



## CONTENIDO

INTRODUCCIÓN .....	6
ALCANCE.....	7
OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN .....	8
1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN .....	9
OBJETIVO.....	9
ALCANCE.....	9
POLÍTICA.....	9
2 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN.....	10
2.1. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES .....	10
OBJETIVO.....	10
ALCANCE.....	10
POLÍTICA.....	10
RESPONSABILIDADES .....	11
2.2. POLÍTICA DE TELETRABAJO .....	12
OBJETIVO.....	12
ALCANCE.....	12
POLÍTICA.....	12
RESPONSABILIDADES .....	12
2.3. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN.....	13
OBJETIVO.....	13
ALCANCE.....	13
POLÍTICA.....	13
RESPONSABILIDADES .....	13
2.4. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS .....	15
OBJETIVO.....	15
ALCANCE.....	15



POLÍTICA.....	15
RESPONSABILIDADES .....	15
2.5. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA.....	16
OBJETIVO.....	16
ALCANCE.....	16
POLÍTICA.....	17
RESPONSABILIDADES .....	17
2.6. POLÍTICA DE RESPALDO DE INFORMACIÓN (BACKUP).....	18
OBJETIVO.....	18
ALCANCE.....	18
POLÍTICA.....	18
RESPONSABILIDADES .....	19
2.7. POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN.....	19
OBJETIVO.....	19
ALCANCE.....	20
POLÍTICA.....	20
RESPONSABILIDADES .....	20
2.8. POLÍTICA DE DESARROLLO DE SOFTWARE.....	21
OBJETIVO.....	21
ALCANCE.....	21
POLÍTICA.....	21
RESPONSABILIDADES .....	22
2.9. POLÍTICA PARA RELACIONES CON PROVEEDORES.....	24
OBJETIVO.....	24
ALCANCE.....	24
POLÍTICA.....	24
RESPONSABILIDADES .....	24



2.10. POLÍTICA DE AUTORIZACIÓN DE NUEVOS RECURSOS DE PROCESAMIENTO.....	25
OBJETIVO.....	25
ALCANCE.....	25
POLÍTICA.....	25
RESPONSABILIDAD.....	26
2.11 POLÍTICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN.....	26
OBJETIVO.....	26
ALCANCE.....	26
POLÍTICA.....	27
RESPONSABILIDAD.....	27
2.12. POLÍTICA DE SEGURIDAD FÍSICA.....	28
OBJETIVO.....	28
ALCANCE.....	28
<b>POLÍTICA</b> .....	28
<b>RESPONSABILIDAD</b> .....	30
2.13. POLÍTICA DE ANTIVIRUS.....	31
OBJETIVO.....	31
ALCANCE.....	31
POLÍTICA.....	32
RESPONSABILIDAD.....	32
2.14. POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO.....	33
OBJETIVO.....	33
ALCANCE.....	33
POLÍTICA.....	33
RESPONSABILIDAD.....	35
2.15. POLÍTICA DE USO DE CONTRASEÑAS.....	35
OBJETIVO.....	35



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 4 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

ALCANCE .....	35
POLÍTICA.....	35
RESPONSABILIDAD .....	36
2.16. POLÍTICA DE USO DE SERVICIOS DE RED .....	37
OBJETIVO.....	37
ALCANCE.....	37
POLÍTICA.....	37
RESPONSABILIDAD.....	37
2.17. POLÍTICA DE USO DE INTERNET .....	38
OBJETIVO.....	38
ALCANCE.....	38
POLÍTICA.....	38
RESPONSABILIDAD.....	40
2.18. POLÍTICA DE USO DE RED PRIVADA VIRTUAL (VPN) .....	40
OBJETIVO.....	40
ALCANCE.....	40
POLÍTICA.....	40
RESPONSABILIDAD.....	41
2.19. POLÍTICA DE CONTROL DE CAMBIOS .....	41
OBJETIVO.....	41
ALCANCE.....	41
POLÍTICA.....	42
RESPONSABILIDAD.....	42
2.20. POLÍTICA DE PROPIEDAD INTELECTUAL .....	43
OBJETIVO.....	43
ALCANCE.....	43
POLÍTICA.....	43



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 5 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

RESPONSABILIDAD .....	44
3 POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN SECRETARÍA DISTRITAL DEL HÁBITAT .....	44
<b>I. IDENTIFICACIÓN DE LA ENTIDAD .....</b>	<b>44</b>
<b>II. MARCO LEGAL DE LA POLÍTICA.....</b>	<b>44</b>
<b>III. DERECHOS DE LOS TITULARES .....</b>	<b>48</b>
<b>IV. DEBERES DE LA SECRETARÍA DISTRITAL DEL HÁBITAT .....</b>	<b>49</b>
<b>V. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES .....</b>	<b>53</b>
<b>VI. TRATAMIENTO DE LA INFORMACIÓN .....</b>	<b>57</b>
<b>VII. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR</b> 60	
<b>VIII. TRATAMIENTO DE DATOS RECOLECTADOS CON ANTELACIÓN A LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN.....</b>	<b>62</b>
<b>IX. PERMANENCIA DE LA INFORMACIÓN EN LAS BASES DE DATOS .....</b>	<b>64</b>
<b>X. VIGENCIA DE LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN.....</b>	<b>64</b>
4 GLOSARIO.....	65
5 CONTROL DE CAMBIOS .....	72
6 ANEXOS.....	73



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 6 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### INTRODUCCIÓN

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

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

El presente documento contiene la política general del SGSI y las políticas específicas de Seguridad de la Información, las cuales deben ser conocidas y cumplidas por todos los servidores públicos y terceros que hagan parte de la Secretaría Distrital del Hábitat y que a su vez tengan acceso a los activos de información de la entidad.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 7 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### ALCANCE

El Subsistema de Gestión de Seguridad de la Información de la SDHT tiene como objetivo contribuir al mejoramiento del cumplimiento de los niveles de seguridad de la información y la protección de los activos de información identificados en la entidad, a través de la definición e implementación de políticas, procedimientos e instructivos, así como la definición de la metodología de gestión de riesgos de seguridad de la información, que permita a la SDHT, identificar riesgos y generar controles como mecanismo para salvaguardar la información.

La documentación del Subsistema de Seguridad de la Información, será monitoreada y revisada periódicamente con el fin de validar su implementación y necesidades de ajuste para el cumplimiento de los objetivos de seguridad planteados y el mejoramiento continuo de los mismos, conforme con los requerimientos normativos descritos en el Modelo de Seguridad y Privacidad de la Información de MinTIC, norma técnica NTC/IEC-ISO 27001:2013, mejores prácticas GTC/IEC-ISO 27002, la normatividad colombiana y procedimientos de la SDHT. El presente documento fue aprobado mediante comité de Seguridad de la Información y de la Tecnologías de la información y las Comunicaciones.

Los funcionarios, contratistas, proveedores y terceras partes son responsables del cumplimiento de los lineamientos definidos en el SGSI, obedeciendo así a los principios de confidencialidad, integridad y disponibilidad de los activos de información determinados por la Secretaría Distrital del Hábitat, para así garantizar las condiciones óptimas de habitabilidad para la población del Distrito Capital. El SGSI cubre y define requerimientos para todos los Sistemas de información de la entidad, como lo son; Sistema de estadísticas y georreferenciación SIHAB, Sistema de Ventana Única de Construcción - VUC, Sistema de estadísticas, reportes y almacenamiento de información de predios SIDEC y Sistema de Información Distrital de Inspección, Control y Vigilancia de Vivienda SIDIVIC, entre otros.

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 8 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### OBJETIVOS DE LA SEGURIDAD DE LA INFORMACIÓN

La SDHT define los siguientes objetivos del SGSI, los cuales serán revisados, comunicados y actualizados de acuerdo con los lineamientos definidos en el sistema integrado de gestión de la entidad:

1. Fortalecer la seguridad de la información, manteniendo la confianza de los ciudadanos, servidores públicos y terceros a través de la revisión, actualización, divulgación y el cumplimiento de las políticas, procedimientos e instructivos definidos dentro del SGSI de la secretaría distrital del hábitat.
2. Llevar a cabo una gestión de riesgos de seguridad de la información con el fin de preservar los niveles de confidencialidad, integridad y disponibilidad de los activos de información de la secretaría distrital del hábitat, los cuales se encuentran definidos en la matriz de inventario de activos de información.
3. Fortalecer la cultura de seguridad de la información, a través de la inclusión de buenas prácticas y conciencia de los servidores públicos y terceros frente a la seguridad de la información en la secretaría distrital del hábitat.
4. Contribuir con la continuidad del negocio de la secretaría distrital del hábitat, mediante la implementación de planes y controles asociados a la seguridad de la información que contribuyan al mantenimiento de los niveles de riesgos aceptables de la entidad, a través de una adecuada gestión de incidentes de seguridad de la información.
5. Apoyar el desarrollo y puesta en marcha de proyectos en todas sus fases de ejecución, buscando garantizar los niveles de seguridad de la información definidos por la secretaría distrital del hábitat y cumplimiento normativo colombiano.





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 9 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### 1 POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

#### OBJETIVO

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

#### ALCANCE

La política general de seguridad de la información aplica a todos los servidores públicos y terceros de la secretaría distrital del hábitat.

Cualquier violación u omisión de las políticas aquí descritas se sancionarán conforme a lo establecido en el código disciplinario único (ley 734 de 2002), lo definido en el proceso control disciplinario establecido por la Secretaría Distrital del Hábitat y lo acordado en el contrato de prestación de servicios suscrito con la entidad.

#### POLÍTICA

La SDHT garantizará las condiciones óptimas de habitabilidad para la población del distrito capital con un compromiso total de la alta dirección, manteniendo la confidencialidad, integridad y disponibilidad de sus activos de información mediante una gestión del riesgo continua, la adopción de buenas prácticas en el uso y gestión de los activos de información, así como la mejora de las competencias y conciencia de los servidores públicos de la entidad, con criterios de decisión aprobados y cumpliendo las normas legales, reglamentarias y contractuales adoptadas por la entidad.

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 10 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

## 2 POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

### 2.1. POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

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



## **RESPONSABILIDADES**

- El Área de Gestión Tecnológica y el Oficial de Seguridad de la Información, establecerán las medidas de seguridad para proteger la información que sea administrada, transmitida o almacenada por los dispositivos móviles de los servidores públicos y terceros de la entidad.
- Los servidores públicos que tengan asignados dispositivos móviles de la entidad, deberán protegerlos de forma física y lógica para evitar el hurto, acceso no autorizado o divulgación de la información almacenada y procesada por estos dispositivos. En caso de ser necesario, se establecerán controles de cifrado de la información, uso de autenticación y copias respaldo.
- El Área de Gestión Tecnológica asignará o denegará a los servidores públicos y terceros el acceso a la información o sistemas de información a través de los dispositivos móviles, conforme los roles y responsabilidades asignados por la entidad y lineamientos determinados por los distintos jefes de área.
- En caso de que se presente el hurto o pérdida de algún dispositivo móvil propiedad de la Secretaría Distrital del Hábitat, el servidor público o tercero responsable de dicho dispositivo, deberá informar el suceso de manera inmediata al jefe de área y al Oficial de Seguridad de la Información de la entidad o persona delegada para dicha actividad, con el objetivo de establecer las medidas de seguridad adecuadas que permitan proteger la información.
- El área de talento humano con el apoyo del Oficial de Seguridad de la Información coordinarán el desarrollo de campañas de sensibilización periódicas a los servidores públicos de la entidad, con el propósito de concientizar acerca del buen uso de los dispositivos móviles.
- Esta política debe ser cumplida por los servidores públicos y terceros que tengan acceso a la información o sistemas de información de la Secretaría Distrital del Hábitat a través de dispositivos móviles.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 12 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### 2.2. POLÍTICA DE TELETRABAJO

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

#### RESPONSABILIDADES

- El Área de Gestión Tecnológica adoptará los procedimientos necesarios, para proteger los datos y/o activos de información que serán accedidos desde los equipos vinculados a las actividades de teletrabajo.
- El Área de Gestión Tecnológica y el Oficial de Seguridad de la Información, definirán los canales de comunicación tales como el establecimiento de VPN's y métodos de autenticación apropiados para controlar el acceso remoto de los usuarios a la información y/o sistemas de información de la Secretaría Distrital del Hábitat, en el momento de realizar actividades de teletrabajo.
- El Área de Talento Humano, con el apoyo del Oficial de Seguridad de la Información y/o Área de Gestión Tecnológica, llevaran a cabo el análisis de los riesgos de seguridad de la información existentes en el sitio del teletrabajo, teniendo en cuenta las instalaciones físicas, el entorno local y todos los lineamientos de seguridad definidos por la Secretaría Distrital del Hábitat.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 13 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- El Área de Gestión Tecnológica conforme a la información remitida por el Área de Talento Humano y/o el jefe del área, asignará, modificará o denegará los accesos a los activos de información durante las actividades de teletrabajo.
- El Oficial de Seguridad de la Información y/o el Área de Gestión Tecnológica, junto con el Área de Talento Humano, llevaran a cabo campañas de sensibilización para promover las buenas prácticas de seguridad asociadas a las actividades de teletrabajo.

### 2.3. POLÍTICA DE CONTROL DE ACCESO A LA INFORMACIÓN

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

#### RESPONSABILIDADES

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 14 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- El acceso a los activos de información será restringido teniendo en cuenta los roles y responsabilidades de los servidores públicos de la Secretaría Distrital del Hábitat. La autorización será otorgada por los responsables de los activos de información, previa solicitud realizada por los Subsecretarios o subdirectores de la Entidad conforme a lo descrito en el Procedimiento de Gestión de Cuentas de Usuario (PS05- PR08). Los registros de acceso y actividades desarrolladas podrán ser auditadas para propósitos de control e investigación a los que haya lugar dentro de la naturaleza de la Secretaría Distrital del Hábitat, y así mismo para minimizar el riesgo de la pérdida de los niveles de seguridad de la información.
- Los servidores públicos y terceros de la Secretaría Distrital del Hábitat tienen como responsabilidad mantener los niveles de seguridad de la información de los activos designados y autorizados, asegurándose que estos sólo sean utilizados para el desarrollo de las labores encomendadas. En caso de observar incidentes de seguridad, los mismos deberán ser reportados conforme a lo establecido en el PS05-PR04 Procedimiento Gestión de Incidentes de Seguridad de la Información.
- Los accesos tanto físicos como lógicos, asignados a los servidores públicos deberán ser desactivados o modificados una vez se termine el vínculo laboral/contractual con la Secretaría Distrital del Hábitat. Esto se realizará conforme a la información remitida por el Área de Talento Humano/ Jefe del Área o Subsecretario de Gestión Corporativa.
- Todos los servidores públicos de la Secretaría Distrital del Hábitat tendrán un identificador único (ID del usuario) para su uso personal que les permita validar los accesos y verificar el buen uso de los activos de información.
- Los responsables de las áreas seguras de la Secretaría Distrital del Hábitat, establecerán los controles necesarios para restringir el acceso, determinando mecanismos de registro que permitan validar datos de identificación de la persona que accede a la información, el motivo del ingreso, el tiempo empleado para el desarrollo de la actividad, y asimismo, velará por que las personas que accedan se encuentren acompañadas por un encargado durante su permanencia en ella.
- El Responsable y/o Encargado del activo de información o área segura, será responsable de realizar revisiones periódicas de los derechos de acceso de los usuarios en intervalos regulares con el fin de mantener un control eficaz de los mismos.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 15 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### 2.4. POLÍTICA DE CONTROLES CRIPTOGRÁFICOS

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

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

#### RESPONSABILIDADES

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 16 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- El Oficial de Seguridad de la Información es el encargado del sistema de cifrado y de las llaves criptográficas de la entidad, quien será el responsable de identificar y establecer los controles necesarios para garantizar los niveles adecuados de seguridad y restringir su acceso sólo a las personas autorizadas.
- Las actividades relacionadas con la administración y eliminación de las llaves criptográficas, deberán ser registradas por las personas encargadas. Cuando las llaves se encuentren en riesgo o se tenga la sospecha que hayan sido divulgadas, o cuando servidores públicos culminen su vínculo laboral/contractual con la Secretaría Distrital del Hábitat, las mismas serán modificadas o eliminadas con el fin de proteger el acceso a la información.
- Las personas autorizadas para el acceso y uso de las llaves criptográficas, velarán por su protección y conservación. Así mismo, mantendrá los niveles de seguridad de la información cifrada o descifrada al nivel de clasificación previamente establecido.
- Los servidores públicos y terceros tendrán la responsabilidad de reportar, mediante el canal autorizado por la entidad, entre los que se encuentra la mesa de ayuda o correo electrónico las posibles vulnerabilidades, amenazas o riesgos asociados al cifrado de la información.

### 2.5. POLÍTICA DE ESCRITORIO LIMPIO Y PANTALLA LIMPIA

#### OBJETIVO

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

#### ALCANCE

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





## **POLÍTICA**

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

- Almacenar los documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.), así como la información física en sitios seguros, por ejemplo: en cajones bajo llave o archivadores. Esto con el fin de evitar el acceso no autorizado, pérdida o daño de la información a cargo.
- Durante los periodos de tiempo en los cuales cesan las actividades en el equipo de cómputo, la sesión se debe bloquear, para evitar accesos no autorizados a la información contenida en el equipo.
- Una vez culmine el proceso de impresión o copiado de documentos, la información debe retirarse inmediatamente por el servidor público responsable, y así mismo, se deberá evitar reutilizar papel que contenga información confidencial.
- De acuerdo con los niveles de clasificación de la información, los archivos o carpetas deberán ser almacenados en rutas que impidan el fácil acceso por parte de terceros, así mismo, se deberá evitar guardarlos en el escritorio del sistema operativo del equipo de cómputo.

## **RESPONSABILIDADES**

- El Área de Gestión Tecnológica con el apoyo del Oficial de Seguridad de la Información, serán los responsables de establecer los controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee de forma automática en un lapso determinado de inactividad.
- A fin de validar el cumplimiento de la presente política, los equipos de cómputo y los lugares de trabajo de los servidores públicos y terceros, podrán ser revisados y auditados por las áreas de control que determine la entidad.
- Los usuarios no deberán almacenar en el escritorio del sistema operativo de sus estaciones de trabajo, documentos, accesos directos a los documentos o a sistemas de información sensibles.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 18 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

### 2.6. POLÍTICA DE RESPALDO DE INFORMACIÓN (BACKUP)

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

Las copias de respaldo serán realizadas conforme al procedimiento definido por la Secretaría Distrital del hábitat, y las mismas serán almacenadas conforme a los mecanismos de protección ambiental como detección de humo, humedad y controles de acceso físicos, con el fin de evitar el acceso no autorizado y garantizar la integridad y seguridad de las mismas.

El proceso de Gestión Tecnológica velará por el aseguramiento de la información durante la generación, transporte y almacenamiento, con el fin que la misma no sea manipulada por personas no autorizadas.



## **RESPONSABILIDADES**

- Los servidores públicos y/o terceros encargados de las copias de respaldo deberán velar porque la información sea almacenada conforme a los procedimientos establecidos, es decir, de una manera controlada y de acuerdo con las necesidades de la Secretaría Distrital del Hábitat. Así mismo, se deberá llevar a cabo pruebas periódicas de las copias y validar su correcto funcionamiento.
- Los servidores públicos y terceros deberán almacenar la información “Crítica del Negocio” requerida para sus procesos operativos, dentro de los sistemas de almacenamientos dispuestos por la Secretaría Distrital del Hábitat. De esta manera, se garantizará la disponibilidad de las copias de respaldo de cada una de las áreas; así mismo, los servidores públicos o terceros serán responsables de depurar periódicamente la información para la optimización de los recursos de la entidad.
- La información que las áreas y/o los servidores públicos almacenan en los equipos y carpetas compartidas de la Secretaría Distrital del Hábitat, debe ser únicamente de carácter institucional y no de uso personal (fotos, música, archivos personales y otros), esto con el fin de optimizar el espacio de los mismos. Cuando se encuentre información de uso personal dentro de los equipos de cómputo o servidores, la misma, será borrada sin previo aviso.
- Los servidores públicos y/o terceros encargados usarán el procedimiento PS05-PR16 Respaldo y restablecimiento de información (backup) de aplicativos y/o infraestructura y PS05-PR17 Respaldo y restablecimiento de información de usuarios (backup) (diario, semanal mensual y anual), establecidos según las necesidades y capacidades de la infraestructura tecnológica de la Secretaría Distrital del Hábitat, con el fin de asegurar que las copias de respaldo sean confiables en caso de emergencia. Estas copias serán retenidas por un periodo de tiempo determinado, de acuerdo con lo establecido en la entidad, resguardadas a través de controles que permitan salvaguardar de manera adecuada los niveles de seguridad.

## **2.7. POLÍTICA DE TRANSFERENCIA O INTERCAMBIO DE INFORMACIÓN**

### **OBJETIVO**

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 20 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### ALCANCE

La política aquí descrita debe ser adoptada por todos los servidores públicos y terceros que realicen transferencia de información de forma interna o externa en cumplimiento de sus funciones acorde al procedimiento PS05-PR09 transmisión o transferencia de información.

### POLÍTICA

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

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

### RESPONSABILIDADES

- La información sólo podrá ser usada para las actividades y labores asignadas dentro de los acuerdos suscritos entre la Secretaría Distrital del Hábitat y las partes interesadas, apoyado con la firma de un acuerdo o cláusulas de confidencialidad de la información.
- La información deberá protegerse de divulgación no autorizada conforme los niveles de clasificación de la información establecidos PS05-PR05 Procedimiento de Clasificación y etiquetado de la Información, donde es necesario cumplir los mecanismos y controles definidos para el tratamiento de esta.
- Para la transferencia de información electrónica, el Área de Gestión Tecnológica en coordinación con El Oficial de Seguridad de la Información, dispondrán los canales de comunicación que brinden niveles de seguridad adecuados para la transferencia de información, adicionalmente, se tendrán presentes los riesgos de seguridad, así como los niveles de clasificación de la información antes del envío de la misma.
- El intercambio de la información se llevará a cabo según los acuerdos establecidos, los cuales deben tener definido como mínimo: las responsabilidades y procedimientos para



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 21 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

la transferencia de información que permita garantizar la trazabilidad y no repudio, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad y los niveles de clasificación de la información a ser intercambiada y tratada por las partes.

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

### **2.8. POLÍTICA DE DESARROLLO DE SOFTWARE**

#### **OBJETIVO**

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

#### **ALCANCE**

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

#### **POLÍTICA**

Los contratos de desarrollo de software se realizará conforme a la Ley 23 de 1982, las obras literarias (dentro de las que se encuentra el software), artísticas y científicas creadas por servidores públicos y particulares contratados mediante prestación de servicios por la Entidad, desarrolladas en cumplimiento de las obligaciones constitucionales y legales del cargo que fungen y/o de las que se establezcan en el contrato, son de propiedad de la Secretaría Distrital del Hábitat, en virtud de la presunción legal de cesión de derechos patrimoniales vigente en el ordenamiento nacional. Lo que significa que, los servidores públicos preservan los derechos morales como autores de las obras, aunque no puedan



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 22 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

utilizarlos para explotarlos en detrimento de los derechos y deberes de la Secretaría Distrital del Hábitat.

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

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

En los casos de adquisición de software a la medida, la SDHT determinará dentro de los contratos definidos con el proveedor, la propiedad de la licencia y los derechos intelectuales de los códigos fuente, así como las condiciones de uso.

### **RESPONSABILIDADES**

- Antes de iniciar el desarrollo de software, el grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica y/o el oficial de seguridad de la información, así como las partes interesadas, acordarán una metodología de desarrollo, identificando detalladamente la estructura de trabajo, responsables, cronograma, alcance, requisitos a cumplir, procesos afectados y requerimientos.
- El grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica junto con el oficial de seguridad de la información, establecerán criterios de aceptación de seguridad para la aprobación del software. La aceptación del software se establecerá a través de los resultados obtenidos de las pruebas planteadas, las cuales tendrán dentro de sus parámetros, la validación de vulnerabilidades, códigos maliciosos, puertas traseras, entre otras.
- Dentro de los requisitos a tener presentes para el desarrollo de software con respecto a la seguridad de la información, es importante determinar: controles para proteger la confidencialidad, disponibilidad e integridad de la información, métodos de autenticación, cifrado de datos, control de roles y privilegios, pistas de auditoria, gestión de sesiones, datos históricos, manejo apropiado de errores, seguridad en las comunicaciones, codificación segura, mecanismos de protección de datos personales, entre otras.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 23 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Antes, durante y después del desarrollo de software, se deberá efectuar un análisis de riesgos donde se determine el impacto y afectación de la materialización de los riesgos a la entidad. Así mismo, se determinarán los controles de seguridad necesarios para la mitigación de estos.
- El grupo técnico que lidere el desarrollo del software, el proceso de Gestión Tecnológica junto con el oficial de seguridad de la información, deberán llevar a cabo revisiones y auditorías informáticas a los desarrollos realizados, con el fin de validar el cumplimiento de los requisitos de seguridad y calidad definidos.
- El grupo técnico que lidere el desarrollo del software y el responsable del proceso de Gestión Tecnológica verificarán y controlarán las versiones del software desarrollado con los respectivos documentos de soporte. Esto con el adecuado control y funcionamiento para garantizar el ciclo de vida de este.
- Los usuarios deberán utilizar diferentes perfiles para el ambiente de desarrollo, de pruebas y de producción; así mismo, se deberá asegurar que cada usuario cuente únicamente con los privilegios necesarios en cada ambiente para el desarrollo de sus funciones.
- Los servidores públicos o terceros que realicen actividades de desarrollo de software, no podrán realizar pruebas, instalaciones o desarrollos de hardware o software directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad, integridad o confidencialidad de la información.
- El grupo técnico que lidere el desarrollo del software y el proceso de Gestión Tecnológica, deberán restringir el acceso a los compiladores, editores, utilidades de los sistemas y otras herramientas de desarrollo desde los sistemas del ambiente de producción y a cualquier usuario que no lo requiera para el desarrollo de su labor.
- El grupo técnico que lidere el desarrollo del software y el proceso de Gestión Tecnológica deberán verificar periódicamente las versiones instaladas tanto en ambiente de pruebas como en producción, con el fin de que las mismas correspondan a las últimas versiones aprobadas. Si llegase a presentarse incongruencia en la revisión realizada, esto será identificado como un incidente de seguridad y se atenderá de acuerdo con el procedimiento PS05-PR04 Gestión de Incidentes de seguridad.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 24 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### 2.9. POLÍTICA PARA RELACIONES CON PROVEEDORES

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

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

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

#### RESPONSABILIDADES

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





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 25 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

- Los propietarios de información que se requiera intercambiar, son responsables de definir los niveles y perfiles de autorización para acceso, modificación y eliminación de esta; por su parte, los custodios de esta información son responsables de implementar los controles que garanticen el cumplimiento de los criterios de confidencialidad, integridad, disponibilidad de acuerdo con la reglamentación vigente y los lineamientos definidos por la Secretaría Distrital del Hábitat.
- En caso de presentarse y/o identifique una amenaza que pueda llegar a afectar la seguridad de la información, se deberá reportar al Oficial de Seguridad de la Información y/o el proceso de Gestión Tecnológica a través de los canales de comunicación establecidos por la entidad.

### **2.10. POLÍTICA DE AUTORIZACIÓN DE NUEVOS RECURSOS DE PROCESAMIENTO**

#### **OBJETIVO**

Establecer los lineamientos generales para asegurar que la conexión de nuevos recursos de procesamiento conservando las características de confidencialidad, disponibilidad e integridad de estos.

#### **ALCANCE**

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

#### **POLÍTICA**

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 26 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

La Secretaría Distrital del Hábitat llevará a cabo control de acceso a la información y/o activos de información contemplando aspectos físicos y lógicos, con el objetivo de garantizar la trazabilidad de las acciones realizadas por los usuarios.

### **RESPONSABILIDAD**

- El(la) Subsecretario de Gestión Corporativa cumplirá la función de autorizar la incorporación de nuevos recursos de procesamiento a la solución integral de telecomunicaciones de la Secretaría Distrital del Hábitat.
- El Oficial de Seguridad de la Información y/o el personal responsable de Gestión Tecnológica evaluarán las vulnerabilidades según procedimiento establecido y el personal responsable de Gestión Tecnológica realizará las conexiones.

### **2.11 POLÍTICA PARA CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN**

#### **OBJETIVO**

Definir el nivel de criticidad, sensibilidad y reserva de la información de la Secretaría Distrital del Hábitat, para garantizar la confidencialidad, integridad y disponibilidad de los activos de información de la SDHT.

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

#### **ALCANCE**

Se aplica a todos los activos de información identificados en la Secretaría Distrital del Hábitat.

La identificación de los activos de información debe tener presente, la información, sistemas de información, software, hardware, personas o lugares para la operación o aquella

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE HABITAT</p>	<b>MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 27 de 73
		VERSIÓN 4
		Fecha 2018/09/26
		Código PS05-MM13

información estratégica requerida para alcanzar los objetivos misionales de la SDHT. Dentro de los activos de información a identificar se pueden encontrar:

- Los portales web de la SDHT y los contenidos que residen en ellos;
- La información que se transmite a través de los diferentes servicios de la SDHT;
- Los servicios de interacción con la comunidad, servicios de transacciones en línea, servicios de recaudo o registro de información, entre otros.
- Los sistemas de información que apoyan los servicios de la SDHT;
- La plataforma tecnológica que soporta los diferentes servicios y sistemas de información (hardware, software, comunicaciones, bases de datos, etc.) de la SDHT;
- La plataforma tecnológica de seguridad implementada por la SDHT;
- Los documentos físicos requeridos para llevar a cabo el desarrollo de las actividades operaciones para el cumplimiento de los objetivos misionales de la SDHT.
- Los activos de información a los que se refiere el Decreto 103 de 2015 que reglamenta la Ley 1712 de 2014 (Ley de Transparencia y Acceso a la Información).

## **POLÍTICA**

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

## **RESPONSABILIDAD**

Los responsables de la información son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, mantener actualizada la clasificación efectuada, y de definir los niveles que podrán tener permisos de acceso a la información.

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 28 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

### **2.12. POLÍTICA DE SEGURIDAD FÍSICA**

#### **OBJETIVO**

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

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

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

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

#### **ALCANCE**

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

#### **POLÍTICA**

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

Los aspectos de la seguridad física a considerar son:



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 29 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- El perímetro de seguridad debe ser claramente definido.
- Las medidas de seguridad que se deban tomar dependerán directamente del valor de los activos de información, su nivel de confidencialidad, y los valores requeridos de disponibilidad.
- El sitio donde se ubiquen los recursos informáticos debe ser físicamente sólido, y protegido de accesos no autorizados factores naturales, empleando mecanismos de control (tarjetas, vallas, alarmas, cerraduras, claves de acceso, etc.), barreras físicas, alarmas, barras metálicas etc.
- Los requerimientos de tipo ambiental deben ser especificados por los diferentes fabricantes de los equipos.
- Debe existir un área de recepción que solo permita la entrada de personal autorizado.
- El equipamiento de soporte como impresoras y fotocopiadoras debe ser instalado adecuadamente en las áreas protegidas para evitar solicitudes de acceso que podrían comprometer la información.
- Las áreas seguras contarán con equipos contra incendio, detección de humo, control de humedad, controles contra huelgas y otros.
- Los backups de información se mantendrán en sitios alejados de los procesamientos principales.
- En las áreas donde se tenga equipos de procesamiento de información, no se permite fumar, tomar ningún tipo de bebidas o consumir alimentos.
- Los equipos deben ser protegidos de fallas de potencia u otras anomalías de tipo eléctrico.
- Los sistemas de abastecimiento de potencia deben cumplir con las especificaciones de los fabricantes.
- El cableado de la red debe ser instalado y mantenido por personal calificado con el fin de garantizar su integridad.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 30 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Los conectores de pared no utilizados deben ser sellados y su estado debe ser formalmente registrado.
- Todo elemento que ingrese debe ser inspeccionado por la compañía de seguridad rigurosamente con el fin de identificar material peligroso y que coincida con su respectiva autorización de ingreso.
- Las áreas de descargue deben estar debidamente identificadas para evitar el acceso a las instalaciones por parte de terceros.
- Los materiales que deban entrar a las instalaciones deben ser inspeccionados debidamente en la zona de descargue, para evitar la entrada de elementos peligrosos a las áreas internas.
- El material entrante o saliente debe ser registrado, con el fin de mantener el listado de inventario actualizado.
- El uso de equipos de procesamiento de la información o software, fuera de las instalaciones de la Secretaría Distrital del Hábitat, debe ser autorizado por el Propietario de la Información de donde el empleado dependa. Esto aplica para computadores personales, agendas electrónicas, teléfonos móviles, etc.

### **RESPONSABILIDAD**

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

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

La instalación o reubicación de equipos de procesamiento o de telecomunicaciones, es responsabilidad única y exclusiva del Subsecretario(a) de Gestión Corporativa. Por lo tanto, los usuarios deben abstenerse de realizar modificaciones en los equipos, infraestructura de red o eléctrica.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 31 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

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

El proceso de bienes, servicios e infraestructura garantizará que todo personal interno y externo que ingrese a un área definida como segura por la SDHT, deberá poseer una identificación a la vista que claramente lo identifique como tal y estas identificaciones serán intransferibles.

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

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

El área de gestión tecnológica velará por que los medios de almacenamiento de información que se den de baja, sean destruidos físicamente o formateados de manera segura a través del uso de herramientas especiales que garanticen y verifiquen que no quede información remanente.

### **2.13. POLÍTICA DE ANTIVIRUS**

#### **OBJETIVO**

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

#### **ALCANCE**

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 32 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### **POLÍTICA**

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

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

- Ejecutar el antivirus al usar dispositivos como USB, CD, DVD.
- Verificar a través del software antivirus los archivos de computo que sean proporcionados por personal externo o interno como programas de software, bases de datos, documentos y hojas de cálculo que tengan que ser descomprimidos.
- No utilizar las facilidades de los exploradores WEB para ejecutar aplicaciones directamente.
- Abstenerse de escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para auto replicarse, dañar, o impedir el funcionamiento de cualquier recurso de procesamiento, archivos de sistema, o software.
- Abstenerse de conectar equipos personales que no contenga antivirus instalado y actualizado a la red de la SDHT.
- Al producirse un incidente se desconectará la estación de la red y se avisará inmediatamente de la presencia del malware para ser eliminado

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

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

### **RESPONSABILIDAD**

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

Los usuarios y terceras partes deberán cumplir con la Política.





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 33 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

### 2.14. POLÍTICA DE USO DE CORREO ELECTRÓNICO CORPORATIVO

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

La Secretaria Distrital del Hábitat, asigna a funcionarios y contratistas una cuenta de correo electrónico corporativa para ejercer sus funciones.

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

- Correos electrónicos no solicitados, sin relación con las actividades de la SDHT, que puedan ofender o causar inconvenientes a quienes lo reciban. Esto incluye el uso de listas de correo, cuando el e-mail enviado no está relacionado con el propósito para el cual la lista de correo utilizada fue creada (SPAM).



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 34 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Correos electrónicos no solicitados requiriéndole a otros usuarios en la Secretaría Distrital del Hábitat o cualquier lugar que continúe reenviando el mismo a otros.
- Correos electrónicos pretendiendo ser de una persona diferente del usuario que realmente envía el correo.
- Material, el cual pueda considerarse sexista, racista, homofóbico, xenofóbico, pornográfico, pedófilico o similarmente discriminatorio y/o ofensivo.
- Material que condene o promueva, directa o indirectamente, actividades criminales o que puedan dañar las actividades de la Secretaría Distrital del Hábitat.
- Texto o imágenes las cuales sean propiedad intelectual de terceros, sin el permiso escrito para dicha divulgación por parte del responsable.
- Material que pueda ser utilizado para vulnerar la seguridad de los computadores o para facilitar el acceso no autorizado a las mismas.
- Material que contenga datos personales de terceros, a menos que hayan dado su consentimiento de forma explícita.

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

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

La Secretaría Distrital del Hábitat se reserva el derecho a pedir las claves de encriptación, en caso de haber sido utilizadas, de acceder y navegar los contenidos del correo electrónico de



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 35 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

los usuarios de acuerdo con sus obligaciones legales y para legitimar los propósitos con los cuales se utiliza el sistema.

### **RESPONSABILIDAD**

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

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

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

### **2.15. POLÍTICA DE USO DE CONTRASEÑAS**

#### **OBJETIVO**

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

#### **ALCANCE**

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

#### **POLÍTICA**

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

- No contener el nombre de cuenta del usuario o partes del nombre completo del usuario en más de dos caracteres consecutivos.
- Tener una longitud mínima de 8 caracteres.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 36 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Incluir caracteres de tres de las siguientes categorías:
  - Mayúsculas (de la A a la Z)
  - Minúsculas (de la a a la z)
  - Dígitos de base 10 (del 0 al 9)
  - Caracteres no alfanuméricos (por ejemplo, !, \$, #, %).
- No repetir las últimas 3 contraseñas utilizadas anteriormente.
- No usar contraseñas por defecto o iguales al nombre de usuario o del perfil del usuario, nombres de familiares, amigos, mascotas, número de teléfono, números de documentos.
- No escribir la contraseña en papel o documentos electrónicos.
- No utilizar la misma contraseña para usos personales o formularios electrónicos.
- No revelar la contraseña de acceso a terceros de ningún sistema de la Secretaría Distrital del Hábitat (aplicativos, internet, correo o ingreso a la red).
- En caso de olvido de la contraseña, se deberá gestionar el cambio de la misma por medio del aplicativo de mesa de ayuda.

### **RESPONSABILIDAD**

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

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

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

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



## **2.16. POLÍTICA DE USO DE SERVICIOS DE RED**

### **OBJETIVO**

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

### **ALCANCE**

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

### **POLÍTICA**

La SDHT controlará el acceso a los servicios de red para garantizar que los usuarios que tengan acceso a las redes y a sus servicios no comprometan la seguridad de los mismos.

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

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

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

### **RESPONSABILIDAD**

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 38 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

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

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

### 2.17. POLÍTICA DE USO DE INTERNET

#### OBJETIVO

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

#### ALCANCE

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

#### POLÍTICA

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

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

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 39 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

Los usuarios que requieran acceso a través de protocolo FTP deberán ser explícitamente autorizados a este tipo de acceso por el Oficial de Seguridad de la Información.

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

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

- Acceso a sitios que puedan considerarse por su contenido sexista, racista, homofóbico, xenofóbico, pornográfico, pedofílico o similarmente discriminatorio y/u ofensivo.
- Acceso para audio o video en línea (TV, Radio, música, etc.).
- Acceso a sitios de juegos en red.
- Descarga de software sin autorización.
- Descarga de archivos de audio o video sin autorización.
- Realizar ataques sobre otros sitios, usuario o servidores.
- Brindar servicios externos desde el puesto de trabajo.
- Acceso a sitios que reproduzcan en forma no autorizada material protegido por los derechos de autor.
- Acceso a sitios que provean instrucciones o claves para utilizar o acceder a software, servicios o sitios en forma ilegal (piratería).

Los usuarios no podrán transferir o publicar información de propiedad de la Secretaría Distrital del Hábitat.

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

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

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

Se permite a los usuarios acceder a Internet para los siguientes usos:

- Acceso a sitios sobre noticias (diarios, radios, agencias, etc.).
- Acceso a Sistemas Bancarios.
- Acceso a Sistemas de Pago Electrónico de servicios.
- Acceso a Sistemas de información sobre transportes, mapas, espectáculos, hotelería.



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

## **RESPONSABILIDAD**

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

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

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

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

#### **OBJETIVO**

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

#### **ALCANCE**

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

#### **POLÍTICA**

La Secretaria Distrital del Hábitat garantiza el acceso por VPN con los protocolos adoptados y adoptando los siguientes controles:

- Uso de encriptación acorde a la criticidad del acceso, y acorde a lo establecido en las políticas relacionadas.





- Establecer niveles de servicio que contemplen los tiempos de mantenimientos y Backup.
- Registrar las acciones de inicio y final de conexión con los datos correspondientes al usuario, dirección IP.
- Disponer de estadísticas periódicas de utilización por usuario.

## **RESPONSABILIDAD**

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

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

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

## **2.19. POLÍTICA DE CONTROL DE CAMBIOS**

### **OBJETIVO**

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

### **ALCANCE**

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

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 42 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### **POLÍTICA**

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

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

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

Los servidores propietarios y/o encargados de los recursos de procesamiento y de comunicaciones, deben realizar las solicitudes de cambio por medio del aplicativo de mesa de ayuda y los procedimientos PS05-PR06 Control de cambio a sistemas de información, aplicativos e infraestructura y PS05-PR07 de pase a producción de sistemas de información.

### **RESPONSABILIDAD**

- El(la) Subsecretario(a) de Gestión Corporativa, el Oficial de Seguridad de la Información y/o el responsable de Gestión Tecnológica definen y aprueban las normas y procedimientos para la gestión del cambio, el personal responsable de Gestión Tecnológica y los responsables de los activos implementan los cambios.
- Los usuarios y terceras partes deberán cumplir con los lineamientos establecidos en esta política.
- Los servidores públicos, contratistas y/o terceros encargados de los recursos de procesamiento y de comunicaciones deberán velar porque la información sea almacenada conforme a los lineamientos establecidos, antes de realizarse algún cambio que pueda afectar la información contenida en los recursos descritos anteriormente y de acuerdo con las necesidades de la Secretaría Distrital del Hábitat.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE HÁBITAT	<b>MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  GESTIÓN DE  SEGURIDAD DE LA INFORMACIÓN</b>	Página 43 de 73
		VERSIÓN 4
		Fecha 2018/09/26
		Código PS05-MM13

## **2.20. POLÍTICA DE PROPIEDAD INTELECTUAL**

### **OBJETIVO**

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

### **ALCANCE**

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

### **POLÍTICA**

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

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

Se garantizará la protección de la propiedad intelectual de software de acuerdo con el marco legal de productos de información y de software, así como el mantenimiento de las licencias.

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



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 44 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### RESPONSABILIDAD

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

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

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

### 3 POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN SECRETARÍA DISTRITAL DEL HÁBITAT

La Secretaría Distrital del Hábitat en cumplimiento de lo dispuesto en la Ley Estatutaria 1581 del 17 de octubre de 2012 y el Decreto 1377 del 27 de junio de 2013, expedido por el Presidente de la República, adopta la Política para el Tratamiento de la Información que se presenta a continuación, que aplicará en la Entidad.

#### I. IDENTIFICACIÓN DE LA ENTIDAD

La Secretaría Distrital del Hábitat es un organismo del Sector Central, con autonomía administrativa y financiera, con domicilio en la ciudad de Bogotá D.C., cuya oficina principal se encuentra ubicada en la Calle 52 N° 13-64, con código postal 110231, dirección web [www.habitatbogota.gov.co](http://www.habitatbogota.gov.co), número del conmutador (1) 3581600 y correo electrónico [serviciociudadano@habitatbogota.gov.co](mailto:serviciociudadano@habitatbogota.gov.co).

#### II. MARCO LEGAL DE LA POLÍTICA

El marco normativo de la Política de Tratamiento de la Información, que la Secretaría del Hábitat adopta, se integra por:



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 45 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Constitución Política de Colombia, artículos 15 y 20.
- Ley 594 de 2000 *“por medio de la cual se dicta la Ley General de Archivos y de dictan otras disposiciones”*.
- Ley 734 *“por la cual se expide el Código Disciplinario Único”*.
- Ley 962 de 2005 *“por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos”*.
- Ley Estatutaria 1266 de 2008 *“por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”*.
- Ley 1341 de 2009 *“por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones”*.
- Ley 1273 de 2009 *“por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado -denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunidades, entre otras disposiciones”*.
- Ley 1437 de 2011 *“por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo”*.
- Ley 1450 de 2011 *“por la cual se expide el Plan Nacional de Desarrollo, 2010-2014”*.
- Ley 1474 de 2011 *“por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública”*.
- Directiva 022 del 27 de diciembre de 2011 *“Estandarización de la información de identificación, caracterización, ubicación y contacto de los ciudadanos y ciudadanas que capturan las entidades del Distrito Capital”*, emitida por la Alcaldía Mayor.
- Ley Estatutaria 1581 de 2012 *“por la cual se dictan disposiciones generales para la protección de datos personales”*.
- Decreto 1377 de 2013 *“por el cual se reglamenta parcialmente la Ley 1581 de 2012”*, proferido por la Presidencia de la República.
- Circular 94 de agosto 22 de 2013 *“Actualización de políticas – marco general sobre la protección de datos personales. Implementación y cumplimiento del Decreto 1377 de 2013 “por la cual se reglamenta parcialmente la Ley 1581 de 2012”, emitida por la Secretaría General.*
- Ley 1712 de 2014 *“por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”*.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 46 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- Decreto 2573 de 2014 “*por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones*” proferido por la Presidencia de la República.
- Decreto 103 de 2015 “*por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones*”, proferido por la Presidencia de la República.
- Ley 1753 del 9 de junio de 2015 “*Por la cual se expide el Plan nacional de Desarrollo 2014-2018 ‘Todos por un nuevo país’*”.
- Decreto 1008 de 2018, “*Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones*”.

### PRINCIPIOS

La Política de Tratamiento de la Información de la Secretaría Distrital del Hábitat se orientará, de manera armónica e integral, por los siguientes principios:

- **LEGALIDAD EN MATERIA DE TRATAMIENTO DE DATOS.** El Tratamiento de los datos personales que el Titular autorice es una actividad reglada que se sujeta a lo establecido en las leyes y las demás disposiciones normativas que las desarrollen.
- **FINALIDAD.** El Tratamiento de los datos personales, que el Titular autorice, debe obedecer a una finalidad legítima acorde con la Constitución y las leyes; ésta debe informársele a los Titulares de la información de manera previa o concomitante con el otorgamiento de la autorización, cuando sea necesario o cuando el Titular solicite información al respecto.
- **LIBERTAD.** El Tratamiento de los datos personales sólo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenida o divulgada sin autorización previa o en ausencia de mandato legal o judicial que releve el consentimiento.
- **VERACIDAD O CALIDAD.** La información contenida en las bases de datos y/o sometida a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible; está prohibido el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 47 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- **TRANSPARENCIA.** En cualquier momento del Tratamiento de los datos personales, se debe garantizar al Titular el derecho a solicitar información acerca de la existencia de datos que le conciernan, la cual se le suministrará sin restricciones por parte del responsable o el encargado del Tratamiento.
- **SEGURIDAD.** La información sujeta a Tratamiento, así como la que resulte de las consultas que de ella hagan los usuarios, se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para garantizar la seguridad de los registros evitando su adulteración, pérdida, consulta o uso no autorizado o fraudulento.
- **CONFIDENCIALIDAD.** Todas las personas naturales o jurídicas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos, están obligadas a garantizar, en todo tiempo, la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento de los datos, pudiendo sólo transmitirlos, transferirlos, suministrarlos o comunicarlos cuando dicha operación corresponda al desarrollo de las actividades autorizadas por la ley y en los términos de la misma.
- **TEMPORALIDAD.** Los datos personales del Titular no podrán ser suministrada a usuarios o terceros cuando deje de servir para la finalidad de la base de datos que se le informó al Titular al momento de obtener su autorización.
- **ACCESO Y CIRCULACIÓN RESTRINGIDA:** El Tratamiento de los datos personales se sujeta a los límites que se derivan de la naturaleza de los mismos, de las disposiciones de la ley y la Constitución. El Tratamiento sólo podrá realizarse por personas autorizadas por el Titular y/o por las personas previstas en la ley. Los datos personales, salvo la información pública, no podrán estar disponibles en internet o cualquier otro medio de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido a los Titulares o terceros autorizados conforme a la ley.

**INTERPRETACIÓN INTEGRAL DE DERECHOS CONSTITUCIONALES.** La presente política y las leyes se interpretarán en el sentido en que se amparen adecuadamente los derechos constitucionales de los Titulares, como son el hábeas data, el buen nombre, la honra, la

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE HÁBITAT	<b>MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  GESTIÓN DE  SEGURIDAD DE LA INFORMACIÓN</b>	Página 48 de 73
		VERSIÓN 4
		Fecha 2018/09/26
		Código PS05-MM13

intimidad y a la información. Los derechos de los Titulares se interpretarán en armonía y de manera equilibrada con el derecho a la información previsto en el artículo 20 de la Constitución y con los demás derechos constitucionales aplicables.

### **III. DERECHOS DE LOS TITULARES**

El Titular de los datos personales tiene los siguientes derechos:

1. Conocer, actualizar y rectificar sus datos personales frente a los Responsables del Tratamiento o Encargados del Tratamiento de la Secretaría Distrital del Hábitat. Este derecho se podrá ejercer, entre otros, frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo Tratamiento esté expresamente prohibido o no haya sido autorizado.
2. Solicitar prueba de la autorización otorgada a los Responsables del Tratamiento o Encargados del Tratamiento de la Secretaría Distrital del Hábitat, salvo cuando expresamente se exceptúe como requisito para el Tratamiento, de conformidad con las leyes.
3. Solicitar y obtener información respecto del uso que se le ha dado a sus datos personales por parte de la Secretaría Distrital del Hábitat.
4. Presentar quejas ante las autoridades competentes por infracciones a lo dispuesto en las leyes y normas relativas al Tratamiento de datos personales.
5. Revocar la autorización y/o solicitar la supresión del dato cuando en el Tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la autoridad competente haya determinado que en el Tratamiento la Secretaría Distrital del Hábitat haya incurrido en conductas contrarias a la ley o la Constitución.
6. Acceder en forma gratuita a los datos personales que hayan sido objeto de Tratamiento.
7. Ejercer el derecho fundamental del hábeas data en los términos de la ley, utilizando los procedimientos de consultas o reclamos sin perjuicio de los demás mecanismos constitucionales o legales.
8. Solicitar el respeto y la protección de los demás derechos constitucionales relacionados con el manejo de la información personal, utilizando el procedimiento de reclamos y peticiones.
9. Asegurar el respeto a los derechos prevalentes de los niños, niñas y adolescentes durante el Tratamiento. Está prohibido el Tratamiento de datos personales de niños, niñas y adolescentes salvo que se trate de datos públicos y que responda o respete el





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 49 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

interés superior de los niños, niñas y adolescentes, se asegure el respeto de sus derechos fundamentales y se cuente con autorización por parte de su representante legal luego de ser escuchada su opinión de acuerdo con su madurez, capacidad y autonomía.

Estos derechos podrán ejercerse por el Titular, sus causahabientes, el representante o apoderado del Titular, siempre y cuando acrediten suficientemente su calidad, también puede hacerse por estipulación a favor de otro o para otro. Para el caso de menores únicamente se podrán ejercer por las personas que están facultadas para representarlos.

#### IV. DEBERES DE LA SECRETARÍA DISTRITAL DEL HÁBITAT

La Secretaría Distrital del Hábitat, en el marco de la política de manejo de la información, asume los siguientes deberes:

##### a) COMO RESPONSABLE DEL TRATAMIENTO

1. Garantizar al Titular el ejercicio pleno y efectivo del derecho de hábeas data en cualquier tiempo.
2. Solicitar y conservar copia de la autorización otorgada por el Titular, de acuerdo con las condiciones establecidas en las normas.
3. Informar al Titular sobre la finalidad de la recolección de los datos y los derechos que le asisten en virtud de la autorización otorgada.
4. Conservar la información bajo condiciones de seguridad que impidan su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información que le suministra al encargado del Tratamiento es veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar la información y comunicar al encargado del Tratamiento sobre las novedades que se reporten frente a los datos que previamente le haya suministrado.
7. Adoptar medidas para que la información que se suministra al encargado del Tratamiento se mantenga actualizada.
8. Realizar las rectificaciones de la información cuando se detecte o informe que es incorrecta, comunicarle esta novedad al encargado del Tratamiento.
9. Transferir y transmitir únicamente datos cuyo Tratamiento esté previamente autorizado.
10. Exigir el respeto a las condiciones de seguridad y privacidad de la información del Titular a los encargados del Tratamiento y a los usuarios.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 50 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

11. Dar trámite a las consultas y reclamos formulados en los términos señalados por la ley.
12. Informar al encargado del Tratamiento cuando un dato se encuentre en discusión por parte del Titular, una vez se haya presentado reclamación y no haya finalizado su trámite.
13. Ajustar y/o diseñar los procedimientos y formatos a que haya lugar en la Secretaría Distrital del Hábitat para garantizar el adecuado cumplimiento del presente documento y en especial, para la atención de consultas y reclamos.
14. Informar al Titular sobre el uso dado a sus datos.
15. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración y/o manejo de la información de los Titulares.
16. Seguir las instrucciones y atender los requerimientos que impartan las autoridades competentes en materia de manejo de la información y protección de datos.

### **b) COMO ENCARGADA DEL TRATAMIENTO**

1. Garantizar al Titular el ejercicio pleno y efectivo del derecho de hábeas data en cualquier tiempo.
2. Conservar la información bajo condiciones de seguridad para impedir la adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
3. Realizar de manera oportuna las actualizaciones, rectificaciones o supresiones de los datos de acuerdo con los términos de las leyes.
4. Actualizar la información reportada por los responsables del Tratamiento dentro de los cinco (5) días hábiles contados a partir de su recibo.
5. Tramitar las consultas y los reclamos formulados por los Titulares en los términos señalados en las leyes.
6. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y, en especial, para la atención de consultas y reclamos por parte de los Titulares.
7. Registrar en la base de datos la anotación “reclamo en trámite” de acuerdo con lo regulado en la ley.
8. Incluir en la base de datos la anotación “información en discusión judicial” una vez sea notificado por la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
9. Abstenerse de circular información que esté siendo controvertida por el Titular y cuyo bloqueo haya sido ordenado por autoridad competente.
10. Permitir el acceso a la información únicamente a las personas autorizadas.
11. Informar a la autoridad competente la ocurrencia de violaciones a los códigos de seguridad y la existencia de riesgos en la administración de la información de los Titulares.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 51 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

12. Atender las instrucciones y requerimientos que impartan las autoridades competentes en materia de manejo de la información y protección de datos.

### c) COMO FUENTE DE INFORMACIÓN

1. Garantizar que la información que se suministra a los operadores de bancos de datos, los responsables del Tratamiento, los encargados del Tratamiento y los usuarios sea veraz, completa, exacta, actualizada y comprobable.
2. Reportar periódica y oportunamente las novedades respecto de los datos que previamente haya suministrado.
3. Adoptar medidas para que la información que suministra se mantenga actualizada.
4. Rectificar la información cuando sea incorrecta e informar lo pertinente a los responsables del Tratamiento, los operadores del Tratamiento, los operadores o los usuarios.
5. Diseñar e implementar mecanismos eficaces para reportar oportunamente la información a los responsables del Tratamiento, los operadores de la información, los encargados del Tratamiento y los usuarios.
6. Solicitar, cuando aplique, y conservar copia o evidencia de la autorización otorgada por el Titular de la información y asegurarse de no suministrar a los operadores ningún dato cuyo suministro no esté previamente autorizado cuando la ley exija que medie autorización para la obtención y Tratamiento de esos datos.
7. Certificar periódicamente que la información suministrada cuenta con la autorización que la ley exige.
8. Resolver reclamos y peticiones de los Titulares de acuerdo con lo que disponen las leyes.
9. Informar al responsable, el encargado o el operador de la información sobre la existencia de solicitudes de rectificación o actualización de la misma para que se incluya la anotación correspondiente en la base de datos hasta que el trámite finalice.
10. Seguir las instrucciones que imparta la autoridad de control en relación con el cumplimiento de las normas relacionadas con el hábeas data y el manejo de la información.

### d) COMO USUARIA DE LA INFORMACIÓN

1. Guardar reserva sobre la información que les sea suministrada por los operadores, las fuentes de información, los responsables y encargados del Tratamiento.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 52 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

2. Utilizar la información a la que tiene acceso únicamente para los fines para los que le fue entregada y en los términos de las leyes.
3. Informar a los Titulares sobre la utilización que le está dando a la información, cuando estos lo requieran.
4. Conservar la información recibida con las medidas de seguridad para impedir su deterioro, pérdida, adulteración, uso no autorizado o fraudulento.
5. Seguir las instrucciones que imparta la autoridad de control en materia del cumplimiento de las normas relacionadas con el hábeas data y el manejo de la información.

### e) **COMO OPERADOR DE LA INFORMACIÓN**

1. Garantizar al Titular de la información el ejercicio pleno y efectivo del derecho de hábeas data y de petición en cualquier tiempo, brindándole la posibilidad de conocer la información que sobre él exista o repose en las bases de datos y de solicitar que esta se actualice o corrija, para esto dispondrá de herramientas para las consultas y reclamos conforme a lo previsto en las leyes.
2. Garantizar que en la recolección, Tratamiento y circulación de datos se respetarán los derechos constitucionales de la persona.
3. Permitir el acceso a la información únicamente a las personas que puedan tener acceso a ella de conformidad con las leyes.
4. Adoptar un manual interno de políticas y procedimiento para garantizar el adecuado cumplimiento de la presente ley y para la atención de consultas y reclamos por parte de los Titulares.
5. Solicitar certificación sobre la existencia de la autorización otorgada por el Titular a la fuente de la información o al responsable del Tratamiento cuando esta sea necesaria conforme a la ley.
6. Conservar los registros almacenados con las medidas de seguridad adecuadas para impedir su deterioro, pérdida, alteración, uso no autorizado o fraudulento.
7. Realizar la actualización y rectificación de los datos de manera periódica y oportuna cada vez que le sean reportadas novedades.
8. Dar trámite a las peticiones, consultas y reclamaciones formuladas por los Titulares en los términos señalados por las leyes.
9. Indicar en el registro individual de la base de datos cuándo la información, que está siendo objeto de Tratamiento o consulta, se encuentra en discusión por parte del Titular debido a una solicitud de rectificación o actualización de esta mientras el trámite no haya finalizado.
10. Permitir el acceso a la información por parte de los usuarios dentro de los parámetros fijados por las leyes.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 53 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

11. Atender los requerimientos y seguir las instrucciones y requerimientos que impartan las autoridades de vigilancia en materia de manejo de la información.

## **V. AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES**

Para la recolección y el Tratamiento de datos personales se exige que la persona natural, Titular de la información, manifieste de manera previa y expresa su consentimiento para que la Secretaría Distrital del Hábitat, a través de sus dependencias, realice el Tratamiento de sus datos. Este consentimiento se consolida en la autorización.

La autorización que se requiere del Titular busca que la persona y la Secretaría Distrital del Hábitat tengan claridad en cuanto a los datos que se van a obtener, el uso que se les dará, la posibilidad de que estos sean transmitidos, transferidos o consultados por otras entidades, el tiempo que estos datos permanecerán en las bases de datos, la finalidad de su recolección y conservación.

En consonancia con lo anterior y en desarrollo de los principios de finalidad y libertad, los datos que se recolecten deben ser únicamente los pertinentes y adecuados para los fines que se persiguen, por esto los jefes de las dependencias que tienen a su cargo la recolección de datos personales para alimentar bases de datos dentro de la Secretaría Distrital del Hábitat, deberán definir cuál es la finalidad de este recaudo de manera clara y concreta y exponer las razones por las cuales esos datos son necesarios para cada caso.

En caso de que se realice algún cambio en el contenido de la presente política o en las finalidades del Tratamiento de los datos personales se deberá solicitar una nueva autorización antes de implementarlos.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 54 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

En cada dependencia en la que se utilicen bases de datos cuyo Tratamiento o consulta requiera autorización, se deberá definir si dentro de los datos que se necesitan están aquellos definidos como sensibles.

### **DATOS SENSIBLES**

Para el Tratamiento de los datos sensibles se requerirá una autorización explícita por parte del Titular, salvo que la ley indique que esta no será necesaria; para obtenerla se deberá informar al Titular que por la naturaleza de los datos no está obligado a autorizar su Tratamiento, cuáles son los datos sensibles que se están recolectando, cuál será la finalidad de la recolección de sus datos y el Tratamiento que tendrán. En ningún caso se podrán imponer condiciones al Titular para obtener su consentimiento para que suministre datos sensibles.

Se permite el Tratamiento de datos sensibles cuando sean necesarios para salvaguardar el interés vital del Titular y se encuentre incapacitado física o jurídicamente, caso en el que será el representante legal el que otorgue la autorización. Estos datos no podrán suministrarse a terceros sin autorización del Titular o su representante.

Cuando los datos sensibles sean necesarios para el reconocimiento, ejercicio o defensa de un derecho dentro de un proceso judicial, se permitirá su uso siempre que se cuente con autorización expresa del Titular o su representante en caso de incapacidad; también se permitirá su uso cuando el Tratamiento tenga una finalidad estadística, histórica o científica pero las dependencias deberán definir y adoptar medidas para la supresión de la identidad de los Titulares.

### **DATOS DE MENORES DE EDAD**



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 55 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

Cuando se trate de datos personales de niños, niñas y adolescentes, se asegurará el respecto de sus derechos. Por regla general está prohibido el Tratamiento de sus datos personales salvo aquellos de naturaleza pública, sin embargo, este se permite cuando el Tratamiento responda y respete el interés superior de los niños, niñas y adolescentes y se asegure el respeto de sus derechos fundamentales. En ese caso, se debe obtener la autorización por parte del representante legal del menor luego de escuchar su opinión tomando en cuenta su madurez, autonomía y capacidad para entender el asunto.

### **FORMATO PARA LA AUTORIZACIÓN**

Cada responsable del Tratamiento de la información deberá definir los formatos que se emplearán para obtener la autorización de los Titulares, para esto tendrán en cuenta la finalidad de la información, la clase de datos que requiere, utilizará un lenguaje claro y adecuado para la población a la que se dirigirá, estos formatos deberán surtir el trámite de aprobación del Sistema de Gestión Documental y se incluirá en las respectivas Tablas de Retención Documental.

La autorización también se puede obtener mediante mecanismos predeterminados usando medios técnicos que faciliten la manifestación automatizada al Titular.

Para que se entienda que la autorización cumple con los requisitos legales debe haber una manifestación escrita, oral o mediante conductas inequívocas del Titular que permitan concluir de forma razonable que se otorgó la autorización, el silencio no es una conducta inequívoca.

En las dependencias de la Secretaría Distrital del Hábitat se preferirá la manifestación escrita de la autorización debido a la facilidad de la conservación de este medio de prueba, sin embargo, en los casos en los que se haya obtenido de manera verbal se entenderá correctamente autorizado y se dejará constancia de ellos indicando la fecha, hora y lugar en que el Titular manifestó su voluntad frente al Tratamiento de sus datos personales. Cuando se trate de datos personales de menores o incapaces, se requerirá que esta siempre conste por escrito.

Es deber del responsable del Tratamiento indicarle al Titular al momento del otorgamiento de la autorización que podrá revocarla y cuál será el procedimiento para la supresión de sus datos de las bases que se administran por la Secretaría Distrital del Hábitat, para eso se



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 56 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

recomienda incluir esta información en los formatos que se adopten para obtener la autorización.

### **REVOCATORIA DE LA AUTORIZACIÓN**

La solicitud de supresión de la información y la revocatoria de la autorización no procederán cuando el Titular tenga un deber legal o contractual de permanecer en la base de datos.

Una vez se reciba la solicitud de revocatoria de la autorización se procederá a su estudio en el menor tiempo posible dentro de los tiempos legalmente definidos y, de ser el caso, a la supresión de la información de la base de datos a la que se refiera la autorización.

### **EXCEPCIONES AL DEBER DE OBTENER LA AUTORIZACIÓN**

No se requiere autorización cuando se trate de datos personales que se encuentren en fuentes de acceso público, independientemente del medio por el cual se tenga acceso, siempre que se trate de datos públicos. Tampoco cuando se trate de información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial, se trate de un caso de urgencia médica o sanitaria, el Tratamiento de la información haya sido autorizado legalmente con fines históricos, estadísticos o científicos, o sean datos relacionados con el registro civil de las personas.

### **AVISO DE PRIVACIDAD**

Cuando no sea posible poner a disposición del Titular las políticas de Tratamiento de la información, los responsables del Tratamiento informarán al Titular, mediante un aviso de privacidad, sobre la existencia de estas políticas y la forma en que podrá acceder a las mismas de manera oportuna y a más tardar al momento de la recolección de los datos personales.





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 57 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

Este aviso de privacidad debe contener como mínimo el nombre o razón social del responsable, los datos de contacto del mismo, el Tratamiento al cual se someterán los datos y la finalidad de este, los derechos que tiene el Titular y los mecanismos dispuestos para que conozca la política de Tratamiento de la información, así como los cambios que se realicen.

Cuando se trate de datos sensibles, el aviso de privacidad deberá señalar de manera expresa el carácter facultativo de la respuesta a las preguntas que versen sobre este tipo de datos, esto no exime al responsable, como representante de la Secretaría Distrital del Hábitat, de dar a conocer la política de Tratamiento de la información que se ha adoptado.

El aviso de privacidad y la autorización deberá conservarse mientras perduren las obligaciones que de estos deriven, para lo cual podrán emplearse medios de almacenamiento electrónicos, informáticos o tecnológicos.

### VI. TRATAMIENTO DE LA INFORMACIÓN

#### RESPONSABLE DEL TRATAMIENTO DE LA INFORMACIÓN EN LA SECRETARÍA DISTRITAL DEL HÁBITAT

El jefe de cada dependencia será el responsable del Tratamiento de la información, en ese sentido, deberá definir quién o quiénes serán los encargados del Tratamiento y adoptar los procedimientos para solicitar la autorización de parte del Titular de los datos personales que se requieran.

#### SUMINISTRO

La información que reúna las condiciones establecidas por las normas de protección de datos personales podrá suministrarse a: i) Los Titulares, sus causahabientes o sus representantes legales; ii) Las entidades públicas o administrativas en el ejercicio de sus funciones legales o por orden judicial; iii) los terceros autorizados por el Titular o la ley.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 58 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

La información solicitada podrá ser suministrada por cualquier medio, incluyendo los electrónicos, según lo requiera el Titular; deberá ser de fácil lectura, sin barreras técnicas que impidan su acceso, y deberá corresponder en todo a aquella que repose en la base de datos.

### CONSULTA

La información personal del Titular que repose en la base de datos se podrá consultar por los Titulares, sus causahabientes y los usuarios autorizados. El encargado del Tratamiento permitirá la consulta de toda la información contenida en el registro individual o que esté vinculada con la identificación del Titular. La consulta se formulará por el medio que el responsable del Tratamiento habilite, siempre y cuando se pueda conservar prueba de esta; será atendida en un término máximo de diez (10) días hábiles a partir de la fecha de recibo de la misma, en caso de que no sea posible atender la consulta en este tiempo se informará al interesado expresando los motivos de la demora y la fecha en que será atendida la consulta, que no podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

### CIRCULACIÓN

La información personal recolectada o suministrada de conformidad con lo dispuesto en las leyes de protección de datos personales podrá ser entregada de manera verbal, escrita o puesta a disposición de: i) los Titulares y las personas debidamente autorizadas por estos, así como a sus causahabientes, mediante el procedimiento de consulta; ii) a los usuarios de la información dentro de los parámetros legales; iii) a las autoridades judiciales previa orden judicial; iv) a las entidades públicas del poder ejecutivo cuando conocer dicha información corresponda al cumplimiento de sus funciones; v) a los órganos de control y demás dependencias de investigación disciplinaria, fiscal o administrativa, cuando esta sea necesaria para el desarrollo de una investigación en curso; vi) a otros operadores de datos cuando medie autorización del Titular o cuando el banco de datos de destino tenga la misma finalidad que la que tiene el operador que entrega el dato o una finalidad que la comprenda; vii) a las personas que sean autorizadas por la ley.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 59 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### **TRANSFERENCIA**

Se permite la transferencia de datos personales a países que proporcionen niveles adecuados de protección de datos de acuerdo con los estándares fijados por la Autoridad de Protección de Datos sobre la materia, que en ningún caso podrán ser inferiores a los que la normatividad nacional establece; la transferencia a países que no acrediten estos estándares está prohibida, salvo que se trate de: i) información cuya transferencia haya sido expresa e inequívocamente autorizada por el Titular; ii) intercambio de datos de carácter médico por razones de salud o higiene pública y así lo exija el Tratamiento del Titular; iii) transferencias bancarias o bursátiles conforme a la legislación aplicable; iv) transferencias acordadas en el marco de tratados internacionales en los que la República de Colombia sea parte y con fundamento en el principio de reciprocidad; v) transferencias necesarias para la ejecución de un contrato entre el Titular y la Secretaría Distrital del Hábitat, o para la ejecución de medidas precontractuales siempre que se cuente con autorización del Titular; vi) transferencias legalmente exigidas para la salvaguardia del interés público, o para el ejercicio, reconocimiento o defensa de un derecho dentro de un proceso judicial.

### **TRANSMISIÓN**

La transmisión de datos personales dentro del Tratamiento de la información implica la comunicación de los datos suministrados y autorizados por el Titular, para que quien los reciba realice un nuevo Tratamiento con los datos que le han sido remitidos. La transmisión debe ser autorizada por el Titular y la Secretaría Distrital del Hábitat, a través de los responsables, debe informarle a cuáles entidades pueden ser transmitidos sus datos y cuál será la finalidad de dicha transmisión.

Las transmisiones internacionales de datos personales que se efectúen entre la Secretaría Distrital del Hábitat y un encargado para permitir que este realice el Tratamiento por cuenta de la entidad, no requerirán ser informadas al Titular ni contar con su consentimiento cuando la relación se de en el marco de un contrato de transmisión de datos personales.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 60 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

El contrato de transmisión de datos personales que suscriba la Secretaría Distrital del Hábitat, en su rol de responsable del Tratamiento, con una persona natural o jurídica que se desempeñe como encargada para adelantar el Tratamiento de datos personales bajo el control y responsabilidad de la entidad, contendrá la delimitación del alcance del Tratamiento, las actividades que el encargado está autorizado a realizar, se definirán las obligaciones de ambas partes con el Titular de la información y se comprometerán a dar aplicación a la presente política de Tratamiento de la información ajustándose a los límites definidos por el Titular al momento de entregar sus datos personales.

## **VII. PROCEDIMIENTO PARA EL EJERCICIO DE LOS DERECHOS DEL TITULAR**

### **TRÁMITE DE CONSULTAS, QUEJAS Y/O RECLAMOS**

Los Titulares de la información, sus causahabientes o representantes legales formularán la petición de consulta por escrito de acuerdo a la estructura del formato que cada dependencia responsable del Tratamiento defina, de esta solicitud se conservará la evidencia por los medios técnicos que se definan en el análisis de retención documental. En dicho formato se requerirá la identificación completa del Titular de la información que se solicita y la acreditación de la calidad en que hace la solicitud.

La petición deberá ser radicada en la oficina de Correspondencia de la Secretaría Distrital del Hábitat y será dirigida al Defensor del Ciudadano de la Entidad, quien la remitirá al responsable del Tratamiento inmediatamente para que la atienda, el término para dar respuesta de fondo a la solicitud es de diez (10) días hábiles contados a partir de la fecha de recibo de la solicitud. En caso de que se requiera tiempo adicional, se deberá comunicar esta circunstancia al solicitante expresando los motivos por los cuales se da la demora y la fecha en que se atenderá la petición, la extensión de tiempo no podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término.

El Titular podrá consultar de forma gratuita sus datos personales al menos una vez cada mes calendario y cada vez que existan modificaciones sustanciales de las políticas de Tratamiento de la información que motiven nuevas consultas.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE HÁBITAT</p>	<b>MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN</b>	Página 61 de 73
		VERSIÓN 4
		Fecha 2018/09/26
		Código PS05-MM13

## **TRÁMITE DE RECLAMACIONES**

Los Titulares de la información, sus causahabientes o representantes legales, que consideren que la información contenida en el registro individual de la base de datos debe ser objeto de corrección o actualización podrán presentar reclamaciones formuladas por escrito dirigido a la Oficina de Atención al Ciudadano de la Secretaría Distrital del Hábitat.

Para las reclamaciones se requerirá que el solicitante indique como mínimo la identificación del Titular, la descripción breve y clara de los hechos que dan lugar al reclamo, la dirección de comunicaciones del solicitante y, en caso de ser necesario, los anexos que soporten la solicitud. En caso de que el escrito resulte incompleto se oficiará al interesado para que subsane las fallas, transcurrido un mes desde la fecha del requerimiento sin que el solicitante presente la información requerida se entenderá que ha desistido del trámite.

Una vez recibida la solicitud completa, el responsable le informará al encargado del Tratamiento para que incluya en la base de datos la anotación “reclamo en trámite” y la naturaleza del mismo, en un término no mayor a dos (2) días hábiles. Esta anotación deberá mantenerse hasta que la reclamación haya sido decidida y se incluirá en la información que se suministra a los usuarios.

Las reclamaciones se atenderán en un término de quince (15) días hábiles contados a partir de la fecha de recibo de la solicitud completa; cuando no sea posible atender la reclamación dentro de este término se informará al solicitante, expresando los motivos de la demora y señalando la fecha en que se dará respuesta a la petición, que no podrá superar los ocho (8) días hábiles siguientes a la fecha del vencimiento del primer término.

Cuando la información cuya reclamación se solicita provenga de una fuente diferente a la Secretaría Distrital del Hábitat, se dará traslado del reclamo a la fuente en un término máximo de dos (2) días hábiles, la cual deberá resolver e informar la respuesta a la Secretaría Distrital del Hábitat en un plazo máximo de diez (10) días hábiles, la respuesta deberá darse al Titular por parte de esta entidad en el plazo máximo de quince (15) días hábiles prorrogables por ocho (8) días hábiles más, de acuerdo con el trámite legalmente establecido.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 62 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

Si la reclamación se radica directamente en la fuente de la información, cuando sea diferente a la Secretaría Distrital del Hábitat, procederá a resolver directamente el reclamo pero deberá informarle a esta entidad sobre la recepción de la reclamación dentro de los dos (2) días hábiles siguientes a su recibo para que se pueda incluir la anotación de “reclamo en trámite” dentro de la base de datos, lo cual se deberá hacer dentro de los dos (2) días hábiles siguientes al recibo de la comunicación por parte de la fuente.

Para dar respuesta a las reclamaciones se realizará una verificación completa de las observaciones hechas por el Titular, asegurándose de revisar toda la información pertinente para dar una respuesta completa al solicitante.

En caso de que el solicitante no se encuentre satisfecho con la respuesta a la petición, podrá recurrir al proceso judicial correspondiente para debatir lo relacionado con la obligación reportada como incumplida, sin perjuicio del ejercicio de la acción de tutela para amparar el derecho fundamental del hábeas data. La acción deberá estar dirigida contra la fuente de la información la cual, una vez notificada, procederá a informar al operador, responsable y encargado del Tratamiento para que incluya la anotación “información en discusión judicial” y la naturaleza de la misma dentro de la base de datos, esta información deberá remitirla dentro de los dos (2) días hábiles siguientes a la notificación y el encargado del Tratamiento la incluirá en la base de datos dentro de los dos (2) días hábiles siguientes a la recepción de la información por parte del responsable. La anotación se mantendrá por todo el tiempo que dure el proceso y hasta que se tenga un fallo en firme. El mismo procedimiento se seguirá cuando la fuente de la información inicie un proceso judicial contra el Titular de los datos personales con ocasión de la información suministrada.

El Titular, su causahabiente o el representante legal, sólo podrá elevar quejas ante la autoridad de protección de datos por violaciones al régimen de Tratamiento de la información, cuando haya agotado el trámite de reclamación o consulta ante el responsable del Tratamiento o la fuente de la información, según sea el caso.

### **VIII. TRATAMIENTO DE DATOS RECOLECTADOS CON ANTELACIÓN A LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN**



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HÁBITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 63 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

Para el Tratamiento de los datos recolectados por la Secretaría Distrital del Hábitat con anterioridad a la presente política se procederá de la siguiente manera:

Los responsables del Tratamiento deberán solicitar la autorización de los Titulares para continuar con el Tratamiento de sus datos personales, para eso utilizará mecanismos eficientes de comunicación y podrán en conocimiento de estos la existencia de la política de Tratamiento de la información adoptada por la entidad y los mecanismos para ejercer sus derechos.

Se considerarán mecanismos eficientes de comunicación, aquellos en los que el responsable o el encargado del Tratamiento usan en el curso ordinario de su interacción con los Titulares registrados en sus bases de datos. Si estos mecanismos imponen al responsable una carga desproporcionada o resulta imposible solicitar a cada Titular el consentimiento para el Tratamiento de sus datos personales y poner en su conocimiento las políticas de Tratamiento de la información de la entidad, el responsable podrá implementar mecanismos alternos para los efectos de publicitar de manera masiva la información, como la publicación en la páginas web oficial de la Secretaría Distrital del Hábitat o en medios de amplia difusión, e informar de esta situación a la Autoridad de Protección de Datos.

Para establecer cuándo existe una carga desproporcionada para el responsable del Tratamiento, se tendrá en cuenta la capacidad económica de la entidad, el número de Titulares, la antigüedad de los datos, el ámbito territorial y sectorial de operación del responsable y el mecanismo alternativo de comunicación que se utilizará, de manera que el hecho de solicitar la autorización a cada Titular implique un costo excesivo y que esto comprometa la estabilidad financiera del responsable, la realización de las actividades propias de la entidad o la viabilidad del presupuesto programado. Se considerará que existe una imposibilidad de solicitar a cada Titular la autorización para el Tratamiento de sus datos personales cuando el responsable no cuente con datos de contacto de los Titulares porque estos no reposan en sus archivos, registros o bases de datos, o porque están desactualizados, incorrectos, incompletos o inexactos.

Treinta (30) días hábiles contados después de la implementación del mecanismo de publicidad masiva de la política de Tratamiento de la información y los mecanismos de protección de datos personales, que la Secretaría Distrital del Hábitat ha adoptado, sin que el Titular haya contactado a la entidad para solicitar la supresión de sus datos personales, el responsable y el encargado del Tratamiento podrán continuar realizando el Tratamiento de la información para las finalidades indicadas de acuerdo con la base de datos que se trate, sin



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 64 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

perjuicio del derecho que le asiste al Titular de solicitar en cualquier momento la supresión de su información o la corrección de la misma.

## **IX. PERMANENCIA DE LA INFORMACIÓN EN LAS BASES DE DATOS**

Los responsables y encargados del Tratamiento solo podrán recolectar, almacenar, usar o circular los datos personales durante el tiempo que definan como razonable y necesario, de acuerdo con las finalidades que justifican la base de datos en consonancia con las disposiciones aplicables a la materia de que se trate y a los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información. Cumplida la finalidad del Tratamiento, se procederá a la supresión de los datos personales, salvo que se requiera su conservación en el cumplimiento de una obligación legal o contractual. Para efectos de la conservación y supresión de los datos personales se estará pendiente de atender las instrucciones que en la materia dicte la autoridad de protección de datos.

## **X. VIGENCIA DE LA POLÍTICA DE TRATAMIENTO DE LA INFORMACIÓN**

La presente política rige a partir de la fecha de expedición de la Resolución que la adopta, y será modificada, actualizada y/o complementada, cuando a ello haya lugar y de conformidad con Constitución, las Leyes y demás normas relacionadas con la materia.





## 4 GLOSARIO

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

- **Activo:** En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización<sup>1</sup>.
- **Activos de información:** Elementos de Hardware y de Software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo<sup>2</sup>.
- **Amenaza informática:** Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la entidad política del Estado. (Ministerio de Defensa de Colombia).
- **Análisis de riesgos:** Proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo<sup>3</sup>.
- **Área Segura:** Aquel sitio donde se maneja información sensible, es decir, refugios que ofrecen mecanismos de seguridad para la organización. Dentro del contexto de la seguridad física, debemos entender el concepto “sitio” como edificio, habitación u oficina donde se albergan cada uno de los servicios o instalaciones.
- **Autenticación:** Mecanismo que se realiza a través de medios, dispositivos o sistemas para validar la identidad de un usuario.
- **Autenticidad:** Propiedad de que una entidad es lo que afirma ser.

<sup>1</sup> <http://www.iso27000.es/glosario.html>

<sup>2</sup> <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=33486>

<sup>3</sup> <http://www.iso27000.es/glosario.html>



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 66 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- **Autoridad de Protección de Datos:** De acuerdo con lo dispuesto en la Ley 1581 de 2012 la Superintendencia de Industria y Comercio, a través de una Oficina Especial para la Protección de Datos Personales, ejercerá la vigilancia para garantizar que en el Tratamiento de datos personales se respeten los principios, derechos, garantías y procedimientos previstos en la citada ley.
- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.
- **Aviso De Privacidad:** Comunicación, verbal o escrita, en la que el responsable del Tratamiento de la información le informa al Titular de los datos personales la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma en que podrá acceder a estas y las finalidades del Tratamiento que se pretende dar a los datos personales que suministre.
- **Base de Datos:** Conjunto organizado de datos personales que serán objeto de Tratamiento.
- **Base de Datos Personal o Doméstica:** Conjunto de datos personales que serán objeto de Tratamiento dentro del marco de la vida privada o familiar de las personas naturales.
- **Causahabiente:** Persona que es sucesora o heredera del Titular de la información a causa del fallecimiento de este.
- **Clasificación de la Información:** es el ejercicio mediante el cual se determina que la información pertenece a uno de los niveles de clasificación estipulado por la entidad. Tiene como objetivo asegurar que la información tenga el nivel de protección adecuado.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** Comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- **Custodio de activo de información:** Personal asignado a un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de administrar y hacer



efectivo los controles que el propietario del activo haya definido, con base en los controles de seguridad disponibles en la entidad.

- **Datos abiertos:** Son todos aquellos datos primarios (sin procesar) que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo custodia de la entidad y que pueden ser puestos a disposición de cualquier ciudadano, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos<sup>4</sup>.
- **Dato Personal:** Cualquier información vinculada, o que pueda asociarse, a una o varias personas naturales determinadas o determinables.
- **Dato privado:** Son los datos que por su naturaleza íntima o reservada sólo son relevantes para el titular.
- **Dato Sensible:** Es aquel que afecta la intimidad del Titular o cuyo uso indebido puede propiciar discriminación; se entienden como sensibles los datos que revelen el origen étnico o racial, la orientación o filiación política, las convicciones y creencias religiosas o filosóficas, el estado de salud, la vida sexual, la información biométrica, la información familiar, la dirección de domicilio, y la pertenencia a sindicatos o a organizaciones sociales, de derechos humanos, promotoras de intereses de partidos políticos o que garanticen derechos y garantías de partidos políticos de oposición. Su Tratamiento está prohibido salvo en las excepciones previstas en las leyes.
- **Dato semiprivado:** Aquel que no tiene naturaleza íntima, reservada, ni pública. Su conocimiento o divulgación puede interesar no solo al Titular sino a un sector o grupo de personas o a la sociedad en general; tienen esta naturaleza los datos financieros, los crediticios, los relacionados con la actividad comercial o de servicios, entre otros.
- **Dato público:** Es el dato calificado como tal según los mandatos de la ley o de la Constitución Política y todos aquellos que no sean semiprivados o privados, de conformidad con la Ley 1266 de 2008. Son públicos, entre otros, los datos contenidos en documentos públicos, sentencias judiciales debidamente ejecutoriadas que no estén sometidos a reserva y los relativos al estado civil de las personas, entre otros; se consideran igualmente datos públicos los relativos al estado civil de las personas, su profesión u oficio, su calidad de comerciante o de servidor público, entre otros.
- **Disponibilidad:** Propiedad de que la información sea accesible y utilizable por solicitud de una entidad y/o persona autorizada.

<sup>4</sup> <http://mintic.gov.co/portal/604/w3-article-5300.html>



- **Encargado del Tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del Tratamiento. Puede darse el caso de que se tenga múltiples roles en el manejo de la información y ser al mismo tiempo responsable del Tratamiento, fuente de información o usuario.
- **Evento de Seguridad:** Ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.
- **Fuente de Información:** Persona natural o jurídica que recibe o conoce datos personales del Titular, en virtud de una relación comercial, de servicio o de cualquier otra índole. Mediante autorización legal o del Titular puede transmitir o transferir estos datos a un responsable o encargado para su Tratamiento. Puede tener múltiples roles en el manejo de la información y ser al mismo tiempo responsable o encargado del Tratamiento.
- **Gestión de claves:** Son controles que realizan mediante la gestión de claves criptográficas.
- **Gestión de incidentes de seguridad de la información:** Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.
- **Gestión de riesgos:** actividades coordinadas para dirigir controlar una entidad con respecto al riesgo. Se compone de la evaluación y el tratamiento de riesgos.
- **Habeas data:** Derecho de cualquier persona a conocer, actualizar y rectificar los datos o la información que se hayan recogido sobre ella en un banco de datos o en archivos de entidades públicas y privadas.
- **Hardware:** Equipos de cómputo y de comunicaciones que por su criticidad son considerados activos de información, no sólo activos fijos.
- **Incidentes de seguridad de la información:** Evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información:** Corresponde a este grupo bases y archivos de datos, contratos, documentación del sistema, investigaciones, acuerdos de confidencialidad, manuales de usuario, procedimientos operativos o de soporte, planes para la continuidad del negocio, acuerdos sobre retiro y pruebas de auditoría entre otros.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 69 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

- **Impacto:** Cambio adverso en el nivel de los objetivos del negocio logrados<sup>5</sup>.
- **Integridad:** Conservar con exactitud la información que fue generada, sin ser manipulada ni alterada por personas o procesos no autorizados.
- **Inventario de activos:** Lista de todos aquellos recursos (físicos, de información, *software*, documentos, servicios, personas, intangibles, etc.) dentro del alcance del *SGSI*, que tengan valor para la entidad y necesiten por tanto ser protegidos de potenciales riesgos.
- **No repudio:** Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido).
- **Medio removible:** Componente extraíble de hardware, usado para el almacenamiento de información; entre los que podemos encontrar: cintas, discos duros removibles, CDs, DVDs y unidades de almacenamiento USB, entre otras.
- **Oficial de Seguridad de la Información:** También denominado CISO (Chief Information Security Officer) es un rol desempeñado por el (la) Subsecretario (a) de Gestión Corporativa y CID y su función principal es la de alinear la seguridad de la información con los objetivos de negocio. De esta forma se avala en todo momento que la información de la entidad está preservada adecuadamente, para el rol de CISO es responsable de:
  - ✓ Generar y establecer políticas de seguridad de la información.
  - ✓ Garantizar la seguridad y privacidad de los datos.
  - ✓ Supervisar la administración del control de acceso a la información.
  - ✓ Supervisar el cumplimiento normativo de la seguridad de la información.
  - ✓ Responsable del equipo de respuesta ante incidentes de seguridad de la información de la organización.
  - ✓ Controlar la arquitectura de seguridad de la información de la empresa.
- **Operador de Información:** Persona, entidad u organización que recibe información de la fuente de datos personales sobre varios Titulares, los administra y los pone en conocimiento de los usuarios bajo los parámetros de la ley. Se sujeta al cumplimiento de

<sup>5</sup> <https://tienda.icontec.org/wp-content/uploads/pdfs/NTC-ISO-IEC27005.pdf>



los deberes y responsabilidades previstos para garantizar la protección de los derechos del Titular de los datos. No es responsable por la calidad de los datos que le sean suministrados por la fuente salvo que este tenga la condición de fuente y operador de manera simultánea.

- **Parte interesada (*Stakeholder*):** Persona u entidad que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.
- **Plan de continuidad del negocio:** Plan orientado a permitir la continuidad de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro.
- **Plan de tratamiento de riesgos:** Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.
- **Proceso:** Conjunto de actividades interrelacionadas o interactuantes que transforman unas entradas en salidas.
- **Propietario de activo de información:** Personal asignado a un cargo, proceso o grupo de trabajo designado por la entidad, que tiene la responsabilidad de definir los controles, el desarrollo, el mantenimiento, el uso y la seguridad de los activos de información asignados.
- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consideraciones.
- **Responsable del tratamiento:** Persona natural o jurídica. Pública o privada. Que por sí misma o en asocio con otros, decide sobre la base de datos o el Tratamiento de los de los mismos. También puede ser fuente de información, encargado del Tratamiento o usuario
- **Segregación de tareas:** Reparto de tareas sensibles entre distintos empleados para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.
- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información.



- **Sistema de Gestión de Seguridad de la Información (SGSI):** Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una entidad para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.
- **Titular de la información:** Es la persona natural o jurídica a quien se refiere la información que reposa en un banco de datos y sujeto del derecho de hábeas data y demás derechos y garantías a que se refiere la presente ley.
- **Transferencia:** Tiene lugar cuando el responsable o el encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor que se convierte en responsable del Tratamiento y que puede encontrarse dentro o fuera del país.
- **Transmisión:** Implica la comunicación de los datos personales, dentro o fuera del territorio de la República de Colombia, con el objetivo de darle un Tratamiento por parte del encargado y de acuerdo con las instrucciones del responsable.
- **Tratamiento:** Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.
- **Trazabilidad:** Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad.
- **Usuario:** Persona natural o jurídica que, en los términos y circunstancias permitidas por la ley, puede acceder a la información personal, de uno o varios Titulares, que ha sido transferida o transmitida por el encargado siguiendo instrucciones del responsable. De acuerdo con el uso que le dé a los datos del Titular, puede transformarse en responsable o encargado del Tratamiento o fuente de información.
- **Vulnerabilidad:** Debilidad de un activo o control que pueda ser explotado por una o más amenazas.



ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

## MANUAL DE POLÍTICAS DEL SUBSISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Página 72 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

### 5 CONTROL DE CAMBIOS

Fecha de Modificación (aaaa/mm/dd)	Versión	Descripción del cambio
2018/07/12	3	<p>Se reestructura redacción de la introducción y el alcance, se definen los objetivos de seguridad de la información y se redefine la política general del subsistema Seguridad de la Información las políticas: autorización de nuevos recursos de procesamiento, Clasificación de activos de información, seguridad física, antivirus, Backup fueron redefinidas, fue eliminada la política de administración de riesgos, la política de intercambio de información modifico su nombre a política de transferencia o intercambio de información y fue ajustada en contenido, la política de uso de correo electrónico fue modificada a uso de correo electrónico corporativo y fue ajustado en contenido y redacción, la política de uso de sistemas de información y dispositivos de comunicación fue eliminada, las políticas de control de acceso y uso de contraseñas fueron ajustado en contenido y redacción, la política de uso de puestos de trabajo modifica su nombre a escritorio limpio y pantalla limpia y ajusta su contenido, las políticas de uso de servicio de red, uso de internet y política de uso de VPN son redefinidas, la política de uso de computación móvil y teletrabajo es dividida en dos: política de uso de dispositivos móviles y política de teletrabajo, la política de adquisición, desarrollo y mantenimiento de sistemas de información modifica su nombre a política de desarrollo de software; las políticas de controles criptográficos, control de cambios y propiedad intelectual se ajustan en redacción y contenido.</p> <p>Se incluye la política de relación con proveedores y la política de tratamiento de la información de la SDHT; se incluye el anexo "Declaración de aplicabilidad SOA" y se actualiza acorde con el organigrama el cargo de "Director de Gestión Corporativa y CID a Subsecretario de Gestión Corporativa y CID.</p>
2018/09/26	4	<p>Según lo aprobado en el comité de seguridad y de las tecnologías de la información y las comunicaciones del 18/09/2018, se reestructura redacción del alcance general del documento y objetivo de las políticas: seguridad física, autorización de nuevos recursos de procesamiento - desarrollo de software - transferencia o intercambio de información.</p>





ALCALDÍA MAYOR  
DE BOGOTÁ D.C.  
SECRETARÍA DE HABITAT

**MANUAL DE POLÍTICAS DEL SUBSISTEMA DE  
GESTIÓN DE  
SEGURIDAD DE LA INFORMACIÓN**

Página 73 de 73

VERSIÓN 4

Fecha  
2018/09/26

Código  
PS05-MM13

## 6 ANEXOS

Anexo 1: Declaración de Aplicabilidad – SOA