uso dentro y fuera de la Entidad.
5. Garantizar las medidas de seguridad físicas de estos dispositivos cuando se dejan desatendidos; se deben resguardar en lugares bajo llave, y/o deben contar elementos de seguridad como con guayas para evitar su hurto o robo.
6. Todos los equipos móviles donde se gestione información institucional deben implementar un esquema de autenticación a través de contraseñas, códigos, patrones o biométricos, los cuales no pueden ser compartidos con otras personas.
7. Los dispositivos móviles de almacenamiento y procesamiento donde se gestione información institucional deben implementar una solución que permita la detección y eliminación de software malicioso.
8. La Subdirección de Investigación e información -SII y los propietarios de sistemas o quien haga sus veces deben implementar los mecanismos necesarios para restringir el uso dispositivos de almacenamiento USB como memorias, discos duros, SD, entre otros; en equipos de la entidad, estableciendo los procedimientos para las excepciones en caso de requerirse el uso de estos.
9. Los dispositivos móviles no deben almacenar la información institucional, sin la debida autorización del dueño del activo de información y sin la implementación de los controles de seguridad definidos para estos dispositivos.
10. En los casos que la entidad requiera almacenar información institucional en un dispositivo externo se deberá garantizar los controles de cifrados definidos por la Secretaria Distrital de Integración Social – SDIS.
11. Los colaboradores deberán informar a la mesa de ayuda y/o cualquier canal autorizado de reporte de incidentes de seguridad de la Entidad; la pérdida, robo, extravío del dispositivo móvil; de igual forma se deberá notificar cualquier comportamiento anómalo asociados con las funcionalidades de los dispositivos y/o activos de información almacenados.
12. Se debe garantizar el uso e instalación de software autorizado por la Entidad; en ninguna circunstancia los usuarios deben instalar software no autorizado en los dispositivos móviles. La entidad debe contar con una línea base estándar de software autorizado.
* Los dispositivos móviles de procesamiento y/o comunicación de propiedad de la Entidad deben estar integrados a una plataforma de administración MDM controlada por la Entidad, con el objetivo de implementar mecanismos de borrado remoto de la información.
* Los dispositivos móviles asignados por la Secretaria Distrital de Integración Social – SDIS tendrán la configuración de seguridad base definida por la Subdirección de Investigación e información -SII.
* Los equipos móviles de procesamiento deben encontrase actualizados en términos de seguridad de acuerdo con lo definido en el procedimiento de configuración base de seguridad, para estos dispositivos.
1. Los dispositivos móviles de propiedad de la Entidad tendrán únicamente la tarjeta SIM asignada por ésta y no deberán tener SIM o memorias adicionales de almacenamiento, las cuales permitan posibles fugas de información institucional.
2. Ante la pérdida o daño del equipo, se deberá informar de manera inmediata a la Mesa de ayuda y/o cualquier canal autorizado y proceder con el procedimiento administrativo por pérdida de elementos establecido por la Entidad.
3. Los usuarios que cuentan con equipos móviles asignados para el desarrollo de sus funciones no deberán tener los permisos para realizar cambios en la configuración, instalación/desinstalación de software posterior a su recibo.
4. Los usuarios de dispositivos móviles asignados por la Entidad evitarán hacer uso de estos en lugares de alto riesgo de robo o pérdida, evitando de esta manera pérdidas o fugas de información de la Entidad.
5. Se debe informar a los usuarios las medidas de seguridad a tener en cuenta sobre los dispositivos móviles institucionales en lugares públicos; ejemplo “no se deben conectar estos dispositivos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.)”.
* Los usuarios de dispositivos móviles institucionales y portátiles mantendrán desactivadas las funciones de redes inalámbricas Wifi, puertos infrarrojos, puerto Bluetooth en cualquier sitio fuera de las instalaciones de la Entidad. De igual forma los usuarios de dispositivos móviles institucionales y portátiles no deben hacer uso de redes inalámbricas públicas.
1. Los equipos deben contar con un borrado seguro antes de ser reasignados o dados de baja de la Entidad.
2. En el caso de presentar pérdida del dispositivo móvil, se deberá seguir el procedimiento de gestión de incidentes de la Secretaria Distrital de Integración Social – SDIS, con el objetivo de garantizar los controles correctivos definidos para ese tipo de incidente, ejemplo: bloqueo de los accesos a los sistemas de información, cambio de claves, borrado de información remota, entre otros, de igual forma el responsable del dispositivo deberá informar sobre la pérdida a la Dirección Administrativa y Financiera y a las autoridades competentes.
	* 1. Lineamientos dispositivos móviles externos:

En caso de utilizar dispositivos personales para el desarrollo de sus obligaciones o funciones, se tendrán en cuenta los siguientes lineamientos:

1. La Subdirección de Investigación e información -SII y los propietarios de sistemas o quien haga sus veces deben definir y aplicar las configuraciones de seguridad en los dispositivos personales de los funcionarios, contratistas o terceros a través de las conexiones de red establecidas para el acceso, almacenamiento generación y transmisión de la información.
2. Los dispositivos móviles autorizados deben contar como mínimo con el cumplimiento de los siguientes requisitos de seguridad:
* Software antivirus actualizado; donde se valide esquema de actualizaciones de firmas, módulos de seguridad activados y programación de escaneos periódicos.
* Garantizar que los dispositivos estén protegidos con contraseñas o patrones de bloqueo, se recomienda activar múltiple factor de autenticación (MFA).
* Es responsabilidad del dueño tomar nota del IMEI en los casos que aplique para solicitar su anulación en caso de pérdida.
* Los dueños de los dispositivos móviles aceptan los controles definidos dentro de sus dispositivos, en los cuales la Entidad ante pérdida o venta de estos, pueda ejecutar acciones de mitigación de riesgos asociados, sobre la información contenida y de propiedad de la Secretaria Distrital de Integración Social – SDIS en estos dispositivos.
* Cuando los dispositivos móviles se utilicen por fuera de las instalaciones de la Entidad, no deben permanecer desatendidos y sin protecciones.
* La entidad deberá disponer de entrenamiento o sensibilización para el personal que usa dispositivos móviles, para incrementar el nivel de concientización sobre los riesgos adicionales que resultan de este tipo de trabajo, y los controles que se deberían implementar todos los colaboradores.
	1. Política de teletrabajo, trabajo en casa o trabajo remoto
		1. Objetivo

Garantizar la seguridad de toda la información y los recursos gestionados cuando se realiza el teletrabajo concientizando a todos los colaboradores, funcionarios, contratistas y proveedores de la importancia de cumplir las medidas de seguridad tanto dentro como fuera de la oficina para garantizar y preservar la confidencialidad, la integridad y la disponibilidad de los activos de información que es accedida, procesada o almacenada a través de la modalidad de teletrabajo, trabajo en casa o trabajo remoto basados en los lineamientos y medidas de soporte para proteger la información.

* + 1. Responsable(s) de la ejecución de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores la Secretaria Distrital de Integración Social – SDIS
* Funcionarios y Contratistas
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.6.2.2 Teletrabajo
	+ 1. Lineamientos:
			1. La Subdirección de Investigación e información -SII junto con la Subdirección de Gestión y Desarrollo del Talento Humano, personal de planta, provisional, contratistas y con los supervisores de contratos; desarrollarán y establecerán los respectivos protocolos de monitoreo sobre las actividades que desarrollan 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 el aplique de acuerdo con la relación contractual o laboral.
			2. El líder del teletrabajador o supervisor del contratista; definirá la información a acceder, aplicaciones, sistemas de información o servicios de la Entidad que se utilizarán para la ejecución de las labores u obligaciones durante el teletrabajo o trabajo en casa o trabajo remoto según corresponda.
			3. La entidad debe realizar verificaciones periódicas del cumplimiento de la política de seguridad y controles asociados al teletrabajo, trabajo en casa o trabajo remoto.
			4. En caso de requerirse conexión remota la Subdirección de Investigación e información -SII debe garantizar el uso de las conexiones VPN “Client to Site” y canales seguros para el acceso, procesamiento, almacenamiento y transporte de los datos.
			5. No se deben realizar conexiones remotas desde sitios como cafés internet o similares consideradas redes públicas y/o no seguras.
			6. Los dispositivos usados para el teletrabajo, trabajo en casa o trabajo remoto deben tener un antivirus actualizado, sistema operativo licenciado y con las actualizaciones, en caso contrario y de manera preventiva se podrá denegar o inhabilitar la conexión remota a los servicios provistos por la Secretaria Distrital de Integración Social – SDIS.
			7. Se debe garantizar por parte de los colaboradores que toda la información generada debe almacenarse en los repositorios autorizados por la Secretaria Distrital de Integración Social – SDIS en caso de ser almacenado en el dispositivo móvil personal se traslada toda responsabilidad frente a los controles de acceso, respaldo, criptografía y demás controles indicados por la Entidad para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en el dispositivo.
			8. Todos los colaboradores en teletrabajo, trabajo en casa o trabajo remoto deben informar las posibles anomalías en los dispositivos institucionales o en la información, así como eventos o incidentes de forma inmediata y seguir los lineamientos para la gestión de incidentes de seguridad de la información.
			9. Todos los colaboradores deberán acogerse y dar cumplimiento a las políticas y controles definidos para el cumplimiento del teletrabajo, trabajo en casa o trabajo remoto.
	1. Política de seguridad del recurso humano
		1. Objetivo(s):
* Asegurar que los colaboradores y terceros comprenden sus responsabilidades y que son idóneos en los roles para los que se consideran.
* Asegurar que los colaboradores y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
* Proteger los intereses de la organización como parte del proceso de cambio de roles o terminación de empleo.
	+ 1. Responsable(s) de la ejecución de la política:
* Dirección de Gestión Corporativa.
* Subdirección de Gestión y Desarrollo del Talento Humano
* Funcionarios y Contratistas
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.7.1.1 Selección
* A.7.1.2 Términos y condiciones del empleo
* A.7.2.1 Responsabilidades de la dirección
* A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información.
* A.7.2.3 Proceso disciplinario
* A.7.3.1 Terminación o cambio de responsabilidades de empleo.
	+ 1. Lineamientos:

La Subdirección de Gestión y Desarrollo del Talento Humano o quien haga de sus veces:

1. Debe establecer y verificar los antecedentes en cumplimiento de los requisitos legales, reglamentarios e internos de todos los candidatos que se pretendan tener una relación contractual o laboral.
2. Definir una lista de verificación que contengan los aspectos necesarios para la revisión de los antecedentes y documentos del personal a vincular de acuerdo con lo que dicta la ley o la reglamentación relacionada y reposar dicha lista y soportes en la carpeta contractual para los contratista u hoja de vida para el personal de planta.
3. Definir los términos y condiciones en materia de seguridad y privacidad de la información teniendo en cuenta las leyes de propiedad intelectual, protección de datos personales y transparencia y acceso a la información pública.
4. Solicitar a los funcionarios y contratistas la firma de acuerdos de confidencialidad y no divulgación de la información institucional.
5. Incluir en la inducción y reducción los temas de seguridad y privacidad de la información.
6. Establecer la documentación y entregables requeridos para la desvinculación de los funcionarios.
7. Informar a la gestión de soporte y mantenimiento tecnológico o quien haga sus veces, las novedades del personal que no se encuentren en servicio activo por diferentes causas y por un periodo superior a 5 días hábiles, una vez éstas hayan sido formalmente establecidas.
8. Para el adecuado cumplimiento de sus funciones u obligaciones, es necesario que se comuniquen los términos y condiciones respecto a la seguridad de la información desde el momento de su vinculación.
9. Los acuerdos contractuales o laborales con los colaboradores deben establecer sus responsabilidades y las de la Secretaria Distrital de Integración Social – SDIS en cuanto a la seguridad de la información, incluyendo acuerdos o cláusulas de confidencialidad sobre la información clasificada o reservada a la que pueda conocer o tener acceso y las responsabilidades sobre el tratamiento de los datos personales.
10. Debe definir y ejecutar un plan de cultura enfocado a la toma de conciencia sobre los deberes y responsabilidades de seguridad de la información y su cumplimiento, así como las actualizaciones regulares sobre las políticas y procedimientos de la Secretaria Distrital de Integración Social – SDIS pertinentes para su cargo o relación contractual.
11. Indicar las responsabilidades y los deberes de seguridad y privacidad de la información que permanecen válidos frente a cambios de funciones, cambios de empleo, finalización de contrato, desvinculación o retiro; actividades que se harán de forma ordenada, controlada y segura, tanto para servidores públicos como contratistas.
12. Comunicar a todos los colaboradores sobre las consecuencias ante el incumplimiento de las políticas de seguridad y privacidad de la información por parte de los funcionarios, contratistas o terceros, la entidad deberá realizar las acciones pertinentes para documentar la situación y escalar a las autoridades competentes en caso de ser necesario.
13. Incluir en los contratos de prestación de servicios; obligaciones referentes a las políticas, lineamientos y directrices en materia de seguridad y privacidad de la información.
14. Informar oportunamente a la mesa de ayuda o quien haga sus veces, las novedades de suspensión y/o terminación de contratos.
15. Debe asignar y promover el uso del carné institucional para todos los funcionarios, contratistas y terceros, utilizándolo en un lugar visible mientras permanezca en las instalaciones de la Secretaria Distrital de Integración Social – SDIS o cuando se encuentre en representación de la Entidad en otros sitios.
16. Adelantar las acciones a los funcionarios públicos que incumplan las políticas y procedimientos de seguridad y privacidad de la información de la Secretaria Distrital de Integración Social – SDIS y llevar a cabo los procesos disciplinarios correspondientes, de conformidad con lo establecido en la ley, particularmente en el Código Único Disciplinario (Ley 734 de 2002 - Ley 1952 de 2019), el Estatuto Anticorrupción (Ley 1474 de 2011) y demás normas que las adicionen, modifiquen, reglamenten o complementen.
17. Indicar al supervisor del contrato o a quien este delegue, la responsabilidad de:
* Consolidar la información de la Secretaria Distrital de Integración Social – SDIS de los contratistas en caso de terminación o cesión del contrato, retiro, investigación, inhabilidades o cambio de obligaciones.
* Informar las novedades de personal que supervisa tan pronto sean conocidas, con el fin de inhabilitar los accesos físicos y lógicos que se tenían en caso de que se requiera.
* Solicitar al área de Infraestructura o quien haga sus veces, una copia de respaldo de la información que tuviera a cargo una vez termine la relación contractual.
* Establecer la documentación y entregables requeridos para la desvinculación de los contratistas de prestación de servicios de acuerdo con los lineamientos de la Secretaria General.

Todos los Funcionarios, Contratistas o proveedores de la Secretaria Distrital de Integración Social – SDIS:

Deben asistir a las sensibilizaciones, entrenamientos, capacitaciones y eventos a los cuales sean convocados como parte del plan de concientización y sensibilización en seguridad de la información.

Abstenerse de divulgar información Pública Clasifica y Pública Reservada de la Entidad, de manera escrita o verbal; de la misma manera, aplica para situaciones donde la revelación de información pueda causar un impacto operativo o repercusiones legales para la Secretaria Distrital de Integración Social – SDIS.

Los supervisores de contrato:

Todos los supervisores de contratos deben informar a los subdirectores, oficial de seguridad o la gestión de soporte y mantenimiento tecnológico, el incumplimiento de las políticas y procedimientos de seguridad y privacidad de la información de la Secretaria Distrital de Integración Social – SDIS, por parte suya o de sus contratistas a cargo.

* 1. Política de gestión de activos
		1. Objetivo(s):
* Identificar los activos de información y definir las responsabilidades de protección apropiadas
* Propender por que la información reciba un nivel apropiado de protección, de acuerdo con su importancia para la Entidad
* Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios removibles
	+ 1. Responsable(s) de la ejecución de la política:
* Subdirección de Investigación e información -SII
* Gestión de soporte y mantenimiento tecnológico
* Tecnologías de la Información
* Infraestructura
* Subdirección Administrativa y financiera
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.8.1.1 Inventario de activos.
* A.8.1.2 Propiedad de los activos.
* A.8.1.3 Uso aceptable de los activos.
* A.8.1.4 Devolución de activos.
* A.8.2.1 Clasificación de la información.
* A.8.2.2 Etiquetado de la información.
* A.8.2.3 Manejo de activos.
* A.8.3.1 Gestión de medios removibles.
* A.8.3.2 Disposición de los medios.
* A.8.3.3 Transferencia de medios físicos.
	+ 1. Lineamientos:

La Subdirección de Investigación e información -SII o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

1. 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 proporcionan a los funcionarios y contratistas para cumplir con los propósitos institucionales.
2. 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.
3. Entregar a los colaboradores los dispositivos informáticos y programas instalados en ellos para el desarrollo de sus funciones.
4. Custodiar todos los medios magnéticos y/o electrónicos de los softwares adquiridos, sus respectivos manuales y licencias de uso; por lo cual se debe dar el adecuado tratamiento de acuerdo con su nivel de clasificación.
5. Antes de destruir o eliminar de manera segura la información o un medio de almacenamiento de información se debe realizar la respectiva copia de respaldo de acuerdo con el procedimiento establecido.
6. Establecer los lineamientos para el borrado seguro de la información institucional, teniendo en cuenta las herramientas de software a utilizar, los responsables de las actividades, las causas por los cuales debe realizarse el borrado seguro de la información, entre otros.
7. Asegurar que cuando cambien de propósito, sean devueltos por garantía, o termine la vida útil de los dispositivos tecnológicos y/o equipos de cómputo, la información Institucional que haya sido almacenada y procesada en estos sea borrada, eliminada y destruida de forma segura.
8. Realizar la valoración de los riesgos para determinar qué elementos deberían destruirse físicamente antes de desecharlos, de acuerdo con el procedimiento de manejo de residuos electrónicos (RAEE), al considerarse que los medios han cumplido su vida útil.
9. Verificar que los equipos de cómputo (portátiles, de escritorio, servidores) no contengan el medio de almacenamiento antes de su disposición final; en caso de tenerlo se debe garantizar que se ejecutaron las actividades de acuerdo con el procedimiento de borrado seguro, usando técnicas para hacer que la información original no sea recuperable.
10. Definir lineamientos para el transporte seguro de medios que contienen información institucional evitando el acceso no autorizado y/o uso indebido.
11. Implementar en las herramientas tecnológicas los lineamientos establecidos para el etiquetado de la información de la Entidad.
12. Para los equipos de cómputo que tienen autorizado el manejo de medios extraíbles tales como Tarjetas de memoria USB, SD, discos duros externos y unidades reproductoras de CD/DVD, deben cumplir mínimo con los siguientes requisitos:
	* Tener habilitado el escaneo automático de virus.
	* Tener configurado el bloqueo de la reproducción automática de archivos ejecutables a través del antivirus o por otro medio.
	* Los dispositivos de almacenamiento de información de propiedad de la Secretaria Distrital de Integración Social – SDIS se constituyen en un activo de información, por lo tanto, el ingreso, uso, movilización y salida debe realizarse siguiendo los lineamientos para este fin.
13. Debe verificar y monitorear que la información que transita a través de la red cuente con los protocolos de seguridad necesarios, asegurando su confidencialidad, disponibilidad e integridad.
14. Debe implementar la utilización de protocolos de seguridad para el cifrado de los datos.

El Grupo de Gestión Documental de la Secretaria General o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

* + - 1. Definir, implementar, monitorear y socializar los lineamientos para el etiquetado de la información física, electrónica y digital de la Entidad con el apoyo del equipo de seguridad de la información y la Dirección de Investigación e Innovación.

Los funcionarios y contratistas deben dar cumplimiento a los siguientes lineamientos:

1. Los activos de información son de propiedad de la Secretaria Distrital de Integración Social – SDIS y el uso de éstos debe ser exclusivamente con propósitos laborales.
2. Los activos de información serán tratados de acuerdo con su nivel de clasificación indicado por los propietarios de los activos de información.
3. Deben usar únicamente los programas y dispositivos autorizados por la Subdirección de Investigación e información -SII.
4. Está prohibido almacenar información de uso personal en los equipos de cómputo o portátiles asignados para el desarrollo de sus funciones u obligaciones.
5. Todos los requerimientos relacionados con: aplicativos, sistemas de información y/o equipos de cómputo, serán solicitados por los lideres de proceso, Director o Subdirector a través de la Mesa de ayuda y/o cualquier canal autorizado para tal fin.
6. La cuenta de correo electrónico debe ser usada para el desempeño de las funciones u obligaciones asignadas por la Secretaria Distrital de Integración Social – SDIS.
7. Está prohibido el envío de información confidencial sin la aplicación previa de los controles de seguridad para salvaguardar la información y/o sin la autorización de los propietarios respectivos de los activos de información.
8. Está prohibido el uso de herramientas de mensajería instantánea no autorizadas por Subdirección de Investigación e información -SII, empleadas para el envío y/o recepción de información pública clasificada y/o pública reservada de la Secretaria Distrital de Integración Social – SDIS.
9. El uso de Internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información.
10. Cuando sea requerido y con la debida autorización y aprobación del responsable del activo, se debe generar un requerimiento de borrado seguro de información, a través de los canales autorizados de la Secretaria Distrital de Integración Social – SDIS.
11. La entidad debe registrar la disposición de los elementos críticos, sea “Información Pública Reservada, Información Pública Clasificada”, y/o medios que la contienen, con el fin de mantener un rastro de auditoría.
12. Devolver los activos de información una vez finalice la vinculación laboral o contractual con la Secretaria Distrital de Integración Social – SDIS.
13. En el momento de un cambio funcional o de empleo, retiro y/o terminación de otros tipos de vinculación, deben realizar la entrega de su puesto de trabajo al Director, Subdirector, o líder de procesos o a quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados durante su permanencia en la Entidad.
14. Luego de escanear, fotocopiar o utilizar un medio reprográfico debe asegurarse de no dejar documentos en los equipos utilizados.
15. Recoger de las impresoras, escáneres, fotocopiadoras y/o medios reprográficos, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.
16. Asegurarse que los documentos y medios de almacenamiento que contengan información sensible no queden de forma desprotegida en el momento de ausentarse de su puesto de trabajo.

Los propietarios de los activos deben dar cumplimiento a los siguientes lineamientos:

1. Establecer los controles durante todo el ciclo de vida del activo de información, teniendo en cuenta la criticidad asignada e informar al SGSI cualquier situación que ponga en riesgo la confidencialidad, integridad, disponibilidad y/o privacidad, alineados con los requerimientos de la Secretaria Distrital de Integración Social – SDIS.
* Promover el uso y gestión adecuado de los activos de información.
* Definir y revisar periódicamente los usuarios, permisos, restricciones, clasificaciones y perfiles de acceso a los activos de información, teniendo en cuenta las políticas de control de acceso aplicables.
* Informar a los colaboradores y terceros que usan o tiene acceso a los activos de información de la entidad, los requisitos de seguridad de la información, los cuales deben ser responsables del uso y abuso que realicen.
* Monitorear periódicamente las actividades que se realizan en los activos de información por parte de los colaboradores y terceros que tienen accesos a los mismos.

Los custodios de los activos deben dar cumplimiento a los siguientes lineamientos:

1. Implementar los controles definidos por el propietario del activo durante todo el ciclo de vida del activo de información.
* Promover el uso y gestión adecuado de los activos de información.
* Monitorear periódicamente los usuarios, permisos, restricciones, clasificaciones y perfiles de acceso a los activos de información, teniendo en cuenta las políticas de control de acceso aplicables.
* Apoyar en el monitoreo de las actividades que se realizan en los activos de información por parte de los colaboradores y terceros que tienen accesos a los mismos.

Los (Directores, Subdirectores y Lideres de Proceso) deben dar cumplimiento a los siguientes lineamientos:

1. Los líderes de procesos son los propietarios de los activos de información, ejerciendo así la facultad de aprobar o revocar el acceso al activo, asignar controles, asignar custodios, clasificarlos, entre otros.
2. Identificar y mantener actualizado el Registro de Activos de Información para los procesos que lideran.
3. Los activos de información contenido en el inventario son propiedad de cada líder de proceso por lo cual deben protegerlos aplicando los controles necesarios para mantener la confidencialidad, integridad, disponibilidad y privacidad de la información
4. Clasificar los activos de información de acuerdo con la Ley 1712 de 2014 o aquella que la sustituta, derogue o adicione.
	1. Política de control de acceso
		1. Objetivo(s):
* Gestionar el acceso a información e instalaciones de procesamiento de información.
* Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
* Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
* Evitar el acceso no autorizado a sistemas y aplicaciones
	+ 1. Responsable(s) de la ejecución de la política:
* Gestión de soporte y mantenimiento tecnológico
* Subdirección de Investigación e información -SII
* Infraestructura
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.9.1.1 Política de control de acceso.
* A.9.1.2 Acceso a redes y a servicios en red.
* A.9.2.1 Registro y cancelación del registro de usuarios
* A.9.2.2 Suministro de acceso de usuarios
* A.9.2.3 Gestión de derechos de acceso privilegiado
* A.9.2.4 Gestión de información de autenticación secreta de usuarios
* A.9.2.5 Revisión de los derechos de acceso de usuarios
* A.9.2.6 Retiro o ajuste de los derechos de acceso
* A.9.3.1 Uso de información de autenticación secreta.
* A.9.4.1 Restricción de acceso a la información.
* A.9.4.2 Procedimiento de ingreso seguro.
* A.9.4.3 Sistema de gestión de contraseñas.
* A.9.4.4 Uso de programas utilitarios privilegiados.
* A.9.4.5 Control de acceso a códigos fuente de programas.
	+ 1. Lineamientos:

Esta política tiene como objetivo preservar 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, se establecen 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, teniendo en cuenta lo siguiente:

El área de tecnología, gestión de soporte y mantenimiento tecnológico o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

1. Debe garantizar entornos con controles de acceso idóneos, los cuales aseguren el perímetro, tanto en la Dirección General como las diferentes sedes o dependencias de la entidad, así como en entornos abiertos para evitar el acceso no autorizado a ellos.
2. Debe controlar las amenazas físicas externas y proveer las condiciones medioambientales requeridas para el funcionamiento de la plataforma tecnológica y para la preservación de sus activos de información digitales y físicos.
3. Garantizar que las redes sean debidamente protegidas contra accesos no autorizados por medio de mecanismos de control de acceso lógico para lo cual deberá:
	* Establecer un procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red de la entidad.
	* Asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.
	* Establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes a las redes o recursos de red la Secretaria Distrital de Integración Social – SDIS, así como divulgar y hacer cumplir las Políticas de Seguridad y Privacidad de la Información.
	* Suministrar una herramienta para realizar conexiones remotas a la red de área local de la entidad de manera segura para todo el personal de la Secretaria Distrital de Integración Social – SDIS y terceros que por su labor así lo requiera, la cual debe ser aprobada, registrada y auditada.
4. El acceso a la Información, sistemas de información y/o aplicaciones de la entidad por parte de los funcionarios, contratistas y terceros debe darse bajo el principio del mínimo privilegio; quiere decir que cada usuario solo debe tener acceso a lo que necesita conocer de acuerdo con sus actividades y rol dentro de la entidad.
5. Definir un procedimiento de Gestión de accesos el cual debe contemplar como mínimo los mecanismos para la solicitud, creación, inhabilitación, suspensión y reactivación de los derechos de acceso, responsables de las solicitudes de accesos, revisiones periódicas de los usuarios y privilegios de acceso, manejo de roles con privilegios de administración sobre los sistemas de información de la entidad, entre otros.
6. Semestralmente de manera aleatoria se deberá realizar una validación de los privilegios y usuarios de acceso de los funcionarios, proveedores y/o terceros sobre la información, aplicaciones y demás servicios de acceso que posea la entidad, además, verificar que los usuarios habilitados cuenten con los permisos y privilegios de acuerdo con sus funciones u obligaciones actuales.
7. Todas las solicitudes de acceso (creación, modificación, bloqueo, inactivación y/o eliminación) a los servicios de red, aplicaciones, información; deben ser solicitadas por los Directores, Secretaria General, subdirectores y lideres de procesos, de acuerdo con las funciones u obligaciones del colaborador.
8. El propietario de los sistemas de información o servicios debe autorizar o denegar el acceso y privilegios requeridos.
9. Los encargados de la administración o gestión de los servicios tecnológicos, sistemas de información e infraestructura, deben definir los mecanismos de acceso a través de roles, perfiles de usuario y segregación de funciones o roles, teniendo en cuenta los niveles de seguridad y clasificación de la información.
10. El acceso a los servicios de red, sistemas de información y aplicaciones de la entidad debe hacerse a través de la autenticación de los usuarios asignados a cada funcionario, contratista y/o tercero (usuario y contraseña) como primera opción del directorio activo, con la cual se garantice la trazabilidad de las acciones que realizan los usuarios.
11. Todas las contraseñas deberán ser tratadas como información pública clasificada, y son de uso personal e intransferible, no se deberán compartir con ninguna persona dentro o fuera de la entidad por ningún medio.
12. Los colaboradores son responsables de la custodia, no divulgación y uso de estas.
13. Ningún usuario podrá acceder un sistema utilizando la cuenta o contraseña de otro usuario.
14. No está permitido almacenar en los navegadores de internet u otros sistemas las credenciales de acceso para ser recordada automáticamente por estos.
15. Asegurarse de que las contraseñas no se encuentren de forma legible en cualquier medio impreso o digital ni dejarlos en un lugar donde personas no autorizadas puedan identificarlos.
16. Utilizar diferentes contraseñas para acceso a los diferentes sistemas de información y servicios institucionales.
17. En caso de ser divulgada la contraseña por error, esta debe ser cambiada de inmediato y se debe reportar el incidente de seguridad de la información de acuerdo con los procedimientos definidos por la Secretaria Distrital de Integración Social – SDIS.
18. Realizar su cambio de contraseña exclusivamente en la plataforma destinada para tal fin. No se podrán modificar por ningún otro medio.
19. Para la creación de la contraseña se debe tener en cuenta:
* No debe utilizar palabras comunes, ni nombres de fácil deducción por terceros, no vincule sus contraseñas con sus datos personales o familiares como fechas de cumpleaños, números de teléfono, números de documento, nombres familiares o de mascotas, entre otros.
* No usar secuencias básicas de teclado (por ejemplo: qwerty, asdf o numeración secuencial 123456789, 987654321).
* No utilizar como contraseña el mismo nombre de usuario.
1. Todas las contraseñas de acceso a los sistemas de información y servicios de la entidad deben cumplir con la siguiente política.
* Longitud mínima de contraseña de diez (10) caracteres.
* La contraseña debe tener al menos una (1) letra del alfabeto latino en mayúscula (A - Z).
* La contraseña debe tener al menos una (1) letra del alfabeto latino en minúscula (a - z).
* La contraseña debe tener al menos un (1) dígito en base decimal (0 - 9).
* La contraseña debe tener al menos un (1) carácter no alfanumérico, como símbolos de exclamación, (¡!), de peso ($), o de almohadilla (#), etc.
1. Los sistemas de información de la Secretaria Distrital de Integración Social – SDIS deben obligar automáticamente a que las contraseñas de las cuentas de usuarios se cambien al menos una vez cada tres (3) meses.
2. El sistema controlará el tiempo de inactividad del usuario y bloqueará la sesión automáticamente después de cinco (5) minutos.
3. Las contraseñas no se deben digitar en texto claro por ningún medio, el usuario debe validar una conexión segura antes de digitar las credenciales de acceso.
4. Cuando se realice la creación de un usuario en un sistema, el administrador puede asignar una contraseña inicial, pero el sistema automáticamente debe solicitar cambio de esta al titular de la cuenta cuando se realice el primer acceso.
5. Garantizar que las contraseñas o claves de Administrador de los diferentes sistemas sean cambiadas con una periodicidad de sesenta (60) días como máximo.
6. Garantizar que el número de sesiones concurrentes de un mismo usuario sea limitado.
7. Garantizar que el usuario sea usado en el equipo que fue asignado respectivamente.
8. Al ingresar cinco (5) intentos fallidos de contraseña en los sistemas de información, se bloqueará el usuario y se deberá gestionar el desbloqueo con base a la validación de la identidad del usuario.
9. Establecer mecanismos para que las contraseñas o claves no sean iguales al nombre de usuario o cualquier variación (al revés, mayúsculas, etc.), alias o sobrenombre de la persona.
10. Proporcionar los mecanismos necesarios para que los funcionarios, contratistas y terceros que olviden, bloqueen o extravíen su contraseña, puedan restablecerla de forma segura.
11. Los funcionarios, contratistas y terceros deben recibir junto con el nombre de usuario una contraseña o clave para acceder a los recursos informáticos de la Entidad, la cual es de cambio obligatorio en el primer uso, garantizando así su responsabilidad y único conocimiento sobre la misma.
12. Implementar en las aplicaciones o servicios que sea posible, la autenticación por único inicio de sesión (single sign on) integrado al directorio activo.
13. Se debe contar con autenticación (preferiblemente doble o triple factor) para acceso a los servicios tecnológicos, sistemas de información e infraestructura de la Secretaria Distrital de Integración Social – SDIS
14. Los accesos lógicos asignados a los colaboradores serán desactivados una vez terminada su vinculación contractual o laboral con la Entidad, por lo que el supervisor o líder inmediato es el responsable de reportar oportunamente cualquier novedad.
15. Se debe suspender el acceso lógico a los sistemas de información, infraestructura y servicios tecnológicos a los colaboradores que no se encuentren en servicio activo por diferentes causas y por un periodo superior a cinco (5) días hábiles, esta novedad debe ser reportada oportunamente por el supervisor o líder inmediato.
16. Todas las partes interesadas deberán conocer los lineamientos y aplicar los controles establecidos con el fin de evitar accesos no autorizados, pérdidas y/o utilización indebida de los activos de información.
17. Definir los lineamientos para las características que deben contener las contraseñas que se aplicarán sobre la plataforma tecnológica, los servicios de red y los sistemas de información.

Gestión de Acceso para Usuarios Privilegiados:

1. La asignación de privilegios especiales debe ser revisado y autorizado por el jefe directo del funcionario o supervisor para el caso de contratistas, y deberá quedar registrado todo el proceso de solicitud y autorización en la herramienta de gestión.
2. Todos los usuarios privilegiados deberán tener habilitado el log de acceso y transacciones en todos los sistemas de información, dispositivos de red, comunicaciones, dispositivos de seguridad y/o cualquier recurso o servicio tecnológico que sea accedido.
3. Garantizar que todas las contraseñas de los usuarios y/o sistemas de información conocidas por el usuario privilegiado sean actualizadas inmediatamente después del retiro y/o movimiento de área del funcionario, contratista y/o tercero.
4. No se deberán realizar accesos con super usuarios (ROOT, administrador, etc.). Estos accesos deben ser autorizados únicamente cuando sean requeridos por fuerza mayor.
5. El área de Subdirección de Investigación e información -SII o quien haga sus veces deberá custodiar las contraseñas que se utilizan para descargar el software de fabricantes de sus páginas web o sitios en internet y las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos.
6. Toda contraseña por defecto o suministrada por algún fabricante o sistema deberá ser reemplazada.
7. Configurar la restricción para no reutilizar hasta cinco (5) contraseñas ya empleadas anteriormente para todos los colaboradores.
8. Para la creación de la contraseña para los administradores o usuarios privilegiados se debe tener en cuenta:
	1. No debe utilizar palabras comunes, ni nombres de fácil deducción por terceros, no vincule sus contraseñas con sus datos personales o familiares como fechas de cumpleaños, números de teléfono, números de documento, nombres familiares o de mascotas, entre otros.
	2. No usar secuencias básicas de teclado (por ejemplo: *qwerty*, *asdf* o numeración secuencial *123456789*, *987654321*).
	3. No utilizar como contraseña el mismo nombre de usuario.
	4. La longitud mínima de la contraseña deberá ser de catorce (14) caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales.
9. Las contraseñas de los administradores deberán ser almacenadas en un lugar seguro y en sobre sellado o en un sistema de gestión de contraseñas institucional. Así mismo, el acceso a éstas, en el evento de requerirse, debe ser en conjunto o con aprobación explícita del líder inmediato. Una vez revelada dicha contraseña, la misma deberá ser cambiada y puesta de nuevo en el lugar seguro designado. Si esta es un activo de información critico o de alto impacto la autorización debe ser analizada y aprobada en conjunto con el CISO y el Subdirector de investigación e investigación.
10. Si el sistema de información o aplicativo contiene la funcionalidad de cambio de contraseña obligatoria en su primer inicio de sesión, puede ser entregada a través de alguna herramienta colaborativa institucional, de lo contrario la contraseña deberá ser entregada de forma personal o telefónicamente.
11. Todas las contraseñas deben estar cifradas durante el transporte, comunicación y almacenamiento.

Inicio de sesión seguro:

1. Asegurarse que el acceso a los servicios de información solo sea posible con un proceso de conexión segura.
2. Implementar los controles necesarios para proteger los servicios de información de intentos de inicio de sesión mediante ataques de fuerza bruta.
3. Generar mensajes de advertencia general indicando que solo los usuarios autorizados pueden acceder al equipo de cómputo.
4. Validar la información de ingreso a los servicios tecnológicos solamente al completar todos los datos de entrada. Si presenta una condición de error, el sistema no debe indicar qué parte de los datos es correcta o incorrecta.
5. Habilitar el registro de los intentos exitosos y fallidos de acuerdo con los perfiles de los usuarios en los sistemas de información necesarios.
6. Garantizar la transmisión segura de contraseñas sobre la red.
7. Asegurar la terminación de sesiones inactivas después de un período de inactividad de cinco minutos, teniendo especial cuidado con lugares de alto riesgo, tales como áreas públicas o externas por fuera de la organización o en dispositivos móviles.

Control de acceso a códigos fuentes de aplicaciones:

1. Implementar los controles necesarios para asegurar que el acceso al código fuente de los aplicativos desarrollados (sistemas de información) sea limitado. Solamente el personal autorizado podrá contar con acceso a esta información y hará un uso moderado de la misma.
2. Proporcionar las herramientas necesarias para realizar control de cambios sobre el código fuente de los aplicativos desarrollados por la misma, las cuales permitirán retroceder a una versión anterior del código.
3. Es el responsable por la aprobación, supervisión y modificación de los códigos fuente de los aplicativos.

Todo funcionario, contratista de la SDIS y/o proveedores externos contratista deben cumplir los requisitos o controles de autenticación, para el caso de equipos de cómputo personales cuando estos accedan a la red de datos de la Entidad solamente podrán utilizarlas para las tareas autorizadas.

1. Gestionar la autorización para realizar una conexión remota a equipos conectados a la red interna desde fuera de la misma.
2. Los usuarios de los recursos tecnológicos y de los sistemas de información, realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual se les ha permitido el acceso.
3. Deben hacerse responsables de las acciones realizadas en la plataforma tecnológica, los servicios de red y los sistemas de información de la entidad, así como del usuario y contraseña asignados para el acceso a estos.
4. Ninguna persona debe compartir sus cuentas de usuario y contraseñas asignados para el ingreso a los servicios de red y los sistemas de información con otros miembros de la entidad o terceros.
5. Dar cumplimiento a los lineamientos establecidos para la gestión de contraseñas, requeridas para el acceso a la plataforma tecnológica, los servicios de red y los sistemas de información que la entidad provee.
6. Proteger la confidencialidad del usuario de acceso o de identificación asignado para acceder a los recursos, servicios y/o sistemas de información, el cual deberá ser de uso personal e intransferible, razón por la cual no deben ser compartidos con otros funcionarios, contratistas o terceros.
7. Son responsables de todas las acciones que se lleven a cabo con las credenciales que le sean asignadas para el desarrollo de sus funciones u obligaciones con la Secretaria Distrital de Integración Social – SDIS
8. Procurar la integridad, la confidencialidad y la disponibilidad de los activos de información de los cuales son propietarios/responsables/custodios, asegurándose que éstos sólo sean utilizados para el desarrollo de las labores encomendadas. En caso de observar posibles eventos e incidentes que afecten la seguridad de la información, los mismos se deben reportar de manera oportuna de acuerdo con los procedimientos establecidos.
9. Todos los funcionarios, contratistas y terceros deberán autenticarse a través de los mecanismos de control de acceso provistos por tecnología, gestión de soporte y mantenimiento tecnológico o quien haga sus veces, antes de poder usar la infraestructura tecnológica de la Entidad.
10. No deben proporcionar información de los mecanismos de control de acceso en las instalaciones e infraestructura tecnológica de la Entidad a personal externo, a menos que se tenga el visto bueno del propietario de la información y de su jefe inmediato.
11. Deben contar con un identificador de usuario (ID) único, personalizado e intransferible para acceder a la infraestructura tecnológica de la entidad.

* 1. Política de criptografía
		1. Objetivo:

Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información.

* + 1. Responsable(s) de la ejecución de la política:
* Tecnologías de la información
* Gestión de soporte y mantenimiento tecnológico
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A
* A.10.1.1 Política sobre el uso de controles criptográficos.
* A.10.1.2 Gestión de llaves.
	+ 1. Lineamientos:

La Subdirección de Investigación e información -SII o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

1. La Secretaria Distrital de Integración Social – SDIS deberá usar e implementar controles criptográficos para proteger la confidencialidad, autenticidad o integridad de la información clasificada de la Entidad al momento de almacenarse o transmitirse.
2. Proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información clasificada de forma interna o externa se realice de forma segura.
3. La información pública reservada y pública clasificada debe almacenarse en repositorios cifrados de acuerdo con sus niveles de confidencialidad e integridad.
4. Se debe disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red de la Secretaria Distrital de Integración Social – SDIS o recursos de la entidad.
5. Todas las llaves criptográficas de la Entidad deben estar resguardadas por los responsables y custodios protegiendo su confidencialidad, integridad y disponibilidad.
6. La administración de llaves criptográficas y certificados digitales estarán a cargo de tecnología, gestión de soporte y mantenimiento tecnológico o quien haga sus veces.
7. Establecer mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.
8. Las llaves criptográficas serán deshabilitadas por tecnología, gestión de soporte y mantenimiento tecnológico o quien haga sus veces, cuando estas se encuentren en riesgo de divulgación o cuando los colaboradores de la Entidad autorizados culminen la relación laboral o contractual con esta.

Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas deben dar cumplimiento a los siguientes lineamientos:

1. Reportar mediante los canales autorizados, los incidentes o potenciales riesgos del sistema de cifrado o llaves criptográficas.
2. No hacer uso, intentar hacer uso o divulgar información de llaves criptográficas sin la debida autorización.
	1. Política de seguridad física y del entorno
		1. Objetivo(s):
* 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.
* Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la Entidad.
	+ 1. Responsable(s) de la ejecución de la política:
* Subdirección de Investigación e información -SII
* Subdirección Administrativa y financiera
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.11.1.1 Perímetro de seguridad física.
* A.11.1.2 Controles de accesos físicos.
* A.11.1.3 Seguridad de oficinas, recintos e instalaciones.
* A.11.1.4 Protección contra amenazas externas y ambientales.
* A.11.1.5 Trabajo en áreas seguras.
* A.11.1.6 Áreas de despacho y carga.
* A.11.2.1 Ubicación y protección de los equipos.
* A.11.2.2 Servicios de suministro.
* A.11.2.3 Seguridad del cableado.
* A.11.2.4 Mantenimiento de equipos.
* A.11.2.5 Retiro de activos.
* A.11.2.6 Seguridad de equipos y activos fuera de las instalaciones.
* A.11.2.7 Disposición segura o reutilización de equipos.
* A.11.2.8 Equipos de usuario desatendido.
* A.11.2.9 Política de escritorio y pantalla limpia.
	+ 1. Lineamientos:
1. El administrador de los centros de cableado y/o administrador del data center o quien haga sus veces son responsables de mantener los controles de temperatura y humedad en los Centros de Cableado, Centro de Datos y archivos en donde se aloja información física.
2. Los cables de energía eléctrica deben estar separados de los cables de comunicaciones para evitar interferencia, El administrador de los centros de cableado y/o administrador del data center serán las responsables del cumplimiento de este lineamiento.
3. Las dependencias que tienen bajo su custodia centros de cómputo y centros de cableado, en conjunto con la Subdirección Administrativa y Financiera, deben velar porque los recursos de la plataforma tecnológica, ubicados en estos sitios, se encuentren protegidos contra fallas o interrupciones eléctricas.

La Subdirección de Investigación e información -SII o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

1. Conectar y mantener conectado los equipos de cómputo de la Entidad a la corriente regulada con el fin de evitar daños en estos y en la información institucional.
2. Realizar el mantenimiento preventivo y correctivo de los equipos de cómputo en la Entidad.
3. Realizar cambios, reubicación y retiros de los equipos de cómputo en la Entidad
4. Implementar mecanismo de bloqueo automático cuando el equipo de cómputo esté inactivo después de tres (3) minutos
5. Implementar mecanismos para mantener el escritorio limpio de los equipos de cómputo de la Entidad

La Subdirección Administrativa y Financiera o quien haga sus veces debe dar cumplimiento a los siguientes lineamientos:

1. Proporcionar los mecanismos tecnológicos para el registro de los visitantes de la Entidad.
2. Definir los perímetros de seguridad física, tomando como base los activos de información de la Entidad de tipologías de áreas seguras.
3. Aplicar los mecanismos de controles necesarios para mantener la seguridad de las instalaciones de procesamiento de información de carácter confidencial
4. En el caso de no existir supervisión en las áreas consideradas seguras, estas deben permanecer bajo llave.
5. Llevar un registro de la fecha y hora de entrada y salida de los visitantes, asimismo, deben ser supervisados a menos que su acceso haya sido aprobado previamente.
6. Aplicar los controles adecuados para evitar que las actividades o información confidenciales procesadas en las áreas seguras sean visibles y audibles desde el exterior.
7. Llevar un control de entrada y salida de los equipos tecnológicos de la Entidad y estos deben ser retirados con previa autorización del director o subdirector.

Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas deben dar cumplimiento a los siguientes lineamientos:

1. Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas (empresas prestadoras de servicios TIC, mantenimiento, etc.) deben portar el carné o identificación en un lugar visible dentro de las instalaciones de la Secretaria Distrital de Integración Social – SDIS
2. Es responsabilidad de cada Colaborador, reportar o notificar al personal de seguridad física o vigilancia si se encuentran visitantes no acompañados y sin la identificación visible.
3. En áreas seguras está prohibido el uso de equipo fotográfico, de video, audio u otro equipo de grabación, tales como cámaras en dispositivos móviles, a menos que se cuente con autorización para ello.
4. Está prohibido el consumo de alimentos o bebidas en el puesto de trabajo.
5. Conservar el escritorio o su espacio de trabajo libre de información institucional una vez finalicen sus labores diarias propias de la Entidad, esta debe ser guardada bajo llave.
6. Los accesos tanto físicos asignados a los colaboradores serán desactivados o modificados una vez terminados los vínculos contractuales o laborales con la Entidad.
7. Los colaboradores que requieran ingresar a los centros de cómputo o centros de cableado deben realizar las solicitudes de acceso a la Subdirección de Investigación e información -SII o quien haga sus veces.
8. Los colaboradores deben respaldar con copias de seguridad locales o salvaguardar la información en los repositorios web, tales como One drive y Sharepoint. Acá debe reposar toda la información institucional que se encuentre en el equipo de cómputo asignado previniendo así la pérdida involuntaria de la misma.
9. Los lugares de trabajo de los colaboradores de la Secretaria Distrital de Integración Social – SDIS deben ubicarse en lugares que no estén expuestos al acceso de personas externas.
10. Los colaboradores que presten servicios de atención al público deberán ubicar el equipo de cómputo asignado para el desarrollo de las actividades, de tal forma que se evite el acceso o revisión de la información por parte de los usuarios que atienden, estos lugares deben estar protegidos por personal de seguridad y monitoreados por un circuito cerrado de televisión.
11. Todos los colaboradores de la Entidad deberán almacenar de manera estricta y en un lugar seguro los documentos y/o dispositivos de almacenamiento que contengan información Pública Reservada, Pública Clasificada o sensible, por lo que deben ser almacenados bajo llave en escritorios y/o sitios de trabajo, aun cuando se retiren de sus puestos de trabajo (recesos, salidas, reuniones, almuerzo o finalización de jornada o labor); estos elementos incluyen: documentos impresos, CD’s, dispositivos de almacenamiento USB y medios removibles en general.
12. Todos los colaboradores de la de la Secretaria Distrital de Integración Social – SDIS. deberán conservar el escritorio o su espacio de trabajo libre de información Pública Reservada, Pública Clasificada o sensible, que pueda ser alcanzada, copiada, alterada y/o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
13. Siempre que el personal se ausente (recesos, salidas, reuniones, almuerzo o finalización de jornada o labor) de su estación de trabajo o en caso de requerir que el equipo este encendido durante la jornada no laboral, este debe ser bloqueado (En Windows con las teclas Windows y L) y apagar el monitor.
14. Los documentos que incluyan información Pública Reservada, Pública Clasificada o sensible que se envíe a las impresoras deben ser recogidos inmediatamente.
15. Se deben implementar controles para asegurar físicamente los computadores portátiles como por ejemplo con guayas de seguridad para evitar robos.
16. Cuando terminen las actividades laborales y contractuales en el día, se deben finalizar o cerrar todas las aplicaciones y dejar los equipos apagados, excepto aquellos que por necesidad del servicio deben permanecer encendidos.
17. No publicar o dejar a la vista, documentos o datos críticos para la Secretaria Distrital de Integración Social – SDIS., como: nombres de usuario, contraseñas, direcciones IP, números de cuentas, archivos de propiedad intelectual, datos personales semiprivados, privados o sensibles y/o cualquier información pública clasificada o pública reservada.
18. Los usuarios que utilicen conexión por escritorio remoto a servidores de la entidad deberán cerrar la sesión inmediatamente se deje de utilizar, cada vez que se realice la conexión deberá pedir las credenciales de acceso.
19. La Subdirección de Investigación e información -SII con el apoyo del Oficial de Seguridad de la Información – CISO establecerán los controles de bloqueo sobre las sesiones de los equipos de cómputo, de los funcionarios para que se bloquee en un lapso determinado.
20. La Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico o quien haga sus veces asegurará que los usuarios tengan la pantalla del equipo limpia y/o libre de archivos, a través de la aplicación de políticas en el equipo de cómputo.
21. La Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico aplicará el protector de pantalla, de forma que se active luego de tres (3) minutos de inactividad.
22. Todas las estaciones de trabajo propias de la Secretaria Distrital de Integración Social – SDIS, deberán usar el protector de pantalla, el cual se activará automáticamente una vez se bloquee la sesión o después de tres (3) minutos de inactividad, y sólo se podrá desbloquear únicamente con la contraseña del usuario.
	1. Política de seguridad en las operaciones
		1. Objetivo(s):
* Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
* Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
* Proteger contra la pérdida de datos.
* Registrar eventos y generar evidencia.
* Asegurarse de la integridad de los sistemas operacionales.
* Prevenir el aprovechamiento de las vulnerabilidades técnicas.
* Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos.
	+ 1. Responsable(s) de la ejecución de la política:
* Subdirección de Investigación en Información - SII
* Dirección de Análisis y Diseño Estratégico
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.12.1.1 Procedimientos de operación documentados.
* A.12.1.2 Gestión de cambios.
* A.12.1.3 Gestión de capacidad.
* A.12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación.
* A.12.2.1 Controles contra códigos maliciosos.
* A.12.3.1 Respaldo de la información
* A.12.4.1 Registro de eventos.
* A.12.4.2 Protección de la información de registro.
* A.12.4.3 Registros del administrador y del operador.
* A.12.4.4 Sincronización de relojes.
* A.12.5.1 Instalación de software en sistemas operativos.
* A.12.6.1 Gestión de las vulnerabilidades técnicas.
* A.12.6.2 Restricciones sobre la instalación de software.
* A.12.7 Controles de auditorías de sistemas de información
	+ 1. Lineamientos:

La Subdirección de Investigación e información -SII o quien haga sus veces debe:

* Documentar, formalizar, mantener actualizado y divulgar 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, procedimientos como: copias de respaldo, mantenimiento de equipos, gestión de cambios, gestión de capacidad, gestión de eventos, entre otros.

Gestión de Cambios:

1. Establecer un procedimiento para la gestión de cambios donde se contemplen los mecanismos para las solicitudes de los cambios a nivel de infraestructura, aplicativos, sistemas de información, bases de datos, servicios tecnológicos de la entidad y en general a los activos de información tecnológicos y los recursos informáticos.
2. Analizar los riesgos, impactos y requisitos de seguridad de la información de los cambios en los componentes tecnológicos, con el fin de no afectar la correcta operación de estos ni de otros servicios.
3. Informar a los propietarios de los activos de información los cambios que se realicen a los servicios, componentes, sistemas de información y/o infraestructura a su cargo.
4. Garantizar que las modificaciones, mejoras o ajustes en las funcionalidades de los sistemas de información están soportadas por las solicitudes y aprobaciones de los usuarios funcionales.

Gestión de Capacidad:

1. Establecer un procedimiento de gestión de capacidad que permita monitorear el uso y las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad.
2. Supervisar continuamente el consumo, demanda y comportamiento de los recursos tecnológicos asignados, con el fin de realizar gestionar oportunamente los cambios y/o ajustes que se requieran y proyectar las futuras necesidades de capacidad.
3. Se deben designar los responsables encargados de realizar la gestión de capacidad de los componentes tecnológicos.

Separación de Ambientes:

1. Definir los lineamientos para la separación de los ambientes: desarrollo, pruebas, preproducción y producción utilizados en el desarrollo de software y soporte de aplicaciones, con el fin de reducir los riesgos de acceso o cambios no autorizados que puedan afectar la confidencialidad, integridad y disponibilidad de los entornos productivos.
2. Debe proveer los recursos necesarios para la implementación e implantación de controles que permitan la separación de ambientes de desarrollo, pruebas, preproducción y producción tanto lógico como físicamente, teniendo en cuenta consideraciones como:
* Controles para el intercambio de información entre los diferentes ambientes.
* Estandarización de las herramientas utilizadas para los diferentes ambientes.
* Gestión de accesos de acuerdo con roles, privilegios y ambientes.
* Separación de redes, bases de datos e información.

Protección contra códigos maliciosos:

1. Implementar controles para la detección, prevención y recuperación contra códigos maliciosos.
2. Instalar, controlar y mantener actualizada en todos los equipos de cómputo y servidores de la entidad una herramienta de antivirus, que permita la gestión centralizada de las amenazas, eventos, estados de los equipos, entre otros.
3. Los equipos de cómputo personales que requieran ser conectados a la red de datos de la entidad deben contar con un antivirus actualizado.
4. Atención de eventos o incidentes resultantes de las plataformas de seguridad perimetral

Todos los funcionarios, contratistas y terceros:

1. Deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben analizarlos con el software antivirus instalado en sus equipos de cómputo.
2. Deben reportar inmediatamente ante la sospecha o evento de infección por virus, a la mesa de ayudas para que realice la revisión y eliminación del virus.
3. No deben realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Office 365, navegadores u otros programas, para detectar y prevenir la propagación de virus.

Copias de Respaldo o Backup

Estos lineamientos son aplicables a todos los sistemas de información, aplicaciones y dispositivos de almacenamiento que contienen información Pública Reservada y Pública Clasificada los cuales son utilizados para la prestación de servicios tecnológicos internos y externos de la Secretaria Distrital de Integración Social – SDIS, por lo que se deben tener en cuenta los siguientes lineamientos:

La Subdirección de Investigación e información -SII, a través del equipo de infraestructura o quien haga sus veces debe:

1. Documentar, divulgar y mantener actualizado un procedimiento de respaldo de información institucional.
2. Definirá la respectiva arquitectura física de conectividad para la solución de respaldo de la información de la Entidad.
3. Definirá la respectiva arquitectura de red de conectividad para la solución de respaldo de la información de la Entidad.
4. En conjunto con los propietarios de los activos de información de tipo Dato/Información/Bases de Datos y con el apoyo del Oficial de Seguridad de la Información – CISO establecerán la información de tipo Pública Reservada y Pública Clasificada a respaldar, estableciendo las estrategias para la generación, retención, rotación y periodicidad de estas.
5. En conjunto con los propietarios de los activos de información de tipo Dato/Información/Bases de Datos y el Grupo de Gestión Documental con el apoyo del Oficial de Seguridad de la Información – CISO establecerán los tiempos de retención de la información de tipo Pública Reservada y Pública Clasificada.
6. Con el apoyo del Oficial de Seguridad de la Información – CISO establecerá el sistema de almacenamiento de los medios en donde se encontrarán almacenadas de forma segura las copias de respaldo de la información de carácter Pública Reservada, Pública Clasificada o información sensible que determine la Secretaria Distrital de Integración Social – SDIS.
7. Asegurará el respectivo protocolo de almacenamiento y custodia de los medios en donde se almacenen las copias de seguridad, sea este proceso llevado a cabo de manera interna o con un externo a la Secretaria Distrital de Integración Social – SDIS
8. Garantizar que las copias de respaldo se almacenen en un lugar remoto, a una distancia suficiente que permita escapar de cualquier daño que pueda ocurrir en el centro de Datos Principal.
9. Asegurará que el software y las licencias respectivas utilizadas tanto para la generación de las copias de seguridad como para la restauración de estas se encontrará resguardada en los servidores destinados para este proceso.
10. Será responsable de garantizar un inventario de las copias de respaldo. Para el caso de las cintas se deben almacenar en un sitio externo de los centros de datos; en donde se deben asegurar y garantizar los protocolos de seguridad a nivel de transporte, almacenamiento y custodia de las cintas, para garantizar la protección física y asegurar que la información y el software esencial de la Secretaria Distrital de Integración Social – SDIS se puedan recuperar después de un desastre o falla del medio.
11. Será el responsable de las pruebas de restauración de las copias de respaldo, las cuales deben realizarse de manera periódica por lo menos 4 veces por año realizando pruebas aleatorias de restauración sobre las copias de respaldo realizadas y guardadas en los diferentes medios de almacenamiento y/o cualquier otro medio que se tenga para este fin, estas pruebas deben realizarse en ambientes de pruebas controlados; no sobrescribiendo el medio original.
12. Generar los correspondientes informes con el resultado de las pruebas de restauración e integridad de los datos restaurados en los ambientes destinados para este fin.
13. Dependiendo del nivel de clasificación del activo de información respaldado, es decir información pública clasificada o pública clasificada deben estar protegidas mediante algoritmos de cifrado.
14. No se almacenarán en las rutas establecidas por La Subdirección de Investigación e información -SII, a través del equipo de infraestructura para la realización de las copias de seguridad; información de tipo personal, videos, fotos, música, y otro tipo de información que no se encuentre relacionada con la Misión y Objetivos Estratégicos de la Secretaria Distrital de Integración Social – SDIS y la cual no hace parte del desarrollo de las funciones y/o responsabilidades asignadas a cada colaborador.
15. Definir los lineamentos para la generación, periodicidad y esquema de ejecución de las copias de respaldo deben ser definidos en procedimientos operativos que debe contener por lo menos:
	* Registros exactos y completos de las copias de respaldo, y procedimientos de restauración documentados.
	* Frecuencia de la Copia de respaldo ejemplo (Backup Full, diferencial, incremental), y alineadas a los requisitos de seguridad y criticidad para la operación continua de la Secretaria Distrital de Integración Social – SDIS.
16. Definir los periodos de retención y eliminación de la información de acuerdo con la normativa relacionada, en donde indican los inventarios de la documentación que ha cumplido con el tiempo de retención establecido en la Tabla de Retención Documental y que son objeto de eliminación.
17. En el caso de sistemas y servicios críticos de continuidad de la operación de la Secretaria Distrital de Integración Social – SDIS, las disposiciones relativas a copias de respaldo incluyen toda la información de sistemas, aplicaciones y datos necesarios para recuperar el sistema completo en caso de evento o desastre en un Centro de datos Alterno, dando cumplimiento y alineado al RPO y RTO definido en el Plan de Continuidad del negocio y plan de continuidad tecnológico para los Planes de Recuperación DRP de la Secretaria Distrital de Integración Social – SDIS
18. La Subdirección de Investigación e información -SII, No es responsable de las copias de respaldo de la información contenida en los equipos de cómputo ni dispositivos de almacenamiento, en caso de requerirse respaldo de la información esta solo podrá ser solicitada por el Director, Subdirector o líder de proceso indicando el lugar donde almacenará la copia de respaldo.

Todos los funcionarios, contratistas y terceros:

1. Los responsables de la ejecución de los respaldos notificarán a La Subdirección de Investigación e información -SII, a través del equipo de infraestructura y al CISO y/o líder inmediato cualquier error e inconsistencia en el proceso de generación de copias de respaldo y/o procesos de restauración fallidos.
2. Es indispensable que los propietarios de los activos de información identifiquen el nivel de clasificación de la información a su cargo, y así mismo, reportar los riesgos identificados a los cuales se encuentra expuesta.
3. Los dueños de proceso, directores o subdirectores serán los autorizados para solicitar en caso de ser necesario y mediante el procedimiento de restauración de copias de seguridad, la restauración de la información, realizando la solicitud a través de la mesa de ayuda.
4. Se debe garantizar por parte de los funcionarios, contratistas y/o terceros que toda la información generada debe almacenarse en los repositorios autorizados por la Secretaria Distrital de Integración Social – SDIS en caso de ser almacenado en los dispositivos móviles no autorizados o equipos locales, se traslada toda responsabilidad frente a los controles de acceso, respaldo, criptografía y demás controles indicados por la Entidad para garantizar la Confidencialidad, integridad y disponibilidad de la información almacenada en el dispositivo.
5. Deben realizar el respaldo de la información institucional mediante los mecanismos o herramientas proporcionadas la Subdirección de Investigación e información -SII, a través del equipo de infraestructura, como la sincronización en nube de la información.

Control de Eventos

La Oficina de control interno o quien haga sus veces debe:

1. Generar y revisar periódicamente registros de auditoría que contengan actividades del usuario, excepciones, fallas y eventos de seguridad de la información de las actividades de los sistemas de información e infraestructura critica.
2. Implementar los controles necesarios por la custodia, confidencialidad, integridad y disponibilidad de los registros de auditoria cumpliendo con los periodos de retención establecidos para dichos registros.
3. En conjunto con los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la entidad.
4. Determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información.
5. Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con el tipo de información y la criticidad de las operaciones.
6. Sincronizar los relojes de los servidores, sistemas de información, telefonía, CCTV, sistemas de información, estaciones de trabajo y todo componente de información; con una única fuente de referencia de tiempo con el fin de garantizar la exactitud de los registros de auditoría.

Control de Software

La Subdirección de Investigación e información -SII, a través del equipo de infraestructura debe:

1. Documentar, actualizar y divulgar los procedimientos para controlar la instalación de software en los equipos de cómputo de la entidad, estableciendo las responsabilidades, restricciones y limitaciones.
2. Garantizar que el software instalado en la plataforma tecnológica cuente con soporte en caso de ser necesario y con los proveedores según sea requerido.
3. Gestionar oportunamente las actualizaciones sobre el software instalado.
4. Validar los riesgos que genera la migración hacia nuevas versiones del software, realizando las correspondientes pruebas y contando con la aprobación del Comité de Cambios.

Gestión de Vulnerabilidades

La Subdirección de Investigación e información -SII, a través del equipo de infraestructura, en conjunto con la Subdirección de análisis e investigación, a través del Oficial de Seguridad de la información, revisará periódicamente (cada seis meses), los resultados de las pruebas de vulnerabilidades técnicas y ethical hacking sobre los recursos de la plataforma tecnológica.

1. Debe revisar cada seis meses o según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos.
2. Debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica cada tres meses.

Restricciones en la instalación del software

La Subdirección de Investigación e información -SII, a través del equipo de gestión de soporte y mantenimiento tecnológico o quien haga sus veces:

1. Es la única dependencia autorizada para realizar la instalación de software o programas en los sistemas operativos de los equipos de cómputo y portátiles institucionales.
2. Debe realizar la instalación de software en los computadores suministrados por la Secretaria Distrital de Integración Social – SDIS, como función exclusiva de esta o a quienes ellos deleguen.
3. Debe autorizar el software adicional que se requiera instalar en equipos de cómputo específicos de la Secretaria Distrital de Integración Social – SDIS.
4. Debe definir, mantener y publicar la lista actualizada del software autorizado y no autorizado para instalar en los computadores la Secretaria Distrital de Integración Social – SDIS.
5. Validar y controlar el uso de software libre teniendo en cuenta las limitaciones para el uso corporativo y validado por el Oficial de Seguridad de la Información.
6. Controlar y validar la instalación y administración de las licencias de programas y software autorizado.

Auditorias de sistemas de información

1. La oficina de control interno o quien haga sus veces, apoyados en los procedimientos de Auditoría Interna, verificarán el cumplimiento de los requisitos de las normas ISO aplicables, la normatividad legal vigente y los requisitos propios de la organización cada año o según sea necesario.
2. La oficina de control interno o quien haga sus veces, debe verificar que las auditorías concluyan la eficacia y eficiencia de los sistemas de información implementados en la institución.
3. La oficina de control interno debe planificar para reducir al mínimo las interrupciones de los procesos, de acuerdo con los requisitos de auditoría y las actividades relacionadas con la verificación de los sistemas operativos.
4. Las áreas responsables y/o propietarias de los sistemas de información donde se encuentren desviaciones, deficiencias o no conformidades, deberán generar y darle cumplimiento, a un plan de mitigación o atención, con el apoyo de la Subdirección de Investigación e información -SII, a través del equipo de infraestructura.
	1. Política de seguridad de las comunicaciones
		1. Objetivo(s):
* Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de soporte.
* Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
	+ 1. Responsable(s) de la ejecución de la política:
* Tecnologías de la información
* Gestión de soporte y mantenimiento tecnológico
* Planeación Estratégica
* Dirección de Análisis y Diseño Estratégico
* Comunicaciones
* Oficina Jurídica
* Dirección Administrativa y Financiera
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarcan la norma NTC-ISO-27001:2013 Anexo A:
* A.13.1.1 Controles de redes.
* A.13.1.2 Seguridad de los servicios de red.
* A.13.1.3 Separación en las redes.
* A.13.2.1 Políticas y procedimientos de transferencia de información.
* A.13.2.2 Acuerdos sobre transferencia de información.
* A.13.2.3 Mensajería electrónica.
* A.13.2.4 Acuerdos de confidencialidad o de no divulgación.
	+ 1. Lineamientos:

La Secretaria Distrital de Integración Social – SDIS establecerá, a través de la Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico o quien haga sus veces, los 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.

Gestión de la seguridad de las redes

El área de infraestructura o quien haga sus veces debe:

1. Identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red, ya sea que los servicios se presten internamente o se contraten externamente.
2. Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red.
3. Implantar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.
4. Mantener las redes de datos segmentadas por dominios, grupos de servicios, grupos de usuarios y ubicación.
5. Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de nivel de servicios de red.
6. Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la institución, acogiendo buenas prácticas de configuración segura.
7. Identificar, justificar y documentar los servicios, protocolos y puertos permitidos en la red de datos de la entidad e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.
8. Instalar protección entre las redes internas y cualquier red externa, que esté fuera de la capacidad de control y administración de la entidad.
9. Garantizar la confidencialidad de la información del direccionamiento y el enrutamiento de las redes de datos.
10. Bloquear el acceso a las páginas de contenido para adultos, mensajería instantánea y demás páginas que no sean de uso corporativo mediante el uso de servidor proxy, firewall o el software que mejor se ajuste a la necesidad.
11. En ningún caso se podrá dejar configuraciones y contraseñas por defecto en los equipos inalámbricos.
12. Garantizar que los usuarios que utilizan las redes inalámbricas cuenten con a las mismas condiciones de seguridad de las redes cableadas en lo que respecta identificación, autenticación, control de contenido de internet y cifrado entre otros.
13. Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de internet, bajo las restricciones de los perfiles de acceso establecidos; implementar mecanismos que permitan la continuidad o restablecimiento del servicio de internet en caso de contingencia interna.
14. Establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de internet, que permitan monitorear continuamente el canal o canales del servicio de internet, en cuanto a carga y tráfico; establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de internet y evitar el acceso a sitios catalogados como restringidos; generar registros de la navegación y los accesos de los usuarios a internet.
15. En acompañamiento de la Dirección de Análisis y Diseño Estratégico y con el apoyo del área de comunicaciones, deben generar campañas para concientizar a todo el personal de la Secretaria Distrital de Integración Social – SDIS y terceros, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de internet.

Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas de la Secretaria Distrital de Integración Social – SDIS:

1. Está prohibido enviar o retransmitir cadenas de correo, mensajes con contenido racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, la moral, las buenas costumbres y mensajes que inciten a realizar prácticas ilícitas o promuevan actividades ilegales.
2. Está prohibido la navegación en sitio de contenido sexualmente explícito, discriminatorio, que implique un delito informático o cualquier otro uso que se considere fuera de los límites permitidos por las Políticas de Seguridad y Privacidad de la Información.
3. Está prohibido la publicación, envío o adquisición de material sexualmente explícito, discriminatorio, que implique un delito informático o de cualquier otro contenido que se considere ofensivo.
4. Hacer uso del servicio de internet que provee la Secretaria Distrital de Integración Social – SDIS para las actividades que guarden relación con su labor dentro de la misma; abstenerse de descargar software no autorizado desde internet, así como su instalación en las estaciones de trabajo asignados para el desempeño de sus labores, a menos que sean autorizados por la Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico, CISO o quien haga sus veces.
5. No deben acceder a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y cualquier otra página que vaya en contra de la ética y la moral, las leyes vigentes del país o las políticas establecidas en este documento, a menos que la labor que tiene en la entidad, así lo demande.
6. No deben utilizar el servicio de internet para el acceso y uso de servicios interactivos o mensajería instantánea como Facebook y otros similares, con el fin de intercambiar información confidencial o de uso interno de la entidad o para actividades que no corresponden con el desempeño de las funciones asignadas.
7. No deben descargar, usar, intercambiar o instalar juegos, música, películas, información que de alguna manera atenten contra la propiedad intelectual de sus autores.
8. No deben ejecutar archivos o herramientas que atenten contra la integridad, disponibilidad o confidencialidad de la infraestructura tecnológica de la Secretaria Distrital de Integración Social – SDIS.
9. Deben asegurarse de que la información audiovisual (videos e imágenes) descargada y utilizada para las labores diarias no atenten contra la propiedad intelectual de sus autores.

Transferencia de Información

Todas las áreas y dependencias de la Secretaria Distrital de Integración Social – SDIS:

1. Definir los procedimientos de transferencia de información entre colaboradores la Secretaria Distrital de Integración Social – SDIS y con terceros, preservando la integridad y confidencialidad de la Información institucional. Los acuerdos de intercambio de información ente entidades debe ser revisado por el responsable del tratamiento de datos personales o el CISO de la Secretaria Distrital de Integración Social – SDIS.
2. Deben establecer acuerdos de confidencialidad, acuerdos macro o convenios con las entidades que por diferentes razones requieran conocer o transferir información catalogada como Pública Clasifica, Pública Reservada o información sensible.
3. En los acuerdos deben estar especificadas las responsabilidades para la transferencia de la información para cada una de las partes y se deberán firmar antes de permitir el acceso o uso de dicha información.
4. La Oficina Jurídica, en acompañamiento con la Dirección de Análisis y Diseño Estratégico el CISO, infraestructura o quien haga sus veces, debe definir los modelos de Convenios o Contratos de Transferencia o Transmisión de datos, Acuerdos de Confidencialidad, Acuerdos de Intercambio, así como las cláusulas de Confidencialidad de información entre la entidad y terceras partes incluyendo los compromisos adquiridos y las penalidades civiles o penales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir:
	* La prohibición de divulgar la información entregada por parte de la entidad a los terceros con quienes se establecen estos acuerdos.
	* La destrucción de dicha información una vez cumpla su cometido.
	* El periodo del acuerdo.
	* Los medios a través de los cuales se compartirá la información.
	* Propietarios de los activos de información a manejar entre las partes
	* Los responsables de la custodia de la información.
5. Se debe establecer en los contratos que se constituyan con terceras partes, los acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de la entidad que les ha sido entregada.
6. Los propietarios y custodios de los activos de información deben proteger la confidencialidad, disponibilidad, integridad y no repudio de la información durante los procesos o actividades de transferencia de la información, estableciendo los riesgos y los canales de transferencia seguros que eviten la divulgación o modificación no autoriza de la información, los cuales permitan brindar los niveles de seguridad apropiados.
7. Los propietarios de los activos de información son los responsables de definir los controles de seguridad, niveles y perfiles de autorización para el acceso, modificación y/o eliminación de estos, garantizando siempre la confidencialidad, disponibilidad, integridad y no repudio, en los acuerdos de confidencialidad entre la Secretaria Distrital de Integración Social – SDIS y proveedores y/o aliados y los cuales deben ser revisados y aprobados por la Oficina Jurídica o quien haga sus veces, en los cuales asumirán las responsabilidades para garantizar la reserva de la información y el alcance frente al tratamiento de esta.
8. Los custodios de los activos de información son responsables de implementar los controles de seguridad definidos por propietarios que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad y no repudio requeridos.
9. En la transferencia de información con terceros, se exigirá el uso de controles criptográficos como mecanismo de control para llevar a cabo dicha actividad.
	* La información utilizada en la transferencia sólo será usada para las actividades autorizadas dentro de los acuerdos suscritos entre la Secretaria Distrital de Integración Social – SDIS y los proveedores y/o aliados de ésta.
	* En las situaciones y/o casos que son indicados por la Ley Colombiana, la Secretaria Distrital de Integración Social – SDIS realizará el uso de certificados de firma digital debidamente emitido por una entidad certificadora autorizada.
	* La transferencia de información se llevará a cabo según los acuerdos establecidos que describen las responsabilidades y procedimientos para la transferencia segura de la información.
	* En el caso de presentarse un incidente de seguridad, el responsable del proceso de la transferencia de la información deberá seguir lo indicado en los procedimientos de gestión de Incidentes en Seguridad de la Información definidos en la Secretaria Distrital de Integración Social – SDIS para la atención de estos.
	* La Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico o quien haga sus veces y/o la Subdirección Administrativa y Financiera o quien haga sus veces, asegurarán que los medios utilizados para llevar a cabo la transferencia de información ya sea de manera física o electrónica, se realiza a través de canales que preserven los niveles de confidencialidad e integridad de la información, conforme a su nivel de clasificación establecido en el inventario de activos de información de la Secretaria Distrital de Integración Social – SDIS.
	* Infraestructura o quien haga sus veces debe definir e implementar las herramientas tecnologías y de telecomunicaciones para llevar a cabo el intercambio de información, tanto a nivel interno como externo.
10. Utilizar únicamente los mecanismos y herramientas proporcionadas por infraestructura o quien haga sus veces para el envío o recepción de información confidencial para la entidad.
11. Queda prohibido que el personal de la Secretaria Distrital de Integración Social – SDIS y terceros revelen o intercambien información confidencial de la entidad por cualquier medio, sin contar con la debida autorización y documento jurídico que la garantice y del titular de la información cuando haya lugar a ello. Para lo anterior y en compañía de la oficina jurídica se establecerán acuerdos de confidencialidad para funcionaros, contratistas y terceros a que haya lugar.

Mensajería Electrónica (correo electrónico y herramientas colaborativas)

Entendiendo la importancia del correo electrónico y las herramientas colaborativas como herramientas para facilitar la comunicación entre funcionarios, contratistas y terceras partes, infraestructura proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad, autenticidad y no repudio de quienes realizan las comunicaciones por este medio.

El área de Infraestructura o quien haga sus veces:

1. Debe establecer y divulgar a nivel institucional un procedimiento para la administración de cuentas de correo electrónico.
2. Garantizar que la plataforma de correo tenga los procedimientos y controles necesarios que permitan detectar y proteger la integridad de la información que viaja a través de esta plataforma.
3. Garantizar que los mensajes electrónicos están protegidos contra código malicioso que puede ser transmitido a través de estos.
4. Generar campañas de concientización a todos los colaboradores (directores, subdirectores, lideres, supervisores de contrato y en si a todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS etc.), respecto a los controles que deben adoptar en el intercambio de información confidencial y de uso interno por medio del correo electrónico.
5. Queda terminantemente prohibido a los usuarios el envío de mensajes masivos a través de correo electrónico; este tipo de mensajes sólo puede ser enviado por usuarios debidamente autorizados. Los usuarios autorizados son: el Administrador de las cuentas de correo, la alta Dirección o Comunicaciones e infraestructura para fines tecnológicos.
6. Es responsabilidad del usuario enmarcar todos los mensajes que envíe a través de correo electrónico dentro de las normas mínimas de respeto y protocolo electrónico, sin incluir contenidos hostiles que molesten a los receptores del mismo, tales como comentarios sobre sexo, raza, religión o preferencias sexuales, tendencia política entre otras que generen algún tipo de discriminación; así mismo, es responsabilidad del usuario reportar a su líder de área la recepción de este tipo de mensajes, quien a su vez deberá reportarla al área que corresponda, en caso de comprometer la seguridad de la información de la entidad.
7. Es responsabilidad del usuario evitar que su cuenta de correo electrónico sea utilizada por terceros (clientes o proveedores).
8. Es responsabilidad del usuario evitar que la información confidencial sea transmitida por medio de su cuenta de correo electrónico, salvo autorización previa emitida por el director subdirector o líder, en cuyo caso los archivos deben viajar en forma Segura (encriptados).
9. Es responsabilidad del Usuario evitar el uso de una cuenta de correo electrónico que pertenezca a otro usuario, si hay necesidad de hacerlo en caso de ausencias, incapacidades o vacaciones, se debe recurrir a mecanismos alternos como redirección de mensajes o mensajes informando la ausencia determinada.

Se establecen los siguientes lineamientos y consideraciones en cuanto al uso del correo electrónico y herramientas colaborativas:

1. Enviar mensajes desde la cuenta de correo electrónico de un usuario con firma de otro.
2. Intentar acceder y/o accesar sin autorización a otra cuenta de correo electrónico.
3. Transmitir mensajes de correo con información sensible o confidencial a personas u organizaciones externas sin autorización expresa del propietario de la información.
4. Participar en cadenas de mensajes que congestionen la red.
5. Es responsabilidad de los usuarios de correo electrónico mantener o archivar los mensajes enviados y/o recibidos para efectos de soportar ante terceros (internos o externos) la ejecución de operaciones o acciones.
6. Es responsabilidad del usuario eliminar periódicamente de sus dispositivos de almacenamiento los mensajes que ya no necesite. Con esto se reducen los riesgos de que otros usuarios puedan acceder a esa información; y, además, se libera espacio en disco.
7. La plataforma de correo electrónico y las herramientas colaborativas se deberán utilizar únicamente para fines institucionales, no debe registrarse la cuenta de correo institucional para recibir información personal, acceso a páginas o servicios en internet personales.
8. Los usuarios son responsables de todas las actividades que se realicen desde su cuenta de correo institucional, por lo que la cuenta de correo electrónico asignada es de carácter individual; por consiguiente, ningún funcionario, en ninguna circunstancia debe utilizar una cuenta de correo que no sea la suya.
9. Las cuentas de correo institucional son de uso personal e intransferible, por lo tanto, es responsabilidad del usuario salvaguardar la contraseña, cambiarla periódicamente, y no prestarla en ninguna circunstancia.
10. Las cuentas de correo institucional son creadas para el uso exclusivo de las actividades institucionales, por lo tanto, el usuario debe hacer uso de este servicio implementando criterios de racionalidad, respeto, responsabilidad, integridad, seguridad y privacidad de la información.
11. Cualquier persona que requiera una cuenta de correo electrónico y/o acceso a las herramientas colaborativas, deberá solicitar el servicio por intermedio de su líder o del supervisor del contrato. Esta solicitud se deberá realizar a través de la mesa de ayuda.
12. No se deberán utilizar para asuntos institucionales las cuentas de correo electrónico personal o ajenas de la Secretaria Distrital de Integración Social – SDIS.
13. Está prohibido utilizar la plataforma de correo electrónico de la entidad o las herramientas colaborativas para realizar proselitismo político o religioso, actividades de negocios privados, distribución de cadenas de mensajes, propagación de falsas alarmas por correo electrónico, diversión, entretenimiento personal y demás condiciones que degraden la condición humana y resulten ofensivas para los miembros de la entidad.
14. El contenido de un correo electrónico que documente una decisión, acción o transacción será considerado como un registro de la entidad y se deberá administrar y guardar en conformidad con la clasificación que tenga.
15. Todos los usuarios deberán reportar a la mesa de ayuda cuando reciban un correo no deseado o con archivos adjuntos sospechosos y cualquier fallo de seguridad incluyendo el uso no autorizado.
16. Únicamente los directores, subdirectores y lideres pueden solicitar cuentas de correo electrónico cuyo nombre no esté asociado a una persona individual sino a una función, grupo de trabajo o área. El uso debe ser congruente con su función, por lo que debe evitarse el envío de correos sobre temas o intereses diferentes al mismo. De esta manera está estrictamente prohibido enviar mensajes controversiales para generar respuestas. El solicitante, o quien él delegue, es responsable directo del contenido de los mensajes generados a través de esas cuentas.
17. No deben enviar archivos que contengan extensiones ejecutables con contenido malicioso, por ningún motivo.
18. Respetar el estándar de formato e imagen corporativa definidos por la entidad para los mensajes electrónicos y deben conservar en todos los casos el mensaje legal corporativo de confidencialidad.
19. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Secretaria Distrital de Integración Social – SDIS y cada usuario, como responsable de su buzón, debe mantener los mensajes relacionados con el desarrollo de sus funciones u obligaciones, por este motivo la información y tráfico de esta se considera de interés para la Entidad.
20. Está prohibido el envío de correos masivos no autorizados por la Oficina de Comunicaciones de la Secretaria Distrital de Integración Social – SDIS.
21. Todos los mensajes enviados por medio de correo electrónico pertenecen a la Secretaria Distrital de Integración Social – SDIS el cual se reserva el derecho de acceder y revelar los mensajes enviados por este medio para cualquier propósito.
22. Tenga en cuenta las recomendaciones de seguridad de la información, no abra correos de dudosa reputación y no descargue contenido peligroso como puedo generar algún tipo de malware o phishing que a su vez pueda afectar la red o los activos de información.
23. Cualquier correo enviado a múltiples usuarios con el propósito de hacer promociones comerciales o enviar información, sin que los usuarios hayan solicitado este servicio, es considerado como SPAM. Todos los correos SPAM y sus originadores deberán ser bloqueados, hasta que el interesado presente por la mesa de ayudas una justificación contraria al respecto. Una solicitud de bloquear una cuenta como SPAM tiene prelación sobre una de desbloquear la misma cuenta. Todo caso de conflicto en la clasificación de cuentas como SPAM será resuelto por la Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico o quien haga sus veces.

Almacenamiento de información en la nube institucional y otras herramientas:

1. El uso del servicio de almacenamiento de archivos en la nube deberá ser solo para fines institucionales y nunca debe usarse para fines personales.
2. Está prohibido almacenar información clasificada como reservada sin cifrar en la nube.
3. Está prohibido almacenar archivos de la Secretaria Distrital de Integración Social – SDIS en nubes públicas como Dropbox, Google Drive, Mega, entre otros.
4. Es responsabilidad del usuario realizar copias de seguridad o solicitar las copias de seguridad de los documentos y/o carpetas que almacena en las herramientas colaborativas.
5. El área de infraestructura o servicios o quien haga sus veces no serán responsables por la pérdida o daño de la información que se encuentra almacenada en el equipo de cómputo de colaborador, dado que la información debe ser almacenada y sincronizada en las herramientas institucionales en la nube.
6. La comunicación por mensajería instantánea y reuniones virtuales deben realizarse únicamente a través de la herramienta institucional autorizada, teniendo en cuenta que solo debe utilizarse para temas laborales.

Administradores de la plataforma de correos y herramientas colaborativas:

1. El Administrador del correo electrónico no deberá revisar el contenido de las comunicaciones de un usuario individual por curiosidad personal o a petición de personas que no hayan tramitado la aprobación debida. Se requiere aprobación antes de monitorear el correo por parte del líder de área o supervisor del contrato. En caso de que el uso del correo reporte alguna actividad que ponga en riesgo la seguridad de la información de la entidad, la Subdirección de Investigación e información -SII o quien haga sus veces podrá realizar la validación de estas actividades, documentando toda acción que se realice y dejando evidencia de los hallazgos encontrados.
2. En caso de requerirse para investigaciones de áreas o entes competentes se podrá realizar monitoreo y revisión de los contenidos almacenados en el servidor de correo corporativo y en las estaciones de trabajo, para tal caso se debe contar con la solicitud formal del Ente respectivo y aprobación por parte Subdirección de Investigación e información -SII y el Oficial de Seguridad CISO.
3. Periódicamente el administrador revisará las cuentas de correo que lleven más de 30 días sin ningún acceso. En caso tal, se procederá a enviar un correo electrónico o comunicación al director, subdirector o líder, donde fue asignada la cuenta, advirtiendo del proceso de eliminación y se darán 15 días calendario adicionales a partir de la fecha de la comunicación para la utilización de las cuentas o la solicitud de no eliminación. Vencidos los 15 días adicionales, se procederá a la eliminación y se entenderá que ya ha sido comunicada la decisión.

* 1. Política de adquisición, desarrollo y mantenimiento de sistemas
		1. Objetivo(s):
* Garantizar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes públicas.
* Garantizar que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
* Asegurar la protección de los datos usados para pruebas.
	+ 1. Responsable(s) de la ejecución de la política:
* Subdirección de investigación en información -SII
* Fábrica de software
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.14.1.1 Análisis y especificación de requisitos de seguridad de la información.
* A.14.1.2 Seguridad de servicios de las aplicaciones en redes públicas.
* A.14.1.3 Protección de transacciones de los servicios de las aplicaciones.
* A.14.2.1 Política de desarrollo seguro.
* A.14.2.2 Procedimientos de control de cambios en sistemas.
* A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación.
* A.14.2.4 Restricciones en los cambios a los paquetes de software.
* A.14.2.5 Principios de construcción de los sistemas seguros.
* A.14.2.6 Ambiente de desarrollo seguro.
* A.14.2.7 Desarrollo contratado externamente.
* A.14.2.8 Pruebas de seguridad de sistemas.
* A.14.2.9 Prueba de aceptación de sistemas.
* A.14.3.1 Protección de datos de prueba.
	+ 1. Lineamientos:

Subdirección de Investigación e información -SII con el apoyo del grupo fábrica de software y el Oficial de Seguridad CISO, son los responsables de planificar, desarrollar y ejecutar las actividades relacionadas con el ciclo de vida del software teniendo en cuenta los requerimientos de seguridad y privacidad de la información de acuerdo con las necesidades de la Secretaria Distrital de Integración Social – SDIS, definiendo los criterios para el desarrollo que se contrate con terceros, así establecer los siguientes lineamientos:

1. Garantizar que el software adquirido y desarrollado tanto al interior de la entidad como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos por la Secretaria Distrital de Integración Social – SDIS.
2. Establecer metodologías para el desarrollo de software, que incluyan la definición de requerimientos de seguridad y las buenas prácticas de desarrollo seguro.
3. Establecer un ambiente de desarrollo seguro durante la ejecución de los proyectos, arquitecturas, software o sistemas, estableciendo metodologías que incluyan requisitos de seguridad en cada una de las fases de los proyectos, acuerdos de soporte, niveles de servicio a terceros, y separación física y virtual de todos los ambientes (producción, preproducción, pruebas, desarrollo, entre otros), a través de técnicas de desarrollo seguras. (Owasp).
4. Debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.
5. Se debe definir la estructura de trabajo con sus respectivos responsables, los criterios de aceptación, las pruebas de funcionalidad y seguridad teniendo en cuenta tanto los requerimientos y cumplimiento de los objetivos estratégicos de la Entidad; las etapas deben estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos de desarrollo y aceptación del software bajo las condiciones de línea base de requerimientos de seguridad frente al desarrollo de aplicaciones.
6. Los responsables (propietarios y custodios) de los sistemas de información deben gestionar la inclusión de los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo.
7. Se debe realizar pruebas de seguridad sobre el código fuente y la aplicación en cada fase de ciclo de vida de desarrollo; de igual forma se deben realizar estas pruebas de seguridad antes y después de la salida a producción.
8. Certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado, garantizando el uso de las últimas versiones estables de librerías utilizadas en el desarrollo de la aplicación.
9. Se deben implementar mecanismos de seguridad (autenticación, autorización y auditoría) en todas las fases del desarrollo de software.
10. Evitar el uso de información que contengan datos personales o información pública clasificada, pública reservada y sensible para propósito de desarrollo y pruebas.
11. Los datos de producción que pasan a los ambientes de desarrollo y pruebas se deben proteger con técnicas que anonimicen, ofusquen y/o enmascaren la información que contenga datos personales.
12. Se deben generar registros de auditoría lectura, borrado, escritura o actualización en los sistemas de información, servidores de aplicaciones y repositorios de datos.
13. La solicitud de nuevos desarrollos de software o modificaciones al software existente se realizará a través de los directores, subdirectores o lideres de proceso de manera formal y de acuerdo con lo establecido en los procedimientos institucionales.
14. La identificación de las necesidades y/o requisitos de seguridad, se definen en la línea base de requerimientos de seguridad para nuevos desarrollos generados.
15. Todas las aplicaciones que no contemplen los mecanismos mínimos de seguridad no pueden ser liberadas a menos que se maneje un proceso de excepción. En el proceso de excepción el líder de proceso, director o jefe de oficina debe firmar un documento de responsabilidad en el que se justifique la razón por la que no se están contemplando esos mecanismos mínimos de seguridad.
16. Cada sistema de información deberá contar con sus manuales de uso, técnicos y administrativos disponibles de acuerdo con los niveles de protección de la información dados por la Secretaria Distrital de Integración Social – SDIS.
17. Documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.
18. Realizar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros y utilizando mecanismos o herramientas de cifrado.
19. Se debe contar con la aprobación de la Subdirección de Investigación e información -SII o quien haga sus veces para la adquisición de los aplicativos o el software en concordancia con la política de seguridad y privacidad de la información y el Manual de lineamientos específicos de seguridad y privacidad de la información.
20. En acompañamiento de fábrica de software y el oficial de seguridad CISO o quien haga sus veces, deben establecer los procedimientos de adquisición o desarrollo de sistemas de información, considerando los requerimientos de seguridad de la información, y posteriormente se asegurarán de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido o adquiridos.
21. Deben definir qué información Pública Clasificada, Pública Reservada o sensible, puede ser eliminada de sus sistemas y solicitar que estos soporten la eliminación de dicha información, como es el caso de los datos personales, financieros, datos médicos, datos personales de niños y niñas, datos biométricos, orientación sexual o cuando estos ya no son requeridos.
22. Planear y ejecutar pruebas funcionales que les permitan contar con la aceptación de los desarrollos y funcionalidades solicitados, lo anterior frente a adquisiciones, cambios o nuevos desarrollos.

Aseguramiento de Código Fuente

Fábrica de software o quien haga sus veces:

1. Los sistemas de información deben limitarse a recibir y validar los datos de entrada, gestionar los eventos de los controles gráficos y proporcionar los datos de salida adecuados para los usuarios, sin exponer ningún tipo de información de la aplicación.
2. Se debe implementar un mecanismo adecuado de gestión de errores, que ofrezca un modo de recuperación seguro y que regrese mensajes adecuados, con mínima información que no afecte y/o comprometa la seguridad de la aplicación y/o sistema de información.
3. No se debe tener credenciales de autenticación (por ejemplo: usuario y contraseña) escritas en el código de la aplicación.
4. De acuerdo con los requisitos de la línea base de seguridad toda aplicación nueva desarrollada deberá implementar un módulo de administración de usuarios.
5. Toda aplicación desarrollada deberá contar con un módulo de seguridad mínimo como RECAPTCHA en el formulario de autenticación de usuarios, para evitar que un robot ejecute peticiones de manera automática; y/o ataques de fuerza bruta.
6. Deben utilizarse mecanismos de transferencia de datos de forma segura bajo protocolos HTTPS, SFTP, FTPS, SSL/TLS, entre otros, con el fin que no se transmita información en texto plano, y que a su vez utilicen algoritmos de cifrado fuertes o reconocidos como seguros.
7. Gestionar los requerimientos de seguridad establecidos para el manejo de sesiones y cookies web.
8. Para servicios web ejemplo webservice, se deberá implementar mecanismos de autenticación y autorización mediante tokens.
9. Se debe asegurar la inclusión de los controles de seguridad definidos por la Entidad y considerando en el top 10 de OWASP, tanto para el desarrollo, como para el testeo de la aplicación.
10. Los desarrolladores deben contar con los conocimientos para evitar que resuelvan las vulnerabilidades que se presenten en el código fuente de los desarrollos.
11. No se debe exponer información de configuración y/o parametrización, que contenga datos personales o información pública clasificada, pública reservada o sensible en la documentación del código fuente, en los logs o bitácora de eventos de los sistemas de información o servidores de aplicaciones.
12. Disponer de ambientes de desarrollo, pruebas, preproducción y producción separados de los demás ambientes, con controles de acceso definidos, contando con infraestructura y personal propios en cada uno de ellos.
13. Validará que los cambios requeridos sobre el software nuevo o en funcionamiento en la Secretaria Distrital de Integración Social – SDIS, se lleven a cabo a través del procedimiento de control de cambios, el cual permite que se documenten y establezcan los requerimientos de seguridad y los niveles de aceptación del cambio.
14. En conjunto con el CISO realizarán un seguimiento a los riesgos asociados a la seguridad de la información y la identificación de controles, los cuales serán tenidos en cuenta en la ejecución del procedimiento de control de cambios, con el objetivo de asegurar la implementación de los controles respectivos en el desarrollo y/o actualización del software.
15. Definirá acuerdos en los procesos de desarrollo y en los cuales quedará establecido con claridad la propiedad de las licencias y derechos intelectuales de los códigos fuentes, así como sus condiciones de usabilidad.
16. Llevará un control de versiones del código fuente y documentación de los sistemas de información, ello con el objeto de verificar el funcionamiento del software y el respectivo control de su ciclo de vida, en un repositorio especializado para este tipo de información.
17. Deshabilitar las funcionalidades de completar automáticamente en formularios de solicitud de datos que requieran información sensible.
18. Cerrar las sesiones activas de las aplicaciones luego que pasen tres (3) minutos sin actividad, terminándolas una vez se cumpla este tiempo.
19. Asegurar que no se permitan conexiones recurrentes a los sistemas de información con el mismo usuario.

Desarrollo Seguro

El área de Fábrica de software o quien haga sus veces:

1. Debe garantizar que el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con 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.
2. En conjunto con los propietarios de los aplicativos deben realizar las pruebas necesarias para asegurar que los sistemas de información desarrollados cumplen con los requerimientos de seguridad establecidos antes del paso a producción, utilizando metodologías establecidas para este fin, documentado las pruebas realizadas y aprobando los pasos a producción.
3. Implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.
4. Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información.
5. Asegurase que los sistemas de información adquiridos o desarrollados por terceros cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.
6. Generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.
7. Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada del sistema.
8. Incluir dentro del procedimiento de gestión de cambios el manejo de los cambios en el software aplicativo y los sistemas de información de la entidad.
9. Considerar buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de los sistemas de información.
10. Proporcionar un nivel adecuado de soporte para solucionar los problemas que se presenten en el aplicativo; dicho soporte debe contemplar tiempos de respuesta aceptables.
11. Desarrollar sistemas de información que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.
12. Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como:
	* Tipos de datos
	* Rangos válidos
	* Longitud
	* Listas de caracteres aceptados
	* Caracteres considerados peligrosos
	* Caracteres de alteración de rutas.
13. Suministrar opciones de desconexión o cierre de sesión de los aplicativos (logout) que permitan terminar completamente con la sesión o conexión asociada, las cuales deben encontrarse disponibles en todas las páginas protegidas por autenticación.
14. Asegurar el manejo de operaciones sensibles o críticas en los aplicativos desarrollados permitiendo el uso de dispositivos adicionales como parámetros adicionales de verificación.
15. Asegurar que los aplicativos proporcionen la mínima información de la sesión establecida, almacenada en cookies y complementos.
16. Garantizar que no se divulgue información confidencial en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.
17. Remover todas las funcionalidades y archivos que no sean necesarios para los aplicativos, previo a la puesta en producción.
18. Prevenir la revelación de la estructura de directorios de los sistemas de información construidos.
19. Remover información innecesaria en los encabezados de respuesta que se refieran a los sistemas operativos y versiones del software utilizado.
20. Evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos. Dichas cadenas de conexión deben estar en archivos de configuración independientes, los cuales se recomienda que estén cifrados.
21. Certificar el cierre de la conexión a las bases de datos desde los aplicativos tan pronto como estas no sean requeridas.
22. Generar los controles necesarios para la transferencia de archivos, como:
	* Exigir autenticación
	* Vigilar los tipos de archivos a transmitir
	* Almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos.
	* Eliminar privilegios de ejecución a los archivos transferidos.
	* Asegurar que dichos archivos sólo tengan privilegios de lectura.
23. Proteger el código fuente de las aplicaciones construidas, de tal forma de que no pueda ser descargado ni modificado por los usuarios.
24. Asegurar que no se permite que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

Desarrollo Externo

Subdirección Administrativa o financiera o cualquier área o centro de costos, que contrate el desarrollo de software debe tener en cuenta los siguientes lineamientos:

1. Cuando se adquieran soluciones ya desarrolladas, se deberán definir con el proveedor previo a la adquisición, los procesos de administración de parches de la aplicación para asegurar que la misma no sea vulnerable, considerando referentes como OWASP.
2. Debe establecer acuerdos de confidencialidad del uso de los datos que pueda llegar a tener para efectos del producto a entregar.
3. Solicitar la generación de acuerdos de licenciamiento, propiedad de códigos y derechos de propiedad intelectual relacionados con el contenido contratado externamente.
4. Solicitar en los pliegos de los procesos las actividades relacionadas con el ciclo de vida del software teniendo en cuenta los requerimientos de seguridad y privacidad de la información de acuerdo con las necesidades de la Secretaria Distrital de Integración Social – SDIS.
5. Definir en los pliegos de los procesos los acuerdos de niveles de servicio relacionados a la calidad y seguridad de los entregables de los sistemas de información.
6. Implementar o utilizar protocolos de comunicación cifrados para intercambiar datos o funcionalidad con los sistemas de información de la Secretaria Distrital de Integración Social – SDIS

Datos de prueba

El área de infraestructura o quien haga sus veces debe:

1. Proteger los datos de prueba que se entregarán a los desarrolladores y personal de pruebas, asegurando que no revelan información confidencial de los ambientes de producción.
2. Garantizar que la información entregada para realizar las pruebas no revelará la información Pública Clasificada, Pública Reservada o sensible de los ambientes de producción.
3. Debe eliminar la información de los ambientes de pruebas, una vez estas han concluido.
4. Garantizar que, en caso de replicar información de producción a los ambientes de desarrollo, pruebas, preproducción esta sea ofuscada o anonimizada para protección de la confidencialidad de esta.
	1. Política de relaciones con los proveedores
		1. Objetivo(s):
* Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
* Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
	+ 1. Responsable(s) de la ejecución de la política:
* Subdirección de Contratación
* Subdirección de Investigación e información -SII
* Oficina Jurídica
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.15.1.1 Política de seguridad de la información para las relaciones con proveedores.
* A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores.
* A.15.1.3 Cadena de suministro de Tecnología de información y comunicación.
* A.15.2.1 Seguimiento y revisión de los servicios de los proveedores.
* A.15.2.2 Gestión de cambios en los servicios de los proveedores
	+ 1. Lineamientos:

La Secretaria Distrital de Integración Social – SDIS, establecerá mecanismos de control en sus relaciones con los proveedores, con el objetivo de asegurar que la información o servicios a los que tengan acceso, cumplan con las políticas y procedimientos de seguridad y privacidad de la información.

Los proveedores de la Secretaria Distrital de Integración Social – SDIS deben dar cumplimiento a los siguientes lineamientos:

1. Deberán contar con planes de contingencia, planes de emergencia, procesos y procedimientos de buenas prácticas en un SGSI (Sistema de gestión de seguridad de la información.)
2. Definir los procedimientos para la gestión de eventos, incidentes, contingencia y recuperación de la información asignada, alineados a los controles de seguridad y privacidad de la Secretaria Distrital de Integración Social – SDIS.
3. Realizar la devolución de activos físicos y/o lógicos, generados, modificados, y/o que tengan almacenados en sistemas de información diferentes a los autorizados por la Secretaria Distrital de Integración Social – SDIS.
4. Dar cumplimiento a los requisitos legales y de reglamentación para la protección de datos, derechos de propiedad intelectual, derechos de autor y los que apliquen a razón del cumplimiento contractual.
5. Guardar la confidencialidad respecto del tratamiento de los datos personales privados y sensibles contenidos en el intercambio de información de acuerdo con lo exigido por la ley 1581 de 2012, su decreto reglamentario y las políticas de protección de datos personales institucionales.
6. No deben utilizar y/o emplear la información que reciban de la contraparte, para fines distintos a los señalados.
7. Utilizar la información que reciba o conozca de la Secretaria Distrital de Integración Social – SDIS únicamente para los fines señalados en la relación contractual.

Los Supervisores de contrato de la Secretaria Distrital de Integración Social – SDIS deben dar cumplimiento a los siguientes lineamientos:

1. Definir los controles de seguridad para el acceso que tendrá el proveedor a la información; dependiendo el tipo de información, los activos entregados, generados procesados, consultados, transmitidos; el proveedor deberá dar cumplimiento a la Política de Seguridad y Privacidad de la Secretaria Distrital de Integración Social – SDIS.
2. Divulgar las políticas y procedimientos de seguridad y privacidad de la información a los proveedores respecto a la concienciación sobre el manejo de la información de la Entidad.
3. Llevar a cabo la evaluación respectiva de riesgos de seguridad y privacidad de la información asociada tanto a la información entregada, generada procesada, consultada, transmitida, eliminada, por los proveedores (terceros, aliados estratégicos).
4. Con el apoyo del Oficial de Seguridad de la Información – CISO revisar que se incluyan los acuerdos de confidencialidad y cumplimiento de políticas de seguridad de la Entidad en los contratos y/o acuerdos con los proveedores.

La Oficina de Control Interno de la Secretaria Distrital de Integración Social – SDIS deben dar cumplimiento a los siguientes lineamientos:

1. Realizar procesos de auditabilidad sobre el cumplimiento de acceso lógico y físico a nivel de los activos de información a los cuales se les ha brindado el permiso a los proveedores (terceros, aliados estratégicos) para consulta, modificación, uso, eliminación y generación de información.

La Subdirección Administrativa y Financiera y la Oficina Jurídica o quien haga sus veces deben dar cumplimiento a los siguientes lineamientos:

1. Incluir los requisitos de seguridad en los procesos de adquisición de productos y/o servicios de tecnología de la información y comunicaciones para la Secretaria Distrital de Integración Social – SDIS.
2. En todos los acuerdos, convenios, contratos con terceras partes, que implique un intercambio, uso o procesamiento de información de la Entidad, se debe solicitar la firma de acuerdos de confidencialidad sobre el manejo de la información.
3. Los acuerdos de confidencialidad de la información deben hacer parte integral de los contratos o documentos que legalicen la relación contractual.
4. Los acuerdos, convenios o contratos que requiera la suscripción de un anexo técnico asociado al intercambio, deben establecer un protocolo de intercambio de la información y se fijarán las condiciones técnicas y controles de seguridad que se utilizarán para proteger la información.

La Subdirección de Investigación e información -SII a través del área de servicios o quien haga sus veces:

1. Debe establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la entidad.
2. Identificar y Mitigar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la Secretaria Distrital de Integración Social – SDIS.

La Subdirección de gestión y desarrollo de talento o quien haga sus veces:

1. Con el apoyo de la Subdirección de Investigación e información -SII y el CISO, deben generar una guía base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad informática, con los que deben cumplir los proveedores de servicios; dicha guía debe ser divulgado a todas las áreas que adquieran o supervisen recursos o servicios tecnológicos.
2. Elaborar modelos de Acuerdos de Confidencialidad y Acuerdos de Intercambio de Información con terceras partes. De dichos acuerdos deberán derivarse una responsabilidad tanto civil como penal para la tercera parte contratada.
	1. Política de gestión de incidentes de seguridad de la información
		1. Objetivo(s):

Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.

* + 1. Responsable(s) de la ejecución de la política:
* Subdirección de Investigación e información -SII
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.16.1.1 Responsabilidades y procedimientos.
* A.16.1.2 Reporte de eventos de seguridad de la información.
* A.16.1.3 Reporte de debilidades de seguridad de la información.
* A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.
* A.16.1.5 Respuesta a incidentes de seguridad de la información.
* A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información.
* A.16.1.7 Recolección de evidencia.
	+ 1. Lineamientos:

Comunidad de la Secretaria Distrital de Integración Social – SDIS:

1. Todos los colaboradores deben reportar a través de la mesa de ayuda; los eventos o incidentes relacionados con la seguridad de la información o con los recursos tecnológicos con la mayor prontitud posible a través de los canales definidos.
2. El reporte de incidentes de seguridad debe contener un mínimo de datos para poder dejar evidencia y soporte de las acciones realizadas, las cuales se deben registrar en el procedimiento definido y que debe estar alineado con la política de seguridad de la información.

La Subdirección de Investigación e información -SII:

1. Los incidentes de seguridad de la información pueden ser detectados por alertas de sistemas de información, colaboradores, proveedores o entidades externas que observen situaciones anormales o la existencia de vulnerabilidades, relacionadas con aspectos técnicos, físicos o procedimentales, que puedan afectar a la infraestructura tecnológica, información física, digital o electrónica, entre otros activos de información.
2. La Subdirección de Investigación e información -SII, realizarán el seguimiento y gestión del tratamiento de los incidentes de seguridad de la información.
3. La Subdirección de Investigación e información -SII debe asignar responsables para el tratamiento de los eventos e incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.
4. Los Directores, Subdirectores o el Oficial de Seguridad - CISO de la entidad, serán las únicas personas autorizadas para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.
5. La Subdirección de Investigación e información -SII con el apoyo de la Dirección de análisis y diseño estratégico deben establecer las responsabilidades y procedimientos para asegurar una respuesta rápida, ordenada y efectiva frente a los incidentes de seguridad de la información.
6. La Subdirección de Investigación e información -SII deben documentar una base de conocimiento con los incidentes de seguridad presentados con sus respectivas soluciones, con el fin de reducir el tiempo de respuesta para los incidentes futuros, partiendo de dichas bases de conocimiento.
7. Deben comunicar a los colaboradores sobre la gestión incidentes, lineamientos, recomendaciones y buenas prácticas con el fin de minimizar la ocurrencia de estos.

El área de gestión de soporte y mantenimiento tecnológico en conjunto con los responsables de la atención del incidente deben:

1. Documentar en la herramienta de gestión designada para tal fin; todos los incidentes presentados, como mecanismo de seguimiento, análisis y control de estos, diligenciando de manera clara, concisa y precisa.
2. Definir los mecanismos para el análisis, contención y erradicación eficiente de los incidentes de seguridad de la información.
3. Identificar los riesgos materializados asociados para su registro o reevaluación en la gestión de riesgos.
4. Si el incidente se presenta por acción, omisión o extralimitación de funciones u obligaciones que van en contravía de la seguridad de la información, se procederán a las investigaciones correspondientes.
	1. Política aspectos de seguridad de la información de la gestión de continuidad de negocio
		1. Objetivo(s):
* La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.
* Asegurar la disponibilidad de instalaciones de procesamiento de información.
* Garantizar la continuidad tecnológica y operacional.
	+ 1. Responsable(s) de la ejecución de la política:
* Dirección de análisis y diseño estratégico
* Subdirección de Investigación e información -SII
* Gestión de soporte y mantenimiento tecnológico
* Subdirección de diseño, evaluación y sistematización
	+ 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.17.1.1 Planificación de la continuidad de la seguridad de la información.
* A.17.1.2 Implementación de la continuidad de la seguridad de la información.
* A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
* A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.
	+ 1. Lineamientos:

La Subdirección de diseño, evaluación y sistematización debe:

1. Realizar periódicamente el Análisis de Impacto de Negocio – BIA identificando la criticidad de los aspectos relacionados a la prestación de productos o servicios críticos de la entidad.
2. Asegurar la continuidad del componente de seguridad de la información ante la ocurrencia de eventos no previstos a través de un Plan de Continuidad de Negocio y un Plan de Recuperación de Desastres a cargo de la Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico.
3. Establecer y ejecutar un plan de pruebas periódico del plan de Continuidad de Negocio que permita evaluar los niveles de recuperación que requiere la entidad, así como los requerimientos de seguridad, funciones, responsabilidades relacionadas con el plan.
4. Asignar roles y responsabilidades detallados en el Plan de Continuidad del Negocio a personal idóneo para la atención de los incidentes de Continuidad del Negocio.
5. Incluir en el plan de concientización y sensibilización información con respecto al uso y apropiación de los temas de Continuidad del Negocio de forma tal que los colaboradores reaccionen de manera eficiente ante un incidente que comprometa su seguridad y el desarrollo de sus actividades en los procesos o la prestación de sus servicios.
6. En caso de presentarse un incidente significativo que conlleve una interrupción de los servicios, se debe gestionar el manejo de la crisis y los mecanismos de comunicación apropiados durante el estado de contingencia.
7. Los procesos que sean desarrollados por terceros deben disponer de planes de continuidad, en caso de que sus actividades afecten el cumplimiento de la misionalidad de la Secretaria Distrital de Integración Social – SDIS y probarlos regularmente.
8. Se debe garantizar que los planes de continuidad del negocio se ejecuten de forma segura sin exponer la información de la entidad.
	1. Política de cumplimiento
		1. Objetivo(s):
* Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.
* Garantizar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
	+ 1. Responsable(s) de la ejecución de la política:
* Oficina Jurídica
* Oficina de Control Interno
* Oficina de asuntos Disciplinario
* Subdirección de Investigación e información -SII
* Dirección de Análisis y Diseño Estratégico
* Subdirección Administrativa y Financiera

* + 1. Responsable(s) del cumplimiento de la política:
* Directores, Subdirectores y Lideres de procesos
* Apoyos a la supervisión de contratos.
* Todos los colaboradores de la Secretaria Distrital de Integración Social – SDIS
	+ 1. Controles que abarca la norma NTC-ISO-27001:2013 Anexo A:
* A.18.1.1 Identificación de la legislación aplicable y de los requisitos Contractuales.
* A.18.1.2 Derechos de propiedad intelectual.
* A.18.1.3 Protección de registros.
* A.18.1.4 Privacidad y protección de información de datos personales.
* A.18.1.5 Reglamentación de controles criptográficos.
* A.18.2.1 Revisión independiente de la seguridad de la información.
* A.18.2.2 Cumplimiento con las políticas y normas de seguridad.
* A.18.2.3 Revisión del cumplimiento técnico.
	+ 1. Lineamientos:

Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas (Secretaria Distrital de Integración Social – SDIS deben dar cumplimiento a los siguientes lineamientos:

1. Está prohibido la descarga, instalación o utilización de aplicativos o programas informáticos que no se encuentren autorizados por la Subdirección de Investigación e información -SII. En caso de presentarse este tipo de eventos, serán considerados como una violación a las Políticas de Seguridad y Privacidad de la Información de la Secretaria Distrital de Integración Social – SDIS.
2. Está prohibido la descarga e instalación de software ilegal o no autorizado por la Secretaria Distrital de Integración Social – SDIS, el incumplimiento o violación de derechos de autor puede acarrearle al Colaborador consecuencias disciplinarias
3. Dar cumplimiento a la Política de Protección de Datos Personales, manual de protección de datos y sus procedimientos inmersos de la Secretaria Distrital de Integración Social – SDIS.

La Subdirección de Investigación e información -SII de la Secretaria Distrital de Integración Social – SDIS debe:

1. Adquirir software respetando los derechos de autor verificando y controlando el licenciamiento, así como los términos de uso.
2. Certificar que todo el software que se ejecuta en la institución esté protegido por derechos de autor y requiera licencia de uso o en su lugar sea software de libre distribución y uso.
3. Designar personal para instalar, configurar y dar soporte a los equipos de cómputo y dispositivos de la entidad.
4. Definir y mantener actualizado el listado de programas y software permitido que cumplan con la reglamentación de derechos de autor, licencias y usos.
5. Implementar controles para la instalación, desinstalación y uso adecuado de programas y software en los equipos institucionales.
6. Es la única área autorizada para la adquisición y administración de software y licenciamiento.
7. Verificar periódicamente que los sistemas de información, servicios e infraestructura tecnológica cumple con los lineamientos de seguridad de la información.

La Oficina de Control Interno Disciplinario de la Secretaria Distrital de Integración Social – SDIS debe:

1. Definir lineamientos para investigar los incumplimientos en la política de Seguridad y Privacidad de la Secretaria Distrital de Integración Social – SDIS el cual podría iniciar un proceso disciplinario.

El área de Gestión Documental o quien haga sus veces debe:

1. Definir lineamientos y controles para conservar la información contenida en los archivos físicos, electrónicos o digitales de la Secretaria Distrital de Integración Social – SDIS, en las condiciones adecuadas y dar cumplimiento a los lineamientos que imparte el Archivo General de la Nación para el clico de vida de la información institucional.

La Dirección de Análisis y Diseño Estratégico debe:

1. Con el apoyo de la oficina Jurídica y el CISO; documentar, publicar, implementar y divulgar la política de Protección de Datos Personales de la Secretaria Distrital de Integración Social – SDIS, para dar cumplimiento a las disposiciones consagradas en la Constitución Política de Colombia, contemplados en los artículos 15 y 20, la Ley 1286 de 2008, la Ley Estatutaria 1581 de 2012 y sus decretos reglamentarios o cualquiera que los sustituya, derogue, adicione o complemente.
2. Definir lineamientos respecto a la implementación y cumplimiento del SGSI, y de la privacidad y protección de información de datos personales.
3. Hacer seguimiento al cumplimiento de las políticas, procedimientos, guías, y demás instrumentos del SGSI.
4. Validar el cumplimiento de la normativa vigente aplicable al tratamiento de datos personales.
5. Apoyar la definición de conceptos asociados al tratamiento datos personales.
6. Definir y divulgar la política y manual de tratamiento de datos personales y avisos de privacidad de la entidad.
7. Articular los procesos de SGSI con la alta consejería TIC del distrito.

La Oficina de Control Interno la Secretaria Distrital de Integración Social – SDIS debe:

1. Realizar las auditorías internas al Sistema de Gestión de Seguridad de la Información de la Secretaria Distrital de Integración Social – SDIS, realizando la revisión independiente de los objetivos de control, controles, políticas, procesos y procedimientos.

La Oficina Jurídica de la Secretaria Distrital de Integración Social – SDIS debe:

1. Identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la Secretaria Distrital de Integración Social – SDIS, relacionados con seguridad de la información.
2. Definir y establecer un procedimiento para verificar los requisitos legales aplicables a la Secretaria Distrital de Integración Social – SDIS
3. Definir y asesorar a las dependencias respecto a los derechos de propiedad intelectual para:
* Mantener la propiedad intelectual de la Secretaria Distrital de Integración Social – SDIS en lo que respecta a código fuente, programas, documentos, derechos de diseño, marcas registradas, patentes, licencias, piezas gráficas, audiovisual, entre otros, cuando las demás dependencias lo requieran.
* Establecer los lineamientos para el cumplimiento de los derechos de autor conforme a la normativa vigente.

La Subdirección Administrativa y Financiera en conjunto con la Oficina Jurídica o quien haga sus veces deben dar cumplimiento a los siguientes lineamientos:

1. Identificar la legislación y los requisitos aplicables a los procesos contractuales.
2. Incluir cláusulas de seguridad y privacidad de la información en los procesos contractuales que aplique, teniendo en cuenta la naturaleza de la ejecución y los activos de información involucrados.
3. Definir y hacer cumplir las directrices para la protección de los registros e información institucional en cuanto a su almacenamiento, manejo y disposición final.

Los Directores, Subdirectores, lideres de proceso, Tecnologías de la información y la gestión de soporte y mantenimiento tecnológico y el ciso, como lideres de los procesos establecidos en la entidad, deben apoyar las revisiones del cumplimiento de las políticas de seguridad y privacidad de la información.

1. Evaluación del lineamiento o Política interna

La evaluación del lineamiento se realizará a través de la aplicación de la herramienta de verificación de controles implementados MSPI de acuerdo con la Política de Seguridad de la información y mediante los informes de seguimiento respectivos.

1. Responsabilidades y competencias

Las responsabilidades de ejecutar este lineamiento, cumplirlo a cabalidad y sin excepciones son todos los funcionarios, contratistas y visitantes de la Secretaria de Integración Social, de acuerdo con lo descrito en los numerales de Responsable(s) del cumplimiento de cada una de las políticas definidas.

1. Administración del lineamiento

Subdirección de Investigación e Información

1. Aprobación del documento

|  |  |  |  |
| --- | --- | --- | --- |
|  | Elaboró | Revisó | Aprobó |
| Nombre | Edna Rocio Univio AmayaJaime Guerrero Clavijo | Mayra Andrea Ruiz Bello | Franky Gonzalez Daza |
| Cargo/Rol | Contratista – Subdirección de Investigación e informaciónContratista – Subdirección de Investigación e información | Gestora SG del proceso Tecnologías de la información | Subdirector de Investigación e información |