MANUAL DEL SUBSISTEMA GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN-SGSI

SECRETARÍA DISTRITAL DE INTEGRACION SOCIAL

ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE INTEGRACIÓN SOCIAL

BOGOTÁ D.C., 2018

TABLA DE CONTENIDO

Contenido

OBJETIVO 3
ALCANCE 3
NORMATIVIDAD 3
TÉRMINOS Y DEFINICIONES 4
GENERALIDADES 6
I. DOMINIO POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN 7
A. Políticas para la seguridad y privacidad de la información 7
B. Compromiso de la alta dirección con la seguridad de la información 8
II. DOMINIO ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 8
C. Comité de Seguridad de la Información 9
D. Teletrabajo 9
III. DOMINIO SEGURIDAD DEL RECURSO HUMANO 10
E. Antes de asumir el empleo 10
F. Durante la ejecución del empleo 11
G. Al terminar o cambiar de empleo 12
IV. DOMINIO GESTIÓN DE ACTIVOS 13
H. Inventario y responsabilidad de los activos 13
I. Clasificación de la información de la SDIS 15
J. Uso aceptable de los activos 17
K. Del manejo de la información 20
L. Manejo de medios 21
M. Devolución de activos 22
V. DOMINIO CONTROL DEL ACCESO 22
VI. DOMINIO CRIPTOGRAFÍA 24
VII. DOMINIO SEGURIDAD FÍSICA Y DEL ENTORNO 24
N. Seguridad del cableado 26
O. Equipos y documentos físico desatendidos 27
P. Protección contra código malicioso 28
Q. Copia de respaldo de información 29
IX. DOMINIO GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN 31

OBJETIVO

Desarrollar las directrices generales y lineamientos que conforman la política de seguridad y privacidad de la información a través de la gestión segura de los activos de información, que debe conocer y cumplir todos los funcionarios, contratistas y terceros de la Secretaría Distrital de Integración Social-SDIS.

ALCANCE

Comprende directrices generales y lineamientos de seguridad y privacidad de la información que serán aplicadas para los aspectos operativos, administrativos y de control, que deben ser cumplidas por los funcionarios, contratistas y terceros de la SDIS y hacen parte del Sistema Integrado de Gestión, del Subsistema Seguridad de la Información.

NORMATIVIDAD

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

- 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”
- Norma Técnica Colombiana ISO-27001 Sistema de Gestión de Seguridad de la Información e ISO-27002 guía de buenas prácticas de seguridad de la información.
- ResoluciónN°1564 de 2010 “Por la cual se creó el Comité de Seguridad de la Información CSI y define sus funciones”.
- Resolución N°0635 de 2017 “Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social”, y todas aquellas normas allí contenidas.
- NTD SIG 001:2011 Norma Técnica Distrital del Sistema Integrado de Gestión para las entidades y organismos distritales.
- Decreto 1499 de 2017. Por medio de la cual se modifica el Decreto 1083 de 2015, Decreto único reglamentario de la función pública, en lo relacionado con el Sistema de Gestión establecido en el artículo de la ley 1753 de 2015.

TÉRMINOS Y DEFINICIONES

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[1]:

- 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 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[2].

Base de datos: es una colección de información organizada con el propósito que sea fácilmente accesible, administrada y actualizada.

[1] ISO/IEC 13335-12004.
[2] ISO/IEC 27000.

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[3].

Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información en todos los servicios de la entidad[4].

Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados[5].

Integridad: propiedad que busca proteger que se modifiquen los datos libres de forma no autorizada[6].

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[7].

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[8].

Riesgo de información: es el proceso sistemático de identificación de fuentes, gestión y estimación de impactos, probabilidades comparando estos componentes contra criterios de

[3] ISO/IEC 27000.
[4] ISO/IEC 27001.
[5] Ibíd.
[6] Ibíd.
[7] Ibíd.
[8] ISO/IEC 27035

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[9].

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.

GENERALIDADES

El manual se desarrolla de acuerdo con la política de seguridad y privacidad de la información y los dominios establecidos en la norma técnica NTC-ISO/IEC COLOMBIANA 27002, para los cuales se indicará su concepto, objetivos, directrices generales y se listarán los subdominios que serán de aplicación y obligatorio cumplimiento en la Entidad.

[9] Ley 1581 de 2012.

I. DOMINIO POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

El dominio de políticas de seguridad brinda apoyo y orientación a la Secretaría Distrital de Integración Social con respecto a la seguridad de la información, por lo cual, se creó la Política de Seguridad y Privacidad de la Información. Para la SDIS se establecen directrices generales para los siguientes subdominios:

A. Políticas para la seguridad y privacidad de la información

Debido a que la información es uno de los activos más importantes de la entidad, así como la necesidad de su protección, la SDIS por medio del Sistema de Gestión de Seguridad de la Información – SGSI tiene como propósito garantizar la seguridad de la información en los aspectos de confidencialidad, integridad y disponibilidad de la información.

El objetivo del subdominio de políticas de seguridad y privacidad de la información es establecer controles, mecanismos y estrategias que permitan mitigar los riegos sobre la triada de la información de la información de la SDIS. De igual forma se busca implementar directrices generales que permitan el manejo adecuado de la información y controlar los incidentes de seguridad de la información presentados en la SDIS.

Directrices generales:

- Los funcionarios y contratistas son responsables de la protección de la información de la entidad a la cual acceden y/o procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, además de reportar los incidentes de seguridad de la información, eventos sospechosos y el mal uso de los recursos.

- La SDIS a través de la Dirección de Gestión Corporativa, debe implementar controles para proteger el perímetro de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas. Además, mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la entidad.

- La SDIS a través de la Subdirección de Investigación e Información, diseñará e implementará controles y estrategias para proteger la información generada, recolectada, procesada y utilizada en el cumplimiento de su misión.

- La SDIS a través de la Subdirección de Investigación e Información se debe encargar de la operación y administración de los recursos tecnológicos que soportan la operación de la entidad e implementar los controles asociados a éstos para proteger la confidencialidad, integridad y disponibilidad de la información.

- De manera conjunta la Subdirección de Investigación e Información y la Subdirección Administrativa y Financiera por medio del grupo de Gestión Documental – SIGA, debe establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información, con el objetivo de garantizar su protección.

- La Subdirección de Investigación e Información definirá de acuerdo con la clasificación de la información, cuáles datos deben ser cifrados y dará las directrices generales necesarias para la implementación de los respectivos controles (dispositivos a emplear, mecanismos de administración de claves, políticas de uso de sistemas de cifrado de datos).

B. Compromiso de la alta dirección con la seguridad de la información

La alta dirección debe apoyar activamente la seguridad de la información dentro de la entidad con un compromiso constante y el conocimiento de las responsabilidades de la seguridad de la información.

Directrices generales:

- Asegurar que las metas de la seguridad de la información están alineadas con la estrategia de la entidad e integradas los procesos institucionales.
- Validar que se mantenga actualizada la política de seguridad de la información.
- La política de seguridad y privacidad de la información se debe revisar una vez al año o cuando se producen cambios significativos, para garantizar que sigue siendo adecuada, suficiente y eficaz.
- Coordinar en toda la entidad la implementación de los controles de seguridad de la información.

II. DOMINIO ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Este dominio busca establecer lineamientos que permitan formar un marco de referencia de gestión para iniciar, controlar la implementación y operación de la seguridad de la información en la SDIS, para lo cual se establecen directrices generales para los siguientes subdominios:

Directrices generales:

- Todos los procesos de la SDIS en el marco del desarrollo de sus proyectos deben tener un componente de seguridad de la información, el cual será acompañado y asesorado por el gestor de seguridad de la información.

- La responsabilidad de la información debe estar en a cargo del dueño de los procesos para evitar conflicto en cuanto a responsabilidades. Lo anterior permite reducir oportunidades de modificación intencional, no autorizada o mal uso de los activos de información de la entidad.

- El gestor del Subsistema de Gestión Seguridad de Información debe mantener contacto con autoridades en materia de seguridad de la información tales como Policía Nacional, Bomberos, Instituto Distrital de Gestión de Riesgos y cambio Climático-IDIGER. Temas relacionados con buenas prácticas o normatividad de seguridad de la información debe ser divulgados a los funcionarios y contratistas de la entidad.

C. Comité de Seguridad de la Información

Es la instancia encargada de asegurar que exista una dirección y apoyo de la alta dirección para soportar la administración y desarrollo de iniciativas sobre seguridad de la información, a través de compromisos apropiados y uso de recursos informáticos adecuados en la SDIS, así como el mantenimiento de la política de seguridad y privacidad de la información a través de todo el organismo. Estáregulado bajo la Resolución 1075 de 30 de junio de 2017, en donde se pueden encontrar las directrices generales en el capítulo 2, así como su objetivo, integrantes, funciones, periodos de sesión, entre otras.

D. Teletrabajo

Este subdominio busca proteger la información a la que se tiene acceso, procesada y/o almacenada en los sitios que se realiza la modalidad de teletrabajo.

Directrices generales:

- Para la modalidad de teletrabajo, la Subdirección de Gestión y Desarrollo del Talento Humano, debe establecer y hacer cumplir los lineamientos necesarios para los funcionarios y/o contratistas postulados a teletrabajo.
- Para llevar a cabo las actividades laborales en la modalidad de teletrabajo, la Subdirección de Investigación e Información debe brindar infraestructura tecnología tales como; VPN, herramientas ofimáticas, disponibilidad de aplicaciones, etc. y de seguridad de la información, para toda aquella información que sea procesada, almacenada y gestionada por parte de los teletrabajadores.

- Está prohibido el acceso no autorizado a información o recursos de la SDIS, por parte de personas que usan el mismo entorno físico del teletrabajador, como familiares, amigos, etc.

III. DOMINIO SEGURIDAD DEL RECURSO HUMANO

El dominio de seguridad del recurso humano se pretende asegurar que los funcionarios y contratistas de la SDIS, cumplan con los procesos de selección, permanencia y desvinculación para así reducir los riesgos como hurto, fraude, y uso inadecuado de la información, para la SDIS se establecen directrices generales para los siguientes subdominios:

E. Antes de asumir el empleo

Este subdominio busca asegurar que los funcionarios y contratistas adquieran sus responsabilidades de acuerdo con los perfiles de los postulantes.

Directrices generales:

- La Subdirección de Gestión y Desarrollo del Talento Humano debe definir controles de validación y verificación del personal en el momento en que se postule al cargo. Estos controles incluirán aspectos legales y de procedimiento.

- La Subdirección de Contratación debe hacer cumplir las listas de chequeo por modalidad de contratación, para realizar la revisión de los antecedentes del personal a contratar por prestación de servicios de acuerdo con lo que establece la Ley y reglamentación vigente.

- La Subdirección de Contratación debe incluir en el pliego de condiciones, de la contratación de terceras partes, la obligación referente a las políticas, lineamientos y directrices generales en materia de seguridad de la información que establece la SDIS.

Términos y condiciones del empleo: Los acuerdos contractuales con funcionarios y contratistas deben establecer las responsabilidades laborales y las de la entidad a nivel de Seguridad de la Información.

- Todos los funcionarios y contratistas deben contar con una inducción respecto de las Políticas de Seguridad de la Información, la cuál será realizada por el Gestor de Talento Humano..

- Para los funcionarios y contratistas a los que se les permita el acceso a información de carácter reservada, y no divulgación deberían firmar un acuerdo de confidencialidad y no divulgación de la misma, antes de tener acceso al procesamiento de información.

- Es responsabilidad de los funcionarios y contratistas el manejo de la información recibida de entidades externas.

- Es responsabilidad de los funcionarios y contratistas la gestión de la información, el tratamiento de la misma y otros activos asociados con información.

F. Durante la ejecución del empleo

Este subdominio busca asegurar que los funcionarios y contratistas se sensibilicen de las responsabilidades sobre la Seguridad de la información y se cumplan.

Directrices generales:

- La Subdirección de Gestión y Desarrollo del Talento Humano y la Subdirección de Contratación deben incluir en los documentos que dispongan las responsabilidades en materia de seguridad de la información para personal de planta y contratistas.

- Los jefes inmediatos y/o supervisores de las dependencias son responsables de solicitar usuario de red, usuario de aplicaciones, cuenta de correo electrónico institucional, etc. para los nuevos funcionarios, contratistas y pasantes, a través de la herramienta destinada para tal fin, de acuerdo al procedimiento de solicitud de creación y modificación de usuarios.

- El jefe inmediato y/o supervisor es responsable de solicitar credenciales y autorizaciones de acceso a los servicios y sistemas de información para los nuevos funcionarios y contratistas de acuerdo con sus funciones y responsabilidades, a través de la herramienta destinada para tal fin.

- Todo software usado en la plataforma tecnológica de la SDIS debe tener su respectiva licencia y acorde con los derechos de autor.

- Los programas instalados en los equipos, son de propiedad de la SDIS, la copia no autorizada de programas o de su documentación, implica una violación a la política general de seguridad y privacidad de la información de la SDIS. Aquellos funcionarios y contratistas que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la SDIS o las sanciones que especifique la ley.

- Los recursos tecnológicos y de software asignados a los funcionarios y contratistas de la SDIS son responsabilidad de cada uno.

- Los funcionarios y contratistas son los responsables de la información que administran en sus equipos y debe abstenerse de almacenar en ellos información no institucional.

- Es responsabilidad de cada funcionario y contratista proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos institucionales.

- Cualquier evento o posible incidente que afecte la Seguridad de la Información, debe ser reportado inmediatamente a la mesa de servicio de la Subdirección de Investigación e Información.

Directrices generales para la responsabilidad de la Dirección

- La Secretaria de Despacho exigirá a todos los funcionarios y contratistas el cumplimiento de la Seguridad de la Información de acuerdo con las políticas y procedimientos establecidos por la SDIS.

- Los funcionarios y contratistas deben estar debidamente informados sobre las funciones y responsabilidades de Seguridad de la Información, antes que se otorgue el acceso a la información o sistemas con información confidencial.

- Todo reporte de incumplimiento de la Política de Seguridad de la Información debe ser informado a través de los canales de la mesa de servicio autorizados por la Subdirección de Investigación e Información.

- Los funcionarios y contratistas que tengan continuamente capacitación en Seguridad de la Información si así lo requieren.

G. Al terminar o cambiar de empleo

Este subdominio busca proteger los intereses de la entidad como parte del proceso de cambio o terminación del empleo.

Directrices generales:

- La Subdirección de Gestión y desarrollo del Talento Humano debe informar oportunamente las novedades de los funcionarios, (cambio de rol y/o responsabilidades, traslados entre otros) a la Subdirección de Investigación e Información para que aplique los procedimientos de actualización de los permisos de acceso a la red y los activos de información asociados al colaborador.

- La Subdirección de Contratación debe informar oportunamente las novedades del personal vinculado por prestación de servicios, (terminación anticipada del contrato, aplazamiento de contratos, etc.) a la Subdirección de Investigación e Información para que aplique los procedimientos de desactivación del usuario en los sistemas de información y los activos de información asociados al contratista.

- Todos los funcionarios y contratistas de la SDIS deben devolver los activos de propiedad material e intelectual que pertenezcan a la SDIS, de acuerdo con las actas de entrega en caso de activos físicos y los manuales de funcionalidades en caso de activos lógicos o de información, de acuerdo a las directrices establecidas por cada dependencia.

- Cuando un funcionario o contratista cese sus funciones o culmine la ejecución de un contrato en la SDIS, el jefe inmediato o supervisor del contrato será el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual de acuerdo con la normativa vigente.

- Entregar el carnet o cualquier medio de autenticación, que lo acredita como funcionario y/o contratista de la entidad y retiro inmediato del mismo, la entrega debe ser a la dependencia encargada del proceso de autenticación física.

IV. DOMINIO GESTIÓN DE ACTIVOS

Este dominio busca establecer y proteger adecuadamente los activos de información de la SDIS, mediante la definición de los responsables de su administración de acuerdo a las responsabilidades de los funcionarios y contratistas de la SDIS.

Directriz general:

Los activos de información, aplicaciones, herramientas tecnológicas y servicios tecnológicos, asignados por la SDIS son para uso exclusivo del cumplimiento de las funciones y obligaciones designadas; razón por la cual la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos se considera propiedad de la entidad y el uso inadecuado de dichos recursos puede conllevar a sanciones disciplinarias y legales correspondientes.

H. Inventario y responsabilidad de los activos

Este subdominio busca identificar los activos de la entidad y mantener la protección de los activos de información mediante la asignación de estos a los funcionarios y contratistas que deban administrarlos de acuerdo con sus roles, funciones y obligaciones.

Directrices generales:

- La SDIS es propietaria de los activos de información y los administradores de estos activos son los funcionarios y contratistas de la SDIS que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología de información y comunicaciones (TIC).

Los Subdirectores y Directores de las dependencias deben mantener un inventario de sus activos de información con tipología datos de manera anual y serán actualizados según el evento en que se requiera realizar después del registro inicial

- Todos los requerimientos de aplicativos, sistemas y equipos informáticos debe ser solicitados a través de la mesa de servicio de la Subdirección de Investigación e Información con su correspondiente justificación para su respectiva viabilidad.

- En caso de ser necesario y previa autorización de la Subdirectora de Investigación e Información, los funcionarios y contratistas de la SII de la SDIS podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de internet o de cualquier otra red o medio, en los equipos informáticos a su cargo.

- La Subdirección de Investigación e Información efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos no autorizados será considerado como una violación a la política de Seguridad y Privacidad de la Información de la SDIS.

- Los recursos informáticos de la SDIS no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.

- Los funcionarios y contratistas no podrán efectuar ninguna de las siguientes labores sin previa autorización de la Subdirección de Investigación e Información:

    - ✓ Instalar software en cualquier equipo de la SDIS.
    - ✓ Bajar o descargar software de internet u otro servicio en línea en cualquier equipo de la SDIS.
    - ✓ Modificar, revisar, transformar o adaptar cualquier software propiedad de la SDIS.
    - ✓ Copiar o distribuir cualquier software propiedad de la SDIS.

- La Subdirección de Plantas Físicas, debe llevar y administrar el inventario valorizado de Hardware de propiedad de la SDIS, discriminado por dependencias.

- En el momento de desvinculación o cambio de labores, los funcionarios y contratistas debe realizar la entrega de su puesto de trabajo jefe inmediato, supervisor del contrato o quien este delegue; así mismo, debe encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación, de acuerdo al procedimiento vinculación y desvinculación.

Clasificación de los activos

Los activos de información serán clasificados de acuerdo con un tipo y clase en la SDIS:

Tipo de activo	Clase de activo
Activos de información	Información digital
	Información física
	Activos de información tipo datos
Activos de tecnologías de la información	Software
	Hardware de TI
	Servicios de TI

Tabla 1. Clasificación de activos de información, basado en la metodología establecida en el Décimo Primer Lineamiento del Sistema Integrado de Gestión Distrital.

Valoración de los activos de información

La valoración del activo de Información se realiza mediante la identificación del impacto para la SDIS por la pérdida de los componentes (confidencialidad, integridad y disponibilidad) de la seguridad de la información, teniendo en cuenta la siguiente tabla de valoración:

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todos los componentes (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus componentes o al menos uno de ellos es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus componentes es baja.

Tabla 2: Niveles de valoración, basado en la guía para la gestión y clasificación de activos de información de MinTIC.

I. Clasificación de la información de la SDIS

Este subdominio busca asegurar que la información tenga un nivel de protección adecuado de acuerdo a la clasificación establecida en el Décimo Primer Lineamiento del Sistema Integrado de Gestión Distrital, la Ley 1712 de 2014, etc. Se considera información toda forma de comunicación o datos digitales, escritos en cualquier medio (magnéticos, visual, papel, digital etc.), que genere la SDIS.

Ejemplo:

- ✓ Formularios, formatos, comprobantes con proveedores etc.

- ✓ Información en los sistemas (misionales, apoyo), equipos informáticos, medios Magnéticos/electrónicos o medios físicos (papel).
- ✓ Otros soportes magnéticos/electrónicos removibles, móviles o fijos.

La información que se maneja en la SDIS tiene diferentes niveles de criticidad en cuanto al riesgo que representa su divulgación, adulteración o indisponibilidad. Por lo anterior, se hace necesario diferenciar la información según el nivel de riesgo que genera su compromiso.

Clasificación de Información	
Categoría	**Descripción**
Información pública reservada	Es aquella información que tiene establecido el carácter de “Dato Sensible”, ya que afecta la intimidad de las personas y su uso indebido puede generar discriminación. El acceso a este tipo de información, el almacenamiento y transmisión están restringidos, solo a aquellos funcionarios y contratistas que se encuentren autorizados por el propietario de la información y su divulgación solo se podrá realizar bajo los parámetros establecidos en la ley 1581. La clasificación de la información y su manejo para dar cumplimiento a la normatividad vigente está a cargo de los administradores funcionales de los sistemas de información y de los funcionarios y contratistas encargados de las bases de datos para su protección. Así mismo, las dependencias que gestionan los documentos físicos que contienen información sensible son las responsables de su custodia.
Información pública clasificada	Es aquella información que, con base en el análisis de riesgo, ha sido clasificada como confidencial por que ha sido restringida a un grupo de funcionarios y contratistas o área en particular. Para su divulgación, se requiere el consentimiento del propietario de la información. También pertenece a esta categoría la información exceptuada por daño de derechos a personas jurídicas. Que corresponde a procesos internos confidenciales, así como la información de participantes de los diferentes proyectos sociales de la SDIS y los datos clasificados como “Datos personales” de acuerdo con la Ley 1581 de 2012, encontrándose datos privados, semiprivados y datos sensibles.
Información Publica	Es aquella información que puede ser distribuida abiertamente al público sin que cause daño alguno a la entidad, a sus funcionarios y contratistas, otras áreas o a otras entidades. Esta categorización solo puede ser asignada por el propietario de la información. Para datos personales de acuerdo con la Ley 1581, se encuentran los datos públicos.

Tabla 3. Conceptos de la legislación vigente y estándares internacionales (Ley 1581, Ley de Transparencia, ISO 27000)

Se deben firmar acuerdos de confidencialidad respectivos con terceros, que incluyan el seguimiento y cumplimiento de las prácticas de gestión segura de la Información establecido en la Política de Seguridad de la Información. Igualmente, si la Información clasificada por la SDIS es requerida por algún ente externo, su entrega está sujeta a la aprobación previa de su responsable y de las instancias establecidas.

J. Uso aceptable de los activos

Todos los funcionarios y contratistas que hagan uso de los activos de la SDIS tienen la responsabilidad de dar cumplimiento a las siguientes directrices generales establecidas para el uso aceptable de los activos de información, entendiendo que el inadecuado de los recursos puede poner en peligro la continuidad de la prestación de los servicios sociales y generar sanciones de acuerdo con las normas y legislación vigente.

Lineamiento de navegación y uso de aplicaciones web

El servicio de Internet suministrado por Secretaría Distrital de Integración social - SDIS, es una herramienta de apoyo a las funciones y responsabilidades de los funcionarios y contratistas, de acuerdo con lo establecido en el lineamiento de navegación y uso de aplicaciones web, por lo tanto, su utilización debe establecer y cumplir las directrices generales que a continuación se mencionan:

- El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación está totalmente prohibidos y su detección será tratada como un incidente de seguridad.

- El bajar archivos provenientes de Internet implica un riesgo para la seguridad de la información, por lo cual se solicita que únicamente se haga cuando sea necesario; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, .pig.

Perfiles de navegación y uso de aplicaciones web

- La Secretaría Distrital de Integración Social cuenta con los perfiles de navegación y uso de aplicaciones web definidos en el lineamiento de navegación y uso de aplicaciones web, estos han sido definidos de acuerdo a las necesidades de los funcionarios y contratistas.

- La Subdirección de Investigación e Información se reserva el derecho de monitorear los accesos y el uso del servicio de Internet de todos los funcionarios y contratistas, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines institucionales.

Uso de la herramienta de correo electrónico

El correo electrónico es para apoyo a las funciones y responsabilidades de los funcionarios y contratistas de la Secretaría Distrital de integración Social-SDIS, por lo tanto, el uso debe sujetarse a las siguientes directrices generales:

- El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales, económicos, comerciales, propaganda, campañas, invitaciones y cualquier otro ajeno a los propósitos de la entidad.

- El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @sdis.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.

- Se debe preferir el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan, cumpliendo con los lineamientos de uso eficiente del papel.

- Está prohibido el envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través del correo de la Secretaria, el Subsecretario, la Dirección Corporativa, Oficina Asesora de Comunicaciones, la Dirección de Análisis y Diseño Estratégico, la Subdirección Gestión y Desarrollo de Talento Humano y la Subdirección de Investigación e Información de la SDIS.

- En las Subdirecciones Locales estará prohibido el envío de correos masivos (más de 25 destinatarios) tanto internos como externos, salvo a través de los correos de los Subdirectores.

- Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deben reportar a la Subdirección de Investigación e Información a través del correo mesadeservicio1035@sdis.gov.co y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM.

- Toda actividad sospechosa respecto a la difusión de contenidos inusuales, en especial si contiene archivos adjuntos con extensiones (.exe, .bat, .prg, .bak, .pif etc.) debe ser reportado al correo mesadeservicio1035@sdis.gov.co y posteriormente eliminado, ya que puede ser contentivo de malware.

- La cuenta de correo Institucional no debe ser revelada a páginas o sitios publicitarios, de compras, deportivos, agencias matrimoniales, casinos o a cualquier otra ajena a los fines de la SDIS.

- Para las comunicaciones de agremiaciones, está prohibido difundir cualquier información de contenido a través del correo electrónico, ya que el único medio autorizado para dicha actividad es la Intranet Institucional.

- Está prohibido el uso del correo para el envío de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor o que atenten contra la integridad moral de las personas o institucionales.

- Todos los correos electrónicos de la SDIS con destino externo deben contener una sentencia de confidencialidad que haga referencia a la responsabilidad del uso de la información enviada. Esta sentencia debe ser proporcionada por la Subdirección de Investigación e Información.

- La SDIS puede supervisar cualquier cuenta de correo electrónico para certificar que se está usando para los propósitos legítimos. El incumplimiento de esta directriz puede conducir a acciones disciplinarias o acciones de índole legal.

Uso de los Recursos Tecnológicos

Los recursos tecnológicos de la SDIS son herramientas de apoyo a las funciones, responsabilidades y obligaciones de los funcionarios y contratistas; por ello, su uso está sujeto a las siguientes directrices generales:

- Los bienes de cómputo se emplean de manera exclusiva y bajo la completa responsabilidad de los funcionarios y contratistas al cual han sido asignados y únicamente para el desempeño de las funciones y responsabilidades del cargo, por lo tanto, no pueden ser utilizados con fines personales o por terceros no autorizados.

- Las impresoras de red son recursos tecnológicos compartidos por lo cual su uso debe ser moderado. La impresión de documentos debe ajustarse a la política cero papel de la entidad.

- Los usuarios no deben mantener almacenada información en los discos duros, de las estaciones cliente, archivos de video, música y fotos que no sean de carácter institucional.

- Es responsabilidad de los funcionarios y contratistas velar por la conservación y cuidado de los activos a su cargo evitando fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos.

- No está permitido realizar derivaciones eléctricas desde las fuentes de corriente regulada ni conectar multitomas a las mismas.

- Sobre los equipos tecnológicos no debe ubicarse elementos pesados, radios de comunicación o teléfonos celulares.

- Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos como destapar, agregar, desconectar, retirar, revisar y/o reparar sus componentes, son los funcionarios y contratistas de la Subdirección de Investigación e Información o quienes sean designados por ellos para tal labor.

- Toda unidad de almacenamiento externo como CDs, DVDs, memorias USB o Discos Duros externos debe ser verificada por el programa antivirus licenciado y autorizado por la Subdirección de Investigación e Información, previo a su ingreso a los recursos de cómputo de la entidad.

- La única dependencia autorizada para trasladar los elementos y/o recursos tecnológicos de un puesto de trabajo a otro es la Subdirección de Investigación e Información, esta función debe ajustarse a los procedimientos y competencias de ésta dependencia.

- Toda asignación y reasignación de los equipos de cómputo será realizada por la Subdirección de Investigación e Información y en concordancia a los procedimientos y competencias de esta dependencia.

- El retiro de recursos tecnológicos de la entidad solo está permitido, previa autorización del equipo de Apoyo Logístico de acuerdo con el procedimiento establecido por esa dependencia.

- La pérdida o daño de elementos o recursos tecnológicos o de alguno de sus componentes debe ser informada de inmediato a la subdirección de Investigación e Información por el funcionario y contratista a quien se le hubiere asignado.

- Toda solicitud o problema de tipo técnico con los equipos tecnológicos debe ser reportado a la mesa de servicios en la extensión 1035, al correo electrónico mesadeservicio1035@sdis.gov.co o a través de la herramienta de gestión.

- Solo está permitido el uso de software licenciado por la entidad y/o aquel que sin requerir licencia sea expresamente autorizado por la Subdirección de Investigación e información.

- Los únicos autorizados para instalar y/o desinstalar programas o herramientas de software son los funcionarios y contratistas de la Subdirección de Investigación e Información. Está prohibido instalar, ejecutar y/o utilizar programas o herramientas de software o hardware no autorizadas por la SII.

- Todo acceso a la red de la Entidad mediante elementos o recursos tecnológicos no institucionales debe ser informado, autorizado y controlado por la SII.

K. Del manejo de la información

Este subdominio busca salvaguardar de manera adecuada la clasificación pública reservada de la información, de los diferentes activos de información de la SDIS.

Directrices generales:

- La copia de información RESERVADA debe ser autorizada por el propietario de la información.
- La información RESERVADA solo podrá ser almacenada en las bases de datos de los sistemas de información dispuestos para este fin, para garantizar su seguridad y respaldo.
- La información RESERVADA debe ser almacenada en los discos de red en las carpetas indicadas con el fin de garantizar su seguridad y respaldo. En ningún caso debe realizarse en el disco duro u otro componente magnético del computador personal.
- El acceso a la información RESERVADA solo podrá ser autorizado por el propietario de la información.
- Está prohibido distribuir información de la SDIS, no pública, a otras entidades o ciudadanos sin la debida autorización.

L. Manejo de medios

El subdominio busca evitar la divulgación, modificación, retiro, destrucción no autorizada de la información que se encuentra almacenada en medios físicos (cintas, discos, etc.).

Directrices generales:

- La ubicación de los medios de almacenamiento debe estar alejada del polvo, humedad o cualquier contacto con químicos corrosivos.
- La Subdirección de Investigación e Información debe proveer los métodos de cifrado de la información, así como debe administrar el software o herramienta utilizado para tal fin.
- Cuando se requiera almacenar información sensible (pública reservada) en medios removibles, debe ser autorizada por el dueño del proceso.
- Es responsabilidad de cada funcionario y contratista tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, para evitar acceso físico y lógico no autorizado, daños, perdida de información o extravió del mismo. En caso de ocurrir algunos de estos eventos se debe informar a la mesa de servicio de la Subdirección de Investigación e Información mediante correo, herramienta de gestión o llamada, de acuerdo a lo descrito en el procedimiento de Gestión Incidentes de Seguridad de la información.

- Se prohíbe el uso de medios removibles con información misional de la SDIS en lugares de acceso al público como: cibercafés o equipos que no garanticen la confidencialidad, integridad y disponibilidad de la información contenida y clasificada como pública reservada.

- Es responsabilidad del usuario no exponer los medios removibles a condiciones ambientales como: (humedad, temperatura, etc.) que puedan afectar su buen funcionamiento del mismo.

M. Devolución de activos

Este subdominio busca devolver todos los activos de la Secretaría Distrital de Integración Social que los funcionarios y contratistas tengan a su cargo, esta devolución será al terminar el empleo, contrato o acuerdo.

Directrices generales:

La Subdirección de Investigación e Información a través de la Subdirección Administrativa y Financiera desarrollará los lineamientos para la devolución de los activos teniendo en cuenta lo siguiente:

- Los funcionarios y contratistas de la SDIS deben devolver todos los activos de la SDIS que se encuentran en su poder a la terminación de su empleo, contrato o acuerdo.

- Cuando se trate de traslado a otros funcionarios y contratistas, se debe instalar de nuevo el sistema operativo, aplicaciones y demás programas básicos de ofimática necesarios.

- Durante el periodo de notificación de la terminación, el jefe inmediato y/o supervisores debe controlar el copiado no autorizado de la información pertinente por parte de los funcionarios y contratistas que han finalizado el empleo.

V. DOMINIO CONTROL DEL ACCESO

Este dominio busca establecer lineamientos que permitan restringir el acceso no autorizado a la información y a instalaciones de procesamiento de información de la Secretaría Distrital de Integración Social.

Directrices generales:

La Subdirección de Investigación e Información establecerá los lineamientos para la política de control de acceso, el acceso a redes y servicios en red teniendo en cuenta lo siguiente:

- La SDIS dispondrá a los funcionarios y contratistas todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones y obligaciones para las cuales fueron contratados, por tal motivo no se permite conectar a la red o instalar dispositivos fijos o móviles, tales como: Computadores portátiles, tablets, enrutadores, agendas electrónicas, celulares inteligentes, Access point, que no sean autorizados por la Subdirección de Investigación e Información.

- La SDIS entregará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible. Siendo responsables los funcionarios, contratistas y terceras partes el manejo que se les dé a las claves asignadas.

- Para los funcionarios, contratistas y terceras partes de la SDIS que acceden a la red interna por acceso remoto deben estar previamente autorizado por la Subdirección de Investigación e Información, se realizará a través de VPN únicamente y exclusivamente para el acceso de la información autorizada.

- La Subdirección de Investigación e Información debe implementar controles de seguridad basados en las capas de red, con el fin de garantizar una interconexión fácil y eficiente, a la vez que se proteja la información y los recursos tecnológicos de la entidad.

- La Subdirección de Investigación e Información debe asegurar que la red inalámbrica de la SDIS tenga métodos de autenticación que evite accesos no autorizados.

- La Subdirección de Investigación e Información, debe establecer controles para la identificación y autenticación de los usuarios provistos por terceras partes en las redes o recursos de red de la SDIS.

- La Subdirección de Investigación e Información debe verificar con una periodicidad de (seis meses) los controles de acceso para los funcionarios y contratistas de la SDIS, con el fin de revisar que dichos usuarios estén activos y tengan acceso permitido únicamente a aquellos recursos de red y servicios tecnológicos para los que fueron autorizados.

- Los funcionarios y contratistas son responsables de los registros y/o modificaciones de información que se hagan a nombre de su cuenta de usuario, toda vez que la clave de acceso es de carácter personal e intransferible.

- Todas las contraseñas debe tener una longitud mínima de ocho (8) caracteres que debe cumplir con las siguientes características: incluir combinación de números, letras mayúsculas, letras minúsculas y caracteres especiales (por ejemplo: @,!, $, %, entre otros).

- Después de tres (3) intentos de acceso fallidos de manera consecutiva por ingreso de usuario y/o contraseña errados, el usuario será bloqueado hasta nueva reactivación por parte del administrador.

- Las contraseñas de acceso a los sistemas de información deben ser cambiadas periódicamente, de igual forma cualquier cambio extemporáneo de contraseña solamente puede ser solicitado por el titular de la cuenta o su jefe inmediato.

- Cuando un funcionario o contratista se retira de la SDIS, todas las credenciales asignadas sobre los recursos informáticos otorgados deben ser inhabilitadas inmediatamente, la solicitud de des-habilitación es responsabilidad del jefe inmediato y/o supervisor a cargo. De acuerdo con el procedimiento de solicitud de creación y modificación de usuarios.

- Las cuentas de usuario en estado activo que cumplan un periodo de cuatro (4) meses sin evidenciar usabilidad de la misma, deberán ser deshabilitadas.

VI. DOMINIO CRIPTOGRAFÍA

Este dominio busca asegurar el uso adecuado de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información en la SDIS.

Directrices generales:

La Subdirección de Investigación e Información desarrollará los lineamientos para los controles criptográficos teniendo en cuenta lo siguiente:

- Para la protección de claves de acceso a sistemas de información, datos y servicios de plataforma.

- La Subdirección de Investigación e Información velará por que la información crítica clasificada como reservada, sea cifrada al momento de almacenarse y/o transmitirse por cualquier medio, cuente con mecanismos de cifrado de datos con el propósito de proteger su confidencialidad e integridad.

- La Subdirección de Investigación e Información debe desarrollar y establecer un procedimiento para el manejo y la administración de llaves de cifrado.

- La Subdirección de Investigación e Información, debe desarrollar y establecer estándares para la aplicación de controles criptográficos.

- El equipo de desarrollo debe asegurar que los controles criptográficos de los sistemas construidos cumplen con los estándares establecidos por la SII. Cifrando la información reservada o restringida y certificar la confiabilidad de los sistemas de almacenamiento de dicha información.

VII. DOMINIO SEGURIDAD FÍSICA Y DEL ENTORNO

Este dominio busca prevenir el acceso físico no autorizado, perdida, robo, daño e interferencia a la información que se encuentren dentro o fuera de las instalaciones de procesamiento de información de la SDIS.

Directrices generales:

- La Subdirección de Investigación e Información debe informar al grupo de Plantas Físicas, el perímetro de las áreas que contienen información pública reservada, para que las instalaciones de procesamiento sensible o crítico sean protegidos de acceso no permitido.

- Se debe registrar de forma obligatorio el uso de bitácora de entrada y salida de los centros de cableado o Data Center para todos los funcionarios, contratistas y terceras partes, de acuerdo al instructivo para el control de acceso a centros de cableado y data center.

- Los privilegios de acceso físico a los centros de cableado o Data Center para los funcionarios, contratistas y terceras partes debe ser eliminados o modificados oportunamente a la terminación de contrato laboral, retiro del cargo o por alguna novedad.

- La red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como los computadores de escritorio, portátiles y pantallas; los otros elementos deben conectarse a la red no regulada.

- Los equipos deben estar protegido contra fallas de energía y otras interrupciones causadas por fallas en el soporte de los servicios públicos.

- Las oficinas e instalaciones donde se maneje información sensible deben contar con sistemas de cámaras.

- Los usuarios deben permanecer con el carné que los identifica como funcionarios y/o contratistas de la SDIS, mientras permanezcan en las instalaciones.

- Todos visitantes, proveedores o terceras partes deben portar la identificación que los acredite como visitante, mientras permanezcan en las instalaciones.

- Todos los visitantes que ingresan a la SDIS deben ser recibidos en las entradas de las dependencias y estar acompañados por la persona a quien visitan durante su permanencia en las instalaciones del mismo.

- Todos los funcionarios y contratistas deben reportar cualquier sospecha de pérdida o robo de carné de identificación a las instalaciones de la SDIS.

- El centro de cableado o data center debe estar separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios.

- En el centro de cableado o data center deben existir sistemas de detección y extinción automáticas de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

- El Grupo de Plantas Físicas debe monitorear y revisar de manera permanente los sistemas de aire acondicionado y sistemas de extinción de incendios (extintor) que hacen parte del centro de cableado o data center.

- Los trabajos de mantenimiento de redes eléctricas, cableados de datos y voz, debe ser realizados por personal especialista y debidamente autorizado e identificado. De acuerdo con directrices establecidas por el Grupo de Plantas Físicas.

N. Seguridad del cableado

Este subdominio busca que el cableado de energía eléctrica y de datos, estén protegidos contra interceptación, interferencia o daño.

Directrices generales:

- La Subdirección de Investigación e Información debe proteger el cableado lógico de las interferencias electromagnéticas producidas por equipos eléctricos y/o industriales.

- Los cables de potencia deben estar separados de los cables de comunicación, siguiendo normas técnicas. Los equipos deben protegerse de fallas de potencia u otras anomalías de tipo eléctrico.

- El correcto uso de las Uninterruptible Power Supply (UPS), se debe probar según las recomendaciones del fabricante, de tal forma que se garantice su operación y el suficiente tiempo para realizar las funciones de respaldo servidores y aplicaciones.

- El Grupo de Plantas Físicas debe probar de manera regular la planta eléctrica, de acuerdo con las recomendaciones del fabricante y por lo menos una vez cada quince días.

- La Subdirección de Investigación e información debe mantener los cables claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.

- El acceso a los centros de cableado (Racks), debe ser controlado acuerdo al instructivo para el control de acceso a centros de cableado y data center.

- La Subdirección de Investigación e Información debe mantener el o los rack marquillados y peinados para poder identificar los puntos de conexión.

- La Subdirección de Investigación e Información debe asegurar que el cableado que transporta datos y de energía debe estar protegido contra la intercepción, interferencia o daños.

O. Equipos y documentos físico desatendidos.

Este subdominio busca asegurar que los funcionarios y contratistas le den la protección adecuada a los equipos y documentos físicos desatendidos.

Directrices generales:

- Los funcionarios y contratistas de la SDIS, durante la ausencias temporales o definitivas no debe conservar sobre el escritorio información propia de la entidad como: documentos físicos o medios de almacenamiento, por lo tanto, se requiere guardar en un lugar seguro para impedir su pérdida, daño, copia o acceso por parte terceros o personal que no tenga autorización para su uso o conocimiento.

- Los funcionarios y contratistas de la SDIS deben bloquear la pantalla del computador a su cargo, cuando se ausenten de forma temporal o definitiva de su puesto de trabajo, para impedir el acceso de terceros no autorizados a la información almacenada en el computador.

- Los funcionarios y contratistas que impriman documentos con clasificación pública reservada, estos deben ser retirados de la impresora inmediatamente y no se debe dejar en el escritorio sin custodia.

- No se deben reutilizar documentos impresos con clasificación pública reservada, este debe ser destruidos y no debe estar como papel reciclable.

- Los lugares de trabajo de los funcionarios, contratistas de la SDIS y terceras partes que prestan sus servicios a la entidad y cuyas funciones no obliguen a la atención directa de ciudadanos debe localizarse preferiblemente en ubicaciones físicas que no queden expuestas al público para minimizar los riesgos asociados al acceso no autorizado de la información o a los equipos informáticos.

  La Subdirección de Investigación e Información debe configurar y mantener en operación el bloqueo automático con tiempo máximo de tres (3) minutos en los computadores de la SDIS.
- Los funcionarios y contratistas de la SDIS deben guardar la información en un lugar diferente al escritorio virtual del computador para reducir el riesgo de acceso no autorizado, pérdida y daño de la información.

- La Subdirección de Investigación e Información debe configurar la opción de ocultar los iconos del escritorio virtual de los computadores de la SDIS.

VIII. DOMINIO SEGURIDAD DE LAS OPERACIONES

Este dominio busca establecer lineamientos para documentar los procedimientos de operación de la subdirección de investigación e información y poner en disposición de todos los funcionarios y contratistas.

Directrices generales:

- La Subdirección de Investigación e Información con el apoyo de la Subdirección de Diseño, Evaluación y Sistematización debe documentar todos sus procedimientos operativos para garantizar la disponibilidad, integridad y confidencialidad de la información.

- La Subdirección de Investigación e Información, debe ejecutar cambios de tecnología de la información (TI) de acuerdo con el procedimiento gestión de cambios de tecnologías de la información, para asegurar la gestión de cambios estándar y de emergencia con respecto a infraestructura, aplicativos y servicios tecnológicos para que estos sean desarrollados bajo estándares de eficacia, seguridad, calidad y permitan determinar los responsables y actividades en la gestión de cambios.

  La Subdirección de Investigación e Información debe tener separados de manera física y lógica loas ambientes de desarrollo, pruebas y producción
- La Subdirección de Investigación e Información debe facilitar a los funcionarios y contratistas manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la SDIS.

- La Subdirección de Investigación e Información debe garantizar que los ambientes de prueba, desarrollo y producción sean similares para prevenir situaciones en las cuales el software desarrollado presente comportamientos distintos y errores.

- La Subdirección de Investigación e Información debe utilizar nombres de dominios diferentes para los ambientes de prueba, desarrollo y producción para evitar confusión y así diferenciar de manera clara cada ambiente.

P. Protección contra código malicioso

La Subdirección de Investigación e Información debe implementar en todas las estaciones de trabajo de la SDIS software de detección y reparación de códigos maliciosos para la verificación de los sistemas, de acuerdo con lo siguiente:

Directrices generales:

- Verificar en tiempo real, la presencia de códigos maliciosos en archivos de medios de almacenamiento masivo extraíbles o en archivos recibidos a través de la red.
- Desplegar tareas de escaneo diario en busca de códigos maliciosos en todas las unidades de almacenamiento de la estación de trabajo.
- Tener la verificación de las páginas web para comprobar la presencia de códigos maliciosos.
- Ningún funcionario ni contratista podrá ejercer actividades de administración sobre su equipo. Los únicos autorizados para desarrollar esta función son los funcionarios y contratistas autorizados por la Subdirección de Investigación e Información o a quien la Subdirección designe para dicha actividad.
- Se prohíbe estrictamente el uso de software no autorizado.
- La Subdirección de Investigación e Información realizará sensibilización a los funcionarios y contratistas sobre la protección contra software malicioso y buenas prácticas de seguridad informática.
- Los funcionarios y contratistas no deben cambiar o eliminar la configuración del software de antivirus, antispyware, antimalware, antispam que defina la Subdirección de Investigación e Información; por lo tanto, únicamente podrán realizar actividades de escaneo de virus en diferentes medios.
- Los funcionarios y contratistas que sospechen o detecten alguna infección por software malicioso debe notificar a la mesa de servicio, para que, a través de ella, la Subdirección de Investigación e Información tome las medidas de control correspondientes.

Q. Copia de respaldo de información

Este dominio busca establecer lineamientos de respaldo de información, software y sistemas, mediante estrategias orientados a la protección de la información y así mitigar la perdida de datos**.**

Directrices generales:

La subdirección de Investigación e Información efectuará copias de la información contenida en los sistemas de información de acuerdo con el siguiente esquema:

- Se realiza copia de seguridad diaria de lunes a viernes a las 8 de la noche.
- Se realiza copia de seguridad semanal los días sábados a las 8 de la noche.
- Se realiza copia de seguridad mensual el día último del mes a las 8 de la noche.
- Se realiza copia de seguridad Anual el último día del año a las 8 de la noche.
- Se realiza para producción de instancias de Oracle diario a partir de las 03:00 p.m.

Se almacena la información de la siguiente manera:

- Se guardan los archivos diarios de las 2 últimas semanas (2 cintas)
- Se guardan los archivos semanales del último mes (4 cintas)
- Se guardan los archivos mensuales del último año (12 cintas)
- Se guardan los archivos anuales de los últimos 10 años (10 cintas)

Adicionalmente, se tendrán en cuenta las siguientes directrices:

- Se deben realizar backups como mínimo, en los servidores donde operan los ambientes de producción de los sistemas misionales.
- Los medios de almacenamiento sobre los cuales residen los backups, debe tener una vida útil de mínimo tres años a partir de su ejecución.
- Los backups deben almacenarse en un lugar seguro, con las condiciones de temperatura y humedad requerida, para su adecuada conservación y durabilidad.
- Los medios magnéticos y/o ópticos donde residen los backups, debe estar debidamente etiquetados y ordenados.
- La Subdirección de Investigación e Información debe contar con el respectivo procedimiento de respaldo de información y restauración de backups de tal forma que permita recuperar los ambientes de trabajo requeridos en tiempos razonables.
- Los backups no generados en los esquemas mencionados para el respaldo de la información, se obtendrán del mensual o en su defecto del último respaldo realizado.

- Los funcionarios y contratistas son responsables de la información que resida en el computador asignado y serán los encargados de mantener copia de sus archivos más sensibles, esta copia debe ser entrada al jefe inmediato, supervisor o quien designe este del cargo o contrato en custodia al finalizar la vinculación.

- Los funcionarios y contratistas pueden hacer uso del almacenamiento en la nube que disponga la Subdirección de Investigación e Información para el respaldo de datos de archivos o documentos institucionales ubicados en los equipos de cómputo de cada usuario.

IX. DOMINIO GESTIÓN DE LOS INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Este dominio busca definir parámetros de detección y gestión de los incidentes de Seguridad de la Información, con el fin de identificar y mitigar riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información de la Secretaría Distrital de Integración Social.

Directrices Generales:

La Subdirección de Investigación e Información debe definir los lineamientos para:

- Los canales de reporte de los Incidentes de Seguridad de la Información.

- Es responsabilidad de los funcionarios y contratistas reportar todos los posibles incidentes de seguridad de la información.

- La Subdirección de Investigación e Información debe dar a conocer a los funcionarios y contratistas de la SDIS los lineamientos establecidos para la Gestión de Incidentes de Seguridad de la Información.

- La Subdirección de Investigación e Información debe realizar la gestión y tratamiento pertinente a todos los incidentes con tipificación alta, media y baja.

- La Subdirección de Investigación e Información debe contar con un plan de respuesta sobre incidentes de Seguridad de la Información.

- La Subdirección de Investigación e Información definirá la clasificación de los Incidentes de Seguridad de la Información para la SDIS.

X. DOMINIO GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Es el conjunto de procedimientos y estrategias definidos para asegurar la reanudación oportuna y organizada de los procesos críticos de la entidad generando un impacto mínimo ante una contingencia, dentro de los cuales se tiene prevenir interrupciones en la operación normal de la SDIS que van en detrimento de los procesos críticos afectados por situaciones no previstas o desastres.

Teniendo en cuenta que es un tema transversal, la SDIS establecerá los responsables que se encargarán de su gestión, administración y coordinación.

La Subdirección de Investigación e Información debe establecer los lineamientos para minimizar los efectos de las posibles interrupciones de la operación (sean éstas resultado de desastres naturales, accidentes, fallas en el equipamiento, acciones deliberadas u otros hechos) y proteger los procesos críticos mediante una combinación de controles preventivos y acciones de recuperación, teniendo en cuenta los siguientes aspectos:

- Análisis de riesgos: Identificar de los procesos críticos y riesgos asociados a la no operatividad de los mismos, así como la valoración objetiva de los riesgos y escenarios identificados, bajo criterios como criticidad de la amenaza, probabilidad de ocurrencia, entre otros.

- Análisis de impacto del negocio: Identificar los productos y servicios críticos de la SDIS teniendo en cuenta todos los componentes que hacen parte de los mismos, como personal, equipos, proveedores entre otros, con el fin de valorizar el impacto que puede contraer una interrupción inesperada en las actividades diarias.

- Estimar los tiempos de recuperación, Identificar los requerimientos de recursos necesarios para el funcionamiento de los procesos críticos.

- Selección de la estrategia de continuidad: Se definen los requerimientos, recursos y roles encargados, los procedimientos y técnicas de recuperación, con base en las dos primeras fases y en los escenarios identificados.

- Ejecución y desarrollo del plan: Establecer e implementar el Plan de recuperación, Procedimientos de capacitación, pruebas de recuperación, divulgación, entre otros. Designación de responsables y asignación de recursos.

- Plan de evaluación y de mantenimiento: Retroalimentación, mejora continua, plan de pruebas periódicas, simulacros y velar porque se cumpla el plan.

Aprobación del documento

	Elaboró	Revisó	Aprobó

Nombre	Dayana Carbonó Carbonó	Katheryn Gonzalez Rocío Gómez Rodríguez	Liliana Pulido Villamil
Cargo/ Rol	Contratista- SII Seguridad de la información	Asesora -Subdirección Investigación e Información Subdirectora Investigación e Información	Directora de Análisis y Diseño Estratégico