MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2023

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

CONTENIDO

1. OBJETIVO

Establecer los lineamientos y/o directrices para el cumplimiento de la Política de Seguridad y Privacidad de la Información, la cual debe ser conocida y cumplida por todos los funcionarios, contratistas y terceros que tengan relación con la Secretaría Distrital de Seguridad, Convivencia y Justicia en pro de velar por los principios de confidencialidad, disponibilidad e integridad de la Información, enmarcado en el cumplimiento legal y normativo aplicable.

2. ALCANCE

El alcance de este documento es establecer los lineamientos y/o directrices para el cumplimiento de la Política de Seguridad y Privacidad de la Información. Este alcance abarca a todos los funcionarios, contratistas y terceros que tengan relación laboral con la Secretaría Distrital de Seguridad Convivencia y Justicia en adelante la SDSCJ, con el propósito de garantizar el cumplimiento de los principios de confidencialidad, disponibilidad e integridad de la Información.

Este alcance incluye la aplicación de medidas de seguridad y controles que se ajusten a los requisitos legales y normativos aplicables. Se debe garantizar el cumplimiento de las leyes y regulaciones pertinentes relacionadas con la protección de la Información.

Los lineamientos y/o directrices establecidas en este alcance deben ser seguidos en todas las actividades relacionadas con la gestión y tratamiento de la Información dentro de la Entidad. Esto incluye, pero no se limita a, la recolección, almacenamiento, procesamiento, transmisión y disposición final de la Información.

Es responsabilidad de cada funcionario, contratista y/o tercero cumplir con los lineamientos y/o directrices establecidas en este manual. El incumplimiento de estos lineamientos y/o directrices puede dar lugar a acciones disciplinarias según lo establecido en las políticas y procedimientos internos.

Este alcance se mantendrá vigente hasta que se realicen modificaciones en la Política de Seguridad y Privacidad de la Información que requieran la actualización de los lineamientos y/o directrices establecidas. En tal caso, se llevará a cabo una revisión y actualización correspondiente.

3. AMBITO DE APLICACIÓN

El ámbito de aplicación de esta manual abarca todos los procesos que integran la Entidad, así como para todos los funcionarios, contratistas y terceros que interactúen y/o tengan responsabilidad sobre la información dentro de la organización.

Este ámbito se extiende a todas las formas de Información, independientemente de su formato o medio de almacenamiento, incluyendo, pero no limitado a documentos físicos, archivos digitales, bases de datos, comunicaciones electrónicas y cualquier otro medio en el cual la Información sea generada, transmitida, procesada o almacenada.

Se aplica a todos los sistemas de información e infraestructura tecnológica utilizados por la Entidad, incluyendo redes de comunicaciones, servidores, equipos informáticos, dispositivos móviles y cualquier otro componente tecnológico que almacene o procese Información.

Este ámbito de aplicación también se extiende a las relaciones con terceros, tales como proveedores, contratistas, socios comerciales y cualquier entidad externa que tenga acceso a la Información de la Entidad. De cualquier forma, se espera que dichos terceros cumplan con los lineamientos y/o directrices establecidas en este alcance en lo que respecta a la gestión y protección de la Información.

Cabe destacar que este ámbito se rige por las leyes y regulaciones aplicables en materia de seguridad y privacidad de la Información a nivel nacional y distrital, así como por las políticas y procedimientos internos establecidos por la Entidad.

4. NORMATIVIDAD ASOCIADA

a. **Constitución Política de Colombia de 1991 – Artículo 15:** Se establece que “todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el estado respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en los archivos de entidades públicas y privadas”.

b. **Ley 1712 De 2014:** Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

c. **Ley 1581 de 2012:** Por la cual se dictan disposiciones generales para la protección de datos personales tiene como objeto “(…) desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales” y que dicta, además de las disposiciones generales para la protección de datos personales.

d. **Ley 1273 de 2009**: Por medio de la cual se modifica el código penal, se crea un nuevo bien jurídico tutelado denominado "De la protección de la información y los datos" y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

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

f. **Decreto 510 de 2019:** “Por el cual se reglamenta el Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 y se dictan otras disposiciones”, en el Artículo 12°.- Coordinación con entidades, nuevos sistemas o plataformas se dispone el numeral número 5, “ … Aplicar los controles necesarios que permitan la protección, privacidad y seguridad de la información de las plataformas tecnológicas, sistemas de información y demás componentes que hagan parte del C4…”, además, en el Artículo 24 dispone lo siguiente: “La información que se suministre a través del Sistema Centro de Comando, Control, Comunicaciones y Cómputo - C4 se considera estratégica para la gobernabilidad, seguridad y convivencia del Distrito Capital por involucrar tanto, aspectos de seguridad ciudadana y elementos materiales probatorios, como del derecho fundamental a la intimidad de los usuarios que se encuentra amparada por reserva constitucional y legal ”.

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

h. **Decreto 612 de 2018:** Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado. "2.2.22.3.14. Integración de los planes institucionales y estratégicos al Plan de Acción. Las entidades del Estado, de acuerdo con el ámbito de aplicación del Modelo Integrado de Planeación y Gestión, al Plan de Acción de que trata el artículo 74 de la Ley 1474 de 2011, deberán integrar los planes institucionales y estratégicos que se relacionan a continuación y publicarlo, en su respectiva página web, a más tardar el 31 de enero de cada año".

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

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

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

l. **Resolución 0025 del 29 de enero de 2021:** De la Secretaría Distrital de Seguridad, Convivencia y Justicia. Por medio de la cual se adopta la nueva Política de Seguridad y Privacidad de la información.

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

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

o. **Conpes 3975 de 2019:** Mediante el cual se establece la Política Nacional para la Transformación Digital e Inteligencia Artificial.

p. **Conpes 3854 de 2016**: Mediante el cual se establecen los lineamientos y directrices de seguridad digital y se tienen en cuenta componentes como la educación, la regulación, la cooperación, la investigación, el desarrollo y la innovación.

5. DOCUMENTOS ASOCIADOS

- C-GT-1 - Caracterización proceso de Gestión de Tecnologías y Sistemas de la Información
- PO-GT-1 - Política de Seguridad y Privacidad de la Información.
- PD-GT-6 - Procedimiento Gestión de Incidentes o Problemas
- PL-GT-1 - Plan de Seguridad y Privacidad de la Información.
- PL-GT-3 - Plan de tratamiento de riesgos de seguridad y privacidad de la información.
- F-GT-953 - Matriz de roles y responsabilidades seguridad de la Información.

6. GLOSARIO

El siguiente glosario describe y define una lista de palabras y expresiones de los términos más relevantes sobre seguridad de la información que se usan dentro del documento, así:

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

Acceso Restringido: Es aquel control que busca restringir de manera parcial o completa el acceso a un activo o sujeto de información.

Acceso No Autorizado: Es aquel control que busca no otorgar permisos de acceso a un activo de información de manera total.

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: (Según el Modelo de Seguridad y Privacidad de la Información MSPI): 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.

- **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 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 (MinTIC basado en ISO/IEC 27000): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según (MinTIC basado en ISO/IEC 27000): Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo.

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 Sistema de Gestión de Seguridad de Información 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.

BIA: Análisis de impacto del negocio por sus siglas en inglés (**Business Impact Analysis**), documento que determina los activos críticos de la Entidad.

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

Código Malicioso: Es todo tipo de software (incluyendo scripts y macros) diseñado para interrumpir las operaciones, reunir información sin autorización, acceder sin autorización a los recursos del sistema, y posiblemente otra conducta abusiva o perjudicial sobre el sistema.

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: Aquel que permite el restablecimiento de la actividad, después de ser detectado un evento no deseable; también permiten la modificación de las acciones que propiciaron su ocurrencia.

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

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

Control preventivo: Es aquel 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.

CVE: Vulnerabilidades y exposiciones comunes por sus siglas en inglés **(Common Vulnerabilities and Exposures):** Entidad que agrupa todas las vulnerabilidades técnicas existentes.

CVSS: Sistema de puntuación de vulnerabilidad común por sus siglas en inglés **(Common Vulnerabilities Score System):** Puntaje de criticidad de cada una de las vulnerabilidades técnicas.

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 ejecutada por personas, grupos, organizaciones con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

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

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

DMZ Zona desmilitarizada por sus siglas en inglés **(Demilitarized Zona):** Zona desmilitarizada que consiste en exponer servicios hacia internet de manera segura.

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.

Evaluación de riesgos: Según la norma ISO/IEC 31000:2018 Gestión del Riesgo, es el proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

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

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

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

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

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

Incidente de seguridad de la información: Es la violación o amenaza inminente a la Política de Seguridad de la Información implícita o explícita. Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del Entidad 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 red o faciliten información con clasificación confidencial o superior.

INM: Instituto Nacional de Metrología: busca garantizar la trazabilidad de las mediciones, el cumplimiento de estándares y facilitar el cumplimiento de parámetros de calidad de los productos que se fabrican o se comercializan en el país.

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, CD, DVD, unidades de almacenamiento USB, diseñados para ser extraídas de la computadora sin tener que apagarla.

NAT Traducción de direcciones de red por sus siglas en inglés **(Network Address Translation):** Mecanismo de traslado de direcciones IP.

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

OWASP Proyecto de seguridad de aplicaciones web abiertas por sus siglas en inglés (**Open Web Application Security Project):** Fundación que trabaja para mejorar la seguridad del software, donde los desarrolladores y tecnólogos protegen la red.

PAT Traducción de dirección de puerto por sus siglas en inglés **(Port Address Translation):** Traslado de direcciones a nivel de puertos de comunicaciones.

Plan de tratamiento de riesgos: 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 Alta 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.

RFC: Petición de cambios por sus siglas en inglés **(Request For Change):** Requisición formal de cambio en espera de ser implementado.

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

RollBack: Por su traducción en inglés: **(Reversión):** en tecnología es toda aquella reversión de una operación a un estado previo después de un cambio.

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.

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

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.

VPN: Red Privada Virtual por sus siglas en inglés **(Virtual Private network):** establece una conexión protegida al utilizar redes públicas, enmascarando su identidad en línea y cifrando su tráfico en la red.

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.

WAF: Cortafuegos de aplicaciones web por sus siglas en inglés **(Web Application Firewall):** Firewall de aplicaciones

7. CONTROLES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION

Los controles de referencia definidos a continuación corresponden a la Norma Técnica Colombiana NTC-ISO/IEC 27001:2013 – Sistema de Gestión de la Seguridad de la información,

establecidos la Entidad con el fin de preservar la confidencialidad, integridad y disponibilidad de los activos de información.

7.1 POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Es responsabilidad de la Alta Dirección, funcionarios, contratistas y proveedores, dar estricto cumplimiento a la Política de Seguridad y Privacidad de la Información y lo descrito en este Manual.

7.1.1 Políticas para la seguridad de la información

La SDSCJ a través de la Resolución 0025 del 29 enero de 2021, adopta la Política de Seguridad y Privacidad de la Información; la cual establece “los lineamientos requeridos para planificar, hacer y verificar un modelo confiable y flexible que defina el marco básico que guiará la implantación de cualquier directriz, proceso, procedimiento, estándar y/o acción, relacionados con la gestión de la seguridad y privacidad de la información – MSPI”, asegurando los principios de confidencialidad, integridad y disponibilidad de la información, de acuerdo con los requisitos legales y normativos en que se ampara el cumplimiento misional de la Entidad.

7.1.2 Revisión de las Políticas para la seguridad de la información

El Comité Institucional de Gestión y Desempeño en el marco del Modelo Integrado de Planeación y Gestión, liderará y facilitará la implementación del SGSI, como habilitador transversal de la Política de Gobierno Digital con apoyo de la Dirección de Tecnologías y Sistemas de la Información de la Entidad.

7.2 ORGANIZACION DE LA SEGURIDAD DE LA INFORMACIÓN

La seguridad de la información es el conjunto de medidas y técnicas utilizadas para controlar y salvaguardar la Información que se manejan dentro de la Entidad, estableciendo los lineamientos específicos que se deben implementar en el entorno general de seguridad de la información a nivel interno y externo de la SDSCJ.

La Política de Seguridad y Privacidad de la Información aplica para todos los funcionarios, contratistas, proveedores y operadores tecnológicos, que tengan vínculo laboral o contractual con la SDSCJ.

7.2.1 Roles y Responsabilidades para la Seguridad de la Información

La SDSCJ, en el marco del Sistema de Gestión de Seguridad de la Información (SGSI), define y asigna roles y responsabilidades de seguridad de la información dentro de la Entidad, establecido en el formato F-GT-953 “Matriz de Roles y Responsabilidades Seguridad de la Información”, facilitando el normal desarrollo de las actividades tecnológicas de la misma.

7.2.2 Separación de Deberes

En la SDSCJ, las personas que tengan acceso a la infraestructura y soluciones tecnológicas, lo podrán realizar de acuerdo con los roles y funciones definidos sobre estos para la ejecución de sus actividades laborales, esto con el fin de reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

Para lo cual, la Dirección de Tecnologías y Sistemas de la Información revisará y actualizará anualmente la matriz de roles y usuarios, aplicaciones, directorio activo, sistemas operativos y base de datos.

7.2.3 Contacto con las autoridades

La SDSCJ establece contactos con entidades competentes, con el objetivo de coordinar e intercambiar información y la gestión de incidentes de seguridad de la información.

Esto a través de la Dirección de Tecnologías y Sistemas de la Información por medio del profesional de seguridad de la información o a quien se delegue, para la atención de incidentes para la atención de incidentes de acuerdo con el (PD-GT-6) Procedimiento Gestión de Incidentes o Problemas o aquellas actividades que afecten o pongan en riesgo la seguridad de la información de la Entidad y/o dar respuesta a requerimientos de información:

CSIRT GOBIERNO	Mesa de servicio CSIRT Gobierno	018000910742 csirtgob@mintic.gov.co
COLCERT Grupo de Respuesta a Emergencias Cibernéticas en Colombia	Respuesta a Emergencias Cibernéticas de Colombia	295 98 97 contacto@colcert.gov.co www.colcert.gov.co/
CAI VIRTUAL Centro Cibernético Policial	Sistema Nacional de Denuncia Virtual Caí Virtual Reporte Incidentes Informáticos Análisis de Malware Transferencia no consentida de activos Ciberseguridad Observatorio Cibercrimen	Línea 112 018000 910112 www.policia.gov.co/ www.caivirtual.policia.gov.co/ www.adenunciar.policia.gov.co/adenunciar/Login.aspx
MINTIC Ministerio de Tecnologías de la Información y las Comunicaciones	Línea anticorrupción Denuncias por actos de Corrupción.	018000912667 soytransparente@mintic.gov.co www.mintic.gov.co
Alta Consejería para las TIC – Gobierno Digital.	Recomendaciones, conceptos, fortalecimiento técnico y apoyo en decisiones de cumplimiento en materia de seguridad y privacidad de la información y ciberseguridad	Teléfono: 3813000 ext. 2001 altaconsejeriadetic@alcaldiabogota.gov.co https://tic.bogota.gov.co/
Fiscalía General de la Nación	Denuncia Virtual	Línea 122 01 8000 9197 48 www.fiscalia.gov.co
DIJIN Dirección de Investigación Criminal e INTERPOL	Delitos Cibernéticos	Línea: 157 018000 910112 www.policia.gov.co/dijin
Gaula Dirección Antisecuestro y Antiextorsión	Antisecuestro y Antiextorsión	Línea: 165 www.policia.gov.co/direcciones/antisecuestro
Bomberos	Emergencia por Incendio	Línea: 119 www.bomberosbogota.gov.co

Cruz Roja	Incidentes Laborales	Línea: 132 www.cruzrojacolombiana.org
Centro Toxicológico	Incidentes laborales	Linea:136
Defensa Civil	Siniestros ambientales	Línea: 144 www.defensacivil.gov.co

7.2.4 Contacto con los grupos de interés especial

El Profesional de Seguridad de la Información, será el encargado de tener contacto con los Grupos de Interés cuando se presenten incidentes que pongan en riesgo la Seguridad de la Información. Así mismo, el encargado de realizar transferencia de conocimientos a las áreas de Entidad, así como realizar el envío de consejos de seguridad en temas de información y tecnología.

ACIS – Asociación Colombiana de Ingenieros de Sistemas	https://acis.org.co/
CISCO (Security consulting)	https://www.cisco.com/c/es_co/index.html
DATASECURE S.A.S	www.datasecure.com.co
DIGIWARE	www.digiware.net/
IBM (Seguridad y Privacidad)	www.ibm.com/co
ISS - Sistemas de seguridad información	https://iss.com.co/
ITECH - Ciberseguridad Y Protección Datos	https://www.itechsas.com/home/
Red Colombia – Información Nacional	https://redcolombia.com.co/
CEA Colombia	https://www.ceacolombia.com/
Antifraude	https://www.antifraude.co/

7.2.5 Seguridad de la Información en la Gestión de Proyectos

La seguridad de la información hace parte de la gestión y administración de proyectos en la SDSCJ, en aras de proveerlos de las seguridades adecuadas, y liderar los de Seguridad de la Información, los cuales cumplen con los lineamientos aplicables que se encuentran en el normograma de la SDSCJ, garantizando la confidencialidad, integridad y disponibilidad de la información.

En la administración y gestión de proyectos de la Entidad, se identifican los riesgos operativos, técnicos, documentales y jurídicos del proyecto que se deben incluir en el formato F-GT-936 “Reporte de ejecución y control: registro de ejecución” y de acuerdo con lo establecido en el procedimiento interno PD-GT-4 “Gestión de proyectos de TI”

Todas las recomendaciones de seguridad de la información deberán ser tomadas en cuenta en todas las etapas del proyecto independiente de la tipología de este. Para lo cual, se debe efectuar una evaluación de riesgos, basada en la seguridad de la información, al inicio de cualquier proyecto para identificar amenazas, vulnerabilidades y riesgos asociados al proyecto.

7.2.6 Política para Dispositivos Móviles

La SDSCJ en el marco de la Política de Seguridad y Privacidad de la Información, definirá la política para dispositivos móviles que permita gestionar de manera eficaz los riesgos ocasionados por la ejecución de actividades laborales a través de dispositivos móviles.

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.

La Dirección de Tecnologías y Sistemas de la Información, en referencia a dispositivos móviles establece las siguientes acciones, así:

a. Monitorear los dispositivos móviles de propiedad de la Entidad asignados a los funcionarios o contratistas que sean utilizados para teletrabajo, trabajo en casa o trabajo remoto con el fin de detectar la instalación de software y/o programas no autorizados y que puedan con llevar de perdida de información.
b. Disponer de control de acceso y segregación de red para los dispositivos móviles que se conecten a la red de la SDSCJ.
c. Disponer de controles de acceso ya sea por contraseña, patrón o huella para los dispositivos móviles de propiedad de la Entidad o en calidad de arriendo, Si el dispositivo móvil o equipo portátil es propiedad del funcionario o contratista que maneje información de la Entidad, este deberá mantener un control de acceso por contraseña, un software antivirus actualizado y conservar los protocolos de seguridad establecidos en el presente manual, en aras de salvaguardar la confidencialidad de la información.
d. Realizar campañas de concienciación sobre el uso adecuado de dispositivos móviles y acceso seguro de las redes Wifi, así como uso adecuado de los servicios VPN de la Entidad, entre otros.
e. Los funcionarios, o contratistas del centro de Comando, Control, Comunicaciones y Computo – C4 y de la Cárcel Distrital de Varones y Anexo de Mujeres, por la criticidad y/o sensibilidad de la información que allí se maneja, tendrán áreas con acceso restringido para dispositivos móviles en el uso, manejo o tomas de material fotográfico y/o video, esto con el fin de asegurar la confidencialidad de la información, garantizar el debido proceso, la cadena de custodia, proteger los datos personales y el uso indebido de información. El uso, procesamiento, descarga, entrega y manejo de grabaciones de audio o video en cualquiera de sus formatos deben contar con autorización del director o jefe de la dependencia o a través de requerimiento por orden judicial pertinente

Es responsabilidad de los funcionarios y contratistas que tiene asignado dispositivos móviles de propiedad o en arriendo de la Entidad:

a. Cuidar y proteger la información física y digital que se maneje a través de dispositivos móviles personales o asignados por la Entidad, esto con el fin de evitar la pérdida, acceso o divulgación de información no autorizada.
b. Reportar a la Dirección de Tecnologías y Sistemas de la Información y a la Dirección de Recursos Físicos y Gestión Documental, el daño, pérdida, robo, o cualquier incidente ocasionado con estos elementos físicos.

c. Hacer buen uso de la información almacenada con base en sus funciones u obligaciones contractuales y de acuerdo con la criticidad de la información que maneja.

Ningún funcionario o contratista le está permitido, salvo autorización expresa de la Dirección de Tecnologías y Sistemas de la Información de:

a. Realizar descarga de contenidos sospechosos o que procedan de fuentes no verificables (tanto a través de correo, como de navegación, dispositivos de almacenamiento), en los dispositivos móviles y equipos portátiles de la Entidad.
b. Cambiar las configuraciones instaladas, desinstalar software, formatear o restaurar de fábrica el equipo asignado, el personal de mesa de servicios son los autorizados a realizar cambios y aplicar las actualizaciones requeridas por los equipos de la Entidad.

7.2.7 Teletrabajo

La SDSCJ definirá la política para implementar medidas de protección, de la información a la que se accede, produce, procesa y almacena en los lugares o sitios de trabajo de acuerdo con los siguientes modelos, a saber:

a. Teletrabajo, modalidad de trabajo no presencial, donde se establece un lugar diferente para la realización de actividades del empleado y de acuerdo con los parámetros establecidos con el empleador, se establece su asistencia a la Entidad, regulado por la Ley 1221 de 2008 “Normas para promover y regular el Teletrabajo y se dictan otras disposiciones” y la resolución 365 de 2018 “Por la cual se implementa el modelo de teletrabajo” de la Entidad.
b. Trabajo en casa, modalidad de trabajo no presencial que se establece de forma transitoria por ocasiones especiales en el lugar de residencia del empleado, establecido en la ley 2088 de 2021 “Por el cual se regula el trabajo en casa y se dictan otras disposiciones”.
   Trabajo remoto, actividad laboral permanente que se desarrolla de forma remota mediante el uso de tecnologías de la información, el empleador y el trabajador no interactúan físicamente, el trabajador solo visitara las instalaciones del empleador, en casos específicos que sean necesario, establecido en la Ley 2101 de 2021 “se reduce la jornada laboral semanal de manera gradual, sin disminuir el salario de los trabajadores y se dictan otras disposiciones”.

La Dirección de Tecnologías y Sistemas de la Información, con el propósito de facilitar el teletrabajo, dispuso el siguiente servicio:

a. Acceso remoto desde redes externas sobre una conexión protegida y/o red privada virtual (VPN - Virtual Prívate Network) hacia la red de área local de la Entidad, estableciendo entornos seguros de trabajo a distancia o teletrabajo, previa solicitud del líder de proceso y autorización de la Dirección de Tecnologías y Sistemas de la Información. De conformidad con el procedimiento interno descrito en el documento PD-GT-1 “Procedimiento Gestión de Requerimiento de TI”, así:

   - Generar solicitud de servicios de tecnología ante la mesa de servicio por los canales de atención previstos para tal fin.

- Anexar formato F-GT-285 “Solicitud Administración de Usuarios” debidamente diligenciado y firmado por el usuario solicitante y el director o jefe de la Oficina solicitante.
- El personal de mesa de servicios realiza los trámites internos correspondientes para la viabilidad y creación de los permisos establecidos asociados al usuario de dominio y notifica por correo electrónico al usuario.
- El usuario toma contacto con la mesa de servicio para la instalación del software y/o aplicaciones requeridas para el uso y acceso a través de red privada virtual VPN.
- El ingreso a la red de la Entidad se realiza a través del usuario y contraseña que se le asigna al funcionario o contratista para el equipo de cómputo, servicios tecnológicos, sistemas de información y servicios ciudadanos digitales.
- El acceso a los equipos de cómputo y/o servidores de la Entidad desde fuera de sus instalaciones sólo será permitido a las personas autorizadas por la Dirección de Tecnologías y Sistemas de la Información previo aval del jefe inmediato.
- Es importante mencionar que, los funcionarios y contratistas que utilicen dispositivos móviles, portátiles, entre otros, en ejecución de sus actividades laborales en modalidad de teletrabajo, serán los responsables de propender la confidencialidad, integridad y disponibilidad de la información.

7.3 SEGURIDAD DE LOS RECURSOS HUMANOS.

La seguridad de los recursos humanos en el trabajo es el conjunto de actividades para tener en cuenta en la prevención de riesgos laborales y cuyo fin es la aplicación de medidas, así como el desarrollo de acciones necesarias para la prevención de riesgos derivados del trabajo.

La seguridad del recurso humano contempla cada una de las etapas provistas en la selección de funcionarios y contratistas, verificación de datos y documentos, ejecución de actividades a desarrollar y la terminación y/o cambio de roles de los usuarios, lo cual, se debe realizar de acuerdo con lo definido en los procedimientos del proceso Gestión Humana y a los de seguridad y privacidad de la información de la Entidad.

Se busca que los funcionarios y contratistas comprendan e interioricen las responsabilidades, planes, procedimientos, guías en materia de seguridad y privacidad de la información que se han establecido en la Entidad.

7.3.1 Selección

En la Entidad, de acuerdo con los procedimientos definidos por la Dirección de Gestión Humana se establecen los requisitos, trámites de selección y vinculación de servidores públicos en la SDSCJ conforme con el procedimiento interno PD-GH-12 “Selección y Vinculación de Personal”, en base a los requerimientos de ley establecidos para tal fin.

La Dirección de Gestión Jurídica y Contractual establece los requisitos, trámites de selección y vinculación de contratistas en la SDSCJ Justicia de acuerdo con lo establecido en el documento MA-GCT-01 “Manual de Contratación, Supervisión e Interventoría” y el procedimiento interno PD-JC-11 “Legalización y Perfeccionamiento de los Contratos” y en base a los requerimientos de ley establecidos para tal fin.

7.3.2 Términos y Condiciones del Empleo.

Los funcionarios o contratistas vinculados a la Entidad deben acatar y cumplir lo requerido en la Ley 1581 de 2012 "*Por la cual se dictan disposiciones generales para la protección de datos personales*", Ley 1712 de 2014 "*Ley de Transparencia y acceso a la Información Pública*" así como lo exigido en la PO-GT-01 "Política de Seguridad y Privacidad de la Información", MA-GT-01 "Manual De Seguridad y Privacidad de La Información" de la Entidad.

Por otra parte, los funcionarios deben diligenciar el formato F-GH-807 "Compromiso de Confidencialidad y no Divulgación de la Información" al inició del empleo y demás normatividad relacionada con seguridad de la información aplicable a la Entidad

7.3.3 Responsabilidades de la Dirección

En la Entidad, la Dirección de Tecnologías y Sistemas de la Información con el apoyo de la mesa Técnica de Seguridad Digital, son las encargadas de hacer seguimiento y control de las aplicación de la seguridad de la información, de acuerdo con las políticas y procedimientos definidos, lo cual debe ser de estricto cumplimiento por parte de los funcionarios, contratistas y terceros, esto durante la realización de las actividades que hacen parte de la creación, administración, procesamiento, manejo, verificación, cadena de custodia y consulta de información en la operación de la Entidad.

Las responsabilidades de la Dirección se encuentran descritas en el formato F-GT-953 "Matriz de Roles y Responsabilidades Seguridad de la Información".

7.3.4 Toma de Conciencia, Educación y Formación en la Seguridad de la Información

En procura de garantizar los principios de confidencialidad, integridad y disponibilidad de la información de la Entidad, por parte de la DTSI se realizan actividades de divulgación, sensibilización e interiorización sobre temas de seguridad de la información en donde se da a conocer el Manual y la Política de Seguridad y Privacidad de la Información y demás temas de interés.

Las formas de difusión de la información para los colaboradores de la Entidad, se realiza de acuerdo con los parámetros que se establecen en el procedimiento interno PD-GT-13 "Procedimiento de Uso y Apropiación".

La DTSI se articulará con la Dirección de Gestión humana en lo que respecta a la gestión del plan institucional de capacitación (PIC) de cada vigencia, en lo que respecta a seguridad de la información, aportando en la elaboración y construcción del diagnóstico de necesidades de capacitación de la Entidad y en la ejecución de las actividades formativas relacionadas con los ejes estratégicos [1] según corresponda:

- Gestión del conocimiento y la innovación.
- Creación de valor público.

[1] La priorización temática del PIC que se ofrece en las entidades públicas se construye sobre la base de las capacidades y conocimientos que se incorporan en estos ejes temáticos. Lo anterior conforme lo definido en el Plan Nacional de Formación y Capacitación 2020 - 2030 - Dirección de Empleo Público - DAFP

- Transformación digital.
- Probidad y ética de lo público.

7.3.5 Proceso Disciplinario

En la Entidad la Oficina de Control interno Disciplinario, ha generado lineamientos en el marco del Código Único Disciplinario, los cuales han sido comunicados a los funcionarios y contratistas. En caso de incurrir en violaciones a la Seguridad y Privacidad de la Información, le acarreará sanciones disciplinarias o legales según corresponda.

7.3.6 Terminación o Cambio de Responsabilidades de Empleo

En referencia a la Terminación o Cambio de Responsabilidades de Empleos en la Entidad se establecen las siguientes actividades:

a. La Dirección de Gestión Humana será la encargada de notificar a través de los medios autorizados para tal fin (Correo electrónico institucional o herramienta de gestión, o ticket mesa de servicio), a la Dirección de Tecnologías y Sistemas de la Información, todas las novedades de los funcionarios como vacaciones, incapacidades médicas, suspensiones, términos laborales, para que se bloquee o suspendan los privilegios de acceso a las diferentes soluciones tecnológicas de la Entidad, según sea el caso.

b. Los supervisores de contratos se encargan de notificar a través de los medios autorizados para tal fin (Correo electrónico institucional o herramienta de gestión, o ticket mesa de servicio) a la mesa de servicio (soporte.tecnico@scj.gov.co) de DTSI, la terminación del vínculo contractual para dar trámite a la cancelación de usuarios y privilegios en las soluciones tecnológicas de la Entidad.

c. Para los funcionarios o contratistas con cambio de roles dentro de la Entidad, el acceso a los activos de información se hará de acuerdo con el nuevo rol asignado, los activos que no correspondan deben permanecen en su respectiva dependencia y serán entregados al jefe directo o supervisor del contrato según corresponda para nueva disposición.

d. Todos los funcionarios o contratistas al finalizar la relación de servicios con la Entidad harán entrega de las credenciales, tarjeta de proximidad, carnet, y entrega de la información entre otros, asignados para el desarrollo de las funciones u obligaciones a la Dirección de Gestión Humana , o Dirección de Recursos Físicos y Gestión Documental según corresponda, realizando todos los trámites requeridos para obtener el paz y salvo con la Entidad de acuerdo a los procedimientos PD-GH-18 “Retiro del servicio de los servidores públicos” y en el caso de los contratistas deben diligenciar y tramitar F-JCT-1144 – “Control De Retiro Para Contratistas De Prestación De Servicios Personales ” definidos para tal fin.

7.4 GESTIÓN DE ACTIVOS.

La identificación, clasificación, actualización y gestión del inventario de activos de la Entidad, permite tener control oportuno sobre su utilización, roles asignados y responsabilidades asociadas a la información de los activos identificados, determinando así los controles de seguridad requeridos y las dependencias responsables de su seguimiento y manejo adecuado. Es importante denotar que, cada activo debe tener un responsable que cumpla con los niveles

de protección y uso apropiado de acuerdo con sus características, clasificación, etiquetado y manipulado de la información.

7.4.1 Inventario de Activos

La Entidad cuenta con el Inventario de activos de información, y con el fin de mantenerlos actualizados se establecen las siguientes actividades:

a. La identificación, valoración, clasificación de activos de la Entidad, se realiza por parte de los líderes de procesos con el acompañamiento de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, de acuerdo con lo definido en la guía G-FD-1 “Guía de Gestión de activos de información” información diligenciada en el formato F-GD-1081” Registro De Activos De Información E Índice De Información Clasificada Y Reservada”.

b. Este inventario de activos de la Entidad deberá ser actualizado con el acompañamiento de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información anualmente o de acuerdo con los cambios normativos vigentes, de acuerdo con lo definido en la Ley 1712 de 2014, Art. 13. Registros de Activos de Información. Todo sujeto obligado deberá crear y mantener actualizado el Registro de Activos de Información haciendo un listado de:

   - Todas las categorías de información publicada por el sujeto obligado;
   - Todo registro publicado;
   - Todo registro disponible para ser solicitado por el publico

c. La Dirección de Tecnologías y Sistemas de la Información, a través del profesional de Seguridad de la Información y la Dirección de Recursos Físicos y Gestión Documental, brindarán acompañamiento técnico a los líderes de los 21 procesos misionales para la identificación de los activos de información de la Entidad.

d. El inventario de Activos de Información bajo el liderazgo de la Dirección de Recursos Físicos y Gestión Documental deberá ser publicado en el sitio web de la Entidad, acorde con lo descrito la Ley 1712 de 2014 “por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional”.

e. Identificar dentro del consolidado de los activos de información, los activos críticos y la Infraestructura Critica Cibernética, actividad que estará a cargo de la Dirección de Tecnologías y Sistemas de la Información a los cuales se les realizará la respectiva gestión de riesgos.

7.4.2 Propiedad de los Activos

Los líderes de procesos o jefe de áreas de la SDSCJ son los propietarios de los activos de información identificados en la Entidad de acuerdo con lo definido en el formato F-GD-1081” Registro De Activos De Información E Índice De Información Clasificada Y Reservada”, no debe existir varios propietarios para un mismo activo de información.

Los líderes de proceso de la SDSCJ deben realizar la validación de los activos de información del proceso a su cargo, con el fin de establecer los riesgos de seguridad de la información a los que éstos se vean expuestos en los casos que aplique, para lo cual se deberán gestionar responsabilidades como:

a. Actualización de los activos e Identificación de nuevos de acuerdo con la periodicidad establecida.
b. Definir los controles, y el apropiado uso de los activos de información identificados en la Entidad.
c. Hacer seguimiento continuo y periódico sobre la evaluación y valoración de los activos de información.
d. Definir el uso permisible de los activos de información.

7.4.3 Uso Aceptable de los Activos

Las reglas de uso aceptable de los activos de la Entidad se aplican a funcionarios, contratistas y terceros que tengan bajo su responsabilidad dichos activos. El cumplimiento de estas reglas es obligatorio y debe abarcar, como mínimo, las siguientes actividades:

a. Aceptar y cumplir las políticas de seguridad de la información establecidas en la Entidad.
b. Proteger contra pérdida, modificaciones y acceso no autorizados a los activos de información de la Entidad.
c. Comprender y aceptar sus responsabilidades frente al acceso a las diferentes soluciones tecnológicas que se tienen o administran en la Entidad.
d. Garantizar la protección efectiva de todos los activos de información de la Entidad, incluidos las Infraestructura Critica Cibernética mediante los controles definidos en las matrices de riesgos de seguridad de la información.
e. Los usuarios que accedan a información de la Entidad son responsables del uso adecuado de los recursos asignados para la ejecución de sus funciones.

7.4.4 Devolución de los Activos

Los funcionarios, contratistas o partes externas que sean responsables o tengan asignados activos de información de la SDSCJ, realizarán la devolución de estos, en el momento de la terminación del empleo, contrato o acuerdo, con la Entidad o se realice una modificación de las funciones u obligaciones contractuales.

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio, realiza el borrado seguro de la información contenida en los equipos de cómputo que funcionarios y contratistas regresen al almacén de la Dirección de Gestión de Recursos físicos y documental al finalizar el vínculo contractual con la Entidad.

7.4.5 Clasificación de la Información

La SDSCJ, debe clasificar la información en términos de requisitos legales, valor, criticidad, y susceptibilidad a divulgación o a modificación no autorizada y es por ello que de acuerdo con la guía G-FD-1 “Gestión de Activos de Información” de la SDSCJ y basado en la Ley 1712 de 2014 “Transparencia y acceso a la información pública” la clasificación de la información la divide en:

a. **Información pública:** es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal, es decir la información pública es aquella que ha sido declarada de conocimiento público por parte de la persona con autoridad para hacerlo o por alguna norma jurídica. Esta información puede ser entregada o publicada sin restricciones a terceros, funcionarios o cualquier persona sin ocasionar daños a terceros ni a los procesos de negocio.

b. **Información pública clasificada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias para el ejercicio de los derechos particulares o privados consagrados dentro de la ley.

c. **Información pública reservada:** es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados dentro de la ley.

Esta clasificación, permite a la Entidad usar los controles clave para garantizar que los activos están protegidos de manera adecuada.

7.4.6 Etiquetado de la Información

El etiquetado de la información está liderado a través de la Dirección de Recursos Físicos y Gestión Documental, de acuerdo con las tablas de retención documental vigentes y los lineamientos del PG-FD-1 “Programa de Gestión Documental” de la Entidad, así como lo establecido en los Ítem 6.1.6 Clasificación y custodia de la información y 6.1.7 Clasificación del Activo de Información de la guía G-FD-1 “Gestión de Activos de Información” de la Entidad.

7.4.7 Manejo de Activos

El manejo de Activos de información se desarrolla de acuerdo con el esquema de clasificación indicado en los Ítem 6.1.6 Clasificación y custodia de la información y 6.1.7 Clasificación del Activo de Información de la guía G-FD-1 “Gestión de Activos de Información”, lo cual establece el acceso por cada nivel de clasificación, el almacenamiento de activos según la especificación de fabricantes y en general cumpliendo los siguientes lineamientos:

a. La información que se genere, procese, administre, custodie por parte de los funcionarios o contratistas se debe usar para los fines propios de la misión de la Entidad, por ningún motivo, la información podrá ser cedida, transferida, divulgada o intercambiada con terceros bajo ninguna circunstancia.

b. Para la transferencia de información de la Entidad, se debe contar con la autorización o permisos de los líderes de proceso o quien haga sus veces.

c. Los terceros, proveedores u operadores tecnológicos que accedan a la información de la Entidad, no están autorizados a realizar copias de la información, ni podrán transferirla a otro equipo a través de la red, sin la autorización escrita de la Entidad.

d. Establecer mecanismos necesarios para que las soluciones tecnológicas de la Entidad cuenten con los controles de protección necesarios para el acceso a la información definida como reservada.

e. Los líderes de proceso deberán establecer el manejo adecuado de los activos de información, teniendo en cuenta su clasificación, y los controles pertinentes definidos de acuerdo con la criticidad o importancia del activo de información.

f. Los funcionarios y/o contratistas a los que se haya asignado un equipo de cómputo en la Entidad, solo podrán almacenar información de carácter estrictamente institucional.

7.4.8 Gestión de Medios Removibles

La SDSCJ, elaborará e implementará las actividades pertinentes para la gestión de medios removibles de acuerdo con el esquema de clasificación adoptado por la Entidad.

7.4.9 Disposición de los Medios

La Dirección de Tecnologías y Sistemas de la Información en referencia a la disposición de los medios, establece los siguientes parámetros:

a. Mediante el formato F-GT-422 “Concepto técnico de elementos de Tecnologías” verificar el estado actual de los medios removibles de la unidad y se genera el concepto técnico para la disposición final de elementos tecnológicos que estén para disposición final.
b. Respaldo de seguridad de información para garantizar la disponibilidad de la información de la plataforma tecnológica que será entregados al almacén de la Dirección de Recursos Físicos y Gestión Documental, para reasignación o etapa de baja de elementos tecnológicos.
c. A través de la solución antivirus instalada para la Entidad, se establece parámetros de escaneo de medios removibles en todos los equipos de cómputo, que permita de forma automática en el momento de inserción de medios físicos, realizar un análisis y tratamiento de todo tipo de programa maligno.
d. Los medios que contienen información de la Entidad deben almacenarse de forma segura, garantizando la confidencialidad de la información.

7.4.10 Transferencia de Medios Físicos

La SDSCJ, a través de la Dirección de Recursos Físicos y Gestión Documental, deberá contar con proveedores de mensajería confiables, encargados de la transferencia de información de manera adecuada cumpliendo con los requisitos establecidos contractualmente.

7.5 CONTROL DE ACCESO

La Entidad asegura el acceso a la información de funcionarios y contratistas en concordancia con la Política de Seguridad y Privacidad de la Información, evitando el acceso no autorizado a las soluciones tecnológicas

El acceso a todos los activos de información y las instalaciones de procesamiento de información de la Entidad, deben estar protegidos contra acceso no autorizado y contar con las medidas de protección necesarias para salvaguardar la información.

7.5.1 Política de control de acceso

En relación con el control de acceso, la SDSCJ establece una política teniendo en cuenta el contexto institucional y lo referente a seguridad de información.

7.5.2 Acceso a redes y a servicios en red

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio, con el fin de permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados, establece lo siguiente:

a. Todo funcionario, contratista, proveedor o usuario externo que requiera acceso a la red y a la infraestructura tecnológica de la SDSCJ, debe estar autenticado y sus conexiones deberán utilizar cifrado de datos, en caso de que los niveles de criticidad de información lo requieran.
b. Las solicitudes de acceso a páginas web no institucionales se realizan ante la mesa de servicios mediante la creación de un ticket o solicitud de servicios, de acuerdo a los cargos y roles de funcionarios u obligaciones establecidos para contratistas, previa autorización del jefe inmediato.
c. La mesa de servicios traslada el incidente al profesional de seguridad de la información quien analiza y gestiona las solicitudes de navegación que debido a sus funciones u obligaciones contractuales necesite un funcionario o contratista de la Entidad, previa solicitud por parte del líder de proceso.
d. Realizar monitoreo de las redes e infraestructura tecnológica de la Entidad.
e. Las conexiones remotas a la red local de la Entidad se deberán realizar a través de una conexión VPN segura, la cual deberá ser aprobada, registrada y auditada, sin excepción alguna por la Dirección de Tecnologías y Sistemas de la Información.
f. Las conexiones establecidas hacia los servicios dispuestos en la nube de la Entidad deben ser establecidos a través de conexiones cifradas por VPN para la gestión de los recursos allí disponibles.
g. La asignación para VPN a los funcionarios y contratistas de la Entidad dependerá de las funciones u obligaciones contractuales, esto con el fin de facilitar la conexión desde un lugar remoto a los servicios informáticos brindados por la Entidad, o por cumplimiento de una resolución de Teletrabajo.
h. La conexión realizada a través del servicio de VPN se debe realizar mediante la herramienta entregada por la Entidad, con respecto a la autenticación y conexión, el funcionario o contratista debe garantizar que se haga desde un equipo seguro.

7.5.2.1 Redes Inalámbricas

En lo referente a las redes inalámbricas, la Dirección de Tecnologías y Sistemas de la Información, establece puntos de control de acceso a las redes inalámbricas de la Entidad, implementando claves de acceso y cifrado de altos estándares de seguridad, método de autenticación a la red a través del usuario institucional, controles de acceso por contraseñas robustas evitando los accesos no autorizados y demás acciones que deriven en el aumento de seguridad de acceso a la red. Para lo cual, se debe;

a. Utilizar la red para fines y uso interno de la Entidad.
b. Ningún usuario realizará actividades que atenten contra el principio de confidencialidad y privacidad de la información.
c. La red inalámbrica de servicio de la Entidad se habilita para acceso de servicios misionales, de apoyo y consultas de internet, únicamente para equipos de cómputo de propiedad y/o en alquiler registrados en el dominio de la Secretara Distrital de

Seguridad, Convivencia y Justicia.

d. La red Inalámbrica de la Entidad para funcionarios y contratistas con equipos de cómputos personales, se habilita conexión a través de una red de consulta a internet, la conexión a servicios y consultas misionales se debe ejecutar sobre la red con un acceso a VPN.
e. El acceso a personal externo de la Entidad que requiera una conexión a la red inalámbrica será autorizado a través de la red de invitados disponible para tal fin, con acceso a consulta de internet, sin acceso a recursos internos de la entidad, previa coordinación con la mesa de servicios de la Entidad.

7.5.3 Registro y cancelación del registro de usuarios

Para el acceso de los funcionarios o contratistas a las soluciones tecnológicas, servicios y en general cualquier recurso de información de la SDSCJ el usuario realiza la solicitud de creación de usuarios, de acuerdo con lo establecido en el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”, a la mesa de servicios, anexando documentación requerida y el formato F-GT-285 “Solicitud Administración de Usuarios” diligenciado previa autorización del líder de proceso.

Una vez se termine el vínculo laboral y/o contractual de funcionario o contratista de la Entidad, se deben deshabilitar y/o retirar inmediatamente los permisos a las soluciones tecnológicas que le fueron asignados. Esto debe ser reportado por los supervisores de contrato, teniendo en cuenta el proceso de paz y salvo que se lleva a cabo en la Entidad.

7.5.4 Suministro de Acceso de Usuarios

La Dirección de Tecnologías y Sistemas de la Información a través de la mesa de servicios será la responsable de la creación, modificación y eliminación de usuarios, contraseñas y privilegios de acceso en la infraestructura y soluciones tecnológicas de la Entidad de acuerdo con lo definido en el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”.

7.5.5 Gestión de derechos de acceso privilegiado

La Dirección de Tecnologías y Sistemas de la Información a través de la mesa de servicios, previo el lleno de requerimientos de seguridad de la Información, según la solicitud radicada para cada caso y de acuerdo a las funciones u obligaciones contractuales de los usuarios, asignarán permisos y privilegios de control de acceso a las diferentes soluciones tecnológicas en la Entidad, de acuerdo a lo definido en el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”, los privilegios de administración en lo posible y de acuerdo a disponibilidad deberán estar distribuidos en personal de planta.

7.5.6 Gestión de información secreta para la autenticación de usuarios

Todo funcionario de la SDSCJ que maneja información sensible para la Entidad deberá diligenciar y firmar el formato F-GH-807 “Compromiso de Confidencialidad y No Divulgación del Información” para mantener un nivel de confidencialidad sobre ésta.

7.5.7 Revisión de los derechos de acceso de usuarios

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio, facilita los accesos de funcionarios o contratistas a los activos de información de la Entidad, los

cuales se ajustan y modifican después de cualquier cambio, promoción, modificación de cargo, terminación de contrato, la revisión se debe realizar con una periodicidad anual.

A su vez, cualquier modificación de funciones, condiciones, obligaciones de los funcionarios o contratistas, será reportado por parte de la Dirección de Gestión Humana y/o la Dirección Jurídica y Contractual según sea el caso, a la Dirección de Tecnologías y Sistemas de la Información, para realizar los ajustes pertinentes en las soluciones tecnológicas.

7.5.8 Retiro o ajuste de los derechos de acceso

Los derechos de acceso a los funcionarios y/o contratistas de la SDSCJ, o terceros que acceden a la información, deben ser retirados al terminar el vínculo contractual o laboral, se deberán ajustar cuando se realicen cambios de acuerdo con lo establecido en el procedimiento interno PD-GT-8 “Administración de Usuarios”.

7.5.9 Uso de información secreta para la autenticación

De acuerdo con el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”, de la SDSCJ, el manejo de cuentas de usuarios y contraseñas son de carácter personal e intransferible, por lo tanto, las operaciones que pongan en riesgo los intereses de la Entidad serán de entera responsabilidad del usuario o funcionario.

Los funcionarios y contratistas deberán utilizar credenciales seguras de ingreso a los servicios tecnológicos designados, de acuerdo con lo establecido en el Ítem 7.5.12 “Gestión de Contraseñas” del presente manual.

7.5.10 Restricción de acceso a la información

La Dirección de Tecnologías y Sistemas de la Información, como responsable de la administración de las soluciones tecnológicas y medios, propenderá para que éstos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso determinados en el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”.

7.5.11 Procedimiento de ingreso seguro

La Dirección de Tecnologías y Sistemas de la Información, entrega a cada funcionario y contratista un usuario y contraseña como medio de autenticación, para el ingreso seguro a las distintas soluciones tecnológicas y servicios, esto a través de la mesa de servicio de acuerdo con el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”.

7.5.12 Sistema de gestión de contraseñas

La Dirección de Tecnologías y Sistemas de la Información, a partir de la información del directorio activo el cual es actualizado periódicamente, establece los siguientes lineamientos para la administración y autenticación de usuarios, así:

1. Usuarios registrados en el Directorio Activo de la Entidad:
   a. Un tiempo de caducidad de las contraseñas de 30 días para las cuentas gestionadas mediante directorio activo.
   b. La contraseña no contiene el nombre del usuario.
   c. Tener una longitud mínima de diez caracteres.

d. Incluir caracteres que cumplan con las siguientes categorías:
    - Mayúsculas (de la A hasta la Z)
    - Minúsculas (de la a hasta la z)
    - Dígitos de base 10 (del 0 al 9)
    - Caracteres no alfanuméricos (¡por ejemplo, !, $, #, %)

e. Restricción de contraseñas usadas y no reúso.
f. Almacena, registra y transmite contraseñas de modo seguro.
g. Bloqueo de cuentas después de 5 intentos de inicio de sesión fallidos.

En todo caso, la mesa de servicio cuenta con privilegios para realizar cambios de contraseña de los usuarios del directorio Activo de acuerdo con los tickets de servicios generados en la herramienta de gestión disponible para la atención de casos.

Para aquellos sistemas de información que no puedan ser integrados con el Directorio Activo de la Entidad, resulta crucial establecer parámetros de autenticación de usuarios alternativos. Estos parámetros deben incluir, al menos, los siguientes aspectos:

2. Sistemas de autenticación mediante Aplicación o sistema de Información, así.

    a. Creación y uso de contraseñas robustas:
        - Longitud mínima de contraseña de diez caracteres.
        - Uso obligatorio de una combinación de letras mayúsculas, minúsculas, números y caracteres especiales (#$%&? +.@-_)
        - Frecuencia requerida para cambiar la contraseña de 30 días.
    b. Cambio de las contraseñas iniciales o temporales después del primer uso.
    c. Bloqueo de cuentas después de cinco intentos de inicio de sesión fallidos.
    d. Implementación de sesiones de autenticación con tiempo límite de inactividad de cinco minutos.
    e. Uso de recaptcha para los sistemas que permita su integración.

3. Sistemas de autenticación mediante la versión del motor de la Base de datos, así:

    a. Creación y uso de contraseñas robustas:
        - Longitud mínima de contraseña de diez caracteres.
        - Uso obligatorio de una combinación de letras mayúsculas, minúsculas y números.
        - Frecuencia requerida para cambiar la contraseña de 30 días.
    b. Cambio de las contraseñas iniciales o temporales después del primer uso.
    c. Bloqueo de cuentas después de cinco intentos de inicio de sesión fallidos.
    d. Implementación de sesiones de autenticación con tiempo límite de inactividad de cinco minutos.
    e. Bloqueo definitivo del usuario que tengan inactividad más de 60 días.

7.5.13 Uso de programas utilitarios privilegiados

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio, con el uso de herramientas tecnológicas disponibles como consola antivirus y reglas de directorio

activo del dominio scj.gov.co, entre otras herramientas disponibles, verificará el uso de programas utilitarios privilegiados de acuerdo con lo siguiente:

a. Reglas que no permitan la instalación o ejecución de programas a usuarios finales.
b. Licenciamiento de software y/o programas dentro de las soluciones tecnológicas de la Entidad.
c. Minimizar el uso de programas utilitarios y/o software especializado a la cantidad mínima posible, para funcionarios y contratistas de acuerdo con el desarrollo de sus funciones.
d. Uso apropiado de los programas utilitarios instalados en la Entidad por parte de funcionarios, contratistas o personal externo.
e. Registro del uso de programas utilitarios del sistema dentro de la Entidad.
f. La mesa de servicio cuenta con autorización de retiro y/o eliminación de los programas utilitarios innecesarios.

7.5.14 Control de acceso a códigos fuente de programas

La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, implementa los lineamientos sobre control de acceso a código fuente de acuerdo con lo establecido por el procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software” de la Entidad.

La Entidad cuenta con un repositorio centralizado y controlado de versiones de códigos fuente, que almacena y gestiona los desarrollos realizados por el grupo de Sistemas de Información. El repositorio se establece utilizando una herramienta de control de versiones, como Git, y está configurado con los respectivos permisos y roles para el equipo de desarrolladores.

7.6 CRIPTOGRAFIA

El propósito es el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información de la Entidad, protegiendo y cifrando la información en el momento de almacenamiento y/o transmisión por cualquier medio.

7.6.1 Política sobre el uso de controles criptográficos

La Dirección de Tecnologías y Sistemas de la Información, define una política sobre el uso de controles criptográficos con el fin de proteger la información, teniendo en cuenta lo siguiente:

a. Utilizará criptografía simétrica para la información transmitida de extremo a extremo, para ello utiliza fuentes de cifrado con VPN sitio a sitio.
b. Verificará el control de acceso con contraseña o cifrado de los archivos que se consideren de alta criticidad o confidencialidad utilizando herramientas como 7-Zip.
c. Los algoritmos de cifrado criptográfico aprobados a utilizar como son: AES, TripleDES, Twofish, DSA, RSA, ECDSA, SHA1 y SHA2, los cuales deben ser utilizados como base de la tecnología de cifrado.
d. Los sistemas de criptografía simétricos deben utilizar llaves con 128 bits o más. Las llaves de los sistemas de criptografía asimétricos deben utilizar longitudes que ofrezcan una robustez similar.
e. Los requerimientos de longitud de llaves de los algoritmos de cifrado serán revisados y actualizados anualmente.

f. Para él envió de información por canales no cifrados, se debe incorporar una capa de seguridad por contraseña a los archivos que se envían y/o realizar proceso de cifrado la información antes de ser transferida.

7.6.2 Gestión de Llaves Criptográficas

Referente a la generación de llaves criptográficas se deben tener en cuenta los siguientes criterios:

a. Seleccionar el algoritmo de cifrado de acuerdo con la necesidad y servicio teniendo en cuenta el lineamiento de controles criptográficos.
b. Seleccionar el tipo de llave y su funcionalidad.
c. Establecer el tiempo de vida del mecanismo de cifrado utilizado.
d. Especificar las llaves o parámetros antes de su uso y emisión.
e. Modificar y/o generar nuevamente las llaves criptográficas en caso de que sean comprometidas.

Existen varias razones por las cuales es posible cambiar una clave:

a. La clave puede estar comprometida.
b. La fecha de vencimiento de la clave está a punto de expirar o se encuentra expirada.
c. Es requerido modificar el algoritmo criptográfico de la VPN o de algún sistema criptográfico utilizado.

7.7 SEGURIDAD FÍSICA Y DEL ENTORNO

La Entidad toma las medidas necesarias para prevenir el acceso no autorizado, daño o interferencia a la información, como la protección ante amenazas asociadas con el ambiente físico, brindando un acceso controlado y restringido a las áreas, instalaciones, equipos y soluciones tecnológicas, estableciendo mecanismos de control que permitan el aseguramiento de los activos, de acuerdo a lo establecido en el instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ” y lo Establecido en el documento MA-GE-1 “Manual Operativo C4”.

7.7.1 Perímetro de Seguridad Física

En la SDSCJ, son áreas de acceso restringido, todos aquellos espacios físicos, lugares de trabajo, oficinas, entre otros de acuerdo con lo definido en el instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ, destinadas a la creación, manejo, análisis, procesamiento o almacenamiento de información crítica y sensible, así como aquellos ambientes de trabajo destinados para la ubicación de equipos/servidores y demás infraestructura tecnológica que soporta la operación de la Entidad.

7.7.2 Controles de acceso físicos

La SDSCJ cuenta con medidas de control de acceso físico de entrada que permite proteger la información, el software y el hardware de daños intencionales o accidentales y de acceso de personas no autorizado, en las áreas de procesamiento de información de acuerdo con lo establecido en el instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ.

7.7.3 Seguridad de oficinas, recintos en instalaciones.

Las instalaciones de la SDSCJ cuentan con servicio de vigilancia y seguridad privada, el cual es prestado por una empresa contratada por la Entidad, quienes cuentan con protocolos y/o lineamientos, para salvaguardar la integridad física de las instalaciones, a través de servicios y controles de acceso de acuerdo con lo establecido en el instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ.

7.7.4 Protección contra amenazas externas y ambientales

La SDSCJ en referencia a la Protección contra amenazas externas y ambientales, teniendo en cuenta lo siguiente:

a. Cumplir con los niveles de humedad y temperatura, de acuerdo con las recomendaciones de uso de equipos tecnológicos por los fabricantes en las instalaciones de procesamiento de información, con el fin de responder de manera adecuada ante incidentes como incendios o inundaciones entre otros.
b. Contar con instalaciones adecuadas para los centros de procesamiento de datos, donde se encuentran ubicados equipos servidores, soluciones tecnológicas, equipos de comunicaciones de voz y datos y otros servicios sensibles para la Entidad, deben estar localizados en lugares seguros, aislado de amenazas potenciales como agua, fuego, polvo interferencia electrónica entre otros, con paredes sólidas, puertas de acceso adecuadas y protegidas para prevenir el uso o acceso no autorizado.
c. Disponer de protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, seguridad en el suministro eléctrico, cableado y sistemas de detección y extinción de incendios.
d. Prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de estos o deterioren la información almacenada en ellos.
e. Cumplir para la protección de suministro de red eléctrica publica lo establecido en el numeral 5.7.8 Servicios de suministro del presente manual.

7.7.5 Trabajo en áreas seguras

Todas las actividades desarrolladas por funcionarios y contratistas en las áreas seguras de la Entidad deben regirse bajo las condiciones mínimas establecidos en el instructivo I-GRF-04: Acceso a las instalaciones de Funcionamiento de la SSCJ y lo Establecido en el documento MA-GE-1 “Manual Operativo C4”.

7.7.6 Áreas de despacho y carga

El acceso a áreas de despacho y carga está restringido, solo personal autorizado e identificado podrá acceder a estos lugares de forma controlada sin acceso a otras áreas de las instalaciones estableciendo mecanismos de control que permitan el aseguramiento de los activos, de acuerdo con lo establecido en el instructivo I-GRF-04: Acceso a las instalaciones de Funcionamiento de la SSCJ y lo Establecido en el documento MA-GE1 “Manual Operativo del C4”.

7.7.7 Ubicación y Protección de los equipos

Los equipos de la SDSCJ tales como, servidores, equipos de comunicaciones y seguridad electrónica, centros de cableado, UPS, subestaciones eléctricas, aire acondicionado, así como estaciones de trabajo y dispositivos de almacenamiento y/o comunicación móvil que contengan información y/o brinden servicios de la Entidad, deben ser ubicados y protegidos estratégicamente dentro de las áreas disponibles que ofrezcan garantías de seguridad que prevenga la pérdida, daño o sustracción de información.

7.7.8 Servicios de suministro

La SDSCJ en referencia a servicio de suministro, establece las siguientes actividades:

a. Establece parámetros de protección de los equipos de procesamiento de información, respecto a fallas de energía u otras interrupciones causadas por los servicios de suministro.
b. Define la periodicidad con la que se debe realizar el mantenimiento de las UPS (Sistema Ininterrumpido de Potencia), plantas eléctricas o grupos electrógenos de respaldo de todas las sedes de la Entidad, en los contratos de mantenimiento que se le asigne.
c. Para sedes propias se tiene un contrato de mantenimiento locativo que lo supervisa la “Dirección de Bienes para la Seguridad, Convivencia y Acceso a la Justicia”. El proceso de contratación incluye todas las UPS.
d. Para sedes en arrendamiento se transfiere el suministro y mantenimiento de UPS (Sistema Ininterrumpido de Potencia) a los dueños de los predios mediante el contrato de arrendamiento, contratos supervisados por la “Dirección de Bienes para la Seguridad, Convivencia y Acceso a la Justicia”.
e. Los centros de procesamiento de datos deben mantener sistema de ventilación y climatización que permita la refrigeración y el acondicionamiento de aire de los equipos allí alojados de acuerdo con las recomendaciones de los fabricantes.

7.7.9 Seguridad del cableado

La SDSCJ en referencia a la seguridad del cableado tanto para sedes propias como en arrendamiento, debe tener en cuenta las siguientes recomendaciones:

a) EL cableado de energía eléctrica da cumplimiento a los lineamientos y buenas prácticas de la Norma Técnica Colombia NTC2050, en el Reglamento Técnico de Instalaciones Eléctricas RETIE y demás normatividades aplicables.
b) El cableado de telecomunicaciones da cumplimiento a las buenas prácticas de las normas y estándares que rigen la materia, tales como ANSI/TIA-568, ANSI/TIA-569, ANSI/TIA-606, ANSI-TIA-607 y las demás que modifiquen, complementen, adicionen o deroguen.
c) Proteger el cableado de humedad o exposición a fuentes de calor que puedan afectar o generar daños a la estructura de este.
d) El cableado de red de datos debe tener protección contra cualquier interceptación no autorizada, interferencias o daño externos o de terceros.
e) El cableado de la red de datos debe estar separado del cableado de la red eléctrica de acuerdo con los estándares aplicables para evitar posibles fallas de interferencias electromagnéticas o descargas electroestáticas.

f) Se debe tener en cuenta las recomendaciones de los fabricantes, así como la realización de rutinas de mantenimientos preventivos – correctivos, que minimicen el riesgo de fallo y perdida de la seguridad del cableado.

7.7.10 Mantenimiento de Equipos

La SDSCJ en referencia a mantenimientos de equipo, establece las siguientes actividades:

a. Todo requerimiento por parte de los usuarios debe ser documentado por la mesa de servicio de acuerdo con los requerimientos solicitados.
b. Cada requerimiento de soporte técnico debe estar gestionado de acuerdo con las instrucciones relacionadas en el procedimiento interno PD-GT-1 “Procedimiento de Gestión de Requerimientos de TI”
c. El soporte técnico se realiza de acuerdo con el procedimiento interno PD-GT-1 “Procedimiento de Gestión de Requerimientos de TI” de la Entidad.
d. El contratista encargado del mantenimiento preventivo y correctivo de los equipos de cómputo debe mantener actualizadas las hojas de vida de estos.
e. El personal autorizado y certificado por el fabricante de los equipos, debe llevar a cabo las reparaciones y servicio sobre los equipos de procesamiento de información.
f. Validar los contratos de soporte vigentes que permitan el mantenimiento preventivo y correctivo (incluidos repuestos) de los equipos de cómputo e infraestructura tecnológica con el fin de asegurar su disponibilidad e integridad.

7.7.11 Retiro de activos

Los bienes al servicio de la Entidad no se pueden retirar de la misma, sin autorización previa de la Dirección de Recursos Físicos y Gestión Documental de acuerdo con los requisitos establecidos en el Instructivo I-GRF-04 “Acceso a las instalaciones de Funcionamiento de la SSCJ”

A su vez, la Dirección de Tecnologías y Sistemas de la Información, mediante el procedimiento interno PD-GT-1 “Procedimiento de Gestión de Requerimientos de TI ” establece las actividades de operación referente a la asignación de equipos tecnológicos a los usuarios o contratistas según la disponibilidad, previo el diligenciamiento de las actas F-GT-540 “Acta De Entrega De Elementos Tecnológicos” y/o según sea el caso acta F-GT-541 “Acta De Préstamo De Elementos Tecnológicos”, asignando responsabilidades individuales en la protección y uso de los mismos.

7.7.12 Seguridad de equipos y activos fuera de las instalaciones

Los funcionarios y contratistas de la SDSCJ son responsables de la seguridad de los equipos de cómputo asignados que se encuentren fuera de las instalaciones de la Entidad, así:

a. En ninguna circunstancia los equipos de cómputo asignados a los funcionarios y contratistas pueden estar abandonados, sin la correspondiente vigilancia y custodia.
b. No se autoriza a ningún usuario, realizar cambios a los controles de seguridad establecidos por la mesa de servicio en los equipos de cómputo de la Entidad.

c. El personal de mesa de servicio son los autorizados por la Dirección de Tecnologías y Sistemas de la Información para realizar cambios a los componentes de las soluciones tecnológicas de la Entidad.
d. Los equipos portátiles deben ser transportados de forma segura, teniendo especial cuidado de no exponerlos a cualquier riesgo que comprometa la confidencialidad de la información y su integridad física.
e. En caso de pérdida o robo de un equipo de la SDSCJ, se deberá informar inmediatamente a la Dirección de Recursos Físicos y Gestión Documental para que se inicie el trámite interno, así mismo la denuncia pertinente ante la autoridad competente, para los casos de los equipos en alquiler, mediante contrato suscrito por la SDSCJ, se debe reportar a través de la mesa de servicio para iniciar el reporte y gestión a través de la Dirección de Tecnologías y Sistemas de la Información.

7.7.13 Disposición segura o reutilización de equipos

La Dirección de Tecnologías y Sistemas de la Información, por medio de la mesa de servicio establece las siguientes actividades en referencia a la disposición segura o reutilización de equipos:

a. Verificar y conceptuar en relación con el estado de los equipos tecnológicos en la Entidad, lo cual estará documentado en el formato F-GT-422 “Concepto Técnico de Elementos de Tecnología” de la Entidad.
b. El equipo asignado a un funcionario o contratista deberá estar debidamente formateado y sin información del anterior usuario.
c. La Entidad se ajusta al procedimiento interno descrito en la guía G-FI-02 “Manejo de residuos de Aparatos Eléctricos y Electrónicos – RAEE” de tal forma que cumpla con lo establecido en ley 1672 del 2013 “Política Pública de Gestión Integral de Residuos de Aparatos Eléctricos y Electrónico- RAEE”.
d. Todo equipo tecnológico para disposición final o reutilización, que contenga información sensible reportada por el usuario, dueño o custodio del activo, se le debe realizar procedimiento de respaldo de información a entregar al líder de proceso, para las acciones o procedimientos que se determinen.
e. Realizar la disposición final de elementos por obsolescencia tecnológica, estará a cargo del almacén de la Dirección de Gestión de Recursos Físicos y Documental, de acuerdo con lo definido en el procedimiento interno PD-FD-14 “Reintegro, Baja y Destinación Final”.

7.7.14 Equipos de usuario desatendido

La Dirección de Tecnologías y Sistemas de la Información, establece unas reglas de Directorio Activo de bloqueo por inactividad mínimo de 30 segundos cuando los equipos están desatendidos.

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.

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.

7.7.15 Política de escritorio y pantalla limpios

Para reducir el acceso o prevenir la pérdida, daño o sustracción de la información por terceros o personal no autorizado, la Entidad definirá una política, teniendo en cuenta lo siguiente:

a. Bloquear sesión de los dispositivos tecnológicos cuando no se esté usando.
b. La información tipificada como clasificada o reservada no debe estar a disposición de terceros.
c. Guardar documentos bajo llave y conservar escritorios libres de documentación.
d. Retirar documentos impresos y darle manejo apropiado.
e. Los equipos de cómputo tendrán parametrizado el cierre de sesión por inactividad de acuerdo con directivas establecidas en el directorio activo para tal fin.

7.8 SEGURIDAD DE LAS OPERACIONES

La seguridad de las operaciones en la Entidad garantiza acciones de prevención, ejecución y control de la información, con el fin de que ésta se encuentre protegida ante pérdida, alteración, acceso no autorizado, código malicioso o cualquier evento irregular que vulnere la integridad de esta.

Las operaciones tecnológicas de la Entidad deben cumplir con las condiciones de seguridad requeridas para mantener la confidencialidad, disponibilidad e integridad de la información.

7.8.1 Procedimientos de operación documentados

La Dirección de Tecnologías y Sistemas de la Información cuenta con procedimientos estandarizados y documentados para la gestión de infraestructura y soluciones tecnológicas de la Entidad, las cuales soportan las soluciones tecnológicas puestas a disposición de los usuarios.

Los procedimientos de operación especifican las instrucciones y operaciones que incluyen atención de requerimientos, control de acceso a plataformas, copias de respaldo de información, requerimientos tecnológicos, gestión de cambios, incidentes de seguridad de la información, administración de usuarios, entre otros.

7.8.2 Gestión de cambios

Los cambios de tecnologías de la información que impacten la prestación de las soluciones y servicios tecnológicos, que agreguen, modifiquen o retiren funcionalidades deben ser evaluados en la sesión del Grupo de Gestión de Cambios de acuerdo con las políticas de operación descrita en el procedimiento interno PD-GT-2 “Gestión de Cambios de TIC” de la Entidad, así:

Las solicitudes de cambio son generadas en la herramienta de gestión por el solicitante del cambio, adjuntando el formato F-GT-278 “Gestión de cambios” debidamente diligenciado, así como los instrumentos de scripts, parametrización de base de datos, aprobación en ambiente de pruebas y demás actividades, a más tardar 24 horas antes de la programación de la sesión de gestión de cambios.

7.8.3 Gestión de capacidad

La Entidad realizara monitoreo, análisis y evaluación del rendimiento y capacidad de su infraestructura tecnológica de procesamiento de información, almacenamiento de información, redes y comunicaciones, con el fin de identificar y controlar el consumo de sus recursos y prever su crecimiento de forma planificada.

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

La Dirección de Tecnologías y Sistemas de la Información, a través del procedimiento interno PD-GT-16 “Gestión de Pruebas Tecnológicas”, procedimiento interno PD-GT-17 “Ciclo De Vida de desarrollo de software” de la Entidad, adoptó los lineamientos para los ambientes separados de producción, pruebas y desarrollo, con el fin de garantizar la integridad de la información procesada, evitar interferencias en el desempeño, reducir los riesgos de acceso o cambios no autorizados en el ambiente de producción.

7.8.5 Controles contra códigos maliciosos

La SDSCJ cuenta con herramientas de seguridad como antivirus, Antispam, antispyware, seguridad perimetral y otras soluciones las cuales brindan protección contra código malicioso, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

Para los equipos tecnológicos de propiedad de funcionarios o contratistas, se debe contar con herramientas de seguridad como antivirus y sistemas operativos licenciados con la instalación de actualizaciones o parches de seguridad vigentes, con el fin de evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicios, es la encargada de autorizar el uso de herramientas de seguridad, aplicando reglas que no permitan la modificación, alteración o desinstalación de la solución antivirus, verificando el estado de actualización permanente.

Los funcionarios o contratistas que detecten algún tipo de amenaza por software malicioso que comprometa la seguridad de la información, deben reportar a la Dirección de Tecnologías y Sistemas de la Información, mediante la mesa de servicio.

7.8.6 Respaldo de Información

La SDSCJ en referencia al respaldo de información, define una política de acuerdo con lo siguiente:

a. Administrar, gestionar y custodiar las copias de respaldo de información generadas sobre los componentes tecnológicos de acuerdo con el procedimiento interno PD-GT-11 “Gestión de Infraestructura y Plataformas Tecnológicas” de la Entidad.
b. La frecuencia y alcance de las copias de respaldo de la información se establece por los líderes de proceso, al igual que los periodos de retención y la criticidad de la información respaldada.
c. Identificar los inventarios de activos de soluciones y componentes tecnológicos que deben ser respaldados.

d. Efectuar copias de respaldo de información antes y después de cualquier cambio en la configuración del componente de la infraestructura tecnológica.
e. Almacenar los logs de ejecución y generación exitosa o fallida de las copias de respaldo de los activos críticos (Bases de Datos, Instancias de la nube, servidores) por un periodo no menor a 1 año
f. Todo evento fallido en la ejecución de las copias de respaldo de información debe ser registrado y notificado al administrador o responsable de la respectiva infraestructura y/o solución tecnológica.
g. Conservar las copias de respaldo en los servicios en nube disponible de la Entidad, y de forma local en dispositivos de almacenamiento conectados a la red que permitan almacenar y recuperar datos en puntos centralizados.

7.8.7 Registro de Eventos

La Dirección de Tecnologías y Sistemas de la Información, cuenta con una solución de captura y correlación de eventos, monitoreando periódicamente las acciones o incidentes generados por la plataforma de seguridad perimetral para prevención de potenciales incidentes de seguridad de la información.

7.8.8 Protección de la Información de Registro

Las soluciones tecnológicas de la Entidad cuentan con controles de información de registro, los cuales están dirigidos a proteger contra cambios no autorizados (Log Information) y contra problemas operacionales con los sistemas de registros de tal manera que se prevenga las alteraciones en los registros y logs.

7.8.9 Registro del administrador y del operador

Las actividades realizadas con los diferentes roles en las soluciones tecnológicas se registran según la necesidad de los analistas funcionales y es potestad de estos la revisión y gestión de los roles.

7.8.10 Sincronización de Relojes

Las soluciones tecnológicas de la Entidad tienen un sistema de sincronización de relojes de, cumpliendo con lo siguiente:

a. Hora legal colombiana y no está permitida la desactivación del sistema de sincronización o la manipulación manual de la hora.
b. Los relojes de todos los sistemas de procesamiento de información relevantes deben estar sincronizados de acuerdo con el Instituto Nacional de Metrología (INM).
c. El ajuste correcto de los relojes de computador es necesario para la exactitud de los registros de auditoría (logs).

7.8.11 Instalación de software en sistemas operativos

La Dirección de Tecnologías y Sistemas de la Información en referencia al control Instalación de software en Sistemas Operativos en los equipos tecnológicos, se ajusta al procedimiento interno PD-GT-1 “Procedimiento Gestión de Requerimiento de TI “de la Entidad, para lo cual, se tener en cuenta las siguientes recomendaciones:

a. Toda la plataforma tecnológica debe utilizar software legal.

b. Instalar software autorizado de acuerdo con su funcionalidad y alcance de licencia.
c. Prohibido copiar, cambiar, sustraer, distribuir software propiedad de la Entidad.
d. Realizar actualización y aplicación de parches de seguridad sobre toda la plataforma tecnológica de la Entidad mediante el procedimiento de gestión de cambios.
e. La mesa de servicio establece una línea base de software autorizado para los equipos de cómputo de la Entidad.
f. La mesa de servicio realiza monitoreo sobre el software operacional instalado en los diferentes equipos de la Entidad, cualquier software adicional que requiera un funcionario o contratista deberá ser solicitado por el líder de proceso mediante caso en la mesa de servicio y aprobado por el profesional de seguridad de la información para proceder con la instalación.
g. No utilizar hardware o software de monitoreo de actividades (analizadores de protocolos, softwares catalogados como “hacking”, etc.) sin la debida autorización de la Dirección de Tecnologías y Sistemas de la Información.

7.8.12 Gestión de las vulnerabilidades técnicas

La Dirección de Tecnologías y Sistemas de la Información realizará el análisis de vulnerabilidades a las soluciones tecnológicas de la Entidad de acuerdo con el alcance del plan de trabajo establecido para cada vigencia. Se documentarán los resultados de cada prueba realizada, y se establecerá el respectivo plan de remediación junto con las acciones a implementar.

Al inicio de cada vigencia se presentará por parte de la DTSI, el plan de trabajo sobre escaneo de vulnerabilidades.

7.8.13 Restricciones sobre la instalación de software

La Dirección de Tecnologías y Sistemas de la Información autorizó a la mesa de servicio en la Entidad, para realizar procedimientos de instalación, cambio, desinstalación, actualización de software de acuerdo al procedimiento interno PD-GT-1 “Procedimiento Gestión de Requerimientos de TI” de la Entidad, cada instalación debe ser generada mediante una solicitud y ticket en la herramienta de gestión para su seguimiento y trazabilidad, ningún usuario final tiene privilegios administrativos para hacer cambios en la plataforma.

7.8.14 Controles de auditoría de sistemas de información.

Todas las auditorías que se realicen a las soluciones tecnológicas de la SDSCJ deberán ser acordadas con el fin de estar autorizadas y controladas, para garantizar la disponibilidad de la información. En la medida de lo posible, estas auditorías para las soluciones tecnológicas críticas de la Entidad se realizarán en horarios no laborales, en coordinación con la Dirección de Tecnologías y Sistemas de la Información.

7.9 SEGURIDAD DE LAS COMUNICACIONES

La seguridad de las comunicaciones en la Entidad asegura la protección de la información en las redes y sus instalaciones, incluyendo transferencia interna o externa de información.

Se establecen mecanismos de control con el fin de proveer y proteger la integridad y confidencialidad de la información contenida y transportada a través de las redes, canales de

comunicaciones, internet y mensajería electrónica.

7.9.1 Controles de redes

La Dirección de Tecnologías y Sistemas de la Información en referencia a los controles para proteger la información de las soluciones tecnológicas se gestionan y controlan las redes de la Entidad. Para lo cual, se requiere cumplir con lo siguiente:

a. Los componentes de red y seguridad perimetral deben contar con contraseñas robustas para poder acceder a los mismos.
b. Únicamente personal autorizado puede ingresar a los equipos de comunicación, dispositivos de red y seguridad perimetral.
c. El acceso administrativo a los equipos de red debe ser centralizado y auditado.
d. Todas las conexiones de administración deben ser bajo conexiones cifradas.
e. Los componentes de red deben ser monitoreados para asegurar su correcta configuración y seguridad.
f. Las conexiones entrantes (Incoming) y salientes (Outbound) entre la red de la de la Entidad y cualquier otra red debe realizarse a través de dispositivos de firewall, evitando divulgación externa de los direccionamientos internos de la Entidad; se deberán configurar listas de acceso donde se garantice que únicamente personal autorizado pueda visualizar estos direccionamientos.
g. Las reglas configuradas en los dispositivos firewall deben estar documentadas, justificadas y aprobadas; dicha documentación deberá ser verificada con una periodicidad mínima de 1 año y aprobado por la Dirección de Tecnologías y Sistemas de la Información.
h. Cuando los equipos, dispositivos de red y seguridad perimetral son registrados para uso en la Entidad, se asigna un nombre de red y dirección IP, de acuerdo con la nomenclatura establecida por la Dirección de Tecnologías y Sistemas de la Información.
i. La definición y diseño del direccionamiento de las redes, así como la aprobación de asignación de direcciones IP fijas en la red es responsabilidad del administrador de redes y telecomunicaciones.
j. Los componentes tecnológicos que sean ingresados a las redes corporativas deben cumplir como mínimo con contraseñas de acceso, antivirus actualizado, firewall del sistema operativo activo y actualizado con los últimos parches de seguridad.
k. Realizar revisiones periódicas como mínimo una vez al año de las configuraciones y estándares aplicados en los diferentes componentes de la red con el fin de evaluar el cumplimiento de los requerimientos de aseguramiento de plataforma.

7.9.2 Seguridad de los servicios de red

La Dirección de Tecnologías y Sistemas de la Información en referencia a la seguridad de los servicios de red pertinentes a la Entidad, toma como referencia los siguientes lineamientos:

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

a. En sedes en arrendamiento los equipos de red que sean suministrado por los dueños de los predios estarán bajo la responsabilidad y administración del personal capacitado y asignado por la Dirección de Tecnologías y Sistemas de la Información.

b. Todos los componentes de red y de seguridad perimetral deben estar actualizados a su último paquete de seguridad estable.
c. Únicamente los servicios requeridos deben estar habilitados, aquellos servicios de red que no se usen deberán estar deshabilitados.
d. Los accesos remotos a la red deben ser autorizados por la Dirección de Tecnologías y Sistemas de la Información.
e. Los equipos o servicios que sean expuestos en la red externa deberán ser ubicado en una DMZ la cual debe ser segmentada mediante dispositivos firewall.
f. Estos servicios expuestos serán protegidos mediante WAF que ha destinado la Entidad para la protección contra ataques informáticos.
g. Los acuerdos de transmisión de información con terceros deben incluir el protocolo de intercambio de información (VPN, Cifrado asimétrico, aseguramiento por contraseña).
h. Los servicios de red deben proporcionar protección contra el acceso no autorizado, modificación o denegación de servicio, el direccionamiento correcto del mensaje, protección contra la confidencialidad, integridad y disponibilidad de la información, niveles de autenticación para los usuarios basados en un control de acceso.

7.9.3 Separación en las redes

La Entidad en referencia a la separación de redes, cumple con las siguientes actividades:

a. Garantizar que los servicios de información, usuarios y soluciones tecnológicas estén separados en diferentes redes.
b. Las redes están segmentadas, en las sedes físicas los servidores y los equipos de usuarios tanto cableados como inalámbricos no ocupan el mismo segmento.
c. En los servicios en nube se tienen segmentados las redes para los ambientes de desarrollo, pruebas y producción.
d. La información acerca del direccionamiento interno, segmentación de red y enrutamiento se encuentra clasificada como confidencial y solo personal autorizado puede acceder a la misma.
e. En la red de la Entidad se incorpora la separación lógica de las redes y el filtrado de tráfico que se intercambie en cada una de estas redes.

7.9.4 Políticas y Procedimientos de Transferencia de Información

La Dirección de Tecnologías y Sistemas de la Información, definirá una política de Transferencia de Información, de acuerdo con lo siguiente:

a. La transferencia de información debe ser realizada en medios controlados para prevenir código malicioso mediante el software antivirus autorizado para la Entidad.
b. Es responsabilidad del funcionario y/o contratista tomar las precauciones apropiadas de no revelar información confidencial de la Entidad.
c. En la transferencia de información se debe garantizar la protección de la información contra el acceso no autorizado durante su tratamiento tomando como referencia los controles criptográficos de referencia en el control 7.6 – Criptografía.

d. No se permite la transferencia de información a través de sitios web externos, ya sean gratuitos o de pago, que puedan poner en riesgo la confidencialidad e integridad de los datos

7.9.5 Acuerdos Sobre Transferencia de Información

La SDSCJ cuenta con cifrado simétrico para la transmisión de la información de sitio a sitio o de extremo a extremo, si se requiere añadir a una nueva Entidad para este tipo de comunicación se requiere realizar la solicitud a la Dirección de Tecnologías y Sistemas de la Información por medio escrito y recibir la autorización por escrito para el establecimiento de dicha comunicación.

7.9.6 Mensajería Electrónica

La SDSCJ cuenta con un sistema de correo electrónico en el dominio @scj.gov.co autorizado para el envío, transferencia y recepción oficial de comunicación electrónica entre funcionarios y contratistas de la Entidad y hacia el exterior.

Para comunicaciones internas y externas se cuenta con servicios de mensajería instantánea Microsoft TEAMS que es un centro de trabajo basado en chats, siendo el único canal autorizado para la comunicación fluida entre funcionarios y/o contratistas de la SDSCJ.

La mensajería electrónica de la Entidad posee controles de detección de correo electrónico no deseado, si un usuario llega a detectar un correo electrónico sospechoso o con contenido difamatorio, de suplantación u otras acciones no autorizadas por la Entidad deberá reportarlo a la Dirección de Tecnologías y Sistemas de la Información generando el respectivo caso en la mesa de servicio con el fin que se declare un incidente de seguridad de la información.

7.9.7 Acuerdos de Confidencialidad o de no Divulgación

La SDSCJ, estableció el formato F-GH-807 “Compromiso de Confidencialidad y No Divulgación de la Información”, para ser diligenciado por los funcionarios de la Entidad con el fin de aplicar normas legales y jurídicas referentes a la seguridad y privacidad de la información.

7.10 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

La seguridad y privacidad en los sistemas de información de la Entidad, debe cumplir con requisitos mínimos de gestión en ambientes seguros garantizando el desarrollo integral de los datos y el aseguramiento de la información sobres redes de área local y redes públicas.

La Entidad debe contar con controles de seguridad de la información como parte integral de los mismos en todo el ciclo de vida.

7.10.1 Análisis y especificación de requisitos de seguridad de la información

La Dirección de Tecnologías y Sistemas de la Información en referencia al análisis y especificación de requisitos de seguridad de la información para los nuevos sistemas de información o para las mejoras de los existentes, toma como referencia las siguientes acciones:

a. Identificar y documentar los requisitos específicos de seguridad de la información que son aplicables a los sistemas y aplicaciones en desarrollo.
b. Lidera los procesos de desarrollo de software para la Entidad, verificando los requisitos relacionados con seguridad de la Información desde las primeras etapas del desarrollo.

c. Aplicar buenas prácticas de seguridad de la información para el aseguramiento de los sistemas de información de la Entidad.
d. Generar conceptos técnicos y evaluación de requerimientos sobre procesos para adquisición de software de la Entidad.
e. El desarrollo de software debe realizarse de acuerdo con el procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software” de la Entidad.

7.10.2 Seguridad de servicios de las aplicaciones en redes públicas

La Dirección de Tecnologías y Sistemas de la Información en referencia a la seguridad de servicios de aplicaciones que pasan en redes públicas, se protege de actividades fraudulentas, divulgación y modificación no autorizada, alineado a los parámetros establecidos en el Instructivo I-GT-02 “Permisos y Navegación Web” en el que se define los controles de navegación con el fin de reducir riesgos y establecer controles para el uso apropiado a Internet.

Todas las soluciones tecnológicas publicadas en redes públicas se encuentran desplegadas en un segmento de red protegido mediante firewall perimetral y firewall de aplicaciones web (WAF).

7.10.3 Protección de Transacciones de los servicios de las aplicaciones

La Dirección de Tecnologías y Sistemas de la Información cuenta con mecanismos de seguridad adecuados para garantizar que la información involucrada en las transacciones realizadas por las aplicaciones de la Entidad en redes públicas se realice de forma segura, para ello se dispone del Firewall perimetral y firewall de aplicaciones Web (WAF) para el aseguramiento de las redes en mención.

7.10.4 Política de Desarrollo Seguro

La Dirección de Tecnologías y Sistemas de la Información, de acuerdo con lo establecido en el procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software” de la Entidad, desarrollará las siguientes actividades:

a. Aplicar el Manual de Desarrollo Seguro a cargo del grupo de Sistemas de Información en el desarrollo de software
b. Aplicar técnicas y metodologías para el desarrollo seguro de las aplicaciones como OWASP, para proteger los procesos transaccionales de los sistemas de información de la Entidad.
c. Incorporar métodos de seguridad de la información en el desarrollo de los sistemas de información en todas las fases del proyecto y ciclo de vida de la información, inclusive desde el mismo levantamiento del requerimiento.

7.10.5 Procedimiento de control de cambios en sistemas

La Dirección de Tecnologías y Sistemas de la Información, realiza cambios a los sistemas de información de acuerdo con lo definido en el procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software”, y el Procedimiento PD-GT-2 “Gestión de cambios”.

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

La Dirección de Tecnologías y Sistemas de la Información, garantiza la revisión técnica de los cambios realizados en la infraestructura y soluciones tecnológicas por parte de personal autorizado

para evitar fallas que afecten la disponibilidad de estos, informando los resultados al grupo de gestión de cambios de la Entidad para su respectiva documentación en las aplicaciones disponibles.

Cuando se cambian las plataformas de operación, se realiza la revisión y pruebas funcionales de las aplicaciones críticas del negocio, para asegurar que no haya impacto adverso en las operaciones o seguridad de la Entidad.

7.10.7 Restricciones en los cambios a los paquetes de software

Para los cambios o modificaciones a paquetes de software se debe verificar por parte de la Dirección de Tecnologías y Sistemas de la información:

a. El software sea licenciado y validar las condiciones de uso para el desarrollo de los cambios a lugar.
b. Los paquetes de software suministrados por el vendedor, proveedor y/o desarrollador, no hayan sufrido modificaciones.
c. Los escenarios usados para las pruebas y cambios por parte del personal de la Entidad deben ser estrictamente controlados
d. Si los cambios son necesarios, el software original se debería conservar, y los cambios se deberían aplicar a la copia designada.
e. Actualización de parches de seguridad más recientes para todo el software actualizado.

7.10.8 Principios de Construcción de los sistemas seguros

Los principios de construcción de los sistemas seguros se deberán establecer, documentar y mantener, los cuales se deben verificar con regularidad por parte de la Dirección de Tecnologías y Sistemas de la Información para asegurar que están agregando valor y mejoras a los estándares de seguridad dentro del proceso de construcción.

Los principios de construcción de seguridad de la información se deben aplicar, en donde sea pertinente, a sistemas de información contratados externamente, por medio de contratos y otros acuerdos vinculantes entre la Entidad y el proveedor.

7.10.9 Ambiente de desarrollo seguro

El ambiente de desarrollo seguro de la Entidad incluye personas, procesos y tecnología asociados con el desarrollo e integración de sistemas considerando los requisitos externos e internos aplicables.

El desarrollador ejecuta el código sobre equipos locales en ambientes de prueba, después el código es migrado a los repositorios centralizados, se deben implementar mecanismos de CI/CD para garantizar el flujo de las implementaciones y sus diferentes versiones.

7.10.10 Desarrollo contratado externamente

La Dirección de Tecnologías y Sistemas de la Información, supervisará y hará seguimiento, Cuando el desarrollo de sistemas es contratado externamente, considerando los requisitos y procedimientos de seguridad de la información descritos en este documento, así mismo como los estándares

descritos en los diferentes procedimientos establecidos en la Entidad, teniendo en cuenta los siguientes puntos en la cadena de suministro externa de la Entidad:

a. Acuerdos y alcance del licenciamiento.
b. Derechos de Propiedad de los códigos.
c. Derechos de propiedad intelectual.
d. Especificaciones técnicas y garantías.
e. Requisitos contractuales para prácticas seguras de diseño, codificación y pruebas.
f. Suministro del modelo de amenaza.
g. Ensayos de aceptación para determinar la calidad y exactitud de los entregables.

7.10.11 Pruebas de seguridad de los sistemas

La Dirección de Tecnologías y Sistemas de la Información, realiza las pruebas de seguridad (análisis de vulnerabilidades y brechas de seguridad), durante el desarrollo de paso a producción de los cambios y/o actualización de las soluciones tecnológicas de la Entidad.

7.10.12 Prueba de aceptación de sistemas

La Dirección de Tecnologías y Sistemas de la Información, debe verificar que se realice un plan formal de pruebas de aceptación y actualización de los nuevos sistemas de información o a los existentes antes de salida a producción, dicha aceptación debe involucrar a usuarios funcionales y pruebas de seguridad considerando capacidad de procesamiento, recuperación ante errores, restauración del sistema, documentación de proceso y cambios, así como capacitación de uso.

7.10.13 Protección de los datos de prueba

La SDSCJ a través de la Dirección de Tecnologías y Sistemas de la Información protegerá los datos de pruebas teniendo especial cuidado con la información catalogada como sensible, no se debe involucrar datos reales o bases de datos de producción en el ambiente de pruebas o de desarrollo, se debe utilizar datos transformados o mecanismos de anonimización de datos.

7.11 RELACIÓN CON LOS PROVEEDORES.

La SDSCJ, en referencia con la relación con los proveedores, garantiza el adecuado cumplimiento de los procedimientos de seguridad de la información, mediante las siguientes acciones.

7.11.1 Política de seguridad de la información para las relaciones con proveedores

Para el intercambio de información de propiedad de la Entidad, los proveedores deben cumplir los parámetros establecidos en el presente manual, la política de seguridad y privacidad de la información, las normas, procedimientos y estándares previstos., adicional a las cláusulas civiles y penales en caso de incumplimientos y demás normas vigentes.

7.11.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores

La Entidad establece los requisitos en el marco de la Política de Seguridad y Privacidad de la Información para cada proveedor garantizando los principios de la confidencialidad, integridad y

disponibilidad de la información, conforme a lo establecido en los contratos o servicios que se suscriban con cada uno de ellos.

7.11.3 Cadena de suministro de tecnología de información y comunicación

La Dirección de Tecnologías y Sistemas de la Información deberá definir los acuerdos de niveles de servicio y las especificaciones técnicas, así.

a. La disponibilidad del proveedor en la prestación de los servicios se define en los contratos establecidos, el proveedor deberá actuar con la máxima diligencia para que la información esté disponible de acuerdo con lo requerido por la Entidad.
b. El proveedor o tercero que preste servicios de desarrollo de software, debe implementar normas o prácticas en el desarrollo de las aplicaciones para garantizar la seguridad de los sistemas conforme a los lineamientos establecidos en la metodología OWASP.

7.11.4 Seguimiento y revisión de los servicios de los proveedores

Los líderes de proceso de la Entidad deberán supervisar y verificar el cumplimiento de las obligaciones contractuales, la calidad de los productos y/o servicios y el cumplimiento de los acuerdos de niveles de servicio establecidos con los proveedores a que haya lugar.

7.11.5 Gestión de cambios en los servicios de los proveedores.

La Dirección de Tecnologías y Sistemas de la Información, será la encargada de verificar y aprobar los cambios en el suministro de servicios que realicen los proveedores a la infraestructura tecnológica, soluciones tecnológicas y demás servicios tecnológicos que puedan afectar las políticas, procedimientos y controles de seguridad de la información, garantizando los principios de confidencialidad, integridad y disponibilidad de la información.

Los proveedores deberán ajustar las ventanas de mantenimiento de acuerdo con los procedimientos internos que la Entidad tiene establecido para tal fin en el procedimiento “PD-GT-02 - Gestión de Cambios”, que permita la unificación de criterios en los mantenimientos programados a las soluciones tecnológicas que corresponda.

7.12 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

Todo incidente de seguridad con la información, debe ser atendido, analizado, documentado y reportado por parte del personal encargado y establecido para tal fin por parte de la Dirección de Tecnologías y Sistemas de la Información, es deber de los usuarios finales realizar los reportes sobre eventos de seguridad de la información e informar si identifican debilidades relacionadas, para lo cual deben generar los casos con los respectivos los tickets de soporte a mesa de servicio para dar atención referente a seguridad de la información.

Se verificará y hará seguimiento por parte del profesional de seguridad de la Información de los eventos e incidentes de seguridad de la información reportados, velando que sean comunicados y atendidos oportunamente, de acuerdo con lo establecido en el procedimiento PD-GT-6-Procedimiento Gestión de Incidentes o Problemas.

7.12.1 Responsabilidades y procedimientos

La Dirección de Tecnologías y Sistemas de la Información, en referencia a responsabilidades y procedimientos de gestión establece el procedimiento interno PD-GT-6 “Procedimiento Gestión de Incidentes o Problemas”, donde se definen las acciones tendientes a contener, reportar, evaluar, mitigar y documentar el impacto de los eventos o incidentes de seguridad de la información.

7.12.2 Reporte de eventos de seguridad de la información

Todo los funcionarios y contratistas de la Entidad deberán reportar a la mesa de servicio, los posibles incidentes de seguridad de la información que afecten los principios de confidencialidad, integridad y disponibilidad a través de los medios autorizados para tal fin (Correo electrónico, llamada telefónica o herramienta de gestión), con el fin de crear un caso donde se documente toda la descripción del evento y las acciones tendientes a contener y mitigar el incidente.

7.12.3 Reporte de debilidades de seguridad de la información

Es responsabilidad de los funcionarios y contratistas que usan las soluciones tecnológicas reportar cualquier situación que se pueda considerar como una debilidad de seguridad de la información o que considere puede afectar la confidencialidad, disponibilidad e integridad de la información a través de la mesa de servicio con las evidencias respectivas que soporten la anomalía presentada.

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

La Dirección de Tecnologías y Sistemas de la Información, se encargará de evaluar y clasificar los eventos o incidentes de seguridad de la información, para luego gestionar, mitigar y documentar dichos incidentes.

7.12.5 Respuesta a incidentes de seguridad de la información

La Dirección de Tecnologías y Sistemas de la Información, será la responsable de dar respuesta a los incidentes de seguridad de la información de acuerdo con lo establecido en el procedimiento interno PD-GT-6 “Procedimiento Gestión de Incidentes o Problemas”, de la Entidad.

7.12.6 Aprendizaje obtenido de los incidentes de seguridad de la información

La Dirección de Tecnologías y Sistemas de la Información, a través de la herramienta de gestión, documenta la información de los incidentes de seguridad de la información reportados, con el fin de ser consultados con posterioridad y generar acciones de mejora que minimicen el impacto de futuros incidentes

7.12.7 Recolección de evidencia

Por parte de la Dirección de Tecnologías y Sistemas de la Información, se recolecta la evidencia, la cual debe cumplir con los procesos de identificación, recolección, adquisición y

preservación de acuerdo con lo establecido en el procedimiento interno PD-GT-6 “Procedimiento Gestión de Incidentes o Problemas”, así:

a. Reunir información básica (Lugar, tipo de información, datos de contacto de la persona que reporta) que llevó a determinar que es un posible incidente de seguridad de la información, información que podrá ser utilizada en la investigación.
b. Recopilar y documentar evidencias e información necesaria producto de la investigación del incidente a través del registro de la herramienta de control.
c. Se debe conservar las pruebas recopiladas, las cuales serán custodiadas por el gestor de incidentes de seguridad de la información, y posteriormente entregadas al director del área donde se reportó el correspondiente incidente de seguridad.
d. Evaluación de los costos, Incluir el nivel de consecuencia y costo del incidente.

7.13 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO

La Entidad proyecta los aspectos de continuidad de seguridad de la información de manera integrada con el sistema de gestión de la continuidad de negocio.

7.13.1 Planificación de la continuidad de la seguridad de la información

a. La SDSCJ debe contar con un plan de continuidad del negocio que contenga los aspectos de seguridad de la información, el cual permitirá a la Entidad definir las actividades necesarias para recuperar y restaurar las operaciones críticas de la Entidad.
b. La Dirección de Tecnología y Sistemas de Información debe establecer un plan de contingencia tecnológica que permita definir las actividades para recuperar y restaurar los sistemas y plataformas tecnológicas que soportan las operaciones críticas de la Entidad con el fin de prevenir las interrupciones en el negocio.

7.13.2 Implementación de la continuidad de la seguridad de la información

Con base en la planificación, la SDSCJ implementa el plan de continuidad del negocio, el cual debe estar debidamente documentado estableciendo los parámetros, procedimientos y controles para asegurar el nivel requerido de continuidad.

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

De acuerdo con la planificación e implementación del plan de continuidad, la SDSCJ deberá realizar la verificación y evaluación periódica definido para la Entidad, teniendo en cuenta los controles implementados de seguridad de la información.

7.13.4 Disponibilidad de instalaciones de procesamiento de información.

Con el fin de garantizar la disponibilidad de las soluciones tecnológicas y para efectos de redundancia, la Secretaría Distrital de Seguridad Convivencia y Justicia a través de la Dirección de Tecnologías y Sistemas de la Información, cuenta con servicios en la nube dispuestas para la operación tecnológica de la Entidad.

7.14 CUMPLIMIENTO

La SDSCJ, en referencia con el cumplimiento de requisitos legales, estatutarias, de reglamentación o contractuales, relacionadas con la seguridad de la información, teniendo en cuenta lo siguiente:

a. Establecer cláusulas contractuales entre la Entidad y cualquier funcionario, contratista, tercero, operador tecnológico o proveedor, en los cuales se especifiquen los compromisos de preservación de los derechos de autor y propiedad intelectual.
b. Establecer cláusulas en los contratos donde se defina el cumplimiento de los requisitos legales y contractuales.
c. Documentar toda la normativa vigente respecto a la seguridad de la información, con el fin de cumplir los requisitos legales y no incurrir en incumplimientos que pueden ocasionar inconvenientes mayores al cumplimiento de la misión.
d. El software que se ejecute en la Entidad está protegido por derechos de autor y cuenta con la licencia de uso y/o software de libre distribución, instalado a través de la mesa de servicio de la Entidad.
e. Los funcionarios y/o contratistas deben cumplir con las leyes de derechos de autor y los acuerdos de licenciamiento de software. No está permitida la duplicación, reproducción de software, ni de documentación sin previa autorización del propietario.
f. La Dirección de Tecnologías y Sistemas de la Información, verifica el cumplimiento de las políticas establecidas en este documento, registra los procedimientos, planes, manuales, instructivos, guías, protocolos, formatos y políticas específicas alineados a la norma técnica Colombiana NTC-ISO-IEC 27001:2013 y la normatividad vigente y aplicable a la Entidad.
g. Se define Política de Tratamiento de Datos Personales donde esté definido el tratamiento de los datos entregados por los usuarios que tengan relación con la Entidad.
h. Las revisiones independientes deben asegurar la conveniencia, adecuación y eficacia continua del enfoque de la organización para gestionar la seguridad de la información. Esta revisión deberá incluir la valoración de las oportunidades de mejora y la necesidad de efectuar cambios hacia la seguridad, incluyendo la política y los objetivos de control.
i. La Dirección de Tecnologías y Sistemas de la Información es la encargada de autorizar los cambios a la plataforma tecnológica de la Entidad.
j. Para autorizaciones y/o viabilidades de desarrollo y uso de soluciones tecnológicas en la Entidad, se requiere solicitud por parte del líder del proceso por medio de la mesa de servicio, la cual debe ser aprobada por la Dirección de Tecnologías y Sistemas de la Información.
k. La Dirección de Tecnologías y Sistemas de la Información realizará la revisión, implementación y mejora continua del Sistema de Gestión de Seguridad de la Información en la Entidad.

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
Edwin Castillo Ortiz – 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