# POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LA SECRETARÍA DISTRITAL DE AMBIENTE

**PROCESO:**

**GESTIÓN TECNOLÓGICA**

**VERSIÓN: 3**

ALCALDÍA MAYOR DE BOGOTÁ D.C.
SECRETARÍA DE AMBIENTE
BOGOTÁ

**CONTENIDO**

## INTRODUCCIÓN

La Secretaría Distrital de Ambiente - SDA adoptó el Sistema de Gestión de Seguridad de la Información-SGSI siguiendo las recomendaciones dispuestas en el Modelo de Seguridad y Privacidad de la Información - MSPI del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, como una herramienta para garantizar la confidencialidad, integridad y disponibilidad de la información, 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.

Consciente de las necesidades derivadas de sus actividades, la SDA implementa 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.

Con lo anterior, se protege, preserva y administra la integridad, confidencialidad, disponibilidad y autenticidad de la información de la SDA, así como la seguridad digital y la gestión de la continuidad de la operación, conforme al mapa de procesos de la entidad y en cumplimiento de los requisitos legales aplicables a 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 SDA 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 lo establecido en el MSPI el cual toma como base la norma ISO/CEI 27001:2022 “Seguridad de la información, ciberseguridad y protección de privacidad – Sistemas de gestión de la seguridad de la información”; 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.

Así mismo, las políticas identifican responsabilidades y establecen los objetivos para una protección apropiada de los activos de información de la entidad, habilitando a las áreas encargadas para orientar y mejorar la administración de seguridad de los activos de información y proveer las bases para su monitoreo a través de toda la SDA, reduciendo el riesgo de que en forma accidental o intencional se divulguen, modifiquen, destruyan o usen en forma indebida.

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

**El Sistema de Gestión de Seguridad de la Información en el Sistema Integrado de Gestión**

El Sistema Integrado de Gestión es el conjunto de subsistemas, componentes y demás elementos de gestión que permiten y favorecen la integración de las orientaciones, procesos, políticas, metodologías, instancias e instrumentos orientados a garantizar un desempeño institucional articulado, armónico y la satisfacción de las necesidades de sus grupos de valor. El Sistema Integrado de Gestión adoptado por la Secretaria Distrital de Ambiente, se encuentra conformado por siete (7) sistemas, los cuales se articulan con el Modelo Integrado de Planeación y Gestión-MIPG, entre estos el Sistema de Gestión de la Seguridad de la Información (SGSI) que establece, implementa, opera, verifica, revisa, mantiene y mejora la protección de los activos de información requeridos para garantizar la sostenibilidad y el éxito de la Entidad y minimizar impactos por la pérdida de confidencialidad, indisponibilidad o corrupción de la información. [1]

La política del SIG se desarrolla a través de siete objetivos, entre los cuales uno responde directamente a la gestión de la seguridad de la información, como sigue:

- ***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.***

## 1. OBJETIVO

Establecer las políticas de seguridad 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.

### 1.1. Objetivos específicos

La presente política de seguridad de la información está orientada al cumplimiento de los siguientes objetivos específicos:

- Proteger la información de la SDA y de todos los grupos de interés en el marco de su gestión, salvaguardando su confidencialidad, integridad y disponibilidad a través del establecimiento de políticas para mitigar los riesgos que vulneren los activos de información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y demás colaboradores de la SDA.
- Generar confianza en los ciudadanos, colaboradores y demás grupos de interés en las gestiones que se adelanten con la SDA.

[1] MANUAL DEL SISTEMA INTEGRADO DE GESTIÓN, PE03-MA01 Versión: 17 Radicado 2020EE175506 del 08 de octubre 2020. Numeral 7 SIG

- Gestionar y mitigar los riesgos que se puedan presentar para proteger los activos de información de la SDA contra ataques, intrusiones, robo, accesos no autorizados y fuga de información que afecte a la imagen, los intereses y el buen nombre de la SDA.
- Propender por un nivel apropiado de concientización, conocimientos y habilidades necesarios para minimizar la ocurrencia de incidentes de seguridad de la información.
- Garantizar la continuidad del negocio frente a la ocurrencia de incidentes.
- Proteger los activos tecnológicos.

## 2. ALCANCE

Inicia con la descripción de los parámetros y disposiciones de las políticas del SGSI, continua con las políticas específicas de seguridad y privacidad de la información y finaliza con la comunicación de estas.
Las políticas del SGSI aplican a todos los funcionarios, contratistas, proveedores y 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 y entidades relacionadas que accedan, ya sea interna o externa a cualquier archivo de información, independiente de su ubicación. Así mismo, estas políticas aplican a toda la información creada, procesada, transmitida o resguardada por la SDA, sin importar el medio, formato, presentación o lugar.

## 3. NORMATIVIDAD (BASE LEGAL)

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, tienen 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", Reglamentada parcialmente por el Decreto Nacional 1377 de 2013, Reglamentada parcialmente por el Decreto 1081 de 2015, 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 27001:2022, el SGSI 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 y 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 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 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 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 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) y Nube Privada III (CCENEG-017-1-2019).

## 4. DEFINICIONES

**ACTIVO DE INFORMACIÓN:** se refiere a 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.

**DATOS PERSONALES:** Según la Ley 1581 de 2012, un dato personal se define como cualquier información que pueda asociarse a una o varias personas naturales determinadas o determinables. Una persona o individuo puede ser identificado directa o indirectamente a través de su nombre, número de identificación, datos de ubicación, información laboral, entre otros.

**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 DE SEGURIDAD DIGITAL**: actividades coordinadas dentro de una organización, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades.

**INFORMACIÓN PÚBLICA CLASIFICADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014.

**INFORMACIÓN PÚBLICA RESERVADA:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014.

**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.

**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.

**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.

**MODELO DE SEGURIDAD Y PRIVACIDAD DE INFORMACIÓN – MSPI**: El Modelo de Seguridad y Privacidad de la Información entrega una guía para construir un Sistema de Gestión de Seguridad de la Información (SGSI), buscando generar una conciencia colectiva sobre la importancia de clasificar, valorar y asegurar los activos de información de la entidad.

**POLÍTICAS 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).

**PRIVACIDAD**: se entiende el derecho que tienen todos los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

**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.

**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.

**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.

**SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN - SGSI:** Conjunto de políticas de administración de la información el cual consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización.

**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.

## 5. RESPONSABILIDAD Y AUTORIDAD

Conforme al manual del SIG de la SDA, el máximo líder del Sistema Integrado de Gestión será el/la secretario (a) Distrital de Ambiente, quién tendrá como responsabilidad la implementación, desarrollo, control y mejora y el seguimiento al cumplimiento de los elementos que conforman el SIG articulados con el Modelo Integrado de Planeación y Gestión - MIPG, así como garantizar los recursos necesarios para su adecuado funcionamiento, en la Secretaría Distrital de Ambiente.

A su vez, la SDA 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.

La política de seguridad de la información de la SDA está acorde con las mejores prácticas definidas en ISO 27001:2022 y el Modelo de Seguridad y Privacidad de la Información, por tanto, todos los servidores públicos, contratistas, colaboradores, así como proveedores y usuarios, son responsables de su aplicación y tomarán las medidas aplicables para garantizar su cumplimiento.

### 5.1. Roles de seguridad de la información

Se deben tener en cuenta los roles establecidos en el manual de seguridad de la información de la SDA sobre la información reservada, clasificada y pública, lo anterior con el fin de cumplir con la responsabilidad definida para cada rol; de esta manera se garantiza el adecuado manejo de la información, teniendo en cuenta los roles y responsabilidades asignadas según el cargo o actividades contractuales establecidas.

Así mismo, los dueños y custodios que se identifican en los activos de información deben tener asignado el rol adecuado, de acuerdo con el acceso que se tiene sobre cualquier activo. Dichos roles, deben estar asignados formalmente.

Imagen 1. Roles seguridad de información


Fuente: Guía MinTIC. Seguridad y Privacidad de la información

## 6. POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

La secretaria Distrital de Ambiente establece las siguientes políticas de seguridad y privacidad de la información.

### 6.1. Seguridad de los recursos humanos

La SDA aplica los lineamientos dados por la norma vigente y los procedimientos internos en los procesos de selección y vinculación de personal, realizando las verificaciones necesarias para confirmar la veracidad de la información suministrada por el funcionario o la persona candidata a contratar.

La Dirección de Gestión Corporativa y a su vez la Subdirección Contractual velan porque en los contratos de proveedores y contratistas que desarrollen dentro de sus actividades el manejo de información sensible de la entidad, incluyan 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 SDA, 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 en el marco del Sistema de Gestión de Seguridad de la Información - SGSI.

### 6.2. Gestión de activos

La SDA 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 serán identificados y/o actualizados cada vez que sea requerido por el líder de proceso asociado con el apoyo de cada enlace del Sistema Integrado de Gestión del proceso y asistidos técnicamente por los profesionales en seguridad de la información de la DPSIA y con los profesionales de gestión documental de la DGC, quienes en su conjunto, 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. Se podrá disponer del acompañamiento de la Dirección Legal Ambiental o un profesional en el área del conocimiento del Derecho que tenga la dependencia para su clasificación. La Gestión de activos se articula con la Política de administración de riesgos de la entidad y los procedimientos que de ella se deriven.

Así mismo, se debe tener en cuenta los siguientes lineamientos:

- Los propietarios de los activos de información deben garantizar que los documentos que se clasifiquen con información parcialmente clasificada cuenten con una versión que contenga solo las partes que sí pueden ser publicadas.
- Se debe prever que los activos de información críticos se encuentren localizados en áreas seguras y debidamente protegidos contra amenazas que puedan afectar su buen uso, disponibilidad y confidencialidad.
- Los activos de información críticos que sean de tipo digital deben estar protegidos con una contraseña.
- Se deben establecer controles o medidas acordes con la valoración de los activos de información y los riesgos asociados.
- Los colaboradores deben almacenar siempre la información digital de la entidad en las ubicaciones donde se esté´ respaldando la información.

- La identificación y/o actualización de los activos se registran en el formato establecido y adoptado por el Sistema Integrado de Gestión de la SDA.

### 6.3.1 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.

Se destinará un espacio físico adecuado para archivar los documentos producidos por cada dependencia de manera clasificada según la codificación definida por la SDA, 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 inmediato 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.

### 6.3.2 Devolución de los activos

Todo funcionario o contratista que se desvincule de la SDA deberá realizar la devolución de los activos de información que tenga asignado y en custodia, lo cual estará soportado con la firma del Paz y Salvo para funcionario y para contratista, de acuerdo con los procedimientos internos establecidos y adoptados para tal fin.

### 6.3.3 Gestión de medios removibles

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

- Todos los medios removibles administrados por el centro de datos 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 contratistas 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 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.

Así mismo, se deberá tener en cuenta lo siguiente:

- Los puertos USB deben estar inhabilitados. Sólo se habilitará previa autorización de la Dirección de Planeación y Sistemas de Información Ambiental.
- Analizar con el antivirus, los medios extraíbles cada vez que sean utilizados en los equipos de la entidad.
- Las aplicaciones serán instaladas únicamente desde los repositorios oficiales provistos por la SDA y por el equipo autorizado.
- En lo posible cifrar los medios extraíbles y siempre guardar en un lugar seguro para evitar la pérdida o robo de la información.
- No guardar información personal en los medios extraíbles asignados por la SDA.
- No conectar los medios extraíbles en lugares que no brinden las garantías de seguridad física necesarias para mitigar la pérdida o hurto de información de la SDA.

### 6.3.4 Disposición de los activos

La SDA establece que para la destrucción del material clasificado debe ser completamente destruido y verificado por el personal de gestión documental y de seguridad de la información. Siempre debe dejarse registro de la destrucción de material reservado y confidencial. La destrucción de material clasificado debe realizarse bajo la estricta supervisión del Oficial de Seguridad de la Información o quien haga sus veces.

Es responsabilidad del dueño del activo de información determinar cuando la información ha dejado de ser útil para la entidad, de acuerdo con su valoración y acorde con la regulación que aplique. Para ello, se debe procurar establecer los mecanismos relacionados con el tratamiento de la información durante su vida útil y usar mecanismos de destrucción o borrado seguro apropiado.

Así mismo, todos los colaboradores deben destruir de forma segura los documentos físicos clasificados como de uso clasificado y reservado. Y, en el caso de desvinculación, deberán asegurar y legalizar la devolución del activo de información bajo su custodia o responsabilidad.
Los registros de destrucción deberán 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, podrá solicitarse la presencia de la oficina de control interno como buena práctica de verificación desde el punto de vista de esquemas de defensa. Estos registros deberán retenerse de acuerdo con lo estipulado en las tablas de retención documental de la entidad.

### 6.3.5 Dispositivos móviles

Los dispositivos móviles deben estar integrados a una plataforma de administración controlada por la SDA, la cual debe permitir configuración de políticas a aplicar en los dispositivos móviles, soporte para la instalación de aplicaciones móviles permitidas por la SDA, control de contenido, actualización de software, backup 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 remoto, configuración segura, aplicación de políticas para usuarios, contraseñas y encriptación, 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 SDA debe contar con una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales; dichas copias deben acogerse al procedimiento 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.

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 área de Almacén de la SDA.

La Dirección de Gestión Corporativa y/o Dirección de Planeación y Sistemas de Información Ambiental debe velar por la instalación de un agente de seguridad o 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 de uso público, o conexiones de establecimientos públicos como hoteles, cafés internet, redes públicas, entre otros.

### 6.3. Control de acceso

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

Para la SDA es prioritario definir el personal que debe tener acceso sobre la información que considera es sensible, por lo cual limita el acceso de usuarios de aplicaciones computarizadas, únicamente a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades y funciones a cargo, debido a que la Entidad debe salvaguardar y custodiar su información de forma adecuada, y más cuando es información categorizada como sensible o tener un carácter confidencial. Así mismo, es necesario restringir el acceso a las instalaciones donde dicha información se encuentra guardada, garantizando así la confidencialidad e integridad de esta.

La administración de la plataforma tecnológica es responsabilidad de la DPSIA, y controla los accesos de los usuarios a través del directorio activo, así como los sistemas de información de la Entidad que formalmente le han sido asignados, en donde se establecen los controles de acceso pertinentes a dichos recursos.

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 y soportes, donde se evidencie que, por solicitud de cada uno de los líderes responsables de los procesos, dueños de la información relacionada y supervisores de los contratos asociados con la solicitud, se autorice a los servidores públicos, colaboradores o terceros, generar y mantener habilitado el acceso a los diferentes sistemas de información de la entidad, por el tiempo requerido y necesario para cumplir con sus actividades. Luego del tiempo solicitado, los administradores de las plataformas deben deshabilitar las credenciales y accesos. Lo anterior, teniendo en cuenta que, por la naturaleza del servicio y operación de la entidad, existen casos en que se realizan solicitudes para mantener usuarios activos, luego de la terminación del contrato relacionado, para terminar tareas como lo relacionado con el paz y salvo, además de entrega de los soportes de actividades.

- Se establece por regla general y en esta política que, una vez terminada la vinculación con la Secretaría Distrital de Ambiente en cualquiera de las modalidades de contratación, se otorgaran quince (15) días calendarios posteriores a la terminación del contrato para surtir los procesos finales de aprobación del informe de actividades y autorización de pagos (IAAP) final y de trámite de paz y salvo, e inmediatamente la DPSIA mediante la

administración del directorio activo de la entidad, cancelará el acceso a los sistemas de información en la entidad, esto en cumplimiento del lineamiento de la ISO 27001 en su control A.9.2.6. Cancelación o ajuste de los derechos de acceso, que indica*: "Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deben cancelar al terminar su empleo, contrato o acuerdo, o se deben ajustar cuando se hagan cambios".* Eso conforme a decisión tomada en Comité Institucional de Gestión y Desempeño de la SDA en sesión # 4 del 4 de agosto de 2023.
Por lo anterior, si se requiere de algún tiempo adicional para terminar actividades relacionadas con sus compromisos con la entidad, como el paz y salvo, este deberá ser solicitado por el jefe inmediato o a quien este delegue y será registrado mediante la mesa de servicios de la SDA con la debida justificación de su solicitud de acceso a los sistemas de información de la entidad.

- En el caso de los funcionarios de carrera administrativa y los cargos de libre nombramiento y remoción, la DGC comunicará a la DPSIA de tal situación, y la DPSIA mediante la administración del directorio activo de la entidad, cancelará el acceso a los sistemas de información en la entidad y deshabilitarán credenciales en un plazo de cero (0) días posterior a la terminación de su vinculación con la entidad. Eso conforme a decisión tomada en Comité Institucional de Gestión y Desempeño de la SDA en sesión # 4 del 4 de agosto de 2023.
  De igual forma, si se requiere acceso adicional a los sistemas de información para terminar actividades relacionadas con sus compromisos con la entidad, gestionar el paz y salvo, este debe ser solicitado y justificado mediante la mesa de servicios de la SDA, por el jefe inmediato y por el superior jerárquico.

- 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, colaborador o tercero.

- En caso de retiro, terminación, jubilación, suspensión, cesión o cambio de cualquier servidor público, colaborador o tercero, se deberá deshabilitar o actualizar los privilegios en los sistemas a los que el usuario estaba autorizado, lo anterior siempre con el soporte documental que respalde la acción y previa comunicación de la Dirección de Gestión Corporativa.

- Asignar las contraseñas de acceso que deberán cumplir con un mínimo de ocho (8) caracteres y la combinación de números, letras mayúsculas y minúsculas, y utilizar caracteres especiales si el sistema lo permite.

- Se establece la regla de cambio de contraseña con una periodicidad de sesenta (60) días como política de seguridad para el cambio de contraseña.

- Generar las reglas de activación y desactivación de usuarios en el Directorio Activo, teniendo en cuenta las solicitudes y reportes remitidos por las dependencias dueñas de

la información contractual, parametrizando los tiempos de vigencia de cada usuario según los términos contractuales y los requerimientos de la Entidad, para terminar sus labores y obligaciones, hasta quedar a paz y salvo con la secretaria.

- Realizar una verificación semestral sobre una muestra representativa de los usuarios que pueden estar activos y que ya no tienen vínculo contractual con la entidad. Lo anterior se puede dar debido a que las dependencias dueñas de la información no han generado los reportes de desactivación.

- Autorizar los accesos a sistemas de información o aplicativos, de acuerdo con los perfiles establecidos y las necesidades de uso, en caso de ser propietario del activo de información.

Es responsabilidad de los usuarios de la SDA:

- Las contraseñas son 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.
- Cambiar la contraseña si se duda de que alguien más la conoce y si ha tratado de dar mal uso de ella.
- Seleccionar 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.
- Restringir el acceso a oficinas, salas de telecomunicaciones, servidores y áreas de trabajo que contengan información clasificada y/o reservada, concediendo el ingreso bajo autorización previa del propietario de la información.
- Solicitar autorización para acceder a la información y aplicaciones de un sistema de información con uso restringido mediante la mesa de servicios.

Es responsabilidad de la Dirección de Gestión Corporativa y Subdirección Contractual (dependencias que administran la información contractual y de talento humano) de la SDA:

- Reportar formalmente y por escrito a la DPSIA, la activación y desactivación de los funcionarios de carrera administrativa o servidores públicos en las diferentes modalidades, y los cargos de libre nombramiento y remoción, en el directorio activo y en los sistemas de información en donde se generaron los accesos, así mismo, todas las novedades o situaciones administrativas, relacionadas con cambios que se deben aplicar sobre los accesos a los diferentes sistemas de información.
- Velar porque se cumpla el protocolo o procedimiento adoptado para el control de ingreso de visitantes a la SDA, así como supervisar los contratos que para este fin se celebren en la entidad.
- Velar porque se utilicen mecanismos para restringir el acceso de personal mediante un método de autenticación.

- Asegurar que las áreas físicas cuenten con las medidas de protección de acceso acorde con el valor de la información que allí se procesa, almacena y transmite. Los sitios restringidos como cuartos técnicos o similares deben tener controles de acceso.
- Velar por la adecuación utilización de la identificación física de los servidores con vinculación con la entidad y de la tarjeta de proximidad para el ingreso a la sede principal de la SDA.

Es responsabilidad de los contratistas/proveedores que realizan tareas de administración de sistemas de información y bases de datos en la SDA:

- Establecer las medidas de control de acceso de los servidores públicos y contratistas, a través de mecanismos de identificación, autenticación y autorización de acceso, a nivel de sistemas de información, bases de datos y servicios de TI de acuerdo con los perfiles y cargos instaurados en la entidad.
- Verificar los controles de acceso de los servidores públicos y contratistas, a fin de validar que los usuarios accedan solamente a los recursos autorizados para la realización de sus tareas.
- Garantizar que el administrador de cada sistema, aplicativo o dispositivo de la Infraestructura Tecnológica, proporcione a su jefe inmediato o supervisor, las contraseñas de administración.

La SDA 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.

Como también las responsabilidades en Seguridad de la Información:

- No se permite ninguna conexión directa de entrada o salida de tráfico entre Internet y la red de la Entidad.
- Los sistemas que proporcionan servicios de acceso público deben ubicarse dentro de un esquema de zona desmilitarizada que permita limitar el tráfico.
- Siempre debe existir un firewall en cada conexión a Internet y entre cualquier zona desmilitarizada y la zona interna de la red.
- Todo cambio en la configuración de firewalls y routers debe seguir el procedimiento definido de control de cambios.
- Se debe mantener actualizados los servicios, protocolos y puertos abiertos en el firewall.
- Realizar revisiones periódicas de la configuración del firewall.
- Relacionar en la matriz de roles y funciones los usuarios que pertenecen a cada rol.
- Mantener actualizados los sistemas operativos con las últimas versiones disponibles.

### 6.3.1 Normas de seguridad para el control de acceso lógico

El control de acceso lógico se refiere a las políticas, procedimientos y mecanismos utilizados para autorizar y regular el acceso a los recursos digitales de una organización, como sistemas informáticos, redes, bases de datos y aplicaciones. Estas normas de seguridad establecen las pautas y requisitos para gestionar y proteger el acceso a los sistemas de información, tanto por parte de usuarios internos como externos. Al seguir estas normas, la SDA puede salvaguardar su información y protegerse de las amenazas cada vez más sofisticadas en el mundo digital. A continuación, se presentan las normas esenciales para cumplir al interior de la entidad:

- El jefe de la dependencia o líder de proceso o quien este delegue, será el único autorizado para solicitar a través de la mesa de servicio el acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información; así mismo debe especificar los privilegios de acceso al cual debe estar vinculado el usuario y la dependencia al cual va a pertenecer, a través de las diferentes categorías de la mesa de ayuda.
- La administración de los perfiles de usuario es responsabilidad de los administradores de cada aplicación (sistema).
- Los administradores de cada aplicación (sistema) deberán crear, modificar, bloquear cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información que no se encuentren ligados al directorio activo con el que cuenta en la actualidad la entidad, cuando esto sea solicitado por el jefe de área o líder de proceso.
- Se deberá seguir el procedimiento de entrega de usuarios y contraseñas al personal interno y externo que tendrán acceso a los servicios de red de la SDA, a los recursos de la plataforma tecnológica o a los sistemas de información.
- Se deberán inhabilitar los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos de la plataforma tecnológica.
- Se deberá verificar periódicamente (mensualmente) las novedades de personal y validar la eliminación, reasignación o bloqueo de las cuentas de acceso de los recursos tecnológicos y sistemas de información de la SDA.
- Se deberá establecer controles de acceso a los ambientes de producción de los sistemas de información y garantizar que solo el personal autorizado tenga los privilegios adecuados para garantizar el acceso a la información.
- Se deberán establecer mecanismos de auditoría al personal encargado de la administración del acceso a los servicios de red, a los recursos de la plataforma tecnológica y a los sistemas de información.
- Se deben tener en cuenta los reportes de las áreas dueñas y responsables de la información de vinculación de usuarios, para activar o desactivar credenciales.
- Los parámetros de desactivación de usuarios en el directorio activo deben obedecer a los reportes remitidos por las áreas dueñas de esta información y teniendo en cuenta los requerimientos solicitados para que los usuarios terminen sus labores y queden a paz y salvo con la entidad. Estos reportes y requerimientos siempre deben tener un respaldo documental.

### 6.3.2 Directrices de seguridad para el control de acceso físico

Las normas o directrices de seguridad para el control de acceso físico son fundamentales para salvaguardar los activos físicos y garantizar la seguridad de las personas y la información dentro de una organización. Al establecer y aplicar estas normas, las organizaciones pueden crear un entorno seguro y protegido, mitigando los riesgos asociados con accesos no autorizados y manteniendo la integridad de sus operaciones. En ese sentido se deben seguir y acatar los siguientes lineamientos:

- Se deberá identificar al personal que requiere acceso a las instalaciones de la SDA, autorizar su ingreso y conceder los privilegios necesarios para el acceso físico.
- Contar con mecanismos de control de acceso para las áreas seguras (el centro de cómputo, la unidad de diagramación administración de infraestructura y oficinas que almacén en información reservada); tales como cámaras, puertas de seguridad, sistemas de control con lectores biométricos, sistema de alarmas, llaves, entre otras, que la SDA considere pertinentes.
- Las puertas de acceso al centro de cómputo, administración de infraestructura, y centros de cableado u otras áreas que alberguen información crítica, deberán permanecer siempre cerradas y aseguradas. De igual manera, los gabinetes y puertas de los equipos que se encuentran en las áreas mencionadas deberán permanecer cerrados.
- Aprobar de manera previa las solicitudes de acceso de terceros al centro de cómputo, administración de infraestructura o a los centros de cableado, además se deberá acompañar permanentemente a los visitantes durante su estancia en las áreas mencionadas.
- Registrar el ingreso de los visitantes al centro de cómputo (data center) y a los centros de cableado en una bitácora ubicada en la entrada de estos lugares de forma visible.
- Se deberá monitorear los ingresos al centro de cómputo permanentemente para identificar accesos no autorizados y para confirmar que los controles de acceso son efectivos.
- Se deberá bloquear de manera inmediata los privilegios de acceso físico a las instalaciones de la SDA tan pronto el personal termine su vinculación.
- Se deberá realizar la devolución del carné institucional tan pronto el personal termine su vinculación con la SDA.
- Se deberá implementar controles de acceso físico al centro de cómputo para evitar la manipulación no autorizada del cableado.

#### 6.3.2.1 Seguridad en zonas donde se lleve a cabo las actividades de tesorería

Dado que las actividades de tesorería donde se realizan transacciones financieras se efectúan en la Subdirección financiera de la SDA, se fortalecerá los controles para los equipos de cómputo y se propenderá por implementar un acceso controlado y/o restringido al área física, por ejemplo a través de un registro y bitácora de visitantes debidamente autorizados y acompañados durante su estancia en la Subdirección, con el propósito de minimizar la probabilidad de fraude en la gestión de las operaciones transaccionales de valores, pagos por archivos planos y dispersiones desde los portales bancarios.

Para ello, de acuerdo con los recursos disponibles, y según análisis del contexto de la Subdirección Financiera, se debe fortalecer el sistema de cámaras de seguridad, así como la verificación de los requisitos para realizar las tareas de tesorero u ordenador del gasto y demás colaboradores que apoyan a esta dependencia.

La Subdirección financiera debe tener suscritos contratos con entidades financieras para la realización de pagos electrónicos, propendiendo por rotar el pago en diferentes entidades, con el fin de garantizar transparencia y reducir el riesgo operativo. Los equipos tecnológicos deben contar con herramientas de control de software malicioso activas y actualizadas, así como con un monitoreo continuo de las condiciones de seguridad para el acceso a portales y la realización de transacciones financieras. Se deben tener reglas específicamente creadas para estos equipos, los cuales deben ser más estrictas y no tendrá excepciones para su manejo, estas reglas deben ser pactadas con la tesorería y divulgadas con el personal que tiene acceso a estos equipos.

Así mismo, los colaboradores que posean claves para las operaciones y transacciones que la entidad les autorice realizar, deben hacer uso responsable de las mismas, efectuando su cambio periódico y solicitando a la entidad financiera correspondiente, la asignación de algún mecanismo adicional a la clave para tener doble autenticación, teniendo claro los procedimientos en el caso de extravío o pérdida, así como el reporte de las ausencias temporales por situaciones administrativas (vacaciones, permisos, licencias, otros). Se debe contar con desagregación de funciones para autorizar transacciones bancarias, estas asignaciones deben estar formalmente asignadas.

Los equipos de cómputo empleados para realizar las transacciones bancarias no deben tener instalado software diferente al autorizado y debe estar asociado con el cumplimiento exclusivo de las labores propias de la Subdirección financiera.

### 6.3.3 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. Así mismo, no podrán asumir en nombre de la SDA posiciones personales en encuestas de opinión, foros u otros accesos similares.

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 SDA, de sus clientes y/o de sus funcionarios, con terceros.

### 6.3.4 No repudio

La SDA 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 SDA debe hacer uso de mecanismos criptográficos: firmas digitales, cifrado de mensajes, códigos de autenticación de mensajes, etc.
- La SDA 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 SDA 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 SDA deberá documentar las evidencias de No-repudio, por medio de registros compuestos 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.

### 6.3.5 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 asignada 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.
- Está 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 tomarán 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 deben enviar archivos adjuntos con extensión ejecutable (programas, librerías, aplicaciones, etc.)
- La información contenida en el buzón es de completa responsabilidad del usuario, en caso de eliminación accidental de correos electrónicos, inclusive de la papelera, se puede pedir apoyo mediante la mesa de servicio. Teniendo en cuenta que 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 cambiar su contraseña e informar al oficial de seguridad de la información.
- 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.
- En caso de recibir correos sospechosos, en los que no se tenga conocimiento o relación de los temas a tratar, además con adjuntos; debe abstenerse de abrirlos y descargar los archivos adjuntos, y debe notificar a Seguridad de la Información, por medio de la mesa de servicios, para adelantar el análisis respectivo.

### 6.3.6 Almacenamiento en la nube y carpetas compartidas

El almacenamiento en la nube 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 vinculadas 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 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 dependencias 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 de contenidos designado por el jefe de cada dependencia.
- Cualquier modificación en el contenido de las carpetas y /o archivos deberá ser tramitada por la dependencia a través del gestor designado.
- Esta unidad solo debe tener registrada información institucional.
- Los administradores de cada dependencia deben velar por mantener actualizada y organizada la información de cada carpeta, de ser necesario eliminar las versiones borradores o las que no se consideren finales.
- Así mismo, se deben asignar permisos sobre carpetas compartidas a grupos de usuarios.
- Habilitar la protección de los archivos de registro de eventos.
- Crear cuentas de administración nombradas de forma que no puedan ser asociadas fácilmente al administrador y con ello evitar dar a conocer los privilegios de dicho usuario

### 6.3.7 Port Security (Puerto seguro de red)

El usuario, funcionario o contratista colaborador de la SDA es el responsable de la seguridad en su puesto de trabajo y del equipo de cómputo asignado para el desarrollo de sus funciones en la SDA. Por lo tanto, la conexión a los puntos de red dispuestos por la entidad, sólo se habilitarán

para los equipos previamente validados por el área de soporte, restringiendo el movimiento de equipos sin previo aviso de la dependencia encargada.

### 6.3.8 Responsables del control de acceso

Se establecen los siguientes responsables del control de acceso:

- **Equipo de Seguridad de la Información:** Hacer seguimiento sobre el cumplimiento de la presente política, para garantizar el adecuado control de acceso lógico y físico.

- **Director(a) de la DPSIA**: Poner a disposición los recursos necesarios para el cumplimiento de los lineamientos descritos en la presente política, y parametrizar los accesos según los requerimientos contractuales, como por ejemplo el directorio activo.

- **Profesional de la Dirección de Gestión Corporativa**: Deberán informar a la DPSIA de cualquier situación administrativa del empleado público o el directivo, ya sea por finalización de la vinculación de cualquier miembro del personal de planta ya sea de libre nombramiento o de carrera administrativa o cualquier otra modalidad de vinculación laboral de la SDA, o por cualquier encargo, vacaciones, permisos o comisiones otorgadas. Estas notificaciones deben quedar por escrito.

- **Profesional de la Subdirección contractual**: Deberá informar a la DPSIA cuando finalice o cuando haya algún tipo de suspensión del contrato de contratistas de la SDA, además definir e implementar los controles de acceso físico, estas notificaciones deben quedar por escrito.

- **Todo el Personal**: No deberán acceder a las áreas seguras sin autorización, a excepción que sea en cumplimiento de sus obligaciones con la SDA. Dar cumplimiento a esta política.

## 6.4. 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

Si es necesario transmitir información que es tipificada por la SDA, como reservada o clasificada, se deben aplicar medidas de tratamiento para cifrar dicha información, en estos casos se puede solicitar asesoría al grupo de seguridad de la información, por medio de la mesa de servicios.
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.

Cuando se compartan claves, se debe garantizar la confidencialidad en su intercambio a través del uso de canales seguros y diferentes a los que se envían la información cuando exista transferencia de esta. Así mismo, se recomienda hacer uso de los certificados SSL para los aplicativos que se encuentran expuestos a internet.

### 6.5. Seguridad física y del entorno

La SDA 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, considerándose 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 SDA 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.

En lo relacionado con el ingreso de visitantes a la SDA, será de obligatorio cumplimiento el acatamiento de los procedimientos internos establecidos y adoptados para tal fin y, las que la entidad adopte junto con la empresa de vigilancia.

Así mismo, será obligación de los colaboradores proteger la identificación que les otorgan autorizaciones de acceso y facultades especiales para acceder a los activos de información, debiendo responder por los actos que se cometan con su identificación y en los que se evidencia negligencia o descuido de sus credenciales o claves de ingreso.

### 6.6. Seguridad de las operaciones

La SDA dispone de los siguientes lineamientos que rigen 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.

#### 6.6.1 Teletrabajo, trabajo en casa y acceso remoto

La SDA implementará los controles adecuados para proteger la confidencialidad, integridad, disponibilidad y privacidad de los activos de información en un ambiente de teletrabajo, de acuerdo con lo establecido en las normas vigentes que regulan y promueven el Teletrabajo a nivel nacional y territorial, Ley 1221 de 2008, Decreto Reglamentario 884 de 2012 del Ministerio

de Trabajo, Decreto 1227 de 2022 y Decreto Distrital 050 de 2023, y en ejercicio de sus facultades legales en especial las que le confiere, los Decretos 109 de 2009 y 806 de 2019, y en particular en las Resoluciones que se expiden en la SDA, las cuales se tienen en cuenta en la definición de las presentes políticas relacionadas con el Teletrabajo, trabajo en casa y acceso remoto.

Lo anterior, busca generar el uso adecuado de las tecnologías de la información, 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.

Indistintamente de la alternativa de trabajo empleada, ya sea teletrabajo (en sus diferentes modalidades, como la autónoma, suplementaria y/o móvil), trabajo en casa o acceso remoto, la información a la que se tiene acceso debe ser protegida para salvaguardar su confidencialidad y privacidad e integridad. Así mismo, se debe garantizar que todos los equipos de cómputo que sean usados en la modalidad de teletrabajo cumplan con los estándares de instalación, configuración y adecuación para la seguridad de la información.

En concordancia con lo anterior, la SDA debe:

- Brindar los permisos de acceso pertinentes a los usuarios que empleen la modalidad de teletrabajo, trabajo en casa o acceso remoto, teniendo en cuenta rol relacionado con los activos de información que se manejan.
- Llevar control sobre los usuarios que trabajan y adelantan sus actividades bajo las modalidades de teletrabajo, trabajo en casa o acceso remoto.
- Monitorear y hacer seguimiento de las conexiones remotas a los servicios corporativos de teletrabajo y trabajo en casa, prestando especial atención a los intentos de conexión que reporten irregularidades y que puedan representar una amenaza para la entidad.
- Sensibilizar a los usuarios sobre cómo mitigar los riesgos asociados a la seguridad de la información y las consecuencias de una materialización.
- En los casos que sea necesario, según el análisis de la información que se adelantará, habilitar una conexión segura a través de VPN para acceder remotamente a los servicios que sean requeridos para el desarrollo de las funciones u obligaciones de los usuarios.
- Restringir el acceso remoto a áreas que por su criticidad deban tener acceso exclusivamente presencial.

Así mismo, los usuarios deben:

- Aplicar las presentes políticas de seguridad de la Información, y reportar por medio de la mesa de servicio, cualquier anomalía o actividad sospechosa que pueda afectar el equipo desde el cual se trabaja, y la información sobre la cual se tiene acceso.

- Adelantar sus funciones, sólo en el sitio que fue previamente validado por la SDA, teniendo en cuenta lo establecido en la Resolución de Teletrabajo adoptada en la Entidad.
- Adoptar medidas de seguridad de la información en el sitio donde se esté realizando el teletrabajo, trabajo en casa o acceso remoto, para evitar el acceso fortuito a la información corporativa por otros usuarios del equipo de cómputo; configurando contraseñas y cuentas de usuario, así como el bloqueo automático por inactividad.

Tener en cuenta las siguientes recomendaciones de protección frente al uso de equipos portátiles:

- Tener un espacio adecuado para trabajar en casa sin riesgo a perder información, por algún tipo de accidente.
- Emplear guayas de seguridad.
- Evitar transportar el equipo portátil si no es necesario.
- Utilizar un maletín apropiado para proteger el equipo portátil en caso de requerir su desplazamiento.
- No consumir alimentos líquidos cerca al equipo de cómputo, aplicando la política de Escritorio y pantalla limpios del presente documento.
- Utilizar métodos apropiados para la destrucción segura de documentos físicos, evitando arrojarlos directamente al contenedor de reciclaje y/o evitar su reutilización en labores domésticas. Se recomienda picar el papel en trozos pequeños que no permitan visualizar su contenido, sobre todo en caso de que sea información tipificada como reservada y clasificada
- Utilizar contraseñas robustas que contengan números, letras y caracteres especiales si el sistema lo permite; garantizando su cambio periódico y uso personal, aplicando lo establecido en la política de Control de acceso, del presente documento.
- Validar que todas las conexiones con servidores y páginas web sean cerradas, utilizando, cuando sea posible, la opción “desconectar” o “cerrar sesión”.
- Realizar copias de seguridad de manera periódica de la información gestionada en los equipos utilizados en teletrabajo, 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 o no institucionales 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, de ser posible habilitar las opciones de actualización automática.
- Mantener actualizado el software antivirus para evitar infecciones con virus o software malicioso, realizando escaneos periódicos y habilitando la verificación automática por parte del antivirus.
- No manejar información de la entidad, en equipos personales o que no se encuentren dentro del dominio de la Entidad.
- No instalar programas o extensiones de navegadores de fuentes desconocidas ya que estas pueden contener malware el cual puede afectar sus dispositivos y tener acceso a la información sensible.

- Llevar el equipo de cómputo que pertenece a la entidad, semestralmente a la sede principal de la SDA para realizar el mantenimiento preventivo y correctivo tanto físico como lógico, para esta labor, programar previamente por medio de la mesa de servicio la actividad.

Y los equipos de cómputo para usuarios de teletrabajo deben contar con las siguientes características:

- Tener un sistema operativo y aplicaciones de trabajo licenciadas.
- Tener un Software de antivirus legal, con la base de firmas actualizada.
- Si es un portátil y el sistema operativo cuenta con la opción de cifrado, se debe cifrar el disco duro donde se trabaja con la información de la entidad.
- Activar el bloqueo automático por inactividad.
- Manejar cuentas de usuario independientes.

### 6.6.2 Escritorio y pantalla limpia

La SDA promoverá la cultura de escritorio y pantalla limpia, 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, post-it, 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, se debe aplicar la política para mantener la pantalla de inicio del equipo de cómputo libre de archivos, salvo los accesos directos a las aplicaciones necesarias para su labor

Se establece la regla de bloqueo automático de la sesión a los cinco (5) minutos por inactividad. Esto debe mantenerse parametrizado en el directorio activo administrado por la Dirección de Planeación y Sistemas de Información Ambiental.

Al imprimir documentos de carácter confidencial, estos deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia, garantizando que al finalizar la jornada de trabajo y/o cuando se ausente de su puesto de trabajo, no deben reposar carpetas, ni oficios en los escritorios, estos deben ser salvaguardados bajo llave.

### 6.6.3 Uso de computadores personales

Los colaboradores y terceros que requieran tener acceso a los recursos de información de la SDA mediante el uso de sus computadores personales deben aceptar y aplicar las políticas y controles emitidos por la entidad, con el fin de proteger los activos de información a los cuales acceden, recordando que la información habilitada es de uso exclusivo para el desarrollo de sus labores dentro de la entidad.

De acuerdo con lo anterior, la configuración de este servicio en los dispositivos se debe realizar únicamente a quienes dadas sus obligaciones requieran el uso de este servicio, previa validación y registro de los equipos por parte del personal de soporte de la SDA.

Los colaboradores y terceros son responsables de salvaguardar toda la información que se almacena en sus dispositivos, y de no instalar software sobre estos equipos, que puedan afectar la información institucional que maneje. Así como de entregar esta información, al momento de su retiro o terminación del contrato, siendo el mantenimiento o reparación de los equipos de responsabilidad de los propietarios.

La SDA se reserva el derecho de monitorear y restringir los accesos que puedan vulnerar la confidencialidad, disponibilidad e integridad de la información, así como desactivar los accesos a los sistemas y a la información de los colaboradores que ya no posean ningún vínculo con la entidad.

### 6.7. Seguridad de las comunicaciones

La SDA aplicará los siguientes lineamientos para el manejo de los recursos con los cuales se gestionan las comunicaciones, en términos de seguridad de la información en la SDA. Este capítulo complementa lo establecido en los apartados anteriores de la Política como el de uso de correo electrónico, almacenamiento en la nube y carpetas compartidas, uso adecuado de internet, puerto seguro de Red, gestión de activos, entre otros, ya que la comunicación de información es transversal en todo el manejo de la seguridad de la Información.

- Las redes deben ser administradas y controladas para proteger la información en los sistemas y aplicaciones. Además, garantizar que se cuenta con dispositivos de seguridad y niveles de servicio apropiados.
  La SDA establece mecanismos de identificación automática de equipos en la red, como medio de autenticación de conexiones.
- La SDA debe propender por 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.
- Se debe monitorear y proteger los servicios de red, para evitar accesos no autorizados, estableciendo los privilegios de acceso de control, solo a usuarios administradores y con el rol adecuado para ejercer tal labor.
  Así mismo, de acuerdo con los recursos disponibles, monitorear accesos a los servicios web, como también intentos de acceso no autorizados.
- En caso de requerir cifrado para transmitir información, se debe aplicar lo indicado en el capítulo de criptografía, y solicitar asesoría por parte del grupo de seguridad de la información de la entidad, lo anterior por medio de la mesa de servicio.
- Para cualquier manejo y transmisión de la información, se debe tener en cuenta lo establecido en el índice de información reservada y clasificada de la entidad, con el fin de dar el manejo adecuado, de acuerdo con la tipificación definida en este instrumento.

- Para atender cualquier necesidad de comunicación de información, se debe tener en cuenta los roles y responsabilidades establecidos en el Manual de Seguridad de la Información de la SDA, así como los lineamientos definidos para los activos de información.

### 6.8. Adquisición, desarrollo y mantenimiento de sistemas

En cuanto a la adquisición, desarrollo y mantenimiento de sistemas, la SDA establece:

#### 6.8.1 Mantenimiento físico de las operaciones

La SDA genera 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 SDA garantiza que el centro de datos 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 centro de datos 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, de acuerdo con el plan de mantenimiento de la infraestructura de la SDA que se establezca.
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.

#### 6.8.2 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 SDA 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.

La privacidad, confidencialidad e integridad del activo de información, con base en el nivel al que pertenezca y el nivel de evaluación de riesgo, deberá ser salvaguardada a través de la aplicación de:

- Cifrado de datos clasificados como reserva: Los datos en tránsito entre diferentes sistemas y el almacenamiento de esta información se deben cifrar con un algoritmo criptográfico. Usar HTTPS para aplicaciones web.
- Control de acceso: Mecanismos de autenticación por usuario y contraseña siguiendo la Política de control de acceso a la información establecida.
- Registro: Registrar eventos que evidencien las acciones realizadas con el fin de tener un registro de auditoría de las acciones que realiza el usuario.
- Validar la integridad de los datos: Implementar opciones que permitan validar la integridad de los datos almacenados y/o transmitidos dependiendo de su criticidad.

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.

### 6.8.3 Gestión del cambio

La SDA 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.

### 6.8.4 Gestión de vulnerabilidades técnicas

La SDA 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.
Aplicar la metodología establecida por la SDA, para el manejo adecuado de los activos de información, teniendo en cuenta el análisis y tratamiento de vulnerabilidades identificadas y que pueden afectar los activos de información. Toda vulnerabilidad debe contar con un análisis y con actividades de control que busquen la mitigación y tratamiento del riesgo asociado a ella y la disminución de su impacto y probabilidad de ocurrencia.

### 6.8.5 Transferencia de información

Con el fin de mantener la seguridad de los activos de información de la entidad, la SDA 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 SDA deben destruir de manera segura la información suministrada, una vez ésta 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 SDA por vía telefónica y/o correo electrónico.

La SDA 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.

En este sentido, las transferencias de información realizadas en la SDA deben tener registros que permitan su trazabilidad, tales como: i) Fecha y hora; ii) Dirección IP; iii) Usuario; iv) Transmisión exitosa/fallida; v) Tamaño de los datos transmitidos y vi) Algoritmo de cifrado o firmado.

### 6.8.6 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 que garanticen la confidencialidad, integridad y disponibilidad de la información, realizándose 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 definirán articuladamente las características de su información, para aplicar los mecanismos a seguir para el respaldo y almacenamiento de la información, validando las copias a intervalos regulares.

La SDA 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 esta, esta deberá ser solicitada a la Dirección Corporativa previa autorización del jefe inmediato, en caso de ser persona distinta al dueño de la información.

### 6.9. Relaciones con los proveedores

La SDA 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, mitigando los riesgos asociados a la confidencialidad de la información.

Desde la construcción de los estudios previos, el jefe de la dependencia interesado en la contratación debe identificar los riesgos de seguridad de la información los cuáles serán parte de la estimación y cobertura de los riesgos del proceso de contratación. De acuerdo con ello, el análisis de riesgos de esta naturaleza debe incluir su identificación, clasificación, probabilidad de ocurrencia estimada, impacto, la determinación de la parte que debe asumirlos, el tratamiento que se les debe dar para eliminarlos o mitigarlos y las características del monitoreo más adecuado para administrarlos.

La gestión de riesgos debe ser un trabajo articulado con las dependencias, la instancia definida en la SDA conforme al esquema de líneas y la política de administración de riesgos adoptada por la entidad, a fin de determinar los requisitos mínimos de seguridad y los controles necesarios por parte del proveedor para ejecutar dicho contrato, siendo necesario dar a conocer a todos los proveedores interesados, las políticas complementarias de seguridad de la información, especialmente las políticas de activos y de control de acceso.

En medio de la etapa contractual, se debe asegurar la inclusión de la cláusula de confidencialidad, protección de datos, derechos de propiedad intelectual y derechos de autor, en la suscripción y perfeccionamiento del contrato que se celebre entre la entidad y aquellos proveedores que tendrán acceso a la información de la SDA.

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.

### 6.10. Gestión de incidentes de seguridad de la información

La SDA está comprometida con la mejora continua del SGSI, por ello 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 y la mesa de servicios de la entidad.

La Alta Dirección a través de la Dirección de Planeación y Sistemas de Información Ambiental 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 por la SDA.

### 6.11. Gestión de continuidad de negocio

La SDA cuenta con un plan de recuperación de desastres (DRP), el cual está compuesto por un conjunto de actividades diseñadas para proteger y recuperar la infraestructura tecnológica de la entidad en caso de un evento de interrupción tecnológica, que afecte las operaciones. Este plan permite minimizar el impacto, sobre la pérdida de información crítica y la operación de los servicios institucionales. Es necesario cumplir con lo establecido en dicho plan, y revisar la pertinencia sobre su actualización cuando sea necesario.

Así mismo, posee un Plan de continuidad del negocio (BCP), el cual tiene como propósito asegurar la reanudación oportuna de las operaciones, en caso de ocurrencia de eventos de interrupción de operaciones, que puedan poner en peligro la reputación y permanencia de la entidad, definiendo procedimientos y estrategias para ejecutar en los momentos de interrupción y preparando al personal para una respuesta adecuada en la menor cantidad de tiempo posible. Cabe mencionar que, este plan debe contener un análisis del impacto al negocio (BIA) a nivel de los procesos identificados en el Mapa de Procesos, una política aplicable de forma transversal y las estrategias respectivas para su aplicación.

Las políticas de seguridad de la información actuales se encuentran alineadas con dichos planes, y deberá revisar la pertinencia sobre su actualización cuando sea necesario.

### 6.12. Cumplimiento

La SDA sancionará cualquier violación a esta política o procedimiento establecido en el SGSI, de acuerdo con lo establecido en la Ley de delitos informáticos 1273 del 2009 y demás aplicables.

La SDA 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 en la mesa de servicios de la entidad o a través de los procedimientos que se establezcan para tal fin. Además, será responsable de preservar la confidencialidad, integridad y disponibilidad de los activos de información en cumplimiento de la presente política.

### 6.13. Privacidad y confidencialidad

La SDA 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:

- **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.

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

- **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.

### 6.13.1 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 o la que la sustituya, modifique o actualice.

### 6.13.2 Manejo de datos personales para ingreso a la entidad

La SDA, 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.

### 6.13.3 Derechos de los titulares de los datos personales

Los titulares de la información cuyos datos personales sean objeto de tratamiento por parte de la SDA 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 SDA 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 SDA, 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 SDA.

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.

### 6.13.4 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.

M 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: +(601) 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___

### 6.14. Comunicación

Estas políticas deben ser publicadas en el aplicativo adoptado por la SDA como repositorio del Sistema Integrado de Gestión-SIG de la entidad y en la sede electrónica 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 adoptadas por la entidad, encaminadas a la apropiación de esta política.

En todo caso, todas las dependencias de la entidad deberán asistir a las capacitaciones o demás herramientas de uso y apropiación que entorno a la seguridad de la información se impartan, con el fin de dinamizar la cultura de la seguridad de la información en todas las operaciones institucionales.

Teniendo en cuenta lo anterior, es obligatorio que todos los usuarios, funcionarios y contratistas colaboradores de la SDA participen en los diferentes espacios que se realicen sobre estas políticas y sobre el manejo adecuado de los sistemas de información, con el fin de fortalecer y mejorar el adecuado manejo y custodia de la información de la entidad.

**CONTROL DE CAMBIOS**

| Versión | Descripción de la modificación | No. Acto Administrativo y fecha |
|---|---|---|
| 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. | Acta sesión #6 del Comité Institucional de Gestión y Desempeño de la SDA 18 de agosto de 2021 |
| 3 | Se actualiza introducción, marco normativo. Se incluyen objetivos específicos y definiciones y roles de Seguridad de la Información Se actualizan las políticas específicas de seguridad y privacidad de la información teniendo en cuenta la actualización de la Norma Técnica NTC-ISO 27001 de 2013 a norma ISO/CEI 27001:2022 “Seguridad de la información, ciberseguridad y protección de privacidad – Sistemas de gestión de la seguridad de la información.<br>Se incluyen nuevos lineamientos relacionados con el Control de acceso, respecto a las normas de seguridad para el control de acceso lógico, directrices de seguridad para el control de acceso físico, seguridad en zonas donde se realizan las actividades de tesorería, Port Security (Puerto seguro de red), responsables del control de acceso. Así mismo, se actualiza la Política asociado al Teletrabajo, trabajo en casa y acceso remoto, de acuerdo con la actualización normativa aplicable y contexto actual de la entidad. Se incluye nuevo lineamiento en la política de Seguridad de las operaciones relacionada con el uso de computadores personales. | Acta sesión #4 del Comité Institucional de Gestión y Desempeño de la SDA del 04 de agosto de 2023<br><br>Radicado 2023IE174378 del 31 de julio de 2023 |

**RESPONSABLES DE ELABORAR O ACTUALIZAR**

| Elaboró | Revisó | Aprobó |
|---|---|---|
| Nombre: Luis Alejandro Ruiz Alonso<br>Cargo: Oficial de Seguridad de la información<br>Contrato SDA –CPS-20231198 de 2023<br>Nombre: Francisco Andrés Daza Cardona<br>Cargo: Profesional equipo Seguridad de la información<br>Contrato SDA –CPS- 20231580 de 2023<br>Nombre: Yeandri Natalia Moreno López<br>Cargo: Enlace Sistema Integrado de Gestión<br>Contrato SDA-CPS-20230154<br>Nombre: Frederick Nicolai Ferro Mojica<br>Cargo: Asesor TI<br>Contrato SDA-CPS-20230706<br><br>Fecha: 07 de julio de 2023 | Nombre: Luisa Fernanda Moreno Panesso<br>Cargo: Directora de Planeación y Sistemas de Información Ambiental<br><br>Nombre: Jorge Álvarez Viviescas<br>Cargo: Apoyo auditoria de Sistemas de Información<br>Contrato SDA-CPS-20231538<br><br>Fecha: 17 de julio de 2023 | Nombre: Comité Institucional de Gestión y Desempeño<br>Fecha: 04 de agosto de 2023<br><br>Radicado 2023IE174378 del 31 de julio de 2023 |