CONTENIDO

INTRODUCCIÓN

El presente manual, tiene como fin determinar los lineamientos generales frente al Modelo de Privacidad y Seguridad de la Información en adelante (MSPI), a través del establecimiento del alcance, objetivos y políticas de Seguridad de la Información, buscando preservar las características de confidencialidad, disponibilidad e integridad de los activos de información de la Secretaria Distrital del Hábitat

Los lineamientos descritos en el presente manual tienen como fin brindar herramientas para que los servidores públicos y terceros de la SECRETARÍA DISTRITAL DEL HÁBITAT realicen un tratamiento de la información de manera adecuada conforme a sus niveles de clasificación, se realice la identificación de los activos de información de la entidad, se realice una adecuada gestión a los riesgos de seguridad de la información y con ello lograr una mejora continua. Lo anterior enmarcado en el estándar internacional ISO/IEC 27001 en su versión 2013 y adaptación a la versión 2022, el Modelo Seguridad y Privacidad de la Información MSPI, en las mejores prácticas de seguridad de la información como el SGSI, legislación colombiana, necesidades y marco estratégico de la SECRETARÍA DISTRITAL DEL HÁBITAT.

El presente documento contiene la política general definida por la SECRETARÍA DISTRITAL DEL HÁBITAT y las políticas específicas de Seguridad de la Información, las cuales deben ser conocidas y cumplidas por todos los servidores públicos y terceros que hagan parte de la Entidad y que a su vez tengan acceso a los activos de información de la entidad.

ALCANCE

Este documento tiene como objetivo contribuir al mejoramiento del cumplimiento de los niveles de seguridad de la información y la protección de los activos de información identificados en la entidad, a través de la definición e implementación de políticas, procedimientos e instructivos, así como la definición de la metodología de gestión de riesgos de seguridad de la información, que permita a la SECRETARÍA DISTRITAL DEL HÁBITAT, identificar riesgos y generar controles como mecanismo para salvaguardar la información.

Las Políticas de Seguridad de la Información, serán monitoreadas y revisadas periódicamente con el fin de validar su implementación y necesidades de ajuste para el cumplimiento de los objetivos de seguridad, conforme con los requerimientos normativos descritos en la Estrategia de Gobierno específicamente en el Modelo de Seguridad y Privacidad de la Información de MinTIC, norma técnica NTC/IEC-ISO 27001:2013 y adaptación a NTC/IEC-ISO 27001:2022, mejores prácticas GTC/IEC-ISO 27002, así como en la normatividad colombiana.

Los funcionarios, contratistas, proveedores y terceras partes son responsables del cumplimiento de los lineamientos definidos en materia de Seguridad plasmados en los documentos que para ese objetivo la SECRETARÍA DISTRITAL DEL HÁBITAT crea y tenga en vigencia como este manual que se alinea al Modelo de Seguridad y Privacidad de la Información MSPI, obedeciendo así a los principios de confidencialidad, integridad y disponibilidad de los activos de información determinados por la Secretaría Distrital del Hábitat, para así propender por las condiciones óptimas de habitabilidad para la población del Distrito Capital. El MSPI cubre y define requerimientos para todos los Sistemas de información de la entidad que actualmente tiene, así como los que se en un futuro sean adoptados no importando la modalidad de desarrollo de estos.

El MSPI se encuentra definido para los todos los procesos pertenecientes al Sistema Integrado de Gestión de la Secretaría Distrital del Hábitat, en todas su sedes y locaciones.

El plan de Control Operacional se encuentra consignado dentro del el plan de acción, específicamente en el Plan de Seguridad y Privacidad de la información, para cada vigencia.

Los indicadores que permitan medir los objetivos son los mismos indicadores de la medición del Plan de Seguridad y Privacidad de la Información, para cada vigencia.

OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La SECRETARÍA DISTRITAL DEL HÁBITAT define los siguientes objetivos del MSPI, los cuales serán revisados, comunicados y actualizados de acuerdo con los lineamientos definidos en el sistema integrado de gestión de la entidad:

1. Fortalecer la seguridad de la información, manteniendo la confianza de los ciudadanos, servidores públicos y terceros a través de la revisión, actualización, divulgación y el cumplimiento de las políticas, procedimientos e instructivos definidos dentro del MSPI de la Secretaría Distrital del Hábitat.

2. Llevar a cabo una gestión de riesgos de seguridad de la información con el fin de preservar los niveles confidencialidad, integridad y disponibilidad de los activos de información de la Secretaría Distrital del Hábitat, los cuales se encuentran definidos en la matriz de inventario de activos de información.

3. Fortalecer la cultura de seguridad de la información, a través de la inclusión de buenas prácticas y conciencia de los servidores públicos y terceros frente a la seguridad de la información en la Secretaría Distrital del Hábitat.

4. Contribuir con la continuidad de los procesos de la Secretaría Distrital del Hábitat, mediante la implementación de planes y controles asociados a la seguridad de la información que contribuyan al mantenimiento de los niveles de riesgos aceptables de la entidad, a través de una adecuada gestión de incidentes de seguridad de la información.

5. Apoyar el desarrollo y puesta en marcha de proyectos en todas sus fases de ejecución, buscando tener los niveles de seguridad de la información definidos por la Secretaría Distrital del Hábitat y cumplimiento normativo colombiano.

1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

OBJETIVO

Establecer lineamientos generales con el propósito de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información, estableciendo y asignando las responsabilidades a los servidores públicos y terceros de la Secretaría Distrital del Hábitat, conforme a los controles de seguridad y privacidad de la información.

ALCANCE

La política general de seguridad de la información aplica a todos los servidores públicos y terceros de la Secretaría Distrital del Hábitat.

Cualquier violación u omisión de las políticas aquí descritas se sancionarán conforme a lo establecido en el código disciplinario único, lo definido en el proceso control disciplinario establecido por la Secretaría Distrital del Hábitat y lo acordado en los contratos independiente sea su modalidad suscritos con la entidad.

POLÍTICA

La SECRETARÍA DISTRITAL DEL HÁBITAT entendiendo la importancia de la adecuada gestión de la seguridad de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información y/o el Modelo de Seguridad y Privacidad de la Información, con un compromiso total de la alta dirección, manteniendo la confidencialidad, integridad y disponibilidad de sus activos de información mediante una gestión del riesgo continua, la adopción de buenas prácticas en el uso y gestión de los activos de información, así como la mejora de las competencias y conciencia de los servidores públicos y colaboradores de la entidad, con criterios de decisión aprobados y cumpliendo las normas legales, reglamentarias y contractuales adoptadas por la Secretaria Distrital del Hábitat.

Los servidores públicos, proveedores, usuarios o terceras partes son responsables por el adecuado manejo y aseguramiento de la información utilizada en el desarrollo de sus actividades, en el cumplimiento de los lineamientos, requisitos, controles y buenas prácticas de seguridad de la información definidas por la entidad, así como la prevención, detección y reporte de cualquier incidente relacionado con la seguridad de la información.

2. ORGANIZACIÓN DE LA SEGURIDAD

2.1 Roles y Responsabilidades

- Los funcionarios, contratistas, proveedores y terceras partes son responsables del cumplimiento de los lineamientos definidos en materia de Seguridad, plasmados en los documentos que para ese objetivo la SECRETARÍA DISTRITAL DEL HÁBITAT, crea y tenga en vigencia como este manual que se alinea al MSPI, obedeciendo así a los principios de confidencialidad, integridad y disponibilidad de los activos de información determinados por la Secretaría Distrital del Hábitat
- El Oficial de Seguridad de la Información es el responsable de la implementación del MSPI, haciendo seguimiento al cumplimiento de las Políticas, procedimientos que para tal fin sean construidos, asesora en caso de requerirse a todo aquel que maneje información de la entidad en materia de riesgos de seguridad de la información, siempre teniendo en cuenta los principios de Confidencialidad, Integridad y Disponibilidad de la Información.
- El Oficial de Seguridad de la Información en la SECRETARÍA DISTRITAL DEL HÁBITAT, es el Subsecretario (a) de Gestión Corporativa o quien el delegue.
- Se dará adopción a los Roles y Responsabilidades que la SECRETARÍA DISTRITAL DEL HÁBITAT tenga para sus dependencias enmarcadas en su misionalidad.

2.2 Contacto con Autoridades y Grupos de Interés

- La SECRETARÍA DISTRITAL DEL HÁBITAT, mantiene contacto con las autoridades competentes para el cumplimiento de la ley, organismos de control y autoridades de supervisión correspondientes.
- El Proceso de Gestión Tecnológica, junto con el Oficial de Seguridad mantienen contacto con grupos de interés, con el fin de tener información actualizada referente a seguridad de la información, como advertencias, actualizaciones, vectores de ataque y vulnerabilidades de Software.

2.3 Separación de Deberes

- Todos los sistemas de información de la SECRETARÍA DISTRITAL DEL HÁBITAT deben implementar reglas de acceso, de tal manera que exista segregación de funciones, entre quien administre, opere, mantenga y audite, y todo aquel que tenga acceso al sistema de información, así como quien otorgue privilegios de estos.
- Todo aquel que tenga acceso a la información de la SECRETARÍA DISTRITAL DEL HÁBITAT, debe tener sus funciones definidas con el fin de reducir el uso no autorizado, indebido o accidental a los activos de información, que para su nivel de confidencialidad este restringido a quien no está autorizado.
- Todos los sistemas de información de la SECRETARÍA DISTRITAL DEL HÁBITAT deben implementar seguimiento a sus acciones dentro del sistema de información, mediante el uso de control de cambios, que para tal efecto el proceso de Gestión Tecnológica tenga en su mapa de procesos, con el fin de verificar, controlar, y auditar los cambios que se realicen en el desarrollo de los sistemas de información, independiente cual sea su modalidad de creación, así como todo lo concerniente con la creación, modificación y asignación de permisos para manejo de bases de datos, ambientes de prueba, producción y afectación a la infraestructura tecnológica de la SECRETARÍA DISTRITAL DEL HÁBITAT.

3. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

3.1. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

OBJETIVO

Establecer los niveles de seguridad de los activos de información para el uso óptimo de los dispositivos móviles (ej. equipos portátiles, teléfonos celulares, tabletas, tarjetas inteligentes entre otros) que administren, trasmitan, almacenen o procesen información definidos por la Secretaría Distrital del Hábitat

ALCANCE

Esta política aplica a todos los servidores públicos y terceros que tengan asignados dispositivos y/o equipos móviles propiedad de la Secretaría Distrital del Hábitat, que tengan acceso a la red de información o cualquier servicio de tecnologías de la información y comunicaciones de la entidad.

POLÍTICA

El proceso de Gestión Tecnológica en coordinación con el Oficial de Seguridad de la Información, establecerán procedimientos y mecanismos de seguridad lógicos para preservar los niveles de seguridad de los activos de información requeridos para permitir el acceso a los mismos a través de los dispositivos de tecnología móviles (equipos portátiles, teléfonos celulares, tabletas, tarjetas inteligentes entre otros), con el fin de salvaguardar la información administrada, trasmitida, almacenada o procesada por éstos. Así mismo, se establecerán los controles de seguridad de la información de acuerdo con la identificación y valoración de los riesgos de seguridad de la información.

Los controles dispuestos por la Secretaría deben ser de estricto cumplimiento por parte de los servidores públicos y terceros que hagan uso de estos y que a través de estos accedan a la información, tecnologías de la información, y comunicaciones o servicios de la entidad.

RESPONSABILIDADES

- El proceso de Gestión Tecnológica y el Oficial de Seguridad de la Información, establecerán las medidas de seguridad para proteger la información que sea administrada, transmitida o almacenada por los dispositivos móviles de los servidores públicos y terceros de la entidad.

- Los servidores públicos que tengan asignados dispositivos móviles de la entidad, deberán protegerlos de forma física y lógica para evitar al máximo el hurto, acceso no autorizado o divulgación de la información almacenada y procesada por estos dispositivos. En caso de ser necesario, se establecerán controles de cifrado de la información, uso de autenticación y copias respaldo.

- El proceso de Gestión Tecnológica asignará o denegará a los servidores públicos y terceros el acceso a la información o sistemas de información a través de los dispositivos móviles, conforme los roles y responsabilidades asignados por la entidad y lineamientos determinados por los distintos jefes de área.

- El Contratista o tercero que utilice dispositivos móviles como equipos de cómputo portátiles de su propiedad para el desarrollo de sus actividades y que acceda a la red de la SECRETARÍA DISTRITAL DEL HÁBITAT, deberá contar son Software Legal instalado en su equipo, de la misma manera contar con Software antivirus licenciado y/o actualizado, para dicho enlace con la red de la SECRETARÍA DISTRITAL DEL HÁBITAT, deberá remitir listado de software utilizado y licencias correspondientes, tanto para el sistema operativo como para las aplicaciones, indicando software, fabricante, versión licenciada y fecha de caducidad de la licencia previa conexión a la red de la entidad, todo esto con el fin de minimizar el riesgo de sufrir de incidentes de seguridad que atenten contra la confidencialidad, disponibilidad e integridad de la información.

- En caso de que se presente el hurto o perdida de algún dispositivo móvil propiedad de la Secretaría Distrital del Hábitat, el servidor público o tercero responsable de dicho dispositivo, deberá informar el suceso de manera inmediata al jefe de área y al Oficial de Seguridad de la Información de la entidad o persona delegada para dicha actividad, con el objetivo de establecer las medidas de seguridad adecuadas que permitan proteger la información.

- El área de talento humano con el apoyo del Oficial de Seguridad de la Información coordinarán el desarrollo de campañas de sensibilización periódicas a los servidores públicos de la entidad, con el propósito de concientizar acerca del buen uso de los dispositivos móviles.

- Esta política debe ser cumplida por los servidores públicos y terceros que tengan acceso a la información o sistemas de información de la Secretaría Distrital del Hábitat a través de dispositivos móviles.

La SECRETARÍA DISTRITAL DEL HÁBITAT se reserva el derecho de monitorear y revisar cuando sea requerido, el software instalado en dispositivos móviles conectados a la red de la entidad.

2.2. POLÍTICA DE TELETRABAJO

OBJETIVO

Establecer los niveles de seguridad de los activos de información definidos por la Secretaría Distrital del Hábitat al momento de realizar actividades de teletrabajo.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros de la Secretaría Distrital del Hábitat que tengan aprobado el desarrollo de actividades de teletrabajo.

POLÍTICA

El proceso de Gestión Tecnológica en coordinación con el Oficial de Seguridad de la Información, establecerán mecanismos de seguridad física y lógica para preservar los niveles de seguridad de los activos de información requeridos para el desarrollo de las actividades de teletrabajo por parte de los servidores públicos y terceros autorizados dentro de la entidad.

RESPONSABILIDADES

- El proceso de Gestión Tecnológica adoptará los procedimientos necesarios, para proteger los datos y/o activos de información que serán accedidos desde los equipos vinculados a las actividades de teletrabajo.

- El proceso de Gestión Tecnológica y el Oficial de Seguridad de la Información, definirán los canales de comunicación tales como el establecimiento de VPN`s y métodos de autenticación apropiados para controlar el acceso remoto de los usuarios a la información y/o sistemas de información de la Secretaría Distrital del Hábitat, en el momento de realizar actividades de teletrabajo.

- El proceso de Talento Humano, con el apoyo del Oficial de Seguridad de la Información y/o proceso de Gestión Tecnológica, llevaran a cabo el análisis de los riesgos de seguridad de la información existentes en el sitio del teletrabajo para los funcionarios de carrera administrativa, teniendo en cuenta las instalaciones físicas, el entorno local y todos los lineamientos de seguridad definidos por la Secretaría Distrital del Hábitat, y la normatividad vigente.

- El proceso de Gestión Tecnológica conforme a la información remitida por el proceso de Talento Humano y/o el jefe del área, asignará, modificará o denegará los accesos a los activos de información durante las actividades de teletrabajo.

- El Oficial de Seguridad de la Información y/o el proceso de Gestión Tecnológica, junto con el proceso de Talento Humano, llevaran a cabo campañas de sensibilización para promover las buenas prácticas de seguridad asociadas a las actividades de teletrabajo.

2.3. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

OBJETIVO

Establecer los lineamientos generales para controlar el acceso a los datos y/o activos de información de la Secretaría Distrital del Hábitat.

ALCANCE

Esta política aplica para todos los servidores públicos y terceros que tengan acceso a los activos de información de la Secretaría Distrital del Hábitat.

POLÍTICA

La Secretaría Distrital del Hábitat, establece los controles de seguridad necesarios que permitan definir los accesos a los activos de información con el fin de preservar los niveles de confidencialidad de la información. Por lo anterior, se determinarán las responsabilidades por parte de los servidores públicos y terceros mediante la celebración de contratos y/o acuerdos de confidencialidad, conforme a los lineamientos implementados por la entidad.

RESPONSABILIDADES

- Los servidores públicos y terceros de la Secretaría Distrital del Hábitat tienen la responsabilidad de velar por la seguridad de los activos información, asegurando que su acceso y uso sea exclusivamente para el desarrollo de las labores encomendadas, con el fin de evitar accesos no autorizados, pérdidas o uso indebido de los activos de información.

- El acceso a los activos de información será restringido teniendo en cuenta los roles y responsabilidades de los servidores públicos de la Secretaría Distrital del Hábitat. La autorización será otorgada por los responsables de los activos de información, previa solicitud realizada por los Subsecretarios o subdirectores de la Entidad mediante los formatos, procedimientos y sistemas de información que para tal fin fueron creados. Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza de la Secretaría Distrital del Hábitat, y así mismo para minimizar el riesgo de la pérdida de los niveles de seguridad de la información.

- Los servidores públicos y terceros de la Secretaría Distrital del Hábitat tienen como responsabilidad mantener los niveles de seguridad de la información de los activos designados y autorizados, asegurándose que estos sólo sean utilizados para el desarrollo de las labores encomendadas. En caso de observar incidentes de seguridad, deberán ser reportados al Proceso de Gestión tecnológica mediante el uso de la Mesa de Ayuda.

• Los accesos tanto físicos como lógicos, asignados a los colaboradores, servidores y funcionarios y todo aquel que haya tenido acceso a estos en la SECRETARÍA DISTRITAL DEL HÁBITAT, deberán ser desactivados o modificados una vez se termine el vínculo laboral/contractual con la Secretaría Distrital del Hábitat. Esto se realizará conforme a la información remitida por el proceso de Talento Humano/ Jefe del Área o Subsecretario de Gestión Corporativa.

• Todos los servidores públicos de la Secretaría Distrital del Hábitat tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar el buen uso de los activos de información.

• Los responsables de las áreas seguras de la Secretaría Distrital del Hábitat, establecerán los controles necesarios para restringir el acceso, determinando mecanismos de registro que permitan validar datos de identificación de la persona que accede a la información, el motivo del ingreso, el tiempo empleado para el desarrollo de la actividad, y, asimismo, velará por que las personas que accedan se encuentren acompañadas por un encargado durante su permanencia en ella.

• El Responsable y/o Encargado del activo de información o área segura, será responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios en intervalos regulares con el fin de mantener un control eficaz de los mismos.

2.4. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

OBJETIVO

Salvaguardar los activos de información de la Secretaría Distrital del Hábitat frente a perdida de la confidencialidad, autenticidad o integridad mediante la adopción de controles criptográficos.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros que mediante su ejercicio de actividades y los niveles de clasificación de la información requieran realizar actividades de cifrado de información.

POLÍTICA

El proceso de Gestión Tecnológica con el apoyo del Oficial de Seguridad de la Información, serán los responsables de definir los mecanismos de cifrados más convenientes frente a las necesidades de la entidad. Estas medidas de seguridad se determinarán con base en el análisis de riesgos y los requisitos de seguridad. Los usos de las herramientas de cifrado de la información serán autorizadas de acuerdo con los roles o responsabilidades de los servidores públicos de la Secretaría Distrital del Hábitat.

Para establecer los controles de cifrado de la información, El Oficial de Seguridad de la Información y/o proceso de Gestión Tecnológica, deben tener en cuenta la normatividad colombiana vigente frente a la protección de datos, estándares de seguridad de la información aplicables y la tecnología existente. Adicionalmente, los responsables de la seguridad de la información serán los encargados de llevar a cabo la activación, recepción y distribución de las llaves criptográficas a los servidores públicos autorizados y vigilarán porque se cumpla de forma óptima el ciclo de vida de estas llaves.

RESPONSABILIDADES

- En los casos que se requiera el uso del sistema de cifrado y/o llaves criptográficas, se deberá solicitar la autorización al Oficial de Seguridad de la Información y/o proceso de Gestión Tecnológica, determinando la necesidad y condiciones de uso.

- El Oficial de Seguridad de la Información y el proceso de Gestión Tecnológica son los encargados del sistema de cifrado y de las llaves criptográficas de la entidad, quienes serán los responsables de identificar y establecer los controles necesarios con niveles adecuados de seguridad y restringir su acceso sólo a las personas autorizadas.

- Las actividades relacionadas con la administración y eliminación de las llaves criptográficas, deberán ser registradas por las personas encargadas. Cuando las llaves se encuentren en riesgo o se tenga la sospecha que hayan sido divulgadas, o cuando servidores públicos culminen su vínculo laboral/contractual con la Secretaría Distrital del Hábitat, las mismas serán modificadas o eliminadas con el fin de proteger el acceso a la información.

- Las personas autorizadas para el acceso y uso de las llaves criptográficas, velarán por su protección y conservación. Así mismo, mantendrá los niveles de seguridad de la información cifrada o descifrada al nivel de clasificación previamente establecido.

• Los servidores públicos y terceros tendrán la responsabilidad de reportar, mediante el canal autorizado por la entidad, entre los que se encuentra la mesa de ayuda o correo electrónico las posibles vulnerabilidades, amenazas o riesgos asociados al cifrado de la información.

2.5. POLÍTICA DE ESCRITORIO Y PANTALLA LIMPIOS

OBJETIVO

Propender que los servidores públicos y terceros de la entidad conserven su puesto de trabajo y pantalla del computador libre de documentos y/o información sensible para la Secretaría Distrital del Hábitat.

ALCANCE

La política aquí descrita aplica a todos los servidores públicos y terceros de la Secretaría Distrital del Hábitat que tengan acceso a la información tanto digital como física de la entidad.

POLÍTICA

Los servidores públicos y terceros deberán adoptar los lineamientos definidos por la Secretaría Distrital del Hábitat para mantener los niveles de seguridad de los activos de información que tienen a su cargo. Para ello se deberá tener presente:

• Almacenar los documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.), así como la información física en sitios seguros, por ejemplo: en cajones bajo llave o archivadores. Esto con el fin de evitar el acceso no autorizado, pérdida o daño de la información a cargo.

• Durante los periodos de tiempo en los cuales cesan las actividades en el equipo de cómputo, la sesión se debe bloquear, para evitar accesos no autorizados a la información contenida en el equipo.

• De utilizar medios de impresión o copiado de documentos, la información debe retirarse inmediatamente por el servidor público responsable, y así mismo, se deberá evitar reutilizar papel que contenga información confidencial.

• De acuerdo con los niveles de clasificación de la información, los archivos o carpetas deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, así mismo, se deberá evitar guardarlos en el escritorio del perfil de usuario o carpetas del sistema operativo del equipo de cómputo.

RESPONSABILIDADES

• El proceso de Gestión Tecnológica con el apoyo del Oficial de Seguridad de la Información, serán los responsables de establecer los controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee de forma automática en un lapso determinado de inactividad.

• A fin de validar el cumplimiento de la presente política, los equipos de cómputo y los lugares de trabajo de los servidores públicos y terceros, podrán ser revisados y auditados por las áreas de control que determine la entidad.

• Los usuarios no deberán almacenar en el escritorio del sistema operativo de sus estaciones de trabajo, documentos, accesos directos a los documentos o a sistemas de información sensibles.

• Los usuarios son responsables por la custodia y las acciones que se realicen a través de los activos informáticos asignados, por lo tanto, es importante que permanezca en el sitio de trabajo cuando se realice cualquier mantenimiento o actualización a los activos de información.

2.6. POLÍTICA DE RESPALDO DE INFORMACIÓN (BACKUP)

OBJETIVO

Establecer la gestión, realización, administración y custodia de las copias de respaldo, con el fin de preservar las características de seguridad de la información en la Secretaría Distrital del Hábitat.

ALCANCE

La presente política debe ser cumplida por los servidores públicos y terceros que realicen la gestión de las copias de respaldo (usuarios, Bases de Datos, Aplicativos, Configuraciones, sistemas de replicación de datos entre otros) de la Secretaría Distrital del Hábitat.

POLÍTICA

La información requerida para el cumplimiento de los objetivos estratégicos de la Secretaría Distrital del Hábitat deberá estar respaldada y ser tratada conforme a los niveles de clasificación de la información y riesgos asociados, de acuerdo con los lineamientos legales, técnicos y administrativos determinados por la entidad.

Las copias de respaldo serán realizadas conforme al procedimiento definido por la Secretaría Distrital del hábitat, y las mismas serán almacenadas en áreas seguras para evitar el acceso no autorizado y la integridad y seguridad de estas.

RESPONSABILIDADES

- Los servidores públicos y/o terceros encargados de las copias de respaldo deberán velar porque la información sea almacenada conforme a los procedimientos establecidos, es decir, de una manera controlada y de acuerdo con las necesidades de la Secretaría Distrital del Hábitat. Así mismo, se deberá llevar a cabo pruebas periódicas de las copias y validar su correcto funcionamiento.

- Los servidores públicos y terceros deberán almacenar la información "Crítica del Negocio" requerida para sus procesos operativos, dentro de los sistemas de almacenamientos dispuestos por la Secretaría Distrital del Hábitat. De esta manera, se tendrá la disponibilidad de las copias de respaldo de cada una de las áreas; así mismo, los servidores públicos o terceros serán responsables de depurar periódicamente la información para la optimización de los recursos de la entidad.

- La información que las áreas y/o los servidores públicos almacenan en los equipos y carpetas compartidas de la Secretaría Distrital del Hábitat, debe ser únicamente de carácter institucional y no de uso personal (fotos, música, archivos personales y otros), esto con el fin de optimizar el espacio de estos. Cuando se encuentre información de uso personal dentro de los equipos de cómputo o servidores, la misma, será borrada sin previo aviso.

• Los servidores públicos y/o terceros encargados usarán los procedimientos creados para tal fin, las copias se realizarán según la metodología adoptada en la SECRETARÍA DISTRITAL DEL HÁBITAT, (diaria, semanal, mensual, semestral y anual), establecidas según las necesidades y capacidades de la infraestructura tecnológica de la Secretaría Distrital del Hábitat, con el fin de asegurar que las copias de respaldo sean confiables en caso de emergencia. Estas copias serán retenidas por un periodo de tiempo determinado, de acuerdo con lo establecido en la entidad, resguardadas a través de controles que permitan salvaguardar de manera adecuada los niveles de seguridad.

2.7. POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN

OBJETIVO

Preservar las características de seguridad de los activos de información de la Secretaría Distrital del Hábitat durante su transferencia tanto interna como externa.

ALCANCE

La política aquí descrita debe ser adoptada por todos los servidores públicos y terceros que realicen transferencia de información de forma interna o externa en cumplimiento de sus funciones.

POLÍTICA

La Secretaría Distrital del Hábitat garantiza la transmisión o transferencia de la información, teniendo en cuenta sus niveles de clasificación y las políticas de seguridad de la información de la entidad descritas en el presente manual.

Para el intercambio de información con otras organizaciones o partes externas se establecerá contratos o acuerdos externos, en los cuales se determinen los controles frente a la transmisión o transferencia y tratamiento, teniendo en cuenta los niveles de clasificación de la información. De igual manera, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y después del tiempo de ejecución de las actividades establecidas.

RESPONSABILIDADES

- La información sólo podrá ser usada para las actividades y labores asignadas dentro de los acuerdos suscritos entre la Secretaría Distrital del Hábitat y las partes interesadas, apoyado con la firma de un acuerdo o cláusulas de confidencialidad de la información.

- La información deberá protegerse de divulgación no autorizada conforme los niveles de clasificación de la información, donde es necesario cumplir los mecanismos y controles definidos para el tratamiento de esta.

- Para la transferencia de información electrónica, El proceso de Gestión Tecnológica en coordinación con El Oficial de Seguridad de la Información, dispondrán los canales de comunicación que brinden niveles de seguridad adecuados para la transferencia de información, adicionalmente, se tendrán presentes los riesgos de seguridad, así como los niveles de clasificación de la información antes del envío de esta.

- El intercambio de la información se llevará a cabo según los acuerdos establecidos, los cuales deben tener definido como mínimo: las responsabilidades y procedimientos para la transferencia de información que permita establecer la trazabilidad y no repudio, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad y los niveles de clasificación de la información a ser intercambiada y tratada por las partes.

- Antes de efectuar la transferencia de información, se deben firmar acuerdos de confidencialidad con las partes interesadas, en los cuales se registren las responsabilidades y se garanticen la reserva de la información y el alcance frente a su tratamiento y uso, durante y después de su transferencia.

- Frente a los Términos y Condiciones La Secretaria Distrital del Hábitat, en adelante la Entidad, es una entidad pública de orden Distrital, en cabeza de la Alcaldía Mayor de Bogotá cuya Misión Liderar la formulación e implementación de políticas de gestión del territorio urbano y rural, en el marco de un enfoque de desarrollo sostenible con el fin de facilitar el acceso a la vivienda y promover el mejoramiento integral del Hábitat en el Distrito Capital. Establece que para su sitio Web o cualquier lugar donde halla intercambio de información su función principal es la de proveer información y servicios, así como la de divulgar y promover políticas, normas y directrices relacionadas con su la misión y objetivos estratégicos de la Entidad. Por ello frente a las condiciones, alcances y límites en el uso; derechos y deberes de los usuarios; alcance y límites de la responsabilidad de los sujetos obligados; contacto para asuntos relacionados con los términos y condiciones; referencia a la política de privacidad y tratamiento de datos personales; referencia a la política de derechos

de autor serán puestas en conocimiento en los sitios web de acuerdo con la normatividad exigida y con base a la normatividad interna.

2.8. POLÍTICA DE DESARROLLO DE SOFTWARE

OBJETIVO

Definir los lineamientos generales para el desarrollo o adquisición de software a la medida en la Secretaría Distrital del Hábitat, determinando los controles de seguridad para su protección.

ALCANCE

La política aquí descrita debe ser adoptada por los servidores públicos y terceros de la Secretaría Distrital del Hábitat que lleven a cabo actividades relacionadas con el desarrollo o adquisición de software a la medida.

POLÍTICA

Los contratos de desarrollo de software se realizará conforme a la normatividad Nacional, las obras literarias (dentro de las que se encuentra el software), artísticas y científicas creadas por servidores públicos y particulares contratados mediante prestación de servicios por la Entidad, desarrolladas en cumplimiento de las obligaciones constitucionales y legales del cargo que fungen y/o de las que se establezcan en el contrato, son de propiedad de la Secretaría Distrital del Hábitat, en virtud de la presunción legal de cesión de derechos patrimoniales vigente en el ordenamiento nacional. Lo que significa que, los servidores públicos preservan los derechos morales como autores de las obras, aunque no puedan utilizarlos para explotarlos en detrimento de los derechos y deberes de la Secretaría Distrital del Hábitat.

Con el fin de que todas las licencias sobre software adquiridas por la Secretaría Distrital del Hábitat gocen de un medio de prueba y publicidad legítimo, seguro y que garantice la autenticidad de la titularidad de estas, la Secretaría Distrital del Hábitat registrará los actos y contratos suscritos al respecto.

Dentro del ambiente de pruebas, no se permite el uso de información sensible de producción, en caso de que sea estrictamente necesario, se deberá realizar el ofuscamiento de los datos o enmascaramiento de datos para conservar la protección de la información. Una vez dicha información no sea requerida, la misma deberá eliminarse de manera segura.

En los casos de adquisición de software a la medida, la SECRETARÍA DISTRITAL DEL HÁBITAT determinará dentro de los contratos definidos con el proveedor, la propiedad de la licencia y los derechos intelectuales de los códigos fuente, así como las condiciones de uso, de la misma manera cualquier desarrollo se le deberá exigir soporte IPv6 nativo en coexistencia con IPv4.

RESPONSABILIDADES

- Antes de iniciar el desarrollo de software, el grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica y/o el oficial de seguridad de la información, así como las partes interesadas, acordarán una metodología de desarrollo, identificando detalladamente la estructura de trabajo, responsables, cronograma, alcance, requisitos a cumplir, procesos afectados y requerimientos.

- El grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica junto con el oficial de seguridad de la información, establecerán criterios de aceptación de seguridad para la aprobación del software. La aceptación del software se establecerá a través de los resultados obtenidos de las pruebas planteadas, las cuales tendrán dentro de sus parámetros, la validación de vulnerabilidades, códigos maliciosos, puertas traseras, entre otras.

- Dentro de los requisitos a tener presentes para el desarrollo de software con respecto a la seguridad de la información, es importante determinar: controles para proteger la confidencialidad, disponibilidad e integridad de la información, métodos de autenticación, cifrado de datos, control de roles y privilegios, pistas de auditoría, gestión de sesiones, datos históricos, manejo apropiado de errores, seguridad en las comunicaciones, codificación segura, mecanismos de protección de datos personales, entre otras.

- Antes, durante y después del desarrollo de software, se deberá efectuar un análisis de riesgos donde se determine el impacto y afectación de la materialización de los riesgos a la entidad. Así mismo, se determinarán los controles de seguridad necesarios para la mitigación de estos.

• El grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica junto con el oficial de seguridad de la información, deberán llevar a cabo revisiones y auditorias informáticas a los desarrollos realizados, con el fin de validar el cumplimiento de los requisitos de seguridad y calidad definidos.

• El grupo técnico que lidere el desarrollo del software y el responsable del proceso de Gestión Tecnológica verificarán y controlarán las versiones del software desarrollado con los respectivos documentos de soporte. Esto con el adecuado control y funcionamiento en el ciclo de vida de este.

• Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.

• Los servidores públicos o terceros que realicen actividades de desarrollo de software, no podrán realizar pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad, integridad o confidencialidad de la información, todo esto debe quedar documentado en control de cambios.

• El grupo técnico que lidere el desarrollo del software y el proceso de Gestión Tecnológica, deberán restringir el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.

• El grupo técnico que lidere el desarrollo del software y el proceso de Gestión Tecnológica deberán verificar periódicamente las versiones instaladas tanto en ambiente de pruebas como en producción, con el fin de que las mismas correspondan a las últimas versiones aprobadas.

El grupo técnico que lidere el desarrollo, prueba y producción, deberá contar con auditoria sobre las bases de datos, diferentes credenciales de acceso y separación de roles, con el fin de evitar la pérdida de confidencialidad de estas.

2.9. POLÍTICA PARA RELACIONES CON PROVEEDORES

OBJETIVO

Establecer los lineamientos generales para preservar los niveles de seguridad y privacidad de los datos y activos de información accedidos por proveedores.

ALCANCE

La política aquí descrita debe ser adoptada por todos los servidores públicos y terceros de la Secretaría Distrital del Hábitat que tengan relación con proveedores, y que éstos accedan a activos de información propiedad de la entidad.

POLÍTICA

La Secretaría Distrital del Hábitat, proveerá los procedimientos y controles adecuados para la preservación de las características de seguridad de los activos de información que van a ser accedidos por los proveedores de la Secretaría Distrital del Hábitat.

Los servidores públicos responsables de los activos de información de la Secretaría Distrital del Hábitat, en ningún caso otorgarán acceso a los activos y/o áreas críticas de la entidad a los proveedores, hasta no haber realizado la formalización de la relación contractual conforme lo determina el Manual de Contratación, la firma de los acuerdos de intercambio de información y la identificación y evaluación de los riesgos.

Los acuerdos de intercambio de información con proveedores velarán por el cumplimiento de las regulaciones legales, propiedad intelectual y protección de datos personales. Así mismo especificarán las consideraciones de seguridad y reserva de la información y las responsabilidades por el mal uso o divulgación de esta.

RESPONSABILIDADES

- El responsable del activo de información antes de otorgar los accesos a los proveedores, deberá validar que se encuentren firmados y formalizados los acuerdos de confidencialidad y/o el acto administrativo que determine los fines de uso, las condiciones

de tratamiento de la información, así como la debida definición de los controles requeridos para preservar las características de seguridad de los activos de información.

• Los propietarios de la información que requieran intercambiar la misma, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo con la reglamentación vigente y los lineamientos definidos por la Secretaría Distrital del Hábitat.

• En caso de presentarse y/o identificar una amenaza que pueda llegar a afectar la seguridad de la información, se deberá reportar al Oficial de Seguridad de la Información y/o el proceso de Gestión Tecnológica a través de los canales de comunicación establecidos por la entidad.

2.10. POLÍTICA DE AUTORIZACIÓN DE NUEVOS RECURSOS DE PROCESAMIENTO

OBJETIVO

Establecer los lineamientos generales para el aprovisionamiento y conexión de nuevos recursos informáticos como sistemas operativos, procesadores, memorias, discos, red, etc. Para que estos nuevos recursos conserven las características de confidencialidad, disponibilidad e integridad de la información.

ALCANCE

Se aplica a todos los nuevos recursos de procesamiento o existentes, que impliquen conexión a la Solución Integral de Telecomunicaciones de la Secretaría Distrital del Hábitat.

POLÍTICA

La Secretaría Distrital del Hábitat, establecerá la conexión de nuevos recursos de procesamiento, con el fin de preservar las características de seguridad sobre los mismos. Por lo anterior, se determinarán las responsabilidades por parte de los servidores públicos y

terceros mediante la celebración de contratos y/o acuerdos de confidencialidad y disponibilidad, conforme a los lineamientos implementados por la entidad.

La Secretaría Distrital del Hábitat en cabeza del el Proceso de Gestión Tecnológica, llevará a cabo control de acceso a la información y/o activos de información contemplando aspectos físicos y lógicos, con el objetivo de tener la trazabilidad de las acciones realizadas en los mismos, por los usuarios, y referentes de los sistemas de información, mediante el formato de control de cambios y/o Mesa de ayuda.

La Secretaria Distrital de Hábitat deberá exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TIC.

RESPONSABILIDAD

- El(la) Subsecretario de Gestión Corporativa junto con el Proceso de Gestión Tecnológica, cumplirá la función de autorizar el aprovisionamiento de nuevos recursos de procesamiento de infraestructura tecnológica para los diferentes sistemas de información de la Secretaría Distrital del Hábitat.

- El Oficial de Seguridad de la Información y/o el personal responsable de Gestión Tecnológica evaluarán las vulnerabilidades del aprovisionamiento para la puesta en marcha de este.

2.11 POLÍTICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

OBJETIVO

Definir el nivel de criticidad, sensibilidad y reserva de la información de la Secretaría Distrital del Hábitat, para propender por la confidencialidad, integridad y disponibilidad de los activos de información de la SECRETARÍA DISTRITAL DEL HÁBITAT.

Clasificar la información para señalar su sensibilidad y criticidad de acuerdo con la confidencialidad, integridad y disponibilidad, garantizando que los activos de información reciban un adecuado nivel de protección.

ALCANCE

Se aplica a todos los activos de información identificados en la Secretaría Distrital del Hábitat. La identificación de los activos de información debe tener presente, la información, sistemas de información, software, hardware, personas o lugares para la operación o aquella información estratégica requerida para alcanzar los objetivos misionales de la SECRETARÍA DISTRITAL DEL HÁBITAT. Dentro de los activos de información a identificar se pueden encontrar:

- Los portales web de la SECRETARÍA DISTRITAL DEL HÁBITAT y los contenidos que residen en ellos;
- La información que se transmite a través de los diferentes servicios de la SECRETARÍA DISTRITAL DEL HÁBITAT;
- Los servicios de interacción con la comunidad, servicios de transacciones en línea, servicios de recaudo o registro de información, entre otros.
- Los sistemas de información que apoyan los servicios de la SECRETARÍA DISTRITAL DEL HÁBITAT;
- La plataforma tecnológica que soporta los diferentes servicios y sistemas de información (hardware, software, comunicaciones, bases de datos, etc.) de la SECRETARÍA DISTRITAL DEL HÁBITAT;
- La plataforma tecnológica de seguridad implementada por la SECRETARÍA DISTRITAL DEL HÁBITAT;
- Los documentos físicos requeridos para llevar a cabo el desarrollo de las actividades operaciones para el cumplimiento de los objetivos misionales de la SECRETARÍA DISTRITAL DEL HÁBITAT.

POLÍTICA

La SECRETARÍA DISTRITAL DEL HÁBITAT garantiza la identificación de los activos de información definiendo el nivel de criticidad, sensibilidad y brinda los controles adecuados encaminados a la preservación de las características de su seguridad (Confidencialidad, Integridad y Disponibilidad).

RESPONSABILIDAD

Los responsables de la información, Jefes de Área, Subsecretarios (as), Subdirectores (as) son los encargados de clasificarla, de acuerdo con su grado de sensibilidad y criticidad; mantener actualizada la clasificación efectuada, y de definir los niveles que podrán tener permisos de acceso a la información.

El custodio de la información se encarga de mantener las medidas de protección establecidas por los responsables.

Cada responsable de la Información supervisará que el proceso de clasificación y rotulado de información de su área de competencia sea cumplido de acuerdo con lo establecido en la presente Política.

2.12. POLÍTICA DE SEGURIDAD FÍSICA

OBJETIVO

Prevenir e impedir accesos no autorizados, daños o robos a los activos de información de la Secretaría Distrital del Hábitat.

Proteger los equipos de procesamiento de información crítica de la Secretaría Distrital del Hábitat ubicándolos en áreas seguras y resguardadas por un perímetro de seguridad definido, con medidas y controles de acceso apropiados. Asimismo, contemplar la protección de este en su traslado y permanencia fuera de las áreas protegidas, por motivos de mantenimiento u otros.

Controlar los factores ambientales que podrían perjudicar el correcto funcionamiento de los equipos informáticos que contienen la información de la Secretaría Distrital del Hábitat.

Implementar medidas para proteger la información manejada por el personal en las oficinas, en el marco normal de sus labores habituales.

ALCANCE

Aplica a todos los recursos físicos asociados a los activos de información de la Secretaría Distrital de Hábitat, relativos a instalaciones, computadores, cableado, expedientes, medios de almacenamiento, etc.

POLÍTICA

Todos los sitios en donde se encuentren sistemas de procesamiento de información, equipos de cómputo, almacenamiento, comunicaciones y expedientes, serán protegidos de accesos no autorizados, mediante el uso controles lógicos o físicos, para evitar intrusiones, y otro tipo de amenazas que puedan afectar su normal operación.

Los aspectos de la seguridad física a considerar son:

- Las medidas de seguridad que se deban tomar dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad.

- El sitio donde se ubiquen los recursos informáticos debe ser protegidos de accesos no autorizados, empleando mecanismos de control (tarjetas, talanqueras, alarmas, cerraduras, claves de acceso, personal de seguridad, etc.).

- Los requerimientos de tipo ambiental deben ser especificados por los diferentes fabricantes de los equipos.

- Debe existir un área de recepción que solo permita la entrada de personal autorizado por un funcionario de la entidad, previa autorización de esta vía correo electrónico y/o autorización escrita.

- El equipamiento de soporte como impresoras y fotocopiadoras debe ser instalado adecuadamente en lugares acondicionados para tal fin, para evitar solicitudes de acceso que podrían comprometer la información.

- Las áreas seguras contarán con equipos contra incendio, detección de humo, control de humedad, todo esto de acuerdo con la infraestructura que posea la SECRETARÍA DISTRITAL DEL HÁBITAT.

- Los Backup de información se mantendrán en sitios alejados de los procesamientos principales.

- En las áreas donde se manipule algún tipo de activo de información, no se permite fumar, tomar ningún tipo de bebidas o consumir alimentos, todo ello para evitar la pérdida de disponibilidad o integridad de la información.

- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico.

- Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes.

- El cableado de la red debe ser instalado y mantenido por personal calificado con el fin de conservar su integridad.

- Todo elemento que ingrese debe ser inspeccionado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respetiva autorización de ingreso.

- Las áreas de descargue deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros.

- Los materiales que deban entrar a las instalaciones deben ser inspeccionados debidamente en la zona de descargue, para evitar la entrada de elementos peligrosos a las áreas internas.

- El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado.

- El uso de equipos de procesamiento de la información o software, fuera de las instalaciones de la Secretaría Distrital del Hábitat, debe ser autorizado por el Propietario de la Información de donde el funcionario, o colaborador dependa. Esto aplica para computadores personales, agendas electrónicas, teléfonos móviles, etc.

- El uso de cualquier tipo de activo documental que contenga información de la entidad, como carpetas, fuera de las instalaciones de la Secretaría Distrital del Hábitat, debe ser autorizado por el Propietario de la Información de donde el funcionario, o colaborador dependa. y debe conservarse la trazabilidad de la autorización y la motivación para tal traslado

- Se deben cumplir los lineamientos aplicables a la entidad de acuerdo con la normatividad técnica colombiana sobre gestión documental, descritas en el MSPI

RESPONSABILIDAD

El(la) Subsecretario(a) de Gestión Corporativa definirá las medidas de seguridad física y ambiental para el resguardo de los activos, en función a un análisis de riesgos y controlará su implementación.

El Oficial de Seguridad y/o el personal responsable de Gestión Tecnológica, definirán las medidas de seguridad a implementar en áreas protegidas y coordinarán su implementación. El personal responsable del proceso de Gestión Tecnológica controlará el mantenimiento de los equipos informáticos, de la entidad de acuerdo con las indicaciones de proveedores tanto dentro como fuera de las instalaciones de la Secretaría Distrital de Hábitat.

La instalación o reubicación de equipos de procesamiento o de telecomunicaciones, es responsabilidad única y exclusiva del Subsecretario(a) de Gestión Corporativa o quien el delegue. Por lo tanto, los usuarios deben abstenerse de realizar modificaciones en los equipos, infraestructura de red o eléctrica sin autorización del Subsecretario(a) de Gestión Corporativa y/o equipo del proceso de Gestión Tecnológica.

Los Subsecretarios definirán los niveles de acceso físico del funcionario, o colaborador de la Secretaría Distrital de Hábitat a las áreas protegidas que estén bajo su responsabilidad.

El uso de equipos de procesamiento de la información o software, fuera de las instalaciones de la Secretaría Distrital del Hábitat, debe ser autorizado por el responsable de los activos de información de donde el funcionario, o colaborador dependa.

El proceso de bienes, servicios e infraestructura establecerá parámetros para que todo personal interno y externo que ingrese a un área definida como segura por la SECRETARÍA DISTRITAL DEL HÁBITAT, posea una identificación a la vista que claramente lo identifique como tal y estas identificaciones serán intransferibles.

El ingreso a las áreas seguras debe ser autorizado por la Subsecretaria y/o Subdirección correspondiente y será monitoreada mediante registros de acceso y salida, los visitantes siempre deberán estar acompañados por personal de la SECRETARÍA DISTRITAL DEL HÁBITAT.

Los servidores, contratistas y terceras partes no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones e infraestructura tecnológica, a menos que se tenga la autorización correspondiente.

El proceso de Gestión Tecnológica velará por que los medios de almacenamiento de información que se den de baja, sean donados o se encuentren en obsolescencia, previamente la información almacenada en estos tenga el respectivo respaldo y estos sean formateados a bajo nivel o de manera segura, a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente, para su posible reúso, donación, o destrucción según sea el caso.

2.13. POLÍTICA DE ANTIVIRUS

OBJETIVO

Definir los lineamientos y controles para el correcto funcionamiento del antivirus y otros recursos de protección en la Secretaría Distrital del Hábitat.

ALCANCE

Se aplica a los servidores, estaciones de trabajo y equipos de cómputo de la Secretaría Distrital del Hábitat, incluyendo dispositivos portátiles que puedan prestar servicio fuera de las instalaciones de la SECRETARÍA DISTRITAL DEL HÁBITAT.

POLÍTICA

Los equipos integrados en el dominio de la Secretaria Distrital del Hábitat deberán tener instalado un antivirus y antispyware, gestionado centralizadamente, el cual se actualizará automáticamente de forma periódica.

Los usuarios deberán ejercer buenas prácticas de uso en los equipos de cómputo, tales como:

- Ejecutar el antivirus al usar dispositivos como USB, CD, DVD, discos externos u otros.
- Verificar a través del software antivirus los archivos de cómputo que sean proporcionados por personal externo o interno como programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos.
- No utilizar las facilidades de los exploradores WEB para ejecutar aplicaciones directamente.

- Abstenerse de escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o impedir el funcionamiento de cualquier recurso de procesamiento, archivos de sistema, o software.
- Abstenerse de conectar equipos personales que no contengan antivirus instalado y actualizado, a la red de la SECRETARÍA DISTRITAL DEL HÁBITAT.
- Al producirse un incidente se desconectará la estación de la red y se avisará inmediatamente de la presencia del malware para ser eliminado.

Asimismo, la Subsecretaría de Gestión Corporativa ejercerá los siguientes controles:

- Monitorear por medio de software especializado y actualizado los computadores y medios informáticos en búsqueda de archivos sospechosos o no autorizados.
- Configurar las aplicaciones de correo electrónico y herramientas de oficina para evitar que se ejecute contenido activo, código móvil y macros automáticamente.
- Al producirse un incidente se gestionará la eliminación del malware.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el personal responsable del proceso de Gestión Tecnológica, tendrá a su cargo la definición de controles para la detección, prevención y protección de la información contra software malicioso con el fin de establecer la seguridad de los datos.

Los usuarios y terceras partes deberán cumplir con la Política.

El Oficial de Seguridad y/o el personal responsable de Gestión Tecnológica definirá las medidas de seguridad a implementar en la gestión de la consola de antivirus y coordinará su implementación. El personal responsable de Gestión Tecnológica controlará la instalación y administración del antivirus en los equipos informáticos en las instalaciones de la Secretaría Distrital de Hábitat.

2.14. POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO

OBJETIVO

Establecer los lineamientos generales para que los servidores públicos y terceros de la entidad, empleen adecuadamente el correo electrónico a fin de utilizar el recurso de forma racional y como potenciador de las actividades de la Secretaría Distrital del Hábitat.

ALCANCE

La política aquí descrita aplica a todos los servidores públicos y terceros de la Secretaría Distrital del Hábitat, que tengan acceso a la información digital albergada en el correo electrónico corporativo de la entidad.

POLÍTICA

La Secretaría Distrital del Hábitat, asigna a funcionarios y contratistas una cuenta de correo electrónico corporativa para ejercer sus funciones según las capacidades de la infraestructura de la SECRETARÍA DISTRITAL DEL HÁBITAT.

La información contenida en el buzón de correo se considera privada, por lo tanto, debe ser manejada como una comunicación directa entre el remitente y su destinatario, los usuarios no deben utilizar los sistemas de correo electrónico de la SECRETARÍA DISTRITAL DEL HÁBITAT para transmitir:

- Correos electrónicos no solicitados, sin relación con las actividades de la SECRETARÍA DISTRITAL DEL HÁBITAT, que puedan ofender o causar inconvenientes a quienes lo reciban. Esto incluye el uso de listas de correo, cuando el e-mail enviado no está relacionado con el propósito para el cual la lista de correo utilizada fue creada (SPAM).
- Correos electrónicos no solicitados requiriéndole a otros usuarios en la Secretaría Distrital del Hábitat o cualquier lugar que continúe reenviando el mismo a otros.
- Correos electrónicos pretendiendo ser de una persona diferente del usuario que realmente envía el correo.
- Material, el cual pueda considerarse sexista, racista, homofóbico, xenofóbico, pornográfico, pedófílico o similarmente discriminatorio y/o ofensivo.
  Material que condene o promueva, directa o indirectamente, actividades criminales o que puedan dañar las actividades de la Secretaría Distrital del Hábitat.

- Texto o imágenes las cuales sean propiedad intelectual de terceros, sin el permiso escrito para dicha divulgación por parte del responsable.
- Material que pueda ser utilizado para vulnerar la seguridad de los computadores o para facilitar el acceso no autorizado a las mismas.
- Material que contenga datos personales, a menos que se cuente con autorización expresa para tal fin.

Asimismo, los usuarios deberán ejercer buenas prácticas de uso en las cuentas de usuario asignadas, tales como:

- Depurar continuamente su buzón de correo, con el fin de mantener siempre espacio disponible para enviar y recibir nuevos mensajes, cada buzón de correo tendrá un espacio limitado de almacenamiento.
- Tener claves de acceso seguras y no entregar la contraseña a personas no autorizadas, teniendo en cuenta que la cuenta de correo utiliza la misma contraseña que la de red.
- Abstenerse de abrir correos de remitentes desconocidos o sospechosos y no activar ningún tipo de enlace ni ejecutar archivos adjuntos.
- Reportar posibles anomalías o irregularidades en mensajes recibidos, comunicándose con la Subsecretaria de Gestión Corporativa y/o Gestión Tecnológica mediante la Mesa de Ayuda.
- Abstenerse de interceptar o revelar comunicaciones electrónicas no autorizadas.
- Utilización de un lenguaje apropiado, evitando palabras ofensivas o discriminatorias.
- Cada usuario es responsable de la información enviada, reenviada o eliminada desde su cuenta de correo
- Abstenerse de enviar información confidencial a personal no autorizado. Los usuarios de datos deben asumir que ningún correo electrónico es seguro.
- Considerar la compresión de los archivos adjuntos, a fin de reducir el uso de ancho de banda.

La Secretaría Distrital del Hábitat se reserva el derecho a pedir las claves de encriptación, en caso de haber sido utilizadas, de acceder y navegar a los contenidos del correo electrónico de los usuarios de acuerdo con sus obligaciones legales y para legitimar los propósitos con los cuales se utiliza el sistema.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el personal responsable del proceso de Gestión Tecnológica definirán y harán seguimiento a los controles a implementar.

Los usuarios en general y las terceras partes tendrán la obligación de cumplir lo establecido en la presente Política.

Los usuarios son responsables por la adecuada administración del correo electrónico y la herramienta de almacenamiento en la nube que use la entidad.

2.15. POLÍTICA DE USO DE CONTRASEÑAS

OBJETIVO

Concientizar a los usuarios respecto de su responsabilidad frente a la utilización de contraseñas.

ALCANCE

Esta política aplica a todos los servidores públicos y terceros que tengan acceso, por medio de un usuario previamente establecido a la red de datos de la Secretaría Distrital del hábitat.

POLÍTICA

La Secretaría Distrital del Hábitat, asigna a funcionarios y contratistas acceso a una cuenta de correo electrónico y sistemas de información corporativos para ejercer sus funciones, el usuario deberá crear una contraseña teniendo en cuenta las siguientes recomendaciones:

- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- Tener una longitud mínima de 8 caracteres.
- Incluir caracteres de tres de las siguientes categorías:
    - Mayúsculas (de la A a la Z)
    - Minúsculas (de la a a la z)
    - Dígitos de base 10 (del 0 al 9)

- Caracteres no alfanuméricos (por ejemplo, !, $, #, %).

- No repetir las ultimas 3 contraseñas utilizadas anteriormente.
- No usar contraseñas por defecto o iguales al nombre de usuario o del perfil del usuario, nombres de familiares, amigos, mascotas, número de teléfono, números de documentos.
- No escribir la contraseña en papel o documentos electrónicos.
- No utilizar la misma contraseña para usos personales o formularios electrónicos.
- No revelar la contraseña de acceso a terceros de ningún sistema de información de la Secretaría Distrital del Hábitat (aplicativos, internet, correo o ingreso a la red).
- En caso de olvido de la contraseña, se deberá gestionar el cambio de esta por medio del aplicativo de mesa de ayuda.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el responsable del proceso de Gestión Tecnológica estarán a cargo de la definición de procedimientos para el control de acceso a los sistemas de información.

El personal responsable del proceso de Gestión Tecnológica implementará las normas y procedimientos definidos.

Los usuarios y terceras partes deberán cumplir todas las directrices asociadas con esta política.

Los servidores públicos y terceros de la entidad tendrán la responsabilidad de mantener las contraseñas de aplicativos, internet, correo electrónico o ingreso a la red en estricta confidencialidad.

2.16. POLÍTICA DE USO DE SERVICIOS DE RED

OBJETIVO

Establecer los lineamientos que se deben tener en cuenta para el uso de los servicios de red por servidores públicos y terceros de la entidad, preservando las características de seguridad de los activos de información de la Secretaría Distrital del Hábitat.

ALCANCE

Aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre el uso de servicios de red.

POLÍTICA

La SECRETARÍA DISTRITAL DEL HÁBITAT controlará el acceso a los servicios de red para que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de estos.

La Subsecretaría de Gestión Corporativa, otorgará el acceso a los servicios y recursos de red, de acuerdo previa solicitud formal, especialmente a las aplicaciones que procesen información clasificada o aplicaciones críticas, o a usuarios que utilicen el acceso desde sitios de alto riesgo; por ejemplo, áreas públicas o externas que están fuera de la administración y del control de seguridad de la Secretaría Distrital del Hábitat.

Para ello la SECRETARÍA DISTRITAL DEL HÁBITAT documentará los procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderán:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el responsable del proceso de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos para el uso de servicios de red.

El personal responsable del proceso de Gestión Tecnológica implementará las normas y procedimientos definidos.

Los Usuarios y Terceras Partes deberán cumplir todas las directrices asociadas con esta política.

2.17. POLÍTICA DE USO DE INTERNET

OBJETIVO

Establecer los lineamientos generales para el uso adecuado de Internet y/o activos de información por parte de los usuarios finales, evitando errores, pérdidas, alteraciones o uso inadecuado de la información en las aplicaciones web de la Secretaría Distrital del Hábitat.

ALCANCE

Aplica a todas las formas de acceso de aquellos a quienes se les haya otorgado permisos sobre el uso de Internet en la Secretaría Distrital del Hábitat.

POLÍTICA

El acceso a Internet provisto a los usuarios de la Secretaría Distrital del Hábitat es exclusivamente para las actividades relacionadas con las funciones que desempeña.

La utilización del software de navegación web designado por la Secretaría Distrital del Hábitat deberá estar configurado con las directivas establecidas.

El acceso a Internet tiene que ser realizado a través de los canales de acceso provistos por la Secretaría Distrital del Hábitat. En caso de necesitar una conexión a Internet especial, ésta tiene que ser notificada y aprobada por los responsables de los procesos y el Oficial de Seguridad de la Información.

Los usuarios que requieran acceso a través de protocolo FTP deberán ser explícitamente autorizados a este tipo de acceso por el Oficial de Seguridad de la Información y/o el personal responsable del proceso de Gestión Tecnológica.

Los usuarios del servicio de Internet están sujetos al monitoreo de las actividades que realizan en la red.

Los usuarios no pueden usar el acceso a Internet para los siguientes propósitos.

- Acceso a sitios que puedan considerarse por su contenido sexista, racista, homofóbico, xenofóbico, pornográfico, pedofílico o similarmente discriminatorio y/u ofensivo.
- Acceso a sitios que reproduzcan en forma no autorizada material protegido por los derechos de autor.
- Acceso a sitios que provean instrucciones o claves para utilizar o acceder a software, servicios o sitios en forma ilegal (piratería).
- Acceso a sitios de juegos en red.
- Descarga de software sin autorización.
- Descarga de archivos de audio o video sin autorización.

Los usuarios no pueden usar el acceso a Internet para los siguientes propósitos, salvo expresa autorización:

- Acceso para audio o video en línea (TV, Radio, música, etc.).
- Acceso a redes sociales autorizadas.
- Realizar ataques sobre otros sitios, usuario o servidores.
- Brindar servicios externos desde el puesto de trabajo.

Los usuarios no podrán transferir o publicar información de propiedad de la Secretaría Distrital del Hábitat sin previa autorización y con la utilización de los canales previstos por la SECRETARÍA DISTRITAL DEL HÁBITAT para tal fin.

Los usuarios no podrán, en ninguna circunstancia utilizar el acceso a Internet para monitorear, interceptar información de otros usuarios a menos que hayan sido autorizados para hacerlo.

Los usuarios del servicio deben asumir que ninguna conexión a Internet es segura, y no deberán enviar información que consideren confidencial a través de este medio.

El acceso a cualquier recurso disponible a través de Internet que no sea el de navegación de sitios, deberá solicitarse en forma justificada para su debida aprobación.

Se permite a los usuarios acceder a Internet para los siguientes usos:
- Acceso a sitios sobre noticias (diarios, radios, agencias, etc.).
- Acceso a Sistemas Bancarios.
- Acceso a Sistemas de Pago Electrónico de servicios.
- Acceso a Sistemas de información sobre transportes, mapas, espectáculos, hotelería.
- Acceso a sitios de capacitación, educación, tecnología.

- Acceso a redes sociales autorizadas
- Acceso a sitios de clientes, proveedores, competencia.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el responsable del proceso de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos para el servicio de Internet.

El personal responsable del proceso de Gestión Tecnológica implementará las normas y procedimientos definidos.

Los Usuarios y Terceras Partes deberán cumplir todas las directrices asociadas con esta política.

2.18. POLÍTICA DE USO DE RED PRIVADA VIRTUAL (VPN)

OBJETIVO

Determinar los lineamientos generales que se deben tener en cuenta para preservar las características de seguridad de la información cuando se realizan conexiones por VPN (Virtual Private Network).

ALCANCE

Aplica a todas las formas de uso de VPN en la Secretaría Distrital del Hábitat.

POLÍTICA

La Secretaría Distrital del Hábitat establecerá el acceso por VPN con los protocolos establecidos y adoptando los siguientes controles:

- Uso de encriptación acorde a la criticidad del acceso, y acorde a lo establecido en las políticas relacionadas.
- Establecer niveles de servicio que contemplen los tiempos de mantenimientos y Backup.

- Registrar las acciones de inicio y final de conexión con los datos correspondientes al usuario, dirección IP.
- Disponer de estadísticas periódicas de utilización por usuario.

RESPONSABILIDAD

El Oficial de Seguridad de la Información y/o el responsable de Gestión Tecnológica estarán a cargo de la definición de normas y procedimientos de uso de VPN.

El personal responsable de Gestión Tecnológica implementará los procedimientos para la conexión y trabajo con la VPN.

El Oficial de Seguridad de la Información y/o el responsable del proceso de Gestión Tecnológica antes de otorgar los accesos remotos por VPN, deberá validar que tenga previa autorización del jefe de área donde se determine los fines de uso, las condiciones para el uso de la VPN, así como la debida definición de los controles requeridos para preservar las características de seguridad de los activos de información.

2.19. POLÍTICA DE CONTROL DE CAMBIOS

OBJETIVO

Establecer los lineamientos para propender por la confidencialidad, integridad y disponibilidad de los recursos de procesamiento de información, comunicaciones, y servicios que trabajen con información sensible para de la Secretaría Distrital del hábitat.

ALCANCE

Aplica a funcionarios de Gestión Tecnológica, Gestión Documental, Terceras Partes, y sistemas de información, por medio de normas, procedimientos, documentación y plataformas técnicas de la Secretaría Distrital del Hábitat.

Los casos en los que no fuera posible la aplicación de la presente política se considerarán como excepciones.

POLÍTICA

Los servicios prestados por terceras partes se deben gestionar de acuerdo con una evaluación de riesgos de seguridad Digital, para mejorar el servicio, implementar nuevas tecnologías, cambios de proveedor y otros.

Se controlará que los cambios en los recursos de procesamiento y de comunicaciones no afecten la seguridad de estos, ni de la información que soportan. Se evaluará el posible impacto operativo de los cambios previstos y se verificará su correcta implementación. Todo cambio deberá ser evaluado previamente en aspectos técnicos y de seguridad.

La modificación, actualización o eliminación de los datos operativos serán realizadas a través de los sistemas que procesan dichos datos y de acuerdo con el esquema de control de accesos implementado en los mismos.

Los servidores propietarios y/o encargados de los recursos de procesamiento y de comunicaciones, deberán realizar las solicitudes de cambio por medio del aplicativo de mesa de ayuda y de acuerdo a los procedimientos, formatos, guías, manuales creados para tal fin.

RESPONSABILIDAD

- El(la) Subsecretario(a) de Gestión Corporativa, el Oficial de Seguridad de la Información y/o el responsable del proceso de Gestión Tecnológica definen y aprueban las normas y procedimientos para la gestión del cambio, el personal responsable de Gestión Tecnológica y los responsables de los activos implementan los cambios.

- Los usuarios y terceras partes deberán cumplir con los lineamientos establecidos en esta política.

- Los servidores públicos, contratistas y/o terceros encargados de los recursos de procesamiento y de comunicaciones, deberán velar porque la información sea almacenada conforme a los lineamientos establecidos, antes de realizarse algún cambio que pueda afectar la información contenida en los recursos descritos anteriormente y de acuerdo con las necesidades de la Secretaría Distrital del Hábitat.

2.20. POLÍTICA DE PROPIEDAD INTELECTUAL

OBJETIVO

Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Secretaría Distrital del Hábitat y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.

ALCANCE

Esta Política se aplica a todo el personal de la Secretaría Distrital del Hábitat. asimismo, se aplica a los activos de información de la Secretaría Distrital del Hábitat.

POLÍTICA

La Secretaría Distrital del Hábitat, será titular de los derechos de Propiedad Intelectual que recaigan sobre las obras e invenciones producidas en el ejercicio de su función, y en las cuales hubieren participado trabajadores, que desempeñen cargos o actividades inventivas o creativas. El software es considerado una obra intelectual que goza de la protección de la Ley 23 de Propiedad Intelectual.

La explotación de la propiedad intelectual sobre los programas de software incluirá, entre otras formas, los contratos de licencia para su uso o reproducción, los productos de software se suministran normalmente bajo acuerdos de licencia que limiten el uso de los productos al equipo específico y su copia a la creación de copias de resguardo solamente.

La SECRETARÍA DISTRITAL DEL HÁBITAT conservará pruebas y evidencias de propiedad de licencias, discos maestros, manuales, etc., asimismo se implementarán controles para evitar el exceso del número máximo permitido de usuarios y se verificará que en los equipos para funcionamiento de la SECRETARÍA DISTRITAL DEL HÁBITAT se instalen productos con licencia y software autorizado.

RESPONSABILIDAD

El(la) Subsecretario(a) de Gestión Corporativa y la Subsecretaría Jurídica analizarán los términos y condiciones de las licencias y definirán los procedimientos correspondientes para salvaguardar la propiedad intelectual.

La Subsecretaria de Gestión Corporativa mantendrá control sobre las licencias que sean instaladas en los equipos de cómputo, estaciones de trabajo y servidores de la entidad.

El proceso de Gestión Tecnológica verificará el tipo de software y determinará la viabilidad para su uso en los activos de información.

3 GLOSARIO

Se expone un glosario de términos frente a palabras que puedan encontrarse en este manual, con el fin de brindar claridad al lector y tomando como referencia la familia de las normas ISO 27001 y definiciones aplicables al Subsistema de Gestión de Seguridad de la Información de la Secretaría Distrital del Hábitat.

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización[1].

- **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo[2].

- **Amenaza informática:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la entidad política del Estado. (Ministerio de Defensa de Colombia).

- **Análisis de riesgos:** Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo[3].

- **Área Segura:** Son lugares donde se encuentra localizada la información crítica para la organización, éstas estarán protegidas por un perímetro de seguridad y por los controles de acceso pertinentes.

- **Autenticación:** Mecanismo que se realiza a través de medios, dispositivos o sistemas para validar la identidad de un usuario.

- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

[1] http://www.iso27000.es/glosario.html
[2] http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486
[3] http://www.iso27000.es/glosario.html

- **Aviso De Privacidad:** Comunicación, verbal o escrita, en la que el responsable del Tratamiento de la información le informa al Titular de los datos personales la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma en que podrá acceder a estas y las finalidades del Tratamiento que se pretende dar a los datos personales que suministre.

- **Base de Datos:** Conjunto organizado de datos personales que serán objeto de Tratamiento.

- **Base de Datos Personal o Doméstica**: Conjunto de datos personales que serán objeto de Tratamiento dentro del marco de la vida privada o familiar de las personas naturales.

- **Causahabiente:** Persona que es sucesora o heredera del Titular de la información a causa del fallecimiento de este.

- **Clasificación de la Información:** es el ejercicio mediante el cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.

- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.

- **Control:** Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas, para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.

- **Custodio de activo de información:** Personal asignado a un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** Son todos aquellos datos primarios (sin procesar) que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo custodia de la entidad y que pueden ser puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos[4].

[4] http://mintic.gov.co/portal/604/w3-article-5300.html

- **Dato Personal:** Cualquier información vinculada, o que pueda asociarse, a una o varias personas naturales determinadas o determinables.

- **Dato privado: S**on los datos que por su naturaleza íntima o reservada sólo son relevantes para el titular.

- **Dato Sensible:** Es aquel que afecta la intimidad del Titular o cuyo uso indebido puede propiciar discriminación; se entienden como sensibles los datos que revelen el origen étnico o racial, la orientación o filiación política, las convicciones y creencias religiosas o filosóficas, el estado de salud, la vida sexual, la información biométrica, la información familiar, la dirección de domicilio, y la pertenencia a sindicatos o a organizaciones sociales, de derechos humanos, promotoras de intereses de partidos políticos o que garanticen derechos y garantías de partidos políticos de oposición. Su Tratamiento está prohibido salvo en las excepciones previstas en las leyes.

- **Dato semiprivado:** Aquel que no tiene naturaleza íntima, reservada, ni pública. Su conocimiento o divulgación puede interesar no solo al Titular sino a un sector o grupo de personas o a la sociedad en general; tienen esta naturaleza los datos financieros, los crediticios, los relacionados con la actividad comercial o de servicios, entre otros.

- **Dato público:** Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la Ley 1266 de 2008. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas, entre otros; se consideran igualmente datos públicos los relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o de servidor público, entre otros.

- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad y/o persona autorizada.

- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. Puede darse el caso de que se tenga múltiples roles en el manejo de la información y ser al mismo tiempo responsable del Tratamiento, fuente de información o usuario.

- **Evento de Seguridad:** Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

- **Fuente de Información:** Persona natural o jurídica que recibe o conoce datos personales del Titular, en virtud de una relación comercial, de servicio o de cualquier otra índole. Mediante autorización legal o del Titular puede transmitir o transferir estos datos a un responsable o encargado para su Tratamiento. Puede tener múltiples roles en el manejo de la información y ser al mismo tiempo responsable o encargado del Tratamiento.

- **Gestión de claves:** Son controles que realizan mediante la administración de claves criptográficas.

- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.

- **Habeas data:** Derecho de cualquier persona a conocer, actualizar y rectificar los datos o la información que se hayan recogido sobre ella en un banco de datos o en archivos de entidades públicas y privadas.

- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.

- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

- **Información:** Corresponde a este grupo 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 auditoria entre otros.

- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados[5].

- **Integridad:** Conservar con exactitud la información que fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.

- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del *SGSI*,

[5] https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf

que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.

- **Negocio:** principales funciones misionales de la entidad.

- **No repudio**: Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).

- **Medio removible:** Componente extraíble de hardware, usado para el almacenamiento de información; entre los que podemos encontrar: cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.

- **Modelo de Seguridad y Privacidad de la Información MSPI:** imparte lineamientos a las entidades públicas en materia de implementación y adopción de buenas prácticas, tomando como referencia estándares internacionales, con el objetivo de orientar la gestión e implementación adecuada del ciclo de vida de la seguridad de la información (Planeación, Implementación, Evaluación, Mejora Continua), permitiendo habilitar la implementación de la Política de Gobierno Digital.

- **Oficial de Seguridad de la Información:** También denominado CISO (Chief Information Security Officer) es un rol desempeñado por el (la) Subsecretario (a) de Gestión Corporativa y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se avala en todo momento que la información de la entidad está preservada adecuadamente, para el rol de CISO es responsable de:
  - ✓ Generar y establecer políticas de seguridad de la información.
  - ✓ Supervisar la administración del control de acceso a la información.
  - ✓ Supervisar el cumplimiento normativo de la seguridad de la información.
  - ✓ Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
  - ✓ Socializar temas relacionados con seguridad de la información.

- **Operador de Información:** Persona, entidad u organización que recibe información de la fuente de datos personales sobre varios Titulares, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la ley. Se sujeta al cumplimiento de los deberes y responsabilidades previstos para establecer la protección de los derechos del Titular de los datos. No es responsable por la calidad de los datos que le sean

suministrados por la fuente salvo que este tenga la condición de fuente y operador de manera simultánea.

- **Parte interesada (*Stakeholder*):** Persona u entidad que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

- **Plan de continuidad del negocio**: Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.

- **Plan de tratamiento de riesgos**: Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

- **Proceso**: Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.

- **Propietario de activo de información:** Personal asignado a un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.

- **Responsable del tratamiento:** Persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros, decide sobre la base de datos o el Tratamiento de los de los mismos. También puede ser fuente de información, encargado del Tratamiento o usuario.

- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)[6].

- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

[6] Guía para la administración del riesgo y el diseño de controles en entidades públicas, VERSIÓN 5

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Sistema de Gestión de Seguridad de la Información (*SGSI*): C**onjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

- **Titular de la información:** Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.

- **Transferencia:** Tiene lugar cuando el responsable o el encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor que se convierte en responsable del Tratamiento y que puede encontrarse dentro o fuera del país.

- **Transmisión:** Implica la comunicación de los datos personales, dentro o fuera del territorio de la República de Colombia, con el objetivo de darle un Tratamiento por parte del encargado y de acuerdo con las instrucciones del responsable.

- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.

- **Usuario:** Persona natural o jurídica que, en los términos y circunstancias permitidas por la ley, puede acceder a la información personal, de uno o varios Titulares, que ha sido transferida o transmitida por el encargado siguiendo instrucciones del responsable. De acuerdo con el uso que les dé a los datos del Titular, puede transformarse en responsable o encargado del Tratamiento o fuente de información.

- **Vulnerabilidad:** Debilidad de un activo o control que pueda ser explotado por una o más amenazas.

4 CONTROL DE CAMBIOS

Fecha de Modificación (aaaa/mm/dd)	Versión	Descripción del cambio
2018/07/12	3	Se reestructura redacción de la introducción y el alcance, se definen los objetivos de seguridad de la información y se redefine la política general del subsistema Seguridad de la Información las políticas: autorización de nuevos recursos de procesamiento, Clasificación de activos de información, seguridad física, antivirus, Backup fueron redefinidas, fue eliminada la política de administración de riesgos, la política de intercambio de información modifico su nombre a política de transferencia o intercambio de información y fue ajustada en contenido, la política de uso de correo electrónico fue modificada a uso de correo electrónico corporativo y fue ajustado en contenido y redacción, la política de uso de sistemas de información y dispositivos de comunicación fue eliminada, las políticas de control de acceso y uso de contraseñas fueron ajustado en contenido y redacción, la política de uso de puestos de trabajo modifica su nombre a escritorio limpio y pantalla limpia y ajusta su contenido, las políticas de uso de servicio de red, uso de internet y política de uso de VPN son redefinidas, la política de uso de computación móvil y teletrabajo es divida en dos: política de uso de dispositivos móviles y política de teletrabajo, la política de adquisición, desarrollo y mantenimiento de sistemas de información modifica su nombre a política de desarrollo de software; las políticas de controles criptográficos, control de cambios y propiedad intelectual se ajustan en redacción y contenido.

Fecha de Modificación (aaaa/mm/dd)	Versión	Descripción del cambio
		Se incluye la política de relación con proveedores y la política de tratamiento de la información de la SDHT; se incluye el anexo "Declaración de aplicabilidad SOA" y se actualiza acorde con el organigrama el cargo de "Director de Gestión Corporativa y CID a Subsecretario de Gestión Corporativa y CID.
2018/09/25	4	Según lo aprobado en el comité de seguridad y de las tecnologías de la información y las comunicaciones del 18/09/2018, se reestructura redacción del alcance general del documento y objetivo de las políticas: seguridad física, autorización de nuevos recursos de procesamiento - desarrollo de software - transferencia o intercambio de información.
2023-05-25	5	Según la Resolución 2710 de 2017 se debe exigir soporte IPv6 nativo en coexistencia con IPv4, en la contratación de bienes y servicios relacionados con las TIC. Por ello se modifican las políticas de desarrollo de Software, política de autorización de nuevos recursos de procesamiento. Se actualiza la política general de seguridad de la información Se restructura redacción general del documento Se incluye la norma técnica ISO 27001:2022 Adición en la Política de seguridad física del componente relacionado con la Guía N° 6 del MSPI

Fecha de Modificación (aaaa/mm/dd)	Versión	Descripción del cambio
		Eliminación del capítulo 3 política de tratamiento de la información secretaría distrital del hábitat. Eliminación de anexos (Anexo 1 Declaración de Aplicabilidad SOA)