ALCALDÍA MAYOR
DE BOGOTÁ D.C.
Secretaría Distrital de Seguridad, Convivencia y Justicia

04 DIC 2017

Resolución Nº 000541

"Por la cual se adopta la Política de Seguridad 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 415 del 30 de septiembre 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 la Constitución Política de Colombia 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 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 la Constitución Política de Colombia, en su artículo 209 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 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 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 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.

Av. Calle 26 # 57 - 83
Torre 7
Pisos: 6,13, 14, 16
Código Postal: 111321
www.scj.gov.co

04 DIC 2017

Resolución Nº 000541

"Por la cual se adopta la Política de Seguridad 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 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 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 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*", 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 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.

04 DIC 2017

Resolución Nº 000541

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

Que mediante el Decreto 1078 de 2015, se expidió 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 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 dada la función establecida en el artículo 2.2.9.1.2.3 del Decreto 1078 de 2015 para el representante legal de los sujetos obligados respecto de la coordinación de la implementación de la estrategia gobierno en línea, 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 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 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 el Decreto 651 del 28 de diciembre de 2011, la Alcaldía Mayor de Bogotá creó el Sistema Integrado de Gestión Distrital – SIGD enmarcado en los Planes Estratégicos y de Desarrollo de las Entidades distritales y generó la obligatoriedad de adoptar en las mismas un enfoque basado en los procesos que se surten en su interior, en las expectativas de los usuarios, destinatarios y beneficiarios de conformidad con las funciones asignadas por el ordenamiento jurídico vigente.

Que el Decreto 652 del 28 de diciembre de 2011, adoptó la Norma Técnica Distrital del Sistema Integrado de Gestión NTD-SIG 001:2011, la cual determina las generalidades y los requisitos mínimos para establecer, documentar, implementar y mantener el SIGD.

Que la Resolución 305 de 2008 expedida por 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 respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.

04 DIC 2017

Resolución Nº 000541

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

Que la citada resolución 305 de 2008 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 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 "*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*", Artículo 12 de la resolución 305 de 2008 de la CDS.

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 el Decreto 413 de 2016, establece la estructura organizacional y las funciones de la Secretaría Distrital de Seguridad, Convivencia y Justicia, y se dictan otras disposiciones.

Que el artículo 8° del Decreto 413 de 2016, consagra entre otras funciones, como funciones de la Oficina Asesora de Planeación (...) *a. Dirigir, implementar y mantener los planes y programas relacionados con los subsistemas que conforman el Sistema Integrado ele Gestión (Gestión Ambiental, Gestión de Calidad, MECI, Seguridad Informática, Seguridad y Salud Ocupacional, Responsabilidad Social, Gestión Documental) de acuerdo con la normatividad vigente sobre la materia.*

Que el artículo 26° del Decreto 413 de 2016, consagra entre otras, como funciones de la Dirección de Tecnología y Sistemas de Información (...) *a)Garantizar el cumplimiento de los lineamientos para el fortalecimiento institucional en materia de TIC y la implementación de la estrategia Gobierno en Línea, de*

04 DIC 2017

Resolución Nº 000541

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

acuerdo con la normatividad vigente; f) Impartir lineamientos tecnológicos para el cumplimiento de estándares de seguridad, privacidad, calidad y oportunidad de la información del Sector y la interoperabilidad de los sistemas que la soportan, así como el intercambio permanente de información; i) Implementar políticas de seguridad informática y de la plataforma tecnológica de la Secretaría, definiendo los planes de contingencia y supervisando su adecuada y efectiva aplicación.

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 en el cumplimiento de sus funciones 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 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.

Que la Política de Seguridad de la Información es una declaración de las responsabilidades y de la conducta aceptada para mantener un ambiente seguro en la Secretaría Distrital de Seguridad, Convivencia y Justicia. Esta Política establece las directrices y los lineamientos relacionados con el manejo seguro de la información.

RESUELVE:

CAPITULO I
DISPOSICIONES GENERALES

ARTÍCULO PRIMERO. 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 SD-SCJ

ARTÍCULO SEGUNDO. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN La SD-SCJ protege la información física y electrónica que almacena, recolecta, produce y gestiona a través de la implementación de controles físicos y lógicos, gestión de riesgos y la 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.

ARTÍCULO TERCERO. ALCANCE Y ÁMBITO DE APLICACIÓN: La Política de Seguridad de la Información proporcionan 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.

La Política de Seguridad y Privacidad de la Información aplica a la SD-SCJ en todos los niveles de la organización, 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 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 SD-SCJ, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

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

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

- Establecer mecanismos y lineamientos para el manejo adecuado de la información.
- Mitigar los incidentes de seguridad de la información en la Secretaría
- Gestionar los riesgos asociados a la seguridad de la información que afecten la confidencialidad, disponibilidad y privacidad de la información de La SD-SCJ.

ARTÍCULO SEXTO. 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:

a) La SD-SCJ establece los roles y responsabilidades relacionados con la presente política de seguridad de la información en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

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

c) La Dirección de Tecnología y Sistemas de la Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, diseñará e implementará la estrategia para proteger la información generada, recolectada, procesada y utilizada en el cumplimiento de su misión.

d) 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.

e) Si bien la Dirección de Tecnología y Sistemas de Información 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; los propietarios de la información son los responsables de los procesos institucionales y por ende de la información registrada, la autorizaran de cambios y la solicitud de modificaciones a realizar sobre los sistemas de información o su información.

f) 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, para su protección.

g) 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 deben aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

h) 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 SD-SCJ 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.

i) Es obligación de todos los funcionarios, contratistas y proveedores adscritos a la SD-SCJ cumplir con la "POLÍTICA DE SEGURIDAD Y PRIVACIDAD 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.

j) Teniendo en cuenta que todos los activos de información deben tener un responsable, la creación de cuentas de usuario y/o correo electrónico genéricos (que no estén asociados a un funcionario o contratista) no estarán autorizadas.

k) Es responsabilidad de los funcionarios y contratistas de la SD-SCJ 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 SD-SCJ 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 SEPTIMO. PRINCIPIOS: La presente política se fundamenta en los siguientes principios:

a) La información es uno de los activos más importantes de SD-SCJ y por lo tanto se espera que sea utilizada acorde con los requerimientos de sus funciones.

b) Confidencialidad de la información de la SD-SCJ y de terceras partes debe ser mantenida, independientemente del medio o formato donde se encuentre y que sea accedida sólo por aquellos que tienen una necesidad legítima para la realización de sus funciones

c) Integridad, la información de la SD-SCJ debe preservar su integridad 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.

d) Disponibilidad, la información de la entidad debe estar disponible cuando sea requerida.

e) Privacidad, la información debe ser preservada y que sea utilizada para los propósitos que fue obtenida.

ARTÍCULO OCTAVO. RESPONSABLES: La SD-SCJ 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 SD-SCJ, quien velará por el cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información.
- El Oficial 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.

PARÁGRAFO 1: No obstante, lo estipulado en el artículo precedente, todos los funcionarios, contratistas y proveedores de la SD-SCJ son responsables del cumplimiento de la Política de Seguridad y Privacidad de la Información.

PARÁGRAFO 2: Se debe constituir la estructura funcional y administrativa referente a la seguridad de la información.

CAPITULO II
RECURSOS HUMANOS

ARTÍCULO NOVENO. GESTIÓN EN EL RECURSO HUMANO: La SD-SCJ a través de la Dirección de Gestión Humana y la Dirección Jurídica y Contractual son responsables de divulgar la Política de Seguridad y Privacidad de la Información a todos los funcionarios o contratistas que se vinculen a la entidad.

La Dirección Jurídica y Contractual 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 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.

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

CAPÍTULO III
SEGURIDAD DE LOS ACTIVOS DE INFORMACIÓN

ARTÍCULO DECIMO. GESTIÓN DE LA SEGURIDAD EN LOS ACTIVOS: La SD-SCJ 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 digital, con el objetivo de garantizar su protección.

ARTÍCULO DECIMO PRIMERO. INVENTARIO Y PROPIEDAD DE LOS ACTIVOS: La responsabilidad de la administración, gestión e implementación de controles de los activos de información está en cabeza

del propietario de los mismos. Los activos de Información de la SD-SCJ deben ser identificados, clasificados y controlados para propender 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 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 Dirección de Tecnología y Sistemas de la Información y la Dirección de Recursos Físicos y Gestión Documental.

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 DECIMO SEGUNDO. 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. En este sentido, es importante resaltar lo preceptuado el Artículo 15 de la Ley 594 de 2000 *"...Los servidores públicos, al desvincularse de las funciones titulares, entregarán los documentos y archivos a su cargo debidamente inventariados, conforme a las normas y procedimientos que establezca el Archivo General de la Nación, sin que ello implique exoneración de la responsabilidad a que haya lugar en caso de irregularidades."*

ARTÍCULO DECIMO TERCERO. 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 SD-SCJ 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 DECIMO CUARTO. 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 SD-SCJ, 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 SD-SCJ, 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 @scj.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
- 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 Dirección de Gestión Humana, la Dirección de Tecnología y Sistemas de la Información.
- 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.
- 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.
- 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 SD-SCJ.
- Está expresamente prohibido el uso del correo para el envío de contenidos insultantes, información de agremiaciones, ofensivos, injuriosos, obscenos, violatorios de los derechos fundamentales, derechos de autor o que atenten contra la integridad moral de las personas o

instituciones.

- Está expresamente prohibido distribuir información de la SD-SCJ 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 Tecnología y Sistemas de la Información.

  Las cuentas de correo electrónico se asignaran de acuerdo a la nomenclatura definida por la Dirección de Tecnología y Sistemas de Información.

b. **INTERNET:** 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 SD-SCJ hacer un uso responsable del Internet y cumplir con las políticas para tal fin aquí establecidas:

- La SD-SCJ, 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.
- La SD-SCJ, a través de la Dirección de Tecnologías y Sistemas de la Información 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, 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; está prohibido la descarga de archivos con extensiones de tipo .exe, .bat, .prg, .bak, .pig.

c. **EQUIPOS DE CÓMPUTO Y OTROS DISPOSITIVOS**: La SD-SCJ 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 dicho usuario y 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 Dirección de Tecnología y Sistemas de la 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 SD-SCJ 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 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 SD-SCJ 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 la Dirección de Tecnologías y Sistemas de la Información previa solicitud a través de la mesa de servicio.
- Es responsabilidad de los funcionarios y contratistas de la SD-SCJ 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 Dirección de Tecnología y Sistemas de la 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 Dirección de Tecnología y Sistemas de la Información 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 Dirección de Tecnología y Sistemas de la Información, en cabeza del equipo de infraestructura de Tecnología de la Información y Comunicaciones, 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 SD-SCJ.

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 SD-SCJ 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 de la Dirección de Gestión Humana y la Dirección Jurídica y Contractual notificar este evento con

una solicitud a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda.

Solo podrán publicarse aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a la SD-SCJ; 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.

CAPÍTULO IV
CONTROLES DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

ARTÍCULO DECIMO QUINTO. CONTROL DE ACCESO: La SD-SCJ a través de La Dirección de Recursos Físicos y Gestión Documental, propende por implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad.

La SD-SCJ a través de la Dirección Jurídica y Contractual y la Dirección de Gestión Humana 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 SD-SCJ 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 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 SD-SCJ 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.

04 DIC 2017

Resolución Nº 000541

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

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. **SEGURDAD FÍSICA Y DEL ENTORNO:** La SD-SCJ 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.

PARÁGRAFO: Todos los funcionarios, contratistas y visitantes que se encuentren en las instalaciones de la SD-SCJ 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 SD-SCJ 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:

- 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 a los sistemas de información designados por la Dirección de Tecnología y Sistemas de Información para el control de los funcionarios y contratistas, adicionalmente 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 SD-SCJ a través de la Dirección de Tecnología y Sistemas de la 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 SD-SCJ 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 la integridad y confidencialidad de la información.

e. **CONTROLES EN LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS:** La Dirección de Tecnología y Sistemas de la 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 el Decreto 413 de 2016. De igual forma la Dirección de Tecnologías y Sistemas de la 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 SD-SCJ 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.

ARTICULO DECIMO SEXTO. SEGURIDAD EN LA GESTIÓN DE CONTINUIDAD DE NEGOCIO: La SD-SCJ a través de la Dirección de Tecnología y Sistemas de la 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.

ARTÍCULO DECIMO SEPTIMO. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN: La SD-SCJ, 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 de seguridad de la información. 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 investigados por la Dirección de Tecnologías y Sistemas de la Información de acuerdo al procedimiento de incidentes de seguridad de la información.

PARÁGRAFO. Para la consecución efectiva de lo establecido en el presente artículo, se debe diseñar, construir y aplicar un protocolo referente al reporte de incidentes de seguridad de la información.

CAPÍTULO V
DISPOSICIONES FINALES

ARTÍCULO DECIMO OCTAVO. ADMINISTRACIÓN DE LA POLÍTICA Y PROCEDIMIENTO DE CAMBIO. Se espera que La Política de Seguridad de la Información se preserven en el tiempo. Sin embargo, se debe hacer una revisión anual o ante cambios estructurales y tecnológicos que afecten a la SD - SCJ, para asegurar que ésta cumple con el cambio de las necesidades de la Entidad. El Líder de Seguridad de la Información es responsable por esta tarea y debe llevarla a cabo considerando los lineamientos institucionales.

Cualquier miembro de la SD – SCJ puede identificar la necesidad de modificar La Política de Seguridad de la Información. Dichas inquietudes y sugerencias deben ser comunicadas al Líder de Seguridad de la Información, responsable por el mantenimiento de la misma, de acuerdo con el procedimiento diseñado para tal fin.

Ante la necesidad de una adición o cambio a la Política, el Líder de Seguridad de la información lo realizará y se ajustará a las medidas tomadas por el órgano colegiado que se debe crear en los términos del parágrafo 2 del artículo octavo de la presente resolución. La formalización de la nueva Política de Seguridad de la

04 DIC 2017

Resolución Nº 000541

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

Información será realizada mediante el procedimiento establecido por dicho órgano.

ARTÍCULO DECIMO NOVENO. PROPIEDAD INTELECTUAL. La Propiedad Intelectual se define como la disciplina jurídica que tiene por objeto la protección de bienes inmateriales, de naturaleza intelectual y de contenido creativo producto del ingenio humano.

Todo el material que es desarrollado por una persona natural o física mientras tenga una vinculación como funcionario o como contratista con la SD – SCJ, 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 SD - SCJ. Las relaciones institucionales de los empleados deben incluir cláusulas que especifiquen los compromisos y cuidados que deben tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad. Así mismo, los contratos de prestación de servicios deben incluir los compromisos y cuidados que deben tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad por parte de los contratistas.

ARTÍCULO VIGESIMO. ADMINISTRACIÓN DEL RIESGO PARA LA SEGURIDAD DE LA INFORMACIÓN. La información de la SD –SCJ, 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 en la Entidad.

Cada usuario de la información debe estar enterado de los procedimientos de reporte de riesgos que puedan tener impacto en la seguridad de la información de la SD - SCJ y se requiere que reporten inmediatamente cualquier sospecha u observación de un incidente a la seguridad de la información.

ARTÍCULO VIGESIMO PRIMERO. DE LA CAPACITACIÓN Y CREACIÓN DE LA CULTURA EN SEGURIDAD DE LA INFORMACIÓN.

La SD - SCJ debe contar con un programa permanente que permita asegurar que los funcionarios,

04 DIC 2017

Resolución Nº 000541

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

contratistas, usuarios y terceros 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 y terceros deben estar enterados de los procedimientos de seguridad de la información que deben aplicar adicionalmente a los que se requieren para realizar su función de trabajo.

ARTÍCULO VIGESIMO SEGUNDO. CUMPLIMIENTO: La Secretaría Distrital de Seguridad, Justicia y Convivencia-SD-SCJ velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con la seguridad de la información.

La SD-SCJ, 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 SD-SCJ implementará y mantendrá los controles necesarios para dar cumplimiento a las disposiciones legales sobre derechos de autor, propiedad intelectual, ley de transparencia y Estrategia de Gobierno en Línea.

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 VIGESIMO TERCERO. SANCIONES. El incumplimiento de la política de seguridad 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, proveedores, visitantes, organizaciones o entidades cooperantes y miembros del público que utilicen los servicios de información proporcionada por la entidad puede generar en la terminación de los contratos y

0 4 DIC 2017

Resolución Nº 000541

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

de las relaciones inter-institucionales y/o la suspensión de los servicios y/o dar lugar al inicio de acciones legales de conformidad con la Ley.

ARTÍCULO VIGESIMO CUARTO. VIGENCIA Y DEROGATORIA: La presente Resolución rige a partir de la fecha de su publicación y deroga las disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

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

0 4 DIC 2017

DANIEL MEJÍA LONDOÑO
Secretario Distrital de Seguridad, Convivencia y Justicia

Elaboró: Diego Ramirez Pulido – Ing. Seguridad de la Información
Revisó: Diana Carolina Peña-Abogada Dirección Tic
Aprobó: Carlos F. Camacho A.- Director de Tecnología y Sistemas de la Información
Aprobó: Julia Elena González Henao – Directora de Recursos Fisicos y Gestión Documental
Aprobó: Efvanny Paola Palmariny Peñaranda-Oficina Asesora de Planeación
Aprobó: Hugo León Duarte – Director de Gestión Humana
Aprobó: Anastasia Juliao Nacith.- Directora Jurídica y Contractual
Aprobó: Gian Carlo Suescun.- Subsecretario de Gestión Institucional