ALCALDÍA MAYOR DE BOGOTÁ D.C.

BOGOTÁ

POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección de Tecnologias y Sistemas de la Información

2025

ALCALDÍA MAYOR DE BOGOTÁ D.C.

SECRETARÍA DE SEGURIDAD, CONVIVENCIA Y JUSTICIA

BOGOTÁ

POLÍTICA ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

CONTENIDO

1. INTRODUCCIÓN.

La Secretaría Distrital de Seguridad, Convivencia y Justicia en adelante la SDSCJ, en atención a los lineamientos establecidos en la Norma Técnica Colombiana NTC ISO/IEC 27001:2022, establece en el presente documento las Políticas Específicas de Seguridad y Privacidad de la Información, que constituyen el marco orientador para la gestión segura, responsable y controlada de la información institucional.

Estas políticas se enmarcan en el Sistema de Gestión de Seguridad de la Información (SGSI) y tienen como propósito proteger los activos de información frente a amenazas internas y externas, garantizando su confidencialidad, integridad, disponibilidad.

El documento consolida los lineamientos aplicables a los distintos ámbitos de la seguridad de la información, tales como la organización interna, la gestión de activos, el control de accesos, la seguridad física, la gestión de incidentes, la continuidad del negocio y la protección de los datos personales, entre otros.

Su aplicación será operacionalizada mediante el Manual de Seguridad y Privacidad de la Información de la Entidad, el cual orienta la puesta en práctica de los lineamientos aquí definidos dentro de los procesos institucionales.

La Entidad reafirma su compromiso con la mejora continua del SGSI, el cumplimiento de los requisitos legales y regulatorios, y la consolidación de una cultura organizacional basada en la protección y uso responsable de la información.

OBJETIVO

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

2. ALCANCE

La SDSCJ gestiona todos los activos de información, incluyendo la información en medios físicos y electrónicos que almacene, produzca, intercambie y gestione. Para ello implementa controles físicos, lógicos y de ciberseguridad, garantizando una gestión efectiva de riesgos y un proceso de mejora continua que permita fortalecer la confidencialidad, integridad y disponibilidad de la información.

El alcance de esta política incluye además la interoperabilidad, la gestión de servicios ciudadanos digitales y la articulación con otros sistemas y plataformas del Estado, conforme a los lineamientos de la Política de Gobierno Digital y demás requisitos legales y normativos. Estas

acciones contribuyen al cumplimiento misional de la Entidad y permiten el uso seguro, confiable y oportuno de la información.

3. GLOSARIO

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.

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

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

DTSI: Dirección de Tecnologías y Sistemas de la Información.

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

Norma Técnica Colombiana NTC-ISO 27001:2022: Estándar para la implementación del sistema de gestión de la seguridad de la información adoptado por ISO.

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

Principios de Seguridad de la información: Confidencialidad, Disponibilidad e Integridad.

SDSCJ: Secretaría Distrital de Seguridad, Convivencia y Justicia.

SGSI: (Sistema de Gestión de Seguridad de la Información). Según (MinTIC) es un conjunto de

políticas, procedimientos, controles y procesos diseñados para gestionar, proteger y garantizar la confidencialidad, integridad y disponibilidad de la información en una organización, basado en estándares como la ISO/IEC 27001:2022.

4. POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN.

Las Políticas Específicas de Seguridad y Privacidad de la Información establecen las directrices particulares que orientan la gestión de la seguridad de la información dentro de la Entidad. Cada una de las políticas descritas en los subnumerales de este capítulo constituye una política independiente y formal, definida para abordar un aspecto específico de la seguridad o privacidad de la información.

A diferencia del Manual de Seguridad y Privacidad de la Información, en el cual se establecen y describen todos los controles adoptados de la Norma Técnica Colombiana NTC ISO/IEC 27001:2022 y el marco general del Sistema de Gestión de Seguridad de la Información, estas políticas específicas desarrollan lineamientos puntuales para su aplicación y cumplimiento.

Todas las políticas se fundamentan en los principios de confidencialidad, integridad y disponibilidad, y se encuentran alineadas con los controles definidos en la NTC ISO/IEC 27001:2022.

Adicionalmente, estas políticas deberán ser revisadas, evaluadas y actualizadas de manera periódica, al menos una vez al año o cuando se presenten cambios normativos, tecnológicos, organizacionales o de riesgos, con el fin de garantizar su vigencia, pertinencia y eficacia dentro del Sistema de Gestión de Seguridad de la Información, así:

4.1. Organización interna.

a. Objetivo.

Establecer las directrices que garanticen una adecuada estructura organizacional, asignación de responsabilidades y coordinación de las actividades relacionadas con la seguridad y privacidad de la información, asegurando la implementación eficaz del Sistema de Gestión de Seguridad de la Información (SGSI) en todos los niveles de la Entidad.

b. Lineamientos.

1. Definir y mantener actualizada la estructura organizacional responsable de la gestión de la seguridad y privacidad de la información.
2. Asignar roles y responsabilidades claras al personal involucrado en la administración del SGSI, asegurando su conocimiento y cumplimiento.
3. Fomentar la comunicación y coordinación entre las dependencias que intervienen en la gestión de la información y los activos institucionales.
4. Asegurar la independencia y objetividad en las funciones de auditoría, evaluación y control del SGSI.
5. Promover la adopción de decisiones sobre seguridad de la información basadas en la gestión del riesgo y en el cumplimiento normativo aplicable.

6. Garantizar que las responsabilidades en materia de seguridad y privacidad se encuentren formalizadas mediante actos administrativos o documentos institucionales.

4.2. Escritorio Limpio y bloqueo de Pantallas.

a. Objetivo.

Establecer los lineamientos y prácticas necesarias para proteger la información institucional frente a accesos no autorizados, pérdidas o divulgaciones indebidas, mediante la implementación de prácticas de escritorio limpio y bloqueo de pantallas en los puestos de trabajo, tanto físicos como virtuales.

b. Lineamientos.

1. Mantener los escritorios, equipos y áreas de trabajo libres de materiales o elementos que contengan información clasificada como confidencial, salvo cuando estén siendo utilizados por personal autorizado, quien deberá asegurar su adecuada protección en todo momento.
2. Los funcionarios y contratistas deberán mantener su puesto de trabajo y escritorio virtual u operativo organizado y libre de archivos o información institucional que pueda ser visualizada, copiada o eliminada por personal no autorizado.
3. Está prohibido el consumo de alimentos o bebidas en áreas donde se manipule información institucional en papel, equipos de cómputo o dispositivos electrónicos, para evitar eventos que puedan comprometer la integridad de los activos de información.
4. Los funcionarios y contratistas deberán bloquear su sesión de usuario al ausentarse del puesto de trabajo y, al finalizar la jornada laboral, cerrar las aplicaciones y apagar el equipo, salvo en casos debidamente justificados, como la ejecución de procesos automatizados o trabajo remoto.
5. La información impresa o almacenada en medios magnéticos clasificada como confidencial deberá permanecer asegurada mediante mecanismos físicos de protección cuando no se encuentre en uso.
6. Los funcionarios con acceso a información clasificada en formato físico deberán prevenir su exposición o divulgación a personas no autorizadas, incluso dentro de espacios compartidos o modulares.
7. La información digital clasificada o reservada deberá ser almacenada únicamente en los repositorios institucionales asignados, garantizando la aplicación de controles de acceso y permisos restringidos conforme a los roles definidos.
8. Los documentos impresos en los servicios institucionales de impresión deberán ser retirados de forma inmediata por el usuario responsable.

4.3. Dispositivos Móviles y Trabajo en Casa.

a. Objetivo.

Establecer las directrices para el uso seguro de dispositivos móviles y el desarrollo de actividades bajo la modalidad de trabajo en casa o teletrabajo, con el fin de proteger la información institucional, minimizar los riesgos asociados al acceso remoto y garantizar la continuidad operativa bajo condiciones seguras.

b. Lineamientos.

I. Dispositivos móviles

1. Los dispositivos móviles únicamente podrán acceder a la información autorizada por los responsables de los procesos, conforme a los niveles de clasificación y los permisos definidos por la Entidad.
2. Los funcionarios y contratistas deberán proteger físicamente los dispositivos móviles asignados, sean propiedad o arrendamiento de la Entidad, evitando su pérdida, hurto o acceso no autorizado.
3. De acuerdo con el nivel de Importancia del Activo de información almacenada en los dispositivos, se deberá realizar copias de respaldo periódicas, conforme a los controles establecidos.
4. Toda conexión de dispositivos móviles a las redes de datos institucionales deberá gestionarse a través de la mesa de servicio, una vez se verifique el cumplimiento de los parámetros técnicos y de seguridad definidos por la Entidad.
5. Los dispositivos móviles deberán configurarse con mecanismos de autenticación seguros, bloqueo automático por inactividad, antivirus actualizado y restricciones de instalación de software no autorizado.
6. Los usuarios deberán utilizar exclusivamente las soluciones tecnológicas y recursos institucionales autorizados, absteniéndose de almacenar información sensible en dispositivos personales o medios externos.
7. Para efectos de esta política, se consideran dispositivos móviles los computadores portátiles, equipos celulares (smartphones), tabletas, agendas digitales, cámaras fotográficas o de video, proyectores, tarjetas de control de acceso y demás equipos tecnológicos asignados o propiedad de la Entidad.

II. Trabajo en casa

1. La modalidad de trabajo en casa o teletrabajo se aplicará a los funcionarios o contratistas cuyas funciones puedan desarrollarse fuera de las instalaciones de la Entidad, siempre que cuenten con los medios tecnológicos y condiciones seguras para el manejo de la información.
2. Todo acceso remoto deberá realizarse a través de canales seguros definidos por la Entidad (VPN institucional).
3. Los colaboradores bajo esta modalidad deberán garantizar la confidencialidad, integridad y disponibilidad de la información que gestionen, aplicando las mismas medidas de seguridad establecidas para el entorno corporativo.
4. Se deberá mantener un entorno de trabajo doméstico o alternativo adecuado, que evite la exposición de información institucional a terceros no autorizados.

5. Los funcionarios y contratistas deberán cumplir con los lineamientos y controles establecidos en el Manual de Seguridad y Privacidad de la Información, así como en las políticas institucionales aplicables.

4.4. Seguridad de los recursos humanos.

a. Objetivo.

Establecer las directrices para garantizar que todos los funcionarios, contratistas y terceros comprendan sus responsabilidades en materia de seguridad y privacidad de la información antes, durante y después de su vinculación con la Entidad, con el fin de reducir los riesgos asociados a errores humanos, uso indebido o acciones malintencionadas que puedan comprometer la información institucional.

b. Lineamientos.

1. La Entidad deberá asegurar que todos los funcionarios y contratistas conozcan y comprendan las políticas y procedimientos relacionados con la seguridad y privacidad de la información antes de asumir sus funciones.
2. Los procesos de selección de personal deberán incluir la verificación de antecedentes y certificaciones de experiencia de acuerdo con los perfiles de cargo y los niveles de acceso a la información requeridos.
3. Todo funcionario, contratista o tercero con acceso a información institucional deberá firmar compromisos de confidencialidad y de cumplimiento de las políticas de seguridad y privacidad de la información.
4. Los roles y responsabilidades en materia de seguridad de la información deberán estar claramente definidos y documentados en los perfiles de cargo o contratos respectivos.
5. Se deberán desarrollar programas de capacitación, inducción y sensibilización permanentes para fomentar la cultura de protección de la información institucional y el cumplimiento de la normativa vigente.
6. Los funcionarios y contratistas deberán reportar de inmediato cualquier evento, anomalía o incidente que pueda afectar la seguridad de la información, a través de la mesa de servicio.
7. En los procesos de desvinculación, terminación de contrato o cambio de funciones, la Entidad deberá asegurar la revocación de accesos, devolución de activos y cumplimiento de las obligaciones de confidencialidad establecidas.
8. La Entidad promoverá una conducta ética y responsable en el manejo de la información, velando por la prevención de conflictos de interés, fraudes o uso indebido de los recursos tecnológicos institucionales.
9. Todo funcionario o contratista deberá proteger la información que le sea confiada y utilizarla únicamente para los fines institucionales autorizados.

4.5. Gestión de Activos

a. Objetivo.

Establecer las directrices para la adecuada identificación, clasificación, inventario, uso, mantenimiento, protección y disposición final de los activos de información de la Entidad, asegurando su confidencialidad, integridad y disponibilidad durante todo su ciclo de vida.

b. Lineamientos.

1. Todos los activos de información de la SDSCJ deben ser identificados, registrados y valorados de acuerdo con su clasificación y custodia, conforme a las categorías establecidas en el Manual de Seguridad y Privacidad de la Información y en la guía de gestión de activos de información e índice de información clasificada y reservada.
2. La identificación y actualización del inventario de activos se debe realizar de forma anual o cuando se presenten cambios relevantes en la normatividad, la estructura organizacional o el mapa de procesos de la SDSCJ.
3. Los propietarios de la información son responsables de mantener actualizado el inventario o matriz de activos, asegurando su revisión periódica y la implementación de controles de seguridad adecuados.
4. Los custodios y usuarios finales deberán garantizar el uso responsable y seguro de los activos de información dispuestos por la Entidad, atendiendo las disposiciones establecidas en las políticas institucionales.

4.6. Control de acceso.

a. Objetivo.

Establecer las directrices para garantizar que el acceso a los sistemas, servicios, Soluciones tecnológicas y activos de información de la SDSCJ sea autorizado, controlado y monitoreado, asegurando que solo las personas debidamente acreditadas accedan a la información conforme a sus funciones y niveles de responsabilidad.

b. Lineamientos.

1. La SDSCJ, a través de la Dirección de Recursos Físicos y Gestión Documental, establece y mantiene los controles necesarios para asegurar que únicamente el personal autorizado tenga acceso a las áreas de trabajo y zonas restringidas, incluyendo el Centro de Datos, Archivo y demás áreas designadas como de acceso controlado.
2. Las dependencias de la Entidad, con apoyo de la Dirección de Tecnologías y Sistemas de la Información, son responsables de definir e implementar los controles, procedimientos e instructivos para la provisión y gestión de accesos a las soluciones tecnológicas, asegurando la asignación de permisos conforme a las funciones y responsabilidades de los usuarios.
3. La Dirección Jurídica y Contractual, la Dirección de Gestión Humana, la Dirección de Operaciones para el Fortalecimiento y los supervisores de contratos comunican de forma

oportuna a la Dirección de Tecnologías y Sistemas de la Información para informar las novedades de ingreso, cambio o retiro de funcionarios y contratistas, con el fin de activar, modificar o revocar los derechos de acceso a los sistemas y recursos tecnológicos.

4. Los accesos físicos y lógicos deberán ser gestionados conforme al principio de privilegio mínimo, evitando la asignación de permisos innecesarios o excesivos.
5. Se deberán aplicar mecanismos de autenticación robusta, tales como contraseñas seguras, autenticación multifactor (MFA) y bloqueo de sesión por inactividad, de acuerdo con los lineamientos del Manual de Seguridad y Privacidad de la Información.
6. Queda prohibido el uso compartido de credenciales, contraseñas o cuentas genéricas que no permitan la trazabilidad del usuario.
7. Los accesos de personal externo (soporte técnico) deberán ser temporales, autorizados y supervisados por la dependencia responsable, y deberán registrarse para fines de auditoría.
8. Todo acceso deberá ser registrado, monitoreado y revisado periódicamente, con el fin de identificar intentos de acceso no autorizado o comportamientos anómalos.
9. Las credenciales de acceso a los servicios de red y a Soluciones Tecnológicas (usuario y clave) son de carácter personal e intransferible; los funcionarios y contratistas de la SDSCJ no deben revelar éstas a terceros ni utilizar claves ajenas y serán responsable del cambio de clave de acceso periódicamente.

4.7. Seguridad física y del entorno.

a. Objetivo.

Proteger las instalaciones, equipos, activos de información y personal de la SDSCJ contra amenazas físicas, ambientales o de acceso no autorizado, garantizando la continuidad de las operaciones y la integridad de la información institucional.

b. Lineamientos.

1. La SDSCJ, a través de la Dirección de Recursos Físicos y Gestión Documental, implementará controles destinados a proteger el perímetro de las instalaciones físicas, gestionar el acceso del personal y su permanencia dentro de las oficinas e instalaciones, y controlar el ingreso a áreas restringidas donde se procese o almacene información clasificada, reservada o crítica para la operación institucional.
2. Se deberán aplicar medidas para mitigar los riesgos y amenazas externas o ambientales, garantizando la seguridad de los activos, los sistemas de información y las infraestructuras de soporte.
3. No se permitirá el ingreso de funcionarios, contratistas, proveedores o terceros a áreas restringidas con dispositivos móviles o electrónicos que permitan la captura de fotografías, video o audio, salvo autorización expresa, con el fin de proteger la información institucional, la confidencialidad de los datos personales, la integridad de la cadena de custodia y el buen nombre de la Entidad.

4. Todos los funcionarios, contratistas, proveedores o visitantes deberán acatar las disposiciones de la Entidad sobre acceso físico, portar en lugar visible su identificación vigente y cumplir los controles definidos para su tipo de vinculación.
5. En el caso del Centro de Comando, Control, Comunicaciones y Cómputo (C4), la Cárcel Distrital de Varones y Anexo de Mujeres, el Centro Especial de Reclusión (CER) y el Centro de Traslado por Protección (CTP), la administración de los controles de acceso restringido estará a cargo de los respectivos responsables de cada instalación. Los directores o jefes de oficina deberán realizar seguimiento permanente a su cumplimiento y reportar de inmediato cualquier novedad o incidente que afecte la seguridad de la información a la Dirección de Tecnologías y Sistemas de la Información.

4.8. Operaciones.

a. Objetivo.

Establecer las directrices necesarias para la operación segura, controlada y continua de los sistemas de información y los recursos tecnológicos de la SDSCJ, protegiendo la información institucional frente a fallas, accesos no autorizados, incidentes o interrupciones que puedan afectar la confidencialidad, integridad o disponibilidad de los servicios.

b. Lineamientos.

1. La Dirección de Tecnologías y Sistemas de la Información será responsable de la operación y administración de los recursos tecnológicos que soportan la gestión institucional, velando por la implementación de controles técnicos y administrativos que mitiguen los riesgos asociados a la infraestructura tecnológica y los sistemas de información.
2. Se deberá implementar un plan de copias de seguridad que proteja la información crítica alojada en el centro de datos de la Entidad y en los servicios en la nube, garantizando su recuperación ante desastres y su disponibilidad continua.
3. Se deberán implementar controles de protección contra códigos maliciosos, incluyendo soluciones antivirus, análisis de comportamiento y monitoreo continuo de vulnerabilidades, con el fin de prevenir, detectar y responder ante posibles infecciones o ataques.
4. Se deberán establecer procedimientos documentados para la ejecución segura de las operaciones, incluyendo la gestión de cambios, gestión de infraestructura tecnológica, gestión de incidentes, gestión de requerimientos de TI, gestión y administración de usuarios.
5. Se deberán proveer los recursos técnicos y humanos necesarios para implementar los controles que garanticen la seguridad y continuidad operativa de los sistemas de información.
6. Los cambios en configuraciones, software o infraestructura tecnológica deberán ser evaluados, aprobados y registrados de acuerdo con el procedimiento de gestión de cambios antes de su implementación, minimizando el impacto en la operación institucional.

7. Las actividades de respaldo, mantenimiento y monitoreo deberán ser ejecutadas únicamente por personal autorizado, debidamente capacitado y con acceso restringido a las funciones asignadas.
8. Los registros de auditoría (logs) deberán conservarse asegurando su integridad, disponibilidad y confidencialidad.
9. Las soluciones tecnológicas deben someterse periódicamente a pruebas de seguridad y gestión de vulnerabilidades para identificar y corregir debilidades técnicas antes de que sean explotadas.
10. Los procesos automatizados y herramientas de administración deberán contar con controles que prevengan el uso indebido de privilegios administrativos o la ejecución de tareas críticas sin autorización.

4.9. Seguridad de las comunicaciones.

a. Objetivo.

Establecer las directrices que permitan fortalecer las condiciones de confidencialidad, integridad, disponibilidad de la información durante su transmisión, intercambio o almacenamiento temporal a través de los distintos medios de comunicación utilizados por la Entidad.

b. Lineamientos.

1. Se establecerán los Acuerdos de Niveles de Servicio (ANS) con los proveedores de conectividad y de soporte de infraestructura de red, para garantizar la disponibilidad y continuidad de los servicios de red e internet en todas las sedes de la Entidad.
2. Establecer el uso de mecanismos de cifrado y protocolos seguros para la transmisión de información sensible o confidencial, tanto en redes internas como externas.
3. Implementar la autenticación, autorización y trazabilidad de los usuarios que acceden a los servicios de comunicación de la Entidad, incluyendo correo electrónico, VPN, servicios en la nube y demás canales habilitados.
4. Asegurar la segregación y protección de las redes institucionales, implementando controles perimetrales y de monitoreo que detecten y mitiguen incidentes de seguridad.
5. Controlar y registrar el acceso remoto a los recursos tecnológicos, asegurando que únicamente se realice por canales autorizados y cifrados.
6. Implementar procedimientos para la gestión segura de incidentes relacionados con las comunicaciones, garantizando la notificación y respuesta oportuna ante eventos que afecten la seguridad de la información.
7. Fomentar el uso responsable de los recursos de comunicación institucional, evitando la divulgación no autorizada de información y asegurando el cumplimiento de las políticas internas de seguridad.

I. Uso del Correo Electrónico Institucional

8. El correo institucional con dominio @scj.gov.co es de uso personal, intransferible y exclusivamente institucional. Está prohibido su uso para fines personales, comerciales o ajenos a la operación de la Entidad.

9. Los correos sospechosos de phishing, spam o software malicioso deberán reportarse de inmediato a la mesa de servicio y serán tratados como incidentes de seguridad.
10. El envío masivo de mensajes deberá realizarse únicamente por los canales oficiales definidos por la Oficina Asesora de Comunicaciones o las áreas autorizadas.
11. La Entidad se reserva el derecho de monitorear el uso del correo institucional para garantizar el cumplimiento de las políticas de seguridad.

II. Acceso a Internet.

1. La Dirección de Tecnologías y Sistemas de la Información establece controles de seguridad en las redes de comunicación internas y externas de la Entidad, definiendo conexiones seguras para el acceso a Internet desde y hacia los activos de información, estableciendo perfiles de navegación según roles y funciones, y garantizando la protección frente a accesos no autorizados, ataques o interceptaciones.
2. La Dirección de Tecnologías y Sistemas de la Información podrá restringir el acceso, establecer límites de ancho de banda, derechos de descarga y horarios de uso, velando por el uso racional y seguro del servicio de Internet.
3. Se prohíbe el acceso o consulta de páginas web con contenido ofensivo, injurioso, obsceno o que vulnere los derechos de autor, así como el uso de herramientas para evadir los controles de navegación o las políticas de seguridad.
4. La descarga de archivos no autorizados o material no institucional desde Internet o correo electrónico está prohibida y será tratada como incidente de seguridad.
5. En los casos donde la operación sea administrada por un operador tecnológico, este deberá implementar los controles necesarios y conexiones seguras para el acceso a Internet, bajo la supervisión de la Dirección de Tecnologías y Sistemas de la Información.

III. Uso y control de equipos tecnológicos institucionales

1. Todos los equipos suministrados por la SDSCJ deberán contar, como mínimo, con un usuario y una contraseña de acceso individual. Esta contraseña será de uso personal e intransferible, siendo el funcionario o contratista responsable del uso, custodia y confidencialidad de las credenciales asignadas.
2. Los dispositivos tecnológicos asignados a funcionarios y contratistas deberán utilizarse exclusivamente para el desarrollo de actividades laborales relacionadas con sus funciones y obligaciones.
3. Está prohibida la instalación de software no autorizado o sin licenciamiento. Solo el personal de la mesa de servicio podrá realizar instalaciones, actualizaciones o reparaciones.
4. Todo contenido, información o archivo almacenado en los equipos institucionales deberá cumplir con los derechos de autor y las licencias aplicables. Se prohíbe almacenar, reproducir o utilizar material que vulnere disposiciones legales o normativas relacionadas con la propiedad intelectual
5. Los equipos deben contar con antivirus activo, actualizaciones automáticas y software con licencias vigentes, administrados por la DTSI.

6. Cuando se presenten ausencias de funcionarios y/o contratistas por incapacidades, vacaciones, licencias, suspensiones de contrato u otras causas, se deberá realizar el bloqueo temporal o definitivo de sus accesos a los sistemas de información, con el fin de prevenir la exposición, alteración o uso indebido de la información, así como la posible suplantación de identidad. La Dirección de Gestión Humana, la Dirección Jurídica y Contractual, la Dirección de Operaciones para el Fortalecimiento y los respectivos supervisores de contrato deberán notificar de manera oportuna dichas ausencias a la Dirección de Tecnologías y Sistemas de la Información, a través de la mesa de servicios, para la ejecución del bloqueo correspondiente.

IV. Cableado Estructurado y Conectividad.

1. En las sedes de la SDSCJ donde exista cableado estructurado, las tomas eléctricas ubicadas en canaletas deberán destinarse únicamente a la conexión de equipos tecnológicos institucionales, como computadores, monitores y teléfonos IP.
2. Los computadores deberán conectarse a las tomas eléctricas reguladas con respaldo de UPS (color naranja), quedando prohibido el uso de dichas tomas para otros dispositivos eléctricos o personales.
3. No se permite a los usuarios instalar, conectar o derivar dispositivos de red tales como switches, hubs o puntos de acceso inalámbrico (Access Point), ni realizar extensiones de red o derivaciones eléctricas no autorizadas.
4. Los operadores tecnológicos que administren la infraestructura de red deberán cumplir con los estándares técnicos de cableado estructurado y redes eléctricas definidos por la Dirección de Tecnologías y Sistemas de la Información (DTSI).
5. Toda conexión a la red institucional o a servicios de Internet deberá estar previamente autorizada y supervisada por la DTSI, incluyendo aquellas realizadas por operadores tecnológicos o terceros contratistas.

V. Sistemas de Información y Conexiones Externas.

1. Solo podrán estar expuestas a Internet las soluciones tecnológicas que deban ser consultadas por usuarios externos autorizados; todas las demás deberán operar de forma interna o mediante conexiones seguras (VPN), previa autorización de la Dirección de Tecnologías y Sistemas de la Información y del jefe inmediato del solicitante.
2. Cuando la operación de los sistemas de información esté a cargo de un operador tecnológico externo, toda conexión externa deberá ser previamente autorizada y controlada por la DTSI.
3. Los sistemas o soluciones tecnológicas administrados por terceros deberán cumplir con los lineamientos del Manual de Seguridad y Privacidad de la Información de la SDSCJ y con los requisitos contractuales de seguridad definidos por la Entidad.
4. Las bases de datos utilizadas por las soluciones tecnológicas de la Entidad sean internos o administrados por un operador tecnológico, serán de propiedad de la SDSCJ, salvo disposición contractual diferente. En tales casos, deberá garantizarse la confidencialidad, integridad y disponibilidad de los datos, así como el tratamiento y protección de datos personales.

5. La interoperabilidad con otros sistemas de información del Estado deberá realizarse siguiendo los estándares establecidos en la política de Gobierno Digital y los requisitos de seguridad definidos por la Entidad.

4.10. Adquisición, desarrollo y mantenimiento de sistemas.

a. Objetivo.

Establecer los lineamientos que garanticen que la adquisición, desarrollo, mantenimiento y actualización de los sistemas de información de la SDSCJ se realicen bajo criterios de seguridad, asegurando la confidencialidad, integridad y disponibilidad de la información institucional durante todo su ciclo de vida.

b. Lineamientos.

1. La Dirección de Tecnologías y Sistemas de la Información está autorizada para la adquisición, desarrollo, administración, mantenimiento e implementación de herramientas, Soluciones tecnológicas, sistemas de información y demás software utilizado por la SDSCJ, asegurando la incorporación de buenas prácticas de desarrollo seguro y estándares de seguridad de información.
2. En los casos donde otras dependencias de la Entidad requieran adquirir soluciones tecnológicas, el proceso deberá contar con el visto bueno previo de la Dirección de Tecnologías y Sistemas de la Información, con el fin de verificar el cumplimiento de los requisitos de seguridad, compatibilidad y sostenibilidad técnica.
3. Cuando el desarrollo o mantenimiento de sistemas de información sea administrado por un operador tecnológico o contratista, este deberá implementar los mecanismos necesarios para proteger la información bajo su responsabilidad, garantizando la confidencialidad, integridad y disponibilidad de los datos institucionales; Implementando medidas que eviten el uso de datos de producción en ambientes de desarrollo, pruebas o certificación
4. Todos los desarrollos, adquisiciones o actualizaciones de sistemas deberán incorporar controles de seguridad desde su fase de diseño, bajo los principios de seguridad por diseño y privacidad por defecto.
5. La Dirección de Tecnologías y Sistemas de la Información deberá asegurar que los sistemas cumplan con los requisitos funcionales y de seguridad definidos por los propietarios de la información, y con las normas y políticas institucionales aplicables.
6. Los cambios, actualizaciones o mantenimientos deberán ser documentados, evaluados y aprobados antes de su implementación en el ambiente productivo, conforme a los procedimientos de gestión de cambios.
7. Se deberán realizar pruebas de aceptación y seguridad antes de la implementación de nuevos sistemas o actualizaciones, verificando su correcto funcionamiento y la ausencia de vulnerabilidades.
8. La SDSCJ deberá realizar, al menos una vez al año, revisiones de los equipos de cómputo y del software instalado, para controlar la presencia de programas no

autorizados, garantizar el cumplimiento de licencias, y verificar la correcta asignación de perfiles de usuario.

9. Los proveedores y desarrolladores externos deberán cumplir con las políticas de seguridad de la información y las cláusulas de confidencialidad establecidas contractualmente por la Entidad.
10. Se deberán mantener copias de respaldo actualizadas de los sistemas de información, y su código fuente cuando aplique estableciendo los controles necesarios para asegurar su disponibilidad en caso de fallas o incidentes.
11. La adquisición, desarrollo y mantenimiento de sistemas de información deberán aplicar estándares abiertos, buenas prácticas de arquitectura e interoperabilidad, así como la gestión de los Servicios Ciudadanos Digitales, garantizando su alineación con el Marco de Referencia de Arquitectura Empresarial (MRAE) y su integración con los procesos institucionales.

4.11. Relaciones con los proveedores.

a. Objetivo.

Establecer los lineamientos para que los proveedores, contratistas y terceros que tengan acceso a los activos de información o recursos tecnológicos de la SDSCJ cumplan con los requisitos de seguridad definidos por la Entidad, protegiendo la confidencialidad, integridad y disponibilidad de la información institucional.

b. Lineamientos.

1. Los proveedores deberán cumplir con las políticas y procedimientos de seguridad y privacidad de la información establecidos por la SDSCJ.
2. Todo acceso a los activos de información por parte de proveedores deberá ser autorizado, documentado y limitado al alcance necesario para la ejecución del contrato.
3. Los proveedores no podrán acceder a áreas restringidas donde se maneje información clasificada o reservada sin la autorización de la Dirección de Recursos Físicos y Gestión Documental.
4. Todo contrato con proveedores deberá incluir cláusulas de confidencialidad y compromisos de cumplimiento de las políticas de seguridad de la información.
5. Los requisitos de seguridad asociados con el acceso de proveedores deberán ser acordados y documentados antes del inicio de la prestación del servicio.
6. Los incumplimientos a los compromisos de seguridad deberán ser reportados a la Dirección Jurídica y Contractual y la Dirección de Operaciones para el Fortalecimiento Institucional, aplicando las medidas correctivas correspondientes.
7. La contratación de proveedores deberá realizarse de acuerdo con el Manual de Contratación de la Entidad y la normativa vigente.

4.12. Gestión de incidentes de seguridad en la información.

a. Objetivo.

Establecer los lineamientos para la identificación, registro, análisis, tratamiento y seguimiento de los incidentes de seguridad de la información, con el fin de minimizar su impacto y prevenir su recurrencia, garantizando la continuidad y la protección de los activos de información de la SDSCJ.

b. Lineamientos.

1. La SDSCJ, a través de la Dirección de Tecnologías y Sistemas de la Información, debe definir, documentar, mantener, publicar y aplicar el procedimiento para atender, valorar, clasificar y dar respuesta a los eventos e incidentes de seguridad de la información que comprometan las operaciones de la Entidad.
2. La Dirección de Tecnologías y Sistemas de la Información deberá promover el reporte oportuno de eventos de seguridad de la información para reducir la probabilidad e impacto de los riesgos asociados.
3. Los eventos e incidentes de seguridad deberán ser analizados de acuerdo con el procedimiento establecido para la gestión de incidentes de seguridad de la información.
4. Todos los usuarios internos y externos que accedan a la información de la Entidad deberán reportar de forma inmediata cualquier evento o incidente de seguridad a la Mesa de Servicio.
5. Los terceros u operadores tecnológicos que reciban reportes de incidentes deberán informar de manera inmediata a la Dirección de Tecnologías y Sistemas de la Información para su análisis y tratamiento.
6. Los incidentes de seguridad deberán registrarse, evaluarse y documentarse junto con las acciones correctivas y preventivas adoptadas para su resolución.
7. La Dirección de Tecnologías y Sistemas de la Información deberá garantizar que las evidencias asociadas a los incidentes sean preservadas bajo custodia y con acceso restringido.
8. Los resultados y lecciones aprendidas de los incidentes deberán ser revisados periódicamente para fortalecer los controles de seguridad y mejorar la capacidad de respuesta institucional.

4.13. Cumplimiento de los términos normativos.

a. Objetivo.

Establecer los lineamientos para que la SDSCJ cumpla con todas las disposiciones legales, reglamentarias, contractuales y normativas aplicables en materia de seguridad y privacidad de la información, así como con los compromisos asumidos frente a terceros, garantizando el tratamiento adecuado y responsable de los activos de información.

b. Lineamientos.

1. Todos los sistemas y procesos deberán cumplir con los requisitos legales, reglamentarios y contractuales aplicables sobre protección de datos personales, derechos de autor y delitos informáticos.
2. Los contratos con terceros deberán incluir cláusulas de confidencialidad sobre seguridad y privacidad de la información.
3. Se deberán implementar controles técnicos y administrativos para asegurar el cumplimiento normativo, incluyendo auditorías y revisión periódica de evidencias.
4. Los incumplimientos o desviaciones detectadas deberán ser reportados y gestionados conforme al procedimiento Gestión de incidentes y problemas.
5. Los funcionarios y contratistas de la Entidad deberán conocer y cumplir las disposiciones del Manual de Seguridad y Privacidad de la Información, así como los lineamientos y demás normas que regulan la protección de la información y los delitos informáticos.
6. El reporte de las evidencias de los controles definidos para la mitigación de los riesgos de seguridad de la información se realizará conforme a lo establecido en la Política de Administración de Riesgos de la Entidad.
7. La Dirección de Tecnologías y Sistemas de la Información deberá mantener registros actualizados de los controles implementados y evidencias de cumplimiento.
8. Toda la información relacionada con cumplimiento deberá conservarse y protegerse conforme a los parámetros de gestión documental y seguridad de la información.

Elaboró: Ing. Diego Mauricio Usme Gonzalez – 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 – 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