RESOLUCIÓN Nº DE

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

LA SECRETARÍA DISTRITAL DE INTEGRACIÓN SOCIAL

En uso de sus facultades legales y en especial las conferidas por el Artículo 365 de la Constitución Política de Colombia, en la Ley 80 de 1993, 1150 de 2007, Acuerdo 257 de 2006, articulo 4 del Decreto Distrital 607 de 2007.

CONSIDERANDO:

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

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

Que en el artículo 209 de la Constitución Política de Colombia, establece que la administración pública, en todos sus órdenes, tiene un control interno, el cual se ejerce en los términos que señale la ley y así mismo, en su artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

Que todos los funcionarios y contratistas de la SDIS deben acogerse a lo estipulado en la Ley 23 de 1982 sobre derechos de autor, la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

Que la Ley 527 de 1999 define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Que en el capítulo VII de la Ley 599 de 2000 se establecen las disposiciones relacionadas con la violación a la intimidad, reserva e interceptación de comunicaciones.

RESOLUCIÓN Nº 0635 DE

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

Que la Ley 1273 de 2009, por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "*De la protección de la información y los datos*" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que la Ley 1581 de 2012 tiene como objeto "(...) *desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales*" y que dicta ", además de las disposiciones generales para la protección de datos personales.

Que la Ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones"*, define en su Artículo 1, que *"el objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información."*

Que mediante el Conpes 3854 de 2016 se establecen los lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

Que el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, número 1078 de 2015, dispone que las entidades que conforman la administración pública están obligados al cumplimiento de políticas y lineamientos de la Estrategia de Gobierno en Línea.

Que en el marco del Decreto 2573 de 2014, se establecen los lineamientos generales de Gobierno en Línea e incorpora los requerimientos de la Ley 1581 de 2012 para la protección de datos personales y se diseñan en el marco de referencia a la norma ISO 27001 en cada uno de sus dominios.

Que mediante la Resolución 305 de 2008, la Comisión Distrital de Sistemas - CDS de Bogotá, D.C. expide las políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación,

seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

Que el artículo 14° del Decreto 607 de 2007, consagra, entre otras, como funciones de la Dirección de Análisis y Diseño Estratégico: (...)*e) Coordinar implementación, mantenimiento y seguimiento del Sistema Integrado de Gestión en la Entidad; f) Diseñar y proponer las políticas para el adecuado funcionamiento de los Sistemas de Información de la Entidad; p) Orientar la formulación y desarrollo de las políticas tanto de los sistemas de información como del desarrollo informático de la Secretaría, en busca del uso de tecnologías que hagan más eficiente la utilización de los recursos físicos, humanos y financieros de la Entidad.*

Que el artículo 16° del Decreto 607 de 2007, consagra, entre otras, como funciones de la Subdirección de Investigación e Información:
(...)*h) Proponer, aplicar y desarrollar las políticas tanto de los sistemas de información como del desarrollo informático de la Secretaría, realizando el procesamiento y control de los mismos, y asistir en lo pertinente a las entidades adscritas.*
ñ) Desarrollar procedimientos y crear planes de contingencia para los sistemas de información.

Que la Resolución 1564 de 2010, expedida por la Secretaría Distrital de Integración Social, crea el Comité de Seguridad de la Información - CSI de la entidad y define sus funciones.

Que en la Resolución 1887 de 2015, mediante la cual se deroga la Resolución 1551 de 2007, se reglamentan las generalidades, operatividad y se dictan otras disposiciones del Sistema de Información de la Secretaría Distrital de Integración Social-SDIS.

Que mediante Circular 007 de 2017 la Secretaría Distrital de Integración Social-SDIS publicó la Política de Seguridad y Privacidad de la Información del sitio web y protección de datos personales.

Que es deber de la Secretaría Distrital de Integración Social – SDIS realizar una gestión responsable de la información, dentro de los parámetros de seguridad y gobierno, que permitan mitigar los riesgos sobre su disponibilidad, confidencialidad e integridad y al mismo tiempo hacer que ésta genere mayor valor a la Entidad para el cumplimiento de su misión y los objetivos trazados en el marco del Plan de Desarrollo Bogotá Mejor para Todos.

RESOLUCIÓN Nº 0635 DE

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

Que la Secretaría Distrital de Integración Social recolecta, procesa, almacena y transmite información en formato físico, electrónico. Dicha información es el activo fundamental para el cumplimiento de la misión de la SDIS y proviene de diversas fuentes, como beneficiarios (niños, familias, víctimas, etc), funcionarios, contratistas, proveedores, operadores y entidades públicas y privadas; la gestión de dicha información requiere un manejo responsable y seguro que permita realizar un buen uso de la misma y mitigar los riesgos sobre su confidencialidad, disponibilidad e integridad.

Que para lograr el buen uso y seguridad de la información, la Secretaría Distrital de Integración Social requiere la implementación de un conjunto de controles, políticas, procesos, procedimientos, estructuras organizacionales y componentes de software y hardware. Que esta implementación requiere desde la identificación de los activos de información y el análisis de riesgos, hasta establecer, implementar y hacer seguimiento continuo a dichos controles y su efectividad; razón por la cual se hace necesario incorporar en el Sistema Integrado de Gestión de la Secretaria de Integración Social el Subsistema de Gestión de Seguridad de la Información que permita identificar y gestionar dichos riesgos.

Que alineados con las políticas de Gobierno en Línea y teniendo en cuenta que ISO 27001 es una norma emitida por la Organización Internacional de Normalización, que describe cómo gestionar la seguridad de la información en una organización, se determina que la implementación del Sistema de Gestión de Seguridad de Información-SGSI se realice en el marco de dicha norma, sobre el cual se desarrolla la Política de Seguridad de la Información.

RESUELVE:

CAPÍTULO I
GENERALIDADES

ARTÍCULO 1. OBJETO: La Presente Resolución tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social, en adelante SDIS.

ARTÍCULO 2. POLÍTICA GENERAL: La SDIS protege la información física y lógica que produce, procesa y administra a través de la gestión de riesgos, la implementación de controles de seguridad y el mejoramiento continuo permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, alineándose con los requisitos legales, normativos y contribuyendo a la misión de la entidad.

ARTÍCULO 3. ALCANCE: La Política de Seguridad y Privacidad de la Información aplica a la SDIS, donde esta tenga presencia, a todos sus funcionarios, contratistas, proveedores, operadores y aquellas personas o terceros, que en razón del cumplimiento de sus funciones y las de la Secretaría Distrital de Integración social, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

ARTÍCULO 4. OBJETIVOS: La Política de Seguridad y Privacidad de la Información de la SDIS tiene como principales objetivos:

a. Establecer controles, mecanismos y estrategias que permitan mitigar los riegos sobre la confidencialidad, integridad y disponibilidad de la información de la SDIS.
b. Implementar lineamientos que permitan el manejo adecuado de la información de la SDIS.
c. Controlar los incidentes de seguridad de la información presentados en la SDIS.

ARTÍCULO 5. PRINCIPOS DE SEGURIDAD: A partir del Modelo de Seguridad y Privacidad de la Información emanado del Ministerio de las Tecnologías Información y las Comunicaciones, la SDIS adopta como principios de seguridad los siguientes:

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

b. Es responsabilidad de la Subdirección de Investigación e Información -SII establecer los lineamientos para la identificación, clasificación y buen uso de los activos de información, para su protección.

c. Las dependencias de la SDIS que tienen la custodia de la información generada en el marco de sus funciones deben aplicar los controles correspondientes para proteger la información

y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

d. Los activos de información, equipos, bienes, aplicaciones, herramientas tecnológicas y servicios de Tecnologías de la Información y las Comunicaciones en adelante TIC, asignadas por la SDIS son para uso exclusivo del cumplimiento de las funciones 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.

e. Es obligación de todos los funcionarios, contratistas y proveedores adscritos a la SDIS cumplir con la "Política de Seguridad de la Información" y propender por la integridad, disponibilidad y confidencialidad de la misma, so pena de que la entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

f. Es de responsabilidad de los funcionarios y contratistas realizar una copia de seguridad de los archivos más sensibles que se almacenan en los equipos de cómputo asignados; esta copia debe almacenarse en los medios designados por la SDIS tales como servidor de archivos, almacenamiento en la nube, DVD, entre otros. Una vez finalizada la vinculación con la entidad se deberá entregar toda la información procesada dentro de los equipos a cargo al jefe inmediato o al supervisor de contrato.

ARTÍCULO 6. RESPONSABLES: La SDIS tiene como responsables de la definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información los siguientes:

- El representante de la alta dirección de la SDIS, quien velará por el cumplimiento y mantenimiento de la Política de Seguridad de la Información.
- El Comité de Seguridad de la Información - CSI de la SDIS, que es el responsable de las decisiones estratégicas relacionadas con el Subsistema de Gestión de Seguridad de la Información en adelante SGSI.
- El Referente del SGSI, quien será designado por la Dirección de Análisis y Diseño Estratégico – DADE, mediante el correspondiente memorando.

PARÁGRAFO: No obstante lo estipulado en el artículo precedente, todos los funcionarios, contratistas y proveedores de la SDIS son responsables del cumplimiento de la política de seguridad y privacidad de la información.

CAPÍTULO II
RECURSOS HUMANOS

ARTÍCULO 7. GESTIÓN EN EL RECURSO HUMANO: La SDIS a través de la Subdirección de Gestión y Desarrollo de Talento Humano y la Subdirección de Contratación es la responsable de divulgar la Política de Seguridad y Privacidad de la Información a todos los funcionarios o contratistas que se vinculen a la entidad.

La Subdirección de Contratación debe realizar las tareas pertinentes para que todos los contratos de prestación de servicios, incorporen las obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad de la Información, el manejo confidencial de la información, la cesión de derecho de autor a la entidad y la protección de datos.

Cuando un funcionario o contratista cese en 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 a la normativa vigente.

CAPÍTULO III
SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

ARTÍCULO 8. GESTIÓN DE LA SEGURIDAD EN LOS ACTIVOS: La SDIS a través de la Subdirección de Investigación e Información -SII, 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.

ARTÍCULO 9. INVENTARIO Y PROPIEDAD DE LOS ACTIVOS: La responsabilidad de la administración y gestión de los activos de información está en cabeza del dueño de los mismos.

RESOLUCIÓN Nº 0635 DE

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

Los activos de Información de la SDIS deben ser identificados, clasificados y controlados para propender su uso adecuado, protección y la recuperación ante cualquier desastre.

Los dueños de la información deben propender para que los custodios mantengan actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez por año. La consolidación de dicho inventario está bajo la responsabilidad de la Subdirección de Investigación e Información y la Subdirección Administrativa y Financiera.

Con el objeto de implementar los controles de seguridad, las dependencias que tienen la custodia de la información en el marco de su función, se encargaran de proteger la información, mantener y actualizar el inventario de activos.

ARTÍCULO 10.CONTROLES A LOS ARCHIVOS DE GESTIÓN: La Subdirección Administrativa y Financiera, por medio del equipo de Gestión Documental, debe implementar controles para garantizar que los archivos de gestión de la entidad cuenten con los mecanismos de seguridad que salvaguarden y conserven de dicha información.

ARTÍCULO 11.CLASIFICACIÓN DE LA INFORMACIÓN: Los propietarios de los activos de información deben documentar la clasificación de seguridad de los activos de los que son responsables y designarán un custodio para cada activo a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la SDIS se debe realizar con base en la ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015 y la ley 594 de 2000 (Ley General de Archivos).

ARTÍCULO 12. USO ACEPTABLE DE LOS ACTIVOS: Los recursos tecnológicos al igual que los archivos, carpetas, bases de datos, aplicaciones y documentos, son activos de información que pertenecen a la SDIS, por lo cual su uso es exclusivamente institucional y es responsabilidad de aquel a quien se asigne o corresponda su uso, el propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso, estos son:

a. **CORREO ELECTRÓNICO**: El correo electrónico institucional asignado es un servicio para la comunicación y colaboración de los funcionarios y contratistas de la SDIS, de uso personal e intransferible, que debe utilizarse responsablemente cumpliendo como mínimo con los siguientes lineamientos:

- 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.
- Acogiéndose a la política de cero papel, se debe priorizar el uso del correo electrónico sobre el envío de documentos físicos, salvo en aquellos casos que la ley indique lo contrario.
- 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 deberán reportar a la Subdirección de Investigación e Información a través de la mesa de servicios y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM.
- Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados a la Subdirección de Investigación e Información a través de la mesa de servicio y serán tratados como incidentes de seguridad de la información.
- La cuenta de correo institucional no podrá ser utilizada para el registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales,

casinos, concursos, sitios de citas o cualquier otro ajeno a las funciones que le correspondan en la SDIS.

- Está expresamente 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 instituciones.
- Está expresamente prohibido distribuir información de la SDIS que no sea considerada de uso público, a otras entidades o ciudadanos, sin la debida autorización de dueño del activo de información.
- El correo electrónico institucional deberá contener junto con la firma un mensaje de confidencialidad, que deberá ser aprobado por la Dirección de Análisis y Diseño Estratégico – DADE y diseñado por la Subdirección de Investigación e Información.

b. INTERNET: Si bien la Subdirección de Investigación e Información – SII establece controles a la navegación de acuerdo a las políticas y perfiles establecidos, es responsabilidad de todos los funcionarios y contratistas de la SDIS hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí establecidas:

- La SDIS, en cabeza de la Subdirección de Investigación e Información-SII, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
- La SDIS, a través de la Subdirección de Investigación e Información -SII se reserva el derecho de monitorear, hacer seguimiento y auditoría al uso que los usuarios le den, para verificar que se haga un uso responsable y racional de dicho recurso.
- El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales dentro del marco institucional y se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, ofensivo, injurioso, obsceno, pornográfico, violatorio de los derechos de autor y todo aquel que atente contra la integridad moral.
- 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.

c. **EQUIPOS DE CÓMPUTO Y OTROS DISPOSITIVOS:** La SDIS podrá hacer entrega a los funcionarios y contratistas de computadores de escritorio, portátiles, Tablet, teléfonos IP, teléfonos inteligentes o dispositivos similares para el desarrollo de sus labores; el manejo de dichos equipos por parte de éstos, conlleva responsabilidades y deben ajustarse a las siguientes directrices generales:

- Aquellos dispositivos que requieran clave de acceso, dicha clave es de uso personal y no podrá ser compartida, razón por la cual la responsabilidad de un posible mal uso recaerá sobre el funcionario o contratista a quien se asignó dicha clave.
- Los dispositivos asignados solo podrán usarse para fines laborales relacionados con las funciones y obligaciones designadas, razón por la cual no hay autorización de instalar software diferente al autorizado por la Subdirección de Investigación e Información.
- Los dispositivos de cómputo y móviles que sean asignados a los funcionarios y contratistas, serán para uso institucional exclusivamente e intransferibles y la responsabilidad de su uso recaerá sobre la persona a la que le fue asignado.
- Teniendo en cuenta que los equipos son para uso institucional, la SDIS se reserva el derecho de monitorear el contenido y software instalado en los equipos de la entidad para verificar el tipo de información, su uso y licenciamiento del software instalado. De esta manera contenidos de música, video, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento, será desinstalado.
- Los únicos autorizados para la instalación de software adicional a las aplicaciones base es el personal técnico que designe la Subdirección de Investigación e Información, previa solicitud a través de la mesa de servicio y luego de la aprobación respectiva (se debe constatar la necesidad de su uso y que la SDIS cuente con el respectivo licenciamiento).
- Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por las

Subdirección de Investigación e Información previa solicitud a través de la mesa de servicio.

- Es responsabilidad de los funcionarios y contratistas de la SDIS mantener copias de seguridad de la información contenida en sus estaciones de trabajo y entregarlas en custodia al jefe inmediato o supervisor del contrato al finalizar la vinculación con la Entidad.
- De acuerdo a la política de consumo de tabaco y sustancias alucinógenas está prohibido fumar, ingerir alimentos o bebidas en el área de trabajo donde se encuentren los elementos tecnológicos tales como computadores de escritorio, portátiles entre otros.
- La Subdirección de Investigación e Información en cabeza del equipo de mesa de servicio deberá aprovisionar los computadores antes de ser entregados, garantizando que:
  - Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.
  - El software instalado sea el software base definido por la Subdirección de Investigación e Información – SII y cuente con el respectivo licenciamiento.
  - Los sistemas operativos y demás aplicativos tengan instaladas las últimas actualizaciones liberadas a la fecha de entrega del equipo.
  - El antivirus este actualizado, funcionando y administrado desde consola.
- Los equipos deberán quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, por seguridad y ahorro de energía entre otras.
- La Subdirección de Investigación e Información, en cabeza del equipo de infraestructura de Tecnologías de la Información y Comunicaciones-TIC, debe implementar servidores para el despliegue de actualizaciones y parches de seguridad y diseñar estrategias que permitan mantener actualizada toda la plataforma computacional de la SDIS.

d. CABLEADO ESTRUCTURADO: En las sedes donde haya cableado estructurado, las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas de color naranja y bajo ninguna circunstancia se puede conectar otros elementos en dichas tomas.

En los puntos de red de los usuarios no está permitido realizar conexiones de switches, hub, acces point u otros dispositivos para realizar derivaciones, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

e. **SISTEMAS DE INFORMACIÓN:** Las credenciales de acceso a la red y a recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los funcionarios y contratistas de la SDIS no deben revelar éstas a terceros ni utilizar claves ajenas. Todo funcionario y contratista será responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

Cuando se presenten ausencias de funcionarios o contratistas por incapacidades, licencias no remuneradas o suspensión de contrato, será bloqueado el acceso a los equipos de cómputo asignados, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. Es responsabilidad del jefe inmediato o supervisor de contrato notificar este evento con una solicitud a la Subdirección de Investigación e Información a través de la mesa de servicios.
Solo podrán publicarse aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a la SDIS; las demás aplicaciones son de uso interno y su acceso desde fuera de la entidad se debe través de conexiones seguras con previa autorización por parte de la Subdirección de Investigación e Información.

CAPÍTULO IV
CONTROLES DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 13.CONTROL DE ACCESO: La SDIS a través de la Subdirección Administrativa y Financiera, propende por implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad.

La SDIS a través de la Subdirección de Contratación y la Subdirección de Gestión y Desarrollo del Talento Humano deben establecer los mecanismos para comunicar a la Subdirección de

Investigación e Información las novedades de ingreso y retiro de los funcionarios y contratistas de la SDIS para gestionar los derechos de acceso a los sistemas, recursos y servicios tecnológicos de la entidad.

La Subdirección de Investigación e Información debe implementar controles, procedimientos e instructivos para proveer el acceso físico y lógico de los recursos informáticos a usuarios autorizados para el cumplimiento de sus funciones estos serán los siguientes:

a. **CONTROLES CRIPTOGRÁFICOS:** La SDIS a través de la Subdirección de Investigación e Información debe implementar lineamientos o directrices del uso adecuado de controles criptográficos, con el fin de establecer un lineamiento que permita servir como guía bajo las mejores prácticas.

   Los propietarios de los activos de información deben identificar las necesidades de criptografía de información de acuerdo al grado de criticidad y privacidad de la misma e informar de dicha necesidad a la Subdirección de Investigación e Información quien debe analizar y si es procedente aprobar.

   La Subdirección de Investigación e Información debe asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información que así lo requiera.

b. **SEGURDAD FÍSICA Y DEL ENTORNO:** 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 (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructuras de soporte a los sistemas de información y comunicaciones.), 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.

PARÁGRAFO: Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones de la SDIS deberán estar debidamente identificados, con un documento que acredite su tipo de vinculación el cual se deberá portar en un lugar visible.

c. **SEGURIDAD DE LAS OPERACIONES:** 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; para este fin debe cumplir con los siguientes lineamientos:

- Implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en el data center de la entidad y su recuperación en caso de desastre.
- Implementar controles para mitigar los riesgos inherentes a códigos maliciosos, sin embargo los usuarios no pueden instalar software en los equipos de propiedad de la Entidad.
- Implementar un procedimiento para la gestión o control de cambios de las TIC donde los cambios en la configuración de los equipos, redes, sistemas de información, bases de datos, aplicaciones o cualquier activo de información de Tecnologías de Información-TI sean revisados, evaluados y aprobados.
- Implementar controles para auditar el acceso y uso de datos por parte de los funcionarios y contratistas, y se reserva el derecho de monitorear la actividad donde se sospecha que se ha producido o pueda producir una violación de la política, asegurando el debido proceso y el respeto por los derechos de las partes involucradas.
- Proveer los recursos necesarios para la implementar controles requeridos para la seguridad de las operaciones.

d. **SEGURIDAD DE LAS COMUNICACIONES:** La SDIS a través de la Subdirección de Investigación e Información establecerá los Acuerdos de Niveles de Servicios-ANS requeridos para que el proveedor de servicios de tecnologías de Información-TI garantice la disponibilidad de las redes WAN e Internet.

La SDIS a través de la Subdirección de Investigación e Información debe implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos de la entidad propendiendo la integridad y confidencialidad de la información.

e. **CONTROLES EN LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS:** La Subdirección de Investigación e Información será la única área autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de aplicaciones, sistemas de información o cualquier componente de TIC, de conformidad con la Circular No. 20 del 23 de junio del 2016 de la SDIS. De igual forma la Subdirección de Investigación e Información velará porque la adquisición, desarrollo interno o externo de sistemas de información incorpore las buenas prácticas para el desarrollo seguro de software y estándares de seguridad informática.

f. **CONTROLES EN LAS RELACIONES CON LOS PROVEEDORES:** La SDIS a través de la Subdirección de Investigación e Información y la Subdirección de Contratación, definirá mecanismos de control que gobiernen sus relaciones con terceros para asegurar que la información a la que accedan tenga el nivel de protección correspondiente y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

ARTICULO 14. SEGURIDAD EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO: La SDIS a través de Subdirección de Investigación e Información dispone de los planes de continuidad de negocio y recuperación de desastres para mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los sistemas de información misionales que sean considerados críticos para la continuación de la operación de la entidad de maneara aceptable.

La entidad destinará los recursos financieros suficientes para proporcionar una respuesta efectiva de TI, para soportar los procesos claves de la entidad en caso de contingencia o eventos catastróficos que afecten la continuidad de su operación.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

ARTÍCULO 15. GESTIÓN DE INCIDENTES DE SEGURIDAD[1] DE LA INFORMACIÓN: La SDIS, a través de la Subdirección de Investigación e Información se encarga de definir, documentar, mantener, publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos de seguridad de la información. De igual forma la SII deberá promover el reporte de eventos de seguridad de la información para reducir la probabilidad e impacto del riesgo inherente a ellos.

Los eventos e incidentes de seguridad de la información serán investigados por la Subdirección de Investigación e Información de acuerdo al procedimiento de incidentes de seguridad de la información.

PARÁGRAFO: El Comité de Seguridad de la Información definirá las funciones y la conformación de un grupo de atención, evaluación y respuesta a incidentes de seguridad.

CAPÍTULO V
DISPOSICIONES FINALES

ARTÍCULO 16. CUMPLIMIENTO: La SDIS velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

La Secretaría Distrital de Integración Social, implementará y mantendrá los controles necesarios para proteger la información de funcionarios, contratistas, beneficiarios, proveedores y demás terceros de los cuales reciba y administre información de conformidad con la Ley de protección de datos personales.

La SDIS implementará y mantendrá los controles necesarios para dar cumplimiento a las disposiciones legales sobre derechos de autor, propiedad intelectual y ley de transparencia.

[1]Incidente de Seguridad: es un evento adverso en un sistema de computadoras, o red de computadoras, que compromete la confidencialidad, integridad o disponibilidad, la legalidad y confiabilidad de la información. Puede ser causado mediante la explotación de alguna vulnerabilidad o un intento o amenaza de romper los mecanismos de seguridad existentes, y puede generar un impacto en la operación de la entidad.

RESOLUCIÓN Nº 0635 DE 12 ABR 2017

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información en la Secretaría Distrital de Integración Social".

Los funcionarios, contratistas y proveedores que violen los requisitos contenidos en esta norma pueden estar sujetos a medidas disciplinarias, penales y administrativas según el caso.

La Política de Seguridad y Privacidad de la Información deberá revisarse y actualizarse cada año o cuando se considere pertinente por cambios normativos, necesidades del servicio o riesgos de seguridad detectados que así lo ameriten.

Así mismo, esta Política que da las directrices generales estará reglamentada por los lineamientos contenidos en un manual de seguridad de la información.

ARTÍCULO 17. VIGENCIA Y DEROGATORIA: La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias incluyendo el Lineamiento de Seguridad Informática- L-TE-001.

PUBLÍQUESE Y CÚMPLASE

Dado en Bogotá D.C., a los días del mes de de

12 ABR 2017

RICHARD ROMERO RAAD
Secretario (e) Distrital de Integración Social

Elaboró: Diego Ferney Ramírez Pulido – Referente del Subsistema de Seguridad de la Información
Carlos Camacho Araque-Asesor de la Subdirección de Información e investigación
Revisó: Mileni Rodríguez Gómez – Gestor de Proceso Mantenimiento y Soporte TIC
Alexandra Rivera Pardo – Subdirectora (e) de Investigación e información
Sofía Navas Pineda – Gestor SIG
Sebastian José Bitar Arango -Asesor de la Oficina Jurídica
Deisy Sabogal Castro-Subdirectora de Contratación
Gina Alexandra Vaca Linares-Subdirectora Administrativa y Financiera
Giovanny Arturo Gonzalez Zapata-Subdirector de Gestión y Desarrollo de Talento Humano

Aprobó: María Carmenza Valverde Pineda - Jefe Oficina Asesora Jurídica
Liliana Pulido Villamil - Directora de Análisis y Diseño Estratégico
María Clemencia Pérez Uribe - Directora de Gestión Corporativa