Control de cambios

Versión	Fecha	Descripción de la modificación
1	28 de diciembre de 2015	Primera versión del Manual
01	28 de noviembre de 2017	Se realiza ajuste de normalización como consecuencia de la entrada en vigencia de la resolución 162 de 2017, que crea el proceso Gerencia de TIC como parte del mapa de procesos de la entidad, y en cumplimiento de lo establecido en la circular 16 del 1 de noviembre de 2017. Los lineamientos operativos descritos en este documento corresponden íntegramente a los aprobados en la versión 1 de fecha 28 de diciembre de 2015, la cual fue aprobada por Juan Carlos Garzón Barreto como líder del proceso Planeación y Gerencia Estratégica, vigente en ese momento.
02	30 de julio de 2018	Segunda versión del Manual. Compilación del GDI-TIC-M004 Manual de Gestión de Seguridad de la Información y GDI-TIC-M001 Manual de Políticas de Uso y Seguridad de la Infraestructura Tecnológica, con su correspondiente actualización a la nueva estructura de la secretaria de Gobierno Derogación Resolución 177/2007 "Políticas para la Administración, Manejo y Uso del Recursos Tecnológico de la Secretaría Distrital de Gobierno de Bogotá". Derogación Circular 15/2006 "Indicaciones para la asignación de los equipos de cómputo" Cambio de nombre a "Manual de Gestión de Seguridad"
03	21 de agosto de 2018	Tercera versión del Manual. Se revisa y corrige la redacción del enunciado de la política en el Numeral 6. Y se revisan en el numeral 10 las funciones para el rol Responsable de orientar la implementación de la Política de Seguridad
04	18 de noviembre de 2021	Se actualiza el objetivo general, los objetivos específicos de la política de seguridad de la información. Se actualiza el enunciado de la política general de seguridad de la información. Se incluyen los 13 dominios de políticas a implementar de acuerdo con el anexo A de la ISO 27001:2013.

Método de Elaboración	Revisa	Aprueba
El documento se elabora de acuerdo con la normatividad que regula la materia, los profesionales de DTI realizan los ajustes correspondientes, con el apoyo metodológico de la Oficina Asesora de Planeación	**Jorge Bernardo Gómez Rodríguez** Director de Tecnologías e Información **Angela Patricia Cabeza Morales** Profesional de revisión de normalización de la OAP	**Ana María Aristizábal Osorio** Subsecretaria de Gestión Institucional Líder de macroproceso Documento revisado y aprobado mediante registro aplicativo Hola No. 201124

TABLA DE CONTENIDO

ÍNDICE DE ILUSTRACIONES

ÍNDICE DE TABLAS

1. PROPÓSITO

La Secretaría Distrital de Gobierno a través de la Dirección de Tecnologías e Información, dando cumplimiento a sus funciones en lo referente a Seguridad y Privacidad de la Información y gestión del riesgo de seguridad digital (ciberseguridad) y buscando un Estado más eficiente, más transparente y participativo, define la siguiente política de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información y seguridad digital de la estrategia de gobierno digital y el Modelo Integrado de Planeación y Gestión-MIPG, según lo establecido en el Decreto 1078 de 2015, el Decreto 1499 de 2017 y el Decreto 1008 de 2018; con esto la entidad vela por la integridad, confidencialidad y disponibilidad de la información y administra el riesgo sobre todos sus activos de información.

2. INTRODUCCIÓN

Hoy día, la información es el activo más valioso para las organizaciones sin importar su tamaño o su naturaleza y por ende la necesidad de bridar protección a la información ante los diferentes riesgos de seguridad de la información a los cuales está expuesta.

La información, en sus múltiples códigos y formas, así como los trámites y servicios que las entidades del Estado proveen a los ciudadanos se consideran un bien público. La Secretaría Distrital de Gobierno en sus funciones de articular las autoridades distritales, garantizar la convivencia pacífica y el cumplimiento de la ley en el Distrito Capital, proteger los derechos y promover los deberes de los ciudadanos y buscar una ciudadanía activa y responsable, entre otras; registra, organiza y transforma datos personales y misionales en información que facilita la toma de decisiones para el cumplimiento de los objetivos de la entidad y permite la publicación de datos abiertos e información que genere transparencia y valor público en entornos físicos y digitales. Esta información en conjunto con las tecnologías utilizadas para su gestión constituye los Activos de Información de la Entidad. En ese sentido, los activos de información que conforman los bienes y servicios que provee la entidad son activos públicos y, por lo tanto, deben protegerse adecuadamente.

La protección y seguridad de los activos de información, parte del concepto fundante de seguridad de la información la cual se desarrolla mediante el principio rector de la gestión de riesgo, y comprende el conjunto de medidas, procedimientos y controles establecidos para el correcto manejo, gestión y control de la información, en todo su ciclo de vida, así como para garantizar sus propiedades fundamentales; la preservación de la confidencialidad, integridad y disponibilidad de la información que se complementan con otras propiedades como accesibilidad, autenticidad, no repudio, entre otros, mediante el resguardo de datos y la protección frente a accesos no autorizados. Conscientes de que la seguridad informática se fundamenta en la existencia de un conjunto de políticas que brinden instrucciones claras y sean el soporte tecnológico y legal de la Alta Dirección, y con el objetivo que estas sean una herramienta para la definición de los estándares y procesos internos de la Entidad, la Secretaría Distrital de Gobierno, a través de este documento define la política de seguridad y privacidad de la información y seguridad digital y reglamenta los lineamientos para la implementación, medición y seguimiento, los roles y responsables de su implementación y mejora continua, y la estrategia para su adopción mediante las pautas para uso y apropiación.

3. OBJETIVO

3.1. OBJETIVO GENERAL

Establecer las políticas de seguridad de la información que regulen la seguridad de la información en la Secretaria Distrital de Gobierno y presentar en forma clara y coherente los elementos que conforman la política de seguridad que deben conocer, acatar y cumplir todos los servidores públicos, contratistas, proveedores y partes interesadas que presten sus servicios o tengan algún tipo de relación con la entidad, bajo el liderazgo de la Dirección de Tecnología e Información

3.2. OBJETIVOS ESPECIFICOS

- Implementar, operar y mejorar de forma continua el Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros conforme a las necesidades de la entidad, y a los requerimientos regulatorios.
- Identificar y asegurar los datos personales de servidores públicos, contratistas, proveedores y partes interesadas.
- Identificar, administrar y minimizar los riesgos de seguridad de la información para mantenerlos en niveles aceptables.
- Establecer lineamientos para sensibilizar y capacitar a servidores públicos, contratistas, proveedores y partes interesadas acerca del Sistema de Gestión de Seguridad de la Información, fortaleciendo el nivel de conciencia de estos, en cuanto a la necesidad de salvaguardar los activos de información.
- Establecer lineamientos para monitorear el cumplimiento de los requisitos de seguridad de la información, mediante el uso de herramientas de diagnóstico, revisiones por parte de la Alta Dirección y auditorías internas planificadas a intervalos regulares.
- Establecer lineamientos para actualizar y proteger los activos de información identificados en la Secretaria Distrital de Gobierno.
- Establecer lineamientos para permitir la continuidad de su operación frente a incidentes de seguridad.
- Gestionar de manera eficaz los riesgos de seguridad y privacidad de la información identificados en la Entidad
- Proteger, salvaguardar y gestionar adecuadamente la información de acuerdo con las políticas. directrices e indicaciones establecidas para las entidades públicas
- Actualizar el enunciado de la política general de seguridad de la información.

4. ALCANCE

Los lineamientos contenidos en la presente política de seguridad de la información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los servidores públicos, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad a través de la recolección, procesamiento, almacenamiento, recuperación, intercambio y consulta de información, con personal interno o externo, en el desarrollo de la misión institucional y el cumplimiento de sus objetivos estratégicos

5. TERMINOS Y DEFINICIONES

- **ACTIVO DE INFORMACION**: algo que una organización valora y por lo tanto debe proteger
- **CONTROL DE ACCESO**: mecanismo que en función de la identificación ya autentificada permite acceder a datos o recursos.
- **CONFIDENCIALIDAD**: Es necesario acceder a la información mediante autorización y control.
- **DERECHO DE AUTOR:** "Son los derechos de los creadores sobre sus obras literarias y artísticas. Las obras que se prestan a la protección por derecho de autor van desde los libros, la música, la pintura, la escultura y las películas hasta los programas informáticos, las bases de datos, los anuncios publicitarios, los mapas y los dibujos técnicos". (OMPI, s.f.)
- **ENTRENAMIENTO:** Proceso utilizado para enseñar habilidades, que permitan a una persona ejecutar funciones específicas asignadas su cargo.
- **EDUCACIÓN**: Formación destinada a desarrollar la capacidad intelectual, moral y afectiva de las personas de acuerdo con la cultura y las normas de convivencia de la sociedad a la que pertenecen.
- **DESARROLLO PROFESIONAL**: Es una fase del crecimiento personal que obedece a las necesidades de autosuperación que experimenta cada individuo; asimismo, el desarrollo profesional del personal de una organización hace parte de los procesos de desarrollo de recursos humanos y es fruto de la inversión que hacen las empresas en las personas que las conforman y que, a través de su trabajo, las engrandecen.
- **DISPONIBILIDAD:** La información deberá permanecer accesible a elementos autorizados**.**
- **FIRMA DIGITAL**: **es un proceso automatizado para la validación de la** firma **de un suscriptor basado en algoritmos y criptografía**
- **FIRMA ELECTRÓNICA: se refiere a todos los métodos para firmar (o validar) un documento electrónico o identificar a una persona.**
- **GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL**: es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones, para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego.
- **HARDWARE:** Son aquellos elementos físicos (CPU, monitor, mouse, teclados, impresoras, parlantes y demás elementos que se encuentren conectados a la CPU).

- **INFRAESTRUCTURA CRÍTICA CIBERNÉTICA NACIONAL**: aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos, o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública.

- **INTEGRIDAD:** la información se mantenga inalterada ante accidentes o intentos maliciosos.

- **LINEAMIENTOS TI:** Son reglas que especifican una acción o respuesta que se debe seguir en una situación determinada. En sí, son especificaciones técnicas que tienen una función instrumental que responden a cómo se implementa una política. Pueden cambiar con frecuencia debido a que los procedimientos manuales, estructura organizacional, procesos del negocio y las tecnologías de la información que se mencionan cambian rápidamente. Son también llamadas política específica o de ámbito técnico. Para efecto de este manual, solo serán llamados lineamientos.

- **MINTIC**: Ministerio de Tecnologías de la Información y las Comunicaciones

- **MEJORES PRÁCTICAS:** Una regla de seguridad específica o una plataforma que es aceptada, a través de la industria al proporcionar el enfoque más efectivo a una implementación de seguridad concreta. Las mejores prácticas son establecidas para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

- **POLITICAS TI:** Son directrices u orientaciones que debe generar la DTI y que indican la intención de la alta gerencia, con el propósito de establecer pautas para lograr los objetivos propuestos en la Estrategia de TI. Son establecidas para que perduren a largo plazo y aplican a grupos grandes de áreas o personas dentro y, muchas veces, fuera de la organización (deben ser cumplidas por los contratistas y terceros que trabajan con la organización y que por sus funciones deben tener acceso a su información y a su infraestructura). Son también llamadas Políticas generales y/o corporativas. Para efecto de este manual, solo serán llamadas políticas

- **PROPIEDAD INTELECTUAL:** "La propiedad intelectual (P.I.) se relaciona con las creaciones de la mente: invenciones, obras literarias y artísticas, así como símbolos, nombres e imágenes utilizados en el comercio.

- La legislación protege la P.I., por ejemplo, mediante las patentes, el derecho de autor y las marcas, que permiten obtener reconocimiento o ganancias por las invenciones o creaciones. Al equilibrar el interés de los innovadores y el interés público, el sistema de P.I. procura fomentar un entorno propicio para que prosperen la creatividad y la innovación". (OMPI, s.f.).

- **RECURSO TECNOLÓGICO:** Son todos los bienes tangibles e intangibles que posee la entidad, que constituyen herramientas informáticas para el desarrollo de las labores diarias. Los recursos tecnológicos y la Información son de propiedad de la Secretaría Distrital de Gobierno y deben ser utilizados únicamente para propósitos legítimos de la entidad. Se permite que los Usuarios utilicen estos Recursos para facilitarles el desempeño de sus tareas. El uso de estos Recursos es un privilegio que puede ser revocado en cualquier momento.

- **RIESGO:** Es el efecto de incertidumbres sobre objetivos y puede resultar de eventos en donde las amenazas cibernéticas se combinan con vulnerabilidades generando consecuencias económicas. Riesgo de seguridad digital: es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan.

- **SEGURIDAD DE LA INFORMACIÓN:** La seguridad de la información es el conjunto de medidas técnicas, operativas, organizativas, y legales que permiten a las organizaciones resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de esta. El concepto de seguridad de la información no debe ser confundido con el de seguridad informática, ya que este último sólo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. La seguridad de la información se encarga de garantizar la integridad, confidencialidad, disponibilidad de nuestra información. Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos de información. [NTC 5411-1:2006]. Disponibilidad: Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada. [NTC 5411-1:2006]. Confidencialidad: Propiedad que determina que la información no esté disponible ni sea revelada a individuos entidades o procesos no autorizados. [NTC5411- 1:2006].

- **SEGURIDAD DIGITAL:** Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país.

- **SERVIDOR PÚBLICO:** Se refiere a todos los empleados, contratistas, consultores o trabajadores temporales de la Secretaría Distrital de Gobierno.

- **SENSIBILIZACIÓN:** Es un proceso que tiene como objetivo principal impactar sobre el comportamiento de una población o reforzar buenas prácticas sobre algún tema en particular.

- **SOFTWARE:** Son aquellos elementos informáticos, sobre los cuales la Secretaría Distrital de Gobierno, tiene el derecho de uso o de propiedad intelectual, que permiten que las labores de procesamiento de Información sirvan como herramienta de productividad y gestión.

- Están conformados entre otros por: A) Sistemas operativos. B) Software de ofimática, c) Software de desarrollo, D) Software comercial, E) Software de comunicaciones

- **SOFTWARE AUTORIZADO:** Sistemas operacionales, paquetes de usuario final y aplicativos, que la Dirección de Tecnología de la Información ha instalado, previo visto bueno para su adquisición, actualización o renovación y con la Autorización legal del proveedor para su uso, o si se trata de licencias otorgadas con el código fuente, para generar modificaciones al mismo. El uso de Software no autorizado o adquirido ilegalmente se considera como una violación a los derechos de autor, previsto en la Ley 603 de 2000.

- **SOFTWARE LICENCIADO:** Se refiere a la obtención del derecho para uso del software de computador.
- **USUARIO:** Se refiere a todos los servidores públicos y cualquier otra persona o entidad que utilice los Recursos Tecnológicos de la Secretaría Distrital de Gobierno.
- **VIRUS:** Secuencia de código que se incluye en un archivo ejecutable (llamado huésped), y cuando el archivo se ejecuta, el virus también se ejecuta, propagándose a otros programas.

6. SANCIONES POR INCUMPLIMIENTO

La inobservancia de las disposiciones de este documento podrá dar lugar según corresponda, a la iniciación de investigaciones y aplicación de sanciones, de conformidad con las disposiciones legales vigentes.

7. POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

NOMBRE DE LA POLÍTICA
Seguridad, Privacidad de la Información y Seguridad digital
ENUNCIADO
La Secretaria Distrital de Gobierno y su Alta Dirección se comprometen en el establecimiento, implementación, mantenimiento y mejora de la seguridad y privacidad de la información, mediante la definición de un modelo de gestión sistemático, adecuado a la gestión de activos, riesgos e incidentes en seguridad de la información, fomentando una cultura en seguridad y privacidad de la información en todos los niveles de la organización, con el fin de apoyar en el cumplimiento de los objetivos estratégicos y al propósito de la Entidad.

Tabla 1 Política de Seguridad y Privacidad de la Información y Seguridad Digital

7.1. LINEAMIENTOS PARA LA IMPLEMENTACION DE LA POLÍTICA SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

Para la implementación de la Política de Seguridad y privacidad de la Información y Seguridad digital a manera de lineamientos, directrices y prohibiciones se definen 13 conjuntos de políticas para la adopción de los controles relacionados con seguridad de la información y la seguridad digital, los cuales se construyen de acuerdo con las características particulares de la Secretaría Distrital de Gobierno, sus activos de información, sus procesos y los servicios de información que presta. A continuación, se presentan los 13 dominios de control que harán parte de la política general de seguridad de la información con el objetivo de hacer una implementación transversal de Seguridad de la Información en la Entidad

7.1.1. Organización de la seguridad de la información

Establecer lineamientos que regulen la seguridad de la información en la Secretaria Distrital de Gobierno presentando de forma clara los elementos que conforman la Política organizacional de seguridad de la información

que deben conocer, acatar y cumplir todos los funcionarios, contratistas, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Entidad.

7.1.2. Seguridad de la información en los recursos humanos

La Secretaria Distrital de Gobierno reconoce la importancia del Talento Humano para el cumplimiento de sus objetivos, por lo tanto, busca establecer responsabilidades para la seguridad de la información de todos los funcionarios y colaboradores de la entidad, con el propósito de velar y actuar en concordancia con la protección de la información; orientando la debida diligencia y el debido cuidado y teniendo en cuenta los niveles de clasificación de la información establecidos por la entidad.

7.1.3. Gestión de activos

La Secretaria Distrital de Gobierno es propietario de los activos de información y los custodios de los activos son los jefes de dependencias o demás usuarios, que estén autorizados y sean responsables por la información de los procesos, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnología a su cargo.

7.1.4. Control de acceso

La Secretaria Distrital de Gobierno en busca de garantizar un adecuado control de acceso a sus activos de información ha definido las políticas para garantizar un adecuado control de acceso, para ello se implementan mecanismos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y en general a todo elemento que de alguna forma acceda a información de carácter público reservado o público clasificado.

7.1.5. Criptografía

La Secretaria Distrital de Gobierno con el objetivo de proteger la confidencialidad, integridad, disponibilidad y no repudio de la información, establece el uso de procedimientos y controles criptográficos para la transferencia de la información, enlaces de comunicaciones, protección de medios fijos y/o removibles, acceso remoto, sobres digitales, firmas electrónicas y digitales con entidades externas, proteger claves de acceso a sistemas, datos y servicios, transmisión de información Pública Reservada, Pública Clasificada, Pública / Pública, cuando sea necesario, para el resguardo de información basado en la evaluación de riesgos.

7.1.6. Seguridad física y del entorno

La Secretaria Distrital de Gobierno, proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso a las instalaciones de la Entidad y a las áreas de procesamiento de información, que aseguren el perímetro de sus instalaciones. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

7.1.7. Seguridad en las operaciones

La Dirección de Tecnologías e Información será la encargada de la operación y administración de los servicios tecnológicos que soportan la operación de la Secretaria Distrital de Gobierno, y velará por la eficiencia de los controles asociados a estos, protegiendo la confidencialidad, integridad y disponibilidad de la información, así como, asegurar que los cambios efectuados sean controlados y debidamente autorizados. De igual manera, debe proveer la capacidad de procesamiento requerida en los servicios tecnológicos y sistemas de información de la entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica de acuerdo con el crecimiento de la Entidad

7.1.8. Seguridad en las comunicaciones

La Secretaria Distrital de Gobierno establecerá, a través de la Dirección de Tecnologías e Información, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; y velará porque se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos. Igualmente, garantizará el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Entidad.

7.1.9. Adquisición, desarrollo y mantenimiento de sistemas de información

La Secretaria Distrital de Gobierno velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos y lineamientos de desarrollo seguro adecuados para la protección de la información de la Entidad.

La Dirección de Tecnologías e Información será la única dependencia de la entidad con la capacidad de adquirir, desarrollar o avalar la adquisición y recepción de software de cualquier tipo, conforme a los requerimientos de las diferentes dependencias, con el fin de garantizar la conveniencia, soporte, mantenimiento y seguridad de la información de los sistemas que operan en la Entidad, así como su integración a la plataforma que se maneja en ella. En consecuencia, cualquier software que opere en la Entidad y no haya sido entregado y/o avalado por la Dirección de Tecnología e Información no serán responsabilidad de esta, no se le brindará soporte y no se le salvaguardará la información

7.1.10. Seguridad de la información en la relación con los proveedores

La Secretaria Distrital de Gobierno mantendrá la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes o que son procesados, comunicados o dirigidos a estos. Igualmente, se deben establecer mecanismos de control contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o colaboradores, cumplan con las Políticas de Seguridad de la Información de la Entidad.

7.1.11. Gestión de incidentes de seguridad de la información

La Secretaria Distrital de Gobierno asegurará que los eventos e incidentes de seguridad de la información que se presentan en los activos de información de la Entidad sean comunicados y atendidos oportunamente, aplicando los procesos definidos con el fin de tomar oportunamente las acciones correctivas.

7.1.12. Aspectos de seguridad de la información para la gestión de la continuidad del negocio

La Secretaria Distrital de Gobierno asegurará que todos los aspectos relacionados con la seguridad de la información se incluyan en los planes de continuidad de negocio de la Entidad y así proteger la información.

7.1.13. Cumplimiento

La Secretaria Distrital de Gobierno velará por la identificación, documentación y cumplimiento de los requisitos legales enmarcados para la seguridad de la información, entre ellas los derechos de autor, propiedad intelectual, protección de datos personales, ley de transparencia y del derecho de acceso a la información pública nacional. Igualmente, velara por la protección de los registros ante cualquier perdida, destrucción, falsificación acceso o liberación no autorizada de acuerdo con los requisitos legislativos, de reglamentación y contractuales de la Entidad.

8. IMPLEMENTACION DE LA POLÍTICA

El Ministerio de las Tecnologías de la Información y las Comunicaciones a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones, a través de las cuales contribuye a la construcción de un Estado más eficiente, más transparente y participativo, implementará el Modelo de Seguridad y Privacidad de la Información, para dar cumplimiento a lo establecido en el componente de seguridad y privacidad de la información de la estrategia de gobierno digital. Mediante el aprovechamiento de las TIC y el modelo de seguridad y privacidad de la información, se trabajará en el fortalecimiento de la seguridad de la información en las entidades, con el fin de garantizar la protección de esta y la privacidad de los datos de los ciudadanos y funcionarios de la entidad, todo esto acorde con lo expresado en la legislación colombiana.
El Modelo de Seguridad y Privacidad de la Información – MSPI, contiene un compendio de buenas prácticas que conducen a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

9. LINEAMIENTO

La Secretaria Distrital de Gobierno, se compromete a implementar un modelo de gestión sistemático y cíclico de Seguridad y Privacidad de la Información y de riesgo de seguridad digital, de acuerdo con los lineamientos consignados en esta política. El modelo debe evidenciar claramente las siguientes etapas:

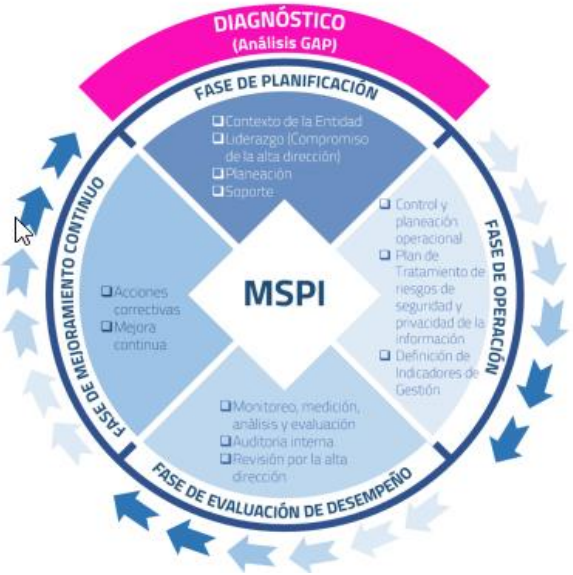

Ilustración 1 – Ciclo de operación del Modelo de Seguridad y Privacidad de la Información y de riesgo de seguridad digital

10. ROLES Y RESPONSABILIDADES DE LA POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

La Alta Dirección de la Secretaría Distrital de Gobierno tiene como responsabilidad aprobar esta política y propender su implementación y sus modificaciones, por esta razón deben crearse dentro de la organización, los siguientes roles que garanticen su cumplimiento, de acuerdo con los lineamientos establecidos en el Modelo Integrado de Planeación y Gestión.

La Ilustración 2 muestra la estructura requerida para el establecimiento de la política de seguridad y privacidad de la información y seguridad digital, y en la Tabla 2 se encuentran descritos los principales roles y funciones en lo referente al desarrollo de esta política:

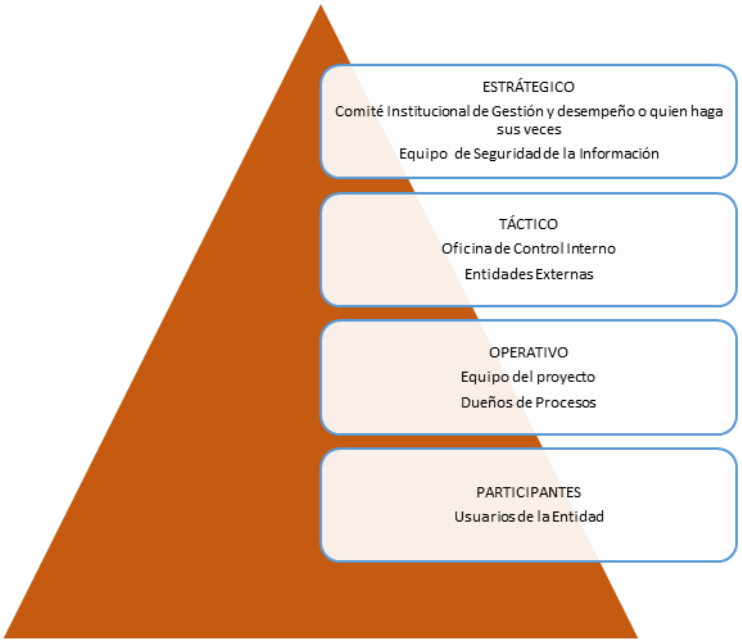

Ilustración 2 Ciclo de vida de las Políticas TI. Creación propia

ROL	PARTICIPANTES	FUNCIONES
Comité Institucional de Gestión y desempeño	Subsecretario(a) de Gestión Institucional, quien lo preside. Asesor del Despacho del Secretario de Gobierno. Director Jurídico Jefe de la Oficina Asesora de Planeación, quien actúa como Secretario Técnico del Comité Jefe de la Oficina Asesora de Comunicaciones Director de Tecnologías e Información Director de Contratación Director de Gestión del Talento Humano Director Financiero Director Administrativo	*Fijar las acciones y estrategias orientadas al buen uso y aprovechamiento de las Tecnologías de Información y la Comunicaciones, así como la gestión y la protección de los activos de información de la Entidad. • Uso y aprovechamiento de Tecnologías de Información y las Comunicaciones • Gestión y Protección de Activos de Información *Articular los esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, sostenibilidad y mejora del modelo de privacidad y seguridad de la información. *Adelantar y promover acciones periódicas de autodiagnóstico para facilitar la valoración interna de la gestión. *Asegurar la implementación y desarrollo de las políticas de gestión y directrices en materia de seguridad digital y de la información.

ROL	PARTICIPANTES	FUNCIONES
		*Fijar acciones y estrategias orientadas al buen uso y aprovechamiento de las Tecnologías de Información y las Comunicaciones, así como a la protección de los activos de información de la Entidad.
Equipo de Seguridad de la Información	Profesionales de la Dirección de Tecnología e Información.	* Liderar el proceso de gestión de incidentes de seguridad, así como la posterior investigación de dichos eventos para determinar causas, posibles responsables y recomendaciones de mejora para los sistemas afectados, ayudando con las cuestiones disciplinarias y legales necesarias. * Trabajar con la alta dirección y los dueños de los procesos misionales dentro de la entidad en el desarrollo de los planes de recuperación de desastres y los planes de continuidad del negocio. * Realizar y/o supervisar pruebas de vulnerabilidad sobre los diferentes recursos tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. * Definir, seguir y controlar la estrategia TI que permita lograr los objetivos y minimizar de los riesgos de la institución. Es el encargado de guiar la prestación del servicio y la adquisición de bienes y servicios relacionados y requeridos para garantizar la seguridad de la información. * Verificar el cumplimiento de las obligaciones legales y regulatorias del estado relacionadas con la seguridad de la información. * Desarrollar y supervisar los resultados del plan de formación y sensibilización establecido para la entidad, con el fin de identificar oportunidades de mejora * Generar y monitorear el cronograma de la implementación del Modelo de Seguridad y privacidad de la información. * Velar por el mantenimiento y actualización de la documentación del proyecto, su custodia y protección.
Oficina de Control Interno	Profesionales delegados del área	* Llevar las auditorías periódicas (mínimo anualmente) al Modelo de Seguridad y Privacidad de la Información de acuerdo con la normatividad vigente.
Entidades Externas	Alta Consejería de las Tics MINTIC, entre otros	* Brindar asesoría con base en su punto de vista macroscópico de una organización y de experiencia en ocasiones similares.

ROL	PARTICIPANTES	FUNCIONES
Equipo del Proyecto	*Profesionales delegados de las áreas. *Equipo responsable del tratamiento de los datos personales: Profesionales de la Dirección de Tecnología e Información.	* Apoyar al Equipo de Seguridad de la Información, de acuerdo con el cronograma establecido. * Coordinar la interacción con consultores externos. * Analizar el riesgo de los activos de información de la Secretaría Distrital de Gobierno y verificar la aplicación de las medidas de seguridad necesarias para la protección de esta. * Tomar las decisiones sobre las bases de datos personales a que hubiere lugar y direccionar las actividades de los encargados de los datos personales. * Generación, revisión, aprobación, seguimiento, apoyo y/o plan de mejora para el cambio de protocolo IPV4 a IPV6 * Autodiagnóstico del MPSI y seguridad digital *Apoyar con el desarrollo de la documentación de seguridad * Apoyar en las diversas actividades del MINTIC relacionadas.
Dueños del proceso	Persona nombrada que ejerce como responsable de un proceso de la organización y/o aplicación especializada relacionada	* Actúa como el "administrador del activo de información" para todos los aspectos de seguridad de la información relacionados con el procesamiento de datos dentro de este proceso particular de la organización. * Clasificar los activos de información de su proceso, de acuerdo con el grado de sensibilidad y criticidad de la misma, documentar y mantener actualizada la clasificación efectuada, y definir qué usuarios deberán tener permisos de acceso a la información de acuerdo a sus funciones y competencia
Usuarios de la Entidad	*Toda persona con vínculo contractual con la Entidad *Personal outsourcing de terceros con contrato con la Entidad *Ciudadanos que requieren de los servicios de la Entidad	*Conocer y dar a conocer, cumplir y hacer cumplir la Política de Seguridad de la Información vigente

Tabla 2 Roles y Responsabilidades

11. DOCUMENTOS RELACIONADOS

11.1. Documentos internos

CÓDIGO SIG	NOMBRE DOCUMENTO
GDI-TIC-PL002	Plan de Seguridad y Privacidad de la Información
GDI-TIC-PL003	Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información
GDI-TIC-F032	Formato identificación, valoración y clasificación de activos de información
GDI-TIC-PL001	Plan Estratégico de las Tecnologías de Información (PETI)

11.2. Normatividad Vigente

Norma	Año	Epígrafe	Artículo(s)
Decreto 1008	2018	Política Gobierno Digital	http://es.presidencia.gov.co/normativa/normativa /DECRETO%201008%20DEL%2014%20DE%20JUNIO%20DE%202018.pdf
Decreto 1078	2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector TIC	http://www.mintic.gov.co/portal/604/articles-9528_documento.pdf
Conpes 3854	2016	Ciberseguridad Colombia	https://colaboracion.dnp.gov.co/CDT/Conpes/Econ%C3%B3micos/3854.pdf Conpes 3854
Decreto 1499	2017	MIPG	http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=71261

11.3. Documentos externos

Nombre	Fecha de publicación o versión	Entidad que lo emite	Medio de consulta
Arquitectura TI	http://www.mintic.gov.co/arquitecturati/630/w3-channel.html	MINTIC	INTERNET
Marco de referencia Arquitectura Empresarial	http://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8114.html	MINTIC	INTERNET

Política Gobierno Digital	http://estrategia.gobiernoenlinea.gov.co/623/w3-propertyvalue-7652.html	MINTIC	INTERNET
Detalle Política Gobierno Digital	http://mintic.gov.co/portal/604/articles-61775_recurso_2.pdf	MINTIC	INTERNET
Manual Gobierno en Línea	http://estrategia.gobiernoenlinea.gov.co/623/propertyvalues-7751_archivo_pdf_manual.pdf	MINTIC	INTERNET
MODELO SEGURDIAD DE LA INFORMACION	http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html	MINTIC	INTERNET
Portal IDECA	https://www.ideca.gov.co/	IDECA	INTERNET
MIPG- FURAG	http://www.funcionpublica.gov.co/web/MIPG	DNP	INTERNET
Portal SECOP	https://www.contratos.gov.co/consultas/inicioConsulta.do	COLOMBIA COMPRA EFICIENTE	INTERNET