

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 1 de 43

## Tabla de Contenido

1.	OBJETIVO GENERAL: .....	5
2.	OBJETIVOS ESPECÍFICOS .....	5
3.	ALCANCE .....	5
4.	LINEAMIENTOS GENERALES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.....	5
5.	DIRECTRICES DE LA ENTIDAD EN SEGURIDAD DE LA INFORMACIÓN: ....	6
6.	POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN .....	6
6.1.	Orientación de la Dirección para la Gestión de la Seguridad de la Información .....	6
6.2.	Políticas para la Seguridad de la Información.....	7
6.3.	Revisión de las políticas para seguridad de la información. ....	7
7.	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.....	7
7.1.	Roles y responsabilidades en seguridad de la información .....	7
7.1.1.	Del Comité Institucional de Gestión y Desempeño – Alta Dirección .....	8
7.1.2.	De la Oficina Asesora de Planeación.....	8
7.1.3.	De la Oficina Asesora de Planeación - Gestión Tecnológica .....	9
7.1.4.	De la Oficina Asesora Jurídica .....	10
7.1.5.	De Gestión Contractual.....	10
7.1.6.	De Gestión del Talento Humano .....	11
7.1.7.	De Control Interno .....	11
7.1.8.	De Control Interno Disciplinario .....	12
7.1.9.	De Gestión Administrativa .....	12
7.1.10.	De Gestión Administrativa - Gestión Documental .....	13
7.1.11.	De Comunicación Estratégica.....	13
7.1.12.	De los Propietarios de los Activos de Información.....	13
7.1.13.	De los custodios de la información .....	14
7.1.14.	De las(os) servidoras y servidores públicos y contratistas.....	15
8.	POLÍTICA DE DISPOSITIVOS MÓVILES .....	16
8.1.	POLÍTICA DE TELETRABAJO.....	17
8.2.	POLÍTICA DE USO DE HERRAMIENTAS COLABORATIVAS (TEAMS, ONEDRIVE).....	19
8.3.	POLÍTICA DE TELEFONÍA MÓVIL, CELULAR Y FIJA .....	20
8.3.1.	Niveles de acceso a los servicios de Telefonía: .....	21

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 2 de 43

8.4. POLÍTICA CORREO ELECTRÓNICO INSTITUCIONAL .....	21
8.5. POLÍTICA ACCESO A INTERNET .....	23
8.6. RECURSOS TECNOLÓGICOS.....	24
8.7. CABLEADO ESTRUCTURADO .....	25
8.8. SISTEMAS DE INFORMACIÓN .....	26
9. SEGURIDAD DE LOS RECURSOS HUMANOS .....	26
10. GESTIÓN DE ACTIVOS .....	26
10.1. GESTIÓN DE MEDIOS DE ALMACENAMIENTO.....	26
11. CONTROL DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN .....	27
11.1. CONTROL DE ACCESO:.....	27
12. CRIPTOGRAFÍA.....	28
13. SEGURIDAD FÍSICA Y DEL ENTORNO .....	29
13.1. SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DEL PREDIO .....	30
13.2. ESCRITORIO Y PANTALLA LIMPIA.....	30
14. SEGURIDAD DE LAS OPERACIONES .....	30
14.1. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS .....	31
14.2. COPIAS DE RESPALDO.....	31
15. SEGURIDAD DE LAS COMUNICACIONES.....	32
15.1. ACUERDOS DE CONFIDENCIALIDAD.....	33
16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS .....	33
17. RELACIONES CON LOS PROVEEDORES .....	34
18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN.....	35
19. GESTIÓN DE CONTINUIDAD DE NEGOCIO .....	35
20. CUMPLIMIENTO .....	36
21. MARCO NORMATIVO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN..	37
22. TÉRMINOS Y DEFINICIONES.....	38
23. REGISTRO DE MODIFICACIONES.....	43


	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 3 de 43

## INTRODUCCIÓN

La Secretaría Distrital de la Mujer, determina la información y los recursos informáticos como activos vitales para el desarrollo de sus funciones de conformidad con la misión y la visión de la Entidad, por lo cual la Alta Dirección se encuentra comprometida con la implementación de un sistema de gestión de seguridad de la información (SGSI) eficiente y robusto que proteja la integridad, confidencialidad y disponibilidad de la información, este proceso será liderado de manera permanente por la Oficina Asesora de Planeación – Gestión Tecnológica.

El siguiente documento presenta de manera organizada las políticas de seguridad de la información, las cuales deben ser adoptadas por todas las servidoras y servidores públicos, contratistas, y terceros que tengan algún tipo de relación con la Secretaria Distrital de la Mujer. Por tal razón los actores antes mencionados, deben ser conscientes que la seguridad de la información es responsabilidad directa de todas(os) y, por tanto, deben conocer, apropiar y aplicar las políticas que la entidad adoptó en esta materia y reportar a la Oficina Asesora de Planeación – Gestión Tecnológica cualquier novedad que se presente en el cumplimiento de esta.


Conforme a la Política General de Seguridad de la Información de la Secretaría Distrital de la Mujer, y en cumplimiento de los objetivos y compromisos trazados por la Entidad frente a la seguridad de la información, que se encuentran consignados en el presente documento, se define el conjunto de políticas y dominios que abarcará la Secretaría en materia de Seguridad de la Información.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 4 de 43

El presente manual tiene como finalidad cubrir los 14 dominios de seguridad de la información y sus controles, conforme a lo que indica la NTC ISO 27001:2013, en función de lo anterior se realiza una breve descripción del propósito de cada uno de los dominios contemplados en dicha norma.

1. **Políticas de seguridad de la Información:** contiene controles que se deben tener en cuenta respecto a cómo deben ser escritas y revisadas las políticas.
2. **Organización de la seguridad de la información:** contiene controles que se deben tener en cuenta respecto a cómo se asignan las responsabilidades, incluye controles para dispositivos móviles y el teletrabajo.
3. **Seguridad de los Recursos Humanos:** contiene controles que se deben tener en cuenta y aplicar antes, durante y después de un empleo.
4. **Gestión de recursos:** contiene controles que se deben tener en cuenta respecto a lo relacionado con el inventario de recursos y su uso aceptable, también la clasificación de la información y la gestión de los medios de almacenamiento.
5. **Control de Acceso:** contiene controles que se deben tener en cuenta respecto a las políticas de control de acceso, gestión de acceso de los usuarios, control de acceso para el sistema y las aplicaciones, y responsabilidades del usuario.
6. **Criptografía:** contiene controles que se deben tener en cuenta respecto a la gestión de encriptación y claves.
7. **Seguridad física y ambiental:** contiene controles que se deben tener en cuenta respecto a áreas seguras, controles de entrada, protección contra amenazas, seguridad de equipos, políticas de escritorio y pantalla despejadas, etc.
8. **Seguridad Operacional:** contiene controles que se deben tener en cuenta relacionados con la gestión de la producción en Tecnologías de Información - TI: gestión de cambios, gestión de capacidad, malware, respaldo, bitácoras, espejos, instalación, vulnerabilidades.
9. **Seguridad de las Comunicaciones:** contiene controles que se deben tener en cuenta respecto a seguridad de redes, segregación, servicios de redes, transferencia de información, mensajería, etc.
10. **Adquisición, desarrollo y mantenimiento de Sistemas:** contiene controles que se deben tener en cuenta respecto a los requerimientos de seguridad y la seguridad en los procesos de desarrollo y soporte.
11. **Relaciones con los proveedores:** contiene controles que se deben tener en cuenta respecto a qué incluir en los contratos, y cómo hacer el seguimiento a los proveedores.
12. **Gestión de Incidentes en Seguridad de la Información:** contiene controles que se deben tener en cuenta para reportar los eventos y debilidades, definir responsabilidades, procedimientos de respuesta, y recolección de evidencias.
13. **Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio:** contiene controles que se deben tener en cuenta respecto a la planificación de la continuidad del negocio, procedimientos, verificación y revisión, y redundancia de TI.
14. **Cumplimiento:** contiene controles que se deben tener en cuenta respecto a identificación de las leyes y regulaciones aplicables, protección de la propiedad intelectual, protección de datos personales, y revisiones de la seguridad de la información.

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 5 de 43

## 1. OBJETIVO GENERAL:

Establecer las directrices y reglas que deben seguir las servidoras y servidores públicos, contratistas y terceros que hagan uso de los servicios tecnológicos y de los sistemas de información de la entidad, para generar una adecuada cultura de seguridad y protección de la información física y digital de la Secretaría Distrital de la Mujer, con el fin de preservar la integridad, disponibilidad y confidencialidad de la información.

## 2. OBJETIVOS ESPECÍFICOS


- Consolidar la cultura de Seguridad de la Información como tema estratégico en la Secretaría Distrital de la Mujer.
- Lograr la protección de la Información física y digital, el hardware, el software, aplicativos, servicios, redes de datos y comunicaciones, por medio de la divulgación, conocimiento, apropiación y cumplimiento de la Política de Seguridad de la Información.
- Definir las medidas esenciales de seguridad de la información física y digital que la Secretaría Distrital de la Mujer debe adoptar, para protegerse apropiadamente contra riesgos y amenazas que podrían afectar la confidencialidad, integridad y disponibilidad de la Información.
- Difundir, socializar y concientizar a todo el personal de la Secretaría Distrital de la Mujer sobre las buenas prácticas en materia de seguridad de la información que permitan garantizar la integridad, confidencialidad y disponibilidad de la información física y digital.

## 3. ALCANCE

Esta política de Seguridad de la Información aplica a toda la entidad, las servidoras y servidores públicos, contratistas y terceros en Nivel Central, las CIOM, Casa Refugio, Casa de Todas y demás escenarios en donde se desarrollen actividades de la Secretaría Distrital de la Mujer, en las cuales se genere, acceda, almacene y se procese información de la entidad, ya sea en medios físicos, electrónicos, haciendo uso de la infraestructura tecnológica, sistemas de información, o información física en medio papel que sea provista por la entidad.

## 4. LINEAMIENTOS GENERALES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La Secretaría Distrital de la Mujer establece que la información es un activo vital para el desarrollo de las actividades del Gobierno Distrital, en razón a que es una herramienta de gran importancia para la toma de decisiones en la entidad, motivo por el cual, la entidad está comprometida con la protección de sus activos de información (colaboradores, información, infraestructura tecnológica, sistemas de información, entre otros), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, continuidad de las operaciones, de la administración y/o gestión de riesgos, creación de una cultura y conciencia de seguridad de la información en las servidoras y servidores públicos

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 6 de 43

contratistas, y personas que hagan uso de los activos de información.

La efectividad de esta política depende finalmente de la responsabilidad del personal que hace parte de la Secretaría Distrital de la Mujer, en vista de que las herramientas de TI y los controles definidos e implementados, por sí solos no son suficientes para garantizar la seguridad de la información de la entidad, sino que se requiere de la participación activa del recurso humano con el que cuenta la Entidad.

Debido a la importancia y sensibilidad de la información, la Secretaría Distrital de la Mujer integra el Sistema de Gestión de Seguridad de la información SGSI dentro del Modelo Integrado de Planeación y Gestión - MIPG, de tal forma que le permite generar su evaluación y mejora continua, basados en la identificación de sus activos de información y en la gestión y tratamiento de riesgos, así como en los planes o actividades de continuidad de la operación, de conformidad con la misión y visión de la entidad.


## 5. DIRECTRICES DE LA ENTIDAD EN SEGURIDAD DE LA INFORMACIÓN:

- Verificar que la política de seguridad de la información esté definida, aprobada, implementada, revisada y actualizada.
- Realizar sensibilizaciones a las servidoras, servidores públicos, contratistas, y demás usuarios en temas de seguridad de la información, para fomentar en la Secretaría, una cultura y conciencia del personal en seguridad de la información.
- Dar a conocer y hacer cumplir por parte de las servidoras, servidores públicos, contratistas, y demás usuarios, los lineamientos, procedimientos, directrices, y buenas prácticas establecidas en el manual de políticas específicas de seguridad de la información, de los sistemas de información e infraestructura tecnológica de la Secretaría.
- Las(os) responsables de las áreas y de los procesos, deben asegurar que todos sus procedimientos incluyan controles de seguridad de la información, para lograr el cumplimiento de la política de seguridad de la información de la Secretaría Distrital de la Mujer, la cual se encuentra alineada con los estándares de la norma NTC-ISO 27001:2013.
- La Secretaría tiene definidos los estándares para instalación, configuración, y uso del hardware y software, los cuales se deben cumplir por parte de las servidoras, servidores públicos, contratistas, y demás usuarios, en tal sentido, cualquier novedad debe ser justificada por quien corresponda y aprobada por la Oficina Asesora de Planeación – Gestión Tecnológica.

## 6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

### 6.1. Orientación de la Dirección para la Gestión de la Seguridad de la Información

La Secretaría Distrital de la Mujer en cumplimiento a su compromiso de velar y garantizar la Seguridad de la Información, crea un esquema donde define y establece los requerimientos de seguridad de la información en el cual contempla la identificación de sus activos de información, tratamiento de riesgos, roles y responsabilidades del personal, gestión y administración de la seguridad de la información, cuya finalidad es salvaguardar la información institucional en todo su ciclo de vida, el cual incluye entre otros, el procesamiento, almacenamiento, administración y transmisión de la información. Los temas relacionados con la Seguridad de la Información en la entidad serán de competencia del Comité

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 7 de 43

Institucional de Gestión y Desempeño en su calidad de representantes de la Alta Dirección.

## **6.2. Políticas para la Seguridad de la Información.**

La Secretaría Distrital de la Mujer define en el presente documento el conjunto de Políticas de Seguridad de la Información, las cuales se encuentran aprobadas, publicadas y se han comunicado a las servidoras y servidores públicos, contratistas, y terceros que tienen relación con la entidad.

## **6.3. Revisión de las políticas para seguridad de la información.**

La política de seguridad de la Información debe ser revisada y/o actualizada por lo menos una (1) vez por año, o cuando se identifiquen cambios importantes en su estructura, objetivos o alguna condición que afecte su aplicabilidad o cumplimiento, con lo cual se asegura su efectividad, y mejora continua, acorde con la normatividad vigente en materia de seguridad de la información.

## **7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.**

### **7.1. Roles y responsabilidades en seguridad de la información**

La Política de Seguridad de la Información es aplicable a todas las áreas y/o dependencias de la Secretaría Distrital de la Mujer y es de cumplimiento obligatorio por parte de todas las servidoras, servidores públicos, en cualquier nivel jerárquico, sean contratistas planta temporal o permanente, definidos como los usuarios, responsables dueños, y/o custodios de la información física y digital, equipos informáticos, así como por otros usuarios que utilicen de una u otra forma los sistemas de información, almacenamiento e infraestructura física, infraestructura tecnológica o redes de comunicaciones y servicios tecnológicos de la Secretaría Distrital de la Mujer.

- El incumplimiento de la Política de Seguridad de la Información dará lugar a la aplicación de las sanciones establecidas de conformidad con los lineamientos del orden nacional y territorial, obligaciones contractuales, código de trabajo, reglamento interno de trabajo de la Secretaría Distrital de la Mujer y demás disposiciones relacionadas, sin perjuicio de las acciones civiles o penales que en su caso puedan resultar aplicables.
- Los proyectos transversales que adelanten las dependencias o procesos de la Entidad, que involucren el uso de Tecnologías de Información, deben contemplar una adecuada gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- Los proyectos que adelante o desarrolle inhouse la Entidad, contemplar la gestión de los riesgos de seguridad asociados a la información del proyecto, lo cual incluye una identificación de los riesgos y la definición de la forma como serán gestionados.
- En aras de velar por la seguridad de la información, se debe realizar una adecuada separación

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 8 de 43

de roles responsabilidades en cada dependencia para reducir las posibilidades de modificación no autorizada o no intencional o el uso indebido de los activos de la Entidad.

- Contacto con autoridades: En caso de incidentes en la seguridad de la información puede resultar necesario mantener informados a los organismos de control del estado o administración. Estos pueden ser comúnmente (autoridades policiales, fiscalía, COLCERT – grupo de respuesta a emergencias cibernéticas, entre otros).
- En relación con el contexto de organización de la seguridad de la información, existen distintos niveles de responsabilidad y autoridades que se deben involucrar en el manejo y uso de la información, así como responsabilidades que se asignan por roles, como se describen a continuación:


#### **7.1.1. Del Comité Institucional de Gestión y Desempeño – Alta Dirección**

- Asegurar la implementación y desarrollo de políticas y directrices en materia de seguridad digital y de la información, mediante el cumplimiento de las siguientes actividades:
- Aprobar y hacer seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para la implementación interna de las políticas de seguridad de la información.
- Socializar la importancia de adoptar la cultura de seguridad de la información a los procesos de la entidad.
- Aprobar acciones y mejores prácticas que contribuyan en la implementación del Sistema de Gestión de Seguridad de la Información.
- Adoptar las decisiones que permitan la gestión y minimización de riesgos críticos de seguridad de la información.

#### **7.1.2. De la Oficina Asesora de Planeación**

- Efectuar acompañamiento a la alta dirección, para asegurar el liderazgo y cumplimiento de los roles y responsabilidades de los líderes de los procesos en seguridad de la información.
- Implementar los controles de seguridad de la información para sus activos de información.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- La Secretaría Distrital de la Mujer a través de la Oficina Asesora de Planeación garantizará la existencia y cumplimiento de las medidas que mantenga el nivel de seguridad de la información acorde con la misión de la Entidad y los recursos disponibles.
- Apoyar y participar metodológicamente en la formulación, aprobación y publicación de metodologías, procedimientos, políticas, lineamientos, manuales, entre otros, del Sistema de Gestión de Seguridad de la Información para la alineación y articulación con MIPG.
- Socializar la metodología para la construcción de los mapas de riesgos a los procesos de la entidad.




	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 9 de 43

### 7.1.3. De la Oficina Asesora de Planeación - Gestión Tecnológica

- Liderar la planificación e implementación del Sistema de Gestión de Seguridad de la Información.
- Implementar los controles de seguridad de la información para sus activos de información.
- Es la dependencia encargada de la Seguridad de la Información, para lo cual debe definir los lineamientos en materia de seguridad de la información de la Secretaría Distrital de la Mujer, analizar periódicamente el nivel del riesgo existente, y proponer soluciones. Una vez autorizada la implementación de las políticas, coordinará a quienes corresponda para su materialización oportuna y correcta, asimismo velar por la aplicabilidad de la política, realización de cambios al documento y actualización.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Brindar apoyo en los temas que requiera el Comité Institucional de Gestión y Desempeño de la entidad, en materia de seguridad de la información y proponer acciones de mejora del Sistema de Gestión de Seguridad de la Información.
- A partir de las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad de la información.
- Instalar y actualizar el antivirus en los equipos de cómputo institucionales de la Secretaría Distrital de la Mujer.
- Incluir en el procedimiento de administración de riesgo los aspectos de seguridad de la información de la entidad.
- Liderar y brindar acompañamiento a los procesos de la Entidad en la gestión de riesgos de seguridad de la información y seguimiento al plan de tratamiento de riesgos.
- Proponer la formulación de políticas y lineamientos de seguridad de la información.
- Definir e implementar socializaciones y divulgaciones de seguridad de la información para todos los involucrados en el manejo de información de la Entidad.
- Efectuar acompañamiento a los procesos en la implementación de la Política de Seguridad de la Información en la Entidad.
- Apoyar a los procesos para dar cumplimiento a las recomendaciones en materia de seguridad de la información.
- Definir e implementar el procedimiento de Gestión de Incidentes de seguridad de la información en la Entidad.
- Instalar y configurar los teléfonos IP y habilitar los puntos de conexión requeridos.
- Realizar el mantenimiento de los teléfonos IP y asignación de controles en en la consola de comunicaciones.
- Mantener un registro actualizado de los requerimientos en materia de telefonía móvil y fija, con sus

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 10 de 43

respectivos niveles de acceso por dependencia.


- Realizar los trámites respectivos con el proveedor del servicio de comunicaciones unificadas en lo relacionado con: traslados, desconexiones temporales o definitivas, cambios de números, reposición de equipos (móviles, teléfonos IP, otros), cambio de proveedor, adquisición de nuevos servicios, entre otros.
- Habilitar los servicios de telefonía fija, móvil, nacional e internacional, de acuerdo a los requerimientos institucionales que se encuentren debidamente justificados.

#### **7.1.4. De la Oficina Asesora Jurídica**

- Brindar asesoría a la Oficina Asesora de Planeación – Gestión Tecnológica, en materia de temas jurídicos y legales que involucren acciones ante las autoridades competentes relacionados con seguridad de la información.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Brindar asesoría al Comité Institucional de Gestión y Desempeño en materia de temas normativos, jurídicos y legales vigentes que involucren acciones ante las autoridades competentes relacionados con seguridad de la información.
- Verificar que los contratos que por competencia deban suscribir los procesos de la Secretaría Distrital de la Mujer, cuenten con cláusulas de derechos de autor, de confidencialidad y no divulgación de la información según sea el caso.
- Representar a la Entidad en procesos judiciales ante las autoridades competentes relacionados con seguridad de la información.
- Apoyar a los procesos en la elaboración del Índice de Información clasificada y reservada de los activos de información de acuerdo con la regulación vigente.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Liderar los temas relacionados con tratamiento de datos personales en la entidad, asesorar a los procesos en lo relacionado con la normatividad vigente y/o actualización de documentación, procesos y procedimientos, dar respuesta a terceros respecto a inquietudes de datos personales.

#### **7.1.5. De Gestión Contractual**

- Incluir acuerdos de confidencialidad y no divulgación de información en los contratos.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 11 de 43

solicitado.


- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Implementar los controles necesarios para dar cumplimiento a la Ley de protección de datos personales, relacionados con los contratistas y terceros.
- Realizar la actualización de la documentación de Gestión Contractual, relacionada con temas de seguridad de la información.

#### **7.1.6.De Gestión del Talento Humano**

- Controlar y salvaguardar la información de datos personales de los servidores públicos de planta de la Secretaría Distrital de la Mujer, en concordancia con la normatividad vigente.
- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Realizar la gestión de vinculación, capacitación, desvinculación del personal de planta dando cumplimiento a la normatividad vigente y a la Política de Seguridad de la Información.
- Incluir acuerdos de confidencialidad y no divulgación de información en los documentos administrativos de posesión del cargo de las servidoras, servidores públicos y en los demás documentos que lo requieran.

#### **7.1.7.De Control Interno**

- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Incluir como unidad auditable el Sistema de Gestión Seguridad de la Información – SGSI – en la formulación del Plan Anual de Auditoría, con el propósito de determinar el nivel de riesgo en el marco de la priorización de trabajos de auditoría, y presentar el análisis correspondiente en el Comité Institucional de Coordinación de Control Interno.
- Realizar las auditorías internas del Sistema de Gestión de Seguridad de la Información de acuerdo

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 12 de 43

con el plan definido en la entidad.


- Informar a quien corresponda, los hallazgos, no conformidades, observaciones y oportunidades de mejora relacionadas con el Sistema de Gestión de Seguridad de la Información.
- Presentar y socializar a quien corresponda, los resultados de las auditorías en materia del Sistema de Gestión de Seguridad de la Información.
- Evaluar y realizar seguimiento al plan de mejoramiento del Sistema de Gestión de Seguridad de la Información en cada uno de los procesos.
- Implementar los controles de seguridad que defina la dependencia de Evaluación y Control de la Gestión Interna para su proceso; contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica cuando sea solicitado.
- En todas sus actividades auditará el cumplimiento de lo consignado en la política de seguridad de la información.
- Establecerá planes de mejora, en caso de encontrar irregularidades en el cumplimiento de la política de seguridad de la información.

#### **7.1.8. De Control Interno Disciplinario**

- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Implementar las acciones disciplinarias correspondientes, por las posibles o presuntas violaciones de la política de seguridad de la información, de acuerdo a la falta en que incurran los servidores públicos de la entidad vinculados y/o desvinculados, según los resultados de la investigación.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.

#### **7.1.9. De Gestión Administrativa**

- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Coordinar y/o realizar el mantenimiento de la infraestructura de seguridad física de las sedes de La Secretaría Distrital de la Mujer.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Realizar el apoyo y/o acompañamiento requerido en la implementación, seguimiento y supervisión

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 13 de 43

de los controles de seguridad física de las sedes de la Secretaría Distrital de la Mujer.

- Gestionar ante la aseguradora cuando corresponda los diferentes eventos y/o incidentes relacionados con la seguridad física que pongan en riesgo la seguridad de la información.
- Gestionar la adquisición y supervisar la instalación y puesta en funcionamiento de los controles de acceso de seguridad física (Biométricos u otros) en las sedes de la Secretaría Distrital de la Mujer.

#### **7.1.10. De Gestión Administrativa - Gestión Documental**

- Implementar controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Reportar de forma inmediata los incidentes de seguridad de la información asociados a sus activos, en la herramienta de mesa de ayuda, con el fin de que la Dirección de Gestión Administrativa y Financiera proceda con el tratamiento respectivo.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Apoyar a los procesos en la actualización, creación y definición de las tablas de retención documental, como insumo para el levantamiento y/o actualización del inventario de activos de información.


#### **7.1.11. De Comunicación Estratégica**

- Implementar los controles de seguridad de la información para sus activos de información, contará con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Producir piezas de comunicación las cuales pueden ser digitales o impresas, con mensajes institucionales relacionados con seguridad de la información para comunicación interna.
- Publicar, divulgar información y mensajes institucionales a través de la página web, pantallas digitales, redes sociales y correo institucional relacionados con seguridad de la información.
- Facilitar la comunicación y divulgación del documento de la Política de Seguridad de la información a los servidores públicos y contratistas de la entidad.

#### **7.1.12. De los Propietarios de los Activos de Información**

- Los directivos de la entidad, como responsables de las diferentes dependencias, son los propietarios

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 14 de 43


de los activos de información que se generen en cumplimiento de las funciones de la dependencia a su cargo. Las(os) lideresas(es) de proceso, proyecto de Inversión y rubro de Funcionamiento.

- Realizar la identificación, clasificación y valoración de los activos de información en su proceso.
- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Realizar la actualización del inventario de activos de información de su proceso cuando se requiera y socializarlo con la Oficina Asesora de Planeación - Gestión Tecnológica y en el caso que competa reportar a Gestión Documental.
- Generar estrategias para garantizar el cumplimiento de los lineamientos del tratamiento de la información para asegurar la integridad, confidencialidad y disponibilidad de los activos de información a su cargo.
- Realizar la implementación y el seguimiento al cumplimiento de las actividades y controles de seguridad de la información en su proceso.
- Gestionar los recursos necesarios para la implementación de los controles de seguridad de la información para la gestión de riesgos sobre los activos de información en su proceso.
- Desarrollar los planes de mejoramiento de seguridad de la información asociados a los resultados de las auditorías internas del Sistema de Gestión de Seguridad de la Información y demás mecanismos de análisis, seguimiento y evaluación.
- Apoyar la planificación, implementación, evaluación de desempeño y mejora continua del Sistema de Gestión de Seguridad de la Información en su proceso.
- Participar en la sensibilización y/o capacitaciones del Sistema de Gestión de Seguridad de la Información.
- Realizar la identificación, evaluación y tratamiento de riesgos sobre los activos de información relacionados con su proceso, con el acompañamiento de la Oficina Asesora de Planeación - Gestión Tecnológica, cuando sea solicitado.
- Reportar a la Oficina Asesora de Planeación - Gestión Tecnológica los incidentes de seguridad de la información, en la herramienta de mesa de ayuda.
- Participar de manera activa en la solución de los incidentes de seguridad de la información.

### **7.1.13. De los custodios de la información**

Custodios de la información son personas, procesos, proveedores u otros, designados por los propietarios de los activos de información para administrar su seguridad.

- Custodiar y cuidar la documentación e información que por razón de su rol conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 15 de 43

- Implementar los controles de seguridad en los activos de información que custodia para garantizar los criterios de confidencialidad, integridad y disponibilidad de la información.
- Reportar los incidentes de seguridad de la información asociados a los activos que custodia, a la Oficina Asesora de Planeación - Gestión Tecnológica en la herramienta de mesa de ayuda.

#### **7.1.14. De las(os) servidoras y servidores públicos y contratistas**

- Dar cumplimiento a los manuales, procedimientos, lineamientos y políticas del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de la Mujer.
- Custodiar y cuidar la documentación e información que por razón de su empleo, cargo o funciones conserve bajo su cuidado o a la cual tenga acceso, e impedir o evitar la sustracción, destrucción, ocultamiento o utilización indebida.
- Reportar de forma inmediata los eventos o incidentes de seguridad de la información a la Oficina Asesora de Planeación – Gestión Tecnológica por medio de la herramienta de mesa de ayuda.
- Administrar y gestionar la información de tal forma que se garanticen los criterios de confidencialidad, integridad y disponibilidad de los activos de información de la Entidad.
- Dar cumplimiento a la Ley de protección de datos personales.
- Dar cumplimiento a la Política de Privacidad y Tratamiento de datos personales de la Entidad.
- Firmar y cumplir los acuerdos de confidencialidad y no divulgación de la información.
- Todas las servidoras y servidores públicos y contratistas de la entidad deben cumplir los acuerdos de confidencialidad y no divulgación de información establecidos en la presente política.
- Participar en las sensibilizaciones y capacitaciones del Sistema de Gestión de Seguridad de la Información de la Secretaría Distrital de la Mujer.
- Todas las servidoras y servidores públicos, contratistas y terceros deben tomar conciencia de su aporte a la eficacia de la seguridad de la información, y aplicarla en beneficio de una mejora del desempeño de sus funciones.
- Todas las servidoras y servidores públicos, contratistas y terceros que se desvinculen de la entidad, deben entregar de manera formal a los supervisores y/o jefes inmediatos, todos los elementos tanto de información física, digital y demás que le fueron entregados o producto de sus funciones u obligaciones.
- Solicitar la expedición del carné que lo acredita como servidora, servidor público y contratista de la Secretaría Distrital de la Mujer.
- Todas las servidoras y servidores públicos, contratistas y terceros deben mantener la confidencialidad de la información por fuera de las instalaciones de la Secretaría Distrital de la Mujer.
- La violación o incumplimiento de las responsabilidades y lineamientos definidos en el Manual de políticas de seguridad de la información de la Secretaría Distrital de la Mujer, será causa de la aplicación de acciones disciplinarias.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 16 de 43


- Todas las servidoras y servidores públicos, contratistas y terceros que participen en un proyecto, tendrán que estar alineados con las políticas de seguridad instauradas.
- Las políticas de seguridad serán dadas a conocer, a través de sensibilizaciones a cada dependencia o proceso, campañas de concientización, videos institucionales, correo electrónico e intranet, para crear en todas las servidoras, servidores públicos, contratistas y terceros una cultura de seguridad.
- Cada usuaria(o) será directamente responsable de clasificar su información y poder someterla a los controles instaurados dependiendo del nivel de confidencialidad, integridad y disponibilidad que requiera.
- Todas las servidoras y servidores públicos, contratistas y terceros, están obligados a hacer un buen uso, racional y ético de los servicios tecnológicos (internet, telefonía fija, móvil, celular, aplicativos, herramientas colaborativas, correo electrónico y demás) provistos por la Entidad, para el debido cumplimiento de sus funciones y actividades contractuales, so pena de las acciones disciplinarias y legales a que haya lugar.
- No se tiene permitido instalar ningún tipo de software en los equipos institucionales.
- Está prohibido omitir, retardar o no suministrar debida y oportuna respuesta a las peticiones, así como retenerlas o enviarlas a un destinatario que no corresponde.
- Está prohibido ocasionar daño o dar lugar a la pérdida de expedientes, documentos o archivos que hayan llegado a su poder por razón de sus funciones/actividades.
- Está prohibido permitir el acceso o exhibir expedientes, documentos, información o archivos a personas no autorizadas.

## 8. POLÍTICA DE DISPOSITIVOS MÓVILES

Gestión de acceso de los dispositivos móviles a la infraestructura tecnológica de la Entidad.

- Los usuarios no deben modificar las configuraciones de seguridad de los dispositivos móviles institucionales, ni instalar programas, ni cambiar las configuraciones de software con las que fueron entregados por la entidad.
- Se debe realizar la actualización de software de los dispositivos móviles (celulares, tabletas, portátiles, otros) institucionales cuando sea requerido y solicitar el apoyo del equipo de soporte de la Oficina Asesora de Planeación – Gestión Tecnológica).
- No está permitido el almacenamiento de información de tipo multimedia, personal o institucional en los dispositivos móviles, para lo anterior se debe hacer uso de los servicios de nube provistos por la Entidad tales como correo, OneDrive y Teams.
- No se permite el almacenamiento de información de credenciales y contraseñas de acceso a los servicios tecnológicos de la Entidad (correo, Teams, OneDrive, otros), en los dispositivos móviles institucionales.
- La Oficina Asesora de Planeación, a través del proceso de Gestión Tecnológica, ha implementado




 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 17 de 43

mecanismos de seguridad para establecer conexiones remotas o VPN hacia la plataforma tecnológica de la Secretaría Distrital de la Mujer.

- Para poder acceder a los servicios de conectividad (wifi), se debe hacer la solicitud por medio del aplicativo de mesa de ayuda, en cuyo caso será validada y gestionada.
- Todas las servidoras, servidores públicos y contratistas a los que se asignen dispositivos móviles, serán responsables del adecuado uso y cuidado de los mismos, en caso de daño por uso indebido, pérdida o robo, deberá notificarlo a la jefa de la Oficina Asesora de Planeación y realizar la reposición del equipo por uno de las mismas, similares o superiores características técnicas, en un plazo no superior a 30 días calendario.
- Todos los dispositivos móviles deben tener configurada una contraseña de acceso y activación del cifrado de disco con Bitlocker con lo cual se minimizan los riesgos asociados a seguridad de la información. En caso de requerirlo debe hacer la solicitud por medio del aplicativo de mesa de ayuda, será validada y gestionada por la Oficina Asesora de Planeación – Gestión Tecnológica.
- Los dispositivos móviles institucionales deben tener instaladas únicamente las aplicaciones autorizadas y configuradas por la Oficina Asesora de Planeación – Gestión Tecnológica.
- Los dispositivos móviles asignados por la Secretaría Distrital de la Mujer deben tener la configuración realizada por la Oficina Asesora de Planeación – Gestión Tecnológica. Asimismo, solo podrá configurarse las cuentas de correo electrónico institucional.
- El sistema de mensajería instantánea autorizado para los dispositivos móviles y de escritorios institucionales es Microsoft Teams.
- Los teléfonos móviles institucionales deben tener únicamente la tarjeta sim asignada por la Entidad, de igual forma la tarjeta sim únicamente debe instalarse en los teléfonos móviles institucionales.
- Los teléfonos móviles institucionales, deben permanecer encendidos y cargados durante las horas laborales de acuerdo con la responsabilidad y requerimientos propios de la dependencia encargada.
- Es responsabilidad de las servidoras y servidores públicos, contratistas y terceros, hacer buen uso de los dispositivos móviles suministrados por la Entidad, para la realización de las actividades propias de su cargo.
- Es responsabilidad de las servidoras y servidores públicos, contratistas y terceros, usuarios de dispositivos móviles evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando al máximo el extravío o hurto del equipo.
- Los dispositivos móviles institucionales no deben ser usados o conectados a redes wifi-públicas de (restaurantes, cafeterías, hoteles, aeropuertos, entre otras).
- Los dispositivos móviles institucionales deben tener instalado y actualizado el software contra códigos maliciosos, y el firewall para prevenir accesos no autorizados.
- El acceso al dispositivo móvil debe estar protegido por una contraseña de encendido la cual se define en la BIOS (Basic Input Output System) del equipo.


## 8.1. POLÍTICA DE TELETRABAJO

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 18 de 43

La Secretaría Distrital de la Mujer, protege la información institucional a la que tienen acceso las servidoras, servidores públicos, contratistas y terceros, desde lugares remotos, por razón y naturaleza de su cargo y actividades contractuales, por lo tanto, el acceso a la información desde ubicaciones diferentes a la oficina puede ser permitida si se demuestra que la información requerida es necesaria para el cumplimiento de sus funciones o actividades, y que existe un control de acceso dado con autorización previa de la jefa(e) inmediato y la aprobación por parte de la jefa(e) de la Oficina Asesora de Planeación y controlado por Gestión Tecnológica, con el fin de garantizar el cumplimiento de esta política. Se establecen los siguientes lineamientos:


- Con ocasión de la implementación de la política de teletrabajo en la Secretaría Distrital de la Mujer, se establece que las herramientas oficiales y permitidas para la realización de las actividades relacionadas con teletrabajo son:
  - Microsoft Teams
  - OneDrive
  - Correo electrónico
- El uso de medios de comunicación como WhatsApp debe ser previamente validado y aceptado por los grupos internos de trabajo, en los cuales se acuerda el uso de este en horas laborales, respetando en todo caso las horas de descanso y fines de semana.
- No está autorizado el uso de WhatsApp para hacer intercambio de información de la Secretaría Distrital de la Mujer, dicha información debe ser enviada o compartida únicamente por medio del uso de las herramientas oficiales antes mencionadas.
- La herramienta oficial de chat y llamadas aprobada por la Secretaría Distrital de la Mujer, son las de Microsoft Teams, las cuales todas las servidoras, servidores públicos, y contratistas deben mantener activos durante su horario laboral y responder con la debida diligencia, tal como si estuviesen realizando sus funciones y actividades en las instalaciones físicas de la entidad.
- En relación con los listados de asistencia, la Secretaría Distrital de la Mujer define que se deben gestionar de la misma forma que se hace cuando las actividades se desarrollan en sitio. Es responsabilidad de cada grupo interno de trabajo la adecuada gestión y resguardo de las mismas, mediante el buen uso de los permisos de acceso que se pueden aplicar a las herramientas antes mencionadas. En relación con lo anterior es de obligatorio cumplimiento que el realizador de las reuniones descargue el listado de participantes de la reunión que genera Microsoft Teams y lo guarde en un equipo de Teams generado al interior de cada área, para llevar el control de asistencia.
- Es responsabilidad de la teletrabajadora(or) garantizar el cumplimiento y disponibilidad de los siguientes requisitos mínimos:
  - Un computador de escritorio o portátil, adecuado para la realización de sus funciones o actividades contractuales.
  - Conexión estable a internet.
  - Tener disponibles y activas las herramientas para teletrabajo en las horas laborales.
  - Un espacio adecuado para la realización de sus funciones o actividades contractuales.
  - Disciplina y cumplimiento del horario laboral, o de las actividades o productos en el caso de los contratistas.
  - Responder de forma oportuna los mensajes, llamadas, correos electrónicos y demás acordados con la jefa(e) inmediato (herramientas oficiales).

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 19 de 43

- Realizar las respectivas pausas activas en concordancia con lo establecido en materia de Seguridad y Salud en el Trabajo.
  - Realizar de forma periódica las actualizaciones de sistemas operativos, software antivirus.
  - No se encuentra permitido el almacenamiento de información institucional en los dispositivos móviles (equipos portátiles) de propiedad de las servidoras, servidores públicos, y contratistas, dicha información se trabajará de forma local según las necesidades del servicio y luego se cargará a Teams o OneDrive y será eliminada del equipo.
- El acceso remoto se puede realizar desde equipos propiedad de la Entidad y equipos de propiedad de las servidoras y servidores públicos, contratistas y terceros debidamente autorizados y configurados por la Oficina Asesora de Planeación – Gestión Tecnológica, que cumplan con niveles de seguridad aceptables antes de permitir la conexión remota a los servicios o recursos de la infraestructura tecnológica de la Secretaría Distrital de la Mujer.
  - Los equipos en los que se realice teletrabajo deben contar con protección contra software malicioso debidamente actualizado, como mínimo debe estar activo Windows Defender y el firewall.
  - Es responsabilidad de los usuarios realizar copias de respaldo de la información de forma mensual y debidamente organizada en su repositorio de OneDrive, para asegurar la continuidad de las funciones realizadas.
  - Todas las servidoras, servidores públicos, contratistas y terceros que requieran conexión remota a los servicios o información de la Secretaría Distrital de la Mujer, deben ser previamente autorizados por la Oficina Asesora de Planeación – Gestión Tecnológica.
  - La conexión remota a servicios o información de la Secretaría Distrital de la Mujer se realiza a través de canales de comunicación seguros como redes privadas virtuales – VPN, en cuyo caso se tendrá en cuenta la disponibilidad de VPN o recursos tecnológicos necesarios para tal fin.
  - El propietario de los activos de información, con el apoyo de la Oficina Asesora de Planeación – Gestión Tecnológica, identificará los riesgos potenciales que puede generar el uso de la información institucional de forma remota, asimismo, adoptará los controles necesarios para la mitigación de dichos riesgos.
  - En caso de pérdida, suplantación de identidad o robo de un equipo portátil o cualquier medio de almacenamiento que contenga información relacionada con la Secretaría Distrital de la Mujer, se realiza inmediatamente el reporte a la jefa(e) inmediata y también realizar la respectiva denuncia ante las autoridades competentes, de la misma forma se requiere realizar el reporte en el aplicativo de mesa de ayuda.

## **8.2. POLÍTICA DE USO DE HERRAMIENTAS COLABORATIVAS (TEAMS, ONEDRIVE)**

- La Secretaría Distrital de la Mujer, proporcionará y garantizará el acceso a las servidoras y servidores públicos, contratistas, a las herramientas de chat, llamadas y reuniones para efectos de comunicación oficial, lo anterior por medio de las herramientas colaborativas.
- La Secretaría Distrital de la Mujer, en cabeza de la Oficina Asesora de Planeación – Gestión Tecnológica, realizará por lo menos una vez al año, jornadas de sensibilización en la

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 20 de 43


apropiación, uso y buenas prácticas en el manejo y uso de las herramientas colaborativas dirigidas a las servidoras y servidores públicos, contratistas, las cuales serán de asistencia obligatoria y oportuna, con la finalidad de aclarar dudas, vacíos y establecer la metodología de empleo de estas.

- La Secretaría Distrital de la Mujer, en cabeza de la Oficina Asesora de Planeación – Gestión Tecnológica, realizará por lo menos una vez al año, jornadas de concientización sobre seguridad informática, en las cuales se buscará evitar errores del personal ante intentos de ciberdelinquentes de explotar dichos errores, por medio de correo ficticios, de llamadas, entre otros.
- Las servidoras y servidores públicos, contratistas están obligados a realizar uso de las herramientas colaborativas de video conferencia y chat como medio oficial para todos los efectos del cumplimiento de sus funciones y actividades contractuales y de todas aquellas de carácter institucional.
- Es responsabilidad de las servidoras y servidores públicos, contratistas reportar de forma oportuna a la Oficina Asesora de Planeación – Gestión Tecnológica, cualquier anomalía que se pueda considerar como un posible fraude o ataque informático en el cual le soliciten entregar datos personales, o de la entidad, transferencia de fondos por medio de mensajes falsos, o cualquier otra acción sospechosa, lo anterior está tipificado como Business Email Compromise – BEC, que también se podría presentar en las herramientas colaborativas.
- La Oficina Asesora de Planeación – Gestión Tecnológica, enviará por lo menos una vez al año por correo electrónico a las servidoras y servidores públicos, contratistas, un listado de contactos útiles y de los accesos a los sistemas de información, servicios informáticos y demás provistos por la Entidad.

### **8.3. POLÍTICA DE TELEFONÍA MÓVIL, CELULAR Y FIJA**

Teniendo en cuenta la necesidad de cubrir el servicio de comunicaciones unificadas, para el caso de telefonía que requiere la Secretaría Distrital de la Mujer, en el marco del cumplimiento de los objetivos estratégicos y misionales, se disponen en el presente manual de políticas los controles aplicables, que las servidoras y servidores públicos, contratistas y terceros deben cumplir de forma obligatoria, con ocasión de la ejecución de sus funciones y actividades contractuales con la Entidad.

- En caso de requerir habilitar las funcionalidades de llamadas nacionales, internacionales y a celular, se debe tramitar por medio de un requerimiento a través del aplicativo de mesa de ayuda dirigido a la jefa de la Oficina Asesora de Planeación, solicitando la activación de un código asociado a la extensión que requiere la funcionalidad, la cual se debe realizar y justificar en el marco de las disposiciones legales vigentes, así como en materia del logro de los objetivos institucionales, por parte de la jefa(e) inmediato de la dependencia que requiere la activación del servicio, quienes son los directos responsables del buen uso que se debe realizar de los bienes y servicios públicos distritales, de los cuales se tiene el deber de salvaguardar, usar y custodiar de forma apropiada. Es de aclarar que los costos directos asociados a la activación y uso de dicho servicio irán con cargo al presupuesto del proyecto que lo solicita.
- Es responsabilidad de las servidoras y servidores públicos, contratistas y terceros, hacer un uso responsable y ético de los servicios de telefonía, aclarando que estos servicios no están disponibles para cubrir temas personales y son de uso exclusivo institucional, el cual también

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 21 de 43

debe ser racionalizado. En caso de detectar que se utilizan de forma personal o irracional, se informará a las dependencias competentes para iniciar las respectivas acciones legales a las que haya lugar.

### 8.3.1. Niveles de acceso a los servicios de Telefonía:


No.	NIVEL DE ACCESO	PERSONAL ASIGNADO
1	Llamadas locales y extensiones internas.	Todas las servidoras, servidores públicos y contratistas.
2	Llamadas nacional e internacional.	Secretaria de la Mujer
3	Llamadas nacional e internacional.	Servidoras, servidores públicos y contratistas que requieran del servicio para el cumplimiento de sus funciones y actividades misionales (previa solicitud y aprobación de la jefa(e) inmediato y aprobación de la jefa de la Oficina Asesora de Planeación, tener en cuenta los costos directos que ocasiona al proyecto que lo requiere).

- En caso de identificar llamadas que no están debidamente registradas y justificadas, se notificará a la dependencia correspondiente para que en un máximo de dos (02) días hábiles se realicen los ajustes pertinentes. En caso de no poder justificarlo se realizará el reporte al área encargada para efectuar los cobros a que haya lugar a las servidoras, servidores públicos y contratistas.
- Todas las servidoras, servidores públicos y contratistas a los que se asignen teléfonos fijos y celulares, serán responsables del adecuado uso y cuidado de los mismos, en caso de daño por uso indebido, pérdida o robo en cuyo evento deberá notificarlo a la jefa de la Oficina Asesora de Planeación y realizar la reposición del equipo por uno de las mismas, similares o superiores características técnicas, en un plazo no superior a 30 días calendario.
- En caso de detectar que los códigos asignados a las servidoras, servidores y contratistas tengan un uso inapropiado o sean utilizados por otros funcionarios, serán responsables de las acciones disciplinarias y legales a que haya lugar.
- Se encuentra prohibido la alteración y cambio de configuración de los teléfonos IP y celulares de la Entidad.
- En caso de requerir realizar llamadas a celulares, se debe solicitar el servicio a las dependencias que cuentan con dicho servicio.
- No es permitido el daño o alteración de las características físicas o técnicas de los equipos celulares o de telefonía IP.

### 8.4. POLÍTICA CORREO ELECTRÓNICO INSTITUCIONAL

Las servidoras, servidores públicos y contratistas a quienes la Secretaría Distrital de la Mujer les asigne una cuenta de correo electrónico institucional, aceptan expresamente que este es un servicio de comunicaciones institucionales y se obligan a respetar y a cumplir los siguientes lineamientos:

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*


 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 22 de 43

- La cuenta de correo electrónico institucional es personal e intransferible, la usuaria(o) de la misma se hace responsable del buen uso y todas las acciones efectuadas sobre la misma.
- La cuenta de correo electrónico institucional debe ser usada únicamente para el desempeño de las funciones u obligaciones contractuales asignadas dentro de la Secretaría Distrital de la Mujer.
- El envío de información institucional debe ser realizado exclusivamente desde la cuenta de correo electrónico que la Secretaría Distrital de la Mujer le proporcionó para tal fin. De igual manera, las cuentas de correo asignadas a las dependencias o áreas de la Entidad no se deben emplear para uso personal.
- De acuerdo con la política de cero papel, se debe priorizar el uso interno del correo electrónico sobre el envío de documentos en físico, salvo en los casos que sea estrictamente necesario.
- Los mensajes y la información contenida en los buzones de correo son propiedad de la Secretaría Distrital de la Mujer y cada usuaria(o), como responsable de su buzón debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones u obligaciones.
- Las servidoras y servidores públicos y contratistas al finalizar su vinculación con la Secretaría Distrital de la Mujer pueden solicitar el backup de su buzón de correo electrónico institucional, previa autorización del jefe inmediato y se debe realizar a través del aplicativo de mesa de ayuda, para lo cual deberá entregar a La Oficina Asesora de Planeación - Gestión Tecnológica un medio de almacenamiento externo para tal fin.
- En caso de requerir realizar envío masivo de mensajes se debe solicitar por medio del aplicativo de mesa de ayuda, previo visto bueno de Comunicaciones, informando la fecha de inicio y fin de la solicitud.
- Terminada la vinculación laboral o contractual con la entidad, la Oficina Asesora de Planeación - Gestión Tecnológica realizará un respaldo del correo electrónico, el cual será resguardado por un periodo de 1 (un) año.

No está permitido:

- Enviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario ni corporativo, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, que vayan en contra de las leyes, o del principio de moralidad administrativa que inciten a realizar prácticas ilícitas o promuevan actividades ilegales o cualquier otro tipo de mensajes que atenten contra la dignidad y la productividad de las servidoras(es) y contratistas de la Entidad o de otras entidades u organismos distritales, o el normal desempeño del servicio de correo electrónico en la Secretaría Distrital de la Mujer.
- Utilizar la dirección de correo electrónico de la Secretaría Distrital de la Mujer como punto de contacto en sitios de comercio, redes sociales tales como Facebook, Twitter, Instagram, MySpace, LinkedIn, entre otras, o cualquier otro sitio que no se tenga descrito en el presente y que no tenga que ver con el cumplimiento de las actividades laborales o contractuales.

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 23 de 43

- El envío y recepción de archivos que contengan extensiones ejecutables.
- El envío de archivos de música y videos.
- Toda información de la Secretaría Distrital de la Mujer generada con los diferentes programas computacionales (Ej. Office, Project, Access, etc.), que requiera ser enviada fuera de la Entidad, y que por sus características de confidencialidad e integridad deba ser protegida, debe estar en formatos no editables (PDF), utilizando las características de seguridad que brindan las herramientas ofimáticas con las que cuenta la Entidad. La información puede ser enviada en el formato original bajo la responsabilidad de las servidoras y servidores remitentes de la misma, únicamente cuando la receptora o receptor de dicha información requiera hacer modificaciones.
- Todos los mensajes enviados deben respetar el estándar de formato, firma e imagen corporativa definido por la Secretaría General de la Alcaldía Mayor de Bogotá D.C., y deben incluir en todos los casos el mensaje legal corporativo de confidencialidad.
- Los correos electrónicos catalogados como tipo SPAM (Cadenas de correos o correos dirigidos masivamente a diferentes destinatarios) deberán ser reportados por la usuaria(o) a Gestión Tecnológica a través del aplicativo de mesa de ayuda y serán tratados como incidentes de seguridad de la información.
- No está permitido el envío o reenvío de ningún tipo de SPAM.
- Todos los mensajes de los cuales se desconozca su origen, remitente o contenido, o se consideren sospechosos, no deben ser abiertos, y es deber inmediato de las servidoras y servidores públicos, y contratistas reportar a la Oficina Asesora de Planeación - Gestión Tecnológica lo sucedido, a través del aplicativo de mesa de ayuda, estos serán tratados como incidentes de seguridad de la información.


### **8.5. POLÍTICA ACCESO A INTERNET**

El internet es una herramienta de trabajo que permite consultar y/o ingresar a muchos sitios web relacionados o no con las actividades propias de la Secretaría Distrital de la Mujer, por lo cual, el uso adecuado de este recurso se debe controlar, verificar y/o monitorear, considerando en todos los casos los siguientes lineamientos:

No está permitido:

- El acceso a páginas relacionadas con pornografía, drogas, alcohol, webproxys, hacking y/o cualquier otra página que vaya en contra de la ética, las leyes vigentes o políticas aquí establecidas.
- El acceso y el uso de servicios interactivos o mensajería instantánea como, Twitter, Web WhatsApp, Instagram, Software para intercambio de archivos P2P, emisoras online, chats personales y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o para fines diferentes a las actividades propias de la Secretaría Distrital de la Mujer.
- El acceso y el uso de servicios interactivos de redes sociales como son Facebook, YouTube,

*Nota: Si usted imprime este documento se considera "Copia No Controlada", por lo tanto, debe consultar la versión vigente en el sitio oficial de los documentos del SIG.*

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 24 de 43

Instagram, entre otros, en la actualidad se encuentra restringido para uso a nivel personal. En caso de que un área o dependencia requiera activarlo con el ánimo de acceder a información de tipo institucional o distrital, debe realizar la solicitud a través del aplicativo de mesa de ayuda, con la debida aprobación y justificación de la jefa(e) inmediato, autorizando exclusivamente a una servidora, servidor público o contratista por área o dependencia, lo anterior se aplica por temas de garantizar el adecuado uso del canal de internet en la Entidad. Posterior a lo anterior, se emitirá la aprobación o no, por parte de la jefa(e) de la Oficina Asesora de Planeación.

- El intercambio de información no autorizada con terceros, por ser de propiedad de la Secretaría Distrital de la Mujer, de sus servidoras y servidores públicos, contratistas y de la comunidad en general.
- La descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual en la Entidad, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros.
- La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet, y/o cualquier tipo de material audiovisual que no cuente con los debidos permisos o licencias de uso.
- Cada uno de los usuarios es responsable de dar un uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas, que atenten contra sus compañeras y compañeros de la Entidad, contra los servidores de otras entidades públicas, contra terceros de la comunidad en general, contra la normativa vigente o contra los lineamientos de seguridad de la información, entre otros.
- Las servidoras y los servidores, al igual que los contratistas de la Entidad y la comunidad en general, no pueden asumir en nombre de la Secretaría Distrital de la Mujer, posiciones personales en encuestas de opinión, foros u otros medios similares.
- El uso de Internet no considerado dentro de las anteriores restricciones está permitido, siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad ni la protección de la información de la Secretaría Distrital de la Mujer.
- La autorización de acceso a Internet se concede exclusivamente para actividades de trabajo. Todos las servidoras y servidores públicos, contratistas y terceros de la Secretaría Distrital de la Mujer tienen las mismas responsabilidades en cuanto al uso de Internet.

## 8.6. RECURSOS TECNOLÓGICOS

El uso adecuado de los recursos tecnológicos asignados por la Secretaría Distrital de la Mujer a sus servidores públicos, y contratistas y la comunidad en general se realizará bajo los siguientes lineamientos:




 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 25 de 43

- La instalación de cualquier tipo de software o hardware en los equipos de cómputo de la Secretaría Distrital de la Mujer es responsabilidad de la Oficina Asesora de Planeación – Gestión Tecnológica, y, por tanto, esta dependencia es la única autorizada para realizar esta labor. Asimismo, los medios de instalación de software deben ser los proporcionados por la Secretaría Distrital de la Mujer a través de esta Área.
- Los usuarios no deben realizar cambios en las estaciones de trabajo, relacionados con la configuración del equipo, tales como conexiones de red, protectores de pantalla corporativos, entre otros. Estos cambios pueden ser realizados únicamente por la Oficina Asesora de Planeación.
- La Oficina Asesora de Planeación debe definir y actualizar de manera periódica, la lista de software y aplicaciones autorizadas que se encuentran permitidas para ser instaladas en las estaciones de trabajo de los servidores públicos, y contratistas. Asimismo, la Oficina Asesora de Planeación debe realizar el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
- Únicamente los servidores públicos, y contratistas autorizados por la Oficina Asesora de Planeación, previa solicitud de la dependencia que lo requiera a través del aplicativo de mesa de ayuda puede conectarse a la red inalámbrica de la Secretaría Distrital de la Mujer.
- La conexión a redes inalámbricas externas para usuarios con equipos portátiles que estén fuera de la oficina y que requieran establecer una conexión a la infraestructura tecnológica de la Secretaría Distrital de la Mujer, debe hacerse bajo los esquemas y herramientas de seguridad autorizados y establecidos por la Oficina Asesora de Planeación.
- Sólo el personal autorizado puede realizar actividades de administración remota de dispositivos, equipos o servidores de la infraestructura tecnológica de la Secretaría Distrital de la Mujer. Las conexiones establecidas para este fin deben utilizar los esquemas y/o herramientas de seguridad y administración definidos por la Oficina Asesora de Planeación.
- La sincronización de dispositivos móviles, tales como celulares, tabletas portátiles u otros dispositivos electrónicos sobre los que se puedan realizar intercambios de información con cualquier recurso de la Secretaría Distrital de la Mujer, debe estar autorizada de forma explícita por la dependencia respectiva, en conjunto con la Oficina Asesora de Planeación - Gestión Tecnológica.
- Los servidores públicos, y contratistas y la comunidad en general, que tengan acceso a los equipos que componen la infraestructura tecnológica de la Secretaría Distrital de la Mujer no pueden fumar, o consumir alimentos cerca de los equipos.

## **8.7. CABLEADO ESTRUCTURADO**

- En los puntos de red de las estaciones de trabajo no está permitido realizar conexiones de Switch, Access Point u otros dispositivos de red para realizar derivaciones, ni se permite realizar conexiones o derivaciones eléctricas que pongan en riesgo la seguridad física por fallas en el suministro eléctrico.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 26 de 43

- Todos los proyectos que realicen las dependencias o áreas de la Secretaría Distrital de la Mujer, que involucren la disponibilidad de puntos de red y puntos eléctricos, deben ser previamente consultados con La Oficina Asesora de Planeación – Gestión Tecnológica, teniendo en cuenta la disponibilidad o posibilidad de habilitación o provisión de los mismos, de acuerdo con la capacidad técnica y capacidades físicas de las instalaciones (edificios, sedes, casas, oficinas, etc.)

## 8.8. SISTEMAS DE INFORMACIÓN

Las credenciales (usuario y clave) de acceso a la red y a recursos informáticos son de carácter estrictamente personal e intransferible; los servidores públicos y contratistas de la Secretaría Distrital de la Mujer no deben revelar éstas a terceros, ni utilizar claves ajenas. Todo servidor público o contratista será responsable del cambio de clave de acceso a los sistemas de información o recursos informáticos periódicamente.

Cuando se presenten ausencias de servidores públicos o contratistas por incapacidades prolongadas, licencias, o suspensión de contrato, es responsabilidad de la Dirección de Talento Humano y la Dirección de Contratación notificar este evento con una solicitud a La Oficina Asesora de Planeación - Gestión Tecnológica a través de la mesa de ayuda, para bloquear el usuario de dominio, con el fin de evitar la exposición de la información y el acceso de terceros, que puedan generar daño, alteración o uso indebido de la información, así como evitar la suplantación de identidad.

## 9. SEGURIDAD DE LOS RECURSOS HUMANOS

La Secretaría Distrital de la Mujer, a través de la Dirección de Talento Humano y la Dirección de Contratación es responsable de divulgar la Política de Seguridad de la Información a todas(os) las(os) servidoras y servidores públicos, contratistas y terceros que se vinculen a la Entidad.


La Dirección de Contratación debe realizar las tareas pertinentes para que todos los contratos de prestación de servicios incorporen las obligaciones que exijan el cumplimiento de la Política de Seguridad de la Información, el manejo confidencial de la información y la cesión de derechos de autor para la Entidad.

Cuando una(un) servidora(or) o contratista cese sus funciones o culmine la ejecución del contrato en la Secretaría Distrital de la Mujer, el jefe inmediato o supervisora(or) del contrato será la(el) encargado de la custodia de los recursos de información.

## 10. GESTIÓN DE ACTIVOS

### 10.1. GESTIÓN DE MEDIOS DE ALMACENAMIENTO

- La Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica debe administrar de forma correcta y óptima el almacenamiento y custodia de los medios de Backup y otros

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 27 de 43

medios digitales o magnéticos de almacenamiento de la Entidad.

- Ninguna servidora ni servidor público, contratista y tercero de la Secretaría Distrital de la Mujer debe copiar, almacenar y/o divulgar información Institucional en medios de almacenamiento personales.
- Todos los servidores públicos y contratistas de la Secretaría Distrital de la Mujer son responsables de la custodia y el resguardo de los medios de almacenamiento institucionales que se encuentren asignados en su inventario.
- El traslado de medios físicos, equipos de cómputo, equipos de comunicaciones entre otros, debe realizarse en un medio de transporte confiable y seguro, con el fin de garantizar su integridad, confidencialidad y disponibilidad.


## 11. CONTROL DE ACCESO Y SEGURIDAD DE LA INFORMACIÓN

### 11.1. CONTROL DE ACCESO:

La Secretaría Distrital de la Mujer, generará controles de acceso que permitan garantizar la protección de la data generada, los cuales van encaminados a garantizar que el acceso a la información independientemente del equipo en el cual repose, no será accedido por personal no autorizado.

Lo anterior, de acuerdo con los controles establecidos en el anexo A de la norma ISO/IEC 27001:2013 y que se referencian a continuación:

- Registro y cancelación de Usuarios: Asegurar el acceso de los usuarios autorizados e impedir el acceso no autorizado a sistemas y servicios.
- Gestión de derechos de acceso privilegiado: Se debe controlar la asignación de usuarios con privilegios elevados, para los sistemas de información y para la infraestructura tecnológica de la entidad.
- Uso de información secreta: Establecer responsabilidades a los usuarios sobre la custodia de su información de autenticación secreta.
- Restricción de acceso a Información: Restringir el uso no autorizado de sistemas y aplicaciones, con controles de acceso basados en permisos de usuario.
- Todos los recursos de información críticos de la Secretaría Distrital de la Mujer tienen asignados los privilegios de acceso de usuarios a partir de los roles y perfiles que cada servidora o servidor público y contratista requiera para el desarrollo de sus funciones y obligaciones, definidos y aprobados por las áreas y/o procesos de la entidad y son administrados por la Oficina Asesora de Planeación a través del Proceso de Gestión Tecnológica.
- Todo servidor público o tercero que requiera tener acceso a los sistemas de información de la Secretaría Distrital de la Mujer debe estar debidamente autorizado y debe acceder a dichos sistemas haciendo uso como mínimo de un usuario (ID) y una contraseña (password) asignado por la Entidad. El servidor público o tercero debe ser responsable por el buen uso de las credenciales de acceso

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 28 de 43


asignadas.

- Todos los activos de información adquiridos y dados de baja deben ser reportados por el responsable de este mediante los formatos establecidos para tal fin.
- Cuando un activo de información es reasignado a otra persona, se debe reportar de forma oficial a quien corresponda, empleando los mecanismos establecidos por la Entidad.
- Todos los activos de información de la Secretaría Distrital de la Mujer, tienen asignado un custodio que tiene la responsabilidad de mantener los controles adecuados para su protección.
- El personal que fue designado como propietario de la información de la Secretaría Distrital de la Mujer, son los encargados de clasificarla de acuerdo con su grado de sensibilidad y criticidad, de documentar y mantener actualizada la clasificación efectuada, y de definir quiénes deben tener permisos de acceso a la información.

## 12. CRIPTOGRAFÍA

La Secretaría Distrital de la Mujer, en cabeza de la Oficina Asesora de Planeación - Gestión Tecnológica, desarrollará las estrategias para proteger la confidencialidad, integridad y disponibilidad de la información, mediante el uso e implementación de técnicas de cifrado para asegurar que la información se proteja adecuadamente. Para lo cual se debe tener en cuenta:

- Implementar controles criptográficos para proteger la información de la entidad que garanticen la confidencialidad, integridad y disponibilidad de la información se debe realizar un análisis de riesgos, que indique los activos de información que requieran estos controles.
- Para la implementación de los controles criptográficos necesarios para proteger los activos de información identificados, resultantes del análisis de riesgo, se debe formular un plan de implementación.
- Es responsabilidad de la Alta Dirección, analizar el plan de implementación de controles criptográficos y asignar los recursos necesarios, sujetos a la planeación, capacidad financiera y presupuestal de la entidad. Se deben utilizar como mínimo controles criptográficos para:
  - Firma electrónica.
  - Autenticación electrónica.
- Las firmas digitales proporcionan un medio de protección de la autenticidad e integridad de los documentos electrónicos, estas pueden aplicarse a cualquier tipo de documento que se procese electrónicamente.
- Al utilizar firmas y certificados digitales, se debe considerar la legislación vigente que describa las condiciones bajo las cuales una firma digital es legalmente válida.
- Se proporcionará una protección adecuada a la infraestructura utilizada para generar, almacenar y archivar claves, considerándola crítica o de alto riesgo.
- Cuando las claves sean comprometidas o cuando un empleado se desvincula de la Secretaría Distrital de la Mujer, se deben revocar los certificados o firmas digitales.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 29 de 43


- La Secretaría Distrital de la Mujer por medio de la Oficina Asesora de Planeación - Gestión Tecnológica, debe aplicar estándares relacionados con algoritmos de cifrado, las longitudes de clave a utilizar y los casos de utilización de cada uno, en lo relacionado con servicios de certificados de sitio seguro, almacenamiento de contraseñas en bases de datos, entre otros servicios.
- Las contraseñas para cifrado de información deben cumplir con la política de contraseñas definidas (caracteres especiales, alfanuméricos y de longitud definida).
- Con el ánimo de reducir la probabilidad de compromiso, las claves deben tener fechas de inicio y caducidad definidas, de manera que sólo puedan ser utilizadas por un lapso no mayor a 12 meses.
- Se deben utilizar algoritmos de cifrado y tamaños de clave que se consideren seguros. Se debe verificar esta condición periódicamente con el objeto de efectuar las actualizaciones correspondientes

Se deben implementar controles criptográficos en:

- Se debe cifrar toda información que sea considerada como crítica para el desarrollo de las operaciones de la Entidad, que pudiera estar expuesta a usuarios no autorizados, en relación con su integridad y confidencialidad. Esto se debe hacer en almacenamiento y en la transmisión de las transacciones de las aplicaciones.
- Para la transmisión de información crítica.
- Instalando certificados digitales en las aplicaciones web.
- Se debe hacer uso e implementación del cifrado por medio de Bitlocker en todos los dispositivos móviles institucionales, de la misma forma se debe activar en los equipos en que se requiera, previa solicitud del jefe inmediato y aprobación por parte de la jefe de la Oficina Asesora de Planeación.

### 13. SEGURIDAD FÍSICA Y DEL ENTORNO

- La Secretaría Distrital de la Mujer, a través de la Dirección de Administrativa y Financiera, debe implementar controles para proteger el perímetro de las instalaciones físicas, controlar el acceso de personas y la permanencia en las oficinas e instalaciones, además mitigar los riesgos y amenazas externas y ambientales, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información de la Entidad.
- Todos los servidores públicos, y contratistas y visitantes que se encuentren en las instalaciones de la Secretaría Distrital de la Mujer, deben estar debidamente identificados, con un documento que acredite su tipo de vinculación el cual deberá ser portado en un lugar visible.
- Se debe implementar un plan de mantenimiento de equipos para mantenerlos en buen funcionamiento y operativos.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 30 de 43

### 13.1. SEGURIDAD DE EQUIPOS Y ACTIVOS FUERA DEL PREDIO

La Secretaría Distrital de la Mujer por medio de la Dirección Administrativa y Financiera, adoptará medidas de seguridad para los activos que se encuentran fuera de las oficinas y/o dependencias de la misma, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones propias de la Entidad.

- Durante un viaje, las computadoras portátiles deberán ser llevadas como equipaje de mano y cuando sea posible, de manera disimulada.
- Seguir instrucciones de los fabricantes para proteger el equipo; por ejemplo, protección contra la exposición a fuertes campos electromagnéticos.
- Controles para el trabajo en casa a través de una evaluación del riesgo y los controles apropiados conforme sea apropiado; por ejemplo, archivos con llave, política de escritorio vacío, controles de acceso para las computadoras y una comunicación segura con la oficina (ver también ISO/IEC 18028 Seguridad de Redes).
- Seguro adecuado para proteger el equipo fuera de las instalaciones de la Entidad, controles para daño, robo o interceptación.

### 13.2. ESCRITORIO Y PANTALLA LIMPIA


Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia para las instalaciones de procesamiento de información.

Con el fin de evitar pérdidas, daños o accesos no autorizados a la información, todos los servidores de la Secretaría Distrital de la Mujer deben mantener la información restringida o confidencial bajo llave cuando sus puestos de trabajo se encuentren desatendidos o en horas no laborales. Esto incluye: documentos impresos, CD, dispositivos de almacenamiento USB y medios removibles en general. Adicionalmente, se requiere que la información sensible que se envía a las impresoras sea recogida manera inmediata.

Todas(os) las usuarias(os) son responsables de bloquear la sesión de su estación de trabajo en el momento en que se retiren del puesto de trabajo y desbloquear sólo con su contraseña. Cuando finalicen sus actividades, se deben cerrar todas las aplicaciones y dejar los equipos apagados. Si las usuarias(os) están ubicados cerca de zonas de atención al público, al ausentarse de su lugar de trabajo deben guardar documentos y medios de uso interno.

Todas las estaciones de trabajo deberán usar el papel tapiz y el protector de pantalla corporativo, el cual se activará automáticamente después de cinco (5) minutos de inactividad y se podrá desbloquear únicamente con la contraseña del usuario.

## 14. SEGURIDAD DE LAS OPERACIONES

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 31 de 43

La Secretaría Distrital de la Mujer a través de la Oficina Asesora de Planeación – Gestión Tecnológica, se debe encargar de la operación y administración de los recursos tecnológicos e implementar los controles asociados, para garantizar la confidencialidad, integridad y disponibilidad de la información. En tal sentido debe cumplir con los siguientes lineamientos:

- Implementar un procedimiento para la gestión o control de cambios en la configuración de los equipos, redes, sistemas de información, bases de datos, aplicaciones o cualquier activo de información o de Tecnologías de Información-TI, ser revisados, evaluados y aprobados.
- Implementar un plan de copias de seguridad que le permita proteger la información crítica alojada en el Centro de Datos de la Entidad, realizar pruebas de funcionamiento aleatorias para garantizar su posterior recuperación.

#### **14.1. PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS**

Se deben implementar controles de detección, de prevención y de recuperación, combinarlos con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos, lo anterior en aras de asegurar la data generada, así como la continuidad del negocio.


La Secretaría Distrital de la Mujer establece que todos los recursos informáticos deben estar protegidos mediante herramientas de hardware o software de seguridad como antivirus, antispam, antispysware u otras aplicaciones que brindan protección contra código malicioso y prevención del ingreso del mismo a la red institucional, en donde se cuente con los controles adecuados para detectar, prevenir y recuperar ante posibles fallos causados por código malicioso. Será responsabilidad de la Oficina Asesora de Planeación – Gestión Tecnológica, autorizar el uso de las herramientas y asegurar que éstas y el software de seguridad no sean deshabilitados en ninguna circunstancia, así como su actualización permanente. Asimismo, la Secretaría Distrital de la Mujer definió los siguientes lineamientos:

No está permitido:

- La desinstalación y/o desactivación del software y herramientas de seguridad, instaladas en los equipos de la Entidad, las cuales deben ser avaladas previamente por la Oficina Asesora de Planeación – Gestión Tecnológica.
- Escribir, generar, compilar, copiar, propagar, ejecutar o intentar introducir cualquier código de programación diseñado para auto replicarse, dañar o afectar el desempeño de cualquier dispositivo o infraestructura tecnológica.
- El uso de código móvil. Éste sólo podrá ser utilizado si opera de acuerdo con las políticas y normas de seguridad definidas y debidamente autorizado.

#### **14.2. COPIAS DE RESPALDO**

Consultar documento “ADMINISTRACIÓN DE BACKUPS Y RESTAURACIÓN DE LA INFORMACIÓN - V3 en Lucha.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 32 de 43

La Oficina Asesora de Planeación - Gestión Tecnológica, realizará copias de respaldo mensual de la información institucional contenida en los repositorios oficiales de cada área o proceso, software de base, e imágenes de los sistemas operativos de la infraestructura de servidores de la entidad y realizará pruebas de restauración aleatorias de acuerdo con la política de copias de respaldo definida. Lo anterior permite tener una protección frente a una eventual catástrofe.

La Secretaría Distrital de la Mujer debe asegurar que la información con cierto nivel de clasificación, la cual es definida por las áreas y/o procesos responsables de la misma, cuya información se encuentra contenida en la plataforma tecnológica de la Entidad, como servidores, dispositivos de red para almacenamiento de información, archivos de configuración de dispositivos de red y seguridad, entre otros, sea periódicamente resguardada mediante mecanismos y controles adecuados que garanticen su protección, integridad y disponibilidad. Se debe hacer pruebas aleatorias de restauración a intervalos regulares, con el fin de asegurar que son confiables en caso de emergencia, las copias de seguridad serán retenidas por un periodo de tiempo definido en el documento de Backup.

Las servidoras y servidores públicos y contratistas de la Entidad serán responsables de salvaguardar la información contenida en cada uno de sus equipos de trabajo en la unidad (D:) de cada estación de trabajo. Se precisa que las unidades de red para las áreas son un espacio de almacenamiento en disco que la entidad pone a disposición de sus usuarios para facilitar la puesta en común de documentos importantes, finales y de misión crítica de un grupo de trabajo, con el fin de facilitar sus funciones en su puesto de trabajo.


La Oficina Asesora de Planeación, a través del proceso de Gestión Tecnológica se encarga de mantener estos espacios de disco en unos equipos centrales, de forma que se gestiona la seguridad ante ataques, accesos no autorizados, virus, disponibilidad y recuperación de la información en caso de deterioro o pérdida dado que se realizan copias de seguridad diariamente.

La Oficina Asesora de Planeación – Gestión Tecnológica establecerá un procedimiento explícito de backup y recuperación de la información que incluya especificaciones acerca de la frecuencia, e información que se respaldará. Adicionalmente, debe disponer de los recursos necesarios para permitir la identificación de ubicación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

## 15. SEGURIDAD DE LAS COMUNICACIONES

- La Oficina Asesora de Planeación - Gestión Tecnológica es responsable de administrar y gestionar la red de la Secretaría Distrital de la Mujer.
- La Oficina Asesora de Planeación - Gestión Tecnológica debe segmentar las redes, con el fin de controlar el acceso a la red.
- Para propósitos de seguridad y mantenimiento de la red, el personal autorizado por la Oficina Asesora de Planeación - Gestión Tecnológica, puede monitorear los equipos de la Secretaría Distrital de la Mujer en cualquier momento.
- Todas las servidoras, servidores públicos, contratistas y terceros de la Secretaría Distrital de la Mujer



 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 33 de 43

deben dar cumplimiento a la reglamentación y leyes relacionadas con delitos informáticos como la Ley 1273 de 2009, asimismo, evitar prácticas o usos que puedan comprometer la seguridad de la información.

- Los terceros con quienes se establece intercambio de información de la Secretaría Distrital de la Mujer deben darle manejo adecuado a la información recibida, en cumplimiento de las políticas, cláusulas y de las condiciones contractuales establecidas.
- Todas las comunicaciones establecidas mediante el servicio de correo, buzones y copias de seguridad se consideran propiedad de la Secretaría Distrital de la Mujer y pueden ser revisadas en caso de requerirse, de una investigación o incidente de seguridad de la información.
- Se encuentra prohibido el uso y la conexión de dispositivos de red tales como: Modem, Router, entre otros, a la red de datos institucional. Así como también la manipulación de cualquier equipo de red por parte de los usuarios que no hacen parte de la Oficina Asesora de Planeación - Gestión Tecnológica.
- La Oficina Asesora de Planeación, a través del proceso de Gestión Tecnológica, permitirá las conexiones remotas a la plataforma tecnológica de la entidad, sólo al personal autorizado y por periodos de tiempo previamente establecidos, de acuerdo con las necesidades y las labores desempeñadas en la Entidad.
- Toda solicitud de conexión remota debe ser solicitada por medio del aplicativo de mesa de ayuda y debe contar con el visto bueno del jefe inmediato y la aprobación de la jefa de la Oficina Asesora de Planeación.

### **15.1. ACUERDOS DE CONFIDENCIALIDAD**

Acuerdos de confidencialidad o de no divulgación. La Secretaría Distrital de la Mujer, identificará, revisará regularmente y apoyará la definición de los requisitos para la definición de los acuerdos de confidencialidad o de no divulgación que reflejen las necesidades de la Entidad en cuanto a la protección de la información.

Las servidoras, servidores públicos, contratistas y terceros de la Entidad y la comunidad en general que requieran retirar información en el desarrollo de sus funciones o actividades, deberán firmar un “Acuerdo de Confidencialidad de la información”, donde individualmente se comprometan a no divulgar, usar o explotar la información confidencial a la que tengan acceso, respetando los niveles establecidos para la clasificación de la información, en los cuales deberá hacerse referencia a que cualquier violación a los mismos será considerado como un “incidente de seguridad”.

## **16. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**


- Se identifica y establecen los requisitos de seguridad en todas las fases del ciclo de vida de desarrollo de software, y se justifica, acuerda y documenta.
- Se incluyen puntos de chequeo de seguridad dentro de las fases del ciclo de vida de desarrollo de software.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 34 de 43

- El cambio de versión de las aplicaciones implementadas en el ambiente de producción se hace de acuerdo con los procedimientos estandarizados de control de cambios en sistemas de información, además, debe contar con controles de seguridad, para esto se hace una copia de respaldo en caso de que se deba realizar marcha atrás, para mantener la integridad de los datos y de los sistemas de información.
- Los sistemas de información que cuenten con ambiente de desarrollo y pruebas se deben utilizar exclusivamente para implementar nuevos desarrollos, modificación, ajuste y/o revisión de código, así como la realización de pruebas tales como verificar y aprobar nuevas funcionalidades técnicas del software, aplicación o sistema de información entre otras que se puedan requerir.
- El paso de software de un ambiente a otro es controlado y gestionado de acuerdo con lo definido en procedimientos estandarizados de control de cambios en sistemas de información.
- Se debe seguir un procedimiento formal para el paso de software, aplicaciones y sistemas de información de un ambiente a otro (desarrollo/pruebas y producción).
- Se deben definir nomenclaturas para identificar los ambientes (desarrollo/pruebas y producción), con el objetivo de evitar confusiones en la ejecución de actividades o procesos propios de cada uno.
- Los desarrolladores de los sistemas de información deben incluir buenas prácticas de desarrollo durante el ciclo de vida de estos, incluyendo lineamientos de seguridad desde el diseño hasta la puesta en producción.
- Los desarrolladores no deben permitir que en las configuraciones, implementaciones, respuestas del sistema o encabezados se divulgue información confidencial (contraseñas, información de la base de datos, direcciones IP, entre otras).
- Los desarrolladores deben eliminar todas las funcionalidades y archivos que no sean necesarios antes de la puesta en producción.
- Los desarrolladores deben evitar incluir las cadenas de conexión a las bases de datos en el código de los aplicativos.
- Los desarrolladores deben almacenar el código fuente de los aplicativos construidos, de tal forma de que no pueda ser descargado, copiado ni modificado por usuarios no autorizados.

## 17. RELACIONES CON LOS PROVEEDORES

- En todos los contratos o acuerdos con contratistas y terceros, que implique intercambio, uso o procesamiento de información de la Secretaría Distrital de la Mujer, se deben establecer acuerdos de confidencialidad sobre el acceso y tratamiento de la información.
- Los acuerdos de confidencialidad de la información deben formar parte integral de los contratos o documentos que legalicen la relación con los contratistas y terceros.
- Los contratistas y terceros que dentro de sus actividades intercambien, utilicen o procesen información de la Secretaría Distrital de la Mujer, deben cumplir con los requisitos de seguridad de la información aquí establecidos

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 35 de 43

- La Oficina Asesora Jurídica debe elaborar e incluir acuerdos de confidencialidad y de Intercambio de Información con terceros relacionados con contratos y/o convenios, entre otros.
- Gestión Contractual debe elaborar e incluir acuerdos de confidencialidad y de Intercambio de Información con terceros relacionados con contratos y/o convenios, entre otros.
- Los supervisores de contratos deben velar por el cumplimiento de los acuerdos de confidencialidad, de intercambio de información y los requisitos mínimos de seguridad de la información por parte de los contratistas y terceros.

## 18. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN


La Secretaría Distrital de la Mujer, promueve el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la Infraestructura Tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas. Con el fin de garantizar el cumplimiento de esta política se establecen los siguientes lineamientos:

- La Oficina Asesora de Planeación - Gestión Tecnológica, llevará el registro de los incidentes de seguridad de la información reportados en la entidad.
- La Oficina Asesora de Planeación - Gestión Tecnológica, debe definir el procedimiento de gestión de incidentes de seguridad de la información en la Secretaría Distrital de la Mujer.
- La Oficina Asesora de Planeación - Gestión Tecnológica, reportará al Comité Institucional de Gestión y Desempeño, los incidentes de seguridad que considere pertinentes para su respectivo trámite interno y/o con las autoridades competentes.
- Todos los servidores públicos y contratistas deben reportar de forma inmediata los eventos o incidentes de seguridad de la información de los recursos tecnológicos o físicos en el aplicativo de mesa de ayuda.
- Se debe dar un tratamiento a todos los incidentes de seguridad de la información reportados.
- La Oficina Asesora de Planeación - Gestión Tecnológica debe designar el personal para gestionar los incidentes de seguridad reportados.

## 19. GESTIÓN DE CONTINUIDAD DE NEGOCIO

La Secretaría Distrital de la Mujer, proporcionará los recursos necesarios tendientes a garantizar la continuidad de las operaciones que realiza la entidad en el cumplimiento de sus objetivos estratégicos y misionales, así como de brindar la normal ejecución en la prestación de los servicios tecnológicos, cuyo objetivo es restablecer las operaciones y normal funcionamiento, con el menor costo, pérdidas posibles y en el menor tiempo, de igual forma se mantendrá una adecuada comunicación con la Alta Dirección, las servidoras, servidores públicos, contratistas y demás partes interesadas.

- Para la Secretaría Distrital de la Mujer, el activo de información más importante es el recurso


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 36 de 43

humano y por lo tanto es su prioridad y objetivo principal establecer las estrategias para protegerlo.

- La Oficina Asesora de Planeación - Gestión Tecnológica, definirá un Plan de Continuidad en el marco de la Seguridad de la Información, que asegure la operación de los procesos críticos, ante la ocurrencia de eventos no previstos o desastres naturales.
- La Oficina Asesora de Planeación - Gestión Tecnológica, es responsable de la Continuidad de la Operación de la Entidad, y es la encargada de mantener documentado y actualizado el Plan de Continuidad de Seguridad de la Información e informar cualquier cambio a todos los interesados.
- Los procesos críticos están soportados en aplicaciones e infraestructura técnica robusta, software y hardware confiable.
- La Oficina Asesora de Planeación - Gestión Tecnológica, es responsable de los planes de continuidad de Operación, por lo tanto, deben ser probados periódicamente y como resultado de estas pruebas se realizan los ajustes correspondientes.
- La Oficina Asesora de Planeación - Gestión Tecnológica, es responsable de identificar, acordar y documentar todas las responsabilidades y los procedimientos para la continuidad de los servicios informáticos.

## 20. CUMPLIMIENTO

- La Secretaría Distrital de la Mujer, velará por la divulgación y cumplimiento de la política de seguridad de la información y la aplicación de la legislación vigente emitida por los entes de control.
- Las servidoras, servidores públicos, contratistas y terceros que tengan conocimiento de alguna violación a las políticas de seguridad, que conozcan alguna vulnerabilidad o que observen actividades que atenten contra la confidencialidad, integridad y/o disponibilidad de la información de la Secretaría Distrital de la Mujer, deben informar la novedad a La Oficina Asesora de Planeación - Gestión Tecnológica o en su defecto a su jefe directo o supervisor.
- La Oficina Asesora Jurídica brindará asesoría a los procesos de la entidad, en el cumplimiento de la normatividad vigente.
- Las servidoras, servidores públicos, contratistas y terceros están obligados a ceder a la Secretaría Distrital de la Mujer los derechos exclusivos de propiedad literaria, licencias, invenciones, u otra propiedad intelectual que ellos creen o desarrollen durante su periodo laboral o contractual con la Entidad. En el caso de terceros, este aspecto se regirá por las condiciones y cláusulas establecidas en el contrato de adquisición de productos y/o servicios, con el objetivo de aclarar y definir la propiedad del software, licencias, entre otros, una vez que el proyecto sea finalizado.
- La Secretaría Distrital de la Mujer, tiene propiedad legal de la información Institucional almacenada, enviada y compartida en todos sus computadores, sistemas de información, correo institucional, herramientas de colaboración y sistemas de comunicación, entre otros que hayan sido transmitidos por medio de estos recursos, por lo cual se reserva el derecho de acceder a esta información sin autorización del autor o usuario del recurso, así como también se reserva el derecho de disponer de toda la información que cualquier servidor público y contratista haya colocado en los medios de


 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 37 de 43

comunicación existentes en la Entidad.

- Los servidores públicos, contratistas y terceros deben cumplir con las disposiciones establecidas por la legislación colombiana vigente, asociados con la protección de datos personales, propiedad intelectual y seguridad de la información, entre otras que apliquen.

## 21. MARCO NORMATIVO POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

- Ley 87 de 1993, “Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del estado y se dictan otras disposiciones, y demás normas que la modifiquen.
- Ley 734 de 2002, del Congreso de la República de Colombia, Código Disciplinario Único.
- Ley 23 de 1982, Sobre Derechos de Autor.
- Ley 594 de 2000, “Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”.
- Decreto 2609 de 2012, Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado”.
- Ley 527 de 1999, “Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- 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 comunicaciones, entre otras disposiciones”.
- Ley 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”.
- Decreto 1083 de 2015. “Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012”
- Decreto 1499 de 2017, “Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 33 de la Ley 1753 de 2015”.
- Decreto 1078 de 2015. “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones” y demás normas que lo modifiquen.
- 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”
- 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”

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 38 de 43

- Ley 1150 de 2007. “Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.”
- 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 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”.
- Decreto 2952 de 2010. “Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008”.
- CONPES 3854 de 2016, “Política Nacional de Seguridad digital”.
- 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.
- Modelo de Seguridad y Privacidad de la Información: modelo de referencia propuesto por el Ministerio de las TIC para que pueda ser adoptado por cualquier organización pública o privada con el fin de salvaguardar y proteger los activos de información que estén bajo su gestión y custodia.
- <http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html>
- Norma Técnica Colombiana - NTC ISO/IEC 27001:2013.


## 22. TÉRMINOS Y DEFINICIONES.

**Administración de riesgos:** Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

**Amenaza:** Potencial ocurrencia de un hecho que pueda manifestarse en un lugar específico, con una duración e intensidad determinadas. Cuando el Agente de riesgo selecciona una víctima contra la cual pretende cometer un acto delictivo, automáticamente se convierte en una amenaza para ella. Se puede considerar que es la materialización del riesgo.

**Archivos:** En informática es también conocido como “file o fichero” la información digital que se almacena en un Disco Duro o cualquier otro medio de almacenamiento identificándolo con un nombre.

**Aplicaciones de Software:** En informática son conocidos como los programas, sistemas operativos, o utilidades instaladas o ejecutadas en los computadores para hacer tareas puntuales. Ej. Windows, Word, Excel, Simisional, Orfeo, etc.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 39 de 43

**Autorización:** Proceso o procedimiento oficial de la Secretaría Distrital de la Mujer por el cual el usuario autenticado recibe los permisos para efectuar acciones sobre elementos de los sistemas de información.

**Clasificación de la información:** Los responsables de los activos de información deben documentar la clasificación de seguridad de los activos de información de los cuales son responsables y designarán un custodio para cada activo, a su vez éste será responsable de la implementación de los controles de seguridad.

La clasificación de la información de la Secretaría Distrital de la Mujer se debe realizar con base en la Ley 1712 de 2014, reglamentada por el Capítulo 2 del Título 1 de la Parte 1 del Decreto 1081 de 2015 y la Ley 594 de 2000 (Ley General de Archivos).

**Compromiso de la Dirección:** Alineamiento firme de la Dirección de la entidad con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de Seguridad de la Información.

**Confidencialidad:** El acceso a la información es permitido exclusivamente al personal autorizado, sin revelar la misma a terceras partes y/o personas.

**Contraseña:** También conocida como Password o clave para obtener acceso a un programa, un computador (servidor, portátil o de escritorio), conexión a la red wifi, acceso al correo, sistemas de información, servicios, etc.

**Correo Institucional:** Es un servicio provisto por la entidad, para la recepción, envío y almacenamiento de mensajes de correo electrónico el cual opera por Internet y cuyo dominio corporativo es el de la Secretaría Distrital de la Mujer (@sdmujer.gov.co).


**Cuenta de Usuario:** Es identificador único el cual es utilizado para identificarse ante un programa, un computador (servidor, portátil o de escritorio), conexión a la red wifi, acceso al correo, sistemas de información, servicios, etc.

**Custodio:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo encargado de administrar y hacer efectivos los controles de seguridad que el propietario de la información haya definido, tales como copias de seguridad, asignación privilegios de acceso, modificación y borrado.<sup>2</sup> Tomado de [https://www.mintic.gov.co/gestionti/615/articles-482\\_G5\\_Gestion\\_Clasificacion.pdf](https://www.mintic.gov.co/gestionti/615/articles-482_G5_Gestion_Clasificacion.pdf)

**Encriptación:** Es un mecanismo informático usado para Cifrado o codificar información para que pueda ser recibida o enviada desde algún programa sin que se muestre su contenido de forma clara, el cual para requiere una contraseña de acceso para descifrar la información.

**Devolución de Activos:** Todos los servidores públicos, y contratistas de la Secretaría Distrital de la Mujer, sin distinción de tipo de vinculación, deben devolver todos los activos de la entidad que se encuentren a su cargo, al terminar su vinculación con la entidad.

**Disco duro:** Es un medio de almacenamiento usado en equipos tecnológicos para guardar información,

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 40 de 43

instalar software o almacenar configuraciones.

**Disponibilidad:** En seguridad informática es un término que hace referencia a la característica de poder acceder a la información en el momento que se requiera.

**CD-ROM, DVD, USB:** Son medios de lectura, almacenamiento y consulta de información digital.

**Equipos de cómputo:** Son también conocidos como computadores, computador personal, computador portátil, cuya finalidad está basada en el ingreso, procesamiento, almacenamiento y salida de información.

**Gestión de la seguridad en los activos:** La Secretaría Distrital de la Mujer a través de los procesos Gestión Tecnológica y Gestión Administrativa deben establecer y divulgar los lineamientos específicos para la identificación, clasificación y buen uso de los activos de información de tipo información, datos, software, hardware y servicios, con el objetivo de garantizar su protección.

**Gestión de riesgos:** Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

**Hardware:** Conjunto de equipos de cómputo, servidores, redes, equipos de seguridad, impresoras, scanner, equipos de almacenamiento, entre otros, que utiliza la Secretaría Distrital de la Mujer.

**Hacker:** Según la RAE. Persona experta en el manejo de computadoras, que se ocupa de la seguridad de los sistemas y de desarrollar técnicas de mejora.

**Impacto:** Resultado de un incidente de seguridad de la información


**Incidente de seguridad:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

**Información:** Es un conjunto de datos ordenados, clasificados y almacenados en cualquier medio (magnético, papel, correo electrónico, conversación telefónica, chat, USB, etc.).

**Información Sensible:** Los datos sensibles son datos personales que revelan origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical e información referente a la salud o a la vida sexual.<sup>6</sup>

**Información Interna:** Es aquella información de uso interno que utilizan las (os) servidoras(es) públicos de la Secretaría Distrital de la Mujer con el propósito de realizar las operaciones normales de la Entidad.



 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 41 de 43

**La información documentada:** (Inglés: Documented information). Información requerida para ser controlada y mantenida por una organización y el medio en el que está contenida<sup>1</sup>

La información documentada puede estar en cualquier formato y medio y desde cualquier fuente y puede referirse al sistema de gestión (incluidos los procesos relacionados), información creada para que la organización funcione (documentación) y/o evidencias de resultados alcanzados (registros)

**Información Pública:** Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de total.<sup>7</sup>

**Información Pública Clasificada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley.<sup>8</sup>

**Información Pública Reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de esta ley.

**Incidente:** Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información

**Inventario de activos:** Los responsables de la información deben propender para que se mantenga actualizado el inventario de sus activos de información y hagan entrega de éste al menos una vez al año. La consolidación de dicho inventario está bajo la responsabilidad de la Dirección de Gestión Administrativa.


**Recursos informáticos:** Software, hardware, sistemas de información.

**Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

**Parche de Seguridad:** Conjunto de ficheros adicionales al software original de una herramienta o programa informático, que sirven para solucionar sus posibles carencias, vulnerabilidades, o defectos de funcionamiento.

**Propietario de la Información:** Es una parte designada de la entidad, un cargo, proceso, o grupo de trabajo que tiene la responsabilidad de garantizar que la información y los activos asociados con los servicios de procesamiento de información se clasifican adecuadamente, y de definir y revisar

<sup>1</sup> Tomado de <https://www.iso27000.es/glosario.html>. Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER</p>	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020 Página 42 de 43

periódicamente las restricciones y clasificaciones del acceso, teniendo en cuenta las políticas aplicables sobre el control del acceso.

**Sistema de información:** Aplicativo que se encarga de administración de datos e información, organizados y listos para su uso, generados para cubrir una necesidad u objetivo.

**SGSI Sistema de Gestión de Seguridad de la Información:** Según [ISO/IEC 27001: 2013]: Sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.

**Software:** Conjunto de programas, sistemas operativos, aplicaciones de ofimática entre otros aplicativos propios y/o tercerizados que utiliza la Secretaría Distrital de la Mujer.

**Software ilegal:** Software o aplicación que ha sido alterado para que pueda ser utilizado sin pagar la licencia a sus desarrolladores originales.


**Terceros:** Personas que no son empleados de la Secretaría Distrital de la Mujer o empresas diferentes al mismo. Ejemplo: Participantes, beneficiarios, proveedores regulares o potenciales de bienes y servicios, empresas candidatas a prestar servicios a la Secretaría Distrital de la Mujer, entes reguladores, consultores, etc.

**Uso Aceptable de los Activos:** La Secretaría Distrital de la Mujer identificará, documentará e implementará reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.

**Usuario:** Cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo, que genere, obtenga, transforme, conserve o utilice información en papel o en medio digital, físicamente o a través de las redes de datos y los sistemas de información de la Unidad, para propósitos propios de su labor y que tendrán el derecho manifiesto de uso dentro del inventario de información.

**Virus:** Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

**Vulnerabilidad:** Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISO/IEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE LA MUJER	<b>SECRETARIA DISTRITAL DE LA MUJER</b>	Código: GT-MA- 3
	<b>GESTIÓN TECNOLÓGICA</b>	Versión: 03
	<b>MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN</b>	Fecha de Emisión: 20 Noviembre 2020
		Página 43 de 43

### 23. REGISTRO DE MODIFICACIONES.

VERSIÓN	FECHA	DESCRIPCIÓN DE LA MODIFICACIÓN
1	17/03/2014	Resolución No. 0061 de 2014 “Por la cual se adopta la Política de Seguridad de la información en la Secretaría Distrital de la Mujer, y se dictan otras disposiciones.”
2	01/07/2019	Resolución 407 de 2019 "Por medio de la cual se actualizó y se adopta la Política de Seguridad de la Información de la Secretaría Distrital de la Mujer y se deroga la Resolución 061 de 2014“. Se reformuló la Política de Seguridad de la Información, se incluyeron roles y responsabilidades, así mismo algunos dominios de la ISO/IEC 27001 y controles para los dominios.
3	20/11/2020	Se establece la Política General de Seguridad y Privacidad de la Información en el marco de la Resolución 407 de 2019 y se establece el <b>Manual de Políticas Específicas de Gestión de Seguridad de la Información</b> , para la implementación de controles de seguridad de la información, los cuales están consignados en el documento, el cual hace parte integral de la <b>Política General de Seguridad de la Información de la Entidad.</b>

	NOMBRE	CARGO
ELABORÓ	Giovanny Benítez Morales	Profesional Contratista
REVISÓ	Blanca Cecilia Liévano Lozano	Profesional Especializada
APROBÓ	Adriana Estupiñan Jaramillo	Jefa Oficina Asesora de Planeación