ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

Dirección de Tecnologias y Sistemas de la Información

MANUAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

www.scj.gov.co

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. ÁMBITO DE APLICACIÓN 4
4. NORMATIVIDAD ASOCIADA 5
5. DOCUMENTOS ASOCIADOS 5
6. GLOSARIO 5
7. CONTROLES ORGANIZACIONALES 11
7.1 Políticas de seguridad de la información. 11
7.2 Roles y responsabilidades en la Seguridad de la Información. 11
7.3 Segregación de deberes. 11
7.4 Responsabilidades de la dirección 11
7.5 Contacto con las autoridades. 12
7.6 Contacto con grupos de interés especial. 13
7.7 Inteligencia de amenazas. 13
7.8 Seguridad de la Información en la gestión de proyectos. 13
7.9 Inventario de información y otros activos asociados. 14
7.10 Uso aceptable de la información y otros activos asociados. 15
7.11 Devolución de activos 15
7.12 Clasificación de la información. 15
7.13 Etiquetado de la información. 16
7.14 Transferencia de información. 16
7.15 Control de acceso 17
7.16 Gestión de identidades 18
7.17 Información de autenticación. 18
7.18 Derechos de acceso. 18
7.19 Seguridad de la información en las relaciones con proveedores. 19
7.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores. 20
7.21 Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC) 20
7.22 Seguimiento, revisión y gestión del cambio de los servicios de los proveedores. 20
7.23 Seguridad de la información para el uso de servicios en la nube. 21
7.24 Planificación y preparación de la gestión de incidentes de seguridad de la información. 21
7.25 Evaluación y decisión sobre eventos de seguridad de la información. 21
7.26 Respuesta a incidentes de seguridad de la información. 21
7.27 Aprender de los incidentes de seguridad de la información. 21
7.28 Recopilación de evidencias. 22
7.29 Seguridad de la información durante una interrupción. 22
7.30 Preparación de las TIC para la continuidad de negocio. 22
7.31 Requisitos legales, legales reglamentarios y contractuales 22
7.32 Derechos de propiedad intelectual. 23
7.33 Protección de registros. 23
7.34 Privacidad y protección de la información de identificación personal. 23
7.35 Revisión independiente de la seguridad de la información. 23
7.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información. 23

7.37 Procedimientos operativos documentados 24
8. CONTROLES DE PERSONAS. 24
8.1 Selección. 25
8.2 Términos y condiciones de empleo. 25
8.3 Conciencia de seguridad de la información, educación y formación. 25
8.4 Proceso disciplinario 26
8.5 Responsabilidades después de la terminación o cambio de empleo. 26
8.6 Acuerdos de confidencialidad o no divulgación. 27
8.7 Trabajo remoto 27
8.8 Informes de eventos de seguridad de la información. 28
9. CONTROLES FÍSICOS. 28
9.1 Perímetros de seguridad física 29
9.2 Entrada física. 29
9.3 Asegurar oficinas, habitaciones e instalaciones 29
9.4 Monitoreo de la seguridad física. 29
9.5 Protección contra amenazas físicas y ambientales 29
9.6 Trabajar en áreas seguras 30
9.7 Escritorio y pantalla limpios 30
9.8 Emplazamiento y protección de equipos 30
9.9 Seguridad de los activos fuera de las instalaciones. 31
9.10 Medios de almacenamiento 31
9.11 Servicios públicos de apoyo 31
9.12 Seguridad del cableado. 32
9.13 Mantenimiento de equipos 32
9.14 Disposición o reutilización segura de los equipos. 33
10. CONTROLES TECNOLOGICOS 33
10.1 Dispositivos de punto final de usuario 33
10.2 Derechos de acceso privilegiado 35
10.3 Restricción de acceso a la información. 35
10.4 Acceso al código fuente 35
10.5 Autenticación segura 36
10.6 Gestión de la capacidad. 37
10.7 Protección contra malware. 37
10.8 Gestión de vulnerabilidades técnicas. 37
10.9 Gestión de la configuración. 38
10.10 Eliminación de información. 38
10.11 Enmascaramiento de datos. 38
10.12 Prevención de fugas de datos. 38
10.13 Copia de seguridad de la información 39
10.14 Redundancia de las instalaciones de procesamiento de información. 39
10.15 Registro 39
10.16 Actividades de seguimiento. 39
10.17 Sincronización de reloj 40
10.18 Uso de programas de utilidad privilegiados. 40
10.19 Instalación de software en sistemas operativos 40
10.20 Seguridad de redes 41
10.21 Seguridad de los servicios de red 42

10.22 Segregación de redes. 42
10.23 Filtrado web. 43
10.24 Uso de la criptografía. 43
10.25 Ciclo de vida de desarrollo seguro. 44
10.26 Requisitos de seguridad de las aplicaciones. 44
10.27 Arquitectura de sistemas seguros y principios de ingeniería. 44
10.28 Codificación segura. 45
10.29 Pruebas de seguridad en el desarrollo y aceptación 45
10.30 Desarrollo externalizado. 45
10.31 Separación de entornos de desarrollo, evidencia y producción. 45
10.32 Gestión del cambio. 46
10.33 Información de las pruebas 46
10.34 Protección de los sistemas de información durante las pruebas de auditoría 46

1. OBJETIVO

Establecer las pautas y orientaciones necesarias para garantizar el cumplimiento de la Política de Seguridad y Privacidad de la Información, la cual debe ser conocida y aplicada por todos los funcionarios, contratistas y terceros vinculados con la Secretaría Distrital de Seguridad, Convivencia y Justicia, con el fin de proteger los principios de confidencialidad, disponibilidad e integridad de la información, en concordancia con las disposiciones legales y normativas vigentes.

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 y/o contractual 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. ÁMBITO DE APLICACIÓN

El ámbito de aplicación de este manual se extiende a todos los funcionarios, contratistas y terceros que interactúen con la información o tengan alguna responsabilidad sobre ella dentro de la Secretaría Distrital de Seguridad Convivencia y Justicia.

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 todas las soluciones e infraestructura tecnológicas utilizados por la Entidad, incluyendo redes de comunicaciones, servidores, equipos informáticos, dispositivos móviles y cualquier otro componente tecnológico que almacene, procese o transmita 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 Secretaría. De cualquier forma, 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

Ver Normas del proceso en https://portalmipg.scj.gov.co

5. DOCUMENTOS ASOCIADOS

- Política de Seguridad y Privacidad de la Información PO-GT-1
- Política de Tratamiento y Protección de Datos Personales PO-GCT-01
- Procedimiento de Gestión de Cambios PD-GT-2.
- Procedimiento Gestión de Incidentes o Problemas PD-GT-6.
- Gestión y Administración de Usuarios PD-GT-8.
- Matriz de roles y responsabilidades seguridad de la Información F-GT-953.

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: Según (MinTIC) Permisos y derechos especiales otorgados a ciertos usuarios para acceder, administrar, o realizar operaciones en sistemas críticos de una organización.

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.

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

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

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

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

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

Amenaza: Según (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.

Auditoría: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad de los controles de Seguridad de Información.

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.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por la Entidad 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.

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

ICC: La Infraestructura Crítica Cibernética 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.) 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.

Norma Técnica Colombiana NTC-ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO Es certificable. Primera publicación en 2005, segunda publicación en 2013, Tercera Publicación en 2022.

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.

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 y Privacidad: 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.

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.

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 ORGANIZACIONALES.

Los controles de referencia definidos a continuación corresponden a la Norma Técnica Colombiana NTC-ISO/IEC 27001:2022 – establecidos en la Entidad con el fin de preservar la confidencialidad, integridad y disponibilidad de la información.

7.1 Políticas de 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, 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.

7.2 Roles y responsabilidades en la Seguridad de la Información.

La SDSCJ, 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.

7.3 Segregación 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 y/o contractuales, esto con el fin de reducir y evitar el uso no autorizado o modificación no intencional sobre los activos de información.

7.4 Responsabilidades de la dirección

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

La Mesa técnica de seguridad digital es la instancia asesora para presentar recomendaciones técnicas, conceptualizaciones, valoraciones, y conceptos sobre seguridad de la información.

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.

7.5 Contacto con las autoridades.

La SDSCJ mantiene comunicación con las entidades competentes con el propósito de coordinar e intercambiar información relacionada con la gestión de incidentes de seguridad de la información.

Esta labor se realiza a través de la Dirección de Tecnologías y Sistemas de la Información, por medio del profesional de seguridad de la información o del funcionario que se designe, siguiendo lo establecido en el (PD-GT-6) Procedimiento de Gestión de Incidentes o Problemas, así como las actividades que puedan afectar o poner en riesgo la seguridad de la información de la Entidad, o que requieran dar respuesta a solicitudes 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	601295 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 6015159700 Ext. 30469 – 30468 dijin.cecip-jef@policia.gov.co 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: 6013813000 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	Sistema de Emergencia	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

Tabla 1. Listado de Contactos con autoridades.

7.6 Contacto con 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, es el encargado de realizar transferencia de conocimientos a las áreas de Entidad.

ACIS – Asociación Colombiana de Ingenieros de Sistemas	https://acis.org.co/
CISCO (Security consulting)	https://www.cisco.com/c/es_co/index.html
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/
Heimcore S.A.S	https://www.heimcore.com.co/

Tabla 2. Listado de Contactos con grupos de interés especial.

7.7 Inteligencia de amenazas.

La Entidad debe recopilar, analizar y utilizar inteligencia sobre amenazas relevantes para los sistemas de información, procesos y activos, con el fin de comprender los riesgos y mejorar la prevención, detección y respuesta ante incidentes de seguridad.

7.8 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.

7.9 Inventario de información y otros activos asociados.

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.

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 y clasificación de los activos de información de la Entidad es realizada por los líderes de proceso, 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 establecido en la Guía G-GD-01 “Guía de Gestión de Activos de Información e Índice de Información Clasificada y Reservada”. La información correspondiente se diligencia en el Formato F-GD-1081 “Registro de Activos de Información e Índice de Información Clasificada y Reservada”.
b. El inventario de activos de información de la Entidad deberá actualizarse con el acompañamiento de la Dirección de Recursos Físicos y Gestión Documental y la Dirección de Tecnologías y Sistemas de la Información, de manera anual o cuando se presenten cambios normativos vigentes. Esta actividad se realiza conforme a lo establecido en el artículo 13 de la Ley 1712 de 2014 – Registros de Activos de Información, el cual dispone que todo sujeto obligado debe crear y mantener actualizado el Registro de Activos de Información, elaborando 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 Recursos Físicos y Gestión Documental en coordinación con La Dirección de Tecnologías y Sistemas de la Información, a través del profesional de Seguridad de la Información, brindará acompañamiento técnico a los líderes de los 21 procesos institucionales —estratégicos, misionales, de apoyo y de evaluación— para la identificación, gestión y actualización de los activos de información de la Entidad, el cual es 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”.
d. La Dirección de Tecnologías y Sistemas de la Información será responsable de identificar, dentro del consolidado de activos de información de la Entidad, aquellos considerados críticos, así como la Infraestructura Crítica Cibernética, a fin de realizar sobre ellos la gestión de riesgos correspondiente, conforme a los lineamientos de la Política de Seguridad de la Información.

7.10 Uso aceptable de la información y otros activos asociados.

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 la política de seguridad y privacidad 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.

7.11 Devolución de activos

Los funcionarios, contratistas o partes externas que sean responsables o tengan asignados activos de información de la SDSCJ deberán restituirlos al finalizar su vínculo laboral, contractual o cualquier acuerdo con la Entidad, o cuando se produzcan modificaciones en sus funciones u obligaciones.

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

7.12 Clasificación de la información.

La SDSCJ clasifica la información considerando los requisitos legales, el valor, la criticidad y la susceptibilidad a divulgación o modificación no autorizada, de acuerdo con la Guía G-GD-01 “Guía de Gestión de Activos de Información e Índice de Información Clasificada y Reservada” y con lo establecido en la Ley 1712 de 2014 “Transparencia y Acceso a la Información Pública”, la Entidad divide la información en las siguientes categorías de clasificación:

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.

7.13 Etiquetado de la información.

El etiquetado de la información está a cargo de la Dirección de Recursos Físicos y Gestión Documental, conforme a las Tablas de Retención Documental vigentes, los lineamientos establecidos en el PG-GD-01 “Programa de Gestión Documental” y lo dispuesto en el ítem 7.2.1.6 “Clasificación y custodia de la información” de la Guía G-GD-01 “Guía de Gestión de Activos de Información e Índice de Información Clasificada y Reservada” de la Entidad.

7.14 Transferencia de información.

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.

a. La Dirección de Tecnologías y Sistemas de la Información, para las actividades de transferencia de Información, se realizan de acuerdo con lo siguiente:
   - ❖ La transferencia de información debe ser realizada en medios controlados para prevenir código malicioso mediante el software antivirus autorizado para la Entidad.
   - ❖ Es responsabilidad del funcionario y/o contratista tomar las precauciones apropiadas de no revelar información confidencial de la Entidad.
   - ❖ En la transferencia de información se debe garantizar la protección de la información contra el acceso no autorizado durante su tratamiento.
   - ❖ 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.
b. Respecto a la información que es solicitada por externos como (entes regulatorios) se debe considerar los siguientes parámetros:
   - ❖ Toda solicitud de entrega de información debe ser formal y cumplir con los requisitos establecidos por la ley. Las solicitudes deben ser claras, indicar el propósito y la razón por la cual se solicita la información, y ser emitidas por autoridades competentes.
   - ❖ Sólo debe entregarse la información cuando así lo exijan entes de control competentes y siempre conforme a lo establecido en la ley.
   - ❖ Si la solicitud incluye datos sensibles o confidenciales (por ejemplo, datos personales sensibles según la Ley 1581 de 2012), se debe evaluar si el solicitante tiene la autoridad para acceder a esos datos bajo las excepciones previstas en la ley.
   - ❖ Toda solicitud debe ser verificada formalmente, para asegurar que es legítima y que se ajusta a los requisitos legales. Esto incluye la validación de que el solicitante es un ente autorizado.
   - ❖ La entrega de información debe limitarse estrictamente a lo necesario, conforme al principio de minimización de datos y proporcionalidad, el cual establece que solo deben transferirse los datos imprescindibles para atender el propósito o la solicitud correspondiente; Cuando la

solicitud sea de carácter general, la entrega deberá restringirse exclusivamente a la información solicitada, evitando la divulgación de datos adicionales, salvo en los casos previstos por la ley, como el acceso a información clasificada o reservada, o la obligación de compartir datos con autoridades competentes en el marco de investigaciones, auditorías u otros procedimientos legales.

- La información solicitada debe entregarse de forma que garantice su seguridad y confidencialidad. Esto puede implicar el uso de canales seguros.

c. 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.

d. 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 comunicaciones electrónicas entre funcionarios, contratistas y entidades externas. No está permitida la creación de buzones de correo para agremiaciones, sindicatos u otras personas jurídicas ajenas a la SDSCJ, garantizando así el uso exclusivo del sistema de correo para fines institucionales.

Para comunicaciones internas y externas se cuenta con servicios de mensajería instantánea Microsoft Teams, reconocido como el único canal autorizado para la comunicación en tiempo real entre funcionarios y contratistas de la SDSCJ.

El uso de plataformas de mensajería no corporativas, tales como WhatsApp Web, Telegram, Messenger o servicios similares, no está permitido en los equipos institucionales para el uso o tratamiento de información de la Entidad, debido a los riesgos asociados a la pérdida de confidencialidad, interceptación de datos y exposición de información sensible; de manera excepcional, su utilización podrá ser autorizada por escrito por el jefe inmediato o responsable del proceso, cuando las condiciones operativas así lo requieran, dejando evidencia formal de dicha autorización mediante solicitud expresa a la mesa de servicio de la DTSI.

La mensajería electrónica institucional cuenta con controles de seguridad que incluyen detección de correo no deseado, suplantación y contenido malicioso; En caso de identificar mensajes sospechosos, difamatorios o no autorizados, el usuario deberá reportarlo de inmediato a la Dirección de Tecnologías y Sistemas de la Información, mediante la mesa de servicio, para la gestión del incidente de seguridad de la información conforme al procedimiento establecido.

7.15 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.

En relación con el control de acceso, la Entidad, considerando el contexto institucional y en línea con las mejores prácticas en seguridad de la información, establece un conjunto de actividades orientadas a garantizar la protección y confidencialidad de la información, alineándose con las normativas vigentes y los estándares internacionales.

7.16 Gestión de identidades

La SDSCJ gestiona las identidades digitales de funcionarios, contratistas y partes externas para asegurar que solo personal autorizado acceda a los sistemas y recursos de información disponibles.

La Dirección de Tecnologías y Sistemas de la Información administra el ciclo de vida de las cuentas de usuario (creación, modificación y eliminación) mediante la mesa de servicio, previa autorización del jefe inmediato, tomando como referencia el procedimiento GT-08 Procedimiento Gestión y Administración de usuarios.

Las cuentas son personales e intransferibles, y deben desactivarse inmediatamente al finalizar el vínculo con la Entidad.

Se realizan revisiones periódicas de accesos y permisos, aplicando los principios de mínimo privilegio y necesidad de acceso, garantizando la confidencialidad e integridad de la información institucional.

7.17 Información de autenticación.

De acuerdo con el procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios” de la SDSCJ, el manejo de cuentas de usuario y contraseñas es de carácter personal e intransferible. En consecuencia, cualquier operación que comprometa los intereses de la Entidad será responsabilidad directa del funcionario o contratista titular de las credenciales.

La Dirección de Tecnologías y Sistemas de la Información debe garantizar la protección de la información utilizada para los procesos de autenticación, asegurando su confidencialidad, integridad y disponibilidad. Las credenciales (contraseñas, claves, tokens o códigos) deben ser almacenadas y transmitidas de forma cifrada, evitando su exposición o divulgación no autorizada.

Los funcionarios y contratistas deberán emplear credenciales seguras para el ingreso a los servicios tecnológicos de la Entidad, de acuerdo con lo establecido en el ítem el control 10.5 Autenticación Segura del presente manual, y conforme a las políticas de seguridad definidas por la Entidad.

7.18 Derechos de acceso.

a. Suministro de acceso de usuarios.

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio, es responsable de la creación, modificación y eliminación de usuarios, contraseñas y privilegios de

acceso en la infraestructura y soluciones tecnológicas de la Entidad, conforme al procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”.

Los funcionarios y contratistas que requieran acceso a los recursos de información, servicios o soluciones tecnológicas de la SDSCJ deberán solicitar la creación de su usuario mediante la mesa de servicio, anexando la documentación requerida y el Formato F-GT-285 “Solicitud Administración de Usuarios” debidamente diligenciado y autorizado por el líder del proceso.

b. 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 y/o contratistas que impliquen modificación de derechos de acceso de usuarios a las soluciones tecnológicas, será reportado por parte de la Dirección de Gestión Humana y/o la Dirección Jurídica y Contractual y/o Dirección de Operaciones según sea el caso, a la Dirección de Tecnologías y Sistemas de la Información, para realizar los ajustes pertinentes en las soluciones tecnológicas.

c. 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”.

Todos los funcionarios o contratistas al finalizar la relación de servicios con la Entidad harán entrega de las credenciales, tarjeta de proximidad, carnet, 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 el formato F-GCT-1144 – “Control De Retiro Para Contratistas De Prestación De Servicios Personales ” definidos para tal fin.

7.19 Seguridad de la información en las relaciones con proveedores.

La DTSI debe asegurar que las relaciones con proveedores consideren los riesgos asociados al acceso, procesamiento, almacenamiento o transmisión de información de la Entidad.

Se deberán implementar medidas de control antes, durante y después de la relación contractual, garantizando que los proveedores cumplan con las políticas de seguridad y privacidad de la información, así como con los procedimientos internos establecidos.

El incumplimiento de estas disposiciones podrá generar sanciones contractuales y la suspensión o terminación de los servicios según lo estipulado en los acuerdos vigentes.

7.20 Abordar la seguridad de la información dentro de los acuerdos con proveedores.

La DTSI deberá asegurar que los contratos y acuerdos con proveedores incluyan cláusulas sobre confidencialidad, protección de datos, gestión de accesos y cumplimiento de las políticas de seguridad de la Entidad.

Cuando los proveedores requieran acceso a sistemas o servicios tecnológicos, deberán hacerlo con credenciales personales, seguras y temporales, conforme al procedimiento PD-GT-8 “Gestión y Administración de Usuarios” y los lineamientos del ítem 7.5.12 “Sistema de gestión de contraseñas”.

La DTSI verificará el cumplimiento de estos requisitos durante la vigencia del contrato y coordinará con las áreas responsables la atención de incidentes de seguridad que involucren a terceros.

7.21 Gestión de seguridad de la información en la cadena de suministro de la tecnología de la información y las telecomunicaciones (TIC)

La Dirección de Tecnologías y Sistemas de la Información sobre la en la cadena de suministro de la tecnología de la información y las telecomunicaciones, establece las siguientes actividades, así:

a. La disponibilidad del proveedor en la prestación de los servicios se establece en los contratos correspondientes. El proveedor deberá actuar con la debida diligencia para garantizar la disponibilidad de la información conforme a los requerimientos de 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 de acuerdo con lo establecido en el MA-GT-02 Manual de Desarrollo Seguro para garantizar la seguridad de los sistemas conforme a los lineamientos establecidos en la metodología OWASP.
c. 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.

7.22 Seguimiento, revisión y gestión del cambio de 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.

7.23 Seguridad de la información para el uso de servicios en la nube.

La SDSCJ establece lineamientos para garantizar la seguridad de la información alojada, procesada o gestionada en servicios de computación en la nube, asegurando el cumplimiento de los requisitos legales, contractuales y de seguridad institucional.

La Dirección de Tecnologías y Sistemas de la Información es responsable de evaluar, aprobar y supervisar el uso de servicios en la nube, verificando que los proveedores seleccionados cumplan con estándares de seguridad, confidencialidad, disponibilidad y protección de datos personales, conforme a la normativa vigente.

El uso de servicios en la nube no autorizados o sin aprobación de la Dirección de Tecnologías y Sistemas de la Información está prohibido, por los riesgos que representa para la seguridad y confidencialidad de la información institucional.

7.24 Planificación y preparación de la 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.

7.25 Evaluación y decisión sobre eventos de seguridad de la información.

La Dirección de Tecnologías y Sistemas de la Información se encargará de evaluar, clasificar y gestionar los eventos o incidentes de seguridad de la información, de acuerdo con lo establecido en el procedimiento interno PD-GT-6 “Gestión de Incidentes o Problemas”, con el fin de mitigar su impacto y documentar las acciones realizadas.

7.26 Respuesta a incidentes de seguridad de la información.

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

7.27 Aprender de los incidentes de seguridad de la información.

La Dirección de Tecnologías y Sistemas de la Información, a través de la herramienta de gestión institucional, documenta los incidentes de seguridad de la información reportados, con el propósito de facilitar su trazabilidad, análisis y la implementación de acciones de mejora que reduzcan el impacto de futuros incidentes.

7.28 Recopilación de evidencias.

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.

7.29 Seguridad de la información durante una interrupción.

a. La SDSCJ debe contar con un plan de continuidad del negocio a cargo de la Oficina Asesora de Planeación, 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.

7.30 Preparación de las TIC para la continuidad de negocio.

Con base en la planificación institucional, la SDSCJ implementa el Plan de Continuidad del Negocio, liderado por la Oficina Asesora de Planeación, el cual debe estar debidamente documentado y establecer los parámetros, procedimientos y controles necesarios para garantizar el nivel requerido de continuidad operativa de los servicios tecnológicos.

La Dirección de Tecnologías y Sistemas de la Información (DTSI) implementa medidas para asegurar la continuidad operativa de los servicios tecnológicos ante incidentes o fallas que puedan afectar la disponibilidad.

7.31 Requisitos legales, legales reglamentarios y contractuales

La SDSCJ cumple con los requisitos legales, reglamentarios y contractuales aplicables en materia de seguridad y privacidad de la información. La Dirección de Tecnologías y Sistemas de la Información vela por que todas las actividades, procesos y sistemas tecnológicos se desarrollen conforme a la normativa vigente, garantizando la protección adecuada de la información institucional y de los datos personales.

7.32 Derechos de propiedad intelectual.

La SDSCJ garantiza el respeto y cumplimiento de los derechos de propiedad intelectual relacionados con el software, contenidos digitales, bases de datos y cualquier otro activo de información utilizado en la Entidad. Todo software que se ejecute en los equipos institucionales debe contar con su respectiva licencia de uso o ser de libre distribución, y únicamente podrá ser instalado o actualizado por la Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio.

Asimismo, queda prohibida la instalación, copia o uso de software no autorizado o sin licencia, así como la reproducción o distribución no autorizada de material protegido por derechos de autor. La Entidad promueve el uso ético y legal de los recursos tecnológicos, velando por el cumplimiento de la normativa nacional sobre propiedad intelectual y las políticas internas de seguridad de la información.

7.33 Protección de registros.

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.

7.34 Privacidad y protección de la información de identificación personal.

La SDSCJ adopta medidas técnicas, administrativas y legales para garantizar la confidencialidad, integridad y disponibilidad de la información personal tratada en sus sistemas, conforme a la normatividad vigente en materia de protección de datos personales.

El tratamiento de información de identificación personal se realiza bajo los principios de legalidad, finalidad, libertad, veracidad, acceso y seguridad, evitando su divulgación o uso no autorizado.

7.35 Revisión independiente de la seguridad de la información.

La SDSCJ garantiza la realización de revisiones independientes de la seguridad de la información con el fin de evaluar la eficacia de los controles implementados y su alineación con las políticas y procedimientos institucionales.

7.36 Cumplimiento de políticas, reglas y estándares de seguridad de la información.

La SDSCJ, en referencia con el cumplimiento de políticas, reglas y estándares, 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 27001:2022 y la normatividad vigente y aplicable a la Entidad.
g. Se define la PO-GCT-01 - Política de Tratamiento y Protección 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. La Dirección de Tecnologías y Sistemas de la Información realizará la revisión, implementación y mejora continua del Modelo de Seguridad y Privacidad de Información de la Entidad.

7.37 Procedimientos operativos 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 de la DTSI incluyen la gestión de requerimientos de TI, Gestión de cambios de TIC, Gestión de proyectos de TI, Gestión de Incidentes o problemas, Gestión y Administración de usuarios, Gestión de Infraestructura y Plataformas Tecnológicas, Uso y Apropiación, Ciclo de vida de desarrollo de Software y gestión de datos abiertos.

8. CONTROLES DE PERSONAS.

La gestión de la seguridad de la información asociada al recurso humano abarca todas las etapas del ciclo de vinculación, desde la selección y verificación de antecedentes de funcionarios y contratistas, hasta la ejecución de sus funciones y la terminación o cambio de roles. Estas actividades deben realizarse conforme a los procedimientos definidos por el proceso de Gestión Humana y los lineamientos de seguridad y privacidad de la información de la Entidad.

Asimismo, se busca que todos los funcionarios y contratistas comprendan y asuman las responsabilidades, procedimientos y buenas prácticas establecidas para proteger la información institucional y minimizar los riesgos asociados al factor humano.

8.1 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 y la Dirección de Operaciones, según corresponda 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”, el MA-GCT-03 – Manual de Contratación y el procedimiento interno PD-GCT-03 “Perfeccionamiento y Legalización de los Contratos” y en base a los requerimientos de ley establecidos para tal fin.

8.2 Términos y condiciones de 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 “Política de Seguridad y Privacidad de la Información PO-GT-1”, “Manual De Seguridad y Privacidad de La Información” de la Entidad MA-GT-01.

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 y para los contratistas, se dispone de los formatos “Acuerdo De Confidencialidad Y Compromiso Con La Seguridad Y Privacidad De La Información De Contratistas F-GT-1610”.

8.3 Conciencia de seguridad de la información, educación y formación.

Con el fin de garantizar los principios de confidencialidad, integridad y disponibilidad de la información institucional, la DTSI desarrolla actividades de divulgación, sensibilización y formación en materia de seguridad de la información, promoviendo la comprensión e interiorización de la Política de Seguridad y Privacidad de la Información y otros lineamientos relevantes para todos los funcionarios y contratistas de la Entidad.

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, específicamente en temas de 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.

8.4 Proceso disciplinario

La Oficina de Control Disciplinario Interno de la Entidad ha establecido lineamientos en el marco del Código Único Disciplinario, los cuales han sido comunicados a todos los funcionarios y contratistas. El incumplimiento de las disposiciones relacionadas con la Seguridad y Privacidad de la Información podrá generar la aplicación de sanciones disciplinarias, contractuales o legales, conforme a la normatividad vigente.

8.5 Responsabilidades después de la terminación o cambio 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 es responsable de notificar a la Dirección de Tecnologías y Sistemas de la Información (DTSI), mediante los medios autorizados (correo electrónico institucional, herramienta de gestión o ticket en la mesa de servicio), todas las novedades relacionadas con los funcionarios y contratistas, tales como vacaciones, incapacidades médicas, suspensiones o finalización del vínculo laboral. Esta comunicación permite gestionar oportunamente el bloqueo o suspensión de los privilegios de acceso a las soluciones tecnológicas de la Entidad, según corresponda.

b. Los supervisores de contratos son responsables de notificar a la mesa de servicio de la Dirección de Tecnologías y Sistemas de la Información (DTSI), mediante los medios autorizados (correo electrónico institucional, herramienta de gestión o ticket en la mesa de servicio), la terminación del vínculo contractual de los contratistas, con el fin de gestionar la desactivación de usuarios y privilegios de acceso en las soluciones tecnológicas de la Entidad.

c. Cuando un funcionario o contratista cambie de rol dentro de la Entidad, sus accesos a los activos de información deberán ajustarse conforme al nuevo perfil asignado. Los activos que ya no correspondan a sus funciones deberán permanecer en la dependencia de origen y ser entregados al jefe inmediato o supervisor del contrato, según corresponda.

d. Asimismo, en caso de cambio de dependencia, el jefe o director de la dependencia de origen deberá solicitar a la mesa de servicio de la (DTSI) la desactivación de los permisos de acceso que no sean necesarios en la nueva asignación.

e. Al finalizar la relación laboral o contractual con la Entidad, todos los funcionarios y contratistas deberán realizar la entrega de credenciales, tarjetas de proximidad, carné, información institucional y demás elementos asignados para el desarrollo de sus funciones, ante la Dirección de Gestión Humana o la Dirección de Recursos Físicos y Gestión Documental, según corresponda. Esta entrega se efectuará conforme a los trámites establecidos para la obtención de paz y salvo institucional, de acuerdo con el procedimiento PD-GH-18 “Retiro del servicio de los servidores públicos” y, en el caso de los contratistas, mediante el diligenciamiento y trámite del formato F-GCT-1144 “Control de Retiro para Contratistas de Prestación de Servicios Personales”

8.6 Acuerdos de confidencialidad o no divulgación.

La Entidad estableció el formato F-GH-807 “Compromiso de Confidencialidad y No Divulgación de la Información”, el cual debe ser diligenciado por los funcionarios para garantizar el cumplimiento de las normas legales y jurídicas relacionadas con la seguridad y privacidad de la información.

Para los contratistas, se dispone de los formatos F-GT-1610 “Acuerdo De Confidencialidad Y Compromiso Con La Seguridad Y Privacidad De La Información De Contratistas” y/o F-GT-1609 “Compromiso De Confidencialidad Y No Divulgación De La Información” (Según el caso), que aseguran el mismo compromiso en el manejo responsable y confidencial de la información institucional.

8.7 Trabajo remoto

La SDSCJ establece las 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:

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.

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 (DTSI), con el propósito de facilitar las modalidades de teletrabajo, trabajo en casa y trabajo remoto, ha dispuesto los servicios y recursos tecnológicos necesarios para garantizar la continuidad operativa, la seguridad de la información y el acceso controlado a los sistemas institucionales desde ubicaciones externas:

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 acceso a las soluciones tecnológica de la Entidad.
- 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 o trabajo en casa, serán los responsables de propender la confidencialidad, integridad y disponibilidad de la información.

8.8 Informes de eventos de seguridad de la información.

Todos los funcionarios y contratistas de la Entidad deberán reportar a la mesa de servicio cualquier incidente de seguridad de la información que pueda afectar los principios de confidencialidad, integridad o disponibilidad, utilizando los medios autorizados (correo electrónico institucional, llamada telefónica o herramienta de gestión). El reporte permitirá la creación de un caso en el que se documente la descripción del evento, las acciones realizadas y las medidas adoptadas para contener, mitigar y prevenir futuros incidentes.

En caso de que algún componente de la infraestructura tecnológica de la Entidad (como sitios web, aplicaciones, servicios en línea o sistemas de información) sea vulnerado o comprometido, el profesional de Seguridad de la Información deberá informar de manera inmediata al ColCERT (Grupo de Respuesta a Emergencias Cibernéticas de Colombia), a través del correo electrónico contacto@colcert.gov.co, conforme a lo establecido en el Protocolo de Gestión de Incidentes de la Información para el Distrito Capital y los procedimientos internos vigentes.

9. CONTROLES FÍSICOS.

Los controles físicos implementados en la SDSCJ tienen como propósito proteger los activos de información, infraestructuras tecnológicas y recursos asociados frente a accesos no autorizados, daños, interferencias o pérdida. Estos controles buscan garantizar que las instalaciones de la Entidad cuenten con medidas adecuadas de seguridad, vigilancia y control de acceso, minimizando los riesgos que puedan comprometer la confidencialidad, integridad y disponibilidad de la información.

9.1 Perímetros 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 SDSCJ, 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.

9.2 Entrada física.

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 y lo establecido en el documento MA-GE-1 “Manual Operativo del C4”.

9.3 Asegurar oficinas, habitaciones e instalaciones

Las instalaciones de la SDSCJ cuentan con un servicio de vigilancia y seguridad privada contratado por la Entidad, cuyo personal aplica protocolos y lineamientos establecidos para salvaguardar la integridad física de las instalaciones y controlar el acceso de personas y bienes. Estas acciones se desarrollan conforme a lo dispuesto en el instructivo I-GRF-04 “Acceso a las Instalaciones de Funcionamiento de la SDSCJ”.

9.4 Monitoreo de la seguridad física.

La SDSCJ cuenta con un contrato suscrito con un proveedor externo para la prestación de servicios de vigilancia y monitoreo de seguridad física, que incluyen el funcionamiento de cámaras de videovigilancia, rondas de seguridad y control de accesos, con el fin de garantizar la protección de las instalaciones y de los activos institucionales.

9.5 Protección contra amenazas físicas y ambientales

La SDSCJ en referencia a la Protección contra amenazas externas y ambientales, tomará en cuenta los siguientes parámetros:

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.

9.6 Trabajar en áreas seguras

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 del C4”.

9.7 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 tendrá en cuenta las siguientes actividades:

a. La información tipificada como clasificada o reservada no debe estar a disposición de terceros.
b. Guardar documentos bajo llave y conservar escritorios libres de documentación.
c. Retirar documentos impresos y darle manejo apropiado.
d. Los equipos de cómputo tendrán parametrizado el cierre de sesión por inactividad de acuerdo con directivas establecidas en el directorio activo para tal fin.
e. 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.
f. La Dirección de Tecnologías y Sistemas de la Información, establece unas reglas de Directorio Activo de bloqueo por inactividad de 240 segundos cuando los equipos están desatendidos.
g. 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.

9.8 Emplazamiento y protección de 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.

9.9 Seguridad de los 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.

9.10 Medios de almacenamiento

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 Tecnología” 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.

9.11 Servicios públicos de apoyo

La SDSCJ en referencia a servicio públicos de apoyo, 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.

9.12 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 NTC-2050, 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.

9.13 Mantenimiento de equipos

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

a. Todo requerimiento realizado por los usuarios deberá ser registrado y documentado por la mesa de servicio, conforme a los procedimientos establecidos y a las características de la solicitud, permitiendo su trazabilidad, gestión y seguimiento.
b. Todo requerimiento de soporte técnico deberá ser gestionado y atendido conforme a lo establecido en el procedimiento interno PD-GT-1 "Procedimiento de Gestión de

Requerimientos de TI" de la Entidad, garantizando la correcta atención, seguimiento y cierre de cada solicitud.

c. El personal autorizado será el responsable de realizar las reparaciones y mantenimiento de los equipos de procesamiento de información, garantizando el cumplimiento de los lineamientos técnicos y de seguridad establecidos por la Entidad.

9.14 Disposición o reutilización segura de los 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 emitir concepto sobre el estado de los equipos tecnológicos de la Entidad, dejando constancia de dicha evaluación en el formato F-GT-422 "Concepto Técnico de Elementos de Tecnología", conforme a los lineamientos establecidos por la Entidad.
b. Todo equipo asignado a un funcionario o contratista deberá ser entregado debidamente formateado, garantizando la eliminación total de la información del usuario anterior y el cumplimiento de las políticas de seguridad y privacidad de la información de la Entidad.
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 Recursos Físicos y Gestión Documental, de acuerdo con lo definido en el procedimiento interno PD-GRF-08 "Reintegro Baja y Destinación Final".

10. CONTROLES TECNOLOGICOS

La SDSCJ implementa controles tecnológicos orientados a garantizar la protección, integridad y disponibilidad de la información institucional. Estos controles permiten prevenir, detectar y responder ante incidentes que puedan comprometer la seguridad de los sistemas y datos.

10.1 Dispositivos de punto final de usuario

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.

a. **Dispositivos móviles.**

La SDSCJ en el marco de la Política de Seguridad y Privacidad de la Información, establece los parámetros sobre los dispositivos móviles que permita gestionar de manera eficaz los riesgos ocasionados por la ejecución de actividades laborales y/o contractuales a través de dispositivos móviles.

Se consideran dispositivos móviles todos aquellos equipos tales como computadores portátiles, teléfonos celulares (smartphones), tabletas, agendas digitales, cámaras fotográficas, cámaras de video, proyectores (video beam), tarjetas de control de acceso, entre otros, que pertenecen o se encuentran asignados a la SDSCJ para el desarrollo de sus actividades institucionales.

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

- Monitorear los dispositivos móviles propiedad de la Entidad asignados a 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 que puedan generar riesgos o pérdidas de información.
- Disponer de control de acceso y segregación de red para los dispositivos móviles que se conecten a la red de la SDSCJ.
- Disponer de controles de acceso (contraseña, patrón o huella) en los dispositivos móviles propiedad de la Entidad o en calidad de arriendo. En caso de que el dispositivo o equipo portátil sea propiedad del funcionario o contratista que maneje información institucional, este deberá mantener un control de acceso por contraseña, contar con software antivirus actualizado y cumplir con los protocolos de seguridad establecidos en el presente Manual, con el propósito de salvaguardar la confidencialidad de la información de la Entidad.
- 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.
- 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 manejada, tendrán acceso restringido para dispositivos móviles, limitando su uso, manejo o la toma de material fotográfico y/o de video, con el fin de asegurar la confidencialidad de la información, garantizar el debido proceso, preservar la cadena de custodia, proteger los datos personales y prevenir el uso indebido de la información. Asimismo, el uso, procesamiento, descarga, entrega o manejo de grabaciones de audio o video, en cualquiera de sus formatos, deberá contar con autorización previa del director o jefe de la dependencia correspondiente, o realizarse únicamente mediante requerimiento por orden judicial pertinente.

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

- 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.

- ❖ 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.
- ❖ 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.

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

- ❖ 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.
- ❖ 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.

10.2 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.

10.3 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”.

10.4 Acceso al código fuente

La Dirección de Tecnologías y Sistemas de la Información es responsable de establecer y aplicar controles que restrinjan el acceso al código fuente de los sistemas desarrollados o mantenidos por la Entidad.

El acceso al código fuente solo será autorizado a personal expresamente designado, de acuerdo con sus funciones y bajo los principios de necesidad y mínima privilegio.

El código fuente se almacenará en repositorios seguros con control de versiones, autenticación y registro de auditoría de todas las actividades realizadas sobre él, garantizando su integridad, trazabilidad y disponibilidad.

Toda modificación o liberación de código deberá realizarse conforme al procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software”, aplicando prácticas de desarrollo seguro y revisiones por pares antes de su despliegue en ambientes productivos.

10.5 Autenticación segura

La Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicio y conforme al procedimiento interno PD-GT-8 “Gestión y Administración de Usuarios”, entrega a cada funcionario y contratista un usuario y contraseña como medio de autenticación para el ingreso seguro a las distintas soluciones y servicios tecnológicas. Con base en la información del directorio activo, se establecen los siguientes lineamientos para la 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.
   e. 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.
   f. Cambio de las contraseñas iniciales o temporales después del primer uso.
   g. Bloqueo de cuentas después de cinco intentos de inicio de sesión fallidos.
   h. Implementación de sesiones de autenticación con tiempo límite de inactividad de cinco minutos.
   i. Uso de recaptcha para los sistemas que permita su integración.

3. Sistemas de autenticación mediante el 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.

10.6 Gestión de la capacidad.

La Entidad realizará 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.

10.7 Protección contra malware.

La Entidad cuenta con herramientas de seguridad como antivirus, antispam, antispyware, seguridad perimetral y otras soluciones tecnológicas que brindan protección contra código malicioso, con el fin de prevenir la divulgación, modificación o daño permanente de la información ocasionados por el ingreso o propagación 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, manteniendo instaladas las actualizaciones y parches de seguridad vigentes, con el fin de prevenir la divulgación, modificación o daño permanente de la información ocasionados por el ingreso o propagación de software malicioso.

La Entidad restringirá el acceso a la red y a los servicios desde equipos que sean identificados como potencialmente peligrosos o que no cumplan con estos requisitos de seguridad.

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.

10.8 Gestión de 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.

10.9 Gestión de la configuración.

La DTSI es responsable de establecer y mantener procedimientos para la gestión de la configuración de los activos tecnológicos de la Entidad, garantizando la integridad, disponibilidad y trazabilidad de los cambios realizados.

Toda configuración en las soluciones tecnológicas de la Entidad deberá estar documentada, actualizada y sujeta a controles de cambio conforme al procedimiento interno PD-GT-2 “Gestión de Cambios de TIC”, asegurando que las modificaciones se realicen de forma controlada y autorizada.

Los cambios o modificaciones a los paquetes de software deben realizarse bajo condiciones seguras y verificables. Se debe confirmar que el software sea licenciado, que los paquetes suministrados por los proveedores o desarrolladores no hayan sido alterados, y que los entornos utilizados para pruebas estén debidamente controlados.

Se conservarán registros de las versiones, componentes y configuraciones implementadas, con el fin de facilitar la identificación de desviaciones, restaurar configuraciones previas y prevenir incidentes de seguridad derivados de cambios no autorizados.

10.10 Eliminación de información.

La DTSI, es la responsable de garantizar la eliminación segura de la información cuando ya no sea requerida para fines operativos, legales o contractuales, evitando su recuperación o uso no autorizado.

Toda actividad de eliminación deberá quedar registrada, asegurando trazabilidad y evidencia del proceso ejecutado.

10.11 Enmascaramiento de datos.

La Dirección de Tecnologías y Sistemas de la Información deberá garantizar el cuidado de la información catalogada como sensible, evitando que en los ambientes de prueba o desarrollo se utilicen datos reales o provenientes de bases de datos de producción. Para estos entornos, se deberán emplear datos transformados, anonimizados o técnicas de enmascaramiento, con el fin de proteger la confidencialidad y privacidad de la información, reduciendo el riesgo de exposición o uso indebido de datos personales o institucionales.

10.12 Prevención de fugas de datos.

La DTSI implementa controles técnicos para prevenir la fuga o exposición no autorizada de información, incluyendo mecanismos de prevención de pérdida de datos, cifrado de información, monitoreo de red, bloqueo de puertos y gestión de accesos.

Se restringe el uso de dispositivos y servicios en la nube no autorizados, aplicando políticas de transferencia segura y almacenamiento controlado.

Los eventos relacionados con posibles fugas de información deberán ser reportados y gestionados conforme al procedimiento de gestión de incidentes de seguridad de la información.

10.13 Copia de seguridad de la información

La SDSCJ en referencia al respaldo de información, establece 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. Además, se debe establecer una solución inmediata hasta que el proceso de respaldo funcione correctamente, garantizando la integridad y disponibilidad de la información
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.

10.14 Redundancia de las instalaciones de procesamiento de información.

La Dirección de Tecnologías y Sistemas de la Información implementa medidas de respaldo y disponibilidad que permitan mantener la operación de los sistemas tecnológicos ante posibles fallas o interrupciones. Estas acciones incluyen copias de seguridad, redundancia en servicios críticos y mecanismos de recuperación que se establezcan en el Plan de Continuidad y Contingencia de la Entidad, garantizando la prestación continua de los servicios institucionales.

10.15 Registro

Todas las actividades realizadas bajo los diferentes roles en las soluciones tecnológicas deberán registrarse en un log de auditoría, el cual se implementará como una práctica estándar en todas las plataformas y sistemas de la Entidad, sin depender de la solicitud de los analistas funcionales.

Este registro deberá incluir las acciones ejecutadas por administradores, operadores y demás usuarios con privilegios, permitiendo un seguimiento completo, trazable y verificable de las operaciones realizadas. La revisión, análisis y gestión de estos registros estará a cargo de los analistas funcionales, quienes deberán garantizar el cumplimiento de las políticas de acceso y seguridad de la información definidas por la Entidad.

10.16 Actividades de seguimiento.

La Dirección de Tecnologías y Sistemas de la Información realiza actividades de monitoreo y seguimiento continuo sobre las soluciones tecnológicas de la Entidad, con el fin de detectar

eventos anómalos, fallas o incidentes de seguridad. Estas acciones permiten tomar medidas preventivas o correctivas oportunas, conforme a lo establecido en los procedimientos internos del proceso Gestión de Tecnologías de la Información.

10.17 Sincronización de reloj

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

a. Los relojes de todos los sistemas de procesamiento de información deben estar sincronizados de acuerdo con el Instituto Nacional de Metrología de Colombia (INM).
b. Los relojes de todos los sistemas de procesamiento de información deben estar sincronizados de acuerdo con el Instituto Nacional de Metrología de Colombia (INM). Adicionalmente, se permite la sincronización con servidores de sincronización confiables de fabricantes, siempre que cumplan con estándares de precisión y confiabilidad. Como los servidores de sincronización de Oracle, y la infraestructura de servidores de sincronización de Fortinet, garantizando así la consistencia temporal en cada plataforma específica para los casos de infraestructura que corresponda.
c. Asimismo, los equipos de cómputo de la Entidad se sincronizarán con el controlador de dominio institucional. No está permitida la desactivación del sistema de sincronización ni la manipulación manual de la hora en ningún equipo, garantizando así la integridad y consistencia de la sincronización horaria en toda la infraestructura de la Entidad.
d. El ajuste correcto de los relojes de computador es necesario para la exactitud de los registros de auditoría (logs).

10.18 Uso de programas de utilidad 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 software.

10.19 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 deben 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.

10.20 Seguridad de redes

La Dirección de Tecnologías y Sistemas de la Información en referencia a los controles para proteger la información de las soluciones tecnológicas gestiona y controla 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 el equipo de infraestructura tecnológica de la DTSI 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 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.

10.21 Seguridad de los servicios de red

La Dirección de Tecnologías y Sistemas de la Información (DTSI) establece lineamientos para garantizar la seguridad, disponibilidad y confidencialidad de los servicios y redes de comunicación de la SDSCJ.

a. Los equipos y componentes de red, incluyendo los ubicados en sedes arrendadas, estarán bajo la administración del personal designado por la DTSI, quien garantizará su mantenimiento, actualización y correcta configuración. Solo se habilitarán los servicios estrictamente necesarios, y todo acceso remoto deberá contar con autorización expresa de la Dirección.
b. Los equipos o servicios expuestos hacia la red externa se ubicarán en una zona desmilitarizada (DMZ), protegidos mediante firewalls y sistemas WAF, conforme a las políticas de seguridad de la Entidad. Los acuerdos de transmisión de información con terceros deberán incorporar mecanismos seguros como VPN, cifrado asimétrico o autenticación por contraseña, asegurando la integridad y protección de los datos.
c. Todo funcionario, contratista, proveedor o usuario externo que requiera acceso a la red deberá autenticarse con credenciales institucionales y, según el nivel de criticidad, usar conexiones cifradas. Las solicitudes de acceso a servicios o sitios web no institucionales se tramitan a través de la mesa de servicios, con la respectiva autorización del jefe inmediato y validación del profesional de seguridad de la información.
d. Las conexiones remotas hacia la red de la Entidad o los servicios en la nube deberán realizarse exclusivamente mediante VPN seguras, aprobadas, registradas y auditadas por la DTSI, utilizando la herramienta oficial y desde equipos verificados como seguros. Cualquier dispositivo identificado como riesgoso por las plataformas de seguridad será bloqueado para proteger la integridad de la red.
e. En cuanto a las redes inalámbricas, la DTSI mantiene puntos de control de acceso con autenticación institucional, cifrado robusto y contraseñas seguras, permitiendo su uso únicamente con fines institucionales. La red Wi-Fi principal está destinada a equipos institucionales registrados en el dominio de la SDSCJ, mientras que el acceso de funcionarios o contratistas con equipos personales se habilita mediante conexión VPN. El personal externo podrá acceder únicamente a la red de invitados, limitada a la navegación en internet, previa coordinación con la mesa de servicios.

10.22 Segregación de redes.

La Entidad en referencia a la segregación 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.

10.23 Filtrado web.

La Entidad implementa controles de filtrado web para garantizar un uso seguro y apropiado de Internet, evitando el acceso a sitios maliciosos o no relacionados con las funciones laborales.

La Dirección de Tecnologías y Sistemas de la Información protege las aplicaciones y servicios en redes públicas frente a actividades fraudulentas o divulgación no autorizada, conforme al Instructivo I-GT-02 “Permisos y Navegación Web”.

Todas las soluciones tecnológicas expuestas en redes públicas están en segmentos protegidos mediante firewall perimetral y WAF, y las solicitudes de acceso a páginas no institucionales se gestionan por la mesa de servicios, previa autorización y validación del área de seguridad de la información.

10.24 Uso de la criptografía.

El propósito es garantizar el uso adecuado de la criptografía para proteger la confidencialidad, autenticidad e integridad de la información de la Entidad. La Dirección de Tecnologías y Sistemas de la Información define los parámetros y controles criptográficos necesarios para su almacenamiento y transmisión segura:

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 el envío 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.
g. Se deberán seleccionar los algoritmos de cifrado, tipos de llaves y su funcionalidad conforme a los lineamientos de controles criptográficos, definiendo el tiempo de vida del mecanismo de cifrado, especificando las llaves o parámetros antes de su uso y emisión, y procediendo a su modificación o regeneración en caso de compromiso.

h. Las claves podrán ser modificadas cuando se identifique un posible compromiso, se encuentren próximas a vencer o vencidas, o cuando sea necesario actualizar el algoritmo criptográfico utilizado en la VPN o en otros sistemas de cifrado de la Entidad.

10.25 Ciclo de vida de desarrollo seguro.

La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, implementa los lineamientos establecidos en el procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software”, garantizando el control de acceso, la gestión y la seguridad del código fuente.

La Entidad cuenta con un repositorio centralizado y controlado de versiones, administrado por el grupo de Sistemas de Información, el cual utiliza herramientas como Git para almacenar, gestionar y versionar los desarrollos realizados, asegurando que solo el personal autorizado tenga acceso según los roles asignados.

Asimismo, se aplican las disposiciones del MA-GT-02 - Manual de Desarrollo Seguro y metodologías reconocidas como OWASP, con el fin de integrar la seguridad en todas las fases del ciclo de vida del software, desde el levantamiento del requerimiento hasta su implementación y mantenimiento.

El ambiente de desarrollo seguro de la Entidad comprende personas, procesos y tecnología orientados a la protección de los sistemas de información. El código se desarrolla en ambientes locales de prueba y se migra posteriormente a los repositorios centralizados, implementando mecanismos de Integración Continua y Entrega Continua (CI/CD) que garantizan el control, la trazabilidad y la calidad de las implementaciones, fortaleciendo así la seguridad de la información institucional.

10.26 Requisitos de seguridad de las aplicaciones.

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.

10.27 Arquitectura de sistemas seguros y principios de ingeniería.

Los principios de construcción de los sistemas seguros se deberán establecer, documentar y mantener de acuerdo con lo establecido en el MA-GT-02 - Manual de Desarrollo Seguro, 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.

10.28 Codificación segura.

La Dirección de Tecnologías y Sistemas de la Información aplica prácticas de codificación segura para prevenir vulnerabilidades durante el desarrollo de software, conforme al procedimiento interno PD-GT-17 “Ciclo de Vida de Desarrollo de Software” y al Manual MA-GT-02 “Desarrollo Seguro”.

El equipo de desarrollo incorpora controles de seguridad desde las fases iniciales del proyecto, aplicando lineamientos OWASP y mecanismos de revisión de código para detectar y corregir errores que puedan comprometer la confidencialidad, integridad o disponibilidad de la información.

10.29 Pruebas de seguridad en el desarrollo y aceptación

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.

La DTSI, debe verificar que se realice 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.

10.30 Desarrollo externalizado.

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.

10.31 Separación de entornos de desarrollo, evidencia y producción.

La Dirección de Tecnologías y Sistemas de la Información, a través del 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.

Los ambientes separados de producción, pruebas y desarrollo se validarán de acuerdo con el sistema de información por sus características, costos operacionales y funcionalidades. Se implementarán los ambientes de producción y de pruebas para cada sistema. Las necesidades de los ambientes de desarrollo requerirán ser viabilizados de acuerdo con los costos y necesidades de cada sistema, debidamente justificado.

10.32 Gestión del cambio.

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.

a. 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.

10.33 Información de las pruebas

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. Asimismo, se controlará el acceso a los entornos de prueba, limitándolo únicamente al personal autorizado y asegurando que toda la información procesada mantenga la confidencialidad e integridad requeridas.

10.34 Protección de los sistemas de información durante las pruebas de auditoría

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.

Elaboró: Diego Mauricio Usme González – Contratista SDSCJ.

Revisó: Jairo Alonso Bohórquez Blanco – Profesional Especializado 222-27.
Francisco Javier Vargas Moncada - Profesional Universitario 219-18.
Diana Camila Méndez Restrepo – Contratista SDSCJ
Diana Carolina Hernandez – Contratista SDSCJ
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