




**MANUAL DE POLITICAS DE SEGURIDAD DE LA  
INFORMACIÓN  
03-MN-01**

Direccionamiento TIC


17 – 09 – 2019  
Versión – 05

<b>Personería</b> de Bogotá, D. C. <hr/> Al servicio de la ciudad		<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
				<b>Versión:</b> 5	<b>Página:</b> 2 de 61
				<b>Vigente desde:</b> 17-09-2019	

CONTROL DE CAMBIOS		
VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	24-11-2015	Versión inicial del documento.
2	27-03-2017	Asociación de la documentación al nuevo mapa de procesos de la Entidad.
3	18-05-2018	Actualización de políticas y aplicación de la guía para la elaboración de documentos MIPER.
4	29-05-2019	Actualización de las políticas de acuerdo con los objetivos de control y controles del anexo A de la norma ISO 27001.
5	17-09-2019	Actualización códigos de documentos y nombre dominio.

Elaboró:	Revisó:	Aprobó:
Ing. Clara Neyra Barrios Profesional Especializado Darley Ocampo Profesional Especializado	Ing. Henry Díaz Dussán Director de TIC	Ing. Henry Díaz Dussán Director de TIC Germán Uriel Rojas Director de Planeación

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. Al servicio de la ciudad 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 3 de 61
			<b>Vigente desde:</b> 17-09-2019	

## TABLA DE CONTENIDO

<b>1. INTRODUCCIÓN .....</b>	<b>5</b>
<b>2. OBJETIVO .....</b>	<b>5</b>
<b>3. ALCANCE .....</b>	<b>6</b>
3.1. ALCANCE / APLICABILIDAD .....	6
3.2. NIVEL DE CUMPLIMIENTO .....	6
<b>4. RESPONSABLES .....</b>	<b>6</b>
4.1. RESPONSABLES DE LOS PROCESOS Y /O DIRECTORES O JEFES DE DEPENDENCIAS .....	6
4.2. DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - DTIC .....	6
4.3. DIRECCIÓN ADMINISTRATIVA Y FINANCIERA .....	7
4.4. DIRECCIÓN DE TALENTO HUMANO .....	7
4.5. FUNCIONARIOS(AS) Y CONTRATISTAS .....	7
<b>5. DEFINICIONES .....</b>	<b>8</b>
<b>6. CONSIDERACIONES GENERALES .....</b>	<b>13</b>
6.1. COMUNICACIÓN Y SOCIALIZACION DE LAS POLÍTICAS .....	14
6.2. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD .....	15
6.3. REVISIÓN DE LAS POLÍTICAS .....	15
<b>7. DESARROLLO DEL DOCUMENTO .....</b>	<b>15</b>
7.1. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN .....	15
7.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN .....	16
7.2.1. Organización interna .....	16
7.2.2. Política para dispositivos móviles .....	17
7.3. SEGURIDAD DE LOS RECURSOS HUMANOS .....	19
7.3.1. Antes de asumir el empleo .....	19
7.3.2. Durante la ejecución del empleo .....	19
7.3.3. Terminación y cambio de empleo .....	20
7.4. GESTIÓN DE ACTIVOS .....	21
7.4.1. Responsabilidad por los activos .....	21
7.4.2. Clasificación de la Información .....	22
7.4.3. Manejo de medios .....	22
7.5. CONTROL DE ACCESO .....	22
7.5.1. Política de Control de Acceso .....	22
7.5.2. Gestión de acceso de usuarios .....	24
7.5.3. Responsabilidades de los usuarios .....	24
7.5.4. Control de Acceso a Sistemas y Aplicaciones .....	25
7.6. CRIPTOGRAFÍA .....	27
7.6.1. Política sobre el uso de los controles criptográficos .....	27
7.7. SEGURIDAD FÍSICA Y DEL ENTORNO .....	28
7.7.1. Áreas seguras .....	28

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. Al servicio de la ciudad 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-MN-01</b>	
		<b>Versión:</b> 5	<b>Página:</b> 4 de 61
		<b>Vigente desde:</b> 17-09-2019	

7.7.2.	Equipos.....	28
7.7.3.	Política de escritorio y pantalla limpia.....	31
7.8.	SEGURIDAD DE LAS OPERACIONES.....	32
7.8.1.	Procedimientos operacionales y responsabilidades.....	32
7.8.2.	Protección contra Códigos Maliciosos.....	33
7.8.3.	Copias de respaldo.....	34
7.8.4.	Registro y Seguimiento.....	35
7.8.5.	Control de software operacional.....	36
7.8.6.	Gestión de Vulnerabilidad Técnica.....	36
7.9.	SEGURIDAD DE LAS COMUNICACIONES.....	37
7.9.1.	Gestión de la seguridad de las redes.....	37
7.9.2.	Políticas y procedimientos de transferencia de información.....	38
7.9.3.	Servicio de acceso a internet.....	42
7.9.4.	Política de seguridad en la nube.....	45
7.10.	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS.....	46
7.10.1.	Requisitos de seguridad de los sistemas de información.....	46
7.10.2.	Seguridad en los procesos de desarrollo y soporte.....	47
7.10.2.1.	Política de desarrollo seguro.....	47
7.11.	RELACIONES CON LOS PROVEEDORES.....	48
7.11.1.	Política de seguridad de la información para las relaciones con los Proveedores.....	48
7.11.2.	Gestión de la prestación de servicios de proveedores.....	49
7.12.	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	50
7.12.1.	Gestión de incidentes y mejoras en la seguridad de la información.....	50
7.13.	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO.....	51
7.13.1.	continuidad de seguridad de la información.....	51
7.14.	CUMPLIMIENTO.....	52
7.14.1.	Cumplimiento de requisitos legales y contractuales.....	52
7.14.2.	Revisiones de seguridad de la información.....	54
7.15.	POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES.....	54
7.15.1.	Alcance de la Política de Protección de Datos Personales.....	54
7.15.2.	Tratamiento de los datos personales por parte de la Personería de Bogotá D.C.....	55
7.15.3.	Efectos de la Autorización:.....	55
7.15.4.	Autorización.....	55
7.15.5.	Finalidades de la autorización.....	57
7.15.6.	Información personal recolectada.....	57
7.15.7.	Deberes de la Personería de Bogotá D.C. cuando actúe como responsable del tratamiento.....	57
7.15.8.	Derechos del Titular de la información personal.....	58
7.15.9.	Seguridad de la información y reserva de la información personal.....	59
7.15.10.	Tratamiento de datos personales de menores de edad.....	59
7.15.11.	Consulta, rectificación y reclamos.....	60
8.	<b>NORMATIVIDAD APLICABLE.....</b>	<b>60</b>

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 5 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 1. INTRODUCCIÓN

Consciente que la información es uno de los activos más importantes para las organizaciones y particularmente para la Personería de Bogotá D.C., en cumplimiento de su misión y sus objetivos, es indispensable establecer estrategias y mecanismos que contribuyan a la protección de la seguridad de la información institucional, independientemente del personal que interactúe con ella y del medio en que se trate, transporte o almacene.

Para ello, la Personería de Bogotá D.C., implementa el Sistema de Gestión de Seguridad de la Información – SGSI para todos los procesos de la Entidad y establece mediante el presente manual, un conjunto de políticas y lineamientos acordes a los requisitos de la norma NTC-ISO-IEC 27001 de 2013, para el uso adecuado de la información institucional y de los recursos y servicios tecnológicos que la soportan, que se constituyen en la base para el diseño y ejecución de procedimientos, protocolos, controles y en general el desarrollo de las actividades diarias de los funcionarios(as) y contratistas y personas que interactúen con la información institucional de la Personería de Bogotá D.C.

Las políticas del presente manual deben ser conocidas por todos los funcionarios(as), contratistas y personas que interactúen con la información institucional de la Personería de Bogotá D.C., y una vez publicado y difundido se constituirá en la base formal para dar cumplimiento a las normativas, lineamientos y políticas establecidas en relación al uso y seguridad la información, y su aplicación será de obligatorio cumplimiento, siendo responsabilidad de todos velar por el cumplimiento de estas políticas y directrices.

El incumplimiento de las políticas del presente manual puede constituir un riesgo para la disponibilidad, integridad y/o confidencialidad de la información institucional, por lo tanto, la Dirección de Tecnologías de Información y Comunicación - DTIC, establecerá los mecanismos que considere necesarios, para verificar su cumplimiento.

## 2. OBJETIVO

Establecer las políticas de seguridad de la información para la Personería de Bogotá D.C., con el fin de cumplir con los requisitos de seguridad, definidos en un SGSI (Sistema de Gestión de Seguridad de la Información) y el MSPI, (Modelo de Seguridad y Privacidad de la Información) de la política de Gobierno Digital, que ayudarán mediante su implementación a preservar la confidencialidad, integridad y disponibilidad de la información en la Entidad.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 6 de 61
			<b>Vigente desde:</b> 17-09-2019	

### 3. ALCANCE

#### 3.1. ALCANCE / APLICABILIDAD

Las políticas contenidas en el presente manual son de obligatorio cumplimiento para todos los directivos(as), funcionarios(as), contratistas y terceros de la Personería de Bogotá D.C., para conseguir un adecuado nivel de protección de las características de seguridad y calidad de la información relacionada.

Las políticas aplican para todas las sedes de la Personería de Bogotá D.C., personerías locales y puntos de atención con que cuente la Entidad.

#### 3.2. NIVEL DE CUMPLIMIENTO

Todas las personas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento a las políticas establecidas en el presente manual.

### 4. RESPONSABLES

#### 4.1. RESPONSABLES DE LOS PROCESOS Y /O DIRECTORES O JEFES DE DEPENDENCIAS

Informar a la Dirección de Tecnologías de Información y Comunicación DTIC las novedades de los funcionarios(as) y Contratistas, así como los permisos de las carpetas o recursos compartidos para los cuales están autorizados(as). Así mismo, deben conocer, promover y asegurar la implementación y cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo dentro de sus dependencias.

#### 4.2. DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN - DTIC

Liderar las actividades relacionadas con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información – SGSI en la Personería de Bogotá D.C., garantizando la divulgación y el seguimiento de las políticas de seguridad de la información al interior de la Entidad, estableciendo los procedimientos, lineamientos y controles que permitan su operatividad y cumplimiento.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 7 de 61
			<b>Vigente desde:</b> 17-09-2019	

#### **4.3. DIRECCIÓN ADMINISTRATIVA Y FINANCIERA**

Responsable del inventario de equipos y su actualización según se establezca en las normas vigentes y de proporcionar los suministros que permitan la operación adecuada de los sistemas de información de la Entidad por medio de los procesos contractuales necesarios tanto para la ampliación de la red como su mantenimiento. Informar a la Dirección de Tecnologías de Información y Comunicación DTIC las novedades referidas a los contratistas que en el desarrollo de sus actividades requieran acceso a información de la Entidad, relacionando claramente los datos de los usuarios entrantes y salientes.

#### **4.4. DIRECCIÓN DE TALENTO HUMANO**


Informar a la Dirección de Tecnologías de Información y Comunicación DTIC toda novedad de personal mediante el formato establecido.

#### **4.5. FUNCIONARIOS(AS) Y CONTRATISTAS**

Conocer y aplicar los procedimientos de seguridad de la información vigentes so pena de incurrir en faltas disciplinarias y/o contractuales.

Reportar oportunamente las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento y resguardar el acceso a los recursos informáticos asignados, mediante la utilización de contraseñas seguras; para tal fin debe concluir las sesiones activas al finalizar las tareas, y/o dejar los equipos bloqueados al retirarse del puesto de trabajo así sea temporalmente.

Asumir la responsabilidad por el manejo del espacio en disco en su equipo de trabajo, realizando revisiones periódicas y eliminación de archivos no necesarios.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 8 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 5. DEFINICIONES

**Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elementos relacionados con el tratamiento de la misma (sistemas, soportes, edificios, personas) que tenga valor para la organización<sup>1</sup>.

**Activo de información:** En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.<sup>2</sup>

**Acuerdo de Nivel de Servicio:** Un Acuerdo de Nivel de Servicio (ANS) es un convenio entre un proveedor de servicios de TI y un cliente. Describe las características del servicio de TI, los niveles de cumplimiento y las sanciones, y especifica las responsabilidades del proveedor y del cliente. Un ANS puede cubrir múltiples servicios de TI o múltiples clientes.

**Aplicaciones o aplicativos:** Las aplicaciones son herramientas informáticas que permiten a los usuarios comunicarse, realizar trámites, entretenerse, orientarse, aprender, trabajar, informarse y realizar una serie de tareas de manera práctica y desde distintos tipos de terminales como computadores tabletas o celulares<sup>3</sup>.

**Autenticación:** Proceso utilizado entre un emisor y un receptor, con el fin de asegurar la integridad de los datos y proporcionar la autenticidad de los datos originales<sup>4</sup>.

**Autorización:** Consentimiento expreso e informado del titular para llevar a cabo el tratamiento de datos personales.

**Backup:** Operación que consiste en duplicar y asegurar datos e información contenida en un sistema informático. Es una copia de seguridad.

**Base de datos:** Todo conjunto organizado de datos Personales que sea objeto de Tratamiento.

<sup>1</sup> Definition ISO 27000:2009. Overview and Vocabulary. Traducción del autor Eddy Pérez – UNEG 2006

<sup>2</sup> <http://www.microsoft.com/spain/technet/recursos/articulos/srsgch01.msp>

<sup>3</sup> <http://www.mintic.gov.co/portal/vivedigital/612/w3-channel.html>

<sup>4</sup> Norma Técnica Colombiana, NTC-ISO 3270

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código:</b> 03-MN-01
			<b>Versión:</b> 5 <b>Página:</b> 9 de 61
	<b>Vigente desde:</b> 17-09-2019		

**Contenido:** Todo tipo de información o dato que se divulga en la intranet y/o página web, entre los que se encuentran: textos, imágenes, fotos, logos, diseños y animaciones<sup>5</sup>.

**Clave de autenticación o Contraseñas:** Clave criptográfica utilizada para la autenticación de usuario y que se utiliza para acceder a los recursos informáticos.

**Copyright:** Derecho exclusivo de un autor o editor a explotar una obra física o digital, literaria, científica o artística.

**Cloud Computing:** Es un nuevo concepto tecnológico que se basa en que las aplicaciones software y los equipos hardware con capacidad de proceso y almacenaje de datos que están ubicados en un Datacenter que permite a los usuarios acceder a las aplicaciones y servicios disponibles a través de Internet o como se conoce coloquialmente a través “la Nube” de Internet, de una forma sencilla y cómoda.

**Clúster:** Conjunto de servidores que trabajan como una única máquina mejorando el desempeño de las transacciones y operaciones implantadas en este sistema.

**CPD:** Centros de Procesamiento de Datos, ubicación física donde se concentran todos los equipos electrónicos necesarios para el procesamiento de la información de una organización.

**CRM:** “Customer Retationship Management”. Gestión de la Relación con el Cliente, son herramientas informáticas dedicadas a la gestión integrada de información sobre clientes. Estas aplicaciones permiten, desde almacenar y organizar esta información, hasta integrar, procesar y analizar la misma.

**Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables (en adelante “Datos Personales” o “Información Personal”).

**Datos sensibles:** Se entiende como datos sensibles aquellos que afecten la intimidad del titular o cuyo uso indebido pueda afectar la intimidad del titular o la potencialidad de generar su discriminación.

<sup>5</sup> <http://www.personeriabogota.gov.co/POLÍTICAS-de-privacidad-y-condiciones-de-uso>

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código:</b> 03-MN-01
			<b>Versión:</b> 5 <b>Página:</b> 10 de 61
	<b>Vigente desde:</b> 17-09-2019		

**Datos públicos:** Aquellos datos que no sean semiprivados, privados o sensibles. Son considerados datos públicos, entre otros, los datos relativos al estado civil de la personas, a su profesión u oficio y a su calidad de comerciante o servidor público.

**Dato semiprivado:** Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general.

**Dato privado:** Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.

**Dominio:** Es un conjunto de computadores, conectados en una red, que confían a uno de los equipos de dicha red la administración de los usuarios y los privilegios que cada uno de los usuarios tiene en la red. Es la parte principal de una dirección en la Web, que usualmente indica la organización o compañía que administra dicha página (personeriabogota.gov.co).

**DVR:** (Digital Video Recorder), grabador de cámaras análogas, digitaliza, graba y administra imágenes enviadas desde cámaras de seguridad analógicas.

**Dirección IP:** La dirección IP (IP es un acrónimo para Internet Protocol) es un número único e irrepetible con el cual se identifica una computadora conectada a una red que corre el protocolo IP.

**Encargado(a) del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

**Intranet:** Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

**Información personal:** Es aquella suministrada por el usuario o el visitante para el registro o consulta de información, la cual incluye datos como nombre, identificación, edad, género, dirección, correo electrónico y teléfono, entre otros<sup>6</sup>.

<sup>6</sup> <http://www.personeriabogota.gov.co/POLÍTICAS-de-privacidad-y-condiciones-de-uso>

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 11 de 61
			<b>Vigente desde:</b> 17-09-2019	

**Internet:** Herramienta de comunicación con decenas de miles de redes de computadoras unidas por el protocolo TCP/IP.

**Integridad:** Propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]

**Intranet:** Es una red de ordenadores privados que utiliza tecnología Internet para compartir, dentro de una organización, parte de sus sistemas de información y sistemas operacionales.

**Log:** Uno o más ficheros de texto automáticamente creados y administrados por un servidor, en donde se almacena toda la actividad que se hace sobre éste<sup>7</sup>.

**Medios de almacenamiento físico:** Se considera como medio de almacenamiento físico las cintas, los disco extraíbles, los DCs y los DVDs entre otros.

**Nombres de Grupos:** Seudónimos utilizados para la clasificación de conjuntos de computadoras dentro del dominio.

**NVR:** (Network Video Recorder), grabador de cámaras IP, graba y administra imágenes ya digitales las cuales son enviadas desde las cámaras IP a través de una red.

**Portal web:** Es un sitio compuesto por varias páginas web, el cual, permite a las personas el fácil acceso a diferentes recursos y servicios en línea que tiene la Entidad. El portal web de la Personería de Bogotá D.C., se encuentra en la dirección **URL: <http://www.personeriabogota.gov.co>**.

**Portal intranet:** Es un sitio compuesto por varias páginas web, el cual, permite a los funcionarios(as) y contratistas de la Entidad el fácil acceso a diferentes recursos y servicios en línea que tiene la Entidad. El portal intranet de la Personería de Bogotá D.C., se encuentra en la dirección **URL: <http://intranet.personeriabogota.gov.co>**.

**Publicar:** Es la acción de hacer visible un contenido o documento desde un portal o sitio web.

<sup>7</sup> <http://www.alegsa.com.ar/Dic/log%20de%20accesos.php>

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 12 de 61
			<b>Vigente desde:</b> 17-09-2019	

**Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.

**Seguridad de la información:** Preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad, no repudio y fiabilidad<sup>8</sup>. [NTC-ISO/IEC 17799:2006]

**Servicio al ciudadano:** Es la asistencia, orientación o intervención que actualmente suministra la Personería de Bogotá D.C., en línea o que proveerá en el futuro, por medio de su portal, como publicación de información, registro, certificados, asistencia, noticias, entre otros.

**Servicio de TI:** Un servicio de tecnologías de la información es un conjunto de productos (Bienes o servicios) que buscan solucionar las necesidades de los clientes de una organización a través del uso de elementos tecnológicos o informáticos.

**Servidor:** Computadora central en un sistema de red que provee servicios a otras computadoras.<sup>9</sup>

**Sistema Informático o de Información:** Se entenderá todo sistema utilizado para generar, enviar, recibir, archivar o procesar de alguna forma mensajes de datos<sup>10</sup>.

**Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, incluyendo, pero sin limitar, la recolección, almacenamiento, uso, circulación o supresión.

**Titular:** Persona natural cuyos datos personales sean objeto de tratamiento.

**Transmisión de datos:** tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia, cuando tenga por objeto la realización de un tratamiento por el encargado o por cuenta del responsable.

<sup>8</sup> Norma Técnica Colombiana, NTC-ISO 27001

<sup>9</sup> <http://www.alegsa.com.ar/Dic/servidor.php#sthash.KgzZbmFA.dpuf>

<sup>10</sup> 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, y se establecen las Entidades de certificación y se dictan otras disposiciones"

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 13 de 61
			<b>Vigente desde:</b> 17-09-2019	

**Transferencia de datos:** La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

**Usuario:** Es un individuo que utiliza una computadora, sistema operativo, servicio o cualquier sistema informático. Por lo general es una única persona<sup>11</sup>. Se autentica e ingresa a los sistemas y sus servicios mediante un nombre de usuario (cuenta) y una contraseña de autenticación.

**VPN:** Red privada virtual, por sus siglas en inglés (Virtual Private Network), es un tipo de tecnología de red utilizada para interconectar de forma segura un computador o dispositivo de red a una red local o privada a través de una red pública como internet.

## 6. CONSIDERACIONES GENERALES

La Dirección de Tecnologías de Información y Comunicación - DTIC de la Personería de Bogotá D.C., entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información - SGSI, buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado y las personas, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Entidad.

Por lo anterior, este Manual de Políticas aplica a toda la Entidad según lo establecido en el alcance, sus funcionarios(as), contratistas y terceros de la Personería de Bogotá D.C, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del Sistema de Gestión de Seguridad de la Información - SGSI estarán determinados por las siguientes premisas:

- Identificar e implementar mecanismos para lograr el cumplimiento de la normatividad en materia de seguridad de la información
- Desarrollar las actividades necesarias para lograr la continuidad y disponibilidad de los sistemas de información de la Personería de Bogotá D.C.

<sup>11</sup> <http://www.alegsa.com.ar/Dic/usuario.php#sthash.AlfaNyCl.dpuf>

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 14 de 61
			<b>Vigente desde:</b> 17-09-2019	


- Fortalecer la cultura de seguridad de la información en los(as) funcionarios(as), terceros(as), contratistas de la Personería de Bogotá D.C. y las personas, a través de la capacitación y sensibilización en el SGSI.
- Realizar una adecuada gestión de riesgos de seguridad de la información Implementando controles que contribuyan a mitigar su probabilidad de materialización.
- Implementar mecanismos que fomenten la transparencia en el acceso a la información, mediante procesos de clasificación y control de acceso a la información.
- Fortalecer y mantener los niveles de confianza de las personas en los procedimientos y servicios que presta la Personería de Bogotá D.C.
- Gestionar de manera adecuada los incidentes de seguridad de la información, generando, documentando y aplicando lecciones aprendidas con el fin de reducir la posibilidad de ocurrencia y/o el impacto de incidentes futuros.
- Mejorar continuamente el desempeño del SGSI, mediante la implementación de acciones correctivas y de mejora que se generen como resultado de las auditorías internas y externas y las revisiones de seguridad de la información.
- La Personería de Bogotá D.C., ha decidido implementa un Sistema de Gestión de Seguridad de la Información - SGSI, soportado en lineamientos claros alineados a las necesidades del negocio y a los requerimientos legales vigentes.

## 6.1. COMUNICACIÓN Y SOCIALIZACION DE LAS POLÍTICAS

Todo funcionario(a) o contratista que ingrese a la Personería de Bogotá D.C., deberá recibir capacitación sobre las políticas establecidas en el presente manual en el momento de su inducción.

La Dirección de Talento Humano remitirá con la debida anticipación a la Dirección de Tecnologías de Información y Comunicación - DTIC, la información de fecha, hora y lugar de las jornadas de inducción.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 15 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 6.2. INCUMPLIMIENTO DE LAS POLÍTICAS DE SEGURIDAD

El incumplimiento de las políticas establecidas en el presente manual, podrá acarrear sanciones disciplinarias, civiles o penales según sea el caso.

## 6.3. REVISIÓN DE LAS POLÍTICAS

El Manual de Políticas de Seguridad de la Información es revisado anualmente o antes de ser necesario, con el fin de mantenerlo actualizado y acorde a los cambios en la infraestructura tecnológica, los procedimientos y servicios que involucran el manejo de la información institucional.

# 7. DESARROLLO DEL DOCUMENTO

## 7.1. POLÍTICA GENERAL DE LA SEGURIDAD DE LA INFORMACIÓN

La Personería de Bogotá D.C., en ejercicio de sus funciones constitucionales, es consciente y reconoce la importancia de preservar la seguridad de la información, la cual se define como el conjunto de medidas adoptadas por una organización, que permiten resguardar y proteger la información para garantizar la confidencialidad, disponibilidad e integridad de la misma, y que constituye factor fundamental para el cumplimiento de su Misión, Visión y Objetivos Estratégicos.

Por tal razón, la Alta Dirección de la Personería de Bogotá D.C., se compromete en todos sus niveles institucionales con la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información y con el cumplimiento de los requisitos aplicables en la materia, adoptando las buenas prácticas de gestión y administración de las tecnologías de la información; de esta manera generará un marco de confianza en el desarrollo de sus obligaciones con el Estado y las personas, junto con el cumplimiento de los requisitos legales y contractuales que le aplican.

La Personería de Bogotá D.C., define los objetivos de seguridad de la información, los cuales se encuentran alineados con los objetivos estratégicos de la Entidad, se apoya en la identificación periódica de las amenazas y vulnerabilidades que signifiquen un riesgo para los principios de la seguridad de la información y en el análisis, valoración y tratamiento de los riesgos que puedan afectar el cumplimiento de los objetivos institucionales.

La presente política aplicará para todos(as) los(as) servidores(as) públicos(as), funcionarios(as), contratistas, proveedores y demás partes interesadas, así como los activos que se encuentran incluidos en el alcance del SGSI.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 16 de 61
			<b>Vigente desde:</b> 17-09-2019	

Todas las personas naturales y jurídicas cubiertas por el alcance y aplicabilidad deberán dar cumplimiento de la política.

La presente política es comunicada y socializada al interior de la Personería de Bogotá D.C., y las partes interesadas a través de los canales de comunicación de la Entidad; está disponible para su consulta cumpliendo con los parámetros de documentación establecidos en el Modelo Integrado de Gestión - MIPG y el Sistema de Gestión de Calidad – SGC, y su incumplimiento, traerá consigo, las consecuencias legales que apliquen a la normativa de la Entidad, incluyendo lo establecido en las normas que competen al Gobierno nacional y territorial en cuanto a Seguridad y Privacidad de la Información se refiere.

## 7.2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

### 7.2.1. Organización interna

#### Lineamientos generales

- La personería de Bogotá D.C., establece el responsable del Sistema de Gestión de Seguridad de la Información – SGSI.
- Los responsables de los procesos y/o supervisores del contrato definirán los roles de usuario que estimen pertinentes en cada uno de sus equipos de trabajo y los niveles de operación siguiendo lo establecido en el procedimiento “*Gestión de usuarios*” Código: 03-PT-01.
- Los roles asociados a cada servicio o sistema de información serán identificados y clasificados por su tipo y uso teniendo como base los siguientes criterios:

Tipo	Rol	Criterios
Internos	Grupo Core IT	Aquellos usuarios que por su función tecnológica y de investigación, gestión y apoyo tienen acceso ilimitado a los servicios y que requieren operar en aspectos técnicos y tecnológicos, instalación, configuración, decisión, administración de servicios y atención al usuario final en procesos, capacitación y procedimientos de sistemas.
	Grupo VIP	Directivos, Asesores, Coordinadores, jefes de área, Oficina de comunicaciones y Funcionarios(as) que por su gestión requieren el acceso especial o privilegiado a recursos tecnológicos y servicios especiales.
	Funcionario(a) y contratista Activo(a)	Todos aquellos usuarios que requieren acceso a la red de datos y comunicaciones, aplicaciones y servicios de TI en general, de acuerdo con las funciones propias del cargo y los niveles de servicio asociados

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 17 de 61
			<b>Vigente desde:</b> 17-09-2019	

Tipo	Rol	Criterios
<b>Externos</b>	Ciudadanos	Personas o terceros con acceso a los servicios de TI, mediante el uso herramientas tecnológicas y/o sistemas de información diseñados especialmente para satisfacer los requerimientos ciudadanos, proveer servicios en pro del cumplimiento de las funciones propias de la Entidad.

- La Dirección de Tecnologías de Información y Comunicación - DTIC, identificará las autoridades competentes a quienes podrá contactar en caso de presentarse algún incidente de seguridad de la información que amerite su intervención; de igual manera establecerá contacto con grupos de interés especializados en seguridad de la información, que puedan contribuir a la gestión de la seguridad de la información en la Personería de Bogotá D.C.
- Para los proyectos desarrollados por la Personería de Bogotá D.C., se deben tener en cuenta las políticas del presente manual, y en todo caso considerar los asuntos relacionados con la seguridad de la información mediante la identificación y tratamiento de riesgos asociados a la información de los proyectos.
- La planeación estratégica de la Dirección de Tecnologías de Información y Comunicación - DTIC, estará alineada con la planeación estratégica institucional y acorde con los objetivos estratégicos y la asignación de recursos. Para ello, se trabaja articuladamente con los demás procesos y de acuerdo a la normatividad legal vigente.
- Para el desarrollo de proyectos que requieran el uso de componentes tecnológicos, los procesos contarán con el apoyo de la Dirección de Tecnologías de Información y Comunicación - DTIC.
- Todos los requerimientos de equipos informáticos, sistemas de información y aplicativos o servicios de software, serán solicitados a la Dirección de Tecnologías de Información y Comunicación - DTIC, quien realizará el análisis pertinente para determinar su viabilidad técnica.

### 7.2.2. Política para dispositivos móviles

La Dirección de Tecnologías de Información y Comunicación - DTIC, es la responsable de establecer las condiciones necesarias para el acceso a los recursos de y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, smartphones, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes). La autorización de conexión de dispositivos móviles a las redes de datos de la Entidad se realiza

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 18 de 61
			<b>Vigente desde:</b> 17-09-2019	


una vez se identifican, gestionan y mitigan los riesgos de seguridad de la información asociados al uso de los dispositivos.

La presente política y controles aplican a todos los dispositivos y equipos móviles de los funcionarios(as), contratistas y terceros, que estén autorizados para conectarse a las redes de datos y comunicaciones de la Entidad, a la información institucional o a cualquier servicio de tecnologías de la información y comunicación de la Personería de Bogotá D.C.

### **Lineamientos generales**

- La Dirección de Tecnologías de Información y Comunicación - DTIC adopta e implementa los mecanismos de seguridad necesarios para salvaguardar la información contenida y transmitida mediante el uso de dispositivos móviles de los funcionarios(as), contratistas y terceros de la Personería de Bogotá D.C., a través de los cuales se les autoriza el acceso a los recursos tecnológicos de la Entidad.
- Los dispositivos móviles solo tienen acceso a la información autorizada por parte de los responsables de los diferentes procesos de la Personería de Bogotá D.C.
- Los usuarios deben proteger física y lógicamente los dispositivos móviles asignados y que son propiedad de la Personería de Bogotá D.C., para prevenir el hurto, acceso o divulgación no autorizada de la información institucional.
- En caso de pérdida o hurto de un dispositivo móvil de propiedad de la Personería de Bogotá D.C., el funcionario(a), contratista o tercero a quien se le haya asignado el dispositivo, será el responsable de informar de manera inmediata a la Personería de Bogotá D.C., a través de la Dirección de Tecnologías de Información y Comunicación - DTIC.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, está autorizada para realizar la desactivación, borrado y retiro de los accesos de los dispositivos móviles a los sistemas de información de la Entidad y demás servicios de TI, cuando el dispositivo móvil haya sido extraviado, hurtado o haya sido comprometida su seguridad.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 19 de 61
			<b>Vigente desde:</b> 17-09-2019	

### 7.3. SEGURIDAD DE LOS RECURSOS HUMANOS

#### 7.3.1. Antes de asumir el empleo

##### Lineamientos generales

- La Dirección de Talento Humano de la Personería de Bogotá D.C., realizará las actividades necesarias para la selección de personal, asegurando la verificación de los requisitos mínimos para proveer los cargos y el cumplimiento de la normatividad vigente.
- Para el ingreso de nuevo personal de planta y la suscripción de contratos o convenios relacionados con servicios de tecnología y/o acceso a información institucional, se debe garantizar que la persona acepte y firme una cláusula donde de conocimiento de las políticas de seguridad de la información y acuerde mantener la confidencialidad de la información, con la suscripción de un acuerdo o compromiso de confidencialidad; este acuerdo se hará extensivo a todos los colaboradores de los Contratistas o terceros para el caso de contratos o convenios.

#### 7.3.2. Durante la ejecución del empleo

##### Lineamientos generales

- La Dirección de Talento Humano es la responsable de Informar a la Dirección de Tecnologías de Información y Comunicación - DTIC, toda novedad de personal mediante el formato establecido.
- La Dirección Administrativa y Financiera, será la responsable de Informar a la Dirección de Tecnologías de Información y Comunicación - DTIC, las novedades de los Contratistas, relacionando claramente en el formato establecido.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, será responsable de la divulgación y el seguimiento de las políticas de seguridad de la información al interior de la Entidad, estableciendo los procedimientos que permitan su operatividad y cumplimiento.
- Los funcionarios(as) y Contratistas de la Personería de Bogotá D.C., deben conocer y aplicar los procedimientos de seguridad de la información vigentes

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 20 de 61
			<b>Vigente desde:</b> 17-09-2019	

so pena de incurrir en faltas disciplinarias y/o contractuales; de igual manera deben reportar oportunamente las debilidades e incidentes de seguridad que detecten o que sean de su conocimiento y resguardar el acceso a los recursos informáticos asignados.

- Los responsables de los procesos y jefes de dependencias deben Informar a la Dirección de Tecnologías de Información y Comunicación - DTIC de los permisos a las carpetas o recursos compartidos de los funcionarios(as) y contratistas para los cuales están autorizados(as); así mismo, deben conocer y asegurar la implementación y cumplimiento de las políticas de seguridad de la información por parte de su equipo de trabajo dentro de sus dependencias.
- Todos los funcionarios(as) o contratistas de la Personería de Bogotá D.C., deben recibir inducción en donde se forme, sensibilice y se den a conocer las políticas del presente manual, procedimientos y las obligaciones frente al Sistema de Gestión de Seguridad de la Información - SGSI; de igual manera, la Entidad deberá mantener informado a todo el personal sobre los cambios y actualizaciones realizadas a las políticas, procedimientos y al SGSI en general.
- La inducción referida al uso de las herramientas tecnológicas será impartida por la Dirección de Tecnologías de Información y Comunicación - DTIC, previa concertación de hora y lugar con la Dirección de Talento Humano, quien remitirá la relación de aquellos usuarios que recibirán la inducción.
- La Personera(o) Distrital, el Personero(a) Auxiliar, los Personeros(as) delegados(as) para las Coordinaciones, los Personeros(as) delegados(as), los Directores(as) y Subdirectores(as), así como los Jefes de Oficina, son responsables de conocer y asegurar la implementación de las políticas de seguridad informática, dentro de sus dependencias, así como del cumplimiento de las políticas por parte de su equipo de trabajo.

### **7.3.3. Terminación y cambio de empleo**

#### **Lineamientos generales**

- Los directores de los procesos y Supervisores de contratistas serán responsables de custodiar la información institucional a cargo de funcionarios(as) y/o contratistas cuando se produzca el retiro o suspensión de personal o terminación o cesión de los contratos.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 21 de 61
			<b>Vigente desde:</b> 17-09-2019	

- La Dirección de Talento Humano es la responsable de Informar a la Dirección de Tecnologías de Información y Comunicación - DTIC, toda novedad de retiro del personal mediante el formato establecido.
- La Dirección Administrativa y Financiera, será la responsable de Informar a la Dirección de Tecnologías de Información y Comunicación – DTIC, las novedades de retiro los Contratistas, relacionando claramente en el formato establecido.

## 7.4. GESTIÓN DE ACTIVOS

### 7.4.1. Responsabilidad por los activos

#### Lineamientos generales

- Todos los activos asociados a la información. institucional, serán identificados, clasificados y valorados, de acuerdo a lo establecido en las tablas de retención documental vigentes y a una metodología de gestión de activos formalmente adoptada.
- Todos los activos de información de la Personería de Bogotá D.C., tendrán un responsable y serán inventariados de acuerdo con la normatividad aplicable para la Entidad.
- Todo funcionario(a), contratista o tercero que haga uso de los recursos y sistemas de información de la Personería de Bogotá D.C., debe tener acceso únicamente a la información necesaria para el desempeño de las actividades que le han sido autorizadas.
- Todo funcionario(a) o contratista deberá devolver los activos informáticos a su cargo, por motivo de retiro definitivo, cambio de puesto de trabajo, suspensión y/o finalización del contrato, haciendo entrega formal del equipo a su cargo y las claves de acceso.
- Todos(as) los funcionarios(as) y contratistas de la Personería de Bogotá D.C., deben reportar sin demoras injustificadas a los responsables de sus dependencias o procesos o a la Dirección de Tecnologías de Información y Comunicación - DTIC, cualquier evento que pueda afectar la integridad, disponibilidad o confidencialidad de los activos de información de la Entidad.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 22 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 7.4.2. Clasificación de la Información

### Lineamientos generales

- La información resultante de los procesos misionales y de apoyo de la Entidad se tratará conforme a los lineamientos y parámetros establecidos en el 12-MN-01 Manual de Gestión Documental.
- Toda la información institucional debe ser identificada, clasificada y documentada de acuerdo con la Guía de Clasificación de la Información o procedimiento formalmente establecido por la Entidad y las normas vigentes.

## 7.4.3. Manejo de medios

### Lineamientos generales

- Se deben implementar acciones, protocolos o procedimientos para el uso y administración de medios informáticos removibles.
- Se deben adoptar procedimientos o mecanismos de eliminación o borrado seguro de la información institucional alojada en cualquier medio extraíble, que ha de ser retirado o reutilizado en la Entidad.
- Los medios removibles que contengan información institucional se deben almacenar en un ambiente seguro y protegido contra el acceso no autorizado y de acuerdo con las especificaciones de los fabricantes o proveedores.
- Todo medio extraíble que vaya a ser utilizado en los equipos de cómputo de la Personería de Bogotá D.C., debe ser analizados con la herramienta de antivirus de la Entidad, para el efecto, se debe tener habilitada la opción de escaneo automático de virus.

## 7.5. CONTROL DE ACCESO

### 7.5.1. Política de Control de Acceso

El Sistema de Gestión de Seguridad de la Información SGSI de la Personería de Bogotá D.C., busca reducir los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de los activos de información de la Entidad que se encuentran a cargo de sus funcionarios(as), contratistas o terceros, para lograr este objetivo se establecen controles que permitan regular el acceso a las redes,

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 23 de 61
			<b>Vigente desde:</b> 17-09-2019	

datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente aquellas clasificadas como áreas de trabajo seguras, como los centros de procesamiento de datos, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado y otras áreas esenciales para el cumplimiento de las funciones misionales de la Entidad.

La Personería de Bogotá D.C., lleva a cabo el control de acceso a la información permitiendo mantener la trazabilidad de las acciones realizadas, identificando entre otros datos relevantes, quién realiza el acceso, las operaciones ejecutadas, fecha, hora, lugar, cantidad de intentos de acceso y accesos denegados.

### **Lineamientos generales**

- El acceso a la red de la Personería de Bogotá D.C., está controlado mediante un dispositivo de seguridad perimetral Firewall, que permite la segregación de redes y el manejo de políticas de acceso a cada una de ellas. La modificación de estas reglas establecidas en el Firewall debe ser aprobada por el personal responsable en la Dirección de Tecnologías de Información y Comunicación – DTIC.
- Los(as) funcionarios(as) y contratistas que tengan acceso a la información institucional, no deben realizar modificaciones sobre ella, sin la debida autorización, y en todo caso, deberán guardar la confidencialidad de la información a la cual tiene acceso.
- Está expresamente prohibido vulnerar los controles de seguridad establecidos por la Dirección de Tecnologías de Información y Comunicación – DTIC; la violación de esta política podrá acarrear consecuencias disciplinarias, civiles y penales según el caso.
- La Dirección de Tecnologías de Información y Comunicación – DTIC, debe asegurar que las redes inalámbricas cuenten con mecanismos de autenticación que evite los accesos no autorizados.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 24 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 7.5.2. Gestión de acceso de usuarios

### Lineamientos generales

- Todos los usuarios de la Personería de Bogotá D.C., tendrán un identificador de red único (ID del usuario) para su uso personal que les permita validar los accesos y verificar su buen uso.
- Los responsables de los activos de información deberán realizar revisiones periódicas de los derechos de acceso de los usuarios autorizados a los sistemas de información a intervalos regulares con el fin de cancelar las cuentas redundantes o inactivas.
- La creación del registro de usuarios para otorgar y revocar el acceso a los sistemas de información, bases de datos y servicios de TI, debe hacerse de acuerdo con lo establecido en el procedimiento “*Gestión de usuarios*” Código 03-PT-01; para la creación o definición del usuario en red se debe seguir las siguientes especificaciones:
  - Primera letra del nombre.
  - Primera letra del segundo nombre, de no tener segundo nombre se continuará con el siguiente ítem.
  - Primer apellido.
  - De coincidir con otro login o identificador de usuario, se agrega la primera letra inicial del segundo apellido.
- La Dirección de Tecnologías de Información y Comunicación – DTIC debe asegurarse, que los usuarios o perfiles de usuario que tienen asignados por defecto los diferentes recursos y/o equipos de la plataforma tecnológica, sean inhabilitados o eliminados.

## 7.5.3. Responsabilidades de los usuarios

### Lineamientos generales

- Todos los usuarios serán responsables de las actuaciones realizadas con su usuario de red y credenciales (usuario y contraseña) asignadas para el uso de los sistemas de información y demás recursos a los cuales se les proporcione acceso.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 25 de 61
			<b>Vigente desde:</b> 17-09-2019	


- Las contraseñas de red son secretas y bajo ninguna circunstancia deben ser compartidas o reveladas a otra persona.
- Los usuarios a los cuales se les otorgue acceso a la red de datos y comunicaciones, sistemas de información y demás servicios de TI que hacen parte de la plataforma tecnológica de la Personería de Bogotá D.D., deben acogerse y acatar las políticas y directrices establecidas por la Entidad para la gestión de contraseñas.
- Los funcionarios(as), contratistas y terceros que tengan acceso a la información de la Personería de Bogotá D.C., no deben realizar modificaciones sobre la información sin la debida autorización, guardar la confidencialidad de la información a la cual tiene acceso y no vulnerar los controles de seguridad establecidos por la Dirección de Tecnologías de Información y Comunicación - DTIC.

#### **7.5.4. Control de Acceso a Sistemas y Aplicaciones**

##### **Lineamientos generales**

- Todos los usuarios a quienes se les autorice el ingreso a los sistemas y aplicaciones de TI, deberán contar con un identificador único (usuario y contraseña), el cual será personal e intransferible.
- El acceso a los sistemas de información y demás recursos de TI de la Personería de Bogotá D.C., será proporcionado por el funcionario responsable de su protección y salvaguarda. La Personería de Bogotá D.C., cuenta con el procedimiento “*Gestión de usuarios*”, Código: 03-PT-01 para tramitar el acceso a la información y sus sistemas de información.
- Se garantizará que los usuarios cambien las contraseñas que les han sido asignadas la primera vez que ingresan al sistema.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, debe asegurarse de identificar al usuario cuando solicita restablecer la contraseña por olvido o bloqueo, para lo cual asignará una contraseña temporal que debe ser cambiada por el usuario una vez ingrese al sistema.
- Las contraseñas establecidas deben ser fuertes, no repetibles en un periodo de tiempo o en cambios anteriores, deben tener una longitud no menor a 8

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 26 de 61
			<b>Vigente desde:</b> 17-09-2019	

caracteres y no deben contener palabras que se asocien a la vida personal de los usuarios (número de cédula, fechas de nacimiento, nombre de los hijos, etc.).

- Las cuentas de red se bloquearán después de tres (3) intentos fallidos con desbloqueo automático a los quince (15) minutos, además el sistema solicitará cambio de clave después de cumplido un periodo de tiempo de noventa (90) días calendario.
- Si se sospecha que las contraseñas han sido empleadas por otras personas, se deben cambiar de inmediato.
- Las contraseñas no deben escribirse ni dejarse en lugares visibles a los demás usuarios o donde personas no autorizadas puedan tener acceso.
- Las contraseñas de administración de servicios (aplicaciones, bases de datos, dispositivos, servidores, controles de acceso, programas especiales y gestores, etc.), deben ser guardadas en documento digital, cifrado y con restricción de clave segura, que solamente podrá ser conocida por el Director de Tecnologías de la Información y Comunicación - DTIC, y solo será entregada en momentos de aplicación de las contingencias o para propósitos específicos de instalación y configuración a los coordinadores de los grupos de TI cuando lo requieran.
- Las contraseñas de administración deben ser cambiadas cuando se haga uso de estas de manera regular y deben cumplir con todos los demás lineamientos generales de políticas de contraseñas establecidos en este documento.
- La eliminación, reasignación o bloqueo de los privilegios de acceso otorgados sobre los recursos tecnológicos, los servicios de red, los sistemas de información y bases de datos, de manera oportuna, cuando los funcionarios(as) y contratistas se desvinculan, toman licencias, vacaciones, son trasladados o cambian de cargo, se realizarán con las novedades enviadas a La Dirección de Tecnologías de Información y Comunicación - DTIC por parte de la Dirección de Talento Humano y la Subdirección de Contratación en el formato establecido o por solicitud del jefe inmediato o supervisor del contrato por medio de la mesa de ayuda.
- La contraseña de administrador local de las estaciones de trabajo nunca caduca, esta contraseña es general para todas las estaciones de trabajo y se usará exclusivamente para efectos de soporte técnico por parte del equipo

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 27 de 61
			<b>Vigente desde:</b> 17-09-2019	

autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC., bajo ninguna circunstancia esta contraseña será revelada a los usuarios no autorizados.

- Se prohíbe el uso de software o programas utilitarios que puedan violar o evadir los controles de seguridad para el acceso seguro a los sistemas y aplicaciones.
- La Dirección de Tecnologías de Información y Comunicación - DTIC implementa las medidas necesarias para limitar el acceso al código fuente de los sistemas de información y/o aplicativos de la Personería de Bogotá D.C.
- Solo se permitirá el acceso al código fuente de los sistemas de información y/o aplicativos de la Personería de Bogotá D.C., al personal autorizado del Grupo de Sistemas de información de la Dirección de Tecnologías de Información y Comunicación - DTIC.

## 7.6. CRIPTOGRAFÍA

### 7.6.1. Política sobre el uso de los controles criptográficos

La Dirección de Tecnologías de Información y Comunicación - DTIC es la encargada de definir los mecanismos de cifrado de información más apropiados frente a las necesidades de la Personería de Bogotá D.C., con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información de la Entidad, adopta los controles de cifrado de datos que reduzcan los riesgos de seguridad de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios(as) y contratistas de la Personería de Bogotá D.C.

#### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC, suministrará las herramientas necesarias para garantizar el cifrado y envío seguro de la información confidencial, sensible, o reservada que será almacenada y/o transmitida al interior o exterior de la Entidad.
- Toda información sensible, confidencial o reservada que se transmita al interior o fuera de la Entidad debe ser encriptada y protegida con una contraseña segura, antes de enviarla al destinatario.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	<b>Código: 03-MN-01</b>	
		<b>Versión:</b> 5	<b>Página:</b> 28 de 61
		<b>Vigente desde:</b> 17-09-2019	

- La contraseña de encriptación debe ser compartida con el destinatario por un medio diferente al del envío de la información.

## 7.7. SEGURIDAD FÍSICA Y DEL ENTORNO

### 7.7.1. Áreas seguras

#### Lineamientos generales


- Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos de comunicaciones y seguridad perimetral y demás infraestructura de TI, serán consideradas como áreas seguras y de acceso restringido para personal no autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC.
- No se permite fumar, ni el ingreso o consumo de alimentos o bebidas en las instalaciones de centros de cómputo y/o de cableado.
- En las dependencias donde se gestione, almacene y procese información de la Personería de Bogotá D.C., deben implementarse controles de acceso seguro, con el fin de prevenir accesos no autorizados, adulteración, pérdida, consulta, daños e interferencia en el funcionamiento de los aplicativos e información de la Entidad.
- Las puertas de acceso a las oficinas e instalaciones de la Personería de Bogotá D.C., deben permanecer cerradas y aseguradas, con el fin de prevenir el acceso de personal no autorizado.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, monitorea periódicamente la temperatura de los espacios destinados como centros de cómputo y/o cableado.

### 7.7.2. Equipos

#### Lineamientos generales

- La administración de hardware conectado a la red y la atención de nuevos requerimientos y adecuaciones, debe realizarse de acuerdo con lo establecido en el procedimiento “Gestión de servicios TI” código: 03-PT-06”;


**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 29 de 61
			<b>Vigente desde:</b> 17-09-2019	

en consecuencia, no pueden conectarse computadores, servidores, dispositivos de comunicaciones como concentradores, switches, enrutadores o cualquier otro hardware a la red, sin la participación y/o supervisión de personal autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC.

- Todos los servidores y equipos de comunicaciones de voz y datos deben estar localizados en lugares seguros para prevenir el uso o acceso no autorizado. De igual forma, deberá contarse con protecciones físicas y ambientales para los activos críticos, incluyendo perímetros de seguridad, controles de acceso físicos, seguridad en el suministro eléctrico y cableado y sistemas de detección y extinción de incendios.
- Se debe prevenir el daño de los equipos por interferencia eléctrica o magnética, riesgo de contaminación por alimentos, bebidas o golpes con objetos que perjudiquen o pongan en riesgo el funcionamiento de los mismos o deterioren la información almacenada en ellos. Se debe evitar colocar encima o cerca de los computadores ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo.
- El suministro de energía eléctrica deberá estar regulado a 110 voltios y con sistema de polo a tierra, salvo especificación en contrario del fabricante o proveedor de los equipos y se debe contar con sistema de energía ininterrumpida (UPS) y/o planta eléctrica para asegurar el apagado controlado y sistemático o la ejecución continua del parque tecnológico que sustenta las operaciones críticas de la Entidad.
- La Dirección de Tecnologías de Información y Comunicación – DTIC deberá elaborar el cronograma de mantenimiento preventivo, el cual será notificado a las dependencias con mínimo 3 días hábiles de antelación con el fin de asegurar la prestación del servicio a los usuarios. Adicionalmente, deberá informarse el nombre e identificación del personal autorizado para realizar las actividades de mantenimiento con el fin de evitar el riesgo de hurto y/o pérdida de equipos.
- Toda solicitud de mantenimiento correctivo o asistencia técnica debe realizarse a través de la herramienta mesa de ayuda en Intranet, implementado por la Dirección de Tecnologías de Información y Comunicación – DTIC.


**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 30 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Ningún funcionario(a) y/o contratista diferente al personal autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC, está autorizado(a) para destapar, intervenir, efectuar reparaciones y/o modificaciones en los equipos de cómputo de la Entidad. El mantenimiento preventivo y correctivo debe ser realizado exclusivamente por personal especializado y autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC.
- Para efectuar el traslado y/o retiro de equipos (incluidos la información y el software) por cambio del funcionario(a) y/o contratista responsable o cambio en la ubicación del equipo, se debe diligenciar el formato *“Asignación y/o Traslado de Bienes Solicitados”* código: 09-RE-03, del proceso Gestión Administrativa.
- Cuando por necesidades del servicio un funcionario(a) y/o contratista requiera temporalmente el uso de un equipo fuera de la Entidad, este debe ser solicitarlo por medio de correo electrónico a la Dirección de Tecnologías de Información y Comunicación - DTIC, quien autorizará mediante un oficio dirigido a la administración del edificio el retiro del dicho elemento.
- Cualquier cambio que se realice en el centro de cómputo o centros de cableado, y que potencialmente afecte los sistemas de información de la Entidad, debe estar previamente autorizado y registrarse en una bitácora de ingreso al centro de cómputo.
- Toda persona que ingrese al centro de cómputo debe estar autorizada y acompañada por un funcionario(a) y/o contratista de la Dirección de Tecnologías de Información y Comunicación - DTIC. Los administradores del centro de cómputo mantendrán un registro de todas las visitas autorizadas a esta área, en el que se identifique nombre del visitante, documento de identificación, fecha, hora de entrada y salida de las instalaciones, actividad por la cual ingresaron y la persona que autorizó su ingreso. A su vez, todo equipo informático ingresado al centro de cómputo deberá ser registrado.
- Constituyen áreas de acceso restringido el centro de cómputo, los cuartos de potencia (Plantas eléctricas, unidades de poder ininterrumpida UPS y cuartos de electricidad) y centros de cableado, por lo que solo el personal autorizado por la Dirección de Tecnologías de Información y Comunicación – DTIC puede acceder a él. Este personal debe portar el carnet de la Entidad que lo acredita como funcionario(a) y/o contratista del área en mención.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 31 de 61
			<b>Vigente desde:</b> 17-09-2019	

### 7.7.3. Política de escritorio y pantalla limpia

Los funcionarios(as), contratistas y terceros de la Personería de Bogotá D.C., deberán adoptar buenas prácticas para el manejo y administración de la información institucional física y/o digital que se encuentre a su cargo, con el fin de evitar que personas no autorizadas accedan a dicha información. Para ello, se deberá tener en cuenta lo siguiente:

#### Lineamientos generales

- Toda vez que el personal se ausente de su lugar de trabajo, debe además de bloquear su estación de trabajo, guardar en un lugar seguro cualquier documento, medio magnético u óptico removible que contenga información confidencial.
- Si la estación de trabajo del personal está ubicada cerca de zonas de atención de público, al ausentarse de su lugar de trabajo debe guardar también los documentos y medios que contengan información de uso interno.
- Al finalizar la jornada de trabajo, el personal debe apagar su equipo de cómputo, guardar en un lugar seguro los documentos y medios que contengan información confidencial o de uso interno, además desconectarse de los sistemas de información y servidores.
- Los usuarios deben mantener el puesto de trabajo y escritorio de los equipos de cómputo, organizado y libre de archivos o información institucional que pueda ser objeto de consulta, copiado, eliminación por personal no autorizado.
- Las estaciones de trabajo y equipos portátiles de la Entidad tendrán aplicado un protector de pantalla definido por la Dirección de Tecnologías de Información y Comunicación - DTIC, que se activará cuando el equipo permanezca inactivo durante un tiempo determinado. La pantalla de autenticación a la red de la Entidad debe requerir solamente la identificación de la cuenta y una clave y no entregar otra información adicional y se configurará el ahorro de energía apagando la pantalla a los quince (15) minutos de inactividad
- El papel tapiz se configura automáticamente en cada uno de los equipos conectados a la red LAN de la Personería de Bogotá D.C., este sirve para difundir información institucional y debe ser remitido por la Oficina Asesora de Divulgación y Prensa.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 32 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Al imprimir información confidencial, reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata de las impresoras para evitar divulgación no autorizada de la información.
- Los archivos digitales que contengan información sensible o confidencial de la Personería de Bogotá D.C., deberán ser almacenados en rutas que impidan el fácil acceso por terceros, y no se deben guardar en el área de escritorio de la pantalla del computador.
- Cuando no estén en uso, los documentos que contienen información confidencial, sensible, reservada o pública clasificada, deben ser almacenados en lugar seguro que impida el acceso de personal no autorizado.

## 7.8. SEGURIDAD DE LAS OPERACIONES


### 7.8.1. Procedimientos operacionales y responsabilidades

#### Lineamientos generales

- La Entidad establecerá procedimientos relacionados con la operación y administración de la información institucional, estarán documentados y serán puestos a disposición del personal que lo requiera.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, deberá mantener y proveer a su personal, los manuales, guías y procedimientos de configuración de equipos, plataformas informáticas y demás servicios de TI.
- Los ambientes de desarrollo, prueba y producción estarán separados físicamente (diferente hardware) siempre que sea posible, y se definirán y documentarán las reglas para la transferencia de software desde el estado de prueba hacia el estado producción.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, cuenta con el procedimiento “*Gestión de Cambios*” Código: 03-PT-04 para el control de cambios en el desarrollo de nuevas aplicaciones y en los diferentes ambientes y en general para cualquier cambio que afecte los servicios y la infraestructura tecnológica que soporta la información de la Personería de Bogotá D.C.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 33 de 61
			<b>Vigente desde:</b> 17-09-2019	

- La Dirección de Tecnologías de Información y Comunicación - DTIC, debe monitorear permanentemente el estado de los recursos y plataformas tecnológicas, (Espacios en disco, memoria, procesamiento, ancho de banda, etc.), así como proyectar el crecimiento de los mismos, con el fin de prever y proyectar las futuras necesidades de ampliación de recursos para garantizar su capacidad y adecuada operación.

### 7.8.2. Protección contra Códigos Maliciosos

#### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC designará el funcionario(a) y/o contratista, responsable del software de antivirus para que administre la plataforma y regule el uso y despliegue de la herramienta en toda la Personería de Bogotá, D.C.
- Todos los equipos de cómputo de propiedad de la Entidad deben tener instalado el software de antivirus debidamente actualizado y licenciado a nombre de la Personería de Bogotá D.C. Por lo tanto todo nuevo equipo debe ser incluido dentro del dominio de la red “perbogota.gov.co”, para que apliquen las actualizaciones y detecciones correspondientes.
- Antes de distribuir, archivos a otros usuarios internos o externos en los equipos de cómputo de la Entidad, se debe hacer un análisis de los archivos y medios con el software de antivirus.
- Está prohibido desinstalar o deshabilitar el software antivirus de los computadores de la Entidad por parte de los usuarios. Si existen indicios de infección por virus informáticos, se debe realizar un análisis del equipo y sus archivos y verificar su eliminación mediante el software de antivirus y reportar el incidente a la Dirección de Tecnologías de Información y Comunicación - DTIC.
- Todo medio de almacenamiento removible como discos duros externos, dispositivos USB, discos compactos, etc, que vaya a ser conectado a un equipo de la Entidad, debe ser analizado con el software de antivirus, como medida previa antes de su uso.
- Está prohibido el uso y/ o instalación de software no autorizado por la Dirección de Tecnologías de Información y Comunicación – DTIC. En caso de necesitar la instalación de algún software, el funcionario(a) y/o contratista

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 34 de 61
			<b>Vigente desde:</b> 17-09-2019	

responsable debe solicitar la autorización y apoyo a la Dirección de Tecnologías de Información y Comunicación – DTIC.

- La Dirección de Tecnologías de Información y Comunicación – DTIC, está facultada para revisar periódicamente la información y el software instalado en los equipos de cómputo de la Personería de Bogotá D.C., y realizará la eliminación de los archivos o información no autorizados que puedan atentar contra la seguridad de la información, así como la desinstalación inmediata del software no autorizado.

### 7.8.3. Copias de respaldo

#### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC, será la responsable de realizar copias de respaldo de la información institucional, gestionando los recursos necesarios y adoptando procedimientos y mecanismos estandarizados que permitan ejecutar y documentar las actividades realizadas, de manera que se garantice la continuidad de la prestación de los servicios de la Entidad y la atención oportuna de contingencias.
- Se deben programar y realizar pruebas de restauración periódicas de la información contenida en las copias de respaldo para comprobar su correcto funcionamiento.
- Los funcionarios(as), Contratistas y terceros responsables de la infraestructura tecnológica, deberán generar las respectivas copias de respaldo y asegurarse de su correcto almacenamiento conforme a los procedimientos establecidos por la Entidad.
- Se considera como información para ser respaldada aquella que es exclusivamente de carácter institucional.
- Las copias de respaldo son almacenadas de forma segura por parte de la Dirección de Tecnologías de Información y Comunicación - DTIC, para garantizar que no sean manipuladas por personas no autorizadas. Se debe llevar un registro de las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de las mismas: fechas de copia, restauraciones, ubicación de medios, etc.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 35 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Al cumplir el ciclo de vida útil, los medios de almacenamiento de las copias de respaldo serán inutilizados de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas.
- Cada usuario deberá tener copia de la información crítica bajo su responsabilidad en el servidor de archivos que la Dirección de Tecnologías de Información y Comunicación - DTIC asigne para tal fin, o en el área de trabajo del servidor de la red que se haya destinado, respetando las cuotas de espacio asignadas.
- Es responsabilidad de cada funcionario(a) o contratista identificar, clasificar y definir la información relevante a respaldar en los medios de almacenamiento autorizados, con el fin de mantener una copia fiel de los datos importantes.
- La custodia de la información que se almacene en los equipos de trabajo quedará bajo la responsabilidad del funcionario(a) o contratista que designe el jefe de cada dependencia.

#### 7.8.4. Registro y Seguimiento

##### Lineamientos generales

- Todas las aplicaciones en producción que la Entidad estime pertinentes y que contengan información misional de la Personería de Bogotá D.C., deben generar logs o trazas de auditoría; igualmente los sistemas que operen y administren información misional valiosa o crítica para la Entidad, deben tener archivos de logs que contengan evidencia sobre los eventos relevantes que sucedan con la información, y con la seguridad necesaria para su consulta, modificación o borrado.
- Todos los logs del sistema y de las aplicaciones deben mantenerse en forma segura, de tal forma que se evite el acceso no autorizado para garantizar la seguridad de esta información.
- Todo software o aplicativo habilitado en ambiente de producción de la Entidad debe incluir archivos logs que registren como mínimo la siguiente información:
  - La actividad realizada en la sesión abierta por el usuario incluyendo la identificación del código del usuario, fecha y hora de ingreso y salida de cada sesión del sistema y aplicaciones invocadas.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 36 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Cambios de información realizados en los archivos de las aplicaciones críticas.
- Adiciones y/o cambios a los privilegios de los usuarios, y fecha y hora de iniciación y terminación de ingreso al sistema de información.

#### **7.8.5. Control de software operacional**

##### **Lineamientos generales**

- La Personería de Bogotá D.C., establece mecanismos para la instalación de software autorizado en los equipos que hacen parte de su infraestructura tecnológica, implementando controles y definiendo el personal responsable de la instalación y soporte.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, validará y realizará las respectivas pruebas calidad y funcionamiento del software a instalar, antes de ser puesto en producción.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, será la responsable de analizar el software y autorizar su instalación, la cual debe ser realizada exclusivamente por personal idóneo y autorizado.
- Se debe mantener un registro actualizado del software propiedad de la Personería de Bogotá D.C.

#### **7.8.6. Gestión de Vulnerabilidad Técnica**

##### **Lineamientos generales**

- La Dirección de Tecnologías de Información y Comunicación - DTIC, revisará periódicamente las vulnerabilidades y debilidades técnicas de los sistemas de información y la infraestructura tecnológica, mediante el uso de herramientas de software especializadas, en pruebas de penetración, detección de vulnerabilidades y verificación de controles. En caso de ser necesario, las revisiones podrán realizarse mediante la contratación de una asistencia técnica especializada. El resultado de las revisiones se presentará

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 37 de 61
			<b>Vigente desde:</b> 17-09-2019	

en un informe técnico para su interpretación y remediación por parte de los especialistas de la Entidad.

- Se prohíbe la instalación de software por parte de personal diferente a los autorizados por la Dirección de Tecnologías de Información y Comunicación - DTIC.

## 7.9. SEGURIDAD DE LAS COMUNICACIONES

### 7.9.1. Gestión de la seguridad de las redes

#### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC, gestiona y establece mecanismos y controles para prestar el servicio de redes de datos y comunicaciones en la Entidad y propende por la protección de los datos y los servicios conectados en las redes de la Personería de Bogotá D.C., contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:
  - Establecer los procedimientos para la administración de los equipos remotos, incluyendo los equipos en las áreas restringidas.
  - Establecer controles especiales para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas, y para proteger los sistemas conectados.
  - Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, implementa los mecanismos necesarios y establece acuerdos de niveles de servicio, para garantizar la disponibilidad de los servicios de redes de datos y comunicaciones.
- Se debe mantener la confidencialidad de las políticas de enrutamiento y direccionamiento de las redes de datos y comunicaciones de la Entidad.
- Las direcciones IP internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la Entidad, serán restringidas, de tal forma que no sean conocidas por usuarios internos,

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 38 de 61
			<b>Vigente desde:</b> 17-09-2019	

clientes o personas ajenas a la Entidad sin la previa autorización de la Dirección de Tecnologías de Información y Comunicación - DTIC.

- Los equipos de acceso a la red estarán protegidos contra accesos no autorizados.
- Los funcionarios(as), contratistas o terceros que desarrollen actividades en los sistemas de información de la Entidad de manera remota, deben utilizar equipos de cómputo seguros que garanticen la no afectación de la seguridad de la red.
- La Personería de Bogotá D.C., implementa mecanismos de segmentación de redes a través de Vlan's, dependiendo de la criticidad de los recursos y servicios involucrados, con el fin de contribuir al control de acceso y optimizar el rendimiento en la red.

#### **7.9.2. Políticas y procedimientos de transferencia de información**


La transferencia de la información institucional de la Personería de Bogotá D.C., se controla según los niveles de clasificación legal de la información establecidos y las políticas de seguridad de la información de la Entidad. En caso de que se requiera intercambiar información sensible, confidencial, reservada o pública clasificada, se deben implementar los controles de cifrado de información de acuerdo con lo establecido en la política de controles criptográficos.

Los intercambios de información con terceros deben estar soportados por medio de contratos o acuerdos debidamente formalizados, determinando los medios y controles para el tratamiento de la información. Así mismo, se firmarán acuerdos de confidencialidad que garanticen la protección de la información durante y posterior al tiempo de ejecución de las labores encomendadas.

#### **Lineamientos generales**

- La Personería de Bogotá D.C., establecerá mecanismos seguros para la transferencia de información institucional internamente y con terceros, en cumplimiento de sus funciones y obligaciones legales.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, proporcionará las herramientas para garantizar la seguridad de la información, durante la transferencia a nivel interno y externo.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 39 de 61
			<b>Vigente desde:</b> 17-09-2019	

- La Entidad proporcionará tecnologías de acceso remoto a sus funcionarios(as) a través de medios como VPN (Red virtual privada), y autorizará su uso de forma particular cuando así se requiera. La Dirección de Tecnologías de Información y Comunicación – DTIC, garantizará un adecuado esquema de seguridad para los mismos.
- Todos los computadores de la Entidad que sean accedidos remotamente a través de mecanismos como Internet, enlaces dedicados y otros, deben ser protegidos por mecanismos de control de acceso aprobados por la Dirección de Tecnologías de Información y Comunicación - DTIC.
- La conexión directa entre los sistemas de información de la Entidad y otra organización o tercero vía redes públicas de datos como Internet, requieren de la aprobación de la Dirección de Tecnologías de Información y Comunicación - DTIC, quien definirá los mecanismos de seguridad apropiados.
- Como requisito para interconectar las redes de la Entidad con otras redes externas, los sistemas de comunicación de terceros deben cumplir con los requisitos de seguridad dispuestos por este documento.
- La Personería de Bogotá D.C., se reserva el derecho de cancelar y/o terminar la conexión a sistemas de terceros, que no cumplan con los requerimientos internos de seguridad y confidencialidad establecidos o acordados.
- Antes de autorizar y establecer las conexiones con sistemas de información de terceros para la transferencia o consulta de información institucional, se deben establecer Acuerdos de Confidencialidad entre las partes, para lo cual se contará con la participación de la Oficina Asesora de Jurídica de la Personería de Bogotá D.C.
- Está prohibido el uso de herramientas de acceso remoto o de transferencia de información que no hayan sido autorizadas por la Dirección de Tecnologías de Información y Comunicación - DTIC.
- Está prohibido el envío o intercambio de información sensible, confidencial o reservada, sin la autorización del responsable o jefe inmediato.
- Para la transmisión o envío interno o externo de información sensible, confidencial o reservada, a través de medios electrónicos, incluido el correo

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 40 de 61
			<b>Vigente desde:</b> 17-09-2019	

institucional, se debe asegurar de aplicar las medidas de seguridad necesarias y como mínimo, cumplir con el numeral “6.6 *POLÍTICAS DE CRIPTOGRAFÍA*” establecidas en el presente manual.

- Está prohibido utilizar el correo electrónico personal, para el envío y recepción de información institucional sensible, clasificada o reservada.
- No está permitido el envío de información institucional sensible, clasificada o reservada a través de plataformas gratuitas como (wetransfer, google drive, droopbox, whatsapp, Messenger, etc).
- No está permitido almacenar información institucional sensible, clasificada o reservada en la nube diferente al Office 365 institucional.
- El servicio de correo electrónico institucional debe ser utilizado exclusivamente para las tareas propias de la función desarrollada por la Personería de Bogotá D.C. El uso del servicio de correo electrónico de la Personería de Bogotá D.C., para fines personales no está autorizado.
- Todo funcionario(a) o contratista inscrito en la Personería de Bogotá D.C., dispondrá de una cuenta de correo electrónico activa, y para su creación se debe seguir con el procedimiento “*Gestión de usuarios*” Código: 03-PT-01” establecido de la Personería de Bogotá D.C.
- El servicio de correo electrónico oficial de la Personería de Bogotá D.C., es el aprobado por la Dirección de Tecnologías de Información y Comunicación - DTIC; los funcionarios(as), contratistas y terceros reconocen y aceptan que los incidentes de seguridad de la información generados por el uso de servicios de correo electrónico no autorizados serán de su entera responsabilidad.
- La clave de acceso al servicio de correo electrónico es personal e intransferible, no debe ser divulgada a ninguna persona, exhibirse en público y para su gestión se debe seguir los controles de protección de contraseñas definidos por el Sistema de Gestión de Seguridad de la Información - SGSI de la Personería de Bogotá D.C.
- Las contraseñas de las cuentas de correo institucional genéricas o que no estén asociadas a un usuario particular, (Por ejemplo *prensa@personeriabogota.gov.co*), deberán ser cambiadas cuando la

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 41 de 61
			<b>Vigente desde:</b> 17-09-2019	

persona encargada de administrarla sea retirada de la Entidad o trasladada de dependencia, o cese su responsabilidad sobre la cuenta de correo.

- La Personería de Bogotá D.C., puede supervisar el uso del servicio de correo electrónico para verificar que se está usando para el cumplimiento de las funciones misionales de la Entidad, en los procesos de verificación de uso apropiado del servicio de correo electrónico se respetará el derecho a la privacidad e intimidad del titular de la cuenta de correo electrónico.
- En los casos en los que se requiera envío o recepción de información confidencial, sensible, reservada o pública clasificada, el usuario del servicio de correo electrónico debe cumplir con las políticas de cifrado y/o criptografía establecidas por la Entidad, y si es el caso solicitar apoyo técnico a la Dirección de Tecnologías de Información y Comunicación - DTIC.
- La vigencia de la cuenta para funcionarios(as) y contratistas comprende el periodo desde la fecha de ingreso o firma del contrato y finaliza el último día de la fecha de retiro o terminación/suspensión del contrato.
- El uso de la cuenta de correo es con fines del cumplimiento de las funciones y/o objeto contractual y su uso es de carácter obligatorio, en ella llegará información oficial de conocimiento necesario para los funcionarios(as) y contratistas de la Entidad.
- Se prohíbe el uso de cuentas de correo gratuito con propósitos institucionales o cuentas de suscripción gratuita a otros proveedores.
- Es responsabilidad del funcionario(a) o contratista depurar su cuenta periódicamente siendo él el único responsable de realizar las copias de seguridad de sus correos.
- El usuario debe leer diariamente su correo y borrar aquellos mensajes obsoletos, para liberar espacio en su buzón de correo.
- Solo podrán enviar correos masivos aquellas dependencias que por su naturaleza de socialización y sensibilización lo requieran a través de la cuenta de correo del jefe de la dependencia; tales como (Secretaría General, Dirección de Talento Humano, Oficina Asesora de Divulgación y Prensa y la Subdirección de Gestión Documental y Recursos Humanos).

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 42 de 61
			<b>Vigente desde:</b> 17-09-2019	

- El incumplimiento por parte del funcionario(a) y/o contratista de los lineamientos o el mal manejo de su cuenta de correo institucional, puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo y en un último caso la notificación a la Dirección de Talento Humano y/o Dirección Administrativa y Financiera para que proceda disciplinariamente.
- No están autorizados los siguientes usos del servicio de correo electrónico y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:
  - Exceder los servicios para los cuales se autorizó la cuenta.
  - Enviar mensajes para la difusión de noticias, mensajes políticos, religiosos, correos sin identificar plenamente a su autor o autores o enviar anónimos.
  - Difundir “cadenas” de mensajes que saturen el servicio entre otros problemas.
  - Perturbar el trabajo de los demás enviando mensajes que puedan interferir con sus actividades laborales.
  - Agredir o lesionar directa o indirectamente a otras personas a través del envío de mensajes con contenido que atente contra la integridad y el buen nombre de las personas o instituciones, cualquier contenido que represente riesgo para la seguridad de la información de la Entidad o esté prohibido por la leyes, regulaciones o normas a las cuales está sujeta la Entidad.
  - Crear, enviar, alterar, borrar mensajes suplantando la idEntidad de un usuario.
  - Abrir, usar o revisar indebidamente la cuenta de correo electrónico de otro usuario, sin contar con la autorización formal del titular de la cuenta.
  - Suscribir las cuentas de correo institucional en servicios externos (comerciales) con fines no gubernamentales o afines a la misión institucional.
  - Enviar correos de información masivos sin estar autorizado para ello.
  - Envío de mensajes no deseados o que puedan ser considerados como SPAM.

### 7.9.3. Servicio de acceso a internet

El servicio de acceso a Internet debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Personería de Bogotá D.C., los usos

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 43 de 61
			<b>Vigente desde:</b> 17-09-2019	

diferentes a los necesarios para el cumplimiento de las funciones de la Entidad son de entera responsabilidad del usuario al que se le asigna la cuenta de acceso al servicio. El acceso al servicio podrá ser asignado a las personas que tengan algún tipo de vinculación con la Personería de Bogotá D.C., ya sea como funcionario(a), contratista o tercero.

Los servicios a los que un determinado usuario pueda acceder desde Internet dependerán del rol que desempeña el usuario en la Personería de Bogotá D.C., y para los cuales este formal y expresamente autorizado.

Todos los funcionarios(as) y contratistas que en el desarrollo de sus funciones utilicen el servicio de acceso a Internet de la Personería de Bogotá D.C., serán responsables del cumplimiento de las políticas de seguridad de la información de Entidad.

Los responsables de la administración de las redes de acceso a internet y los equipos de seguridad de la Personería de Bogotá D.C., deben implementar y monitorear permanentemente los controles necesarios para evitar la circulación de información o contenidos desde Internet hacia la red de la Entidad que puedan constituirse en riesgos para la seguridad de la Información.

### **Lineamientos generales**

- Los recursos y servicios de Internet se usarán primordialmente para asuntos institucionales. El uso personal no debe interferir con la operación eficiente de los sistemas de la institución, ni con los deberes y obligaciones de las personas establecidas en los diferentes reglamentos y manuales de la Entidad.
- Todo usuario es responsable de informar de contenidos o acceso a servicios que no le estén autorizados o no correspondan a sus funciones dentro de la Personería de Bogotá D.C.
- Todo usuario es responsable tanto del contenido de las comunicaciones como de cualquier otra información que se envíe desde la red de la Personería de Bogotá D.C., o descargue desde Internet empleando la cuenta de acceso a Internet que se le ha suministrado.
- La Personería de Bogotá D.C., puede supervisar el acceso del servicio de Internet para certificar que se está usando para el cumplimiento de las

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 44 de 61
			<b>Vigente desde:</b> 17-09-2019	

funciones institucionales, en los procesos de verificación del uso apropiado del servicio de acceso a Internet se respetan el derecho a la intimidad y privacidad del titular de la cuenta de acceso a Internet.

- La Dirección de Tecnologías de Información y Comunicación DTIC procederá al bloqueo de sitios que se detecten como peligrosos o que atenten contra la seguridad de la información o que puedan interferir con el normal funcionamiento de los sistemas de información.
- El uso indebido del servicio de internet por parte de un usuario puede ocasionar la suspensión temporal del servicio y en caso de reincidencia, la suspensión del mismo.
- No están autorizados los siguientes usos del servicio de acceso a Internet y pueden constituir un incidente de seguridad de la información con las consecuencias legales correspondientes:
  - Descargar y/o distribuir archivos con virus, gusanos, troyanos y/o la transmisión de archivos de imagen, sonido y video que no sean de tipo institucional.
  - Acceder, descargar o transmitir información sometida a derechos de autor cuando no se tienen los derechos respectivos (juegos, música, videos, obras literarias, pictóricas, imágenes, etc).
  - Descargar archivos o instalar programas de sitios web desconocidos o gratuitos sin previa autorización de la Dirección de Tecnologías de Información y Comunicación - DTIC.
  - El acceso a sitios de música, juegos u otros sitios de entretenimiento on-line.
  - El acceso a sitios Web considerados como ilegales por la normatividad colombiana, incluidos aquellos que hacen parte de la ley de delitos informáticos y aquellos prohibidos por la Ley de Infancia y Adolescencia.
  - El acceso a material pornográfico o a sitios Web de contenido para adultos relacionados con desnudismo, erotismo o pornografía, salvo en los casos que estén debidamente autorizados en cumplimiento de las funciones, caso particular de investigaciones en procesos disciplinarios o administrativos; en tal caso se deben gestionar los mecanismos de acceso seguro en canales

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 45 de 61
			<b>Vigente desde:</b> 17-09-2019	

protegidos y configurados por personal autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC.

- Acceder a sitios web de carácter discriminatorio, racista o material potencialmente ofensivo para las personas, incluyendo, bromas de mal gusto, prejuicios, menosprecio o acoso.
- Acceder a sitios de “hacking” o sitios reconocidos como inseguros para la seguridad de la información, los cuales puedan poner en riesgo la integridad, disponibilidad y confidencialidad de la información de la Personería de Bogotá D.C., salvo en los casos que se requiera para el cumplimiento de las funciones, en cuyo caso se deben gestionar los mecanismos de acceso seguro en canales protegidos y configurados por personal autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC.

#### **7.9.4. Política de seguridad en la nube**

La Personería de Bogotá D.C., en su propósito de cumplir con los lineamientos de apoyo a las actividades de mayor importancia, provee algunos de sus servicios de TI a través de computación en la nube. Con el fin de garantizar la seguridad de la información de los activos y servicios alojados en la nube, la Personería de Bogotá D.C., deberá tener en cuenta y aplicar en los procesos de contratación del servicio, los procedimientos establecidos por la Entidad para la gestión de los riesgos de seguridad de información, y en ningún momento se deberá incluir activos de información ni servicios en la nube a los cuales el resultado del análisis de riesgos no arroje un nivel aceptable para la seguridad de la información.

#### **Lineamientos generales**

- En los casos que se requiera el almacenamiento de información institucional sensible clasificada como confidencial, reservada o pública clasificada, se debe garantizar su acceso restringido mediante contraseña de usuario segura.
- Todos los usuarios de servicios de computación en la nube de la Personería de Bogotá D.C., deben mantener especial cuidado con la información institucional y en todo momento aplicar y cumplir los controles de seguridad que se definan en el presente manual para el uso seguro de la información.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 46 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 7.10. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS

### 7.10.1. Requisitos de seguridad de los sistemas de información

#### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC, se asegurará que, en los procesos de adquisición de nuevos sistemas de información, o de mejora a las aplicaciones de software existentes, se incluyan los requisitos suficientes para garantizar la seguridad de la información de acuerdo a las normas y estándares de desarrollo de software, y a las disposiciones del presente manual.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, será responsable de ejecutar las pruebas necesarias junto con los desarrolladores y/o proveedores externos, que garanticen que las aplicaciones de software adquiridas o mejoradas cumplan con los requisitos de seguridad de la información y exigidos.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, deberá asegurarse que todas las aplicaciones de software desarrolladas o adquiridas cuenten con los respectivos acuerdos de licenciamiento, condiciones de uso y derechos de propiedad intelectual.
- La actualización de la información contenida en los portales Web e Intranet de la Personería de Bogotá D.C., debe hacerse de acuerdo a lo establecido en la *“Guía para la actualización de los portales web e intranet Institucionales” Código 03-GU-01.*
- En caso de que algún componente o servicio del portal Web e Intranet se encuentre en mantenimiento o no disponible por fallas técnicas, se debe publicar una imagen o texto que informe al usuario sobre dicho evento.
- La redacción de cada uno de los contenidos de los portales Web e Intranet de la Personería de Bogotá D.C., está a cargo de los gestores de contenido asignados por cada dependencia y deberá producirse conforme a lo establecido en la *“Guía para la actualización de los portales web e intranet Institucionales” Código: 03-GU-01.*

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 47 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Los cambios solicitados que requieran modificación de la estructura básica de los portales Web e Intranet o creación de otras nuevas, serán ejecutados exclusivamente por la Dirección de Tecnologías de Información y Comunicación - DTIC.

## 7.10.2. Seguridad en los procesos de desarrollo y soporte

### 7.10.2.1. Política de desarrollo seguro

Para el desarrollo de software al interior de la Personería de Bogotá D.C., se debe realizar un proceso de planificación de los desarrollos en donde se determine la respectiva metodología a utilizar; las etapas de desarrollo; la estructura de componentes a elaborar, los respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad, teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de la Personería de Bogotá D.C. Las etapas de desarrollo deberán estar debidamente documentadas, con el objeto de generar registros de trazabilidad frente a los requerimientos, desarrollo y aceptación del software.

### Lineamientos generales

- Los requerimientos de nuevos desarrollos o ajustes a las aplicaciones existentes serán realizadas por los responsables de las dependencias propietarias de estas por la mesa de ayuda, de acuerdo al procedimiento formalmente establecido.
- La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad, se documentan entre la dependencia solicitante y la Dirección de Tecnologías de Información y Comunicación - DTIC. Los requerimientos del software se deben validar durante el proceso de aceptación del desarrollo de software.
- Para el desarrollo y puesta de producción del software, se debe contar con ambientes separados de desarrollo, pruebas y producción, determinando roles y responsabilidades claramente establecidas a fin de evitar modificaciones no autorizadas del código fuente del software.
- Los cambios requeridos sobre el software de la Personería de Bogotá D.C., se controlan a través del procedimiento de “Gestión de Cambios” Código: 03-PT-04, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos de los

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 48 de 61
			<b>Vigente desde:</b> 17-09-2019	

cambios es necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su adecuada gestión.

- En los procesos de desarrollo, la Personería de Bogotá D.C., se asegura de establecer las condiciones necesarias para la transferencia de los derechos de propiedad intelectual de códigos fuentes.
- La Dirección de Tecnologías de Información y Comunicación - DTIC se debe asegurar que los desarrollos de software en la Entidad se realicen utilizando herramientas de programación licenciadas y reconocidas.
- Los desarrollos de software en la Entidad deben contar con los manuales técnicos y de usuario además de la respectiva documentación de acuerdo a la metodología utilizada.
- Para la realización de pruebas, los datos utilizados no deben contener información real de los ambientes de producción, se deben preparar conjuntos de datos de prueba especiales que impidan la pérdida de confidencialidad de la información institucional.

## 7.11. RELACIONES CON LOS PROVEEDORES

### 7.11.1. Política de seguridad de la información para las relaciones con los Proveedores

Para los servicios contratados con proveedores en los cuales se requiera del intercambio de información institucional, se deben establecer Acuerdos de Confidencialidad y de intercambio de información en los que se definan claramente los requerimientos de seguridad de la información, incluida la obligación de cumplir con lo establecido en el presente manual y sus respectivas cláusulas civiles y penales en caso de incumplimientos.

El responsable del activo de información debe definir la finalidad de la autorización de acceso a la información que se otorgue al proveedor y documentar la autorización del acceso a los datos de acuerdo con el fin previsto.

Siempre que se otorgue acceso a la información de la Personería de Bogotá D.C., a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de la Entidad y las cláusulas requeridas para proteger la información a acceder.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 49 de 61
			<b>Vigente desde:</b> 17-09-2019	

### Lineamientos generales

- Los proveedores de la Personería de Bogotá D.C., deberán cumplir las políticas de seguridad en cuanto a la confidencialidad de la información de la Entidad.
- La Personería de Bogotá D.C., establecerá con los proveedores Acuerdos de Niveles de Servicio (ANS) con sus respectivas penalizaciones en caso de incumplimiento de los niveles acordados para cada servicio contratado, y realizará el seguimiento periódico de los mismos.
- Antes de conceder acceso a la información institucional de la Personería de Bogotá D.C., se debe dar a conocer el presente manual a los proveedores a los cuales se otorgará el permiso.
- Antes de conceder permisos de acceso a la información a los proveedores, el responsable del activo debe analizar la justificación de la necesidad del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso y los controles mínimos de seguridad a tener en cuenta frente al tratamiento de la información.
- En ningún caso se otorgará acceso a los sistemas de información o áreas seguras de la Personería de Bogotá D.C., hasta no haber formalizado la relación contractual y firmado el acuerdo de confidencialidad con los Proveedores.
- En contratos y acuerdos que se establezca con proveedores, se deben considerar y dar tratamiento a los riesgos de seguridad de la información asociados con el cumplimiento de las obligaciones contractuales, la calidad de los productos y servicios adquiridos y la seguridad de la información institucional.

#### 7.11.2. Gestión de la prestación de servicios de proveedores

##### Lineamientos generales

- La Personería de Bogotá D.C., será responsable de hacer el seguimiento periódico, supervisar y velar por el cumplimiento de las obligaciones contractuales y la calidad de los productos y servicios, así como el

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 50 de 61
			<b>Vigente desde:</b> 17-09-2019	

cumplimiento de los acuerdos de niveles de servicio establecidos con sus Proveedores.

- La Dirección de Tecnologías de Información y Comunicación - DTIC, será la encargada de aprobar los cambios que deban realizar sus Proveedores durante la prestación de los servicios, garantizando los principios de seguridad de la información y teniendo en cuenta la criticidad del servicio afectado.
- Los Proveedores de productos o servicios de la Personería de Bogotá D.C., deben abstenerse de realizar cambios que afecten la prestación de los servicios contratados con la Entidad o generen riesgo para la seguridad de la información institucional, sin previo aviso y autorización de la Dirección de Tecnologías de Información y Comunicación - DTIC.

## **7.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**

### **7.12.1. Gestión de incidentes y mejoras en la seguridad de la información**

#### **Lineamientos generales**

- La Personería de Bogotá D.C., establece los responsables para el tratamiento de los incidentes relacionados con la seguridad de la información, en concordancia con las competencias, responsabilidades y los activos a su cargo.
- Todos los funcionarios(as) y contratistas y de la Entidad deberán reportar de manera oportuna a la Dirección de Tecnologías de Información y Comunicación - DTIC, las debilidades e incidentes de seguridad que detecte o que sean de su conocimiento.
- El responsable de seguridad informática o de los activos afectados durante un incidente de seguridad, será el encargado del seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como de su comunicación al jefe inmediato y a los propietarios de la información afectada.
- La Dirección de Tecnologías de Información y Comunicación - DTIC, será la responsable de establecer el procedimiento para la gestión de incidentes de seguridad de la información, en el cual se deben considerar y determinar los

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 51 de 61
			<b>Vigente desde:</b> 17-09-2019	

criterios para clasificar un evento de seguridad como un incidente, así como los pasos a seguir para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.

- Todo evento que se clasifique como un incidente de seguridad, debe ser documentado y tratado de forma inmediata y de acuerdo a los procedimientos formalmente implementados por la Entidad.
- La solución de un incidente se registrará en una base de conocimientos y lecciones aprendidas, con el fin de que pueda ser consultada y sirva de apoyo oportuno para la prevención de eventos recurrentes o similares. La recurrencia de un incidente deberá ser tratada como un problema.
- La Personería de Bogotá D.C., dará cumplimiento a lo relacionado con Ciberdefensa y Ciberseguridad del Estado Colombiano, según lo dispuesto por los Entes responsables, y reportará cualquier evento o incidente relacionado a los organismos encargados como COLCERT, CSIRT, Policía Nacional, Fiscalía General, etc.


## 7.13. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DEL NEGOCIO

### 7.13.1. continuidad de seguridad de la información

#### Lineamientos generales

- La Personera(o) de Bogotá D.C., el Personero Auxiliar, los Personeros Delegados para las Coordinaciones, los Personeros Delegados, los Directores y Subdirectores, así como los Jefes de Oficina, serán los responsables de identificar las amenazas que puedan ocasionar interrupciones de los procesos y/o las actividades de la Entidad, evaluarán los riesgos para determinar el impacto de dichas interrupciones, identificarán los controles preventivos, y recomendarán ajustes a los planes de contingencia necesarios para garantizar la continuidad de las actividades de la Personería de Bogotá D.C.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 52 de 61
			<b>Vigente desde:</b> 17-09-2019	

- La Dirección de Tecnologías de Información y Comunicación - DTIC, Formulará los planes, controles y procedimientos necesarios, para asegurar la continuidad de las operaciones en las cuales se de tratamiento a la información institucional de la Personería de Bogotá D.C.
- Los planes deben incluir procedimientos de emergencia, escenarios de contingencia, responsabilidades asignadas, directorio de contactos, plan de capacitación, plan de comunicaciones, plan de adquisiciones, plan de pruebas, entre otros.
- En las instalaciones, plataformas o sistemas donde se procese o almacene información institucional crítica, se deben implementar medidas de redundancia suficientes para asegurar la disponibilidad de la información.


## 7.14. CUMPLIMIENTO

### 7.14.1. Cumplimiento de requisitos legales y contractuales

#### Lineamientos generales

- La Personería de Bogotá D.C., con la participación de la Oficina Asesora de Jurídica y la Dirección de Tecnologías de Información y Comunicación - DTIC, identificará, documentará, actualizará cuando sea necesario, y dará cumplimiento a la normatividad y requisitos legales relacionados con la seguridad de la información, que estén directamente relacionados con el ejercicio de sus funciones,
- Se deben implementar mecanismos o procedimientos para evitar el incumplimiento de las normas de propiedad intelectual, derechos de autor y el uso de software patentado.
- Cuando el personal de soporte técnico de la Dirección de Tecnologías de Información y Comunicación - DTIC encuentre programas instalados en los equipos de la Entidad sin autorización, procederá con la desinstalación inmediata de los mismos.
- Las licencias de uso de software estarán bajo custodia de la Dirección de Tecnología de Información y Comunicación - DTIC. Así mismo, los manuales y los medios de almacenamiento (CD, cintas magnéticas, dispositivos, etc.), que acompañen a las versiones originales de software.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 53 de 61
			<b>Vigente desde:</b> 17-09-2019	

- La Dirección de Tecnologías de Información y Comunicación - DTIC es la única dependencia autorizada para realizar copia de seguridad del software original, cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización puede conllevar a las sanciones administrativas y legales pertinentes.
- El software adquirido por la Personería de Bogotá D.C., no puede ser copiado o suministrado a terceros sin la debida autorización de la Dirección de Tecnologías de Información y Comunicación - DTIC y/o sin que se suscriba algún tipo de contrato o convenio por parte de la Personería de Bogotá D.C., y el tercero.
- Se prohíbe el uso e instalación de juegos, software pirata o que aun siendo software libre no esté autorizado por la Dirección de Tecnologías de Información y Comunicación - DTIC para su uso.
- Se prohíbe el acceso y consulta de páginas web o material pornográfico en los computadores de la Personería de Bogotá D.C. De igual manera está prohibido almacenar archivos de música o videos o cualquier otro elemento que requiera para su uso de una licencia relacionada con derechos de propiedad intelectual, patentes o similares.
- Los funcionarios(as), contratistas o terceros responsables de la publicación de la información en los sitios Web e Intranet de la Entidad, deberán atender el cumplimiento a las normas en materia de propiedad intelectual y demás políticas establecidas en el presente manual, y bajo ninguna circunstancia deben publicar información sensible, reservada o confidencial que se encuentre en poder de la Personería de Bogotá D.C.
- La Entidad efectuará constantes revisiones al cumplimiento de las normas en materia de propiedad intelectual registro de auditoria.
- La Dirección de Tecnologías de Información y Comunicación DTIC podrá autorizar el uso de material o software declarado como de uso libre, el producido por ella misma o el producido por el titular o propietario externo cuando medie autorización de este, en los términos y condiciones acordados y lo dispuesto en la normatividad vigente; para esto la Dirección de Tecnologías de Información y Comunicación - DTIC se asegurará que el software cumpla con los requisitos mínimos de seguridad y licenciamiento para su uso.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 54 de 61
			<b>Vigente desde:</b> 17-09-2019	

## 7.14.2. Revisiones de seguridad de la información

### Lineamientos generales

- La Dirección de Tecnologías de Información y Comunicación - DTIC, verificará permanentemente el cumplimiento de los controles, procedimientos y directrices establecidos en el Sistema de Gestión de Seguridad de la Información – SGSI de la Personería de Bogotá D.C., y velará por el cumplimiento de las políticas establecidas en el presente manual.

## 7.15. POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

La política de protección de datos personales en virtud de lo consagrado en la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013 y el Decreto 1074 de 2015 aplicado a todo dato personal que hayan sido suministrado o que se suministre a la Personería de Bogotá D.C., aplica y da cumplimiento a la normatividad vigente en materia de protección de datos de carácter personal.

### Lineamientos generales


- El responsable del tratamiento de datos personales es la Personería de Bogotá D.C.
- Los funcionarios(as) y contratistas de la Personería de Bogotá D.C., deben, observar, acatar y cumplir las órdenes e instrucciones de carácter legal que aplica la Entidad respecto al manejo de los datos de carácter personal cuya divulgación o indebido uso pueda generar un perjuicio a los usuarios, en cumplimiento de los derechos contenidos en el artículo 15 de la Constitución Política de Colombia, Ley 1266 de 2008, Ley 1273 de 2009, Ley 1581 de 2012, Decreto Reglamentario 1377 de 2013, Decreto 1074 de 2015 y demás disposiciones complementarias.

### 7.15.1. Alcance de la Política de Protección de Datos Personales

La política de protección de datos personales se aplicará a todas las bases de datos y/o archivos que contengan datos personales que sean objeto de tratamiento por parte de la Personería de Bogotá, D.C., incluso aquella información que haya sido obtenida o recolectada con anterioridad a la Ley 1581 de 2012 y cualquier otro dato que sea susceptible de ser tratado por la Personería de Bogotá, D.C.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.



<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 55 de 61
			<b>Vigente desde:</b> 17-09-2019	

### **7.15.2. Tratamiento de los datos personales por parte de la Personería de Bogotá D.C.**

La Personería de Bogotá D.C., en el desarrollo de su misión, actúa como responsable y/o encargado del tratamiento de datos personales que se encuentren en sus bases de datos. En consecuencia, podrá solicitar, consultar, compartir, informar, reportar, procesar, modificar, actualizar, aclarar, compilar, sustraer, ofrecer, enviar, intercambiar, adquirir, retirar, divulgar, obtener, transferir, transmitir, almacenar, utilizar, recolectar, usar, circular, suprimir, en general y en adelante, dar tratamiento, a datos personales de las personas que requieren servicios propios de la Personería de Bogotá D.C., funcionarios(as), proveedores y contratistas.

### **7.15.3. Efectos de la Autorización:**

Para todos los efectos, se entiende que la autorización por parte de los titulares a favor de la Personería de Bogotá D.C., para el suministro y/o tratamiento de sus datos personales, realizada a través de sus sitios web o por medio de cualquier canal adicional, físico, telefónico, electrónico, o personal, implica el entendimiento y la aceptación plena de todo el contenido de la presente política y de manera voluntaria, el titular y/o sus representantes, según sea el caso, le concede(n) a la Personería de Bogotá D.C., su autorización para que utilice dicha información personal conforme a las estipulaciones mencionadas.

### **7.15.4. Autorización**

El usuario declara haber recibido explicación o haber o consultado la presente política, obligándose a leerla, conocerla y consultarla en desarrollo del derecho que le asiste como titular de datos personales, sin perjuicio de haber recibido de parte de la Personería de Bogotá D.C., una clara, cierta y adecuada ilustración respecto de la misma, la cual además se ha puesto a su disposición en la página web de la Personería de Bogotá D.C., [www.personeriabogota.gov.co](http://www.personeriabogota.gov.co) en consecuencia, el usuario manifiesta que acepta en su integridad la presente política, y autoriza a la Personería de Bogotá, D.C., para que obtenga y le de tratamiento a sus datos personales, de acuerdo con los siguientes parámetros de uso:

Si el usuario no está de acuerdo con la presente política, no podrá suministrar información alguna que deba registrarse en una de las bases de datos de la Personería de Bogotá, D.C., por tanto, dicho usuario, deberá abstenerse de

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 56 de 61
			<b>Vigente desde:</b> 17-09-2019	

hacer uso de los servicios que ofrece la Entidad que haga necesario el suministro de información por parte suya.

La Personería de Bogotá, D.C., mantiene parámetros de seguridad y buen uso de los datos personales apropiados y acordes con la normativa que le rige como Entidad pública, en consecuencia, les dará a los mismos los usos adecuados para mantener la confidencialidad requerida de acuerdo con lo establecido en esta política y en la legislación vigente.

Los datos personales tratados por la Personería de Bogotá, D.C., podrán ser transferidos o transmitidos a Entidades que pertenezcan directa o indirectamente para llevar a cabo los usos y finalidades autorizadas por los usuarios para el desarrollo de las funciones propias de la Entidad, y prestar los servicios que puedan cumplir con la misión y que exista autorización legal para suministrar datos personales a un tercero. En todos los eventos, dicha información se conservará bajo estricta confidencialidad y será sometida a un tratamiento riguroso, respetando los derechos y las garantías del ciudadano, de conformidad con lo previsto en la ley.

La Personería de Bogotá, D.C., podrá utilizar proveedores de servicios y/o procesadores de datos que trabajen en su nombre, incluyendo, contratistas, delegados, outsourcing, tercerización o aliados, con el objeto de desarrollar servicios de alojamiento de sistemas, de mantenimiento, servicios de análisis, servicios de mensajería por email, servicios de entrega, entre otros. En consecuencia, el usuario entiende y acepta que mediante la presente autorización faculta a estos terceros, para acceder a su información personal, en la medida en que así lo requieran para la prestación de sus servicios. Sin perjuicio de lo anterior, se precisa que tanto los funcionarios(as) de la Entidad como las Entidades competentes protegen en todos los casos, la confidencialidad de la Información personal a su cargo.

La Personería de Bogotá, D.C., podrá recolectar información que se encuentre en el dominio público para crear o complementar sus bases de datos. A dicha información se le dará el mismo tratamiento señalado en la presente política, con las salvedades contenidas en la ley.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 57 de 61
			<b>Vigente desde:</b> 17-09-2019	

#### **7.15.5. Finalidades de la autorización**

A los datos personales que le sean suministrados a la Personería de Bogotá, D.C., se les dará un tratamiento conforme a una o algunas de las siguientes finalidades:

- Compartir con las Entidades competentes la información, para el desarrollo de sus funciones o para complementar o enriquecer la prestación de los servicios de la Personería de Bogotá, D.C.
- Dar tratamiento en medios físicos, digitales o por cualquier medio, asegurando el correcto registro y la utilización de las páginas web de la Personería de Bogotá, D.C.
- Registrar y administrar dentro de sus bases de datos la información adquirida en virtud de la relación existente entre el usuario y la Personería de Bogotá, D.C., de acuerdo a la naturaleza jurídica de dicha relación (laboral, civil, comercial, etc).
- Prevenir y detectar el fraude, así como otras actividades ilegales.

#### **7.15.6. Información personal recolectada**


La información personal que la Personería de Bogotá D.C., puede recolectar y someter a tratamiento es la siguiente:

- Nombre completo del titular de la información.
- Identificación.
- Fecha de nacimiento.
- Domicilio.
- Dirección para notificación.
- Teléfonos de contacto.
- Correo electrónico.
- Identidad de género.

#### **7.15.7. Deberes de la Personería de Bogotá D.C. cuando actúe como responsable del tratamiento**

Sin perjuicio de lo contenido en la ley, son deberes de la Personería de Bogotá, D.C., en calidad de responsable del tratamiento, los siguientes:

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 58 de 61
			<b>Vigente desde:</b> 17-09-2019	


- Garantizar al ciudadano, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
- Solicitar y/o conservar, la respectiva autorización otorgada por el titular.
- Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
- Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
- Garantizar que la información a la que se le da tratamiento, sea veraz, completa, exacta, actualizada, comprobable y comprensible. Rectificar si es del caso.
- Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
- Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
- Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
- Informar a solicitud del titular sobre el uso dado a sus datos.
- Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información del titular.

#### **7.15.8. Derechos del Titular de la información personal**

El titular de la información personal suministrada a la Personería de Bogotá, D.C., tendrá los siguientes derechos:

- Conocer, actualizar y rectificar su información personal gratuitamente.

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 59 de 61
			<b>Vigente desde:</b> 17-09-2019	

- Solicitar prueba de la existencia de la autorización otorgada a la Personería de Bogotá, D.C.
- Ser informado respecto al uso que se le ha dado a su información personal.
- Revocar la autorización y solicitar la supresión del dato cuando no se haga un uso conforme a los usos y finalidades autorizados.
- Presentar consultas y reclamos referentes a la información personal.

#### **7.15.9. Seguridad de la información y reserva de la información personal**

- La información personal no será destinada a uso o finalidades distintas a las establecidas en la presente política, razón por la cual la Personería de Bogotá, D.C., procurará proteger la privacidad de la información personal y conservarla bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, así como el respeto de los derechos del titular, según lo estipulado en la ley.
- La Personería de Bogotá, D.C., se encuentra eximida de responsabilidad, frente a las obligaciones adquiridas a través del presente aviso de privacidad, cuando por cualquier circunstancia una autoridad competente solicite que sea revelada la información personal, para actuaciones judiciales o administrativas vinculadas a cualquier tipo de obligación, proceso, investigación, persecución, o actualización de datos o acción de interés público.
- La presente política permanecerá mientras el dato se encuentre en las bases de datos de la Personería de Bogotá, D.C., y no sea de dominio público.

#### **7.15.10. Tratamiento de datos personales de menores de edad**

- En aplicación de lo establecido en la ley, la Personería de Bogotá, D.C., procederá a efectuar el tratamiento de la Información personal; de niños, niñas y adolescentes, respetando el interés superior de los mismos y asegurando, en todos los casos, el respeto de sus derechos fundamentales y garantías mínimas.
- En todos los eventos en los que se requiera dar tratamiento a la información personal de menores de edad, la Personería de Bogotá, D.C., obtendrá la

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 60 de 61
			<b>Vigente desde:</b> 17-09-2019	

autorización de sus representantes legales, que para este efecto son el padre y/o madre o tutor.


#### 7.15.11. Consulta, rectificación y reclamos

- **Consulta:** Las consultas y solicitudes deben ser dirigidas por el titular a través de cualquier medio y a cualquiera de los contactos que se señalan más adelante, y serán atendidas en los términos establecidos por la ley y la respuesta podrá ser entregada por cualquier medio físico o electrónico.
- **Rectificaciones y Reclamos:** Cuando el titular de la información o sus causahabientes consideren que su información debe ser corregida, actualizada o suprimida, o cuando adviertan un presunto incumplimiento por parte de la Personería de Bogotá, D.C., de sus deberes en materia de protección de datos personales contenidos en la legislación aplicable y en la presente política de privacidad, podrán presentar un reclamo de la siguiente manera:
  - Presentar solicitud escrita frente al requerimiento específico.
  - La Personería de Bogotá, D.C., resolverá el reclamo en los términos establecidos por la ley, por cualquier medio físico o electrónico y en la dirección de notificación que haya incluido en el respectivo reclamo.

## 8. NORMATIVIDAD APLICABLE

TIPO DE NORMA	NÚMERO	AÑO	EMISOR	ARTÍCULOS (APLICACIÓN)
Ley	23	1982	Congreso de la República	Toda la norma
Ley	1266	2008	Congreso de la República	Toda la norma
Ley	1273	2009	Congreso de la República	Toda la norma
Ley	1581	2012	Congreso de la República	Toda la norma
Ley	1712	2014	Congreso de la República	Toda la norma
Decreto	2573	2014	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.	Toda norma
Decreto	1074	2015	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.	Capítulo 25, 26

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.

<b>Personería</b> de Bogotá, D. C. <small>Al servicio de la ciudad</small> 	<b>MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN</b>		<b>Código: 03-MN-01</b>	
			<b>Versión:</b> 5	<b>Página:</b> 61 de 61
			<b>Vigente desde:</b> 17-09-2019	

TIPO DE NORMA	NÚMERO	AÑO	EMISOR	ARTÍCULOS (APLICACIÓN)
Decreto	1078	2015	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.	Título 9, Capítulo 1
Decreto	1759	2016	Ministerio de Comercio, Industria y Turismo.	Toda la norma
Decreto	1008	2018	Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.	Toda la norma
Norma técnica colombiana NTC-ISO	31000	2011	Information Technology Security Techniques	Toda la norma
Norma técnica colombiana NTC-ISO-IEC	27001	2013	Information Technology Security Techniques	Toda la norma
Documento CONPES Política Nacional de Seguridad Digital	3854	2016	Consejo Nacional de Política Económica y social - CONPES	Toda la norma

**Nota:** Si este documento se encuentra impreso se considera Copia no Controlada. La versión vigente está publicada en la intranet de la Personería de Bogotá, D. C.