ALCALDÍA MAYOR
DE BOGOTÁ D.C.
SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

RESOLUCION No. 000851 DE 31 DIC 2019 000851

( )

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

EL SECRETARIO DISTRITAL DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

En uso de sus facultades legales y en especial, las conferidas por el Acuerdo 637 del 31 de marzo de 2016 y Decreto 413 de 2016 y

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 20 de nuestra carta política establece: *"Se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios masivos de comunicación."*

Que el artículo 74 ejusdem dispone 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 el artículo 209 ídidem establece que la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley y en consecuencia, el 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 Secretaría Distrital de Seguridad, Convivencia y Justicia 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 594 de 2000, tiene por objeto establecer las reglas y principios generales que regulan la función archivística del Estado.

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

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

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 Estatutaria 1266 de 2008 Dicta las disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

Que la Ley Estatutaria 1581 de 2012, Por la cual se dictan disposiciones generales para la protección de datos personales 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 Estatutaria 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 el artículo 45 de la Ley 1753 del 9 de junio de 2015, por la cual se expide el Plan Nacional de Desarrollo 2014 - 2018 "Todos por un nuevo país", cuya vigencia se mantuvo con la Ley 1955 de 2019 *"Por el cual se expide el Plan Nacional de Desarrollo 2018-2022, Pacto por Colombia, Pacto por la Equidad"* señala que se deben establecer estándares, modelos y lineamientos de tecnologías de la información y las comunicaciones para los servicios al ciudadano y aplicarán, entre otros, para los siguientes casos: ... c) Autenticación electrónica, d) Publicación de datos abiertos, ... f) Implementación de la estrategia de Gobierno en Línea, g) Marco de referencia de arquitectura empresarial para la gestión de las tecnologías de información en el estado, ... j) Interoperabilidad de datos como base para la estructuración de la estrategia que sobre la captura, almacenamiento, procesamiento, análisis y publicación de grandes volúmenes de datos (Big Data) formule el Departamento Nacional de Planeación., así como en el parágrafo 2 inciso a) Carpeta ciudadana electrónica: (...)

Que en el marco del Decreto Nacional 2573 de 2014, establece 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 el Decreto 1078 de 2015, es el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

Que el Decreto 1078 de 2015 dispone que las entidades que conforman la administración pública serán sujetos obligados para el cumplimiento de las políticas y los lineamientos de la Estrategia de Gobierno en Línea, estableciendo en su artículo 2.2.9.1.2.1 como uno de sus cuatro componentes el de la Seguridad y privacidad de la Información, comprendido por las acciones transversales a los componentes de TIC para Servicios, TIC para el

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

Gobierno Abierto y TIC para la Gestión, tendientes a proteger la información y sistemas de información, del acceso, divulgación, interrupción o destrucción no autorizada.

Que conforme el artículo 2.2.9.1.2.3 del Decreto 1078 de 2015, el cual establece como Responsable de coordinar la implementación de la Estrategia de Gobierno en línea en los sujetos obligados al representante legal de la Entidad, se hace necesario reestructurar la política de seguridad de la información de la Secretaría Distrital de Seguridad, Convivencia y Justicia para que se encuentre en consonancia con las normas de protección de datos personales contenidas en la Ley Estatutaria 1581 de 2012, las normas de transparencia y acceso a la información de la ley 1712 de 2014, así como en aquellas que las han reglamentado.

Que el Decreto 103 de 2015 "Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones", reglamenta todo lo concerniente a la transparencia y el acceso a la información pública.

Que el Decreto 1080 de 2015 "Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".

Que mediante el Conpes 3854 de 2016 el cual contiene la *"POLÍTICA NACIONAL DE SEGURIDAD DIGITAL"* 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 Nacional 1499 de 2017 *"Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015"*, es la norma que crea el *"MODELO INTEGRADO DE PLANEACIÓN Y GESTIÓN"*.

Que el Decreto Nacional 1008 de 2018 *"Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital y se subroga el capítulo 9 de la parte 2 del libro del Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones"*, establece el habilitador transversal de seguridad de la información como elemento fundamental para el logro de los propósitos de la misma.

Que la Directiva No. 005 de 2005, de la Alcaldía Mayor de Bogotá, establece la necesidad de aplicación por parte de las Entidades del Distrito Capital, de las políticas generales de tecnología de información y comunicaciones, en su gestión informática; con las cuales se pretende sentar bases para que la Administración Distrital cuente con la información necesaria para la toma de decisiones y para un real acercamiento a la ciudadanía a través de una eficiente prestación de servicios.

Que la Resolución 305 de 2008 de la Comisión Distrital de Sistemas de Bogotá, estableció las políticas públicas para las Entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones, y establece en su artículo 9 como objetivo: "La utilización creciente de las Tecnologías de la Información y las Comunicaciones -TIC-, genera beneficios para las entidades, organismos y órganos de control del Distrito Capital, mejorando el cumplimiento de la misión y la prestación de servicios a la ciudadanía. Sin embargo, por ser la información el activo más importante de la organización, es necesario protegerla frente a los posibles

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

riesgos derivados del uso de las nuevas tecnologías, para garantizar la seguridad de la información, en aspectos tales como disponibilidad, confiabilidad, accesibilidad e integridad de la misma, en los términos de la Directiva 05 de 2005 del Alcalde Mayor de Bogotá".
Que el Artículo 12 ejusdem establece: *"Los datos y la información utilizada por todos las entidades, organismos y órganos de control del Distrito Capital para su funcionamiento administrativo y el cumplimiento de sus funciones misionales, constituyen un patrimonio con valor económico que requiere las garantías administrativas y jurídicas para su conservación y ejercicio del derecho pleno de uso, por parte de la Administración Distrital, y en tal sentido, es un "bien público" de valor estratégico y patrimonial".*

Que el artículo 4 del Acuerdo Distrital 637 de 2016 estableció como objeto de la Secretaría Distrital de Seguridad, Convivencia y Justicia "(...) orientar, liderar y ejecutar la política pública para la seguridad ciudadana, convivencia y acceso a los sistemas de justicia; la coordinación interinstitucional para mejorar las condiciones de seguridad a todos los habitantes del Distrito Capital, en sus fases de prevención, promoción, mantenimiento y restitución; el mantenimiento y la preservación del orden público en la ciudad; la articulación de los sectores administrativos de coordinación de la Administración Distrital en relación con la seguridad ciudadana y su presencia transversal en el Distrito Capital, la coordinación del Sistema Integrado de Seguridad y Emergencias NUSE 123, la integración y coordinación de los servicios de emergencia; y proporcionar bienes y servicios a las autoridades competentes, con el fin de coadyuvar en la efectividad de la seguridad y convivencia ciudadana en Bogotá D.C.

Que el literal p) del Artículo 5 del Acuerdo Distrital 637 de 2016, establece dentro de las funciones de la Secretaría: *"p. Liderar, orientar y coordinar la implementación de las tecnologías de la información y la comunicación estratégica para el fortalecimiento de la convivencia, la seguridad y la justicia, en coordinación con las entidades distritales, territoriales y nacionales competentes".*

Que en la Resolución 541 del 2017, la Secretaría de Seguridad, Convivencia y Justicia adoptó la Política de Seguridad de la Información y se definen lineamientos para su uso, actualización y aplicación.

Que mediante Resolución 712 de 2018, se conforma el Comité Institucional de Gestión y Desempeño de la Secretaría de Seguridad, Convivencia y Justicia.

Que el Decreto Distrital 510 de 2019 *"Por el cual se reglamenta el Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 y se dictan otras disposiciones"*, establece en el numeral 5 del Artículo 12°.- Coordinación con entidades, nuevos sistemas o plataformas, *"(...) Aplicar los controles necesarios que permitan la protección, privacidad y seguridad de la información de las plataformas tecnológicas, sistemas de información y demás componentes que hagan parte del C4 (...)",*.

Que el Artículo 24 ibídem dispone: *"La información que se suministre a través del Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 se considera estratégica para la gobernabilidad, seguridad y convivencia del Distrito Capital por involucrar tanto, aspectos de seguridad ciudadana y elementos materiales probatorios, como del derecho fundamental a la intimidad de los usuarios que se encuentra amparada por reserva constitucional y legal".*

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

Que la Secretaría Distrital de Seguridad, Convivencia y Justicia, recolecta, procesa, modifica, almacena y transfiere información en formato físico y digital; dicha información es un activo fundamental para el cumplimiento de la misión de la Secretaria y proviene de diversas fuentes como funcionarios, contratistas, gestores, proveedores, operadores y entidades públicas y privadas; por lo cual 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 Seguridad, Convivencia y Justicia requiere la implementación de un conjunto de controles, políticas, procesos, procedimientos, estructuras organizacionales y componentes de software y hardware. 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 Seguridad, Convivencia y Justicia el Sistema de Gestión de Seguridad de la Información que permita identificar y gestionar dichos riesgos.

Que la Norma ISO 27001 es la norma estándar para la seguridad de la información expedida por la Organización Internacional de Normalización.

Que alineados con la política de Gobierno Digital 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, la Secretaría Distrital de Seguridad, Convivencia y Justicia determina que la implementación del Sistema de Gestión de Seguridad de Información-SGSI se realice en el marco de dicha norma sobre la cual se desarrolla la Política de Seguridad de la Información.

Que la Política de Seguridad y Privacidad de la Información es una declaración de las responsabilidades y de la conducta aceptada para funcionarios, contratistas, proveedores y terceros operadores que en razón del cumplimiento de sus funciones u obligaciones tienen acceso a la información de la entidad, lo anterior con el fin de mantener un ambiente seguro en la Secretaría Distrital de Seguridad, Convivencia y Justicia, de Esta Política establece las directrices y los lineamientos relacionados con el manejo seguro de la información.

Que en aplicación de la Resolución 541 del 2017 y en el marco de la implementación del sistema de gestión de seguridad de la información de la Secretaria Distrital de Seguridad, Convivencia y Justicia, y después de establecer los controles para dar cumplimiento a lo establecido en el Anexo A de la norma ISO/IEC 27001, estándar internacional para la seguridad de la información, se evidenció en mesas de trabajo que era necesario fortalecer los lineamientos de seguridad de la información descritos en la resolución 541 de 2017, toda vez que no se consideraban algunos activos de información críticos de la entidad y no se definían los lineamientos necesarios para asegurar los mismos de los diferentes riesgos a los cuales pudieran estar expuestos.

Que se hace necesario considerar los temas de seguridad de la información específicos relacionados con la operación de la Cárcel Distrital de Varones y Anexo de Mujeres, los cuales no están contemplados en la resolución 541 de 2017.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

Que dado lo anterior, se hace necesario adoptar mediante resolución la nueva política de seguridad y privacidad de la información, Seguridad digital y el plan de recuperación de desastres, así como definir los lineamientos para su uso y manejo.

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO 1. DEFINICIÓN. La Política de Seguridad y Privacidad de la Información es el documento que establece el compromiso y el enfoque de la Secretaría Distrital de Seguridad Convivencia y Justicia en la gestión de la seguridad y privacidad de la información.

ARTÍCULO 2. OBJETO. La presente resolución tiene como objeto adoptar la Política de Seguridad y Privacidad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, en adelante SDSCJ.

ARTÍCULO 3. ALCANCE. La SDSCJ protegerá todos los activos de información, especialmente la información física y electrónica que almacene, produzca y gestione a través de la implementación de controles físicos y lógicos, realizando una efectiva gestión de riesgos y un proceso de mejora continua, permitiendo incrementar los niveles de confidencialidad, integridad y disponibilidad de la información, apoyándose en los requisitos legales y normativos contribuyendo al cumplimiento misional de la entidad.

PARÁGRAFO 1: La Política de Seguridad y Privacidad de la Información proporciona los lineamientos requeridos para implantar un Modelo de Seguridad de la Información confiable y flexible y define el marco básico que guiará la implantación de cualquier directriz, proceso, procedimiento, estándar y / o acción, relacionados con la Seguridad de la Información

PARÁGRAFO 2: La SDSCJ en el marco de la presente Política de Seguridad y Privacidad de la Información implementará controles para los operadores tecnológicos que operan en las dependencias, teniendo en cuenta que éstos realizan la administración, operación, soporte, mantenimiento y custodia de las plataformas tecnológicas que cumplen las funciones para llevar a cabo la misionalidad de la entidad.

ARTÍCULO 4. ÁMBITO DE APLICACIÓN: La Política de Seguridad y Privacidad de la Información aplica a la SDSCJ en todos los niveles de la organización, a todos sus funcionarios, contratistas, proveedores, operadores o aquellas personas o terceros, que en razón del cumplimiento de sus funciones u obligaciones y las de la Secretaría Distrital de Seguridad, Convivencia y Justicia, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como a los entes de control, entidades relacionadas que acceden, ya sea interna o externamente, a cualquier activo de información independiente de su ubicación. Así mismo, la presente Política aplica a toda la información creada, procesada o utilizada por la SDSCJ, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

ARTÍCULO 5. OBJETIVO PRINCIPAL: El principal objetivo de la Política de Seguridad y Privacidad de la Información, es que la SDSCJ asegure que su información sea accedida sólo por aquellas personas autorizadas que tienen una necesidad legítima para la realización de sus funciones del negocio (Confidencialidad); así mismo que esté protegida contra modificaciones no planeadas, realizadas con o sin intención (Integridad), y que esté disponible por aquellas personas autorizadas cuando está sea requerida (Disponibilidad) y que sea utilizada para los propósitos que fue obtenida (Privacidad).

ARTÍCULO 6. OBJETIVOS ESPECIFICOS: La Política de Seguridad y Privacidad de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia tiene como objetivos específicos:

1. Establecer mecanismos y lineamientos para el manejo adecuado de la información.
2. Mitigar los incidentes de seguridad de la información en la SDSCJ.
3. Gestionar los riesgos asociados a la seguridad de la información que afecten la confidencialidad, disponibilidad y privacidad de la información de la SDSCJ.

ARTÍCULO 7. DECLARACIONES: A partir del Modelo de Seguridad y Privacidad de la Información emanado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, la Secretaría Distrital de Seguridad, Convivencia y Justicia declara:

1. La Secretaría Distrital de Seguridad, Convivencia y Justicia, establece los roles y responsabilidades relacionados con la presente Política de Seguridad y Privacidad de la información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

2. La entidad protege la información producida, custodiada y transmitida en desarrollo de sus procesos misionales.

3. La Dirección de Tecnología y Sistemas de Información, diseña e implementa la estrategia para proteger la información generada, recolectada, procesada y utilizada, así mismo, suministra y gestiona las herramientas de hardware y software para el procesamiento y almacenamiento de la información y a su vez implementa controles para mitigar los riesgos sobre dicha información., sin embargo, los propietarios de la información son los responsables de los procesos institucionales y por ende de la información registrada, así como de la autorización de cambios. De igual manera, los propietarios serán responsables de todas las modificaciones solicitadas de la información registrada en los sistemas de información.

4. La Dirección de Tecnología y Sistemas de la Información establecerá los lineamientos para la identificación, clasificación y buen uso de los activos de información digitales, para su protección.

5. La Dirección de Recursos Físicos y Gestión Documental es la facultada para establecer los lineamientos para la identificación, clasificación y buen uso de los activos de información física, con el fin de proteger la misma.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

6. Las dependencias de la Secretaría Distrital de Seguridad, Convivencia y Justicia que tienen la custodia de la información generada en el marco de sus funciones se encuentran capacitadas para aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

7. Los activos de información, equipos, bienes, aplicaciones, bases de datos, herramientas tecnológicas y servicios de Tecnologías de la Información y las Comunicaciones en adelante TIC, asignados a las personas por la SDSCJ son para uso exclusivo del cumplimiento de las funciones u 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 las sanciones disciplinarias y legales correspondientes.

8. Los funcionarios, contratistas, proveedores de la SDSCJ tienen la obligación de cumplir lo establecido en la "POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" y propender por la integridad, disponibilidad y confidencialidad de la misma, so pena que la entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

9. Los sistemas de información y aplicaciones entregados y administrados por operadores tecnológicos que no están integrados al dominio de la SDSCJ, deben ser responsabilidad en su uso y manejo por el mismo operador tecnológico.

10. Todos los activos de información tienen un responsable, en lo que tiene que ver la creación de cuentas de usuario y/o correo electrónico genéricos (que no estén asociados a un funcionario o contratista) no estarán autorizadas.

11. Los funcionarios y contratistas de la SDSCJ son responsables de realizar 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 SDSCJ tales como servidor de archivos, almacenamiento en la nube, medios magnéticos, 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.

12. Los operadoress tecnológicos que tengan suscritos contratos con la SDSCJ, tienen la responsabilidad de salvaguardar la información contenida en los equipos administrados por ellos, que sea de la entidad y entregar aquella que sea pertinente al finalizar el contrato.

13. La SDSCJ con apoyo de la Dirección de Tecnología y sistemas de Información y a través del convenio suscrito con el operador tecnológico que administra la operación del C4, debe extender los controles de seguridad de la información en los recursos tecnológicos dispuestos en entidades que pertenecen al sistema integrado de seguridad y emergencias.

14. Los terceros y funcionarios de éstos que hacen uso de los activos de información de la SDSCJ, deben cumplir los lineamientos descritos en la política de seguridad y privacidad de la información.

PARAGRAFO: La SDSCJ que tiene recursos tecnológicos destinados para la operación del C4 en entidades que pertenecen al sistema integrado de seguridad y emergencias, debe extender sus controles hasta estos activos que se encuentran distribuidos y administrados por los operadores tecnológicos quienes deben cumplir la Política de Seguridad y Privacidad de la Información de la SDSCJ.

ARTÍCULO 8. PRINCIPIOS: La presente Política se fundamenta en los siguientes principios:

1. **Responsabilidad:** La información es uno de los activos más importantes de la SDSCJ por lo tanto se espera que sea utilizada por las personas acorde al cumplimiento de sus funciones u obligaciones.
2. **Confidencialidad:** la información de propiedad de la SDSCJ y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y será accedida sólo por aquellas personas que tienen una necesidad legítima para la realización de sus funciones.
3. **Integridad:** las personas que accedan a la información de propiedad de la SDSCJ deben preservar la integridad de misma independientemente de su residencia temporal o permanente, o la forma en que sea transmitida y que esté protegida contra modificaciones no planeadas, realizadas con o sin intención.
4. **Disponibilidad:** la información de propiedad de la SDSCJ debe estar disponible a las personas autorizadas cuando sea requerida.
5. **Privacidad:** la información de propiedad de la SDSCJ debe ser preservada y utilizada para los propósitos que fue obtenida.

ARTÍCULO 9. RESPONSABLES: La SDSCJ tiene como responsables de la definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información los siguientes:

1. El Representante de la Alta Dirección de la SDSCJ, quien velará por el cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información.
2. El Comité Institucional de Gestión y Desempeño es el encargado de liderar y facilitar la implementación de la estrategia de Gobierno Digital y de seguridad digital en la entidad y fungir como su respectivo comité.
3. El Director de Tecnologías y Sistemas de la Información, quien es el encargado de implementar las políticas de seguridad informática y de la plataforma tecnológica de la SDSCJ definiendo los planes de contingencia y supervisando su adecuada y efectiva aplicación.
4. Persona encargada de apoyar la Implementación de Gobierno Digital quien es el encargado de realizar seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.
5. Persona encargada de la implementación del Sistema de Gestión de Seguridad de la Información o quien haga sus veces, será designado por de la Dirección de Tecnologías y Sistemas de la Información, de manera formal, será el encargado de gestionar y participar en la construcción de metodologías, planes, programas, proyectos e instrumentos que estén relacionados con el Sistema de Gestión de Seguridad de la Información.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

6. Los líderes de procesos son los responsables que se apliquen al interior de cada dependencia los lineamientos definidos en la Política de Seguridad y Privacidad de la información de la entidad.

PARÁGRAFO: No obstante, lo estipulado en el presente artículo, todos los funcionarios, contratistas y proveedores de la SDSCJ y son responsables del cumplimiento de la Política de Seguridad y Privacidad de la Información.

CAPITULO II
DIVULGACIÓN

ARTÍCULO 10. DIVULGACIÓN: La SDSCJ a través de la Oficina Asesora de Comunicaciones es la responsable de divulgar la Política de Seguridad y Privacidad de la Información y los lineamientos descritos en el manual de seguridad de la información a todos los funcionarios o contratistas que se vinculen a la entidad.

La Dirección Jurídica y Contractual, Dirección de Gestión Humana y la Dirección de Operaciones deben realizar las tareas pertinentes para que todos los contratos de prestación de servicios, contratos de planta de personal y contratos de operadores que administran, operan, soportan, mantienen y custodian activos de información de la SDSCJ respectivamente incorporen las funciones u obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad y Privacidad de la Información, el manejo confidencial de la información, la cesión de derecho de autor a la entidad y la protección de datos personales.

Cuando un funcionario o contratista cese en sus funciones o culmine la ejecución de un contrato en la SDSCJ, el jefe inmediato o supervisor del contrato será el encargado de la custodia de los recursos de información

PARÁGRAFO. Todos los funcionarios, contratistas, recurso humano de terceros y operadores de la Secretaría de Seguridad, Convivencia y Justicia deben cumplir con los lineamientos descritos en el "Manual de seguridad y Privacidad de la Información".

CAPÍTULO III
SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

ARTÍCULO 11. GESTIÓN DE LA SEGURIDAD EN LOS ACTIVOS: La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información y la Dirección de Recursos Físicos y Gestión Documental, debe establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información física y digital, con el objetivo de garantizar su protección.

ARTÍCULO 12. PROPIEDAD DE LOS ACTIVOS: Los activos de Información de la SDSCJ deben ser identificados, clasificados y controlados para propender por su uso adecuado, protección y la recuperación ante cualquier desastre.

Los propietarios de la información deben propender para que los custodios mantengan actualizado el inventario de los activos de información asignados y hagan entrega de éste al menos una vez por año. La consolidación de dicho

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

inventario está bajo la responsabilidad de la Dirección de Tecnología y Sistemas de la Información y la Dirección de Recursos Físicos y Gestión Documental.

Es responsabilidad de los custodios y usuarios finales el adecuado uso de los activos de información que la SDSCJ ha dispuesto para el cumplimiento de sus funciones u obligaciones.

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

En el caso de los operadores tecnológicos, se deben implementar los controles de seguridad necesarios para asegurar los activos de información y la información que están bajo responsabilidad de estos y están al servicio o son propiedad de la SDSCJ.

ARTÍCULO 13. CONTROLES A LOS ARCHIVOS DE GESTIÓN: La Dirección de Recursos Físicos y 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 dicha información.

ARTÍCULO 14. 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.

La clasificación de la información de la SDSCJ 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, la ley 594 de 2000 (Ley General de Archivos) y la Ley 1581 de 2012 (Ley de Protección de Datos Personales).

PARAGRAFO: Los operadores tecnológicos de la SDSCJ durante la ejecución contractual y con el fin de garantizar el adecuado uso de la información, deben cumplir con los lineamientos del manejo y clasificación de la información definida por la entidad de acuerdo a lo establecido en la normatividad vigente.

ARTÍCULO 15. 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 SDSCJ, 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. Dentro de los recursos se encuentran los siguientes:

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

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

1. 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.
2. El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @scj.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
3. Está prohibido el envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través del correo del Secretario(a), el Subsecretario(a) de Gestión Institucional, el Subsecretario() de Acceso a la Justicia, el Subsecretario(a) de Inversiones y Fortalecimiento de Capacidades Operativas, el Subsecretaria(o) de Seguridad y Convivencia, las respectivas direcciones de cada una de las Subsecretarias, la Oficina Asesora de Planeación, la Oficina Asesora de Comunicaciones, La Oficina del Centro de Comando, Control, Comunicaciones y Cómputo - C4, La Dirección de la Cárcel Distrital de Varones y Anexo de Mujeres, La Dirección de Gestión Humana, la Dirección de Tecnología y Sistemas de la Información. El Secretario y los Subsecretarios podrán solicitar dichos permisos para otras cuentas de manera permanente o transitoria, diligenciando el respectivo formato y su justificación.
4. Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM.
5. Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información.
6. 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 y obligaciones que le correspondan en la SDSCJ.
7. Está expresamente prohibido el uso del correo para el envío de contenidos vulgares, agresivos o insultantes, información de agremiaciones, ofensivos, injuriosos, obscenos, violatorios de la propiedad intelectual o que atenten contra la integridad moral de las personas o instituciones.
8. Está expresamente prohibido distribuir información de la SDSCJ que no sea considerada de uso público a otras entidades o ciudadanos, sin la debida autorización de propietario del activo de información.
9. El correo electrónico institucional deberá contener junto con la firma un mensaje de confidencialidad, que deberá ser aprobado por la Dirección de Tecnología y Sistemas de la Información.
10. Teniendo en cuenta que el correo electrónico es exclusivamente para uso institucional, la SDSCJ se reserva el derecho de monitorear el contenido. 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 podrán ser borrados sin previa consulta.
11. Las cuentas de correo electrónico se asignarán de acuerdo a la nomenclatura definida por la Dirección de Tecnología y Sistemas de Información.

b. **INTERNET:** La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, define los controles necesarios y conexiones seguras para el acceso a internet desde cualquier activo de información que lo requiera garantizando los niveles de seguridad adecuados.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

Si bien la Dirección de Tecnología y Sistemas de la Información establece controles a la navegación de acuerdo a las políticas y perfiles establecidos, es responsabilidad de todos los funcionarios y contratistas de la SDSCJ hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí establecidas:

1. La SDSCJ, en cabeza de la Dirección de Tecnología y Sistemas de la Información, 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.

2. La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información se reserva el derecho de monitorear, hacer seguimiento y auditoría a los usuarios, para verificar que se haga un uso responsable y racional de dicho recurso.

3. 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, vulgar, ofensivo, injurioso, obsceno, pornográfico, violatorio de los derechos de autor y todo aquel que atente contra la integridad moral.

4. 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.

5. El descargar archivos provenientes de Internet implica un riesgo para la seguridad de la información, así como un riesgo de infracción al régimen legal de derechos de autor, por lo cual se solicita que únicamente se haga cuando sea necesario.

6. La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, debe coordinar con los operadores tecnológicos que requieran acceso o interconexión a la infraestructura o a los activos de información de la entidad para acceder a internet o a canales de comunicación externos, los controles que se deben seguir para dicha interconexión y operación.

7. En los casos donde la operación sea administrada por un operador tecnológico, éstos deben contar con los controles necesarios y conexiones seguras para el acceso a internet en las sedes de la SDSCJ. La Dirección de Tecnología y Sistemas de Información o el supervisor del contrato debe realizar el monitoreo correspondiente.

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

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

1. 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 dicho usuario y clave.
2. Los dispositivos asignados solo podrán usarse para fines laborales relacionados con las funciones y obligaciones correspondientes, razón por la cual no tienen autorización de instalar software diferente al autorizado por la Dirección de Tecnología y Sistemas de la Información.
3. 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.
4. Teniendo en cuenta que los equipos son para uso institucional, la SDSCJ 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.
5. Los únicos autorizados para la instalación de software adicional a las aplicaciones base es el personal técnico que designe la Dirección de Tecnologías y Sistemas de la Información, previa solicitud a través de la mesa de ayuda y luego de la aprobación respectiva (se debe constatar la necesidad de su uso y que la SDSCJ cuente con el respectivo licenciamiento). En los casos donde la operación de mesa de servicio sea manejada por un operador tecnológico externo, estos serán los únicos autorizados para realizar instalación de software adicional en los equipos.
6. Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por la Dirección de Tecnologías y Sistemas de la Información previa solicitud a través de la mesa de servicio. En los casos donde la operación de mesa de ayuda sea manejada por un operador tecnológico externo, estos serán los únicos autorizados para realizar el proceso en mención.
7. Es responsabilidad de los funcionarios, contratistas y operadores tecnológicos que tengan relación con la SDSCJ 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.
8. La Dirección de Tecnología y Sistemas de la Información a través del contratista que realiza la operación de la mesa de servicio deberá aprovisionar los computadores antes de ser entregados, garantizando que:

8.1. Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.

8.2. El software instalado se el software base definido por la Dirección de Tecnología y Sistemas de la Información y este cuente con el respectivo licenciamiento.

8.3. Los sistemas operativos y demás aplicativos deberán tener instaladas las últimas actualizaciones estables a la fecha de entrega del equipo.

8.4. El antivirus deberá permanecer actualizado, funcionando y administrado desde consola.

8.5. Cuando aplique, en caso de que la operación sea realizada por un operador tecnológico, este debe coordinar las actividades necesarias con el personal de la mesa de servicio para el aprovisionamiento de los equipos de cómputo.

9. 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.
10. La Dirección de Tecnología y Sistemas de la Información, en cabeza del personal de infraestructura o en su caso el operador tecnológico encargado, 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 SDSCJ.

c. **CABLEADO ESTRUCTURADO**: En las sedes de la SDSCJ 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 naranjas y bajo ninguna circunstancia se puede conectar otros elementos eléctricos a los asignados en dichas tomas.

En los puntos de red de los usuarios no está permitido realizar conexiones de switches, hub, access 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.

Los operadores tecnológicos que en el cumplimiento de sus obligaciones administren infraestructura de la SDSCJ deben cumplir con las normas técnicas y estándares para el cableado estructurado de las redes de datos y redes eléctricas.

En los casos donde las conexiones son instaladas y administradas por un operador tecnológico, las conexiones a la red de datos de la SDSCJ deben ser autorizadas por la Dirección de Tecnología y Sistemas de Información.

Las conexiones destinadas a servicios de datos e internet por parte de los operadores tecnológicos, deben ser autorizadas por la Dirección de Tecnología y Sistemas de Información de la SDSCJ.

d. **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 SDSCJ 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.

1. Cuando se presenten ausencias de funcionarios o contratistas por incapacidades, vacaciones, 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, por lo que la persona indicada, que puede acceder al equipo es el supervisor del contrato. Es responsabilidad de la Dirección de Gestión Humana, la Dirección Jurídica y Contractual, la Dirección de Operaciones y los respectivos Supervisores de los contratos, notificar este evento con una solicitud a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda.

2. En los casos donde la operación sea administrada por un operador tecnológico, la Dirección de Gestión Humana de la SDSCJ debe notificar a ésta, cualquiera novedad que se presente con el personal asociado

a la operación, con el fin de realizar las actualizaciones correspondientes en los equipos utilizados por el personal.

3. Solo podrán publicarse aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a la SDSCJ; las demás aplicaciones son de uso interno y su acceso desde fuera de la entidad se debe realizar a través de conexiones seguras con previa autorización por parte de la Dirección de Tecnología y Sistemas de la Información.

4. En los casos donde la operación sea administrada por un operador tecnológico, las conexiones externas deben ser autorizadas por la Dirección de Tecnología y Sistemas de Información de la SDSCJ.

5. En los casos donde los sistemas de información son administrados por un operador tecnológico o son propiedad de un tercero, estos deben cumplir con los lineamientos específicos de seguridad de la información descritos en el manual de seguridad de la información de la SDSCJ.

6. Las bases de datos a las que se conectan los sistemas de información internos o los sistemas de información administrados por un operador tecnológico para la operación son de la SDSCJ.

e. **SISTEMA DE VIDEOVIGILANCIA DE LAS SEDES DE LA SD SCJ**: Las credenciales de acceso a los sistemas de video vigilancia de todas las áreas que hagan parte de la SDSCJ, son de carácter estrictamente personal e intransferible; los operadores, funcionarios y contratistas de la SDSCJ no deben revelar éstas a terceros ni utilizar claves ajenas.

Los operadores tecnológicos que realizan la administración, el soporte y mantenimiento del sistema de video vigilancia de la ciudad de Bogotá, deben cumplir los lineamientos definidos tanto en la presente política como los definidos en el manual de seguridad de la información de la SDSCJ. El supervisor del contrato debe realizar el seguimiento y control del cumplimiento de la presente política.

CAPÍTULO IV
CONTROLES DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO 16. CONTROL DE ACCESO: La SDSCJ a través de La Dirección de Recursos Físicos y Gestión Documental, deben implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad.

Las dependencias de la SDSCJ con apoyo de La Dirección de Tecnología y Sistemas de la Información deben definir los controles, procedimientos e instructivos para proveer el acceso físico y lógico a los recursos físicos e informáticos, así como el perfilamiento de los usuarios autorizados para el cumplimiento de sus funciones, en las distintas sedes de la entidad.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

La SDSCJ a través de la Dirección Jurídica y Contractual, la Dirección de Gestión Humana, la Dirección de Operaciones y los respectivos supervisores de los contratos, deben establecer los mecanismos para comunicar a la Dirección de Tecnología y Sistemas de la Información, las novedades de ingreso y retiro de los funcionarios y contratistas de la SDSCJ para gestionar los derechos de acceso a los sistemas de información, recursos y servicios tecnológicos de la entidad.

La Dirección de Tecnología y Sistemas de la Información con apoyo de las dependencias de la SDSCJ 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 deberán ser los siguientes:

a. **CONTROLES CRIPTOGRÁFICOS**: La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la 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 Dirección de Tecnologías y Sistemas de la Información quien debe analizar y si es procedente aprobar.

La Dirección de Tecnologías y Sistemas de la 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. **SEGURIDAD FÍSICA Y DEL ENTORNO:** La SDSCJ a través de la Dirección de Recursos Físicos y Gestión Documental, 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.

La Secretaría Distrital de Seguridad , Convivencia y Justicia a través de la Dirección de Recursos Físicos y Gestión Documental, debe implementar los mecanismos necesarios para identificar las áreas de acceso restringido con el fin que no se permita el ingreso de funcionarios, contratistas, proveedores o terceros con dispositivos móviles, electrónicos, para tomas de fotografías o video, con el objeto de asegurar la información tanto digital como física de manera visual, de audio, de texto y documentación física de situaciones que afecten, la cadena de custodia, confidencialidad de la información, datos personales, uso indebido de la información y el buen nombre de la entidad.

Todos los funcionarios, contratistas, proveedores o terceros de la SDSCJ deben acatar lo definido por la entidad para el acceso a las áreas de acceso restringido.

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

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

En los casos específicos del Centro de Comando, Control, Comunicaciones y Cómputo-C4 y la Cárcel Distrital de Varones y Anexo de Mujeres, éstos serán los responsables de la administración de los controles definidos para el cumplimiento del artículo, los directores o jefes de oficina realizarán el seguimiento al cumplimiento de los mismos y reportarán cualquier novedad que afecte la seguridad de la información a la Dirección de Tecnologías y Sistemas de Información de la SDSCJ.

c. **SEGURIDAD DE LAS OPERACIONES**: La SDSCJ a través de la Dirección de Tecnología y Sistemas de la Información se debe encargar de la operación y administración de los recursos tecnológicos que soportan la operación de la entidad y propender por la implementación de los controles asociados a éstos para mitigar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información; para este fin debe cumplir con los siguientes lineamientos:

1. 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.
2. 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.
3. 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.
4. Implementar controles para auditar el acceso y uso de datos por parte de los funcionarios o contratistas, a los sistemas de información designados por la Dirección de Tecnología y Sistemas de Información.
5. Proveer los recursos necesarios para la implementación de los controles requeridos para la seguridad de las operaciones.

PARÁGRAFO 1. La SDSCJ a través de la Dirección de Tecnología y sistemas de Información, se reserva el derecho de monitorear la actividad donde se sospecha que se ha producido o pueda producir una violación de la Política de Seguridad y Privacidad de la Información, asegurando el debido proceso y el respeto por los derechos de las partes involucradas

PARÁGRAFO 2. En los casos donde la operación sea administrada por un operador tecnológico y con el fin que las operaciones cumplan con las condiciones de seguridad de la información requeridas para mantener la confidencialidad, integridad y disponibilidad de la información; este debe cumplir con los lineamientos establecidos y la SDSCJ con los responsables del SGSI realizarán el respectivo seguimiento para el cumplimiento de los mismos.

d. **SEGURIDAD DE LAS COMUNICACIONES**: La SDSCJ a través de la Dirección de Tecnología y Sistemas de la Información o en quien delegue, 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 SDSCJ a través de la Dirección de Tecnología y Sistemas de la Información debe implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos de la entidad propendiendo por la integridad, confidencialidad y disponibilidad de la información.

En los casos donde la operación es administrada por un operador tecnológico, este debe implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos, propendiendo por la integridad, confidencialidad y disponibilidad de la misma.

e. **CONTROLES EN LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**: La Dirección de Tecnología y Sistemas de la Información de la SDSCJ, será la única área autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de aplicaciones, sistemas de información. De igual forma la Dirección de Tecnologías y Sistemas de la Información velará porque en la adquisición, desarrollo interno o externo de sistemas de información se incorporen las buenas prácticas para el desarrollo seguro de software y estándares de seguridad informática.

Para los contratos en ejecución relacionados con recursos y componentes tecnológicos anteriores al inicio de la vigencia de la presente resolución, deben ser controlados por el responsable delegado de la SDSCJ.

En los casos donde la operación es administrada por un operador tecnológico, este debe implementar los mecanismos necesarios para proteger la información almacenada en los sistemas de información, propendiendo por la integridad, confidencialidad y disponibilidad de la misma.

En los casos donde otras dependencias de la SDSCJ requieran adquirir aplicaciones, el proceso debe llevar un visto bueno de la Dirección de Tecnología y sistemas de Información

f. **CONTROLES EN LAS RELACIONES CON LOS PROVEEDORES**: La SDSCJ a través de la Dirección de Tecnología y Sistemas de la Información y la Dirección Jurídica y Contractual, definirán mecanismos de control que aseguren que la información a la que tenga acceso un tercero, cuente con un nivel de protección adecuado y que éstos cumplan con las políticas y procedimientos de seguridad de la información establecidos.

ARTÍCULO 17. SEGURIDAD EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO: La SDSCJ deberá disponer de un plan de continuidad de negocio y a través de la Dirección de Tecnología y Sistemas de la Información del plan de recuperación ante desastres tecnológicos - DRP con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos misionales que sean considerados críticos para la continuación de la operación en la entidad de manera 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.

PARÁGRAFO: En los casos donde la operación es administrada por un operador tecnológico, este debe disponer de un plan de recuperación ante desastres, con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos misionales que sean considerados críticos para la continuación de la operación en la entidad.

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

ARTÍCULO 18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información se encarga de definir, documentar, mantener, publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos e incidentes de seguridad de la información que se presenten y que comprometan las operaciones de la misma. De igual forma la Dirección de Tecnologías y Sistemas de la Información 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 analizados por la Dirección de Tecnologías y Sistemas de la Información de acuerdo al procedimiento de incidentes de seguridad de la información.

Todos los usuarios tanto internos como externos que accedan a la información de la SD SCJ, deben realizar el respectivo reporte de eventos e incidentes de seguridad de la información a la mesa de servicio, operador tecnológico o a quien corresponda, de acuerdo a lo descrito en el procedimiento de gestión de incidentes de seguridad de la información, con el fin que estos sean analizados y evaluados a fin de mitigar los riesgos que puedan comprometer las operaciones de la entidad y amenazar la seguridad de la información de la misma.

Todos los terceros, operadores tecnológicos a los que se les reporten eventos e incidentes de seguridad de la información deben informar sobre estos, mensualmente a la Dirección de Tecnologías y Sistemas de Información con el fin que se realice un análisis de los mismos para mitigar los riesgos que comprometan las operaciones de la entidad.

ARTÍCULO 19: METODO DEFINIDO PARA OPERAR: La SDSCJ establece que la presente Política de Seguridad y Privacidad de la Información operará por medio del "MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN" en el cual se encuentran los lineamientos detallados para el cumplimiento en la implementación y monitoreo del Sistema de Gestión de Seguridad de la Información.

ARTÍCULO 20: ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO. Se espera que La Política de Seguridad y Privacidad de la Información se preserve en el tiempo. Sin embargo, se debe hacer revisiones ante cambios normativos, estructurales y tecnológicos que afecten a la SDSCJ, para asegurar que ésta cumple con el cambio de las necesidades de la entidad. La persona encargada de apoyar la implementación del sistema de gestión de seguridad de la Información es responsable por esta tarea y debe llevarla a cabo considerando los lineamientos institucionales.

ARTÍCULO 21. PROPIEDAD INTELECTUAL. Todo el material que es desarrollado por una persona natural o física mientras tenga una vinculación como funcionario o como contratista con la SDSCJ, se considera que los derechos patrimoniales son propiedad de la entidad y que es de uso exclusivo de la misma, por lo tanto, debe ser protegida contra un develado, descubrimiento o uso que menoscabe los intereses institucionales, misionales, reputacionales, económicos y en general cualquier perjuicio contra la SDSCJ, en los términos de la ley 23 de 1982 y sus normas reglamentarias y aquellas que la modifiquen.

La Dirección Jurídica y Contractual, la Dirección de Gestión Humana y la Dirección de operaciones, deben realizar las tareas pertinentes para que en los contratos suscritos con empleados, contratistas, terceros y operadores

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

tecnológicos se incluyan las cláusulas correspondientes que especifiquen los compromisos y cuidados que se debe tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad.

ARTÍCULO 22. ADMINISTRACIÓN DEL RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN. La información de la SDSCJ, se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, se debe realizar periódicamente un análisis respecto al impacto en seguridad de la información, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable.

Establecidos el nivel de riesgo y el valor de la información, se debe realizar una evaluación formal de riesgos, para que estos sean identificados, evaluados y se apliquen las acciones necesarias para subsanarlos o mitigarlos acorde con los niveles de riesgo permitidos por la Entidad.

Todos los líderes de procesos de la SDSCJ, acompañados por el Oficial de Seguridad de la Información, deben realizar la identificación, clasificación y tratamiento de riesgos de seguridad de la información, que puedan comprometer las operaciones de la entidad y amenazar la seguridad de la información de acuerdo a lo definido en la Política de Administración de Riesgos de la entidad. El reporte de las evidencias de los controles definidos para la mitigación de los riesgos se realizará de acuerdo como lo establezca la Oficina Asesora de Planeación de la entidad.

ARTÍCULO 23. CONCIENCIACIÓN EN SEGURIDAD DE LA INFORMACIÓN. La SDSCJ debe contar con un programa de concienciación en seguridad de la información permanente que permita garantizar que los funcionarios, contratistas, usuarios, terceros u operadores tecnológicos que accedan a la información de la entidad, estén informados acerca de sus responsabilidades en Seguridad de la Información y de las continuas amenazas que ponen en riesgo la información de la entidad.

Los funcionarios, contratistas, usuarios, terceros u operadores tecnológicos deben conocer y aplicar los procedimientos de seguridad de la información de la SDSCJ.

ARTÍCULO 24. CUMPLIMIENTO: La Secretaría Distrital de Seguridad, Justicia y Convivencia-SDSCJ, velarán por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

La SDSCJ, implementará y mantendrá los controles necesarios para proteger la información de funcionarios, contratistas, beneficiarios, proveedores y terceros de los cuales reciba y administre información de conformidad con la Ley de Protección de Datos Personales.

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

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

"Por la cual se adopta la Política de Seguridad y Privacidad de la Información y se definen lineamientos para su uso, actualización y aplicación"

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 establece las directrices generales estará reglamentada por los lineamientos contenidos en un manual de seguridad de la información.

ARTÍCULO 25. SANCIONES. El incumplimiento de la Política de Seguridad y Privacidad de la Información por parte de los servidores públicos de la Secretaría Distrital de Seguridad, Convivencia y Justicia puede llevar a la adopción de sanciones disciplinarias de conformidad con la Ley 734 de 2002 "Código Disciplinario Único". Así mismo, el incumplimiento por parte de los aprendices, practicantes, contratistas, proveedores, visitantes, organizaciones o entidades cooperantes y miembros del público que acedan a información de la entidad o utilicen los servicios de información proporcionados por la misma puede generar la terminación de los contratos y de las relaciones interinstitucionales y/o la suspensión de los servicios y/o dar lugar al inicio de acciones legales de conformidad con la Ley.

ARTÍCULO 26. VIGENCIA Y DEROGATORIA: La presente Resolución rige a partir del día siguiente a la fecha de su publicación y deroga las disposiciones que le sean contrarias, en especial la Resolución 541 de 2017.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los 31 DIC 2019

JAIRO GARCÍA GUERRERO
Secretario Distrital de Seguridad, Convivencia y Justicia

Elaboró: Lourdes Maria Acuña Acuña – Contratista / Héctor Paramo - Contratista
Revisó: Diego Ramírez – Contratista - Diana Carolina Peña-Contratista
Aprobó: Andrés J. Solorzano Ulloa.- Director de Tecnología y Sistemas de la Información
Aprobó: Anastasia Juliao Nacith.- Directora Jurídica y Contractual
Aprobó: Gian Carlo Suescun.- Subsecretario de Gestión Institucional