POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

1. INTRODUCCION.

La Secretaría Distrital de Seguridad, Convivencia y Justicia, 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 1008 de 2018 por medio del cual se establecen los lineamientos referentes 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, 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 gestiones activos de información en la entidad, orientación que en adelante se denominara “Política General de Seguridad de la Información”.

Es así como a partir de las disposiciones legales correspondientes, el presente documento establece la Política de Seguridad de la Información para la Secretaría Distrital de Seguridad, Convivencia y Justicia como eje rector del Sistema Integrado 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 Integrado 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 servidores, contratistas y terceros de la Secretaría Distrital de Seguridad, Convivencia y Justicia, conforme a los controles de seguridad y privacidad determinados por la entidad, en concordancia con la normatividad técnica de la familia ISO 27000:2013, 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 los operadores tecnológicos (contratistas y proveedores) que operan para la SDSCJ, teniendo en cuenta que éstos realizan la administración, operación, soporte, mantenimiento y custodia de las plataformas tecnológicas que cumplen las funciones para llevar a cabo la misionalidad de la Entidad.

4. GLOSARIO

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.

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

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.

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 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.

5. MARCO LEGAL Y/O NORMATIVO

Para consultar el marco legal y normativo por favor remítase al normograma del proceso de gestión de tecnología de la información de la dirección de tecnologías y sistemas de la información - DTSI

6. DECLARACIÓN DE LA POLÍTICA

A partir del Modelo de Seguridad y Privacidad de la Información emanado por el Ministerio de las Tecnologías de la Información y las Comunicaciones, la Secretaría Distrital de Seguridad, Convivencia y Justicia, 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 A través del proceso Gestión de Tecnología de Información que lidera la Dirección de Tecnologías y Sistemas de la Información, se 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 como responsables de los procesos institucionales y por ende de la información registrada, así como de la autorización de cambios. De igual manera, los propietarios serán responsables de todas las modificaciones solicitadas de la información registrada en los sistemas de información.

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

5. A través del proceso de Gestión de Recursos Físicos y Documental, liderado por la Dirección de Recursos Físicos y Gestión Documental, se establecerán 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 Secretaría Distrital de Seguridad, Convivencia y Justicia que tienen la custodia de la información generada en el marco de sus funciones se encuentran capacitadas para aplicar los controles correspondientes para proteger la información y mantener actualizado el inventario de activos de información relacionados con su servicio y funciones.

7. Los activos de información, equipos, bienes, aplicaciones, bases de datos, herramientas tecnológicas y servicios de Tecnologías de la Información y las Comunicaciones en adelante TIC, asignados a las personas por la SDSCJ son para uso exclusivo del cumplimiento de las funciones u obligaciones designadas; razón por la cual la información almacenada, procesada y generada a través de dichos activos, herramientas y dispositivos se considera propiedad de la entidad y el uso inadecuado de dichos recursos puede conllevar a las sanciones disciplinarias y legales correspondientes. En este sentido, los dispositivos personales que sean utilizados por los funcionarios, proveedores y contratistas

para adelantar acciones de la Secretaría, serán dispuestos dependiendo de las definiciones y dictámenes legales correspondientes.

8. Los funcionarios, contratistas, proveedores de la SDSCJ tienen la obligación de estudiar y 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 que sean administrados por operadores tecnológicos que no están integrados al dominio de la SDSCJ, deben ser responsabilidad en su uso y manejo por el mismo operador tecnológico y la Dirección de Tecnologías y Sistemas de la Información establecerá los lineamientos de seguridad que se deban cumplir.

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 cuentas de servicio (utilizadas para la administración y gestión de software o hardware directamente con los proveedores – Oracle, Microsoft, tales como notificaciones.judiciales@scj.gov.co, atencionalciudadano@scj.gov.co, etc.), deberán estar asociadas a un funcionario o contratista quien adelantará su gestión, siendo debidamente administradas y gestionadas por la Dirección de Tecnología y Sistemas de la Información junto con los líderes de área o responsables directos.

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 administrados por ellos, que sea de la entidad y entregar aquella que sea pertinente al finalizar el contrato, teniendo en cuenta que deben propender por la integridad, disponibilidad y confidencialidad de esta de acuerdo a las normas legales vigentes.

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

15. Los terceros y funcionarios de éstos que hacen uso de los activos de información de la SDSCJ deben cumplir los lineamientos descritos en la Política de Seguridad y Privacidad de la Información.

16. Los funcionarios, contratistas y terceros se comprometen a hacer uso adecuado de los dispositivos móviles para el acceso a los servicios corporativos de movilidad proporcionados por la entidad, tales como escritorios remotos y aplicaciones virtuales, correo, comunicaciones unificadas, redes virtuales privadas (VPN), entre otros. Los dispositivos móviles de propiedad de la entidad son de estricto uso para el cumplimiento de la misionalidad de la misma y por ende se deben gestionar desde la Dirección de Tecnología y Sistemas de la Información para efectos del software instalado, cuotas de servicio y demás consideraciones que se deben tener en cuenta frente a estos dispositivos, en el entendido que guardan información de alta sensibilidad, pues son utilizados por altos directivos y se deben definir consideraciones especiales para su gestión. Los dispositivos móviles de los funcionarios, contratistas o terceros que no son propiedad de la entidad, deben ser aislados en VPN o redes WIFI que sean restringidas y aisladas de las redes de la entidad.

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

18. La Entidad ante la Superintendencia de Industria y Comercio – SIC, el registro de las bases de datos con datos personales que se tengan dentro de la SDSCJ.

19. 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 activar el procedimiento de gestión de incidentes y, 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.

6.1 Principios

1. **Responsabilidad:** La información es uno de los activos más importantes de la SDSCJ por lo tanto se espera que sea utilizada por las personas, acorde al cumplimiento de sus funciones u obligaciones.
2. **Confidencialidad**: La información de propiedad de la SDSCJ y de terceras partes 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 o en los casos legales correspondientes.
3. **Integridad**: Las personas que accedan a la información de propiedad de la SDSCJ deben preservar la integridad de esta, independientemente de su residencia temporal o permanente, o la forma en que sea transmitida. De la misma manera, debe estar protegida contra modificaciones no planeadas, realizadas con o sin intención.
4. **Disponibilidad**: La información de propiedad de la SDSCJ debe estar disponible a las personas autorizadas cuando sea requerida.
5. **Privacidad**: La información de propiedad de la SDSCJ debe ser preservada y utilizada para los propósitos que fue obtenida.

6.2 Responsables

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

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. El (la) Director (a) de Tecnologías y Sistemas de la Información, quien es el encargado(a) de:

a. Implementar las políticas de seguridad informática y de la plataforma tecnológica de la SDSCJ contenidas en los controles definidos dentro de la declaración de aplicabilidad y dentro de esta política, definiendo los planes de contingencia y supervisando su adecuada y efectiva aplicación.
b. Implementar la Política de Gobierno Digital y, por ende, realizar seguimiento a la implementación del Sistema de Gestión de Seguridad de la Información a partir de la construcción de metodologías, planes, programas, proyectos e instrumentos que estén relacionados con el Sistema de Gestión de Seguridad de la Información.

4. El (la) Director (a) de Recursos Físicos y Gestión Documental, quien es el(la)responsable de establecer los lineamientos para la identificación, clasificación y buen uso de los activos de información física al interior de la Entidad, con el fin de proteger la misma.
5. Los líderes de procesos definidos en el Sistema Integrado de Gestión, como responsables de aplicar los lineamientos definidos en esta política.
   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

6.3 Divulgación

La SDSCJ a través de la Oficina Asesora de Comunicaciones es la responsable de divulgar la Política de Seguridad y Privacidad de la Información y los lineamientos descritos en el Manual de Seguridad de la Información 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 de prestación de servicios, contratos de planta de personal y contratos de operadores que administran, operan, soportan, mantienen y custodian activos de información de la SDSCJ respectivamente incorporen las funciones u obligaciones correspondientes a exigir el cumplimiento de la Política de Seguridad y Privacidad de la Información, el manejo confidencial de la información, la cesión de derecho de autor a la entidad y la protección de datos personales.

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

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

https://portalmipg.scj.gov.co/lib/download.php?nivel1=a054VmZRbHVsejE2bHJsTHlMUUlEY3pIMDhCR0lBTkpFRDE5TmJWSFBaWW9BSXdSRnQveEF3OTVOejdFb0VKUG0xVkdrS3I0NXRlVStPbXpjZGlZSGc9PQ==&nivel2=RWdETk82RUpNMFgrUWxKVFljenR2dWpEUzl4d3U5VmdhRkh1Mm94ai9pdz0=

6.4 Seguridad de los Activos de Información

Mediante las siguientes políticas se van a adelantar la identificación, registro, gestión, uso y clasificación de los activos de información de la Entidad.

6.4.1 Gestión De La Seguridad En Los Activos.

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

6.4.2 Propiedad De Los Activos

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

Los propietarios de la información deben propender para que los custodios de los activos mantengan actualizado el inventario Matriz de Activos de Información y realicen las actualizaciones programadas una vez al año 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.

Con el objeto de implementar los controles de seguridad de información, las dependencias de la SDSCJ que tienen la custodia de la información, en el marco de su

función, se encargarán de proteger la información, y propender para que el propietario mantenga y actualice el inventario de activos de la información y proponer las mejoras correspondientes, para más información diríjase a la Declaración de Aplicabilidad.

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

6.4.3 Controles a Los Archivos De Gestión.

La Dirección de Recursos Físicos y Gestión Documental, debe implementar controles para garantizar que los archivos de gestión de la entidad cuenten con los mecanismos de seguridad que salvaguarden y conserven dicha información.

6.4.4. Clasificación de la Información.

Los propietarios de los activos de información deben documentar la clasificación de seguridad de los activos de los que son responsables y designarán un custodio para cada activo, con el apoyo de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, según sea el caso (activo digital o activo documental).

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.

6.4.5. Uso Aceptable de los Activos.

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

Las credenciales de acceso a la red y a recursos informáticos (usuario y clave) son de carácter estrictamente personal e intransferible; los servidores y contratistas de la SDSCJ

no deben revelar éstas a terceros ni utilizar claves ajenas. Todo servidor y contratista será responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

En los casos donde la operación del recurso sea administrada por un operador tecnológico (contratista), la Dirección de Gestión Humana de la SDSCJ debe notificar al operador, cualquier novedad que se presente con el personal asociado a la operación, con el fin de realizar las actualizaciones correspondientes en los equipos utilizados por el personal junto con el cambio de contraseñas respectivo.

Dentro de los recursos se encuentran los siguientes:

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

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. El único correo electrónico autorizado para el manejo de la información institucional es el asignado con el dominio @scj.gov.co pues este cumple con los parámetros de seguridad y requerimientos de ley para tal fin.
3. Está prohibido el envío de correos masivos (más de 100 destinatarios) tanto internos como externos, salvo a través del correo del Secretario(a), el Subsecretario(a) de Gestión Institucional, el Subsecretario (a) de Acceso a la Justicia, el Subsecretario(a) de Inversiones y Fortalecimiento de Capacidades Operativas, el Subsecretaria(o) de Seguridad. El secretario y los Subsecretarios podrán solicitar dichos permisos para otras cuentas de manera permanente o transitoria, diligenciando el respectivo formato y su justificación.
4. Los correos electrónicos catalogados tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) se deberán reportar a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información. No está permitido el envío o reenvío de ningún tipo de SPAM. En el caso de recibir correos con problemas de seguridad, se debe adelantar el procedimiento para gestión de Incidentes de seguridad.
5. Todos aquellos mensajes sobre los que se dude su origen, remitente o contenido o se consideren sospechosos, deben ser reportados a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de ayuda y serán tratados como incidentes de seguridad de la información.

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

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

1. La Dirección de Tecnología y Sistemas de la Información, define las políticas, restricciones de acceso, ancho de banda máximo a utilizar, horarios, derechos de descarga de archivos, permisos de navegación y demás relacionados, para garantizar el uso eficiente y racional del Internet.
2. La Dirección de Tecnologías y Sistemas de la Información se reserva el derecho de monitorear, hacer seguimiento y auditoría a los usuarios, para verificar que se haga un uso responsable y racional los recursos de la Entidad.
3. El uso del Internet deberá ajustarse a las necesidades de la función u obligaciones contractuales dentro del marco institucional y se prohíbe expresamente el acceso o consulta de páginas Web con contenido insultante, vulgar, ofensivo, injurioso, obsceno, pornográfico, violatorio de los derechos de autor y todo aquel que atente contra la integridad moral.

4. El acceso a sitios Web o la instalación de aplicaciones para intentar evadir los controles y políticas de seguridad de navegación está totalmente prohibidos y su detección será tratada como un incidente de seguridad, con las responsabilidades correspondientes.
5. El descargar archivos provenientes de Internet implica un riesgo para la seguridad de la información, así como un riesgo de infracción al régimen legal de derechos de autor, por lo cual se solicita que únicamente se haga este tipo de procesos cuando se cuente con los permisos correspondientes y teniendo en cuenta que cada persona es responsable por la seguridad de la información y por el cumplimiento de los derechos de autor. En el caso de archivos adjuntos a un correo electrónico, se debe tener en cuenta que sea información para la ejecución de su labor y en caso contrario, es la responsabilidad del servidor o contratista el tratamiento y uso de este y por ende del riesgo que proviene de dicha descarga.
6. La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, debe coordinar con los operadores tecnológicos que requieran acceso o interconexión a la infraestructura o a los activos de información de la entidad para acceder a internet o a canales de comunicación externos, los controles que se deben seguir para dicha interconexión y operación.
7. En los casos donde la operación sea administrada por un operador tecnológico, éstos deben contar con los controles necesarios y conexiones seguras para el acceso a internet en las sedes de la SDSCJ. La Dirección de Tecnología y Sistemas de Información o el supervisor del contrato debe realizar el monitoreo correspondiente.

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

1. Aquellos dispositivos que requieran clave de acceso, dicha clave será de uso personal y no podrá ser compartida, razón por la cual la responsabilidad de un posible mal uso recaerá sobre el funcionario o contratista a quien se asignó dicho usuario y clave.
2. Los dispositivos asignados solo podrán usarse para fines laborales relacionados con las funciones y obligaciones correspondientes, razón por la cual no tienen autorización de instalar software diferente al autorizado por la Dirección de Tecnología y Sistemas de la Información.
3. Los dispositivos de cómputo y móviles que sean asignados a los funcionarios y contratistas serán para uso institucional exclusivamente e intransferibles y la responsabilidad de su uso recaerá sobre la persona a la que le fue asignado.
4. Teniendo en cuenta que los equipos son para uso institucional, la SDSCJ se reserva el derecho de monitorear el contenido y software instalado en los equipos

de la entidad para verificar el tipo de información, su uso y 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.

5. Los únicos autorizados para la instalación de software adicional a las aplicaciones base es el personal técnico que designe la Dirección de Tecnologías y Sistemas de la Información, previa solicitud a través de la mesa de ayuda y luego de la aprobación respectiva (se debe constatar la necesidad de su uso y que la SDSCJ cuente con el respectivo licenciamiento). En los casos donde la operación de mesa de servicio sea manejada por un operador tecnológico externo, estos serán los únicos autorizados para realizar instalación de software adicional en los equipos, bajo las consideraciones definidas por las SDSCJ.
   De la misma manera, la Dirección de Tecnologías y Sistemas de la Información define un listado con todo el software que puede ser instalado en los computadores de la Entidad y el listado básico que es instalado, al momento de realizar formateo y entrega de un computador a un contratista o servidor. En este sentido, la instalación de software es exclusiva de las personas encargadas para tal fin e indicadas por la Dirección de Tecnologías y Sistemas de la Información.
6. Los únicos autorizados para realizar cambio de partes, actualizaciones, destapar, desconectar, retirar, y/o reparar equipos, son los técnicos de soporte designados por la Dirección de Tecnologías y Sistemas de la Información previa solicitud a través de la mesa de servicio. En los casos donde la operación de mesa de ayuda sea manejada por un operador tecnológico externo, estos serán los únicos autorizados para realizar el proceso en mención.
7. Cuando se aprovisionen o entreguen los respectivos equipos de cómputo al personal asignado dentro de la entidad se debe garantizar:
   a. Sean formateados a bajo nivel para que la información de los anteriores usuarios no sea recuperable o accesible.
   b. El software instalado sea el software base definido por la Dirección de Tecnología y Sistemas de la Información y este cuente con el respectivo licenciamiento.
   c. Los sistemas operativos y demás aplicativos 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 Tecnología y Sistemas de la Información.
   d. El antivirus deberá permanecer actualizado, activado, funcionando y administrado desde consola.
   e. Cuando aplique, en caso de que la operación sea realizada por un operador tecnológico, este debe coordinar las actividades necesarias con el personal

de la mesa de servicio para el aprovisionamiento de los equipos de cómputo.

8. Los equipos deberán quedar apagados cada vez que el funcionario o contratista no se encuentre en la oficina durante la noche, por seguridad y ahorro de energía entre otras, 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 ya sea para desarrollar contingencia o continuidad de negocio.
9. La Dirección de Tecnología y Sistemas de la Información, en cabeza del personal de infraestructura o en su caso el operador tecnológico encargado, debe implementar servidores para el despliegue de actualizaciones y parches de seguridad y diseñar estrategias que permitan mantener actualizada toda la plataforma computacional de la SDSCJ.
10. Cuando se presenten ausencias de servidores o contratistas por incapacidades, vacaciones, licencias no remuneradas o suspensión de contrato, será bloqueado el acceso a los equipos de cómputo asignados, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad, por lo que la persona indicada, que puede acceder al equipo es el supervisor del contrato. Es responsabilidad de la Dirección de Gestión Humana, la Dirección Jurídica y Contractual, la Dirección de Operaciones para el Fortalecimiento y los respectivos Supervisores de los contratos, notificar este evento con una solicitud a la Dirección de Tecnologías y Sistemas de la Información a través de la mesa de servicios.

d. Cableado Estructurado: En las sedes de la SDSCJ donde haya cableado estructurado, las tomas eléctricas ubicadas en las canaletas deberán ser usadas únicamente para la conexión de computadores, monitores o teléfonos IP. Los computadores deben ser conectados en las tomas naranjas y 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 realizar derivaciones, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

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

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

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

e. Sistemas de Información.

1. Cuando Solo podrán estar expuestas aquellas aplicaciones o sistemas de información que deban ser consultados por personas externas a la SDSCJ (ciudadanos y demás gente del común); las demás aplicaciones son de uso interno y su acceso desde fuera de la Entidad se debe realizar a través de conexiones seguras (VPNs) 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 Tecnología y Sistemas de Información de la SDSCJ.

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

3. 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.

f. 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, 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, Oficina Centro de Comando, Control, Comunicaciones y Computo-C4 y Cárcel Distrital de Varones y Anexo de Mujeres a otros recursos dispuestos en otras instalaciones o dependencias de la Entidad, deben cumplir los lineamientos definidos tanto en la presente política, así como los definidos en el Manual

de Seguridad de la Información de la SDSCJ. El supervisor del contrato debe realizar el seguimiento y control del cumplimiento de la presente política.

6.5 Controles de Acceso y Seguridad de la Información

6.5.1 Control De Acceso:

La SDSCJ a través de La Dirección de Recursos Físicos y Gestión Documental, deben implementar controles para que sólo el personal autorizado pueda acceder a las áreas de trabajo de la entidad, 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 SDSCJ con apoyo de La Dirección de Tecnología y Sistemas de la Información deben definir los controles, procedimientos e instructivos para proveer el acceso físico y lógico a los recursos físicos e informáticos, así como el perfilamiento de los usuarios autorizados para el cumplimiento de sus funciones, en las distintas sedes de la entidad.

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 Tecnología y Sistemas de la Información, las novedades de ingreso y retiro de los funcionarios y contratistas de la SDSCJ para gestionar los derechos de acceso a los sistemas de información, recursos y servicios tecnológicos de la Entidad.

La Dirección de Tecnología y Sistemas de la Información con apoyo de las dependencias de la SDSCJ debe implementar controles, procedimientos e instructivos para proveer el acceso físico y lógico de los recursos informáticos a usuarios autorizados para el cumplimiento de sus funciones. Estos deberán ser los siguientes:

6.5.1.1 Controles Criptográficos

La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información debe implementar lineamientos o directrices del uso adecuado de controles criptográficos, con el fin de establecer un lineamiento que permita servir como guía bajo las mejores prácticas.

Los propietarios de los activos de información deben identificar las necesidades de criptografía de información de acuerdo 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 la criptografía para proteger la confidencialidad, integridad y disponibilidad de la información que así lo requiera.

6.5.1.2 Seguridad Física y del Entorno

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

La SDSCJ 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. en consecuencia, todos los servidores, 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, éstos serán los responsables de la administración de los controles definidos para el cumplimiento del artículo, los directores o jefes de oficina realizarán el seguimiento al cumplimiento de los mismos y reportarán cualquier novedad que afecte la seguridad de la información a la Dirección de Tecnologías y Sistemas de la Información de la SDSCJ.

6.5.1.3 Seguridad de las Operaciones.

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

1. Implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en el Data Center de la entidad y su recuperación en caso de desastre.
2. Implementar controles para mitigar los riesgos inherentes a códigos maliciosos.
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 Tecnología 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 Negocio que propenda por la mitigación de los riesgos sobre la confidencialidad, integridad y disponibilidad de la información en los casos de incidentes seguridad.

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

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

6.5.1.4 Seguridad de las Comunicaciones.

La SDSCJ a través de la Dirección de Tecnología y Sistemas de la Información o en quien delegue,

1. Establecerá los Acuerdos de Niveles de Servicios-ANS requeridos para que el proveedor de servicios de tecnologías de Información-TI garantice la disponibilidad de las redes WAN e Internet.
2. Implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos de la entidad propendiendo por la integridad, confidencialidad y disponibilidad de la información.
3. Implementar los mecanismos necesarios para proteger la información que se transporta a través de las redes de datos, propendiendo por la integridad, confidencialidad y disponibilidad de esta, en los casos donde la operación es administrada por un operador tecnológico.

6.5.1.5 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, será la única área autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de herramientas, aplicaciones y sistemas de información, velando por que incorporen las buenas prácticas para el desarrollo seguro de software y estándares de seguridad informática y la aplicación de los estándares de desarrollo seguro. En los casos donde otras dependencias requieran adquirir aplicaciones, el proceso debe llevar un visto bueno de la Dirección de Tecnología 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, ajustes a los perfiles de usuario, de tal manera que ningún usuario pueda adelantar instalaciones y la desinstalación correspondiente del software que no esté avalado por la Entidad, so pena de solicitar los procesos disciplinarios correspondientes para los usuarios que entran a generar dichas prácticas.

La Dirección de Tecnología y Sistemas de la Información debe implementar un repositorio de los instaladores probados y avalados para ejecutar las instalaciones necesarias y un listado restringido con las licencias correspondientes para cada programa, con todos los controles de seguridad que puede necesitar dicho repositorio.

6.5.1.6 Controles en las Relaciones con los Proveedores.

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

6.5.1.7 Seguridad en la Gestión de Continuidad de Negocio.

La SDSCJ deberá disponer de un Plan de Continuidad de Negocio y a través de la Dirección de Tecnología y Sistemas de la Información, 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.

6.5.1.8 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, mensualmente 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.

6.6 Método Definido Para Operar

La SDSCJ establece que la presente Política de Seguridad y Privacidad de la Información operará por medio del “*Manual de Seguridad y Privacidad de La Información*” en el cual

se encuentran los lineamientos detallados para el cumplimiento, implementación y monitoreo del Sistema de Gestión de Seguridad de la Información.

6.7 Administración de la Política y Procedimiento de Cambio

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

6.8 Propiedad Intelectual

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

La Dirección Jurídica y Contractual, la Dirección de Gestión Humana y la Dirección de operaciones 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 Dirección de Tecnología y Sistemas de la Información debe adelantar acciones para el guardado de archivos dentro de los equipos de la entidad y en ese sentido, generar procesos para el borrado de archivos que no deban estar en los computadores, tales como archivos de video (mp4, avi, flv, etc.), archivos de audio (3gp, mp3, etc.), fotografías, etc. Hay que tener en cuenta que ciertos usuarios deben estar dentro de las excepciones, toda vez que el cumplimiento de sus funciones está orientado a la producción de dicho material, caso en el cual se debe documentar y adelantar las solicitudes correspondientes para poner en firme dicha excepción.

6.9 Administración del Riesgo Para la Seguridad de la Información.

La información de la SDSCJ se debe proteger con base en su valor y en el riesgo en que se pueda ver comprometida. Por lo tanto, se debe realizar por lo menos una vez cada año, un análisis respecto al impacto en seguridad de la información, para determinar o actualizar el valor relativo de la información, el nivel de riesgo a que está expuesta y el respectivo responsable, actualizando la matriz de activos de información.

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

Todos los líderes de procesos de la SDSCJ, acompañados por el Oficial de Seguridad de la Información 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 de acuerdo con lo definido en la Política de Administración de Riesgos de la entidad. El reporte de las evidencias de los controles definidos para la mitigación de los riesgos se realizará de acuerdo como lo establezca la Oficina Asesora de Planeación de la entidad.

6.10 Concienciación en Seguridad de la Información.

La SDSCJ debe contar con un programa de concientización y/o capacitación (según sea el caso) en seguridad de la información permanente, que permita garantizar que los funcionarios, contratistas, usuarios, terceros u operadores tecnológicos que accedan a la información de la entidad, estén informados acerca de sus responsabilidades en Seguridad de la Información y de las continuas amenazas que ponen en riesgo la información de la entidad. Así mismo, se debe adelantar una capacitación y/o concientización sobre Seguridad Digital para toda la entidad por lo menos dos veces por año, buscando estrategias para que la mayor cantidad de personas sean permeadas con este tipo de información.

Los funcionarios, contratistas, usuarios, terceros u operadores tecnológicos deben conocer y aplicar los procedimientos de seguridad de la información de la SDSCJ desde el mismo momento de ingresar a la Entidad.

6.11 Cumplimiento

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

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

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

6.12 Perspectivas Para Tener en Cuenta

Contemplando lo consignado en el Reporte de Ciberseguridad: Riesgos, Avance y el Camino a seguir en América Latina y el Caribe, publicado por el Banco Interamericano de Desarrollo – BID y la Organización de Estados Americanos –OEA en octubre de 2020, la SDSCJ fijará nuevas perspectivas de trabajo, las cuales se deberán planear y ejecutar a partir de las consideraciones definidas por el Gobierno Nacional. Gobierno Distrital y por los estándares internacionales. En ese sentido, los aspectos sobre los que se debe trabajar son:

1. **Resiliencia**: Permitir a la Entidad, lograr los niveles de resiliencia definidos a nivel internacional a partir de la creación de capacidad, entendiéndose por resiliencia como la capacidad para sobreponerse a una eventualidad asociada con seguridad de la información).

2. **Colaboración Internacional / Nacional en Temas de Ciberseguridad y Seguridad de la Información**: Adelantar agendas de trabajo para crear redes de cooperación entre las entidades distritales, nacionales e internacionales, propendiendo por generar masa crítica a nivel de seguridad y poder de esta manera, hacer frente a las amenazas, consolidar estrategias de defensa e incrementar el pie de fuerza y de defensa a partir de las capacitaciones y el seguimiento de políticas referentes al tema.

3. **Cooperación publico/privada**: Definir esquemas de cooperación entre las entidades públicas y la empresa privada, con el fin de poder fortalecer los temas de seguridad de información y ciberseguridad.

4. **Directrices para uso de servicios de nube**: Solicitar al gobierno nacional y distrital las directrices para uso de servicios en nube.

5. **Seguridad de información en Internet de las Cosas (IoT por sus siglas en ingles Internet Of Things):** Definir acciones referentes al uso, mejores prácticas y aseguramiento de dispositivos IoT, con el fin de poder tener una perspectiva más precisa de su utilización, adopción y aseguramiento de infraestructura IoT.

Elaboró: Diego Mauricio Usme Gonzalez – Contratista SDSCJ

Revisó: Jorge Eliecer Velásquez Perilla – Contratista SDSCJ.

Rafael Humberto López Saavedra – Contratista SDSCJ.

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