POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

CONTENIDO

1. INTRODUCCIÓN.

La Secretaría Distrital de Seguridad, Convivencia y Justicia en adelante la SDSCJ, de conformidad con lo establecido en el Decreto Único Reglamentario 1078 de 2015 por medio del cual se expide el Decreto Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones; el Decreto 767 de 2022 por medio del cual se establecen los lineamientos generales a la Política de Gobierno Digital; la ley Estatutaria 1581 de 2012 por la cual se dictan disposiciones para la protección de datos personales; el Documento CONPES 3854 de 2016 en donde se establece la Política Nacional de Seguridad Digital y con las políticas institucionales establecidas bajo el marco del decreto 1499 de 2017, mediante el cual se modificó el decreto 1083 de 2015 Decreto Único Reglamentario del sector de la Función Pública, que actualizó el Modelo Integrado de Planeación y Gestión – MIPG, Resolución 500-2021 MinTIC "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital" y establece el criterio de cumplimiento en materia a de gestión de la seguridad de la información, el cual debe ser acatado y atendido por todos aquellos que gestionan activos de información en la Entidad, orientación que en adelante se denominara "Política de Seguridad y privacidad de la Información".

Es así como a partir de las disposiciones legales correspondientes, el presente documento establece la Política de Seguridad y privacidad de la Información para la SDSCJ como eje rector del Sistema de Gestión de Seguridad de la Información y con el objetivo de orientar a la Entidad al cumplimiento de las directrices nacionales frente a Seguridad Digital y Gobierno Digital.

2. OBJETIVO

Establecer los lineamientos generales del Sistema de Gestión de Seguridad de la Información con el propósito de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información, definiendo y asignando responsabilidades a los funcionarios, contratistas y terceros de la SDSCJ, conforme a los controles de seguridad y privacidad determinados por la Entidad, en concordancia con la normatividad técnica de la familia ISO 27000, los dictámenes definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, a partir del modelo de mejora continua y dando cumplimiento a las disposiciones legales en materia de Seguridad de la Información.

3. ALCANCE

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

La Política de Seguridad y Privacidad de la Información es el eje principal del Sistema de Gestión de Seguridad de la Información, proporciona los lineamientos generales requeridos para implementar un Modelo de Seguridad y Privacidad de la Información confiable y flexible y define el marco básico que guiará la implementación de cualquier directriz, proceso, procedimiento, estándar y / o acción, relacionados con la Seguridad de la Información.

La Entidad en el marco de la presente Política de Seguridad y Privacidad de la Información debe implementar controles para funcionarios y/o contratistas que operan para la SDSCJ, teniendo en cuenta que éstos realizan la administración, operación, soporte, mantenimiento o custodia de las plataformas tecnológicas que cumplen las funciones para llevar a cabo la misionalidad de la Entidad.

4. GLOSARIO

Acceso Privilegiado: Según (MinTIC) es el nivel de permisos especiales que permite a usuarios o procesos realizar acciones críticas como administrar sistemas, gestionar usuarios o acceder a datos sensibles, requiriendo controles estrictos para prevenir riesgos de seguridad.

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: (Guía no. 5 de MINTIC - Guía para la Gestión y Clasificación de Activos de Información MinTIC Versión 1) En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal, clasificada en:

- **Información:** Corresponden a este tipo datos e información almacenada o procesada física o electrónicamente tales como: bases y archivos de datos contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría, entre otros.
- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Recurso humano:** Aquellas personas que, por su conocimiento, experiencia y criticidad para el proceso, son consideradas activos de información.
- **Servicio:** Servicios de computación y comunicaciones, tales como Internet, páginas de consulta, directorios compartidos e Intranet.
- **Software:** Software de aplicación, interfaces, software del sistema, herramientas de desarrollo y otras utilidades relacionadas.
- **Otros:** Activos de información que no corresponden a ninguno de los tipos descritos anteriormente, pero deben ser valorados para conocer su criticidad al interior del proceso

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 Desarrollo: Según (MinTIC) Entorno destinado a la creación y modificación de software, en el cual los desarrolladores trabajan sobre el código fuente de una aplicación sin que este afecte los sistemas en producción, este ambiente permite realizar pruebas y ajustes en las funcionalidades de los sistemas en una configuración aislada, asegurando que cualquier cambio o error en el código no interfiera con los usuarios finales

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.

Auditoría: 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.

Desviación (Seguridad de la Información): Malas prácticas adelantadas por las personas y que generan posibles incidentes o riesgos.

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

DTSI: Dirección de Tecnologías y Sistemas de la Información.

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 y privacidad 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.

Excepciones (Seguridad de información): Casos especiales que no cumplen una política, procedimiento o regla.

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 Crítica 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 y privacidad 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: Según (MinTIC) se define como una técnica utilizada por ciberdelincuentes para manipular a las personas y obtener información confidencial, como contraseñas, datos personales o financieros, aprovechándose de la confianza, el desconocimiento o la presión psicológica.

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 por sus siglas en inglés **(International Organization for Standardization)**: Organización Internacional de Normalización, con sede en Ginebra (Suiza).

ITIL Biblioteca de Infraestructura de Tecnologías de Información por sus siglas en inglés **(Information Technology Infrastructure Library)** Un conjunto de prácticas detalladas, gestión de servicios y la gestión de activos, que se centran en alinear los servicios de Tecnologías de Información con las necesidades del negocio.

Log Information por su traducción en inglés (registro de información): En informática, se usa el término log, para el registro de todo el historial de eventos de un archivo, una base de datos o una aplicación.

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, diseñados para ser extraídas de la computadora sin tener que apagarla.

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

Norma Técnica Colombiana NTC-ISO 27001: Estándar para la implementación del sistema de gestión de la seguridad de la información adoptado por ISO.

Plan de tratamiento de riesgos por su traducción del inglés **(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 y Privacidad: Documento que establece el compromiso de la Entidad 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.

SDSCJ: Secretaría Distrital de Seguridad, Convivencia y Justicia.

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). Según (MinTIC) es un conjunto de políticas, procedimientos, controles y procesos diseñados para gestionar, proteger y garantizar la confidencialidad, integridad y disponibilidad de la información en una organización, basado en estándares como la ISO/IEC 27001.

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

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 [ISO-IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

5. MARCO LEGAL Y/O NORMATIVO

Para consultar el marco legal y normativo por favor remítase al normograma del del proceso Gestión de Tecnologías de Información. El cual puede ser consultado en: https://portalmipg.scj.gov.co/

6. DECLARACIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

A partir del Modelo de Seguridad y Privacidad de la Información emanado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, la SDSCJ entendiendo que la información es uno de sus activos más valiosos y de mayor importancia, declara:

1. Establece los roles y responsabilidades relacionados con la presente política en lo que tiene que ver con el gobierno, gestión, administración y operación en la seguridad de la información.

2. La Entidad protege la información producida, custodiada y transmitida en desarrollo de sus procesos para el cumplimiento de su misionalidad.

3. La Entidad a través del proceso Gestión de Tecnología de Información que lidera la DTSI, diseña e implementa la estrategia para proteger la información generada, recolectada, procesada y utilizada, así mismo, suministra y gestiona las herramientas de hardware y software para el procesamiento y almacenamiento de la información y a su vez implementa controles para mitigar los riesgos sobre dicha información, sin embargo, los propietarios de la información son los responsables de la información registrada, el procesamiento, modificaciones y la autorización de cambios realizadas en los sistemas de información.

4. La Dirección de Recursos Físicos y Gestión Documental, con apoyo técnico de la Dirección de Tecnologías y Sistemas de la Información, establece los lineamientos para la gestión adecuada de los activos de información.

5. A través del proceso de Gestión Documental, liderado por la Dirección de Recursos Físicos y Gestión Documental, se establecen los lineamientos para la identificación, clasificación y buen uso de los activos de información física, con el fin de proteger la misma.

6. Las dependencias de la SDSCJ responsable de la custodia de la información generada en el marco de sus funciones deben estar capacitadas para aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

7. Las soluciones tecnológicas de la SDSCJ son para uso exclusivo del cumplimiento de las funciones u obligaciones designadas; razón por la cual la información almacenada, procesada y generada se considera propiedad de la Entidad y el uso inadecuado de dichos recursos puede conllevar a las sanciones disciplinarias y legales correspondientes.

   En este sentido, los dispositivos personales que sean utilizados por los funcionarios, contratistas y terceros para adelantar actividades de la Entidad, serán dispuestos dependiendo de las definiciones y dictámenes legales correspondientes.

8. Los funcionarios, contratistas y proveedores de la SDSCJ tienen la obligación de cumplir lo establecido en la "*Política de Seguridad y Privacidad de la Información*" y propender por la integridad, disponibilidad y confidencialidad de esta, so pena que la Entidad tome las medidas disciplinarias, legales y administrativas correspondientes.

9. Los sistemas de información, aplicaciones en sitio y aplicaciones en nube administrados por operadores tecnológicos externos al dominio de la SDSCJ, son responsabilidad de dichos operadores en cuanto a su gestión y administración, en todo caso la DTSI establece los lineamientos de seguridad que deben cumplirse.

10. Todos los activos de información tienen un responsable el cual definirá los niveles de acceso dependiendo de las necesidades correspondientes.

11. Las cuentas de usuario y/o correo electrónico genéricas o de servicio, utilizadas para la administración y gestión de servicios internos o externos, ya sean institucionales o de proveedores, debe estar asociadas a un funcionario o contratista responsable de su gestión, con la autorización del líder y/o director de área, y será administradas y gestionadas por la DTSI.

12. Los funcionarios y contratistas de la SDSCJ deben almacenar la información de la Entidad únicamente en los medios designados por la SDSCJ tales como servidor de archivos, almacenamiento en la nube, medios magnéticos, entre otros. Una vez finalizada la vinculación con la Entidad se deberá entregar toda la información procesada dentro de los equipos a cargo, al jefe inmediato o al supervisor de contrato y hacer entrega del inventario correspondiente al jefe inmediato.

13. Los operadores tecnológicos que tengan suscritos contratos con la SDSCJ tienen la responsabilidad de salvaguardar la información contenida en los equipos, dispositivos y/o servicios de almacenamiento bajo su administración, entregando la información pertinente al finalizar el contrato, asegurando su integridad, disponibilidad y conforme a las normas legales vigentes.

14. La Entidad con apoyo de la Dirección de Tecnologías y Sistemas de la Información y a través del convenio suscrito con el o los operadores tecnológicos, según corresponda y que administra la operación del C4, debe extender los controles de seguridad de la información en el componente tecnológico usado por las entidades externas que presten servicios dentro del Sistema Integrado de Seguridad y Emergencias.

15. Los funcionarios, contratistas y/o terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios internos de la Entidad, tales como escritorios remotos, aplicaciones virtuales, correo electrónico, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros. Los dispositivos móviles de propiedad de la Entidad son de estricto uso para el cumplimiento de las funciones y obligaciones establecidas con la Entidad y son gestionados desde la DTSI para efectos del software instalado, cuotas de servicio y demás consideraciones relevantes. Los dispositivos móviles de los funcionarios, contratistas y/o terceros que no son propiedad de la Entidad,

deben ser aislados en VPN o redes WIFI que sean restringidas y separadas de las redes de la Entidad.

16. La Entidad debe realizar el registro y actualización de las bases de datos con datos personales que posee ante la Superintendencia de Industria y Comercio (SIC).

17. Cualquier desviación o excepción a nivel de seguridad de la información, debe ser tenida en cuenta por el responsable del procedimiento en el que se encuentra dicho problema y ser registrada dentro del mismo. En el caso de evidenciarse una desviación o excepción, el responsable debe iniciar el procedimiento de Gestión de Incidentes o problemas, además, adelantar la gestión de riesgos, los controles pertinentes y hacer seguimiento a la efectividad de estos, teniendo como base la concientización y capacitación en dicha temática.

18. La Dirección de Tecnologías y Sistemas de la Información lleva a cabo el análisis de vulnerabilidades de las soluciones tecnológicas de la Entidad, considerando las prioridades definidas en el plan de trabajo, así como los recursos económicos y técnicos que se tengan disponibles para cada vigencia.

7. LINEAMIENTOS DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

7.1 Principios de Seguridad de la Información

Confidencialidad: La información de propiedad de la SDSCJ y de terceras partes entregada a la Entidad, debe ser mantenida, independientemente del medio o formato donde se encuentre y será accedida sólo por aquellas personas que tienen una necesidad legítima para la realización de sus funciones y/o el cumplimiento de obligaciones o en los casos legales correspondientes.
Disponibilidad: La información de propiedad de la SDSCJ debe estar disponible a las personas autorizadas cuando sea requerida.
Integridad: Las personas que accedan a la información de propiedad de la SDSCJ deben preservar la integridad de esta. De la misma manera, debe estar protegida contra modificaciones no planeadas, realizadas con o sin intención.

7.2 Responsables

La SDSCJ tiene como responsables de la definición, implementación y mantenimiento de la Política de Seguridad y Privacidad de la Información los siguientes actores:

1. Un Representante de la Alta Dirección (Secretario, Subsecretario o Jefe Oficina) de la SDSCJ o quien sea asignado para tal fin, es quien velará por el cumplimiento y mantenimiento de la Política de Seguridad y Privacidad de la Información de la Entidad.

2. El Comité Institucional de Gestión y Desempeño es el encargado de liderar y facilitar la implementación de la estrategia de Gobierno Digital y de Seguridad Digital y propender por el mejoramiento continuo del sistema, su evaluación, seguimiento y desempeño.
3. La Mesa Técnica de Seguridad Digital, es la instancia asesora para presentar recomendaciones técnicas, conceptualizaciones, valoraciones, y conceptos sobre seguridad de la información.
4. El (la) Director (a) de Tecnologías y Sistemas de la Información, quien es el encargado (a) de:
   - Implementar los controles definidos en la presente política y lo definido dentro Privacidad Manual de Seguridad y Privacidad de la información, supervisando su adecuada y efectiva aplicación.
   - Implementar la Política de Gobierno Digital a partir de la construcción de metodologías, planes, programas, proyectos e instrumentos que estén relacionados con el Modelo de Seguridad y Privacidad de la Información.
5. El (la) Director (a) de Recursos Físicos y Gestión Documental, es el responsable de establecer los lineamientos para la identificación, clasificación y buen uso de los activos de información física al interior de la Entidad.
6. Los líderes de procesos definidos en el mapa de procesos de la Entidad, como responsables de aplicar los lineamientos definidos en esta política.
7. El profesional de seguridad de la Información es la persona idónea técnicamente, para alinear las iniciativas de seguridad de información con los objetivos misionales, buscando el cumplimiento del objetivo del sistema integrado de seguridad de la información.

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

7.3 Divulgación

La SDSCJ en coordinación de la Oficina Asesora de Comunicaciones y la Dirección de tecnologías y Sistemas de Información son los responsables de divulgar la Política de Seguridad y Privacidad de la Información y los lineamientos descritos en el Manual de Seguridad de la Información y los respectivos documentos y procedimientos a todos los funcionarios o contratistas que se vinculen a la Entidad.

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

Cuando un funcionario y/o contratista cese en sus funciones laborales y/o culmine la ejecución de un contrato en la SDSCJ, el jefe inmediato o supervisor del contrato será el encargado de la custodia de los activos de información a cargo de dicho usuario.

Todos los funcionarios, contratistas y terceros de la SDSCJ deben cumplir con los lineamientos descritos en el “Manual de Seguridad y Privacidad de la Información”.

7.4 Activos de Información.

La SDSCJ a través de la Dirección de Recursos Físicos y Gestión Documental en apoyo de la Dirección de Tecnologías y Sistemas de la Información, establecen los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información física y digital, con el objetivo de garantizar su protección.

7.4.1. Propiedad De Los Activos.

Mediante los siguientes parámetros se van a adelantar la identificación, registro, gestión, uso y clasificación de los activos de información de la Entidad:

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

La identificación y actualización del inventario de activos de información se realiza anualmente o cuando sea necesario debido a cambios en la normatividad vigente, modificaciones en la estructura organizacional de la SDSCJ, o en su mapa de procesos. Los propietarios de la información son responsables de mantener actualizado el inventario y/o la Matriz de Activos de Información, realizando las actualizaciones programadas o cuando se requiera.

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

Para los operadores tecnológicos que prestan servicios a la SDSCJ, se deben implementar controles de seguridad establecidos en el Manual de Seguridad y Privacidad de la Información necesarios para garantizar la protección de los activos de información bajo su responsabilidad.

7.4.2. Controles a Los Archivos De Gestión.

La Dirección de Recursos Físicos y Gestión Documental, establece controles a los archivos de gestión de la Entidad para que cuenten con los mecanismos de seguridad que salvaguarden y conserven dicha información.

7.4.3. Clasificación de la Información.

Los propietarios de los activos de información deben documentar la clasificación de los activos de los que son responsables, designando un custodio para cada activo, con el apoyo de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información.

La clasificación de la información de la SDSCJ se debe realizar con base en la ley 1712 de 2014 reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015, la ley 594 de 2000 (Ley General de Archivos), la Ley 1581 de 2012 (Ley de Protección de Datos Personales) y las leyes que se definan al respecto.

Los operadores tecnológicos de la SDSCJ durante la ejecución contractual y con el fin de garantizar el adecuado uso de la información, deben cumplir con los lineamientos del manejo y clasificación de la información definida en el presente documento.

7.4.4. Uso Aceptable de los Activos.

Las soluciones tecnológicas (hardware, software, información de cualquier índole, servicios, etc.) al igual que los archivos, carpetas, bases de datos, Sistemas de Información y documentos, son activos de información que pertenecen a la SDSCJ, por lo cual su uso es exclusivamente institucional y es responsabilidad de aquel a quien se asigne o corresponda su uso, el propender por su confidencialidad, integridad, disponibilidad, privacidad y buen uso.

Las credenciales de acceso a los servicios de red y a Soluciones Tecnológicas (usuario y clave) son de carácter personal e intransferible; los funcionarios y contratistas de la SDSCJ no deben revelar éstas a terceros ni utilizar claves ajenas y serán responsable del cambio de clave de acceso periódicamente.

7.4.4.1 **Correo Electrónico**:

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

1. El correo electrónico asignado debe ser para uso única y exclusivamente institucional y no podrá ser utilizado para fines personales, económicos, comerciales, propaganda, campañas, invitaciones y cualquier otro uso ajeno a los propósitos de la Entidad.
2. No está permitida la creación de buzones de correo para agremiaciones, sindicatos u otras personas jurídicas ajenas a la SDSCJ, garantizando así el uso exclusivo del sistema de correo para fines institucionales.
3. El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @scj.gov.co, el cual cuenta con los parámetros de seguridad y requerimientos de ley para tal fin.
4. El envío masivo de correos dentro de la Entidad está restringido a los canales oficiales de comunicación previstos para tal fin, las solicitudes de envío masivo de mensajes deben ser gestionadas a través de la Oficina Asesora de Comunicaciones y/o las áreas autorizadas para tal fin.
5. Los correos electrónicos catalogados como tipo Spam, Phishing o que contengan Software Malicioso (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de servicio y serán tratados como incidentes de seguridad de la información.
6. Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados a la Dirección de Tecnologías y Sistemas

de la Información a través de la mesa de servicio y serán tratados como incidentes de seguridad de la información.

7. La cuenta de correo institucional no podrá ser utilizada para el registro o autenticación, en páginas o sitios publicitarios, de comercio electrónico, deportivos, redes sociales, casinos, concursos, sitios de citas o cualquier otro ajeno a las funciones y obligaciones que le correspondan en la SDSCJ.
8. Está prohibido el uso del correo para el envío de contenidos agresivos, insultantes, ofensivos, injuriosos, obscenos, que violen la propiedad intelectual o que atenten contra la integridad moral de las personas o instituciones.
9. Está expresamente prohibido distribuir información de la SDSCJ que no sea considerada de uso público a otras entidades o ciudadanos, sin la debida autorización de propietario del activo de información.
10. El correo electrónico institucional deberá contener junto con la firma un mensaje de confidencialidad, que deberá ser aprobado por la Dirección de Tecnologías y Sistemas de la Información.
11. Teniendo en cuenta que el correo electrónico es exclusivamente para uso institucional, la SDSCJ se reserva el derecho de monitorear el contenido. De esta manera contenidos de música, video, fotos o identificados como potencialmente peligrosos que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario y/o contratista podrán ser borrados sin previa consulta.
12. Las cuentas de correo electrónico se asignarán de acuerdo con la nomenclatura definida por la Dirección de Tecnologías y Sistemas de la Información.

7.4.4.2 Internet:

La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, define los controles necesarios y conexiones seguras para el acceso a internet desde y hacia cualquier activo de información que lo requiera, garantizando los niveles de seguridad adecuados y estableciendo los controles a la navegación, de acuerdo con los perfiles de navegación establecidos, es responsabilidad de todos los funcionarios y contratistas de la SDSCJ hacer un uso responsable del acceso a Internet y cumplir con las directrices establecidas para tal fin:

1. La Dirección de Tecnologías y Sistemas de la Información, define las restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
2. La Dirección de Tecnologías y Sistemas de la Información se reserva el derecho de monitorear, hacer seguimiento y validación del uso de red y equipos tecnológicos, para para asegurar que se utilicen de manera responsable y racional los recursos de la Entidad.
3. El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales. Se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, vulgar, ofensivo, injurioso, obsceno o violatorio de los derechos de autor.
4. El acceso a sitios web o la instalación de herramientas para evadir los controles y políticas de seguridad de navegación está estrictamente prohibido. Su detección será tratada como un incidente de seguridad, con las responsabilidades correspondientes.

5. La descarga de archivos no autorizados (desde Internet, correo electrónico) representa un alto riesgo para la seguridad de la información y una posible violación de los derechos de autor, Por lo tanto, es responsabilidad de los funcionarios y/o contratistas evitar descargas no autorizadas de material no institucional que pueda comprometer la integridad y confidencialidad de la información.
6. La SDSCJ, a través de la DTSI, debe coordinar con los operadores tecnológicos que requieran acceso o interconexión a las diferentes soluciones tecnológicas de la Entidad, los controles, parámetros y configuraciones necesarias para acceder a Internet o a canales de comunicación externos de forma segura.
7. En los casos donde la operación sea administrada por un operador tecnológico, éstos deben contar con los controles necesarios y conexiones seguras para el acceso a internet en las sedes de la SDSCJ. La DTSI o el supervisor del contrato debe realizar el monitoreo correspondiente.

7.4.4.3 Equipos de Cómputo y Otros Dispositivos:

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

1. Todos los equipos suministrados por la SDSCJ deben contener, como mínimo, un usuario y clave de acceso. Dicha clave será de uso personal e intransferible. La responsabilidad de uso recaerá sobre el funcionario o contratista a quien se asignó.
2. Los dispositivos tecnológicos asignados a funcionarios y contratistas solo podrán usarse para fines laborales relacionados con las funciones y obligaciones correspondientes, razón por la cual no tienen autorización de instalar software diferente al autorizado por la Dirección de Tecnologías y Sistemas de la Información.
3. Teniendo en cuenta que los equipos son para uso institucional, la SDSCJ se reserva el derecho de monitorear el contenido y software instalado en los equipos de la Entidad para verificar el tipo de información, su uso y el licenciamiento del software instalado. De esta manera, contenidos de música, video, fotos o demás que no correspondan al desempeño de las funciones u obligaciones contractuales respectivas del funcionario o contratista podrían ser borrados sin previa consulta. Así mismo, el software no autorizado o sin licenciamiento será desinstalado.
4. El personal de la mesa de servicio es el único autorizado por la DTSI para la instalación de software, para los casos de software diferente al establecido como base, debe contar con previa solicitud autorizada por el jefe o director del área de acuerdo con los parámetros establecidos para tal fin.
5. La DTSI define un listado con todo el software autorizado para los equipos de cómputo de la Entidad (Licenciado y de uso libre “Open Source”).
6. La mesa de servicios está autorizada para realizar cambios de partes, actualizaciones, desconectar, retirar y/o reparar equipos designados por la DTSI. En los casos donde la operación de la mesa de servicio sea gestionada por un operador tecnológico externo, este será el único autorizado para realizar dichos procesos
7. Cuando se aprovisionen o entreguen los respectivos equipos de cómputo al personal asignado dentro de la Entidad, este debe:

a. Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.
b. El software instalado y definido por la Dirección de Tecnologías y Sistemas de la Información debe contar con el respectivo licenciamiento.
c. Los sistemas operativos y demás Software deberán tener instaladas las últimas actualizaciones estables a la fecha de entrega del equipo, excepto que haya necesidades específicas para instalar una versión en especial, la cual debe ser soportada por la Dirección de Tecnologías y Sistemas de la Información.
d. El antivirus deberá permanecer actualizado, activado, funcionando y administrado desde consola.
e. Para los casos que la operación sea realizada por un operador tecnológico, este debe coordinar las actividades necesarias con el personal de la mesa de servicio para el aprovisionamiento de los equipos de cómputo.

8. Los equipos deberán quedar apagados cada vez que el funcionario y/o contratista no se encuentre en el lugar de trabajo por razones seguridad de la información y ahorro de energía. En el caso de necesitar dejar prendido un equipo, se debe contar con las autorizaciones del jefe inmediato y del Director de Tecnologías y Sistemas de la Información.
9. La Dirección de Tecnologías y Sistemas de la Información configura los servidores para el despliegue de actualizaciones, parches de seguridad y estrategias que permitan mantener actualizada toda la plataforma computacional de la SDSCJ.
10. Cuando se presenten ausencias de funcionarios y/o contratistas por incapacidades, vacaciones, licencias no remuneradas, suspensión de contrato, y demás consideraciones, debe ser bloqueado el acceso a los usuarios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. Es responsabilidad de la Dirección de Gestión Humana, la Dirección Jurídica y Contractual, la Dirección de Operaciones para el Fortalecimiento y los respectivos Supervisores de los contratos, notificar la ausencia de los usuarios con una solicitud a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de servicios.

7.4.4.4 Cableado Estructurado:

En las sedes de la SDSCJ donde haya cableado estructurado, las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas naranjas (Las cuales corresponde a un circuito eléctrico regulado con respaldo de UPS) y en ninguna circunstancia se puede conectar otros elementos eléctricos a los asignados en dichas tomas.

En los puntos de red de los usuarios no está permitido realizar conexiones de switches, Hub, Access Point u otros dispositivos para compartir accesos a servicios de red e internet, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

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

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

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

7.4.4.5 Sistemas de Información.

1. Solo podrán estar expuestas aquellas Soluciones Tecnológicas que deban ser consultados por personas externas a la SDSCJ, las demás son de uso interno y su acceso desde fuera de la Entidad se debe realizar a través de conexiones seguras (VPN) con previa autorización por parte de la Dirección de Tecnologías y Sistemas de la Información y del jefe inmediato, quien da el aval para dicho acceso.
2. En los casos donde la operación del Sistema de información de la Entidad sea administrada por un operador tecnológico externo (Contratista), las conexiones externas deben ser autorizadas por la Dirección de Tecnologías y Sistemas de Información de la SDSCJ.
3. En los casos donde las soluciones tecnológicas de la Entidad son administradas por un operador tecnológico o propiedad de un tercero, estos deben cumplir con los lineamientos específicos de seguridad de la información descritos en el Manual de Seguridad y Privacidad de la Información de la SDSCJ.
4. Las bases de datos a las que se conectan los sistemas de información internos o los sistemas de información administrados por un operador tecnológico para la operación son de la SDSCJ, siempre y cuando la información y el sistema de información sea de propiedad de la SDSCJ o en su defecto se definan las formas de utilización y propiedad dentro de las obligaciones contractuales correspondientes.

7.4.4.6 Sistema de Videovigilancia de las Sedes de la SDSCJ.

Las credenciales de acceso a los sistemas de video vigilancia de todas las áreas que hagan parte de la SDSCJ son de carácter estrictamente personal e intransferible; los operadores tecnológicos, funcionarios y contratistas de la SDSCJ no deben revelar éstas a terceros ni utilizar claves ajenas.

Los operadores tecnológicos que realizan la administración, el soporte y mantenimiento del sistema de video vigilancia y demás soluciones tecnológicas dispuestos en otras instalaciones o dependencias de la Entidad, deben cumplir los lineamientos definidos en la presente política, así como los establecidos en el Manual de Seguridad y Privacidad de la Información de la SDSCJ.

7.5 Controles de Acceso y Seguridad de la Información

7.5.1 Control De Acceso:

La SDSCJ a través de La Dirección de Recursos Físicos y Gestión Documental, establece controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la

Entidad, teniendo en cuenta las áreas de acceso restringido y los controles de acceso correspondientes (Centro de Datos, Archivo, y demás áreas designadas como restringidas en la Entidad).

Las dependencias de la Entidad con apoyo de La Dirección de Tecnologías y Sistemas de la Información definen los controles, procedimientos e instructivos para proveer el acceso las soluciones tecnológicas, así como la asignación de permisos a usuarios autorizados para el cumplimiento de sus funciones, en las distintas sedes de la Secretaría.

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

La Dirección de Tecnologías y Sistemas de la Información con apoyo de las dependencias de la SDSCJ implementa controles, procedimientos e instructivos para proveer el acceso físico y lógico de los recursos informáticos a usuarios autorizados para el cumplimiento de sus funciones y obligaciones contractuales.

7.5.2 Controles Criptográficos

La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información implementa directrices para el uso adecuado de controles criptográficos, con el propósito de establecer una guía basada en las mejores prácticas.

Los propietarios de los activos de información deben identificar las necesidades de criptografía de información de acuerdo con el grado de criticidad y privacidad de esta e informar de dicha necesidad a la Dirección de Tecnologías y Sistemas de la Información quien debe analizar el requerimiento y si es procedente, aprobar.

La Dirección de Tecnologías y Sistemas de la Información debe asegurar el uso adecuado y efectivo de los métodos criptográficos que aplica para proteger la confidencialidad, integridad y disponibilidad de la información que así lo requiera.

7.5.3 Seguridad Física y del Entorno

La SDSCJ a través de la Dirección de Recursos Físicos y Gestión Documental, implementa controles para proteger el perímetro de las instalaciones físicas, controlar el acceso del personal y la permanencia en las oficinas e instalaciones, así como controlar el acceso a áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información clasificada y reservada, así como aquellas en las que se encuentren los equipos y demás infraestructuras de soporte a los sistemas de información y comunicaciones), además mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información de la Entidad.

La SDSCJ a través de la Dirección de Recursos Físicos y Gestión Documental, implementa 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. En consecuencia, todos los funcionarios, contratistas, proveedores o terceros y visitantes de la SDSCJ deben acatar lo definido por la Entidad para el acceso a las áreas de acceso restringido, y circular en las instalaciones de la debidamente identificados, con un documento que acredite su tipo de vinculación el cual se deberá portar en un lugar visible.

En los casos específicos del Centro de Comando, Control, Comunicaciones y Cómputo-C4 y la Cárcel Distrital de Varones y Anexo de Mujeres, Centro Especial de Reclusión (CER) y Centro de Traslado por Protección (CTP) éstos serán los responsables de la administración de los controles de acceso restringido, los directores o jefes de oficina realizarán el seguimiento al cumplimiento de estos y reportarán cualquier novedad que afecte la seguridad de la información a la Dirección de Tecnologías y Sistemas de la Información de la SDSCJ.

7.5.4 Seguridad de las Operaciones.

La Dirección de Tecnologías y Sistemas de la Información se debe encargar de la operación y administración de los recursos tecnológicos que soportan la operación de la Entidad y propender por la implementación de los controles asociados a éstos para mitigar los riesgos sobre la confidencialidad, integridad y disponibilidad de la información; para este fin debe cumplir con los siguientes lineamientos:

1. Implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en el Data Center de la Entidad y la información almacenada en servicios en nube y su recuperación en caso de desastre.
2. Implementar controles para mitigar los riesgos inherentes a códigos maliciosos.
3. Implementar controles para auditar el acceso y uso de datos por parte de los funcionarios o contratistas, a los sistemas de información designados por la Dirección de Tecnologías y Sistemas de la Información.
4. Proveer los recursos necesarios para la implementación de los controles requeridos para la seguridad de las operaciones.
5. Definir e implementar un Plan de Continuidad y Contingencia de Servicios Tecnológicos que propenda por la mitigación de los riesgos sobre la confidencialidad, integridad y disponibilidad de la información.

7.5.5 Seguridad de las Comunicaciones.

La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información o en quien delegue:

1. Establecerá los Acuerdos de Niveles de Servicios - ANS requeridos para que los proveedores de servicios conectividad y de soporte de infraestructura de red garanticen la disponibilidad de los servicios de red e internet en todas las sedes.

2. Implementar los mecanismos necesarios para proteger la información que circule a través de las redes de datos de la Entidad propendiendo por la integridad, confidencialidad y disponibilidad de la información mediante establecimiento de conexiones VPN entre las sedes, nivel central y los servicios dispuestos en nube.

7.5.6 Controles en la Adquisición, Desarrollo Y Mantenimiento de herramientas, aplicaciones y/o Sistemas.

La Dirección de Tecnologías y Sistemas de la Información de la SDSCJ, está autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de herramientas, aplicaciones y sistemas de información y demás software, velando por que incorporen las buenas prácticas para el desarrollo seguro de software y estándares de seguridad informática. En los casos donde otras dependencias requieran adquirir soluciones Tecnológicos, el proceso debe llevar un visto bueno de la Dirección de Tecnologías y Sistemas de la Información.

En los casos donde el desarrollo o mantenimiento del sistema de información sea administrado por un operador tecnológico (contratista), este debe implementar los mecanismos necesarios para proteger la información almacenada en los sistemas de información, propendiendo por la integridad, confidencialidad y disponibilidad.

Anualmente, se adelantará una revisión de los computadores y el software que es instalado en los mismos, de tal manera que se ejecuten controles de instalación de software que no esté avalado por la Entidad, ajustes a los perfiles de usuario.

7.5.7 Controles en las Relaciones con los Proveedores.

La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información, la Dirección Jurídica y Contractual, y la Dirección de operaciones, definirán mecanismos de control que aseguren que la información a la que tenga acceso un tercero cuente con un nivel de protección adecuado y que éstos cumplan con las políticas y procedimientos de seguridad y privacidad de la información establecidos.

Para la mitigación de los posibles riesgos asociados con el acceso de proveedores a los activos de información de la Entidad, deben ser acordados y documentados entre la SDSCJ y los proveedores, los requisitos de seguridad de la información con el fin de asegurar la protección de dichos accesos.

1. Los proveedores tendrán acceso limitado a información reservada y clasificada de la SDSCJ.
2. Los proveedores no podrán tener acceso a áreas o zonas donde se encuentre información clasificada y/o reservada en la Entidad. Sí fuera necesario su ingreso a determinadas áreas, será necesaria la autorización por parte de la Dirección recursos Físicos y Gestión Documental.
3. Los proveedores que tengan relaciones contractuales con la Entidad, se les incluirá dentro de su contrato una cláusula de confidencialidad de la información.

4. Para la contratación de los proveedores se realizará según lo establecido en el Manual de Contratación de la Entidad.

7.5.8 Seguridad en la Gestión de Continuidad de Negocio.

La SDSCJ deberá disponer de un Plan de Continuidad de Negocio y a través de la Dirección de Tecnologías y Sistemas de la Información, implementar el Plan de Recuperación ante desastres tecnológicos - DRP con el fin de mantener la funcionalidad, confidencialidad, integridad y disponibilidad de los recursos tecnológicos misionales que sean considerados críticos para la continuación de la operación en la Entidad de manera aceptable.

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

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

7.5.9 Gestión de Incidentes de Seguridad de la Información.

La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información se encarga de definir, documentar, mantener, publicar y aplicar los procedimientos para atender, valorar, clasificar y dar respuesta a los eventos e incidentes de seguridad de la información que se presenten y que comprometan las operaciones de esta. De igual forma la Dirección de Tecnologías y Sistemas de la Información deberá promover el reporte de eventos de seguridad de la información para reducir la probabilidad e impacto del riesgo inherente a ellos.

Los eventos e incidentes de seguridad de la información serán analizados por la Dirección de Tecnologías y Sistemas de la Información de acuerdo con el procedimiento de incidentes de seguridad de la información.

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

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

7.6 Dispositivos Móviles.

Se establece los parámetros sobre el uso de los dispositivos móviles que permita gestionar de manera eficaz los riesgos ocasionados por la ejecución de actividades laborales a través de estos.

Considérese Dispositivos Móviles a todos los Computadores portátiles, Equipos Celulares (Smartphone), Tabletas, Agendas Digitales, Cámaras Fotográficas, Cámaras de Video, Proyectores de Video (Video Beam), Tarjeta de Control de acceso, entre otros, que pertenecen o están asignados a la SDSCJ.

Los dispositivos móviles solo deben tener acceso a la información autorizada por parte de los responsables de los diferentes procesos, de igual manera, los funcionarios y contratistas deben proteger físicamente los dispositivos móviles asignados y que son propiedad y/o arrendamiento de la Entidad para evitar la pérdida, acceso o la divulgación no autorizada de la información institucional.

De acuerdo con los niveles de clasificación legal de la información almacenada en el dispositivo móvil, se determinará la necesidad de aplicar controles de cifrado de datos, así como la ejecución de copias de respaldo periódicas, por ende, se hace necesario el establecimiento de las condiciones necesarias para el acceso a los recursos de red y activos de información de la SDSCJ a través de los dispositivos de tecnología móviles.

La autorización de conexión de dispositivos móviles a las redes de datos de la Entidad se realiza por parte de la mesa de servicio, una vez se establezcan todos los parámetros de seguridad de la información dispuestos para estos.

En todo caso se debe cumplir con los parámetros establecidos en el Manual de Seguridad y Privacidad de la Información en lo referente a los dispositivos Móviles.

7.7 Teletrabajo

Definir los lineamientos relativos al ejercicio del teletrabajo por parte de los funcionarios y/o contratistas de la Entidad, que realice sus funciones mediante la modalidad de teletrabajo, ya sea de manera temporal o permanente, y mediante la cual genere, procese, consulte, almacene, transmita y en general realice cualquier actividad o acción sobre la información institucional de la SDSCJ.

Entiéndase modalidad de Teletrabajo los empleos cuyas funciones se pueden desarrollar fuera de las sedes de la Entidad, siempre que se cuente con las tecnologías de la información y las comunicaciones necesarias para adelantar actividades relacionadas con las funciones y responsabilidades, sin riesgos de seguridad de la Información.

Dentro de las condiciones mínimas para acceder a la modalidad de Teletrabajo, los colaboradores de la Entidad deberán desempeñar funciones y actividades que puedan ser cumplidas fuera del lugar de trabajo con apoyo de las tecnologías de la información TI.

7.8 Escritorio y Pantalla Limpia

Establecer por parte de la SDSCJ, normas de escritorios limpios para proteger documentos físicos y dispositivos de almacenamiento removibles, del mismo modo normas de pantallas limpias para

toda la Entidad, a fin de reducir los riesgos de acceso no autorizado, perdida o daño de la información; y de esta manera responsabilizar a todos los funcionarios y/o contratistas sobre el cuidado de los activos de Información de la SDSCJ.

1. Se deben mantener los escritorios físicos y áreas de trabajo libres de todo material o elemento que contenga información clasificada como confidencial, a menos que esta esté siendo utilizada por personal autorizado, el cual deberá garantizar el aseguramiento adecuado de la misma en todo momento.
2. Los funcionarios y contratistas deben mantener el puesto de trabajo y escritorio de los equipos de cómputo, organizado y libre de archivos o información institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.
3. Se debe evitar el consumo de alimentos o bebidas en áreas de trabajo donde se encuentre ubicada la información institucional en papel, equipos de cómputo, dispositivos electrónicos o cualquier medio de almacenamiento que pueda llegar a ser afectado por el derrame de líquidos o residuos de alimentos.
4. Es responsabilidad de todos los funcionarios y contratistas de la SDSCJ, bloquear la sesión de sus equipos de cómputos al ausentarse del puesto de trabajo, así como cerrar las sesiones activas.
5. Los funcionarios o contratistas que usen equipos de cómputos en la Entidad deberán apagar sus equipos en horas no laborales, salvo casos específicos para equipos que deben correr software o aplicación específica de acuerdo con la naturaleza de las funciones u obligaciones del usuario, así como para actividades relacionadas con teletrabajo o trabajo en casa
6. Toda información impresa y/o en medios magnéticos que sea clasificada como confidencial, y que no esté siendo utilizada, deberá permanecer asegurada de forma adecuada y segura.
7. Todo funcionario que tenga acceso a información confidencial en medios físicos deberá prevenir su divulgación o acceso a personas no autorizadas que trabajen en ambientes o módulos o que sean ajenas a la Entidad.
8. La información digital que sea clasificada o reservada de la SDSCJ deberá ser almacenada en los repositorios asignados para tal fin que impidan el acceso por personal no autorizado, asignando permisos de acceso restringido a la misma.
9. Es responsabilidad de los funcionarios y/o contratistas al usar los servicios de impresión retirar de forma inmediata cualquier tipo de documento impreso.
10. Todo documento que contenga información clasificada y/o reservada no podrá ser reciclado; y deberá ser destruido de tal manera que se impida la reconstrucción de dicha información.

7.9 Copias de Respaldo.

Establecer los parámetros aplicables a la infraestructura y las soluciones tecnológicas, con el fin de garantizar la administración y gestión de las copias de respaldo y pruebas de restauración de la Información de la Entidad.

La SDSCJ, protegerá toda la información mediante el uso de copias de respaldo y pruebas de restauración de los datos contenidos en medios de almacenamiento, equipos de cómputo, servidores, repositorios o directorios, configuraciones, aplicativos y/o servicios de nube y demás elementos de almacenamiento de la Entidad.

7.10 Método Definido Para Operar

La SDSCJ establece que la presente Política de Seguridad y Privacidad de la Información se operacionaliza a través del "*Manual de Seguridad y Privacidad de La Información*" en el cual se encuentran los lineamientos detallados para el cumplimiento, implementación y monitoreo de esta.

7.11 Administración de la Política y Procedimiento de Cambio

La Política de Seguridad y Privacidad de la Información se preserva en el tiempo. Sin embargo, se debe hacer revisiones ante cambios normativos, estructurales y tecnológicos que afecten a la SDSCJ, para asegurar que ésta cumple con el cambio de las necesidades de la Entidad. La Alta Dirección es la encargada de apoyar la implementación del sistema de gestión de seguridad de la Información de acuerdo con los lineamientos institucionales.

7.12 Propiedad Intelectual

Todo el material desarrollado por una persona natural o jurídica mientras tenga una vinculación como funcionario y/o contratista con la SDSCJ se considera como derechos patrimoniales de propiedad exclusiva de la Entidad. Dicho material debe ser protegido contra cualquier divulgación, descubrimiento o uso que perjudique los intereses institucionales, misionales, reputacionales, económicos, o cause cualquier daño a la SDSCJ conforme a lo establecido en la ley 23 de 1982 sus normas reglamentarias y aquellas que la modifiquen.

La Dirección Jurídica y Contractual, la Dirección de Gestión Humana y la Dirección de operaciones para el Fortalecimiento, deben realizar las tareas pertinentes para que en los contratos suscritos con empleados, contratistas, terceros y operadores tecnológicos se incluyan las cláusulas correspondientes que especifiquen los compromisos y cuidados que se debe tener con la información susceptible de protección por parte del régimen de propiedad intelectual y en lo referente a la confidencialidad.

Con el fin de cumplir las leyes sobre propiedad intelectual, la DTSI debe adelantar acciones para el guardado de archivos dentro de los equipos de la Entidad y en ese sentido, establecer parámetros para el borrado de archivos no institucionales que no deban estar en los computadores, tales como archivos de video (mp4, avi, flv, etc.), archivos de audio (3gp, mp3, etc.), fotografías, etc. Es importante considerar que ciertos usuarios deben estar dentro de las excepciones, ya que el cumplimiento de sus funciones está orientado a la producción de dicho

material. En estos casos, se debe documentar y gestionar las solicitudes correspondientes para formalizar dicha excepción.

7.13 Administración del Riesgo Para la Seguridad de la Información.

Los líderes de procesos de la SDSCJ, acompañados por el profesional de Seguridad de la Información o quien haga sus veces, deben realizar la identificación, clasificación y tratamiento de riesgos de seguridad de la información, que puedan comprometer las operaciones de la Entidad y amenazar la seguridad de la información , El reporte de las evidencias de los controles definidos para la mitigación de los riesgos se realizará de acuerdo de acuerdo con lo definido en la Política de Administración de Riesgos de la Entidad.

7.14 Concienciación en Seguridad de la Información.

La SDSCJ debe contar con un plan de concientización y/o capacitación en seguridad de la información y privacidad de la Información, que permita garantizar que los funcionarios, contratistas y terceros que accedan a la información de la Entidad estén informados acerca de los riesgos y amenazas que ponen en riesgo la información de la Entidad.

7.15 Cumplimiento

La SDSCJ velará por la identificación, documentación y cumplimiento de la normatividad vigente y aplicable relacionada con seguridad de la información.

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

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

Elaboró: Diego Mauricio Usme González – Contratista SDSCJ

Revisó: Jairo Alonso Bohórquez Blanco – Profesional Especializado 222-27.
Francisco Javier Vargas Moncada - Profesional Universitario 219-18.
Diana Camila Méndez Restrepo – Contratista SDSCJ
Diana Carolina Hernandez – Contratista SDSCJ
Armando Alfonso Leyton González– Contratista SDSCJ.
Jorge Eliecer Velásquez Perilla – Contratista SDSCJ.
Rafael Humberto López Saavedra – Contratista SDSCJ.
Zuleima Astrith Mancera Silva – Contratista SDSCJ.

La información de aprobación de este documento podrá ser consultada en el sistema “Portal MIPG” - https://portalmipg.scj.gov.co