MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

TABLA DE CONTENIDO

1. INTRODUCCIÓN

"Las denominadas agendas o planes son los términos que comúnmente los gobiernos de la región usan para denominar el mecanismo para el desarrollo "armónico y coherente", de las iniciativas de Gobierno Electrónico. Habitualmente comprenden un período de 3 a 5 años. Idealmente las agendas deben estar alineadas con los objetivos estratégicos del desarrollo tecnológico y digital del país" (A. Nasser, 2011)

Entendiendo lo anterior, a lo largo de este milenio, Colombia a través del Ministerio de Tecnologías de la Información y las Comunicaciones-MINTIC ha desarrollado políticas en cuanto a gobierno digital se refiere, que permiten que tanto el estado colombiano como los ciudadanos puedan trabajar sobre una base de eficiencia, transparencia y accesibilidad.

Para poder llevar a cabo esto, es necesario que desde la gestión interna de las entidades se comprenda a todo nivel la importancia de los diferentes habilitadores transversales de la política de gobierno digital en la consecución de los objetivos propuestos donde la tecnología aporta al cumplimiento estratégico de la misionalidad de las mismas.

Uno de estos habilitadores transversales, corresponde al de seguridad de la información, el cual busca que las entidades públicas implementen los lineamientos de seguridad necesarios en todos sus procesos, trámites, servicios, sistemas de información, infraestructura y en general.

Teniendo en cuenta lo anterior, y con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información, la alta dirección de la Secretaría Distrital de Seguridad, Convivencia y Justicia-SDSCJ, mediante resolución adopta la política de seguridad y privacidad de la información, estableciendo directrices generales que deben ser aplicadas por cada uno de los funcionarios y/o contratistas de la Entidad, con el propósito de mitigar los riesgos a los que día a día éstos se ven expuestos.

Este manual de seguridad de la información, es una declaración detallada de la alta dirección de la SDSCJ, donde se precisan los lineamientos de seguridad y privacidad de la información definidos por la Secretaria Distrital de Seguridad, Convivencia y Justicia, los cuales deben ser adoptados por todos los funcionarios, contratistas y terceros que tengan relación con la entidad.

En la Secretaria de Seguridad Convivencia y Justicia – SDSCJ, la seguridad y privacidad de la información permiten realizar el aseguramiento de la identificación, valoración y gestión de los activos de información además de los riesgos, en función del impacto que constituyen para la entidad, que son de un alto valor; por lo tanto debemos entender que el manual de seguridad es el método definido para operar la política de la seguridad y privacidad de la información de la SDSCJ. El manual a su vez es un proceso integrado por una serie de estrategias, medidas preventivas y reactivas para proteger la información y mantener su confidencialidad, disponibilidad e integridad.

Por último, se entiende que las políticas del Sistema de Gestión de Seguridad de la Información-SGSI de la SDSCJ, aplican a toda la entidad y son de obligatorio cumplimiento para la Alta Dirección, Directores de área, Jefes de Oficina, funcionarios, contratistas, terceros, operadores y en general todas las personas que en razón del cumplimento de sus funciones y de la SDSCJ accedan a la información de la entidad.

2. OBJETO DEL DOCUMENTO

Es el instrumento de apoyo de la SD-SDJ, donde se establecen los lineamientos, directrices e instrucciones para el cumplimiento de la política de seguridad y privacidad de la información de manera detallada, la cual debe ser conocida y cumplida por todos los funcionarios, contratistas y operadores de la Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ en pro de velar por la Confidencialidad, Disponibilidad e Integridad de la Información de la Entidad, enmarcado en el cumplimiento legal y normativo que aplica a la SDSCJ

3. GLOSARIO DE TÉRMINOS

Acceso Privilegiado: Que cuenta con una ventaja exclusiva o especial.

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de no una conformidad, de tal forma que no se vuelva a presentar

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo

Activo de información: se refiere a cualquier información o elemento que tiene valor

estratégico para los procesos de negocio de la entidad. (Sistemas, soportes, edificios, hardware, recurso humano).

- **Datos**: Corresponde a los elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la SDSCJ.
- Aplicaciones: Corresponde al software que se utiliza para la gestión de la información.
- **Personal:** Corresponde a todo el personal de la SDSCJ, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la SDSCJ.
- **Servicios**: Corresponde a los servicios internos, suministrados al interior de la entidad o servicios externos; suministrados por la entidad a un tercero; cliente o usuarios
- **Tecnología**: Corresponde a los equipos utilizados para gestionar la información y las comunicaciones.
- **Instalaciones**: Corresponde a todos los lugares en los que se aloja información de la entidad.

Ambiente de Pruebas: conjunto de elementos de hardware y software que soportan los sistemas de información utilizados para verificar la funcionalidad de los desarrollos de software y aplicativos y realizar los ajustes necesarios antes de ser puestos en funcionamiento en el ambiente de producción de la entidad.

Ambiente de Producción: conjunto de elementos de hardware y software que soportan los sistemas de información utilizados por los funcionarios para la ejecución de las operaciones de la Entidad En este ambiente deben residir aplicaciones en producción, bibliotecas o directorios que contengan archivos de datos, bases de datos, programas ejecutables o compilados.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: uso sistemático de una metodología para estimar los riesgos e identificar sus fuentes, para los activos o bienes de información.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticidad: Es la propiedad que garantiza que la identidad de un sujeto o recurso es la que declara y se aplica a entidades tales como usuarios, procesos, sistemas de información.

Autorización: Proceso o procedimiento oficial, por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos del sistema de información o activos físicos.

Backup o copia de seguridad: copia de respaldo de la información.

Confidencialidad: propiedad que garantiza que la información no sea accedida, ni sea revelada a personas, entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas; y que pueden ser de carácter administrativo, técnico o legal.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Criticidad: medida del impacto que tendría la organización debido a una falla de un sistema y que éste no funcione como es requerido.

Custodio: ente, área, proceso o persona encargada de preservar y resguardar la información entregada y que generalmente son de propiedad de otro proceso o área.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Disponibilidad: principio que garantiza que la información esté accesible y utilizable cuando lo requieran las personas, entidades o procesos autorizados

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y

correlacionando otros tipos de información.

Encriptación: Proceso que permite volver ilegible la información que se considera importante. Una vez la información esta encriptada solo puede accederse aplicando una clave.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento de seguridad de la información: situación detectada en un sistema, servicio o red que indica una posible violación de la política de seguridad de la información, un fallo de las salvaguardas o una situación desconocida hasta el momento y que puede ser relevante para la seguridad de la información de la entidad.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

ICC: La Infraestructura Crítico Cibernético son las infraestructuras estratégicas soportadas por tecnologías de información y comunicaciones (TIC) o tecnologías de operación (TO) cuyo funcionamiento es indispensable por lo que su perturbación o destrucción tendría un grabe impacto sobre los servicios esenciales.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente de seguridad de la información: es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información, tales como, un acceso no autorizado o intento del mismo; uso, divulgación, modificación o destrucción no autorizada de información; un impedimento en la operación normal de las redes, sistemas o recursos informáticos.

Información confidencial: información, restringida o secreta, que es extremadamente sensible y únicamente puede ser conocida por personas específicas dentro de la Entidad.

Para compartir esta información con terceros debe existir autorización expresa (escrita) de las directivas de la entidad. Toda la información definida como reserva bancaria será clasificada como Confidencial

Infraestructura de procesamiento de información: cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red1 o faciliten información con clasificación confidencial o superior.

Integridad: principio que garantiza que la información sea exacta, coherente y completa desde su creación hasta su destrucción.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza)

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Medio removible: medio que permite llevar o transportar información desde un computador a otro. Los medios removibles incluyen cintas, discos duros removibles, CDs, DVDs, unidades de almacenamiento USB.

No-Repudio: es una propiedad de la seguridad de la información en la cual el emisor no puede negar el envío o recepción.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Principios de Seguridad de la información: confidencialidad, disponibilidad e integridad.

Propietario/responsable de la información: individuo, entidad o unidad de negocio que tienen bajo su responsabilidad la administración para el control, producción, desarrollo, mantenimiento, uso y seguridad de los activos de información. Los propietarios de la información deben garantizar la seguridad, integridad, disponibilidad y confidencialidad de la información y deben coordinar la implementación de políticas con otros propietarios de información y con propietarios de infraestructura. Los propietarios deben especificar cómo se debe utilizar la información y como se debe proteger, además de definir cómo se administrarán los procedimientos de control y cómo se aplicarán los niveles apropiados de protección para la información acorde con su clasificación (Pública, Pública Clasificada y Pública Reservada).

Propietarios de infraestructura: administradores de recursos tecnológicos utilizados para el manejo y/o administración de la información. Son responsables por la funcionalidad, operación, continuidad, manejo y uso de todos los sistemas compartidos, las redes, el soporte y el mantenimiento, el software estándar, los sistemas telefónicos y de comunicaciones, y los servicios relacionados. Los propietarios de infraestructura son responsables de coordinar los servicios de recuperación de los elementos de tecnología informática y de implementar y manejar efectivamente las funciones y procedimientos de seguridad para cumplir con las necesidades de los propietarios de la información y de la Entidad.

Responsable de activo de información:

Seguridad de la Información: consiste en resguardar y proteger la confidencialidad, integridad y disponibilidad de la información que maneja la entidad, mediante un conjunto de medidas preventivas y correctivas.

Sensibilidad: nivel de impacto que una divulgación no autorizada podría generar.

Servicio: es cualquier acto o desempeño que una persona puede ofrecer a otra, que es esencialmente intangible y que no conlleva ninguna propiedad. Su producción puede o no estar ligada a un producto físico.

SGSI: Sistema de Gestión de Seguridad de la Información.

Soportes físicos: documentos en soporte físico (cartas, informes, normas, contratos) y en medios de almacenamiento físico.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante encripta los datos de la víctima y exige un pago por la clave de descifrado.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información

Terceros: toda persona, jurídica o natural, como proveedores, contratistas o consultores, que provean servicios o productos a la entidad.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se pueden rastrear únicamente hasta dicha entidad.

Usuarios: personas que, directa o indirectamente, tengan algún tipo de relación con la Entidad y/o que tengan acceso a los recursos tecnológicos de la entidad, por ejemplo: funcionarios, contratistas, terceros, proveedores, entre otros.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIIEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

4. MARCO LEGAL

- **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".

- **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.

- **Ley 1266 de 2008**: por la cual se dictan 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.

- **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.

- **Decreto 1377 De 2013:** Por el cual se reglamenta parcialmente la Ley 1581 de 2012" y se dictan disposiciones generales para la protección de datos personales.

- **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.

- **Conpes 3854 de 2016**: Mediante el cual 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.
- Decreto 413 de 2016: Mediante el cual se establece la estructura organizacional y las funciones de la Secretaría Distrital de Seguridad, Convivencia y Justicia, y se dictan otras disposiciones.

- **Resolución 541 de 2017**: Por la cual se adopta la política de seguridad de la información en la SDSCJ y se definen lineamientos para su uso, actualización y aplicación.

- **Resolución 645 de 2018**: Por la cual se adopta la política de protección de datos personales de la SDSCJ.

- **Decreto 1008 de 2018:** Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.

- **Resolución 712 de 2018**: Mediante la cual se conforma el Comité Institucional de Gestión y Desempeño de la Secretaría de Seguridad, Convivencia y Justicia.

- **Decreto 510 de 2019:** "Por el cual se reglamenta el Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 y se dictan otras disposiciones", en el Artículo 12°.- Coordinación con entidades, nuevos sistemas o plataformas se dispone el numeral número 5, " ... 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...", además, en el Artículo 24 dispone lo siguiente: "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 ".

- **Conpes 3975:** mediante el cual se establece la Política Nacional para la Transformación Digital e Inteligencia Artificial.

- **Decreto 2106 de 2019**: por el cual se dictan normas para simplificar, suprimir y reformar trámites , procesos y procedimientos innecesarios existentes en la administración pública.

5. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

De acuerdo a lo descrito en la resolución 541 de 2017, en el artículo segundo, La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, 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.

Por tanto, es responsabilidad de la Alta Dirección, funcionarios, contratistas y proveedores dar estricto cumplimiento a la política general de seguridad de la información y a las políticas anexas descritas en este manual.

El Comité Institucional de Gestión y desempeño, en el marco del Modelo Integrado de Planeación y Gestión liderará y facilitará la implementación del Sistema de Gestión de Seguridad de la Información – SGSI, como habilitador transversal de la política de gobierno digital y con apoyo de la Dirección de Tecnología y Sistemas de Información, velará por la puesta en funcionamiento y el fortalecimiento de controles que permitan mitigar la exposición a riesgos de Seguridad de la Información en la Entidad, así mismo se propenderá por la implementación y la mejora continua del SGSI de la SDSCJ, así como la divulgación y apropiación de las políticas y procedimientos transversales para la Entidad que se encuentren en el SGSI. De igual manera se revisarán las políticas de seguridad de la información, cada año o cuando existan cambios en la entidad, que deban ser incluidos en la misma.

La Secretaría Distrital de Seguridad, Convivencia y Justicia – SDSCJ, deberá tener en cuenta las políticas de seguridad de la información para la ejecución de proyectos en la Entidad.

6. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Los objetivos de control definidos a continuación corresponden a los definidos en la Norma ISO/IEC 27002:2013 y están asociados a los controles que establecerá la Secretaría Distrital de Seguridad, Convivencia y Justicia con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información de la entidad.

A.6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.	
OBJETIVO:	Establecer los lineamientos específicos que se deben implantar en el entorno general de seguridad de la información a nivel interno y externo de la Secretaría Distrital de Seguridad, Convivencia y Justicia.
ALCANCE:	Esta política aplica para todos los funcionarios, contratistas, proveedores, operadores tecnológicos con los cuales la Secretaría Distrital de Seguridad, Convivencia y Justicia establezca un vínculo contractual.

A.6.1 Organización interna

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información establece la Matriz de Roles y Responsabilidades del SGSI el cual se describe en el anexo 1 del presente manual.
- La Alta Dirección de la Secretaría Distrital de Seguridad, Convivencia y Justicia, velará por el cumplimiento y mantenimiento de la política de seguridad y privacidad de la información.
- El Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Seguridad, Convivencia y Justicia liderará y facilitará la implementación de la estrategia de Gobierno Digital y de seguridad de la información en la Entidad y se desempeñará como su respectivo comité.
- El Director de Tecnologías y Sistemas de Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia garantizará el cumplimiento de los lineamientos para el fortalecimiento institucional en materia de TIC y la implementación de la Estrategia de Gobierno Digital.

- La Dirección de Tecnología y Sistemas de Información, designará al oficial de seguridad de la información de la entidad.

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, será la encargada de definir e implementar el plan de seguridad de la información acorde con los objetivos estratégicos de la Entidad.

- La Dirección de Tecnología y Sistemas de Información definirá una arquitectura de seguridad para la Entidad y facilitará la incorporación de las mejores prácticas de seguridad de la información en todas las áreas de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

- La Dirección de Tecnología y Sistemas de Información participará activamente en los proyectos de la Entidad para recomendar los controles que sean pertinentes para administrar o mitigar los riesgos asociados a seguridad de la información.

- La Dirección de Tecnología y Sistemas de Información velará porque se realicen las pruebas de seguridad de manera periódica a los sistemas de información desarrollados, adquiridos o contratados por la Entidad.

- La Dirección de Tecnología y Sistemas de Información, participará y brindará acompañamiento a las áreas de la SDSCJ en lo referente al Sistema de Gestión de Seguridad de la Información alineándolo al Sistema Integrado de Gestión, de acuerdo con lo establecido por la Oficina Asesora de Planeación de la Entidad.

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, apoyará a las áreas de la entidad, en la adecuada identificación, clasificación y valoración de los activos de información

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, realizará conjuntamente con las áreas de la Entidad la adecuada administración y evaluación de los riesgos de seguridad digital.

- La Dirección de Tecnología y Sistemas de Información, velará por la confidencialidad, integridad y disponibilidad de la información de la SDSCJ brindando los lineamientos para el manejo y adecuada protección de los activos de información de la Entidad.

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, deberá establecer y mantener una relación cercana con las autoridades y grupos de interés o foros de especialistas en seguridad de la información, para que éstos puedan ser contactados de manera oportuna en caso que se presente un incidente de seguridad de la información.

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, deberá implementar los controles necesarios con el fin que exista segregación de funciones que permitan identificar quien administra, opera, mantiene o audita los sistemas de información de la entidad.

- En los casos que la operación admnistrada por un operador tecnológico, este deberá implementar controles adicionales a los definidos por la Dirección de Tecnología y Sistemas de Información de la SDSCJ.

- La Dirección de Tecnología y Sistemas de Información de la SDSCJ, deberá definir por medio de la PMO los diferentes riesgos de seguridad de la información en la gestión de los proyectos de TIC. Por lo cual deberá tener en cuenta los objetivos de seguridad de la información, valorar los riesgos de seguridad presentados en los proyectos y hacer seguimiento a los mismos.

- Los líderes de cada uno de los procesos de la SDSCJ propenderán por la protección de la información, velando por la debida confidencialidad, integridad, disponibilidad, de la misma.

- Los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia, deben dar cumplimiento a las políticas de seguridad de la información y participar en las jornadas de sensibilización o divulgación de las mismas, las cuales serán lideradas por La Dirección de Tecnología y Sistemas de Información y la Dirección de Gestión Humana.

- 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.

- Los funcionarios, contratistas o terceros que tengan acceso a la información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, deben tener definidas sus funciones, con el fin de reducir el uso indebido y no autorizado a los activos de información de la entidad.

- Los funcionarios, contratistas y terceros de la SDSCJ, especialmente los del Centro de Comando, Control, Comunicaciones y Computo – C4 y de la Carcel Distrital de Varones y Anexo de Mujeres, por la criticidad de la información allí manejada, tendrán áreas restringidas de acceso con dispositivos móviles, electrónicos, para tomas de fotografías o video, con el fin 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, el buen nombre de la SDSCJ.

- La SDSCJ a través de la Dirección de Recursos Fisicos y Gestión Documental, deberá establecer los mecanismos necesarios para realizar el control de acceso al personal que ingrese, de manera que se pueda identificar la persona, área que visita en la entidad (autorizados y no autorizados). De igual manera proporcionar al personal de seguridad las indicaciones que se deben entregar al ingresar a la entidad.

- La SDSCJ deberá realizar control al personal que realice grabaciones de video, de audio, copie o escanee algún documento digital o físico, para que por las razones que justifiquen el hecho, estén debidamente autorizadas por la entidad; en caso de no estar autorizadas las evidencias deberán ser borradas de los medios por los cuales se obtuvieron.

- Los funcionarios, contratistas o terceros no deben realizar grabaciones de video, de audio sin la debida autorización.

A.6.2 Dispositivos móviles y teletrabajo

- La Dirección de Tecnología y Sistemas de Información, revisará los equipos de cómputo de los funcionarios o contratistas que sean utilizados para teletrabajo.

- La Dirección de Tecnología y Sistemas de Información, realizará el cifrado de discos de los computadores portátiles, para preservar la confidencialidad de la información en caso de hurto o robo de los equipos.

- La Dirección de Tecnología y Sistemas de Información, velará porque los dispositivos móviles que se conecten a la red de la Secretaría Distrital de Seguridad, Convivencia y Justicia tengan control de acceso y segregación.

- Los funcionarios y contratistas de la SDSCJ deberán reportar la pérdida, robo o cualquier incidente relacionado con los computadores portátiles que tienen asignados a la Dirección de Tecnología y Sistemas de Información y a la Dirección de Recursos Físicos.

- Los funcionarios que manejen información de la SDSCJ a través de dispositivos móviles personales o entregados por le entidad, deberán protegerla física y lógicamente con el fin de evitar el hurto, acceso o divulgación de información no autorizada.

- Todo dispositivo móvil de la SDSCJ deberá tener control de acceso ya sea por contraseña, patrón o huella.

- Los funcionarios y contratistas deberán evitar la descarga de contenidos sospechosos o que procedan de fuentes no verificables (tanto a través de correo, como de navegación) en los dispositivos móviles y equipos portátiles entregados por la entidad.

- Los funcionarios y contratistas que tengan asignado un dispositivo móvil de la SDSCJ, serán responsables de hacer buen uso de la información de la Entidad que sea almacenada en estos dispositivos teniendo en cuenta que éste es para uso exclusivo de sus funciones u obligaciones contractuales.

- Los funcionarios y contratistas que tengan asignado un dispositivo móvil de la SDSCJ no están autorizados a cambiar la configuración, desinstalar software, formatear o restaurar de fábrica el equipo asignado. Únicamente debe aceptar y aplicar las actualizaciones requeridas por el equipo.

- La Dirección de Tecnología y Sistemas de Información deberá definir las condiciones y restricciones con el fin de velar por la confidencialidad, disponibilidad e integridad de la Información para la aprobación de los casos de Teletrabajo en la Entidad.

- Los funcionarios y contratistas que requieran acceder a los recursos informáticos de la SDSCJ fuera de las instalaciones de la Entidad, deberán realizarlo a través de una conexión de red virtual privada (VPN), previa autorización del líder de proceso y de la Dirección de Tecnología y Sistemas de Información.

- Los funcionarios y contratistas que utilicen dispositivos móviles, portátiles entre otros equipos suministrados por la SDSCJ, serán responsables del préstamo de los equipos asignados.

- La Dirección de Tecnología y Sistemas de Información, se reserva el derecho de monitorear las conexiones que se establecen para teletrabajo.

- La Dirección de Tecnología y Sistemas de Información, en los procesos de concienciación deberá incluir los riesgos adicionales de seguridad en el uso de dispositivos móviles.

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información autorizará la creación de las VPN a los contratistas o funcionarios para que realicen sus actividades mediante teletrabajo, previa autorización del jefe inmediato o supervisor de contrato.

A.7 SEGURIDAD DE LOS RECURSOS HUMANOS.	
OBJETIVO:	Asegurar que los funcionarios de la entidad entiendan las responsabilidades en materia de Seguridad de la información, con el fin de mitigar sus riesgos.
ALCANCE:	Esta política aplica para todos los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia establezca un vínculo contractual.

A.7.1 Antes de Asumir el Empleo

- La Dirección de Gestión Humana y la Dirección Jurídica y Contractual realizarán las correspondientes verificaciones de antecedentes de todos los funcionarios o contratistas respectivamente, candidatos a un empleo en la Secretaría Distrital de Seguridad, Convivencia y Justicia, de acuerdo al perfil al cual se este aplicando.

- La Dirección de Gestión Humana y la Dirección Jurídica y Contractual, deberán establecer los mecanismos necesarios para que los funcionarios y contratistas aprueben el tratamiento de los datos personales de acuerdo a la Ley 1581 de 2012 en la firma del contrato con la Secretaría Distrital de Seguridad, Convivencia y Justicia.

- La Dirección de Gestión Humana y la Dirección Jurídica y Contractual, deberán establecer los mecanismos necesarios para que los funcionarios y contratistas adopten desde el comienzo de la relación contractual lo descrito tanto en la política de seguridad de la información como en este manual.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia a través de la Dirección de Tecnología y Sistemas de Información, implementará las acciones necesarias para que los funcionarios y contratistas entiendan sus responsabilidades con respecto a la seguridad de la información de la entidad.

A.7.2 Durante la Ejecución del Empleo

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de La Dirección de Tecnología y Sistemas de Información velará por la continua sensibilización y toma de conciencia a los funcionarios y contratistas respecto de las políticas de seguridad de la información establecidas en la Entidad y a las responsabilidades de seguridad de acuerdo a los cargos desempeñados.

- Todos los funcionarios, contratistas y terceros de la SDSCJ, en especial los del Centro de Comando, Control, Comunicaciones y Computo – C4 y de la Cárcel Distrital de Varones y Anexo de Mujeres, por la criticidad de la información allí manejada, deberán cumplir las políticas de seguridad de la información de la Secretaria de Seguridad Convivencia y Justicia SDSCJ, durante la realización de las actividades que hacen parte del procesamiento o consulta de información en los recursos tecnológicos.

- Todos los funcionarios, contratistas y terceros de la SDSCJ, en especial los del Centro de Comando, Control, Comunicaciones y Computo – C4 y de la Cárcel Distrital de Varones y Anexo de Mujeres, por la criticidad de la información allí manejada, deberán almacenar la información de la operación, únicamente en los repositorios autorizados la SDSCJ.

- Todos los funcionarios, contratistas y terceros de la SDSCJ deberán cambiar las contraseñas en los diferentes sistemas de información y recursos tecnológicos de manera periódica por lo menos cada 3 meses.

- El incumplimiento de las políticas de seguridad de la información de la SDSCJ y del manual de seguridad y privacidad de la información por parte de los funcionarios,contratistas y terceros de la Entidad podrá incurrir en sanciones disciplinarias o legales según corresponda.

A.7.3 Terminación y Cambio de Empleo

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, deberá comunicar a los funcionarios y contratistas, las responsabilidades respecto a seguridad de la información que se derivan de la terminación o cambio de empleo.

- La Secretaría Distrital Seguridad, Convivencia y Justicia, a través de la Dirección de Recursos Físicos y Gestión Documental y Dirección de Tecnología y Sistemas de

Información deberá establecer los mecanismos para que los funcionarios o contratistas hagan entrega de los implementos entregados para el desarrollo de las funciones u obligaciones; entre las que se encuentran credenciales, tarjeta de proximidad, carnet entre otros.

- La Dirección de Tecnologías y Sistemas de Información, deberá retirar o cambiar las credenciales de los funcionarios y contratistas en el momento de la terminación o cambio de empleo respectivamente.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, deberá informar a los clientes, contratistas y /o proveedores de la terminación o cambio de empleo de un funcionario y/o contratista especifico.

A.8 GESTION DE ACTIVOS	
OBJETIVO:	Velar porque los activos de información de la Secretaría Distrital de Seguridad, Convivencia y Justicia tengan un propietario y que cumplan con el nivel de protección y uso apropiado.De igual manera establer los controles necesarios para la protección de los activos de información de la entidad.
ALCANCE:	Aplica para los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

A.8.1 Responsabilidad de los activos

- Los líderes de los procesos de la SDSCJ serán los propietarios de los activos de información identificados para sus procesos y no deberán existir varios propietarios para un mismo activo de información. activos

- La identificación, clasificación y valoración de activos de la SDSCJ, deberá ser realizado por los lideres de proceso, en el formato de registro de activos de información F-FD-513, de acuerdo a lo definido en la guía de gestión de activos de información G-FD-1 de la Entidad. Este proceso que debe ser actualizado anualmente o de acuerdo a los cambios normativos vigentes.

- Los funcionarios, contratistas y usuarios de los activos de información y de la información de la SDSCJ deben:
  - Aceptar y cumplir las políticas de seguridad de la información establecidas en la Entidad
  - Proteger contra pérdida, modificaciones y acceso no autorizados a los activos de información y la información de la Entidad.
  - Comprender y aceptar sus responsabilidades frente al acceso a los diferentes sistemas de información que se tienen o administran en la Entidad. activos

- La Dirección de Tecnología y Sistemas de Información, atraves del oficial de Seguridad de la Información y la Dirección de Recursos Físicos y Gestión Documental, atraves de funcionario delegado brindarán el acompañamiento técnico a los líderes de proceso para la identificación de los activos de información de todos los procesos de la entidad.

- El inventario de Activos de Información de la Secretaría Distrital de Seguridad, Convivencia y Justicia deberá ser publicado en el sitio web de la Entidad, acorde con lo descrito la Ley 1712 de 2014.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, deberá identificar dentro del consolidado de los activos de información identificados en los procesos, los activos críticos y los ICC a los cuales les realizará la respectiva gestión de riesgos.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, deberá asegurar la protección efectiva de todos los activos de información de la entidad, incluidos las ICC.

- Las partes externas que accedan a información de la Entidad deberán ser responsables del uso que hacen de los recursos asignados para la ejecución de sus funciones.

- Los lideres de proceso de la Secretaría Distrital de Seguridad, Convivencia y Justicia, deberán realizar la respectiva aceptación de los activos de información del proceso a su cargo, con el fin de establecer posteriormente los riesgos de seguridad digital a los que estos se vean expuestos.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, debe asegurar que todos los funcionarios, contratistas o partes externas que hagan uso de activos de información de la entidad, hagan la respectiva devolución de los mismos, en el momento de la terminación del empleo, contrato o acuerdo.

- Los propietarios de los activos de información deberán garantizar la devolución de los mismos, una vez se finalice el vínculo con la Entidad o se realice una modificación de las funciones u obligaciones contractuales.

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio,

deberá realizar el borrado seguro de la información contenida en los equipos de cómputos que funcionarios y contratistas devuelven al finalizar el vínculo contractual con la Entidad

A.8.2 Clasificación de la Información

- Los activos de información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, se deben clasificar de acuerdo con su confidencialidad, disponibilidad e integridad, teniendo en cuenta lo descrito en la guía de gestión de activos de información G-FD-1 de la SDSCJ, lo cual ponderará la importancia o criticidad el activo indicando si es Alta, Media o Baja.

- Únicamente el Líder de Proceso como propietario de la Información podrá reasignar o cambiar el nivel de clasificación de los activos de información, así mismo una vez realizado el cambio, deberá cumplir con los siguientes aspectos:

  - ✓ Asignarle una fecha de modificación de la clasificación del activo.
  - ✓ Comunicarlo a La Dirección de Tecnología y Sistemas de Información y Dirección de Recursos Físicos y Gestión documental.
  - ✓ Comunicar los cambios realizados para que los usuarios del activo de información conozcan la nueva clasificación.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección de Recursos Físicos y Gestión Documental, deberá establecer los mecanismos necesarios para proteger la información catalogada como Información Pública reservada, teniendo en cuenta el medio en el esta que se encuentre.

- La información sensible y la información pública reservada deberá protegerse incluso en los ambientes de pruebas.

- Los funcionarios y contratistas de la SDSCJ, no deben divulgar información pública clasificada o pública reservada de la Entidad a personas no autorizadas o a entes externos, a menos que se realice por el canal oficialmente establecido y con la aprobación previa del líder de proceso al cual pertenece el activo de información.

- La información que se obtenga, genere o procese en la Secretaría Distrital de Seguridad, Convivencia y Justicia, sólo podrá ser utilizada para los fines propios de la misión de la SDSCJ, por ningún motivo, la información podrá ser vendida, ni transferida o intercambiada con terceros ni a título oneroso o gratuito.

- La información de la Entidad no debe ser divulgada sin contar con los permisos correspondientes, además, ningún funcionario, contratista o proveedor debe copiarla o extraerla en el momento en que se retire de la Entidad o durante su permanencia.

- Los terceros,proveedores u operadores tecnológicos que accedan a la información de la Secretaría Distrital de Seguridad, Convivencia y Justicia, no deben hacer copias de la información suministrada por la Entidad, ni podrán transferirla a otro equipo a través de la red, sin la autorización escrita de la Entidad

- La Dirección de Tecnología y Sistemas de Información, deberá establecer los mecanismos necesarios para que los sistemas de información de la Entidad, cuenten con los controles de protección requeridos para el acceso a la información definida como reservada.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia deberá establecer los mecanismos necesarios para el adecuado etiquetado de la información, de acuerdo con el nivel de clasificación asignado teniendo en cuenta los tipos de información descritos en la guía de gestión de activos de información G-FD-1.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnología y Sistemas de Información,deberá establecer los mecanismos necesarios para el manejo, procesamiento, almacenamiento de la información pública clasificada y pública reservada de la Entidad.

- Los líderes de procesos deberán velar por el manejo adecuado de los activos de información, teniendo en cuenta su clasificación, de igual manera, propenderá por implementar los controles pertinentes de acuerdo a la criticidad o importancia del activo de información.

- Los funcionarios y/o contratistas a los que se haya asignado un equipo de computo en la entidad, no debe almacenar información, como música, videos y fotos que no sean de carácter estrictamente institucional.

A.8.3 Manejo de Activos

- La Dirección de Tecnología y Sistemas de Información implementará la política sobre la restricción y uso de medios removibles en la Entidad y validará las excepciones que haya lugar con los líderes de cada proceso.

- Todos los medios removibles que contengan información de la entidad deben estar ubicados en un ambiente protegido y seguro, de acuerdo con las especificaciones del fabricante.

- Con el fin de velar por la disponibilidad de la información para aquellos medios removibles que entren en su fase de obsolescencia, se deberá realizar oportunamente una copia de respaldo que mitigue la pérdida de información.

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio velará porque los equipos de cómputo asignados a los funcionarios y contratistas cuenten con las herramientas de seguridad necesarias, las cuales deben estar debidamente configuradas y actualizadas con el fin que se escanee de forma automática todos los medios removibles que son conectados a los mismos.

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio velará porque los medios que contienen información de la SDSCJ, se almacenacen de forma segura y tengan una adecuada disposición final, según sea el caso, por ejemplo, incineración, destrucción, o el borrado de información antes de ser reutilizados dentro de la Entidad.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección de Recursos Físicos y Gestión Documental, deberá contar con proveedores de mensajería confiables, los cuales serán los encargados de la transferencia de información de manera adecuada cumpliendo con los requisitos establecidos contractualmente.

A.9 CONTROL DE ACCESO	
OBJETIVO:	Propender para que el acceso a todos los activos de información de la entidad, estén protegidos contra acceso no autorizado y cuenten con las medidas de protección necesarias para salvaguardar la información.
ALCANCE:	Aplica para todos los funcionarios y contratistas que tengan y otorguen permisos sobre los activos de información de la entidad sistemas de información, bases de datos o servicios de información de la Secretaría Distrital de Seguridad, Convivencia y Justicia.

A.9.1 Requisitos del negocio para control de acceso

9.1.1 Política de control de acceso

- El acceso a plataformas, aplicaciones, servicios y en general cualquier recurso de

información de La Secretaría Distrital de Seguridad, Convivencia y Justicia, debe ser asignado de acuerdo con la identificación previa de requerimientos de seguridad de la Información, de acuerdo a las funciones u obligaciones contractuales.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnología de Sistemas de Información deberá implementar los controles tanto físicos como lógicos con el fin de preservar la confidencialidad, integridad y disponibilidad de la información de la entidad.

9.1.2 Acceso a redes y a servicios en red

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio establece un procedimiento mediante el cual cualquier funcionario, contratista, proveedor o usuario externo que requiera acceso a la red y a la infraestructura tecnológica de la Secretaría Distrital de Seguridad, Convivencia y Justicia, sea por Internet, acceso telefónico o por otro medio, debe estar autenticado y sus conexiones deberán utilizar cifrado de datos, en caso que los niveles de criticidad de información lo requieran.

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información, tiene establecidos grupos de navegación en los cuales está permitido el acceso a páginas de internet acorde con los cargos y roles que se ejercen por los funcionarios en la Entidad u obligaciones contractuales.

- La Dirección de Tecnología y Sistemas de Información analizará las solicitudes de cambios de grupos de navegación que en razón de sus funciones u obligaciones contractuales llegase a necesitar un funcionario o contratista de la Entidad, previa solicitud por parte del líder de proceso.

- La Dirección de Tecnología y Sistemas de Información realizará el monitoreo de las redes e infraestructura tecnológica de la entidad.

VPN

- Las conexiones remotas a la red local de la Secretaría Distrital de Seguridad, Convivencia y Justicia, se deberan realizar a través de una conexión VPN segura suministrada por la SDSCJ, la cual deberá ser aprobada, registrada y auditada, sin excepción alguna. Por la Dirección de Tecnologías y Sistemas de Información.

- La asignación para VPN a los funcionarios y contratistas de la Entidad, dependerá de las funciones u obligaciones contractuales, esto con el fin de facilitar la conexión desde un

lugar remoto a los servicios informáticos brindados por la Entidad, o por cumplimiento de una resolución de Teletrabajo.

- La conexión realizada a través del servicio de VPN se debe realizar mediante la herramienta entregada por la SDSCJ, con respecto a la autenticación y conexión, el funcionario o contratista debe garantizar que se haga desde un equipo seguro.

Redes inalámbricas

- La Dirección de Tecnología y Sistemas de Información deberá asegurar que las redes inalámbricas de la SDSCJ, cuenten con métodos de autenticación que evite accesos no autorizados.

- Para el personal externo a la SDSCJ que requiera una conexión a la red inalámbrica de la Entidad se creará un usuario temporal con su respectiva contraseña, previa autorización del funcionario o contratista que esté atendiendo la visita o personal externo. El servicio otorgado será limitado de acuerdo a los requerimientos y monitoreado por la Dirección de tecnología y Sistemas de Información

9.2 Gestión de acceso de usuarios

9.2.1 Registro y cancelación del registro de usuarios

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio establece un procedimiento para el registro y cancelación de usuarios, el cual se lleva a cabo en el inicio y terminación de la vinculación contractual de funcionarios o contratistas de la entidad.
- La asignación de usuarios y perfiles, para los funcionarios y contratista de la SDSCJ a los distintos aplicativos o sistemas de información, deben estar asociados con sus funciones u obligaciones contractuales.

- La Entidad establecerá privilegios para el control de acceso, de cada usuario o grupo de usuarios a los distintos aplicativos, sistemas de información o medios. Así mismo, velará porque los funcionarios y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus funciones. Lo anterior teniendo en cuenta que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

- Todo funcionario o contratista que requiera tener acceso a los sistemas de información de La Secretaría Distrital de Seguridad, Convivencia y Justicia debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y contraseña (password) asignado por la Entidad.

- Cada funcionario es responsable del uso y manejo de las credenciales asignadas, evitando compartirlas y publicarlas en medios legibles.

- Todos los recursos de información de La Secretaría Distrital de Seguridad, Convivencia y Justicia tendrán asignados los privilegios de acceso de usuarios con base en los roles y perfiles que cada funcionario y contratista requiera para el desarrollo de sus funciones u obligaciones contractuales.

- La Dirección de Tecnología y Sistemas de Información será la responsable de la creación, modificación y eliminación de usuarios, contraseñas y privilegios de acceso en la infraestructura de tecnológica y sistemas de información.

- Una vez se termine el vínculo contractual, con un funcionario o contratista de la Entidad, se deben deshabilitar y/o retirar inmediatamente los permisos que le fueron asignados a los distintos aplicativos, sistemas de información o medios. Esto debe ser reportado por el líder del proceso, teniendo en cuenta el proceso de paz y salvo que se lleva a cabo en la entidad

9.2.3 Gestión de derechos de acceso privilegiado

- Todo derecho de acceso privilegiado a los recursos informáticos de la SDSCJ debe ser debidamente autorizados, registrados y controlados por el Director de Tecnologías y Sistemas de Información.

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio, no debe otorgar privilegios especiales o de administradores a los equipos asignados a los funcionarios o contratistas de la entidad,

- La asignación de derechos de acceso privilegiado o usuarios administradores, en los casos que aplique deberá otorgarse a funcionarios o contratistas teniendo en cuenta sus funciones y obligaciones contractuales. Este usuario privilegiado deberá ser un usuario de red diferente al asignado para ingresar a su equipo de cómputo y para el desarrollo de sus actividades regulares.

- Una vez termine el vínculo contractual, con un funcionario o contratista de la Entidad, se deben deshabilitar y/o retirar inmediatamente los permisos privilegiados que le fueron asignados a los distintos aplicativos, sistemas de información o medios.

9.2.4 Gestión de información secreta para la autenticación de usuarios

- Todo funcionario o contratista de la SDSCJ que maneja información secreta deberá firmar una declaración para mantener un nivel de confidencialidad sobre está.

9.2.5 Revisión de los derechos de acceso de usuarios

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio, velará porque los accesos de los funcionarios o contratistas a los activos de información de la Entidad se revisen después de cualquier cambio, promoción, cambio de un cargo a un nivel o superior, o terminación de contrato, con una periodicidad anual como mínimo.

9.2.6 Retiro o ajuste de los derechos de acceso

- Los derechos de acceso a los funcionarios y/o contratistas de la SDSCJ, o terceros que acceden a la información, deben ser retirados al terminar el vinculo contractual o se deberán ajustar cuando se realicen cambios.

9.3 Responsabilidades de los usuarios

9.3.1 Uso de información secreta para la autenticación

- Los funcionarios y contratistas deberán utilizar credenciales seguras de ingreso a los servicios o sistemas de información designados, las cuales deben contener entre 8 y 14 caracteres, números, letras y caracteres especiales.

- Los funcionarios y contratistas deberán mantener confidencialidad de sus contraseñas o claves de acceso a los sistemas de información asegurándose de que no sea divulgada en ninguna instancia.

- Los funcionarios y contratistas deben evitar llevar registros (por ejemplo, post-it,en papel, en un archivo digital o en un dispositivo portátil), contraseñas o claves de acceso a los sistemas de información.

9.4 Control de acceso a sistemas y aplicaciones

9.4.1 Restricción de acceso a la información

- La Dirección de Tecnología y Sistemas de Información, como responsable de la administración de los distintos aplicativos, sistemas de información y medios, propenderá para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso.

- La Dirección de Tecnología y Sistemas de Información velará porque los desarrolladores, tanto internos como externos, acojan las buenas prácticas de desarrollo seguro en los aplicativos y así controlar el acceso lógico, evitando accesos no autorizados a los sistemas de información del Entidad.

9.4.2 Procedimiento de ingreso seguro

- La Secretaría Distrital de Seguridad Convivencia y Justicia, a través de la Dirección de Tecnología y Sistemas de Información, para el ingreso seguro a los distintos aplicativos, sistemas de información y servicios entrega a cada funcionario y contratista un usuario y contraseña como medio de autenticación.

- La Secretaría Distrital de Seguridad Convivencia y Justicia, a través de la Dirección de Tecnología y Sistemas de Información, para garantizar la protección de ingreso mediante fuerza bruta, lleva un registro (Log) con los intentos exitosos y fallidos.

- La Secretaría Distrital de Seguridad Convivencia y Justicia, a través de la Dirección de Tecnología y Sistemas de Información establece los mecanismos necesarios para que en los distintos aplicativos, no permite la visualización de las contraseñas que se esté ingresando.

- La Secretaría Distrital de Seguridad Convivencia y Justicia, a través de la Dirección de Tecnología y Sistemas de Información, establece los mecanismos necesarios que permitan la terminación de las sesiones de los aplicativos o sistemas de información después de un período de inactividad.

9.4.3 Sistema de gestión de contraseñas

- Las contraseñas de usuarios de los distintos aplicativos o sistemas de información cumplen con los parámetros mínimos de complejidad (número mínimo de caracteres, uso de mayúsculas y minúsculas, uso de caracteres especiales, entre otros)

- La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio establece un tiempo de caducidad de las contraseñas de 45 días para los equipos de computo

9.4.4 Uso de programas utilitarios privilegiados

- La Dirección de Tecnologías y Sistemas de información, deberá separar entre programas utilitarios del sistema y software de aplicaciones.

- La Dirección de Tecnologías y Sistemas de información, deberá limitar el uso de programas utilitarios del sistema a la cantidad mínima viable de funcionarios autorizados.
- La Dirección de Tecnologías y Sistemas de información deberá evitar que funcionarios o personal externo tomen conocimiento de la existencia y modo de uso de los programas utilitarios instalados en la Entidad.
- La Dirección de Tecnologías y Sistemas de información deberá llevar registro del uso de programas utilitarios del sistema, dentro de la Entidad.
- La Dirección de Tecnologías y Sistemas de información, deberá definir y documentar los niveles de autorización para programas utilitarios del sistema.
- La Dirección de Tecnologías y Sistemas de información deberá retirar o deshabilitar todos los programas utilitarios innecesarios.

9.4.5 Control de acceso a códigos fuente de programas

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección de Tecnología y Sistemas de Información establece los mecanismos necesarios para controlarel acceso al código fuente, a fin de preservar su confidencialidad su confidencialidad e integridad y en pro de conservar su propiedad intelectual. Los únicos usuarios autorizados son los desarrollares de cada uno de los aplicativos de la entidad.

A.10 CRIPTOGRAFÍA	
OBJETIVO:	Velar porque la información de la Entidad esté protegida y cifrada en el momento de almacenamiento y/o transmisión por cualquier medio.
ALCANCE:	Aplica para todos los funcionarios y contratistas que manejen sistemas de información de la Entidad.

10. 1Controles criptográficos

10.1.1 Política sobre el uso de controles criptográficos

La Dirección de Tecnología y Sistemas de Información debe establecer los mecanismos necesarios para que la información confidencial que sea transportada mediante medios removibles este debidamente cifrada.

- Todos los funcionarios de la SDSCJ tienen la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales de los sistemas de información y de la herramienta en relación a los posibles riesgos asociados al cifrado de la información.

- La Dirección de Tecnología y Sistemas de Información debe establecer mecanismos para la protección de llaves criptográficas y la recuperación de información cifrada, en caso de llaves perdidas.

A.11 SEGURIDAD FÍSICA Y DEL ENTORNO	
OBJETIVO:	Brindar un acceso controlado y restringido a las áreas y equipos de la Entidad, con el fin de proteger la información.
ALCANCE:	Aplica para todos los funcionarios y contratista que tengan acceso a las áreas seguras.

A.11.1 Áreas Seguras

11.1.1 Perímetro de Seguridad Física

- En La Secretaría Distrital de Seguridad, Convivencia y Justicia se consideran áreas de acceso restringido a aquellas destinadas al procesamiento o almacenamiento de información crítica y sensible, así como en las que se encuentren los equipos/servidores y demás infraestructura tecnológica que soporta la operación de la Entidad.

- Para el ingreso a la sala de operación del NUSE, centros de cableados y data center, se deberá realizar el registro en la planilla de visitantes destinadas para tal fin.

- Se debe restringir el uso de celulares y/o cualquier dispositivo móvil de comunicación en las instalaciones de la SDSCJ, especialmente las instalaciones de la sala de operación

del NUSE y en la Cárcel Distrital de Varones y Anexo de Mujeres, donde se maneje información sensible.

- La SDSCJ debe contar con las medidas de control de acceso físico que permitan proteger la información, el software y el hardware de daños intencionales o accidentales, en las áreas de procesamiento de información.

11.1.2 Controles de acceso físicos

- La SDSCJ debe contar con los controles de acceso apropiados a las áreas seguras, con el fin de permitir el acceso únicamente a personal autorizado.

- La SDSCJ a través de los contratos de vigilancia debe establecer los mecanismos de control de acceso a las áreas de la entidad.

11.1.3 Seguridad de oficinas, recintos e instalaciones

- La SDSCJ debe establecer los mecanismos y controles apropiados para asegurar el ingreso a las oficinas, recintos e instalaciones donde se maneje información sensible.

11.1.4 Protección contra amenazas externas y ambientales

- La SDSCJ debe cumplir con los requerimientos ambientales (temperatura, humedad, etc.), en las instalaciones de procesamiento de información, con el fin de responder de manera adecuada ante incidentes como incendios o inundaciones entre otros.

11.1.5 Trabajo en áreas seguras

- La SDSCJ debe establecer los procedimientos respectivos para el trabajo en áreas seguras.

11.1.6 Áreas de despacho y carga

- La SDSCJ debe establecer los controles apropiados para las áreas de despacho y carga, con el fin de no permitir el ingreso de personal no autorizado a las instalaciones de la entidad.

- **A.11.2 Equipos**

11.2.1 Ubicación y Protección de los equipos

- Los funcionarios y/o proveedores, que tengan acceso a las instalaciones de La Secretaría Distrital de Seguridad, Convivencia y Justicia, no pueden fumar o consumir algún tipo de alimento cerca de los equipos de computo.

- Los equipos de La Secretaría Distrital de Seguridad, Convivencia y Justicia tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aire acondicionado, planta telefónica, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan y/o brinden servicios de soporte a la información crítica de las áreas, deben ser ubicados y protegidos adecuadamente para prevenir la pérdida, daño, robo de información.

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información y esta a su vez mediante la mesa de servicio debe establecer los controles necesarios para proteger los equipos de cómputo entregados a los funcionarios y/o contratistas, con el fin de reducir los riesgos de amenazas y peligros del entorno.

11.2.2 Servicios de suministro

- La SDSCJ debe garantizar la protección de los equipos de procesamiento de información, respecto a fallas de energía u otras interrupciones causadas por los servicios de suministro.

- La SDSCJ debe evaluar permanentemente la capacidad de crecimiento de los equipos de procesamiento, con el fin que no se presenten interrupciones en el negocio por sobrecargas no dimensionadas.

- La SDSCJ mediante la Dirección de Recursos Físicos y Gestión Documental debe definir la periodicidad con la que se debe realizar el mantenimiento de las ups de las plantas de todas las sedes de la entidad.

11.2.3 Seguridad del cableado

- La SDSCJ debe garantizar que el cableado de energía eléctrica y telecomunicaciones cuente con las especificaciones necesarias y se encuentre protegido contra cualquier interceptación, interferencia o daño de terceros.

- La SDSCJ establece restricciones para el acceso a los centros de cableado y datacenter, donde únicamente tiene acceso el personal autorizado.

11.2.4 Mantenimiento de Equipos

- La SDSCJ debe contar con los contratos de soporte vigentes que permitan el mantenimiento preventivo y correctivo de los equipos de computo con el fin de asegurar su disponibilidad e integridad continua.

- El contratista encargado del mantenimiento preventivo y correctivo de los equipos de cómputo debe mantener actualizadas las hojas de vida de los mismos.

- La SDSCJ debe establecer que únicamente el personal autorizado debe llevar a cabo las reparaciones y servicio sobre los equipos de procesamiento de información.

11.2.5 Retiro de activos

- La SDSCJ debe establecer los mecanismos y controles apropiados para asegurar el retiro de los equipos, información o software de las instalaciones de la entidad.

11.2.6 Seguridad de equipos y activos fuera de las instalaciones

- Todos los funcionarios y contratistas de La Secretaría Distrital de Seguridad, Convivencia y Justicia son responsables de velar por la seguridad de los equipos de cómputo que se encuentren fuera de las instalaciones de la Entidad.

- Bajo ninguna circunstancia los equipos de cómputo asignados a los funcionarios y contratistas pueden estar desatendidos en lugares públicos o a la vista, sin la correspondiente vigilancia y custodia.

- Esta prohibido intentar vulnerar los controles establecidos en los equipos de cómputo, los cuales son establecidos con el fin que no se coloque en riesgo la información de la entidad.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a cualquier riesgo que comprometa la confidencialidad de la información y su integridad física.

- En caso de pérdida o robo de un equipo de la Secretaría Distrital de Seguridad, Convivencia y Justicia, se deberá informar inmediatamente a la Dirección de Recursos

Físicos y Gestión Documental para que se inicie el trámite interno y se realizar la denuncia ante la autoridad competente.

- El retiro de equipos de cómputo, periféricos, dispositivos de almacenamiento, software y medios magnéticos con información considerada crítica de La Secretaría Distrital de Seguridad, Convivencia y Justicia, fuera de las instalaciones de la Entidad debe seguir los procedimientos establecidos por la Dirección de Tecnología y Sistemas de Información.

11.2.7 Disposición segura o reutilización de equipos

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información y esta por medio de la mesa de servicio debe asegurar que una vez sea asignado un equipo de cómputo a un funcionario o contratista, el equipo debe estar debidamente formateado.
- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información y esta por medio de la mesa de servicio debe establecer un procedimiento para la disposición segura de los equipos.

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información y esta por medio de la mesa de servicio debe definir un proceso para dar de baja equipos de computo.

- La SDSCJ debe asegurar que todo equipo que contenga información sensible, se le realice el respectivo proceso de backup, información que debe ser entregada al líder de proceso, con el fin que este sea dispuesto o entregado a otro funcionario.

11.2.8 Equipos de usuario desatendido

- Es responsabilidad de todos los funcionarios y contratistas de la Secretaría Distrital de Seguridad, Convivencia y Justicia, bloquear la sesión de sus equipos de cómputos al ausentarse del puesto de trabajo, así como cerrar las sesiones activas y dejar los equipos apagados una vez finalice la jornada laboral.
- La Dirección de Tecnología y Sistemas de Información a través de la mesa de servicio cuando los equipos están desatendidos, debe establer una política de bloqueo con inactividad mínimo de 45 segundos.

11.2.9 Escritorio y pantalla limpia

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Información debe establecer las políticas correspondientes de escritorio limpio y pantalla limpia.

- Los funcionarios y/o contratistas deben asegurar que la información tipificada como

clasificada o reservada no se encuentre a la vista de terceros no autorizados.

A.12 SEGURIDAD DE LAS OPERACIONES	
OBJETIVO:	Velar porque las operaciones de la Entidad, cumplan con las condiciones de seguridad requeridas para mantener su confidencialidad, disponibilidad e integridad de la información.
ALCANCE:	Aplica para toda la información que se administre en la Entidad a través de los diferentes sistemas de información.

A.12.1 Procedimientos operacionales y responsabilidades

12.1.1 Procedimientos de operación documentados

- La Dirección de Tecnología y Sistemas de Información apoyará en la emisión de conceptos y recomendaciones acerca de las soluciones de seguridad, seleccionadas para la infraestructura tecnológica de la entidad.

- Los procedimientos de operación como mínimo deberán especificar las instrucciones para la ejecución de cada actividad

12.1.2 Gestión de cambios

- La SDSCJ debe contar un procedimiento que permita garantizar que los cambios que se generen sobre cualquier componente de tecnología, como consecuencia de un requerimiento de usuario, de la solución de un incidente o de una actualización sean controlados, gestionados y autorizados adecuadamente.

12.1.3 Gestión de capacidad

La entidad mantendrá un proceso continuo de monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

- La Dirección de Tecnología y Sistemas de Información debe documentar un procedimiento de gestión de capacidad que permita establecer los requisitos que son críticos para la entidad.

12.1.4 Separación de los ambientes de desarrollo, pruebas, y operación

- La SDSCJ a través de la Dirección de Tecnología y Sistemas de Infomración, debe definir ambientes separados de producción, pruebas y desarrollo, con el fin de garantizar la integridad de la información procesada, evitar interferencias en el desempeño, reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.

A.12.2 Protección contra software malicioso

12.2.1 Controles contra códigos maliciosos

- La Secretaría Distrital de Seguridad, Convivencia y Justicia debe contar con las herramientas de seguridad tales como antivirus, AntiSpam, antispyware, seguridad perimetral y otras aplicaciones que permitan brindan la adecuada protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

  La Dirección de Tecnología y Sistemas de Información, a través de la mesa de servicio la encargada de implementar las herramientas de seguridad como antivirus, AntiSpam, antispyware, asegurando que no sean deshabilitadas bajo ninguna circunstancia y cuenten con las respectivas actualizaciones.

- Los funcionarios y/o contratistas que detecten alguna infección por software malicioso deben reportar a La Dirección de Tecnología y Sistemas de Información, mediante la mesa de servicio, como un incidente de seguridad de la información.

  Los funcionarios y/o contratistas tienen prohibido, la desinstalación y/o desactivación de software y herramientas de seguridad aprobadas por la Dirección de Tecnología y Sistemas de Información.

- Los funcionarios y/o contratistas tienen prohibido, escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.

- Los funcionarios y/o contratistas tienen prohibido, utilizar medios de almacenamiento físico o virtual que no sean de carácter corporativo.

A.12.3 Copias de respaldo

12.3.1 Respaldo de Información

- La Dirección de Tecnología y Sistemas de Información velará porque la información sea resguardada mediante mecanismos y controles adecuados que preserven su confidencialidad, integridad y disponibilidad.

- La Dirección de Tecnología y Sistemas de Información debe disponer a los funcionarios y/o contratistas, los medios necesarios para respaldar la información más sensible.

- Los funcionarios y/o contratistas son los responsables de realizar copias de respaldo de la información más sensible.

- La Dirección de Tecnología y Sistemas de Información debe contar con un procedimiento de respaldo de la información de bases de datos y establecer periodos de prueba de las mismas.

A.12.4 Registro (Logging) y Seguimiento

- La Dirección de Tecnología y Sistemas de Información deberá realizar monitoreo periódico sobre los aplicativos y velar por la generación de los registros de auditoría (log´s).

- La Dirección de Tecnología y Sistemas de Información mantendrá sincronizados los relojes de todos los sistemas de procesamiento de información con una única fuente de referencia de tiempo.

A.12.5 Control de software operacional

12.5.1 Instalación de software en sistemas operativos

- La Dirección de Tecnología y Sistemas de Información, realizará monitoreo sobre el software operacional instalado en los diferentes equipos de la entidad, cualquier software adicional que requiera un funcionario o contratista de la SDSCJ deberá ser solicitado por el líder de proceso y aprobado por la esta Dirección para proceder con la instalación.

- La Dirección de Tecnología y Sistemas de Información debe propender porque frecuentemente se realice la actualización de parches y/o actualizaciones en toda la plataforma tecnológica de la entidad.

- La Dirección de Tecnología y Sistemas de Información debe contar con el respetivo versionamiento para las aplicaciones desarrolladas para la entidad.

- La Direccion de Tecnología y Sistemas de Información a través de la mesa de servicio establece una línea base de software autorizado para los equipos de cónputo de la entidad.

A.12.6 Gestión de la vulnerabilidad técnica

12.6.1 Gestión de las vulnerabilidades técnicas

- La Dirección de Tecnología y Sistemas de Información, realizará periodicamente el análisis de vulnerabilidades a la plataforma tecnológica de la SDSCJ y la remediación de los hallazgos que se deriven del citado análisis.

12.6.2 Restricciones sobre la instalación de software

- La Dirección de Tecnología y Sistemas de Información debe implementar los mecanismos necesarios para evitar la instalación de software no autorizado en los equipos de cómputo de la entidad.

- La Dirección de Tecnología y Sistemas de Información, debe establecer el software base que debe ser instalado en los equipos de computo de los funcionarios y/o contratistas de acuerdo a sus funciones y obligaciones.

A.12.7 Consideraciones sobre auditorías de sistemas de información

- Todas las auditorías que se realicen a los sistemas de información de la SDSCJ deberán estar autorizadas y controladas, para velar por la disponibilidad de la información. Estas Auditorías para los sistemas de información críticos de la Entidad se realizarán en horarios no laborales.

A.13 SEGURIDAD DE LAS COMUNICACIONES	
OBJETIVO:	Establecer mecanismos de control con el fin de proveer y proteger la integridad y confidencialidad de la información contenida y transportada a través de las redes, canales de comunicaciones, internet y mensajería electrónica.
ALCANCE:	Aplica para toda información que se maneje en la entidad a través de redes y mensajería

	electrónica.

13.1 Gestión de la seguridad de las redes

13.1.1 Controles de redes

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, debe establecer los mecanismos necesarios, en pro de velar por la confidencialidad, integridad y disponibilidad de la información, mediante la segmentación de las redes.

- La Dirección de Tecnología y Sistemas de Información es la responsable de establecer el perímetro de seguridad necesario para proteger los segmentos de red, de acuerdo con el nivel de criticidad del flujo de la información transmitida.

- La Dirección de Tecnología y Sistemas de Información es la responsable de establecer los controles necesarios para que los funcionarios, contratistas o visitantes de la SDSCJ se autentiquen para poder hacer uso de los servicios de red de la entidad.

- La Dirección de Tecnología y Sistemas de Información debe gestionar los registros y logs de los administradores de la plataforma tecnológica de la entidad.

13.1.2 Seguridad de los servicios de red

- Los proveedores de servicios de redes de la SDSCJ deben asegurar contar con los respectivos mecanismos de seguridad que permitan la disponibilidad y niveles de servicio requeridos por la Entidad.

13.1.3 Separación en las redes

- La Dirección de tecnología y Sistemas de Información debe garantizar que los servicios de información, usuarios y sistemas de información estén separados en diferentes redes.

- La Dirección de Tecnología y Sistemas de Información es la encargada que todos los procesos de separación de redes se encuentren debidamente documentados.

13.2 Transferencia de información

- La SDSCJ a través de la Dirección de Recursos Físicos y Gestión Documental, debe establecer un procedimiento de trasferencia de información con las partes externas, en el cual se debe detallar la protección que debe tenerse especialmente con los datos

personales en el proceso de transferencia.

- La SDSCJ velará por la protección de la información contra el acceso no autorizado, uso indebido o corrupción de la misma y durante su tratamiento, para lo cual se deberá tener en cuenta la política de controles criptográficos.

- La SDSCJ debe establecer acuerdos de confidencialidad con las partes externas en donde se realice procesos de transferencia de información, teniendo en cuenta la normativa vigente.

A.14 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	
OBJETIVO:	Asegurar que la Entidad cuente con controles de seguridad de la información como parte integral de los mismos en todo el ciclo de vida.
ALCANCE:	Aplica para todos los sistemas de información vigentes y los que se adquieran en la entidad.

14.1 Requisitos de seguridad de los sistemas de información

14.1.1 Análisis y especificación de requisitos de seguridad de la información

- La Dirección de Tecnología y Sistemas de Información es la única dependencia de la SDSCJ encargada de los procesos de desarrollo de software para la entidad.

- Todas las dependencias y oficinas de la SDSCJ que realicen procesos para la adquisición de software debe solicitar aval a la Dirección de Tecnología y Sistemas de Información.

- La Dirección de Tecnología y Sistemas de Información debe definir los requisitos apropiados para asegurar los sistemas de información de la entidad.

- La Dirección de Tecnología y Sistemas de Información deberá realizar las pruebas de funcionamiento y de seguridad a los nuevos sistemas de información, actualizaciones y aplicaciones en el ambiente de pruebas, con el fin de obtener la aprobación correspondiente para desplegar en el ambiente de producción.

- Las áreas de la SDSCJ que requieran la adquisición de software para sus operaciones, deben evaluar los requerimientos con la Dirección de Tecnología y Sistemas de Información antes de la adquisición correspondiente.

- La Dirección de Tecnología y Sistemas de Información es la única autorizada para realizar la instalación de software y sistemas de información en las diferentes áreas de la entidad.

14.1.2 Seguridad de servicios de las aplicaciones en redes públicas

- La Dirección de Tecnología y Sistemas de Información debe contar con los mecanismos de seguridad adecuados para garantizar las transacciones realizadas por las aplicaciones en redes públicas.

14.2 Seguridad en los procesos de desarrollo y de soporte

14.2.1 Política de Desarrollo Seguro

- La Dirección de Tecnología y Sistemas de Información debe implementar un procedimiento para el desarrollo seguro.

- La Dirección de Tecnología y Sistemas de Información debe implementar técnicas para el desarrollo seguro de las aplicaciones de la entidad.

- La Dirección de Tecnología y Sistemas de Información, debe aplicar las metodologías apropiadas para proteger los procesos transaccionales de los sistemas de información de la entidad.

14.2.2 Procedimiento de control de cambios en sistemas

- La Dirección de Tecnología y Sistemas de Información debe establecer un procedimiento de gestión de cambios donde se evaluar los requerimientos solicitados por los usuarios respecto a los sistemas de información con el fin de atender los requerimientos del negocio.

14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación

- La Dirección de Tecnología y Sistemas de Información, debe garantizar que cuando se realice una revisión técnica de las plataformas de operación, se realicen las pruebas correspondientes en todas las aplicaciones de la Entidad, con el fin de responder a los requerimientos del negocio.

14.2.8 Pruebas de seguridad de los sistemas

La Dirección de Tecnología y Sistemas de Información, debe garantizar que se realicen las correspondientes pruebas de seguridad a todas las aplicaciones, actualizaciones solicitadas.

14.2.9 Prueba de aceptación de sistemas

La Dirección de Tecnología y Sistemas de Información, debe garantizar que se realice un proceso formal de pruebas de aceptación de los nuevos sistemas de información y actualizaciones solicitadas.

14.3 Datos de prueba

14.3.1 Protección de los datos de prueba

- La Secretaría Distrital de Seguridad Convivencia y Justicia protegerá los datos de pruebas teniendo especial cuidado con la información catalogada como sensible.

- La Dirección de Tecnología y Sistemas de Información, debe establecer mecanismos para no hacer uso de datos personales que no hayan sido debidamente autorizados para el proceso respectivo.

A.15 RELACIÓN CON LOS PROVEEDORES	
OBJETIVO:	Garantizar el adecuado cumplimiento de los procesos de seguridad de la información de los proveedores que tienen relación con la SDSCJ.
ALCANCE:	Aplica a todos los proveedores y terceros que tengan relación con la SDSCJ

15.1 Seguridad de la información en las relaciones con los proveedores

- Los proveedores de la SDSCJ deberán tener en cuenta lo establecido por la Entidad respecto a los aspectos de seguridad de la información.

- Todo proveedor de la SDSCJ que tenga acceso a los activos de información de la entidad y preste los servicios a la SDSCJ deben contar con políticas, normas y estándares de seguridad de la información al interior de su entidad.

- Los proveedores de la SDSCJ deben proteger la confidencialidad, integridad y disponibilidad de la información, cuando los servicios contratados así lo requieran.

- La disponibilidad del proveedor en la prestación de los servicios, es la definida en los contratos establecidos con la SDSCJ, sino se han establecido niveles de servicio, el proveedor deberá actuar con la máxima diligencia para que la información de la SDSCJ esté disponible de a cuerdo a lo requerido por la Entidad.

- Todo proveedor o tercero que preste servicios de desarrollo de software a la SDSCJ, debe implementar normas o las mejores prácticas de la industria en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas.

- La SDSCJ, debe establecer acuerdos de confidencialidad en la relación con los proveedores que manejan información de la entidad.

- La SDSCJ, deben 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 a todos los proveedores.

A.16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	
OBJETIVO:	Velar porque los eventos e incidentes de seguridad de la información sean comunicados y atendidos oportunamente, de acuerdo con el procedimiento establecido para tal fin.
ALCANCE:	Aplica para todos los eventos e incidentes que sea informados.

16.1 Gestión de incidentes y mejoras en la seguridad de la información

16.1.1 Responsabilidades y procedimientos

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, contará con un procedimiento de incidentes de seguridad de la información donde se definan las acciones respectivas a tomar.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, debe contar con el rol de gestor de incidentes de seguridad de la información, quien será el encargado de realizar el proceso de análisis, documentación, evaluación y respuesta de los mismos.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia realizará las acciones tendientes a contener y mitigar el impacto de los eventos o incidentes de seguridad de la

información de acuerdo con lo descrito en el Procedimiento de Gestión de Incidentes de Seguridad de la Información.

16.1.2 Reporte de eventos de seguridad de la información

- Todo los funcionarios y contratistas deberán reportar cualquier situación que se pueda considerar evento o incidentes de seguridad de la información o que considere puede afectar la confidencialidad, disponibilidad e integridad de la información a través de la mesa de servicio.

16.1.3 Reporte de debilidades de seguridad de la información

- Todo los funcionarios y contratistas deberán reportar cualquier situación que se pueda considerar como una debilidad de seguridad de la información o que considere puede afectar la confidencialidad, disponibilidad e integridad de la información a través de la mesa de servicio.

16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos

- La Dirección de Tecnología y Sistemas de Información, se encargará de clasificar y evaluar los eventos o incidentes de seguridad de la información.

- Los eventos catalogados como mayores o catastróficos, que puedan afectar el negocio deben ser evaluados en el comité de gestión institucional de la SDSCJ, con el fin de evalúalos y definir las acciones correspondientes.

16.1.5 Respuesta a incidentes de seguridad de la información

- La Dirección de Tecnología y Sistemas de Información, será la responsable de dar respuesta a los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento de gestión de incidentes de seguridad de la información de la entidad.

16.1.6 Aprendizaje obtenidos de los incidentes de seguridad de la información

La Dirección de Tecnología y Sistemas de Información, debe establecer los mecanismos para que la información de los incidentes de seguridad de la información reportados, queden almacenados con el fin que sean consultados con posterioridad.

A.17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	
OBJETIVO:	Establecer los mecanismos de recuperación y restauración de la Entidad.
ALCANCE:	Aplica a todos los funcionarios y/o contratistas, terceros que tengan relación con la SDSCJ.

17.1 Continuidad de Seguridad de la Información

17.1.1 Planificación de la continuidad de la seguridad de la información

- La SDSCJ debe contar con un plan de continuidad del negocio que contenga los aspectos de seguridad de la información, el cual permitirá a la entidad definir las actividades necesarias para recuperar y restaurar las funciones críticas de la entidad.

- La Dirección de Tecnología y Sistemas de Información debe establecer un plan de contingencia tecnológica que permita definir las actividades para recuperar y restaurar los sistemas y plataformas tecnológicas que soportan las operaciones críticas de la entidad con el fin de prevenir las interrupciones en el negocio.

17.1.2 Implementación de la continuidad de la seguridad de la información

- La SDSCJ a través de la Subdirección de Gestión Institucional deberá implementar un plan de continuidad del negocio, el cual debe estar debidamente documentado estableciendo los procesos, procedimientos y controles para asegurar el nivel requerido de continuidad.

17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.

- La SDSCJ a través de la Subdirección de Gestión Institucional deberá realizar una verificación y revisión periódica del plan de continuidad del negocio definido para la entidad, teniendo en cuenta los aspectos de seguridad de la información.

17.2 Redundancias

17.2.1 Disponibilidad de instalaciones de procesamiento de información

- La SDSCJ debe contar con instalaciones de procesamiento de información que tengan la disponibilidad necesaria para atender los requerimientos del negocio en caso de un evento mayor o catastrófico.

A.18 CUMPLIMIENTO	
OBJETIVO:	Cumplir todas las directrices de seguridad de la información de acuerdo con lo establecido en la normatividad aplicable.
ALCANCE:	Aplica a todos los funcionarios y/o contratistas, terceros que tengan relación con la SDSCJ.

18.1 Cumplimiento de requisitos legales y contractuales

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección Juridica y Contractual y la Dirección de Gestión Humana deberá establecer cláusulas contractuales entre la entidad y cualquier funcionario, contratista, tercero, operador tecnológico o proveedor, en los cuales se especifiquen los compromisos de preservación de los derechos de autor y propiedad intelectual.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección Juridica y Contractual y la Dirección de Gestión Humana deberá establecer las respectivas clausulas de reserva y confidencialidad de la información en los contratos suscritos con los diferentes funcionarios, contratistas, proveedores, operadores tecnológicos o terceros.

- La Secretaría Distrital de Seguridad, Convivencia y Justicia, a través de la Dirección Juridica y Contractual y la Dirección de Gestión Humana deberá establecer clausulas dentro de cualquier contrato donde se defina el cumplimiento de los requisitos legales.

- La SDSCJ deberá documentar toda la normativa vigente respecto a la seguridad de la información, con el fin de cumplir los requisitos legales y no incurrir en incumplimientos que pueden ocasionar inconvenientes mayores al negocio.

- La Dirección de Tecnología y Sistemas de Información, velará porque todo el software que se ejecute en la entidad este protegido por derechos de autor y requiera licencia de uso o sea software de libre distribución.

- Los funcionarios y/o contratistas de la SDSCJ deben cumplir con las leyes de derechos de autor y los acuerdos de licenciamiento de software. No esta permitido la duplicación, reproducción de software, ni de documentación sin previa autorización del propietario.

- La Dirección de Tecnología y Sistemas de Información, velará por el cumplimiento de las políticas establecidas en este documento, registrar los procesos, procedimientos, manuales, instructivos, formatos y políticas específicas alineados al estándar internacional ISO 27001:2013 y la normatividad vigente y aplicable a la Entidad.

- La Dirección de Tecnología y Sistemas de Información realizará la revisión, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI en la Entidad.

- La SDSCJ deberá contar con una política de privacidad y protección de datos personales donde este definido el tratamiento de los datos entregados por los usuarios que tengan relación con la entidad.

7. ANEXO 1 – MATRIZ DE ROLES Y RESPONSABILIDADES

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
Representante Legal (Director General)	Secretario de Seguridad, Convivencia y Justicia	Responsable por el Direccionamiento Estratégico e impulso del SGSI	Secretario de Seguridad, Convivencia y Justicia	
		Aprobar la asignación de recursos para la implementación del SGSI		
		Empoderar al equipo directivo para apoyar a la implementación del SGSI		
		Promover la divulgación de las políticas de seguridad de la información en la entidad.		
Representante de la Dirección General para el SGSI	Director de Tecnologías y Sistemas de la Información	Liderar la definición, implementación, ejecución, seguimiento y divulgación del Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC), así como su alineación con la estrategia de la Entidad.	Director de Tecnologías y Sistemas de la Información	Resolución Nro. 301 del 26 de Julio de 2018
		Generar e implementar estrategias y proyectos de tecnologías de la información y las comunicaciones, que permitan la optimización de procesos, incremento de la productividad y ahorro de recursos.		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		Designar los responsables de liderar el desarrollo, implementación y mantenimiento de los sistemas de información, Estrategia de Gobierno Digital, Seguridad de la Información, Arquitectura de TI e Infraestructura Tecnológica de la Entidad.		
		Velar por la prestación eficiente de los servicios tecnológicos necesarios para garantizar la operación de la Entidad según criterios de calidad, oportunidad, seguridad, escalabilidad y disponibilidad.		
		• Las demás responsabilidades establecidas por la ley.		
		Garantizar el cumplimiento de los lineamientos para el fortalecimiento institucional en materioa de TIC y la implementación de la Estrategia Gobierno en Línea, de acuerdo con la normativa vigente		
		Impartir lineamientos en materia tecnológica para definir políticas, estrategias y prácticas que soporten la gestión institucional y del sector		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		Garantizar la aplicación de estándares, buenas prácticas y principios para el suministro de la información a cargo de la Secretaría, de acuerdo con las disposiciones y políticas institucionales.		
		Dirigir el plan institucional y orientar la elaboración del plan estratégico sectorial en materia de información de manera oportuna y eficiente.		
		Impartir lineaientos 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.		
		Implementar políticas de seguridad informática y de la plataforma tecnológica de la Secretaría, defininiendo los planes de contingencia y supervisando su adecuada y efectiva aplicación.		
		Asesorar al despacho en la definición de los estándares de datos de los sistemas de información y de seguridad informática de competencia de la Secretaria.		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
Líder Implementación de Gobierno Digital	Director de Tecnologías y Sistemas de Información Líder de Implementación de Gobierno Digital	Definir la estrategia para la implementación de la política de gobierno digital en la entidad.	Director de Tecnologías y Sistemas de Información Líder de Implementación de Gobierno Digital	Contrato de Prestación de Servicios
		• Definir los elementos básicos del sistema de Gestión de Seguridad de la Información alineados con el plan estratégico de la Entidad y con el Modelo Integrado de Planeación y Gestión – MIPG		
		•Elaborar estrategias de gestión para velar por la conservación de la Confidencialidad, Disponibilidad e Integridad de la Información, de acuerdo con la normatividad vigente.		
		Realizar seguimiento a la implementación del Marco de Arquitectura Empresarial en la entidad.		
		Realizar seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información en la Entidad.		
Líder Operativo del Sistema de Gestión de Seguridad de la Información - SGSI	Director de Tecnologías y Sistemas de Información (Oficial	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.	Director de Tecnologías y Sistemas de Información (Oficial de	Contrato de Prestación de Servicios

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
	de Seguridad de la Información)	Brindar acompañamiento a las áreas de la Secretaría Distrital de Seguridad, Convivencia y Justicia en la identificación, clasificación y valoración de los activos de información de la entidad, para su adecuada gestión.	Seguridad de la Información)	
		Brindar acompañamiento a las áreas de la Secretaría Distrital de Seguridad, Convivencia y Justicia en la identificación de los riesgos de seguridad digital de la entidad, para su respectivo tratamiento.		
		Liderar la gestión de riesgos de seguridad digital en la entidad.		
		Definir los planes de sensibilización y entrenamiento de seguridad de la información para los funcionarios y/o contratistas de la entidad.		
		Sensibilizar a la áreas de la Entidad frente a las políticas y procedimientos relacionados con el Sistema de Gestión de Seguridad de la Información y con la normatividad aplicable relacionada con el SGSI.		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		Liderar el Comité de Gestión de Cambios Tecnológicos en la Entidad.		
		Apoyar la elaboración de los documentos procedimientos, políticas, manuales, instructivos relacionados con el Sistema de Gestión de Seguridad de la Información.		
		Supervisar la respuesta a incidentes de seguridad de la información en la entidad.		
		Apoyar en la definición de los requerimientos minimos de seguridad que deben cumplir los sistemas de información de la entidad.		
		Definir las métricas de seguridad de la información.		
Comité Institucional de Gestión y Desempeño	Comité Institucional de Gestión y Desempeño	Aprobar y hacer seguimiento, por lo menos una vez cada tres (3) meses, a las acciones y estrategias adoptadas para la operación del Modelo Integrado de Planeación y Gestión – MIPG.	• El(la) Secretario(a) de la entidad o su delegado, • El(la) Subsecretario(a) de Gestión Institucional o su delegado, • El(la) Jefe(a) de la	Resolución 712 de 28 Diciembre de 2018 Resolución 017 del 14 de enero de 2019
		Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		mejora del Modelo Integrado de Planeación y Gestión – MIPG.	Oficina Asesora de Planeación o su delegado, • El(la) Director(a) Financiero(a) o su delegado • El(la) Director(a) de Recursos Físicos y Gestión Documental o su delegado, • El(la) Director(a) Jurídico y Contractual o su delegado, • El(la) Director(a) de Gestión Humana o su delegado, • El(la) Director(a) de Tecnologías y Sistemas de la Información	
		Proponer al Comité Sectorial de Gestión y Desempeño, iniciativas que contribuyan al mejoramiento en la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG.		
		Presentar los informes que el Comité Sectorial de Gestión y Desempeño y los organismos de control requieran sobre la gestión y el desempeño de la entidad.		
		Adelantar y promover acciones permanentes de autodiagnóstico para facilitar la valoración interna de la gestión.		
		Asegurar la implementación y desarrollo de las políticas de gestión y directrices dictadas por las autoridades competentes.		
		Aprobar y hacer seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de gestión.		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		Definir mejoras al Modelo Integrado de Planeación y Gestión implementado por la entidad, con especial énfasis en las actividades de control establecidas en todos los niveles de la organización y estudiar y adoptar las mejoras propuestas por el Comité Institucional de Coordinación de Control Interno.		
		Efectuar recomendaciones al Comité Institucional de Coordinación de Control Interno en relación con las políticas de gestión y desempeño que puedan generar cambios o ajustes a la estructura de control de la entidad.		
		Generar espacios que permitan a sus participantes el estudio y análisis de temas relacionados con políticas de gestión y desempeño, buenas prácticas, herramientas, metodologías u otros temas de interés para fortalecer la gestión y el desempeño institucional y así lograr el adecuado desarrollo de sus funciones.		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
		Las demás asignadas por el representante legal de (la entidad) que tengan relación directa con la implementación, desarrollo y evaluación del Modelo.		
		Liderar y facilitar la implementación de la estrategia de Gobierno Digital y de seguridad digital en la entidad y fungir como su respectivo comité.		
Lideres de Proceso	Director de Gestión Humana Director Oficina Asesora de Planeación Director Financiero Director de la Subsecretaría de Gestión Institucional Director de Tecnologías y Sistemas de Información Director Juridico Director de la Oficina de	Liderar, Impulsar, apoyar, evaluar y hacer seguimiento al sistema Integrado de Gestión Distrital y su marco de referencia MIPG	Director de Gestión Humana Director Oficina Asesora de Planeación Director Financiero Director de la Subsecretaría de Gestión Institucional Director de Tecnologías y Sistemas de Información Director Juridico Director de la Oficina de Comunicaciones	Resoluciones de delegación
		Liderar las políticas de gestión y desempeño institucional de la entidad.		
		Delegar un gestor de proceso para realizar la Identificación, clasificación y valoración los activos de información de la entidad.		
		Apoyar la identificación y actualización de los activos de información de seguridad de la información de cada dirección.		
		Delegar un gestor de proceso para realizar la Identificación, clasificación y valoración los riesgos de seguridad digital		

ROL	CARGO	RESPONSABILIDADES	INTEGRANTES	ACTO ADMINISTRATIVO/CONTRATO
	Comunicaciones Jefe de Centro de Comando, Control, Comunicaciones y Cómputo - C4 Director de la Carcel Distrital de Varones y Anexo de Mujeres	Apoyar la identificación e implementación de controles para la mitigación de los riesgos de seguridad digital.	Jefe de Centro de Comando, Control, Comunicaciones y Cómputo - C4 Director de la Carcel Distrital de Varones y Anexo de Mujeres	
		Aplicar los lineamientos definidos en la política de seguridad de la información de la entidad.		
		Proveer los recursos necesarios para la implementación del SGSI al interior de cada dirección.		
		Promover y divulgar los procesos de sensibilización en seguridad de la información al interior de cada dirección		
		Aplicar los procesos diciplinarios a que haya lugar cuando se presente un incidente de seguridad de la información mayor o catastrofico dentro de cada dirección.		

8. CONTROL DE CAMBIOS

CONTROL DE CAMBIOS		
No. VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	30/11/2019	Documento Original
2	13/03/2020	Se ajustan logos de Alcaldía y de la Certificación ISO 9001-2015 Calidad

	ELABORÓ	REVISÓ	APROBÓ
NOMBRE	Lourdes María Acuña Acuña Diego Ramírez Pulido	Marcela Senestrari Castro Eliecer Vanegas Murcia	Diana Lucia Sanchez Morales
CARGO	Contratista - Seguridad de la Información Contratista Líder Gobierno TI	Contratista Líder Operativo MIPG Contratista – Líder Estrategia TI	Directora de Tecnologías de Información
FIRMA