SECRETARÍA DE HACIENDA

RESOLUCIÓN N° SDH-000172
(13 de mayo de 2022)

"Por la cual se adopta la Política de seguridad de la información y seguridad digitalde la Secretaría Distrital de Hacienda"

EL SECRETARIO DISTRITAL DE HACIENDA

En uso de las facultades que el literal o) del artículo 4° del Decreto 601 de 2014, modificado por el artículo 1° del Decreto 364 de 2015 y,

CONSIDERANDO:

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"*[1].

Que la Ley 1273 de 2009[2] crea un nuevo bien jurídico tutelado denominado *"De la protección de la información y los datos"* preservando integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Que la Ley 1341 de 2009[3] definió la organización institucional en materia TIC, identificando las autoridades en materia de "definición de política regulación, vigilancia y control de las TIC". En este sentido, la Resolución 305 de 2008,[4] expedida por la Comisión Distrital De Sistemas De Bogotá, D. C, hace énfasis en la obligación que tienen las entidades distritales de observar la Ley 1341 de 2009.

Que el artículo 2.2.22.2.1 del Decreto 1083de 2015,[5] estableció las políticas de Gestión y Desempeño Institucional, específicamente los numérales "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

Que el Decreto Nacional 1499 de 2017[6] sustituyó el título 22 del Decreto 1083 de 2015, estableciendo el objeto e instancias de dirección y coordinación del Sistema de Gestión y adoptando el nuevo Modelo Integrado de Planeación y Gestión -MIPG.

Que este mismo Decreto en sus artículos 2.2.22.3.1. y 2.2.22.3.2 adopta la versión actualizada del Modelo Integrado de Planeación y Gestión –MIPG, entendido como un marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

Que a nivel Distrital el Modelo Integrado de Planeación y Gestión – MIPG fue adoptado por elDecreto 591 de 2018,[7] como marco de referencia para el ajuste del diseño, la implementacióny la mejora continua del Sistema Integrado de Gestión Distrital - SIGD, con el fin de fortalecerlos 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 Decreto 807 de 20198 adopta en el Distrito Capital el Sistema de Gestión contemplado en las normas antes citadas, el cual se articula entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y *de Seguridad de la Información*.

Que el artículo 19 del Decreto Distrital 807 de 2019 señala que los Comités Institucionales de Gestión y Desempeño son los encargados de orientar la implementación y seguimiento del Sistema de Gestión y la operación del MIPG, articulando todas las áreas de la entidad, recursos, herramientas, estrategias y políticas de gestión y desempeño institucional, de acuerdo con la normatividad vigente en la materia.

Que la Secretaría Distrital de Hacienda, a través de la Resolución No. SHD-000014 del 29 deenero de 2019, creó el Comité Institucional de Gestión y Desempeño de la entidad y dictó lasdisposiciones para su funcionamiento.

Que con el fin de incorporar todas las modificaciones que conlleva el acatamiento de las nuevas disposi-

---

1 *Constitución Política de la República de Colombia.*

2 *Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.*

3 *Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones.*

4 *Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre.*

5 *"Por medio del cual se expide el Decreto único Reglamentario del Sector de Función Pública",*

6 *Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015*

7 *Por medio del cual se adopta el Modelo Integrado de Planeación y Gestión Nacional y se dictan otras disposiciones. Esta norma fue derogada por el Decreto 807 de 2019*

8 *Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital.*

ciones en un solo cuerpo normativo, a través de la Resolución No. SHD-000575 del 18 de diciembre de 2020, la Secretaría Distrital de Hacienda reorganizó el Sistema de Gestión y el Comité Institucional de Gestión y Desempeño de la entidad y dictó las disposiciones para su funcionamiento.

Que mediante Acta número 2 del 4 de febrero del 2022, el Comité Institucional de Gestión y Desempeño, una vez presentada la mencionada política y de acuerdo con el trabajo previo de las instancias, *"los miembros del comité, en mayoría absoluta, recomienda al señor secretario adoptar el documento de política presentado".*

Que con la implementación de la política de seguridad de la Información se busca generar un marco de actuación y reflejar el compromiso de la entidad frente a la implementación y mantenimiento de procesos que garanticen la protección de la integridad, la disponibilidad y laconfidencialidad de la información propia o de terceros, administrada por la Secretaría, dandogarantía de cumplimiento frente a las diferentes regulaciones, leyes y normas aplicables.

Que la Secretaría Distrital de Hacienda está comprometida con la implementación de mecanismos e instrumentos que permitan proteger, preservar y administrar la confidencialidad,integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en la Entidad, apoyada en la participación de los servidores públicos, contratistas y particulares que ejercen funciones públicas en la entidad.

Que teniendo en cuenta los cambios normativos, es pertinente actualizar la Política de Seguridad de la Información y Seguridad, con el objetivo de acatar la normatividad vigente, asícomo definir los lineamientos frente al uso y manejo de la información, e incluir disposiciones sobre firma electrónica, para la Secretaría Distrital de Hacienda.

Que el proyecto de regulación fue publicado a través del portal LEGALBOG durante 5 días hábiles, desde el 5 hasta el 12 de abril de 2022, sin que se hubieren recibido observaciones o sugerencias, por parte de la ciudadanía. Lo anterior en cumplimiento a lo establecido en el numeral 8 del artículo 8 de la Ley 1437 de 2011.

En mérito de lo expuesto,

RESUELVE:

Artículo 1. Objeto. Adoptar la Política de Seguridad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda, contenida en el Anexo 1, el cual forma parte integral de la presente resolución. Esta política debe publicarse en el Subsistema de Gestión de Seguridad de la Información (SGSI) de la entidad.

A través del correo institucional de la entidad, la Oficina Asesora de Comunicaciones informará a los servidores públicos y contratistas de la Secretaría Distrital de Hacienda la adopción de esta política.

Artículo 2. Vigencia. La presente Resolución rige a partir de la fecha de su publicación en el Registro Distrital y deroga la Política de Seguridad y Privacidad de la Información que fue adoptada el 25 de abril del 2017.

PUBLÍQUESE Y CÚMPLASE.

Dada en Bogotá, D.C., a los trece (13) días del mes de mayo de dos mil veintidós (2022).

JUAN MAURICIO RAMÍREZ CORTÉS
Secretario Distrital de Hacienda

SUBSUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código: POL – 05
Versión: 3

Tabla de contenido

Resumen

El presente documento es una actualización de la Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda, y se dictan lineamientos para el uso y manejo de la información.

La Constitución Política de Colombia en su artículo 15 consagra que todas las personas tienen derecho a su intimidad personal, 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.

La Ley 1341 de 2009 definió la organización institucional en materia TIC, identificando las autoridades en materia de "definición de política regulación, vigilancia y control de las TIC", entre las que se encuentra el Ministerio de Tecnologías de la Información y las Comunicaciones ("MinTIC"), la Comisión de Regulación de Comunicaciones ("CRC") y la Agencia Nacional del Espectro ("ANE"), tal como lo señalan los artículos 16 y siguientes de la referida Ley. En este sentido, resulta necesario que la Resolución CDS 305 de 2008 haga énfasis en la obligación que tienen las entidades distritales de observar la Ley 1341 de 2009 o aquella que la modifique o sustituya y los lineamientos de las autoridades nacionales competentes.

El Decreto Nacional 415 de 2016 impone la obligación de liderar una gestión estratégica TIC que incluya la definición, implementación, ejecución, divulgación y seguimiento de un Plan Estratégico de Tecnología y Sistemas de Información ("PETI"), el cual está incorporado en las estrategias de Gobierno en Línea del MinTIC en materia de arquitectura empresarial dentro del componente TIC para gestión ("Arquitectura TI"). Por lo tanto, se hace necesario replantear la existencia del Plan Estratégico de Sistemas de Información ("PESI") del que habla la Resolución CDS 305 de 2008, de tal forma que los esfuerzos de las entidades distritales se orienten al cumplimiento de las obligaciones que la normatividad nacional impone en materia de PETI.

Si bien la Resolución CDS 305 de 2008 hizo referencia al Decreto Nacional 1151 de 2008 y al correspondiente manual de Gobierno en Línea de la época, tal normatividad fue objeto de revisión y desarrollos posteriores por parte del MinTIC. El Decreto en mención fue derogado y reemplazado por el Decreto Nacional 2573 de 2014, el cual a su vez fue compilado por el Decreto Nacional 1078 de 2015, siendo este el que condensa en la actualidad la normatividad aplicable en materia de Gobierno en Línea (en especial en los artículos 2.2.9.1.1.1. y siguientes).

La Resolución 004 de 2017, "por la cual se modifica la Resolución 305 de 2008", expedida por la Comisión Distrital de Sistemas, en su articulado señala:

> "Artículo 1°-: Modificar el nombre del título del Capítulo Primero del Título I de la Resolución CDS 305 de 2008, el cual se denominará en lo sucesivo "Plan Estratégico de TIC - ("PETI")".
>
> "Modifica el nombre del título del Capítulo Primero del Título I de la Resolución CDS 305 de 2008, el cual se denominará en lo sucesivo "Plan Estratégico de TIC - ("PETI").", y modifica el ARTÍCULO 5°: Modificar el artículo 9 de la Resolución CDS 305 de 2008, el cual en lo sucesivo tendrá el siguiente tenor:
>
> Artículo 9. SEGURIDAD DIGITAL, Artículo 9°-:
>
> Modificar el artículo 29 de la Resolución CDS 305 de 2008, el cual en lo sucesivo tendrá el siguiente tenor: "Artículo 29. Integridad y Disponibilidad de la Información: Las entidades, organismos y órganos de control del Distrito Capital deben garantizar la integridad y disponibilidad de la información por parte de otras entidades y de la ciudadanía, atendiendo a los mandatos y las limitaciones impuestas por la Ley de Transparencia (Ley 1712 de 2014 o aquella que la modifique, complemente o sustituya) y

la normatividad de Gobierno en Línea. Esta obligación incluye, mas no se limita a la obligación de publicación de Datos Abiertos, contenida en la Ley de Transparencia. Parágrafo 1: Las medidas de seguridad e integridad de la información deben adoptarse en cada caso concreto y derivarse del análisis que haga la entidad respectiva respecto del carácter público de la información y los flujos de esta.

ARTÍCULO 6°: Modificar el artículo 16 de la Resolución CDS 305 de 2008, el cual en lo sucesivo tendrá el siguiente tenor: "Artículo 16. POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN", el ARTÍCULO 7°: Modificar el título del Capítulo Tercero del Título I de la Resolución CDS 305 de 2008, el cual se denominará en lo sucesivo "Acceso a Información Pública y Gobierno en Línea".

La Ley 1712 de 2014 adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "Por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", establece las directrices para la calificación de información pública; en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

El artículo 2.2.9.1.1.3. del Decreto 1078 de 2015, subrogado por el artículo 1 del Decreto 1008 de 2018, determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través de este se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano, con el fin de sentar las base normativa en relación a seguridad de la información, privacidad y tratamiento de datos personales.

El artículo 2.2.22.2.1 del Decreto 1083 de 2015, "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública", establece las políticas de Gestión y Desempeño Institucional, específicamente los numérales "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital".

El Documento CONPES 3854 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El Documento CONPES 3995 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital, de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

A su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios

existentes en la administración pública", establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

La Secretaría Distrital de Hacienda, a través de la Resolución No. SHD-000575 de 2020, creó el Comité Institucional de Gestión y Desempeño de la entidad y dictó las disposiciones para su funcionamiento.

En cumplimiento de la citada normativa del orden nacional, el Distrito Capital expidió el Decreto Distrital 807 del 24 de diciembre de 2019, "Por medio del cual se reglamenta el Sistema de Gestión en el Distrito Capital", y se dictan otras disposiciones", y adoptó el Sistema de Gestión de qué trata el artículo 2.2.22.1.1 del Decreto Nacional 1083 de 2015, modificado por el artículo 1 del Decreto Nacional 1499 de 2017, a través de la implementación del Modelo Integrado de Planeación y Gestión –MIPG.

El artículo 4 del Decreto Distrital 807 de 2019, en concordancia con el artículo 2.2.22.1.5 del Decreto 1083 de 2015, señala que "El Sistema de Gestión se complementa y articula, entre otros, con los Sistemas Nacional de Servicio al Ciudadano, de Gestión de la Seguridad y Salud en el Trabajo, de Gestión Ambiental y de Seguridad de la Información. (...)"

El artículo 5 del Decreto Distrital 807 de 2019, "Por medio del cual se reglamenta el Sistema de Gestión en e/Distrito Capital y se dictan otras disposiciones", en concordancia con el artículo 2.2.22.3.2 del Decreto Nacional 1083 de 2015, definió el Modelo Integrado de Planeación y Gestión -MIPG como "(...) el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio".

Ahora bien, en el marco de la Resolución CDS 305 de 2008, "Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre", se hizo referencia al Decreto Nacional 1151 de 2008 y al correspondiente manual de Gobierno en Línea de la época, la Secretaria Distrital de Hacienda, mediante el Comité del Sistema Integrado de Gestión del 26 de enero de 2017, aprobó y pública la actualización a las políticas de seguridad y privacidad de la información.

De otra parte, la Ley 527 de 1999 en el artículo 2º literal c), define la firma digital "como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación".

El artículo 1 del Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, define la firma electrónica como: métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

El Decreto Ley 2106 de 2019, "Por el cual se dictan normas para simplificar, suprimir y reformar

trámites, procesos y procedimientos innecesarios existentes en la administración pública", a través de sus artículos 14 y 15, atribuye al MinTIC la potestad de regular la forma en que las autoridades deben integrar a su sede electrónica todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes, que permitan la realización de trámites, procesos y procedimientos a los ciudadanos de manera eficaz.

El referido artículo 15 otorga la competencia al MinTIC para señalar los términos en que las autoridades deben integrar su sede electrónica al Portal Único del Estado colombiano, que funciona como una sede electrónica compartida a través de la cual los ciudadanos accederán a la información, los procedimientos, los servicios y los trámites que se deban adelantar ante las autoridades. Para tales efectos, el mismo artículo atribuye al MinTIC la función de establecer las condiciones de creación e integración de dichos portales, e igualmente dispone que las ventanillas únicas existentes deben integrarse al Portal Único del Estado Colombiano.

La Resolución 500 del 10 de marzo del 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, tiene por objeto establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital.

Teniendo en cuenta los cambios normativos, es necesario actualizar la Política de Seguridad de la Información y Seguridad, así como definir los lineamientos frente al uso y manejo de la información, e incluir disposiciones sobre firma electrónica, para la Secretaría Distrital de Hacienda.

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

DISPOSICIONES GENERALES

Ámbito de aplicación. La Política de Seguridad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda, aplica a todos sus servidores públicos, contratistas, proveedores, operadores, entidades adscritas, y aquellas personas o terceros que en razón del cumplimiento de sus funciones en la Secretaría Distrital de Hacienda compartan, utilicen, recolecten, procesen, intercambien o consulten su información, al igual que a las entidades de control, y demás entidades relacionadas que accedan, ya sea interna o externamente a cualquier activo de información, independientemente de su ubicación.

De igual manera, esta política aplica a toda la información creada, procesada o utilizada por la Secretaría Distrital de Hacienda, sin importar el medio, formato, presentación o lugar en el cual se encuentre.

Política de Seguridad de la Información y Seguridad de la Secretaría Distrital de Hacienda. La Secretaría Distrital de Hacienda, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información enmarcado en el Subsistema de Gestión de Seguridad de la información, protege, preserva y administra la confidencialidad, la integridad, la disponibilidad, la autenticidad, la privacidad y no repudio de la información que circula en la Entidad, de acuerdo con lo estipulado en el mapa de procesos, mediante una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, propender por la continuidad de la operación de los servicios tecnológicos y dar cumplimiento a los requisitos legales, reglamentarios y regulatorios, orientados a la mejora continua y al alto desempeño del Subsistema de Gestión de Seguridad de la información, promoviendo así el acceso, uso efectivo y apropiación masiva de las Tecnologías de la Información y las Comunicaciones - TIC, a través de políticas y programas, para mejorar la calidad de vida de los ciudadanos y el incremento sostenible del desarrollo del Distrito Capital.

Objetivo General: La política de seguridad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda pretende generar un marco de actuación y reflejar el compromiso de la entidad frente a la implementación y mantenimiento de procesos que garanticen la protección de la integridad, disponibilidad y confidencialidad de la información propia o de terceros, administrada por la Secretaria, dando garantía de cumplimiento frente a las diferentes regulaciones, leyes y normas aplicables.

Objetivos específicos:

- **a.** Definir, formular y formalizar los elementos normativos sobre los temas de protección de la información.
- **b.** Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios.
- **c.** Dar lineamientos que permitan establecer mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información de la Secretaría Distrital de Hacienda.
- **d.** Establecer lineamientos frente al proceso de Gestión Documental, para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
- **e.** Fortalecer la cultura organizacional a través de la concienciación y apropiación de la seguridad y privacidad de la información y la seguridad digital.

f. Dar cumplimiento a los requisitos legales y normativos en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal.

POLÍTICAS ESPECIFÍCAS DE MANEJO DE INFORMACIÓN

Política de seguridad de los recursos humanos. La Secretaría Distrital de Hacienda debe desplegar esfuerzos para generar conciencia y apropiación en los servidores públicos de la entidad, sobre sus responsabilidades en el marco de la Política de Seguridad de la Información y Seguridad Digital, con el fin de reducir los riesgos de la información, el mal uso de las instalaciones y recursos tecnológicos y así asegurar la confidencialidad, integridad y disponibilidad de la información.

1. Con el mismo fin, debe incluir en las minutas de los contratos y convenios, cualquiera que sea su naturaleza o modalidad, cláusulas y obligaciones frente al cumplimiento de la Política de Seguridad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda, las cuales deberán ser divulgadas a través de los supervisores e interventores de los contratos, a proveedores, a operadores y aquellas personas o terceros que en razón del cumplimiento de sus funciones, obligaciones y las que con la Secretaria Distrital de Hacienda, compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

2. Así mismo la Secretaría Distrital de Hacienda deberá fomentar la participación de los servidores de la entidad en las convocatorias para el fortalecimiento de capacidades en Seguridad digital realizadas por el Gobierno Distrital, Nacional u organismos internacionales.

Política de Gestión de Activos. La Secretaría Distrital de Hacienda establecerá y divulgará los lineamientos específicos para la identificación, clasificación, valoración, rotulado y buen uso de los activos de información, con el objetivo de garantizar su protección. Dichos lineamientos se impartirán teniendo en cuenta los siguientes literales:

a. Inventario de Activos: Los activos de la Secretaría Distrital de Hacienda deben ser identificados, clasificados, valorados y controlados para garantizar su uso, protección y recuperación ante desastres. Por tal motivo, se debe diseñar una metodología con los lineamientos necesarios para llevar el inventario de los activos de información, discriminado por procesos y dependencia, tipo, nivel de criticidad, clasificación, ubicación, responsable, custodio, y demás atributos que la entidad defina.

b. Protección: Con el objetivo de establecer los controles de seguridad físicos y digitales, las dependencias que tienen la custodia de la información generada en el marco de su función se encargarán de proteger la información, así como de mantener y actualizar el inventario de activos de información relacionados con sus servicios (información física o digital, software, hardware y recurso humano), bajo los parámetros que establezca la Dirección de Informática y Tecnología.

c. Archivos de Gestión: Se debe implementar controles para que los archivos de gestión cuenten con los mecanismos de seguridad apropiados, de acuerdo con las Tablas de Retención Documental y Tablas de Control de Acceso, con el fin de proteger y conservar la confidencialidad, integridad y disponibilidad de la información física de la Secretaría Distrital de Hacienda.

d. **Clasificación de la Información:** La Subdirección de Gestión Documental deberá establecer una metodología para la clasificación y rotulado de la información de la Secretaría Distrital de Hacienda, en el marco de la Ley 594 de 2000 (Ley General de Archivos), la Ley 1712 de 2014, reglamentada por el Título 1 de la Parte 1 del Libro 2 del Decreto 1081 de 2015 y el Decreto 1080 de 2015 y demás normatividad que reglamente la clasificación de información de las entidades públicas del país. Así mismo, la Dirección de Informática y Tecnología implementará una herramienta informática que permita rotular la información digital y la Subdirección de Gestión Documental mecanismos para rotular la información física, de acuerdo con la metodología establecida.

e. **Firma de documentos:** Las firmas de documentos que produzca la Secretaría Distrital de Hacienda será válida en cualquiera de los siguientes métodos, garantizando la confiabilidad, integridad, autenticidad y disponibilidad de la información de los documentos expedidos por los servidores públicos, contratistas y terceros que ejerzan funciones públicas en la entidad, en el marco de sus funciones y competencias:

I. En físico con firma autógrafa mecánica.
II. Con firma digital de persona natural asignadas por la Dirección de Informática y Tecnología, según lo dispuesto por la Ley 527 de 1999.
III. Con firma electrónica, de acuerdo con lo dispuesto en el Decreto 2364 de 2012 y el Decreto 1287 de 2020, para lo cual la Dirección de Informática y Tecnología deberá adquirir o implementar un aplicativo integrado con el sistema de gestión documental que contenga como mínimo lo siguiente:

a. Control seguro de acceso y uso al aplicativo, sincronizado con el directorio activo, garantizando que solo personal vinculado pueda hacer uso del mecanismo de firma electrónica;
b. Múltiples controles para la autenticación y firma del documento electrónico, garantizando que el firmante es quien dice ser;
c. El sistema debe solicitar la firma digitalizada o escaneada y quedar estampada en el documento junto con el nombre completo, cargo, correo electrónico institucional del servidor o contratista que firma;
d. Identificador único provisto por el sistema que permita la verificación de la veracidad del documento;
e. Fecha de creación y finalización de la firma provisto por el servidor y sincronizado con la hora legal colombiana de acuerdo con lo establecido en el numeral 14 del artículo 6 del Decreto 4175 de 2011;
f. Estado del trámite de firma;
g. Firma digital de persona jurídica de la Secretaría Distrital de Hacienda según sea el caso;
h. En ningún caso se debe utilizar firmas facsímil, salvo en aquellos que se autorice por Resolución, expedida por el Secretario Distrital de Hacienda, indicando para que fin y porqué medios podrá ser utilizada.

Política de Control de Acceso. Los propietarios de los activos de información, teniendo en cuenta el tipo de activo, deberán adoptar las medidas de control de acceso a nivel de red, sistema operativo, sistemas de información, servicios de tecnologías e infraestructura física (instalaciones y oficinas) establecidas, todo esto con el fin de mitigar riesgos asociados al acceso a la información, infraestructura tecnológica e infraestructura física de ingreso de personal no autorizado y así propender por salvaguardar la integridad, disponibilidad y confidencialidad de la información de la Secretaría Distrital de Hacienda.

Política de Criptografía. La Dirección de Informática y Tecnología dispondrá de herramientas que permitan el cifrado de la información clasificada y reservada para proteger su confidencialidad, integridad y disponibilidad. El cifrado de la información se realizará por solicitud de los usuarios o de manera general cuando así lo requiera la Secretaría Distrital de Hacienda.

Política de Privacidad. La Secretaría Distrital de Hacienda deberá disponer de controles necesarios para la protección de la información de los servidores públicos, contratistas y partes interesadas externas, en los términos de la Ley 1581 de 2012 y sus decretos reglamentarios, así como la política de tratamiento de datos personales de la Secretaría Distrital de Hacienda.

1. La Secretaría Distrital de Hacienda dispondrá de formatos de autorización y uso de datos personales, así como su tratamiento, en lo que respecta al uso de datos semiprivados, privados y sensibles; dicho formato debe ser claro y detallado en lo referente a la recolección de la información de los servidores públicos y contratistas de la Secretaría Distrital de Hacienda; así mismo, deberá ser firmado por todos los servidores públicos y contratistas como parte de sus obligaciones.

2. La Secretaría Distrital de Hacienda dispondrá de formatos de autorización, por parte de los ciudadanos, para la captación y uso de imágenes, videos o cualquier medio audiovisual, de conformidad con lo dispuesto en las normas vigentes sobre protección de datos personales, en especial la Ley 1581 de 2012 y el Decreto 1074 de 2015, así como su autorización libre, expresa e inequívoca a la Secretaría Distrital de Hacienda. Los formatos deberán prever la opción en que el ciudadano sea menor de edad y se deberá establecer un procedimiento para el caso en que el ciudadano no autorice dicho tratamiento.

Política de Seguridad Física y del Entorno. La Secretaría Distrital de Hacienda adoptará medidas para la protección del perímetro de seguridad de sus instalaciones físicas para controlar el acceso y permanencia del personal en las oficinas, instalaciones y áreas restringidas (áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones), con el fin de mitigar los riesgos, amenazas externas, ambientales y evitar afectación a la confidencialidad, integridad y disponibilidad de la información de la entidad.

Política de Seguridad de las Operaciones. La Dirección de Informática y Tecnología de la Secretaría Distrital de Hacienda será la encargada de la operación y administración de los recursos tecnológicos que soportan la operación. Así mismo, velará por la eficiencia de los controles asociados a los recursos tecnológicos, protegiendo la confidencialidad, integridad y disponibilidad de la información e implantará un comité de control de cambios, en donde se realice un análisis de riesgos previamente, para que los cambios efectuados sobre los recursos tecnológicos y sistemas de información en ambientes de producción sean controlados y debidamente autorizados; así mismo implementará mecanismos para controlar la información en los ambientes de desarrollo y prueba. De igual manera, proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la entidad, al igual que desarrollará mecanismos de contingencias y recuperación ante desastres, con el fin de propender por la disponibilidad de los servicios de TI en el marco de la operación de la Secretaría Distrital de Hacienda.

De igual manera, la Dirección de Informática y Tecnología debe realizar y mantener respaldos de la información de la entidad en medio digital, control interno velará por la verificación de dichos controles, de manera que estén disponibles siempre, con el objetivo de recuperarla en caso de cualquier tipo de falla. La Dirección de Informática y Tecnología efectuará las copias respectivas, de acuerdo con el esquema definido previamente, en un procedimiento que enmarque la gestión de las copias de seguridad de la información digital, sistemas de información, bases de datos y demás recursos tecnológicos de la entidad.

Dicho procedimiento se hará bajo la dirección de la Dirección de Informática y Tecnología, con el apoyo de los líderes de proceso y deberá estar alineado con la gestión documental de la entidad, con el fin de determinar la información a respaldar, la periodicidad, los tiempos de retención, recuperación, restauración y los mecanismos para generar el menor impacto en la prestación del servicio durante el tiempo de la indisponibilidad de la información.

En el evento que alguna dependencia haga uso de una plataforma tecnológica fuera de las instalaciones físicas y en el marco de las funciones misionales u operacionales de la Secretaría Distrital de Hacienda, deberá cumplir con lo establecido en la presente política y los lineamientos dispuestos por la Secretaría Distrital de Hacienda, en Seguridad de la Información.

Política de Seguridad de las Comunicaciones. La Dirección de Informática y Tecnología establecerá los mecanismos necesarios para proveer la disponibilidad de la infraestructura de red y de los servicios tecnológicos que dependen de ellas; así mismo, dispondrá y monitoreará los mecanismos necesarios de seguridad para proteger la integridad y la confidencialidad de la información de la Secretaría Distrital de Hacienda.

Se establecerán mecanismos estratégicos para que el intercambio de información con las partes interesadas internas o externas, se realice asegurando su integridad. En el evento que los acuerdos de intercambio de información requieran del desarrollo de servicio web (web service) o de cualquier otro medio tecnológico, el intercambio deberá realizarse con los controles criptográficos definidos en la política de criptografía de la Política de Seguridad y Privacidad de la Información del presente documento y será coordinado por la Dirección de Informática y Tecnología con los mecanismos establecidos para tal fin.

Política de Seguridad para la Adquisición, Desarrollo y Mantenimiento de Sistemas. La Dirección de Informática y Tecnología garantizará que el desarrollo interno y externo de los sistemas de información, cumpla con los requerimientos de seguridad adecuados para la protección de la información de la Secretaría Distrital de Hacienda, para lo cual establecerá una metodología que detalle los requerimientos de seguridad para el desarrollo, pruebas, puesta en producción y mantenimiento de los sistemas de información.

En el marco del Plan Estratégico de Tecnologías de la Información (PETI), la Dirección de Informática y Tecnología es la única dependencia de la entidad con la capacidad de adquirir, desarrollar e implementar soluciones tecnológicas para la Secretaría Distrital de Hacienda, así como de avalar la adquisición y recepción de software de cualquier tipo en el marco de convenios y contratos con terceros, conforme a los requerimientos de las dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la entidad.

En consecuencia, cualquier software que opere en la Secretaría Distrital de Hacienda deberá contar con la autorización de la Dirección de Informática y Tecnología y deberá reportarse y

entregarse cumpliendo con los lineamientos técnicos y presupuestales de dicha dependencia, con el fin de salvaguardar la información, brindar el soporte y demás procesos técnicos que permitan su recuperación en caso de algún incidente o siniestro.

En caso de que alguna dependencia adquiera, desarrolle o realice mantenimientos a sistemas de información dentro del desarrollo misional u operacional de la Secretaría Distrital de Hacienda, deberá cumplir con lo establecido en la presente política y deberá solicitar acompañamiento de la Dirección de Informática y Tecnología.

Política de Seguridad para Relación con Proveedores. La Secretaría Distrital de Hacienda establecerá las disposiciones necesarias para asegurar que la información que se genere, custodie, procese, comparta, utilice, recolecte, intercambie o a la que se tenga acceso con ocasión de la celebración de un contrato, sea custodiada por los proveedores, siguiendo los lineamientos establecidos en seguridad de la información por la SDH. De igual manera en el seguimiento en la ejecución, se garantizará que los supervisores velen por el cumplimiento de las políticas y procedimientos de seguridad de la información durante la ejecución de los contratos, estos lineamientos deberán ser comunicados a los proveedores.

Política de Gestión de Incidentes de Seguridad de la Información. La Secretaría Distrital de Hacienda, a través de la mesa de servicio de la subdirección de servicios de TI, promoverá entre los servidores públicos y contratistas de la entidad, el reporte y seguimiento de incidentes. Así mismo, asignará responsables para el tratamiento de estos y definiría un triage, que permita establecer cuáles de los incidentes que se reportan a través de la mesa de servicios corresponden a seguridad de la información y los escalará a seguridad de la información para ser registrado como evento de riesgo y posteriormente investigado y gestionado de acuerdo con el procedimiento vigente.

El secretario, como representante de la Secretaría Distrital de Hacienda, definirá las personas idóneas para reportar incidentes de seguridad ante las autoridades de defensa nacional, policía, fiscalía y de control; quienes serán los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas, medios de comunicación o la ciudadanía. La delegación de esta potestad se podrá hacer formal, por medio de acto administrativo, si se considera necesario.

Política de la Continuidad de la Operación de los Servicios. La Dirección de Tecnología deberá disponer de estrategias y planes de contingencia tecnológica para garantizar la continuidad de los servicios de los sistemas de información de la SDH, de acuerdo con las necesidades establecidas por los procesos, y de acuerdo con las Políticas de Gestión de Continuidad del Negocio, adoptada por la SDH.

Así mismo, las estrategias adoptadas para garantizar la recuperación y continuidad tecnológica, deberán cumplir con las reglas y políticas establecidas y adoptadas en materia de seguridad de la información por parte de la SDH.

Política de Cumplimiento. La Secretaría Distrital de Hacienda velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados en la seguridad y privacidad de la información, de acuerdo con lo establecido por el gobierno nacional, entre ellos los referentes a derechos de autor y propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional, entre otras que se encuentren vigentes y de obligatorio cumplimiento en el distrito y los lineamientos a nivel nacional.

Política de Seguridad de la Información en la gestión de proyectos. La Secretaría Distrital de Hacienda velará por la inclusión de los requerimientos y consideraciones en materia de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios durante la fase y las metodologías de formulación de los proyectos de la entidad. Así mismo, todos aquellos criterios y requerimientos se deben implementar desde las fases iniciales de los proyectos. En el mismo sentido, se deberá incluir dentro de su plan de auditorías la revisión de su cumplimiento e implementación.

La Dirección Jurídica debe velar porque, en todos los estudios precontractuales de los proyectos o contratos a celebrar con la Secretaría Distrital de Hacienda, se incluyan los requerimientos y consideraciones referentes a Seguridad de la Información, Seguridad Digital y Continuidad de la operación de los servicios que se están contratando.

Política de Seguridad de la Sede Electrónica. La Dirección de Informática y Tecnología será la encargada de la administración y gestión de la sede electrónica de la Secretaría Distrital de Hacienda, en donde se deberán integrar todos los portales, sitios web, plataformas, ventanillas únicas, aplicaciones y soluciones existentes. Para la operación de la sede electrónica se deberá definir e implementar, en concordancia con las dependencias responsables de trámites, procesos y procedimientos dirigidos a los ciudadanos, las medidas jurídicas, organizativas y técnicas que garanticen la calidad, seguridad, privacidad, disponibilidad, integridad, confidencialidad, accesibilidad, neutralidad e interoperabilidad de la información y de los servicios, de acuerdo con los lineamientos emitidos por MinTIC, para la estandarización de las ventanillas únicas, portales de programas transversales y unificación de sedes electrónicas.

RESPONSABILIDADES DE LOS COLABORADORES FRENTE AL USO DE LOS SERVICIOS TECNOLÓGICOS

Política de Seguridad Digital. Todos los colaboradores que hagan uso de los recursos tecnológicos de la Secretaría Distrital de Hacienda tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable; entendiendo que el uso no adecuado de los recursos pone en riesgo la seguridad, estabilidad y continuidad de la operación de los servicios y, por ende, el cumplimento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

a. Del uso del correo electrónico. El correo electrónico institucional es una herramienta de apoyo a la ejecución de funciones y obligaciones de los servidores públicos y contratistas de la Secretaría Distrital de Hacienda, cuyo uso se facilitará en los siguientes términos:

i. El único servicio de correo electrónico autorizado para el manejo o transmisión de la información institucional en la entidad es el asignado por la Dirección de Informática y Tecnología, que cuenta con el dominio @shd.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad, evitando ataques de virus, spyware y otro tipo de software malicioso.
ii. El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional, en consecuencia, no debe ser utilizado con fines personales, económicos, comerciales o cualquier otro ajeno a los propósitos de la entidad.
iii. En cumplimiento de la iniciativa institucional del uso aceptable del papel y la eficiencia administrativa, se debe preferir el uso del correo electrónico al envío de documentos físicos, siempre que la ley lo permita.

iv. Los mensajes de correo están respaldados por la Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, se establecen las entidades de certificación y se dictan otras disposiciones, la cual establece la validez de los mensajes de datos.
v. La Dirección de Informática y Tecnología implementará herramientas tecnológicas que prevengan la pérdida o fuga de información de carácter reservada o clasificada, de conformidad con la Ley 1712 de 2014.
vi. Se prohíbe el envío de correos masivos internos o externos, con excepción de los enviados por el despacho del Secretario Distrital de Hacienda, Subsecretarias, Oficina Asesora de Comunicaciones, Oficina Asesora de Planeación, o áreas previamente autorizadas, así como de la Dirección de Informática y Tecnología, solamente en caso de ventana de mantenimientos de los servicios de TI. Los correos masivos deben cumplir con las características de comunicación e imagen corporativa.
vii. Todo mensaje de correo electrónico enviado por la Secretaría Distrital de Hacienda mediante plataformas externas deberá hacerse con la cuenta de la entidad y utilizando el dominio @shd.gov.co, con el fin de que no sean catalogados como spam o suplantación de correo.
viii. Para apoyar la gestión de correo electrónico de directivos, el titular debe solicitar a la mesa de servicios la delegación del buzón correspondiente, relacionando los colaboradores que podrán escribir o responder en nombre del titular, con el fin de mitigar la suplantación.
ix. Todo mensaje SPAM, cadena, de remitente o contenido sospechoso, debe ser inmediatamente reportado a la Dirección de Informática y Tecnología, a través de la Mesa de Servicios, como incidente de seguridad según el procedimiento establecido, y deberán acatarse las indicaciones recibidas para su tratamiento, lo anterior, debido a que puede contener virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif, o explícitas referencias no relacionadas con la misión de la entidad (como por ejemplo: contenidos eróticos, alusiones a personajes famosos). Está expresamente prohibido el envío y reenvío de mensajes en cadena.
x. La cuenta de correo institucional no debe ser revelada en páginas o sitios publicitarios, de comercio electrónico, deportivos, agencias matrimoniales, casinos, o cualquier otra ajena a los fines de la entidad.
xi. Está expresamente prohibido el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y que atenten contra la integridad moral de las personas o instituciones.
xii. Está expresamente prohibido distribuir información oficial de carácter clasificada o reservada de la Secretaría Distrital de Hacienda a otras entidades o ciudadanos, sin la debida autorización del despacho del Secretario, quien es el responsable ante las autoridades de velar por la integridad y confidencialidad de la información de la entidad.
xiii. El cifrado de los mensajes de correo electrónico institucional será necesario siempre que la información transmitida esté catalogada como clasificada o reservada en el inventario de activos de información o en el marco de la ley.
xiv. El correo electrónico institucional en sus mensajes debe contener una sentencia de confidencialidad, que será diseñada por la Dirección de Informática y Tecnología con el apoyo de la Oficina Asesora de Comunicaciones, dicha sentencia debe reflejarse en todos los buzones con dominio @shd.gov.co.
xv. Está expresamente prohibido distribuir, copiar o reenviar información de la Secretaría Distrital de Hacienda, a través de correos personales o sitios web diferentes a los autorizados, en el marco de las funciones u obligaciones contractuales.
xvi. Cuando un servidor público o contratista cesa en sus funciones o culmina la ejecución de contrato con la Secretaría Distrital de Hacienda, no se le entregará copia de los buzones de correo institucionales a su cargo, salvo autorización expresa del Secretario,

Subsecretarios, por orden judicial, por solicitud de la Oficina de Control Interno o de la Subdirección del Talento humano, Oficina de Control Interno Disciplinario como parte de un proceso de investigación. En cualquier caso, esta acción debe ser autorizada por Seguridad de la Información.

La Secretaría Distrital de Hacienda, a través de la Dirección de Informática y Tecnología, se reserva el derecho de monitorear los accesos y el uso de los buzones de correo institucional de todos sus servidores públicos o contratistas. Además, podrá realizar copias de seguridad del correo electrónico en cualquier momento sin previo aviso y limitar el acceso temporal o definitivo a todos los servicios y accesos a sistemas de información de la entidad o de terceros operados en la misma, previa solicitud expresa del supervisor del contrato, jefe inmediato, secretario, subsecretarios, Oficina de Control Interno Disciplinario o del Subdirección del Talento humano a la Dirección de Informática y Tecnología. Para ello, al inicio de la relación laboral o contractual se deberá comunicar a los servidores públicos y contratistas que la Secretaría Distrital de Hacienda realiza el referido monitoreo.

b. Del uso de Internet: La Dirección de Informática y Tecnología, en conjunto con el Oficial de la Seguridad de la Información o quien haga sus veces, establecerá políticas de navegación basadas en categorías y niveles de usuario por jerarquía, funciones u obligaciones. Será responsabilidad de los servidores públicos y contratistas las siguientes, entre otras:

i. Los servicios a los que un determinado usuario pueda acceder en internet dependerán del rol o funciones que desempeña en la Secretaría Distrital de Hacienda y para las cuales esté formal y expresamente autorizado por su jefe o supervisor y solo se utilizará para fines laborales.
ii. Abstenerse de enviar, descargar y visualizar páginas con contenido insultante, ofensivo, injurioso, obsceno, violatorio de los derechos de autor o que atenten contra la integridad moral de las personas o instituciones.
iii. Abstenerse de acceder a páginas web, portales, sitios web y aplicaciones web que no hayan sido autorizadas por la Secretaría Distrital de Hacienda.
iv. Abstenerse de enviar y descargar cualquier tipo de software o archivo de fuentes externas y de procedencia desconocida.
v. Abstenerse de propagar intencionalmente virus o cualquier tipo de código malicioso.

La Secretaría Distrital de Hacienda, a través de la Dirección de Informática y Tecnología, se reserva el derecho de monitorear los accesos y el uso del servicio de Internet, además de limitar el acceso a determinadas páginas de Internet, los horarios de conexión, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro uso ajeno a los fines de la Entidad.

c. Del uso de los recursos tecnológicos: Los recursos tecnológicos de la Secretaría Distrital de Hacienda son herramientas de apoyo a las labores y responsabilidades de los servidores públicos y contratistas. Por ello, su uso está sujeto a las siguientes directrices:

i. Los bienes de cómputo que provea la entidad se emplearán de manera exclusiva y bajo la completa responsabilidad del servidor público o contratista al cual han sido asignados, únicamente para el desempeño de las funciones del cargo o las obligaciones contractuales pactadas. Por tanto, no pueden ser utilizados con fines personales o por terceros no autorizados por la Dirección de Informática y Tecnología, salvo que medie solicitud formal del Secretario, subsecretarios, directores, subdirectores, jefes de Oficina, a través de la Mesa de Servicios.

ii. Sólo está permitido el uso de software licenciado por la entidad y aquel que, sin requerir licencia, sea expresamente autorizado por la Dirección de Informática y Tecnología,
iii. En caso de que el servidor público o contratista deba hacer uso de equipos ajenos a la Secretaría Distrital de Hacienda, éstos deberán cumplir con la legalidad del Software instalado, sistema operativo y antivirus licenciado, actualizado y solo podrá conectarse a la red de la Secretaría Distrital de Hacienda, una vez esté avalado por la Dirección de Informática y Tecnología.
iv. Los servidores públicos y contratistas deberán realizar y mantener las copias de seguridad de su información y entregarla a la entidad al finalizar la vinculación.
v. Está expresamente prohibido el almacenamiento en los discos duros de computadores de escritorio, portátiles o discos virtuales de red, archivos de video, música y fotos que no sean de carácter institucional, así como información institucional que no sea de apoyo a la gestión o que atenten contra los derechos de autor o propiedad intelectual de los mismos. La DIT ha dispuesto para garantizar el almacenamiento de información institucional espacios de carácter colaborativo para tal fin como One Drive, Sharepoint y sitios compartidos como la unidad X (espacio asignado a cada servidor público) y el File Server con asignación de espacio compartido para cada una de las dependencias de la entidad (despacho del Secretario de Hacienda, Subsecretaría y Oficinas Asesoras) y direcciones de la SDH cuya administración es responsabilidad del delegado de cada dependencia. Por lo anterior la DIT a través de la Subdirección de Servicios de TIC no realiza toma de backup de la información consignada en los discos duros de los equipos institucionales.
vi. Los servidores públicos y contratistas deberán utilizar las herramientas tecnológicas que proporcione la Dirección de Informática y Tecnología para gestionar la información digital de la Secretaría Distrital de Hacienda.
vii. No está permitido ingerir alimentos o bebidas en el área de trabajo donde se encuentren elementos tecnológicos o información física que pueda estar expuesta a daño parcial o total y por ende, a la pérdida de la integridad de ésta.
viii. No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo los elementos tecnológicos por fallas en el suministro eléctrico a los equipos de cómputo, salvo en aquellos casos autorizados expresamente por la Subdirección Administrativa y Financiera.
ix. Las únicas personas autorizadas para hacer modificaciones o actualizaciones en los elementos y recursos tecnológicos, como destapar, agregar, desconectar, retirar, revisar o reparar sus componentes, son las designadas para tal labor por la Dirección de Informática y Tecnología.
x. La Dirección de Informática y Tecnología realizará control y monitoreo sobre los dispositivos de almacenamiento externos como USB, CD-ROM, DVD, Discos Duros externos, entre otros, con el fin de prevenir o detectar fuga de información clasificada y reservada.
xi. La única dependencia autorizada para trasladar los elementos y recursos tecnológicos de un puesto a otro es la Dirección Corporativa, a través de la Subdirección Administrativa y Financiera, con el fin de llevar el control individual de inventarios. En tal virtud, toda reasignación de equipos deberá ajustarse a los procedimientos y competencias de la gestión de bienes de la Entidad.
xii. La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, deberá ser informada de inmediato a la Dirección de Informática y Tecnología por el servidor público o contratista a quien se le hubiere asignado; en caso de que el equipo de cómputo sea propiedad de la Secretaría Distrital de Hacienda, deberá reportarse a la Subdirección Administrativa y Financiera, siguiendo los procedimientos establecidos para este tipo de siniestros, sin perjuicio de las acciones penales y disciplinarias que requiera adelantar según sea el caso.

xiii. La pérdida de información deberá ser informada con detalle a la Dirección de Informática y Tecnología, a través de la Mesa de Servicios, como incidente de seguridad.

xiv. Todo incidente de seguridad que comprometa la confidencialidad, integridad o disponibilidad de la información física o digital deberá ser reportado a la mayor brevedad a la Dirección de Informática y Tecnología, a través de la Mesa de Servicios, siguiendo el procedimiento establecido.

xv. La Dirección de Informática y Tecnología es la única dependencia autorizada para la administración del software de la Secretaría Distrital de Hacienda, el cual no deberá ser copiado, suministrado a terceros ni utilizado para fines personales.

xvi. Todo acceso a la red de la entidad, mediante elementos o recursos tecnológicos no institucionales, deberá ser informado, autorizado y controlado por la Dirección de Informática y Tecnología.

xvii. La conexión a la red wifi institucional para servidores públicos y contratistas deberá ser administrada desde la Dirección de Informática y Tecnología mediante un SSID (Service Set Identifier) único; la autenticación deberá ser con usuario y contraseña de directorio activo.

xviii. La conexión a la red institucional para visitantes deberá tener un SSID y contraseñas administradas por la Dirección de Informática y Tecnología, las contraseñas deberán cambiar con frecuencia.

xix. La red wifi para servidores públicos y contratistas estará disponible para sus equipos personales, teniendo en cuenta las capacidades técnicas, contractuales y lineamientos de seguridad establecidos por la Secretaria Distrital de Hacienda.

xx. Los equipos deben quedar apagados cada vez que el servidor público o contratista no se encuentre en la oficina o durante la noche, o cuando se encuentre de permiso, vacaciones, licencia médica o no remunerada, esto, con el fin de proteger la seguridad y optimizar los recursos de la entidad, si necesita realizar actividades remotas se deberá solicitar, autorización a creación de usuarios, con la justificación correspondiente.

xxi. Todo dispositivo personal que requiera acceder a los servicios tecnológicos de la entidad debe acogerse a las políticas de seguridad de la información y deberá ser verificado por la Subdirección de Servicios de TI, que el software del sistema operativo y el antivirus, sean licenciados.

xxii. Las herramientas corporativas instaladas en los dispositivos móviles institucionales serán gestionadas por la Dirección de Informática y Tecnología, con el fin de proteger la confidencialidad, integridad y disponibilidad de la información de la entidad, garantizando el cumplimiento de la política de Privacidad de la Política de Seguridad y Privacidad de la Información del presente documento, de igual manera los backup's de estos dispositivos se deberá almacenar en los repositorios de la entidad.

d. Del uso de los sistemas o herramientas de información: Todos los servidores públicos y contratistas de la Secretaría Distrital de Hacienda son responsables de la protección de la información a la que acceden y procesan, así como de evitar su pérdida, alteración, destrucción y uso indebido, para lo cual se dictan los siguientes lineamientos:

i. Se prohíbe el préstamo de las credenciales de acceso a la red y a los recursos informáticos (Usuario y Clave), entre usuarios, contratistas y particulares que ejerzan funciones públicas en la entidad.

ii. Se prohíbe el uso de usuarios genéricos, superusuarios y roles de administración sin encontrase previamente asignados y autorizados por seguridad de la información y control interno, estos roles deben estar custodiados por control interno y seguridad de la información.

iii. Todo servidor público y contratista es responsable del cambio periódico de su clave de acceso a los sistemas de información o recursos informáticos.
iv. Todo servidor público y contratista es responsable de los registros y modificaciones de información que se hagan a nombre de su cuenta de usuario.
v. En ausencia del servidor público o contratista, el acceso a la estación de trabajo será bloqueada con una solicitud a la Dirección de Informática y Tecnología, a través de la Mesa de Servicios, con el fin de evitar la exposición de la información y el acceso a terceros, que puedan generar daño, alteración o uso indebido, así como a la suplantación de identidad. La Subdirección del Talento Humano debe reportar de inmediato, cualquier tipo de novedad de servidores públicos, a su vez los supervisores de contrato deben reportar oportunamente todas las novedades del contratista.
vi. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con la Secretaría Distrital de Hacienda, suspenderá los privilegios sobre los recursos informáticos otorgados, de forma inmediata una vez surta efecto el acto administrativo se realizará la comunicación por parte de talento humano y la SAC a la Subdirección de Servicios de TIC.
vii. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución de contrato con la Secretaría Distrital de Hacienda, el jefe inmediato o supervisor es el encargado de la custodia de los recursos de información, incluyendo la cesión de derechos de propiedad intelectual, de acuerdo con la normativa vigente.
viii. Cuando un servidor público o contratista cesa sus funciones o culmina la ejecución del contrato con la Secretaría Distrital de Hacienda deberá tramitar el formato de paz y salvo a través del formato de constancia de entrega y presentarlo totalmente diligenciado ante la Subdirección del Talento Humano y para el caso de los contratistas ante el Supervisor de contrato correspondiente.
ix. Todos los servidores públicos y contratistas de la entidad deben dar estricto cumplimiento a lo estipulado en la Ley 23 de 1982 "Sobre derechos de autor", la Decisión 351 de 1993 de la Comunidad Andina de Naciones, así como cualquier otra que adicione, modifique o reglamente la materia.

Lineamientos de las Políticas de Seguridad de la Información. Todas las políticas identificadas en este documento se deberán desarrollar de manera detallada y clara en la Declaración de Aplicabilidad y en el Manual de Gestión de Seguridad de la Información.

REVISIÓN

Revisión. La Política de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Hacienda será revisada anualmente o antes, si existiesen modificaciones que así lo requieran, para que sea siempre oportuna, suficiente y eficaz. Este proceso será liderado por el Oficial de Seguridad y Privacidad de la Información o quien haga sus veces y revisado y aprobado por el Comité del Modelo Integrado de Gestión o quien haga sus veces.

CONTROL DE CAMBIOS

VERSIÓN	FECHA	DESCRIPCIÓN DE CAMBIOS
1	30/07/2014	Elaboración de la mesa técnica SGSI aprobado comité SIG de 26/04/2014.
2	26/01/2017	Actualización general, alineación a las directrices de MINTIC. Se incluye la política de tratamiento de datos personales. Aprobado por comité del 26/01/2017.
3	27/01/2022	Actualización general de la Política de Seguridad y Privacidad de
		la Información y Seguridad Digital, y se definen lineamientos frente al uso y manejo de la información y se definen las condiciones de uso de los portales web. Aprobado por comité del 04/02/2022