INTRODUCCIÓN

Consciente de las necesidades derivadas de sus actividades, la Secretaría Distrital de Ambiente adoptó el Sistema de Gestión de Seguridad de la Información-SGSI como una herramienta para garantizar la confidencialidad, integridad y disponibilidad, administrando los riesgos, cumpliendo con la legislación vigente, y generando una cultura de seguridad de la información en los servidores públicos y demás partes interesadas. Así mismo, se encuentra adoptando las políticas de gestión y desempeño del Modelo Integrado de Planeación y Gestión-MIPG, específicamente en lo concerniente a la política de gobierno digital, política de seguridad digital y política de transparencia y acceso a la información.

Mediante la implementación de este sistema de gestión como parte del Modelo de Seguridad y Privacidad de la Información-MSPI se protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información de la Secretaria Distrital de Ambiente, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos de la SDA y en cumplimiento de los requisitos legales y reglamentarios propios de la entidad, previniendo incidentes mediante la gestión de riesgos de seguridad y privacidad de la información, la implementación de controles de seguridad físicos y digitales, orientados a la mejora continua en la gestión y el desempeño del Sistema de Gestión de Seguridad de la Información, con la finalidad de prestar servicios con calidad y transparencia a la ciudadanía en general y las demás entidades territoriales y nacionales.

En tal sentido, la Secretaria Distrital de Ambiente adopta el presente documento que contiene las políticas de seguridad de la información, como compromiso y responsabilidad que tiene la entidad con la confidencialidad, integridad y disponibilidad de la información, de acuerdo con el numeral 4.2.1 literal b. de la Norma Técnica NTC-ISO 27001 de 2013, las cuales se implementan a partir de los planes, procedimientos y controles, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la entidad, así como los recursos necesarios para su implementación y operatividad.

De igual forma estas políticas específicas de seguridad de la información se articulan de forman directa con la política del Sistema Integrado de Gestión de la SDA, como se presenta a continuación:

POLITICA DEL SISTEMA INTEGRADO DE GESTIÓN[1]

La Secretaria Distrital de Ambiente, como autoridad ambiental del Distrito Capital promueve, orienta y regula acciones que permitan el adecuado aprovechamiento de los recursos naturales, así como la recuperación, protección y conservación sostenible del territorio para garantizar un ambiente sano y armónico con la región.

Busca fortalecer la oferta de bienes y servicios ambientales mediante la prevención y control de los impactos negativos en estrecha relación con los procesos participativos territoriales.

[1] MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN, PE03-MA01 Versión: 17 Radicado 2020EE175506 del 08 de octubre 2020.

Está comprometida con el bienestar de los servidores, desde un enfoque de prevención basado en la seguridad y salud en el trabajo que evoluciona de manera continua desde la innovación y conocimiento.

De igual manera, preserva la memoria institucional a través del fortalecimiento y uso de las tecnologías de la información, la administración y conservación documental, ***bajo estándares de confidencialidad, integridad y disponibilidad.***

Igualmente, está comprometida con la satisfacción de las necesidades de los grupos de valor a través de la implementación y mejora continua del Sistema Integrado de Gestión y del Modelo Integrado de Planeación y Gestión, en el marco de la responsabilidad social y la cultura de autogestión, autocontrol y autoevaluación de la entidad, para el cumplimiento de los requisitos legales y otros requisitos.

La política del SIG se desarrollará a través de los siguientes objetivos:

- *Mantener la mejora continua mediante la optimización de los procesos de la entidad, en procura de la satisfacción de las necesidades y expectativas de las grupos de valor.*
- *Implementar el 100% de las actividades establecidas en los programas de Gestión Ambiental que permitan controlar y/o mitigar los impactos negativos significativos de la entidad.*
- *Identificar los peligros, evaluar y valorar los riesgos estableciendo los respectivos controles para prevenir y mitigar los accidentes de trabajo, lesiones y enfermedades laborales, así como proteger la Seguridad y Salud en el Trabajo de todos los funcionarios, contratistas, subcontratista y visitantes de la SDA, mediante la desarrollo continuo del SG-SST, fomentando una cultura preventiva y de auto cuidado, en cumplimiento con la normatividad nacional legal vigente aplicable en materia de riesgos laborales.*
- ***Mantener la confidencialidad, integridad, disponibilidad de los activos de información, y la protección de datos personales, mediante la gestión los riesgos, que permita establecer un marco de confianza a las partes interesadas en concordancia con la misión y visión de la entidad.***
- *Coordinar y controlar las actividades específicas que afecten la creación, recepción, ubicación, acceso y preservación de los documentos para garantizar la organización y disponibilidad de la documentación e información sirviendo como soporte al cumplimiento de la misión de la entidad, facilitando el acceso y consulta por parte de los usuarios, aplicado los instrumentos archivísticos que apoyan la gestión documental articulado con los sistemas de información en la administración pública.*
- *Promover la eficacia de las operaciones de las entidades y organismos del Estado para que estas logren el cumplimiento de la misión y los objetivos propuestos de acuerdo con la normatividad y políticas del Estado, a través de los principios de autocontrol, autorregulación y autogestión.*
- *Promover la vinculación de la comunidad en procesos ambientalmente sustentables liderados por la Secretaría Distrital de Ambiente.*

MARCO NORMATIVO

Que el artículo 15 de la Constitución Política de Colombia, consagra que *"todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, debiendo el Estado respetarlos y hacerlos respetar. De igual modo, tiene derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas"*. Que el artículo 209 ibidem, establece que, *"la administración pública, en todos sus órdenes, tendrá un control interno, el cual se ejercerá en los términos que señale la ley"*, y así mismo, en el artículo 269 impone a las autoridades de las entidades públicas la obligación de diseñar y aplicar, según la naturaleza de sus funciones, métodos y procedimientos de control interno.

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

Que según la Norma Técnica ISO 27001:2013, el SGSI (Sistema de Gestión de Seguridad de la Información) proporciona un modelo para crear, implementar, hacer funcionar, supervisar, revisar, mantener y mejorar la protección de los activos de información para alcanzar los imperativos estratégicos de la entidad. Un SGSI implica crear un plan de diseño, implementación, y mantenimiento de una serie de procesos que permitan gestionar de manera eficiente la información, para asegurar la integridad, confidencialidad y disponibilidad de la información.

Que la Ley 1712 de 2014 *"Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones",* tiene por objeto *"regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información".*

Que el Decreto 1078 de 2015 Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, subrogado por el Decreto Nacional 1008 de 2018, en el artículo 2.2.9.1.1.3 señala que la Política de Gobierno Digital *"se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3° de la Ley 489 de 1998, 3° de la Ley 1437 de 2011, 2° y 3° de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2° de la Ley 1341 de 2009"*, y en particular los principios de innovación, competitividad, proactividad, seguridad de la información.

Que en el CONPES 3854 de 2016 se establece la Política Nacional de Seguridad Digital en la República de Colombia, para realizar una gestión de riesgos de seguridad digital, con el fin de promover un entorno digital confiable y seguro, que maximice los beneficios económicos y sociales de los colombianos, impulsando la competitividad y productividad en todos los sectores de la economía.

Que el artículo 2.2.9.1.2.1 del Decreto Nacional 1008 de 2018, define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes, que son las líneas de acción que orientan el desarrollo de su implementación, y habilitadores transversales, los cuales, son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los componentes y el logro de los propósitos de la Política de Gobierno Digital.

Que teniendo en cuenta el Modelo de Seguridad y Privacidad de la Información- MSPI, que conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permite garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

Que el Decreto Nacional No. 1083 de 2015, Decreto Único del Sector Función Pública, modificado por el Decreto Nacional No. 1499 de 2017, establece el Modelo Integrado de Planeación y Gestión (MIPG), el cual integra los sistemas de gestión de la calidad y de desarrollo administrativo creando un único sistema de gestión articulado con el sistema de control interno, el cual se actualiza y alinea con los mejores estándares internacionales.

Que mediante el Decreto Distrital 591 de 2018 se adopta para el Distrito Capital el Modelo Integrado de Planeación y Gestión - MIPG de que trata el Decreto Nacional 1083 de 2015, sustituido por el Decreto 1499 de 2017, como marco de referencia para el ajuste del diseño, la implementación y la mejora continua del Sistema Integrado de Gestión Distrital - SIGD, con el fin de fortalecer los mecanismos, métodos y procedimientos de gestión y control al interior de los organismos y entidades del Distrito Capital y adecuar la institucionalidad del sistema y de las instancias correspondientes con el modelo nacional.

Que el numeral 2 del artículo 8 de Decreto Distrital 807 del 24 de diciembre de 2019, indica que la institucionalidad del MIPG en el Distrito Capital está conformada por un conjunto de instancias que de manera coordinada establecen las reglas, condiciones, políticas y metodologías que facilitan la implementación, evaluación y seguimiento del modelo, contando, entre esta instancias, con el Comité Institucional de Gestión y Desempeño, comité encargado de orientar la implementación y seguimiento del Sistema de Gestión y la operación del Modelo Integrado de Planeación y Gestión – MIPG, entre estas las políticas de gestión y desempeño: política de gobierno digital y política de seguridad digital.

Que en los acuerdos marco- mecanismos de agregación de demanda dispuestos por Colombia Compra Eficiente, para facilitar la adquisición de bienes y servicios por parte de las entidades estatales, entre los que se tiene:

Nube Pública III (Acuerdo Marco CCE-908-1-AMP-2019). incluye: 1) Servicios de computación en la Nube, TI que los Cloud Service Providers prestan a través de su infraestructura, entre los cuales se encuentran laaS (Almacenamiento, Computo, Servicio Redes y seguridad de red y perimetral incluye acceso remoto, Backup y Recuperación frente a desastres, entre otros); PaaS (Administración y Gestión de Datos, Desarrollo y ejecución de aplicaciones, Servicios móviles, Integración, Analítica e Inteligencia Artificial, Automatización de procesos y gestión de contenidos, Blockchain, IOT (Internet de las

Cosas), Seguridad, Identidades y Accesos Monitoreo y gestión de plataformas, Servicios de geolocalización y clima, entre otras); 2) servicios de capacitación; 3) servicios profesionales; 4) Servicios de Migración; 5) soluciones; y 6) soporte.

Nube Privada III (CCENEG-017-1-2019): Los servicios de Nube Privada son aquellos que permiten a las Entidades Estatales, acceder a recursos informáticos de laaS (Almacenamiento, Alojamiento, Procesamiento, Seguridad) PaaS y Servicios Complementarios, disponibles a través de Centros de Datos de los proveedores. Para el Segmento 1 el Proveedor deberá contar con dos (2) Centros de Datos, principal y alterno, que permitirán a las Entidades Estatales acceder a servicios laaS (Almacenamiento, Alojamiento, Procesamiento, Seguridad), PaaS y Servicios Complementarios en los niveles de disponibilidad oro y plata. Ei Proveedor del Acuerdo Marco podrá prestar los Servicios de Nube Privada de acuerdo con el nivel de disponibilidad solicitado por la Entidad Estatal. Para el segmento 2. Debido a que el proveedor pondrá a disposición un (1) Centro de Datos, las Entidades Estatales no contarán en este Segmento con servicios de redundancia, ni los servicios relacionados con replicación geográfica o local de datos. El Segmento 2 busca incentivar la adopción y apropiación de los servicios de Nube Privada a entidades del orden territorial.

1. OBJETIVO

Establecer las políticas de seguridad de la información para preservar la confidencialidad, integridad, disponibilidad de los activos de información, la protección de datos personales**,** mediante la gestión de los riesgos, que permita además establecer un marco de confianza a las partes interesadas en concordancia con la plataforma estratégica de la entidad.

2. ALCANCE

La política del SGSI aplica a todos los funcionarios, contratistas, proveedores, aquellas personas o terceros que, debido al cumplimiento de sus funciones u obligaciones, compartan, utilicen, recolecten, procesen, intercambien o consulten su información, así como los entes de control, entidades relacionadas que accedan, ya sea interna o externa a cualquier archivo de información, independiente de su ubicación. Así mismo, esta Política aplica a toda la información creada, procesada o utilizada por la SDA, sin importar el medio, formato o presentación o lugar.

3. AUTORIDAD Y RESPONSABILIDAD

La Secretaría Distrital de Ambiente establece como máxima autoridad del Sistema de Gestión de Seguridad de la Información al Comité Institucional de Gestión y Desempeño quien es responsable de la orientación estratégica para la administración de los activos de información, la sostenibilidad y mejora del Sistema en la Entidad.

Según la “Guía para la gestión de solicitudes de evaluación de una iniciativa o proyecto de tecnología de la información” se cuenta con el modelo de gobierno para gestionar las solicitudes de evaluación de iniciativa o proyecto de TI, mediante la organización interna de

un Comité ejecutivo de TIC y de mesas técnicas integradas por profesionales de la dependencia conforme a su conocimiento y experticia. En este sentido la mesa de Seguridad y privacidad de la Información lidera y gestiona bajo los lineamientos de la Política de Gobierno Digital y las normas en seguridad de la información, la elaboración, diagnóstico, implementación y seguimiento del Modelo de Seguridad y Privacidad de la información-MSPI de la Secretaría Distrital de Ambiente.

Todos los servidores públicos, funcionarios y contratistas, así como proveedores y usuarios son responsables de la aplicación de las políticas de seguridad y privacidad de la información.

4. GLOSARIO

GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL: es el conjunto de actividades coordinadas dentro de una organización, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital sean apropiadas para el riesgo y los objetivos económicos y sociales.

INFRAESTRUCTURA CRÍTICA CIBERNÉTICA NACIONAL: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

LINEAMIENTOS TI: Son reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. En sí, son especificaciones técnicas que tienen una función instrumental que responden a cómo se implementa una política. Pueden cambiar con frecuencia debido a que los procedimientos manuales, estructura organizacional, procesos del negocio y las tecnologías de la información que se mencionan cambian rápidamente. Son también llamadas política específica o de ámbito técnico. Para efecto de este manual, solo serán llamados lineamientos.

MEJORES PRÁCTICAS: Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

POLITICAS TI: Son directrices u orientaciones que debe generar la DTI y que indican la intención de la alta gerencia, con el propósito de establecer pautas para lograr los objetivos propuestos en la estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas y terceros y que por sus funciones deben tener acceso a la información y a su infraestructura).

RIESGO DE SEGURIDAD DIGITAL: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

SEGURIDAD DE LA INFORMACIÓN: La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información. Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información.

SEGURIDAD DIGITAL: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante la gestión del riesgo de seguridad digital; la implementación efectiva de medidas de ciberseguridad; y el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

SOFTWARE: Son aquellos elementos informáticos, sobre los cuales la Secretaría Distrital de Gobierno, tiene el derecho de uso o de propiedad intelectual, que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión. Están conformados entre otros por: A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones

SOFTWARE AUTORIZADO: Sistemas operacionales, paquetes de usuario final y aplicativos, que la Dirección de Tecnología de la Información ha instalado, previo visto bueno para su adquisición, actualización o renovación y con la Autorización legal del proveedor para su uso, o si se trata de licencias otorgadas con el código fuente, para generar modificaciones al mismo. El uso de Software no autorizado o adquirido ilegalmente se considera como una violación a los derechos de autor, previsto en la Ley 603 de 2000.

SOFTWARE LICENCIADO: Se refiere a la obtención del derecho para uso del software de computador.

5. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La SDA adopta las siguientes políticas de seguridad de la información, como compromiso y responsabilidad que tiene la entidad con la confidencialidad, integridad y disponibilidad de la información, de acuerdo con el numeral 4.2.1 literal b. de la Norma Técnica NTC-ISO 27001 de 2013, las cuales se implementan a partir de los planes, procedimientos y controles, asegurando la integración de los requisitos del sistema de seguridad en los procesos de la entidad, así como los recursos necesarios para su implementación y operatividad.

5.1. SEGURIDAD DE LOS RECURSOS HUMANOS

La Secretaría Distrital de Ambiente garantizará procesos de selección de personal de acuerdo con los lineamientos dados por la norma vigente, realizando las verificaciones necesarias para confirmar la veracidad de la información suministrada por el funcionario o contratista candidato a contratar.

La Dirección de Gestión Corporativa y a su vez la Subdirección Contractual debe velar porque los contratos de proveedores y contratistas que desarrollen dentro de sus actividades el manejo de información sensible de la entidad cuenten con cláusulas contractuales respecto a la propiedad intelectual, cláusulas de confidencialidad y manejo de seguridad de información perteneciente a la SDA.

El personal provisto por terceras partes que realicen labores en o para la Secretaría Distrital de Ambiente, se acoge a las *Cláusulas de Confidencialidad* y a *las políticas de seguridad de la información* descritas contractualmente, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

De igual forma, la entidad propenderá por la generación de la cultura de los funcionarios y contratistas de la SDA con relación a la seguridad de la información, con el fin de reducir el riesgo, gestionar adecuadamente los activos y proteger las instalaciones, así como con los demás procedimientos y puntos de control generados dentro del marco del Sistema de Gestión de Seguridad de la Información.

5.2. GESTIÓN DE ACTIVOS

La Secretaría Distrital de Ambiente establece métodos de protección para la propiedad legal del contenido de cualquier documento (físico, electrónico y digital) que se genere, obtenga, adquiera, transforme o controle durante el desarrollo de sus funciones.

La entidad se compromete mediante los líderes de los procesos y responsables, a identificar y proteger los activos de información, con el fin de garantizar su administración y control.

Los activos de información deberán ser identificados y/o actualizados cada vez que sea requerido por el líder de proceso asociado, y será asistido por el enlace del Sistema Integrado de Gestión, quienes deberán determinar la clasificación de los activos de

información de acuerdo con la criticidad, sensibilidad y reserva de esta, teniendo en cuenta la Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014, Decreto 103 de 2015, entre otras que puedan aplicar de acuerdo con la naturaleza de la entidad, con el acompañamiento de la Dirección Legal Ambiental o un profesional en el área del Derecho que tenga las dependencia.

La identificación y/o actualización deberá registrarse en el formato establecido por el Sistema Integrado de Gestión.

5.2.1. Etiquetado de la Información

Los documentos clasificados serán manejados, preparados, copiados y entregados sólo al personal autorizado. Se establecerán acuerdos periódicos para revisiones de seguridad en la producción y copiado.

En cada dependencia se destinará un espacio físico adecuado para archivar los documentos de manera clasificada según la codificación definida por la Secretaria Distrital de Ambiente, conforme a los lineamientos de la gestión documental de la entidad.

La utilización de equipos de reproducción tales como fotocopiadoras, impresoras, escáneres para documentos con clasificación RESERVADA o CONFIDENCIAL serán debidamente autorizadas por el supervisor o jefe del funcionario o contratista.

Se tratará como material clasificado los siguientes medios: discos, cintas, bocetos preliminares, notas o bocetos de trabajo, fotografías, plantillas y planos o los que se determinen en los procedimientos de gestión documental.

5.2.2. Devolución de los Activos

Todo funcionario o contratista que se desvincule de la Secretaría Distrital de Ambiente deberá realizar la devolución de activos de información que tenga asignada y en custodia, en el formato de Paz y Salvo para funcionario y para contratista, de acuerdo con los procedimientos establecidos para tal fin.

5.2.3. Gestión de medios removibles

Para un adecuado uso y permiso de los medios removibles de la Secretaría Distrital de Ambiente se tendrán en cuenta los siguientes lineamientos de cumplimiento obligatorio:

Todos los medios removibles administrados por el data center que contengan información sensible o confidencial serán almacenados en un ambiente seguro y vigilado según las especificaciones del fabricante.

En los medios removibles que sean reutilizados por funcionarios o contratista se deberá realizar un borrado seguro de la información encontrada en dicho medio, antes de realizar alguna reasignación.

Se verificará los medios removibles que ya no se utilicen, y que se dispongan para eliminar, retirar o trasladar de las instalaciones de la entidad. La información contenida en los medios removibles será borrada con un procedimiento seguro y documentado. Para el retiro de

dichos medios se debe contar con la autorización de la Dirección de Planeación y Sistemas de Información Ambiental, además se hace exclusión para medios removibles completamente en desuso.

La información crítica o sensible de la entidad que se encuentre almacenada en un medio removible cuya vida útil es menor al tiempo de retención de la información establecida por la entidad, deberá respaldarse en otro medio para su conservación y prevenir pérdida de información.

Cuando se requiera transferir información de archivo de gestión al archivo central deberá almacenarse en el medio disponible para este fin y cuando se requiera pasar la información a archivo histórico se deberá disponer de los medios de transferencia documental para la información clasificada que posee la entidad para este fin.

Es de exclusiva responsabilidad de cada funcionario y contratista tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

En caso de ocurrir pérdida, modificación o daño de la información o del medio, se debe informar al responsable de seguridad de la información o quien haga sus veces, mediante la mesa de servicio de la entidad y el procedimiento de gestión de incidentes de TI.

5.2.4. Disposición de los activos

La Secretaría Distrital de Ambiente establece que la destrucción del material clasificado se debe mantener hasta que sea completamente destruido y verificado. Siempre debe dejarse registro de la destrucción de material RESERVADO Y CONFIDENCIAL.

Los registros de destrucción deberían incluir: la fecha, la firma de la persona que realiza la destrucción y la autorización del procedimiento por parte del jefe inmediato. Para el caso de material RESERVADO Y CONFIDENCIAL, el jefe de la oficina de control interno participará como garante del procedimiento. Estos registros deberán retenerse de acuerdo con lo estipulado en las tablas de retención documental de la entidad.
La destrucción de material clasificado debe realizarse bajo la estricta supervisión del Oficial de Seguridad de la Información o quien haga sus veces.

5.2.5. Dispositivos Móviles

Los dispositivos móviles deben estar integrados a una plataforma de administración controlada por la Secretaría Distrital de Ambiente, la cual debe permitir:

- Configuración de políticas a aplicar en los dispositivos móviles, soporte para la instalación de aplicaciones móviles permitidas por la Entidad, control de contenido, actualización de software, backups y restauraciones, aprovisionamiento y monitoreo de software autorizado, recuperación de información del dispositivo, ubicación del dispositivo, restricción de acceso a redes, desactivación, borrado y bloqueo remotos, configuración segura, aplicación de políticas para usuarios, contraseñas y encripción, validación contra el directorio activo de la Entidad.

- Los dispositivos móviles deben tener contraseña de ingreso y bloqueo del equipo.

Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la SDA con el fin de realizar funciones propias de su cargo o actividades contractuales asignadas en la entidad.

La Secretaría Distrital de Ambiente debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse al procedimientos de backup de la SDA.

En caso de requerir instalación de aplicaciones adicionales en el dispositivo móvil se debe solicitar a la mesa de servicios para su gestión, valoración y posterior aprobación si es el caso, y configuración en el MDM.

Ante la pérdida del equipo, ya sea por sustracción o extravío, deberá dar cuenta en forma inmediata a la Dirección de Gestión Corporativa como dependencia que administra el Almacén de la Secretaría Distrital de Ambiente.

La Dirección de Gestión Corporativa debe instalar un software de antivirus para los dispositivos móviles institucionales.

Los usuarios deben evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, o conexiones de establecimientos públicos como hoteles, cafés internet, redes públicas, entre otros.

5.3. CONTROL DE ACCESO

La Secretaría Distrital de Ambiente gestiona el control de acceso de los funcionarios, contratistas, proveedores y usuarios a las redes, aplicaciones, información física, sistemas de información, e instalaciones de procesamiento de información.

Es responsabilidad de la Dirección de Planeación y Sistemas de información Ambiental y de la Dirección de Gestión Corporativa:

- Gestionar el control de acceso a los sistemas y servicios por medio de equipos de seguridad perimetral, administración de aplicativos, sistemas de información, bases de datos, portal cautivo y controladores de dominio a servidores públicos y terceros.
- Mantener los registros donde cada uno de los líderes responsables de los procesos que haya autorizado a los servidores públicos o terceros, el acceso a los diferentes sistemas de información de la entidad.
- Establecer y verificar que los datos de acceso a los sistemas están compuestos por un nombre de usuario, una contraseña y que sean únicos para cada servidor público o tercero.
- En caso de retiro, terminación, jubilación, suspensión, cesión o cambio de cualquier servidor público o tercero, se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado.

- Asignar las contraseñas de acceso que deberán cumplir con un mínimo de 8 caracteres y la combinación de números, letras mayúsculas y minúsculas, en lo posible utilizar caracteres especiales.
- Mantener la regla de cambio de contraseña con una periodicidad de 45 días como política de seguridad para el cambio de contraseña.

Es responsabilidad de los usuarios de la Secretaría Distrital de ambiente:

- Las contraseñas serán de uso personal e intransferible y no se deben escribir en medios físicos (documentos, notas o archivos).
- No se debe habilitar la opción – "recordar clave en este equipo", que ofrecen los programas.
- Cambia tu contraseña si piensas que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Selecciona contraseñas que no sean fáciles de descifrar
- No utilizar la opción de almacenar contraseñas en Internet.
- No utilizar contraseña con números telefónicos, nombre de familia, etc.

La Secretaría Distrital de Ambiente se compromete a regular el acceso a la información bajo su control o custodia de acuerdo a su clasificación a través de disposiciones relacionadas con perfiles de usuario (y los ítems de seguridad que ello implique), delimitando y otorgando autorización para el acceso a la información de acuerdo a la labor propia de cada servidor público, así como la demarcación de perímetros de seguridad para zonas con infraestructura crítica de información, a estas dependencias ingresarán únicamente personal autorizado y se tendrá e implementará los debidos controles para su uso y operación.

5.3.1. Uso adecuado de internet

La Dirección de Planeación y Sistemas de Información Ambiental debe proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso establecidos.

La Dirección de Planeación y Sistemas de Información Ambiental debe monitorear continuamente el canal o canales del servicio de Internet.

La Dirección de Planeación y Sistemas de Información Ambiental debe establecer procedimientos y junto con la Dirección de Gestión Corporativa implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos y de alta peligrosidad.

La Dirección de Planeación y Sistemas de Información Ambiental debe generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implantar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Los usuarios del servicio de Internet deben evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus labores diarias.

No se permite el acceso a páginas relacionadas con pornografía, drogas, alcohol, violencia, hacking y/o cualquier otra página que vaya en contra de la ética moral, las leyes vigentes o políticas establecidas en este documento.

No se permite la descarga, uso, intercambio y/o instalación de juegos, aplicaciones web de uso personal, redes sociales, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica de la entidad.

No se permite el intercambio no autorizado de información de propiedad de la Secretaría Distrital de Ambiente, de sus clientes y/o de sus funcionarios, con terceros.

5.3.2. No repudio

La Secretaria Distrital de Ambiente debe producir, validar, mantener, y poner a disposición de la entidad, pruebas o evidencias irrefutables respecto a la transferencia de información en cada uno de sus procesos a nivel interno y externo, buscando información suficiente sobre la ocurrencia de un evento, el momento en el que ocurrió y las partes que intervinieron.

- La Secretaria Distrital de Ambiente debe hacer uso de mecanismos criptográficos: firmas digitales, cifrado de mensajes, códigos de autenticación de mensajes, etc.

- La Secretaria Distrital de Ambiente establecerá el procedimiento de No-repudio de Origen proporcionando al receptor de un objeto digital una prueba infalsificable del origen de dicho objeto, lo cual evitará que el emisor niegue el envío de la información o tenga éxito ante el juicio de terceros.

- La Secretaria Distrital de Ambiente establecerá el procedimiento de No-repudio de Recepción proporcionando al emisor la prueba de que el destinatario legítimo de un mensaje u objeto digital genérico, realmente lo recibió, evitando que el receptor lo niegue posteriormente y consiga sus pretensiones.

- La Secretaría Distrital de Ambiente deberá documentar las evidencia de No-repudio, por medio de registros compuesto por cuatro fases distintas. En primer lugar, la fase de generación de la evidencia; en segundo lugar, la fase de transferencia; en tercer lugar, la fase de verificación y almacenamiento de la evidencia, que consiste en comprobar la firma digital y guardar la información para un uso posterior; y, por último, la fase de resolución de disputas, en caso de que éstas tengan lugar.

5.3.3. Correo electrónico

El correo electrónico de la SDA con dominio *@ambientebogota.gov.co* es proporcionado para apoyar las comunicaciones de los funcionarios y contratistas de la SDA, para el uso apropiado se requiere cumplir con lineamientos expresos y sin excepción en los equipos de cómputo, dispositivos móviles, aplicaciones o navegadores. Con el objetivo de cumplir con el criterio de buen uso del correo electrónico se debe cumplir con lo siguiente:

- El usuario es responsable de todas las actividades realizadas con sus cuentas de acceso al buzón y cuenta de usuario asignado en la entidad.
- Es una falta grave entregar credenciales y ofrecer su cuenta de correo electrónico (e-mail) a personas no autorizadas, su cuenta es exclusiva del cargo, está es intransferible.
- El correo electrónico es una herramienta para el intercambio de información entre personas, no debe ser usada para difusión de información masiva tipo spam o cadenas.
- El usuario debe verificar los destinatarios y no enviar correos a cuentas que no desean recibir información relacionada con la SDA.
- Están prohibido utilizar el correo electrónico para cualquier propósito comercial o financiero.
- No se debe propagar “cartas en cadenas”, ni en esquemas piramidales de índole personal, político, religioso o inapropiado.
- Periódicamente la administración de cuentas de correo revisará que cuentas llevan más de 60 días sin ningún acceso, en caso tal, se procederá a enviar una comunicación de las cuentas sin uso y se darán 30 días adicionales a partir de la fecha de la comunicación para la utilización de las cuentas. Vencidos los treinta días, de no presentarse uso se procederá a su eliminación y se entenderá que el usuario ya ha sido comunicado y se tomaran las medidas necesarias para hacer uso de la licencia.
- El uso inapropiado de las cuentas de correo suministradas por la SDA, así como la violación a las políticas de uso descritas, tendrá como consecuencia la desactivación temporal o permanente.
- El password o clave que se establece es generado automáticamente, se recomienda cambiarlo la primera vez que acceda a la plataforma de correo electrónico de Google (Gmail).
- No se pueden enviar archivos adjuntos con extensión ejecutable (programas, librerías, aplicaciones, etc.)
- Se recomienda hacer backup periódico cada 30 días, la información contenida en el buzón es de completa responsabilidad del usuario, en caso de eliminación accidental de correos electrónicos, inclusive de la papelera, pida a poyo en la mesa de ayuda. No se asegura una recuperación de los correos al 100%.
- Si por cualquier razón el usuario sospecha o sabe que la seguridad de su cuenta se ve comprometida de cualquier forma, debe reiniciar su contraseña e informar al oficial de seguridad de la información. Por seguridad se recomienda que la Entidad cambie las contraseñas de sus cuentas mínimo cada cuarenta y cinco (45) días.
- La SDA se compromete a no ceder a terceros su información. Cada usuario es responsable de la información que maneja sobre todo si esta es sensible o confidencial.

5.3.4. Drive y carpetas compartidas

El drive es un servicio que proporciona un lugar de almacenamiento para los archivos, así como la posibilidad de crear documentos de texto, hojas de cálculo, presentaciones, formularios y carpetas. Además, permite compartirlos con otros usuarios. Todas las cuentas de usuario de la SDA tienen acceso a un espacio personal de almacenamiento en la nube y un espacio compartido con todos los usuarios de una dependencia.

- La publicación y distribución de cualquier tipo de contenido mediante Google drive o las aplicaciones vinculadas a las cuentas de G Suite deberán realizarse de acuerdo con la legislación vigente sobre protección de datos de carácter personal.
- El contenido en Google drive de las carpetas compartidas, debe albergar documentos finales o aprobados. Las carpetas de las cuentas personales pueden almacenar documentos de trabajo o documentos finalizados. Por ninguna razón se debe transferir a las carpetas información personal excepto si está es soporte de una actuación pública o parte de la gestión contractual con la SDA.
- Queda prohibido el uso de las cuentas de Google drive, los servicios y aplicaciones vinculados a ella para actividades financieras, comerciales o publicitarias.
- Los usuarios son responsables de todas las actividades realizadas con sus cuentas de Google Drive.
- Es una falta grave facilitar y ofrecer acceso a la propia cuenta a personas no autorizadas por la SDA o su representante legal.

Unidad compartida: La unidad compartida de Google **Drive** permite almacenar, buscar y acceder a archivos en un espacio compartido por un grupo, información que pertenece al grupo y no a un usuario concreto.

- La información institucional gestionada por las diferentes áreas debe estar registrada en la unidad compartida asignada a cada dependencia.
- La estructura de las carpetas y archivos de la unidad estará a cargo del gestor designado por el jefe de cada área.
- Cualquier modificación en el contenido las carpetas y /o archivos deberá ser tramitada por el área a través del gestor designado.
- Esta unidad solo debe tener registrada información institucional.

5.4. CRIPTOGRAFÍA

Con el fin de conservar la confidencialidad, integridad, privacidad, autenticidad y no repudio de la información, la Secretaría Distrital de Ambiente utiliza controles criptográficos en los siguientes casos:

- Uso de aplicativos, enlaces de comunicaciones, y protección de dispositivos portables.
- Protección de claves de acceso a sistemas, datos y servicios.
- Transmisión de información clasificada, fuera del ámbito de la entidad

La gestión de claves se realiza a través del Directorio Activo durante todo su ciclo de vida. Las claves criptográficas que por alguna razón se vuelven no seguras o aquellas que ya no

son usadas por algún usuario o grupo deben ser eliminadas del sistema para evitar comprometer la información.

5.5. SEGURIDAD FÍSICA Y DEL ENTORNO

La Secretaría Distrital de Ambiente se compromete a proteger las áreas destinadas al procesamiento o almacenamiento de información sensible y aquellas donde se encuentra la infraestructura de servidores que dan soporte a los sistemas de información y comunicaciones, considerándolas áreas de acceso restringido a través de medidas de control de acceso físico, así como estableciendo métodos de protección para la infraestructura tecnológica al servicio de la Entidad, con el fin de prevenir su pérdida o daño por situaciones internas, externas, ambientales, de seguridad perimetral o de uso.

Con relación a las instalaciones de la Entidad, la Secretaría Distrital de Ambiente se compromete a gestionar constantemente sistemas de vigilancia y seguridad perimetral, así como planes de mantenimiento para la salvaguarda de un ambiente seguro e idóneo para las actividades desarrolladas en cada una de sus sedes.

5.6. SEGURIDAD DE LAS OPERACIONES

La DPSIA debe tener una serie de normas que rijan la seguridad de las operaciones, el comportamiento tanto de los funcionarios y contratistas que ahí laboran como de los que hacen uso de las facilidades que esta dirección les proporciona; a continuación, presentamos las normas requeridas.

5.6.1. Teletrabajo

La Secretaria Distrital de Ambiente implementará los controles adecuados para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información en un ambiente de teletrabajo, asignando permisos, generando autenticaciones y conexiones seguras de acuerdo con la sensibilidad de la información por acceder, verificando los aspectos de seguridad física, del entorno y el suministro de elementos tecnológicos.

5.6.2. Trabajo en casa

La Secretaria Distrital de Ambiente deberá recomendar la implementación de controles adecuados para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información para el trabajo en casa, dentro de los cuales se encuentran:

- Realizar copias de seguridad de manera periódica de la información gestionada en los equipos utilizados en trabajo en casa, haciendo uso de los medios de almacenamiento que la Entidad disponga para tal fin.
- Evitar el envío de archivos con información de la entidad, por medios no oficiales como whatsapp, dropbox, wetransfer, correos de dominio gratuito, etc.
- Cerrar la sesión cuando no se esté usando el dispositivo, tanto en casa como en lugares públicos.
- Mantener actualizado el sistema operativo con los últimos parches de seguridad liberados por el fabricante, si trabaja desde su propio dispositivo.

- Instalar y mantener actualizado el software antivirus, de un fabricante reconocido, para evitar infecciones con virus o software malicioso.
- Tener un espacio adecuado para trabajar en casa sin riesgo a perder información, por algún tipo de accidente.

No instalar programas o extensiones de navegadores de fuentes desconocidas ya que estas suelen traer malware el cual puede afectar sus dispositivos y extraer la información sensible.

5.6.3. Escritorio y pantalla limpios

La Secretaría Distrital de Ambiente promoverá la cultura de escritorio y pantalla limpios, donde cada servidor público de la entidad se compromete a mantener protegida la información en sus áreas de trabajo a través de la correcta custodia y disposición de documentos, CD, dispositivo USB, y cualquier otro medio de almacenamiento, así como bloqueando la sesión de su estación de trabajo en el momento en que se ausente.
De igual forma existe el compromiso de mantener la pantalla de inicio del equipo de cómputo libre de archivos, salvo los accesos directos a las aplicaciones necesarias para su labor.
Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

5.7. SEGURIDAD DE LAS COMUNICACIONES

Las redes deben ser administradas y controladas para proteger la información en los sistemas y aplicaciones. Además, cuentan con dispositivos de seguridad y niveles de servicio apropiados. Se establecerán mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones.

La Secretaría Distrital de Ambiente debe contar con segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La división de estos segmentos debe ser realizada por medio de dispositivos perimetrales e internos de enrutamiento y de seguridad si así se requiere.

5.8. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

5.8.1. Mantenimiento físico de las operaciones

La Secretaría Distrital de Ambiente deberá generar acciones de seguridad constantes basadas en la planificación de la operación, controlando los procesos y ejecutando los planes que permitan cumplir con los objetivos propuestos por el Sistema de Gestión de Seguridad y Privacidad de la Información, con base a la valoración y tratamiento de los riesgos evidenciados para cada uno de los activos de información de la entidad. Toda labor realizada debe contar con la correcta documentación sobre los planes ejecutados y los métodos usados para garantizar la salvaguarda de la información.

La Secretaría Distrital de Ambiente garantiza que el Data Center se encuentre separado de áreas que tengan líquidos inflamables o estén en riesgo de inundaciones e incendios, implementando mecanismos de revisión y control del ingreso de cualquier tipo de material

al Centro de Cómputo, además deben existir sistemas de detección y extinción automáticas de incendios e inundación y alarmas en caso de detectarse condiciones inapropiadas.

Los niveles de temperatura y humedad relativa en el Data Center deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo allí instalada, para lo cual se deben usar sistemas de aire acondicionado.

Se debe monitorear y revisar de manera permanente el estado de los componentes de soporte físico, eléctrico y ambiental que hacen parte del Centro de Cómputo, como son el sistema de aire acondicionado y el sistema de detección y extinción de incendios, entre otros.

Cuando se realicen trabajos de mantenimiento correctivo en redes eléctricas, cableados de datos y voz, deben ser realizados por personal especializado y debidamente autorizado e identificado.

Se deben realizar mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS, plantas eléctricas, y sistema de aire acondicionado.

Se deben realizar mantenimientos preventivos y correctivos de los servidores, equipos de comunicaciones y de seguridad que conforman la plataforma tecnológica de la Secretaría Distrital de Ambiente.

5.8.2. Ambiente de desarrollo seguro

La SDA debe garantizar un ambiente de desarrollo seguro durante la ejecución de los proyectos, arquitecturas, software o sistemas, estableciendo metodologías que incluya requisitos de seguridad en cada una de las fases del proyecto, acuerdos de soporte y niveles de servicio a terceros, y separación física y virtual en los ambientes de operación, todo a través de técnicas de programación seguras. Así mismo, cada sistema de información deberá contar con sus manuales de uso y técnicos disponibles de acuerdo con los niveles de protección de la información dados para estos datos, así como la arquitectura del software.

Los administradores de los sistemas de información son responsables de realizar las pruebas para asegurar que cumplen con los requerimientos de funcionamiento establecidos antes del paso a producción de los sistemas. Estas pruebas deben realizarse por entrega de funcionalidades nuevas, por ajustes de funcionalidad o por cambios sobre la plataforma tecnológica.

Los propietarios de los sistemas de información deben aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

La Secretaría Distrital de Ambiente debe implantar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas por el equipo de control de cambios o el líder de desarrollo. Se debe contar con

sistemas de control de versiones para administrar los cambios de los sistemas de información.

Los desarrolladores de los sistemas de información de la SDA deben considerar las buenas prácticas y lineamientos de desarrollo seguro durante el ciclo de vida de estos, pasando desde el diseño hasta la puesta en marcha.

Los desarrolladores de la SDA deben construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

Se deben asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla, teniendo en cuenta aspectos como: tipos de datos, rangos válidos, longitud, listas de caracteres aceptados, caracteres considerados peligrosos y caracteres de alteración de rutas, entre otros.

Los aplicativos desarrollados proporcionarán la mínima información de la sesión establecida, almacenada en cookies y complementos, entre otros.

Se debe garantizar que no se divulgue información sensible en respuestas de error, incluyendo detalles del sistema, identificadores de sesión o información de las cuentas de usuarios; así mismo, deben implementar mensajes de error genéricos.

Las funcionalidades y archivos que no sean necesarios para los aplicativos se removerán, previo a la puesta en producción, además se debe prevenir la revelación de la estructura de directorios de los sistemas de información construidos.

Los desarrolladores de la SDA deben implementar los controles necesarios para la transferencia de archivos, como exigir autenticación, vigilar los tipos de archivos a transmitir, almacenar los archivos transferidos en repositorios destinados para este fin o en bases de datos, eliminar privilegios de ejecución a los archivos transferidos y asegurar que dichos archivos sólo tengan privilegios de lectura.

Se debe proteger el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado ni modificado por los usuarios. Además, no se debe permitir que los aplicativos desarrollados ejecuten comandos directamente en el sistema operativo.

5.8.3. Gestión del cambio

La Secretaría Distrital de Ambiente debe establecer una metodología sobre las labores de control de cambio para el software en producción, comunicaciones y en general cualquier modificación de la infraestructura tecnológica, con el objetivo de no afectar la seguridad de los activos de información, evaluando los riesgos ante los cambios previstos y verificar su correcta implementación, reduciendo lo máximo posible la afectación en la operatividad de la entidad.

5.8.4. Gestión de vulnerabilidades técnicas

La Secretaría Distrital de Ambiente identificará vulnerabilidades técnicas del conjunto de plataformas tecnológicas, de comunicaciones y de seguridad que soporten los activos de información, con el fin de proponer actividades para gestionarlas, de acuerdo con los controles establecidos.

5.8.5. Transferencia de información

Con el fin de mantener la seguridad de los activos de información de la entidad, la Secretaría Distrital de Ambiente establecerá acuerdos de confidencialidad con los funcionarios, contratistas y partes interesadas que por diferentes razones requieran conocer o intercambiar información clasificada y reservada, de acuerdo con los niveles y perfiles de autorización para acceso, modificación, divulgación y eliminación de la información dada por los propietarios. De igual forma el supervisor del contrato o jefe inmediato debe asegurar que todos los activos sean devueltos y la información pertinente sea transferida, de acuerdo con los procedimientos establecidos para tal fin.

Los terceros con quienes se intercambia información sensible de la Secretaría Distrital de Ambiente deben destruir de manera segura la información suministrada, una vez esta cumpla con la función para la cual fue enviada y demostrar la realización de las actividades de destrucción.

No está permitido el intercambio de información sensible de la Secretaría Distrital de Ambiente por vía telefónica y/o correo electrónico.

La Secretaria Distrital de Ambiente debe garantizar soluciones de intercambio de información seguros, así como adoptar controles de cifrado de información que permitan el cumplimiento del procedimiento para el intercambio de información en cada uno de los medios utilizados.

5.8.6. Copias de respaldo de la información

La información definida y contenida en la plataforma tecnológica de la entidad, como servidores, archivo de configuración, dispositivos de red, estaciones de trabajo, entre otros, debe ser periódicamente resguardada mediante mecanismos y controles adecuados que garanticen la confidencialidad, integridad y disponibilidad de la información, realizándolas conforme al procedimiento adoptado por la entidad.

Las dependencias encargadas de la información en conjunto con la Dirección de Planeación y Sistemas de Información Ambiental y la Dirección de Gestión Corporativa deberán definir y aplicar la estrategia a seguir para el respaldo y almacenamiento de la información, validando las copias a intervalos regulares.

La Secretaria Distrital de Ambiente velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

La información que reposa en las estaciones de trabajo, serán de responsabilidad directa de cada usuario, en caso de requerir copia de la misma, esta deberá ser solicitada a la Dirección Corporativa previa autorización del jefe inmediato, en caso de ser persona distinta al dueño de la información.

5.9. RELACIONES CON LOS PROVEEDORES

La Secretaría Distrital de Ambiente deberá establecer métodos y requisitos para el control de la información con relación al acceso, procesamiento, almacenamiento, comunicación o suministro de componentes de infraestructura de TI, garantizando el aislamiento de los sistemas de información ante posibles conexiones y accesos inseguros.

Durante la ejecución del contrato, todas las actividades realizadas en los sistemas de información por parte de los proveedores deben ser monitoreadas por el supervisor o el profesional encargado a quien se le presta el servicio o producto.
En caso de evidenciar abuso en los accesos se reportará el incidente respectivo conforme al procedimiento establecido.

5.10. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Secretaria Distrital de Ambiente comprometida con la mejora continua del SGSI, establecerá y ejecutará procedimientos para identificar, analizar, valorar, tratar y aprender de los incidentes de seguridad de la información que se presenten en la Entidad.

Todo servidor público deberá reportar los eventos o incidentes de seguridad que se presenten junto con los registros o soportes que se posean, realizando la correcta identificación, recolección, adquisición y preservación de estos, según el procedimiento de gestión de incidentes que tenga vigente la entidad.

La Alta Dirección o a quien delegue, serán los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos para hacer pronunciamientos oficiales ante entidades externas, a través de los canales de comunicación autorizados.

5.11. GESTIÓN DE CONTINUIDAD DE NEGOCIO

La Entidad establecerá una estructura de gestión adecuada para mitigar y responder a una crisis, desastre o incidente, usando personal con la autoridad, experiencia y competencia necesarias, desarrollando y aprobando planes, procedimientos de respuesta, retorno y recuperación, poniéndolos a prueba para asegurar que son coherentes con los objetivos de seguridad en la continuidad de negocio, con el fin de lograr que los procesos críticos tengan instalaciones alternas y sus activos de información cuando se requieran.

5.12. CUMPLIMIENTO

La Secretaria Distrital de Ambiente sancionará cualquier violación a esta política o procedimiento establecido en el Sistema de Gestión de la Seguridad y Privacidad de la

información SGSPI, de acuerdo con lo establecido en la ley de delitos informáticos 1273 del 2009 y demás aplicables.

La Secretaria Distrital de Ambiente velará por el cumplimiento de la legislación relacionada con la seguridad de la información, entre ella la referente a derechos de autor y propiedad intelectual.

Todo servidor público en la SDA es responsable de registrar y reportar las violaciones a la seguridad, confirmadas o sospechadas, además será responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política.

5.13. PRIVACIDAD Y CONFIDENCIALIDAD

La Secretaría Distrital de Ambiente establece controles, instalando las medidas técnicas y organizativas necesarias para evitar la pérdida, mal uso, alteración, acceso no autorizado y robo de los datos facilitados por los usuarios, en cumplimiento de la Ley Estatutaria 1581 de 2012, Decreto 1377 de 2013 y demás normativa vigente en el tema. La Entidad, en ninguna circunstancia utilizará la información recopilada para otra acción diferente a su misionalidad y al objeto de recolección, previa autorización informada del titular de los datos a excepción de los terceros autorizados por el titular o por la ley.

Entiéndase como datos personales los siguientes tipos de datos:

- *De Identificación*: Nombre, apellido, tipo de identificación, número de identificación, fecha y lugar de expedición, nombre, estado civil, sexo, firma, nacionalidad, datos de familia, firma electrónica, otros documentos de identificación, lugar y fecha de nacimiento o muerte, edad, huella, ADN, iris, Geometría facial o corporal, fotografías, vídeos, fórmula dactiloscópica, voz, etc.

- *De Ubicación*: como los relacionados con la actividad comercial o privada de las personas como dirección, teléfono, correo electrónico, etc.

- *De contenido socioeconómico*: como estrato, propiedad de la vivienda, Datos financieros, crediticios y/o de carácter económico de las personas, Datos patrimoniales como bienes muebles e inmuebles, ingresos, egresos, inversiones, historia laboral, experiencia laboral, cargo, fechas de ingreso y retiro, anotaciones, llamados de atención, nivel educativo, capacitación y/o historial académico de la persona, etc.

- *Sensibles*: como los relacionados con la salud de la persona en cuanto a órdenes y relación de pruebas complementarias como laboratorio, imágenes diagnósticas, endoscópicas, patológicas, estudios, etc. diagnósticos médicos, generales o especializados, psicológicos o psiquiátricos, medicamentos y/o tratamientos médicos o terapéuticos de cualquier tipo, los relacionados con la pertenencia a sindicatos, organizaciones sociales, de derechos humanos, religiosas, políticas; datos relacionados con las convicciones religiosas, filosóficas y/o políticas, los datos de preferencia, identidad y orientación sexual de la persona, origen étnico-racial, personas de la tercera edad o menores de 18 años en condición de pobreza, datos sobre

personas en situación de discapacidad personas con limitaciones psicomotoras, auditivas y visuales en condiciones de pobreza, personas víctimas de la violencia, personas en situación de desplazamiento forzado por violencia, madres gestantes o lactantes o cabeza de familia en situación de vulnerabilidad, menores en condición de abandono o protección, etc.

5.13.1. Responsabilidades de los funcionarios y contratistas en el manejo de datos personales

Es responsabilidad de funcionarios y contratistas garantizar la protección de los datos personales que se obtengan del ejercicio misional de los usuarios y ciudadanía en general, tal y como lo establece la Circular SDA No. 1 de 2013.

5.13.2. Manejo de datos personales para ingreso a la entidad

La Secretaría Distrital de Ambiente, como responsable del tratamiento de los datos personales de las personas naturales que ingresan a la entidad, solicitará la autorización al usuario para el tratamiento, recolección, almacenamiento, gestión y eliminación de sus datos personales.

Los datos personales que se entregan por parte de las personas al ingreso de la SDA, tales como huella digital e imágenes (datos sensibles), nombre y número de cédula, sólo serán usados para efectos de control de acceso de visitantes a las instalaciones y por ende no serán transferidos ni comercializados con terceros. Solo se solicitarán datos personales estrictamente necesarios para los fines mencionados y tales datos serán obtenidos bajo los principios de finalidad, calidad, circulación restringida en la ley 1581 de 2012.

5.13.3. Derechos de los titulares de los datos personales

Los titulares de la información cuyos datos personales sean objeto de tratamiento por parte de Secretaría Distrital de Ambiente podrán conocer en cualquier momento los datos personales sobre los cuales la SDA está realizando el tratamiento. De igual manera, el titular puede solicitar en cualquier momento, que sus datos sean actualizados o rectificados. El titular de la información debe ser informado por la SDA, previa solicitud, respecto del uso que ésta les ha dado a sus datos personales.

El titular de la información podrá solicitar a la Secretaría Distrital de Ambiente la eliminación de sus datos personales o revocar la autorización otorgada para el tratamiento de estos, mediante la presentación de una solicitud. No obstante, la supresión de la información y la revocatoria de la autorización no procederán cuando el titular de la información tenga un deber legal o contractual de permanecer en la Base de Datos y/o Archivos, ni mientras se encuentre vigente la relación entre el Titular y la Secretaría Distrital de Ambiente, en virtud de la cual fueron recolectados sus datos.
El titular de la información podrá acceder de forma gratuita a sus datos personales objeto de Tratamiento por parte de la Secretaría Distrital de Ambiente.

Así mismo la entidad no cederá a terceros los datos personales de los usuarios que se obtengan a través de cualquier mecanismo sin su consentimiento expreso. Sin perjuicio de lo anterior, el usuario consiente en que se cedan sus datos personales cuando así sea requerido por las autoridades administrativas competentes o por mandato judicial.

5.13.4. Formato de autorización para el tratamiento de datos personales

Para efectos del tratamiento de los datos personales recolectados, la SDA, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, solicitará a todas las personas su autorización para que, de manera libre, previa, expresa y voluntaria permitan continuar con su tratamiento. Para lo cual deberá utilizarse el siguiente formato tanto en los canales presenciales como en los canales tecnológicos:

Autorización de tratamiento de datos personales

Declaro de manera libre, expresa, inequívoca e informada, que **AUTORIZO** a la **SECRETARIA DISTRITAL DE AMBIENTE** para que, en los términos del literal a) del artículo 6 de la Ley 1581 de 2012, realice la recolección, almacenamiento, uso, circulación, supresión, y en general, tratamiento de mis datos personales, incluyendo datos sensibles, como mis huellas digitales, fotografías, videos y demás datos que puedan llegar a ser considerados como sensibles de conformidad con la Ley, para que dicho tratamiento se realice con el fin de lograr las finalidades relativas a ejecutar el control, seguimiento, monitoreo, y, en general todos los trámites y servicios; así como para garantizar la seguridad de sus instalaciones.

Declaro que se me ha informado de manera clara y comprensible que tengo derecho a conocer, actualizar y rectificar los datos personales proporcionados, a solicitar prueba de esta autorización, a solicitar información sobre el uso que se les ha dado a mis datos personales, a denunciar por el uso indebido de mis datos personales, a revocar esta autorización o solicitar la supresión de los datos personales suministrados y a acceder de forma gratuita a los mismos.

Declaro que la información por mí proporcionada es veraz, completa, exacta, actualizada y verificable.

Mediante la aceptación del presente documento, manifiesto que reconozco y acepto que cualquier consulta o reclamación relacionada con el tratamiento de mis datos personales podrá ser elevada verbalmente o por escrito ante la SDA, como responsable del tratamiento, cuyo portal web es: www.ambientebogota.gov.co, teléfono de atención: +57(1) 3778899, Sede Principal ubicada en la Avenida Caracas No. 54 – 38, Bogotá - Colombia.

NOMBRE: _____
EMPRESA: _____
DIRECCIÓN: _____
CORREO ELECTRÓNICO: _____

¿AUTORIZA EL TRATAMIENTO DE SUS DATOS PERSONALES SENSIBLES? SI___NO___

6. COMUNICACIÓN

Estas políticas deben ser publicadas en el aplicativo ISOLUCIÓN y en la página web de la entidad y comunicada a todos los servidores públicos, proveedores y usuarios de la entidad a través de las herramientas de comunicación interna y externa con las que cuenta la entidad, encaminadas a la apropiación de esta política.

En todo caso, todas las dependencias de la entidad deberán socializar y asistir a la capacitación de seguridad de la información, a fin de dinamizar la cultura de la seguridad de la información en todas las operaciones institucionales.

CONTROL DE CAMBIOS

Versión	Descripción de la modificación	No. Acto Administrativo y fecha
1	Adopción	Resolución 363 del 22 de abril de 2016
2	Actualización de las políticas de seguridad y privacidad de la información, teniendo en cuenta Decreto Nacional 1008 de 2018, entre ellas se actualizaron las políticas de: Seguridad de los recursos humanos y seguridad de las operaciones; se adicionaron políticas de seguridad frente al uso del correo electrónico, el drive y carpetas compartidas, trabajo en casa, seguridad de las comunicaciones; se ajustó la política de adquisición, desarrollo y mantenimiento de sistemas, mantenimiento físico de las operaciones y de Privacidad y confidencialidad; se eliminó política relacionada con controles de revisión y auditoría.	Acta sesión #6 del Comité Institucional de Gestión y Desempeño de la SDA 18 de agosto de 2021.