 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 1 de 42

1. Objetivo general

Desarrollar políticas complementarias que aseguren la gestión efectiva de la seguridad y privacidad de la información en la Secretaría Distrital de Integración Social, mediante lineamientos específicos para proteger la confidencialidad, integridad, disponibilidad y cumplir la normativa vigente, todo dentro del marco del Sistema de Gestión de Seguridad de la Información y la Política General de Seguridad y Privacidad de la entidad.

2. Objetivos específicos

- Identificar e implementar tecnologías que fortalezcan la seguridad de la información en la entidad.
- Desplegar el Sistema de Gestión de Seguridad de la Información.
- Proteger la información y los activos de la entidad.
- Gestionar y mitigar los riesgos asociados a los activos de información.
- Garantizar la disponibilidad, integridad y confidencialidad de la información.
- Concientizar a funcionarios y contratistas sobre el uso adecuado de los activos de información, asegurando su confidencialidad, privacidad e integridad.
- Cumplir con los lineamientos de la Estrategia de Gobierno Digital y Seguridad de la Información.
- Establecer pautas generales para la protección de datos personales y sensibles, garantizando su autenticidad, confidencialidad e integridad.
- Regular la recolección, tratamiento, almacenamiento y protección de datos personales, asegurando su gestión adecuada en conformidad con las normativas vigentes, aplicable a funcionarios, contratistas, usuarios y terceros.

3. Alcance

El presente documento aplica a todos los funcionarios, contratistas, proveedores, operadores, entes de control y a los terceros que debido al cumplimiento de sus funciones y las de la Secretaría Distrital de Integración Social - SDIS, compartan, utilicen, recolecten, procesen, intercambien o consulten información de forma interna o externa, independientemente de su ubicación y soporte.


4. Vigencia

El presente lineamiento rige a partir de la fecha de su expedición, o hasta que sea derogada por disposiciones que le sean contrarias.

5. Marco conceptual

- Access Point: (Punto de Acceso Inalámbrico) es un dispositivo de red que interconecta equipos de comunicación inalámbricos¹.

¹ (2021, September). Cisco. https://www.cisco.com/c/es_mx/solutions/small-business/resource-center/networking/what-is-access-point.html.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 2 de 42

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización².
- Acuerdo de confidencialidad: documento en el que funcionarios, contratistas y terceros se comprometen a mantener la confidencialidad de la información de la SDIS.
- Almacenamiento en la nube: modelo de servicio que almacena, administra y respalda información de forma remota a través de internet³.
- Aplicaciones: software utilizado para la gestión de la información en la entidad.
- Autenticación: procedimiento de comprobación de identidad de un usuario al acceder a un recurso tecnológico o sistema de información⁴.
- Base de datos: colección organizada de información para facilitar su acceso, administración y actualización⁵.
- Centros de cableado: espacios físicos donde se ubican dispositivos de comunicación y cables tecnológicos⁶.
- Cifrado: procedimiento que utiliza un algoritmo para transformar datos en un formato seguro, solo interpretable con la clave adecuada⁷.
- Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados⁸.
- Control de acceso: Significa garantizar que el acceso a los activos esté autorizado y restringido según los requisitos comerciales y de seguridad⁹.
- Criptografía: proceso para proteger la información mediante su transformación en un formato seguro para ocultar su contenido y prevenir modificaciones no detectadas¹⁰.
- Dato sensible: dato personal que requiere protección especial por su impacto en la intimidad del titular y el riesgo de discriminación¹¹.
- Declaración de aplicabilidad: (Inglés: Statement of Applicability; SOA). Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001¹².
- Disponibilidad: propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada¹³.

² Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>

³ Microsoft Azure. (2024). Microsoft.com. <https://azure.microsoft.com>.

⁴ Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>

⁵ (2020, November 24). Oracle.com; Oracle. <https://www.oracle.com/co/database/what-is-database/>

⁶ *La importancia del cableado estructurado del Centro de Datos | EnRed*. (2024). En-Red.mx. <https://en-red.mx/la-importancia-del-cableado-del-centro-de-datos/>

⁷ Kaspersky. (2018, November 21). *Cifrado de datos y cómo hacerlo*. / . <https://latam.kaspersky.com/resource-center/definitions/encryption?srsId=AfmBOoqUrhWzLeyQCTLHQjQqYW82JjYHnXs5k4z679mBvrF87L-Lmir>

⁸ Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>

⁹ Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>


¹⁰ Kaspersky. (2018, November 21). *Cifrado de datos y cómo hacerlo*. / . <https://latam.kaspersky.com/resource-center/definitions/encryption?srsId=AfmBOoqUrhWzLeyQCTLHQjQqYW82JjYHnXs5k4z679mBvrF87L-Lmir>

¹¹ *Ley 1581 de 2012 - Gestor Normativo*. (2023, August 9). Funcionpublica.gov.co.

<https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

¹² Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>

¹³ Agustín López. (2017). *Glosario. Iso27000*.Es. <https://www.iso27000.es/glosario.html>

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 3 de 42

- Firmware: (programación en firme) software que opera físicamente el hardware en dispositivos tecnológicos¹⁴.
- Evento de Seguridad de la Información: (Inglés: Information security event). Ocurrencia identificada del estado de un sistema, servicio o red de comunicaciones que indica una posible violación de la política de seguridad de la información o falla de los controles, o una situación previamente desconocida que puede ser relevante para la seguridad¹⁵.
- Información: activo fundamental para la entidad, que requiere protección adecuada y puede incluir datos en diversos formatos y medios.
- Incidente de seguridad de la información: ocurrencia que indica una posible violación de la seguridad de la información o una falla de los controles.
- Información pública: es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal¹⁶.
- 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 la ley 1712 de 2014¹⁷.
- 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 la ley 1712 de 2014¹⁸.
- Integridad: Propiedad de la información relativa a su exactitud y completitud¹⁹.
- Malware: (software malicioso) programa que causa mal funcionamiento en un sistema informático.
- Plataforma tecnológica: conjunto de hardware y software que permite el funcionamiento de aplicaciones y sistemas.
- Riesgo de información: el riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización²⁰.
- Seguridad de la información: preservación de la confidencialidad, integridad y disponibilidad de la información en todos los servicios de la entidad.
- Software: conjunto de programas y rutinas que permiten realizar tareas en un sistema de información.
- Spam: mensajes no solicitados enviados de forma masiva, generalmente de tipo publicitario, que pueden perjudicar al receptor.
- UPS: dispositivo con elementos almacenadores de energía que suministra energía eléctrica por un tiempo limitado a dispositivos conectados.

¹⁴ Análisis de firmware en dispositivos industriales | INCIBE-CERT | INCIBE. (2021). Incibe.es. <https://www.incibe.es/incibe-cert/blog/analisis-de-firmware-en-dispositivos-industriales#:~:text=Un%20firmware%20se%20define%20como,las%20funciones%20b%C3%A1sicas%20del%20mismo.>

¹⁵ Agustín López. (2017). Glosario. Iso27000.Es. <https://www.iso27000.es/glosario.html>


¹⁶ Ley 1581 de 2012 - Gestor Normativo. (2023, August 9). Funcionpublica.gov.co. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

¹⁷ Ley 1581 de 2012 - Gestor Normativo. (2023, August 9). Funcionpublica.gov.co. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

¹⁸ Ley 1581 de 2012 - Gestor Normativo. (2023, August 9). Funcionpublica.gov.co. <https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981>

¹⁹ Agustín López. (2017). Glosario. Iso27000.Es. <https://www.iso27000.es/glosario.html>

²⁰ Agustín López. (2017). Glosario. Iso27000.Es. <https://www.iso27000.es/glosario.html>


 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN	Código: LIN-TI-002
	LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 4 de 42

- Virus informático: software que altera el funcionamiento normal de los equipos de cómputo sin el permiso del usuario.
- VPN: (Red Privada Virtual) tecnología que conecta uno o varios equipos a una red privada a través de internet.

6. Marco normativo

El diseño e implementación del Sistema de Gestión de Seguridad de la Información -SGSI- de la Secretaría Distrital de Integración Social -SDIS se basa en la normatividad exigida por el Ministerio de Tecnologías de la Información y Comunicaciones -MINTIC-:

- Política General de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social.
- Guía 2 Modelo de Seguridad y Privacidad de la Información -MSPI- V1.
- Ley 1581 de 2012 denominada “Protección de Datos Personales”.
- Ley 1273 de 2009, "Delitos Informáticos" protección de la información y los datos.
- Ley 1712 de 2014, “De transparencia y del derecho de acceso a la información pública nacional”
- Conpes 3995 de 2020, de “Política Nacional de Confianza y Seguridad Digital”.
- Conpes 3701 Lineamientos de política en ciberseguridad y ciberdefensa, orientados a desarrollar una estrategia nacional que contrarreste el incremento de las amenazas informáticas que afectan significativamente al país. Adicionalmente, recoge los antecedentes nacionales e internacionales, así como la normatividad del país en torno al tema.
- Conpes 3854 Política Nacional de Seguridad digital. Establece un marco institucional claro en torno a la seguridad digital.
- Modelo Integrado de Planeación y Gestión MIPG versión 2 – 2018.
- Modelo de Seguridad y Privacidad de la Información (MSPI), Política de Gobierno Digital, Ministerio de Tecnologías de la Información y las Comunicaciones.
- Guía para la administración del riesgo y el diseño de controles en entidades públicas (DAFP, 2018) Guía que unificar la metodología existente para la administración del riesgo de gestión y corrupción, con el fin de hacer más sencilla la utilización de esta herramienta gerencial para las entidades públicas y así evitar duplicidades o reprocesos.
- ISO/IEC 27001:2013 y 2022 Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos. Especifica los requisitos para establecer, implantar, mantener y seguir mejorando los Sistemas de Gestión de Seguridad de la Información (SGSI) en el contexto de las organizaciones.
- Resolución 500 de 2020 del Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Decreto 767 del 2022 del Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC, “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”

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN	Código: LIN-TI-002
	LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 5 de 42

- Manual de gobierno Digital del Ministerio de las Tecnologías de la Información y las Comunicaciones – MINTIC.
- Artículo 12 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”.
- Artículo 17 Decreto 648 de 2017 Por la cual se refieren los roles de las Unidades u Oficinas de Control Interno.

7. Desarrollo del Lineamiento o Política Interna


La Política General de Seguridad y Privacidad de la Información y Seguridad Digital de la Secretaría Distrital de Integración Social basa su estructura en el Modelo de Seguridad y Privacidad de la Información -MSPI- el cual hace parte integral de la estrategia de Gobierno Digital mediante el desarrollo del habilitador transversal de seguridad de la información y de la cual se desprenden políticas específicas orientadas a la mejora continua y alto desempeño del Sistema de Gestión de la Entidad, en lo atinente a la seguridad y privacidad de la información y seguridad digital. Es importante referir que la política se adoptó mediante resolución, la cual indica que, “será revisada anualmente o cuando la Entidad lo considere necesario, en los escenarios de posibles cambios de entorno interno, externo y/o cuando sea solicitado por la normativa colombiana. Este proceso será liderado por el Oficial de Seguridad de la Información o quien haga sus veces y será aprobados por el Comité Institucional de Gestión y Desempeño de la Secretaría Distrital de Integración Social”.

Para la Secretaría Distrital de Integración Social (SDIS), la política se enmarca como un lineamiento conforme a los criterios establecidos en el listado maestro de documentos, de acuerdo con el procedimiento de control de documentos PCD-SG-001. Este lineamiento se entiende como una *directriz general de cumplimiento obligatorio a mediano y largo plazo, equiparándose al concepto de política interna*.

Los lineamientos específicos desarrollados en el presente lineamiento guiarán el comportamiento del personal en cumplimiento de la responsabilidad asignada para la Formulación e implementación de políticas públicas poblacionales orientadas al ejercicio de derechos, alineado con la protección y preservación de la colección de datos organizada para dar servicio a muchas aplicaciones al mismo tiempo, al combinar los datos de manera que parezcan estar en una sola ubicación, con el fin de preservar los principios de confidencialidad, integridad y disponibilidad de la información y se convierten en la base para la implementación de los controles, procedimientos y/o estándares.

Cada lineamiento se compone de la siguiente estructura:

- Objetivo y definición: Describe la intención de la política
- Responsable(s) de la ejecución de la política – Alta Dirección: Describe quién es el responsable de dar los lineamientos y las acciones para cumplir los requisitos de la política y está conformada por la alta dirección.
- Responsable(s) del cumplimiento de la política: Describe quién es el responsable de hacer cumplir los lineamientos y las acciones para cumplir los requisitos de la política.
- Indicador: medida cuantitativa o cualitativa utilizada para evaluar, comparar y monitorear el desempeño, el progreso o el cumplimiento de la política.


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 6 de 42

- e) Declaración de aplicabilidad: Identifica y justificar los controles de seguridad que se aplican dentro de cada política.
- f) Controles que abarca la norma NTC-ISO-27001:2013 Anexo A: hace referencia a los controles de la norma, y en los cuales se dan los lineamientos y cumplimiento de esta.
- g) Lineamientos Generales: es la descripción de como la entidad da cumplimiento a los controles definidos en la norma ISO 27001:2013.


7.1. Lineamientos

7.1.1 Política organización de la seguridad de la información

Objetivo y definición	Establecer un marco de referencia de gestión que inicie y controle la implementación y operación de la seguridad de la información en la Secretaría Distrital de Integración Social (SDIS), definiendo roles, responsabilidades y directrices para la implementación y operación de controles de seguridad.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Análisis y Diseño Estratégico • Subdirección de Investigación e información – SII
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la Secretaría Distrital de Integración Social. • Proveedores y partes interesadas
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de políticas y procedimientos de seguridad revisados y actualizados. • Fórmula: $(\text{Número de políticas y procedimientos revisados} / \text{Total de políticas y procedimientos de seguridad}) * 100$ • Fuente: Informe de implementación del MSPI • Meta: 100% • Frecuencia de medición: Anual
Declaración de aplicabilidad	Se implementa un marco de gestión de seguridad de la información para garantizar que todos los aspectos de la seguridad de la información estén debidamente organizados y controlados.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.6.1.1 Asignación de responsabilidades para la seguridad de la información.</p> <p>A.6.1.2 Separación de deberes.</p> <p>A.6.1.3 Contacto con las autoridades.</p> <p>A.6.1.4 Contacto con grupos de interés especial.</p>
Lineamientos Generales	<ul style="list-style-type: none"> ✓ Referir el rol de la alta dirección en cuanto a: “Orientar y apoyar por parte de la alta dirección de la entidad a través del comité” ✓ La SDIS, a través de su Comité Institucional de Gestión y Desempeño, tiene la responsabilidad de proteger los activos de información identificados y clasificados por la entidad. Esto incluye información, procesos, tecnologías y personas involucradas. El comité apoya la

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN	Código: LIN-TI-002
	LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 7 de 42

	<p>implementación del Sistema de Gestión de Seguridad de la Información (SGSI) basado en el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Este sistema busca preservar la confidencialidad, integridad, disponibilidad, privacidad y continuidad de las operaciones, promoviendo una cultura de seguridad entre los funcionarios y colaboradores de la entidad siguiendo las directrices de la norma NTC-ISO/IEC 27001:2013.</p> <ul style="list-style-type: none"> ✓ Los Roles y responsabilidades para la seguridad de la información son los dispuestos a continuación: <ul style="list-style-type: none"> a. Líder de Seguridad de la Información - CISO, quien será el encargado de liderar los temas relacionados con seguridad y privacidad de la información, continuidad del negocio, protección de datos personales, entre otros. b. Gestor de Seguridad de la Información quien se encargará de apoyar la implementación, fortalecimiento, revisión, medición y mejora continua del SGSI. c. La Subdirección de Investigación e información - SII es responsable del diseño y determinación de las políticas, orientaciones estratégicas, planes, programas y proyectos de la SDIS, en relación con el MSPI; promoviendo y apoyando la implementación en la Entidad de una cultura de la gestión orientada por resultados. d. Funcionarios, contratistas, proveedores de la SDIS son responsables de conocer, divulgar y dar cumplimiento a las Políticas de Seguridad y Privacidad de la Información. ✓ La información deberá estar bajo la responsabilidad del Líder de dependencia para evitar conflicto y reducir oportunidades de modificación (intencional o no) no autorizada o mal uso de los activos de información de la SDIS. ✓ La SDIS a través de la Subdirección de Investigación e información - SII y los propietarios de sistemas o quien haga sus veces, deberá establecer y mantener una relación cercana con las entidades responsables de atender emergencias y desastres en cada territorio, zona o ubicación geográfica, así como con los grupos de interés y foros de especialistas en seguridad y privacidad de la información, para que puedan ser contactados de manera oportuna en caso de que se presente un incidente de seguridad y privacidad de la información. ✓ Los funcionarios, contratistas y proveedores de la SDIS. que en ejercicio de sus funciones u obligaciones tengan acceso a la información, infraestructura tecnológica y/o a los sistemas de información, deben contar con una definición roles y responsabilidades respecto de la información a la que acceden o producen de conformidad con las tablas de control de acceso de la entidad, así como del nivel de acceso y privilegios establecidos sobre los activos de información, el índice de información clasificada y reservada y/o la información misma, con el fin de reducir y evitar el uso o modificación no autorizada sobre la información de la Entidad.
--	--


 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 8 de 42

7.1.2. Política de seguridad de la información en la gestión de proyectos.


Objetivo y definición	Incluir la identificación y gestión de riesgos de seguridad de la información en la gestión de todos los proyectos de la Secretaría Distrital de Integración Social (SDIS), asegurando que se consideren adecuadamente a lo largo del ciclo de vida del proyecto.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Análisis y Diseño Estratégico • Subdirección de Investigación e información - SII
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de proyectos con análisis de riesgos de seguridad de la información incluidos. • Fórmula: $\text{Número de proyectos con análisis de riesgos de seguridad de la información} / \text{Total de proyectos gestionados} \times 100$. • Fuente: Documentación de cada proyecto, incluyendo planes, informes y actas, para identificar si se ha incluido un análisis de riesgos de seguridad de la información. • Meta: 100%. • Frecuencia de medición: Mensual o trimestral, en función del número de proyectos activos.
Declaración de aplicabilidad	Todos los proyectos deben incluir la identificación y evaluación de riesgos de seguridad de la información en su planificación y ejecución, asegurando que se mitiguen adecuadamente.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	A.6.1.5 Seguridad de la información en la gestión de proyectos.
Lineamientos Generales	<ul style="list-style-type: none"> ✓ La Subdirección de Investigación e información - SII y los propietarios de sistemas o quien haga sus veces como líderes de la gestión de proyectos deben establecer los lineamientos para la identificación y tratamiento de riesgos de seguridad de la información en todas las fases de los proyectos institucionales, de acuerdo con la metodología establecida por la SDIS definiendo los roles, responsabilidades y procedimientos necesarios para la gestión de estos.

7.1.3. Política de dispositivos móviles y trae tu propio dispositivo (BYOD)


Objetivo y definición	Establecer medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de los activos de información que son accedidos, modificados, generados, transmitidos y/o eliminados desde dispositivos móviles, tanto institucionales como personales (BYOD).
-----------------------	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 9 de 42

Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Análisis y Diseño Estratégico • Subdirección de Investigación e información - SII • Subdirección Administrativa y Financiera
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la Secretaría Distrital de Integración Social – SDIS
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de tráfico de red cifrado conforme a los lineamientos de la entidad. • Fórmula: Porcentaje de tráfico cifrado = Volumen de tráfico de red cifrado / Volumen total de tráfico de red *100 • Fuente: Plataformas de Monitoreo de Redes (NAC): Herramientas que monitorizan el acceso y comportamiento de los dispositivos en la red, verificando que las conexiones estén cifradas conforme a las políticas de la organización.
Declaración de aplicabilidad	Se aplican controles específicos para el acceso y manejo de la información desde dispositivos móviles y personales, garantizando la seguridad de los activos de información.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	A.6.2.1 Política de uso de dispositivos para movilidad
Lineamientos Generales	<p>Lineamientos para el Uso y Gestión de Dispositivos Móviles:</p> <p>Seguridad y Gestión de Dispositivos Móviles:</p> <ul style="list-style-type: none"> ✓ Los dispositivos móviles asignados o autorizados, como tabletas, celulares y computadoras portátiles, deben contar con medidas de seguridad para mitigar riesgos y proteger la información sensible de la SDIS. ✓ Se debe mantener un registro actualizado de los dispositivos autorizados para su uso dentro y fuera de la entidad. ✓ Es necesario garantizar la seguridad física de estos dispositivos, almacenándolos en lugares seguros bajo llave y usando elementos de seguridad como guayas para prevenir robos. ✓ Los equipos móviles deben estar protegidos mediante autenticación (contraseñas, códigos, patrones o métodos biométricos) y contar con software para detección y eliminación de software malicioso. <p>Restricciones y Controles:</p> <ul style="list-style-type: none"> ✓ La Subdirección de Investigación e Información (SII) debe implementar mecanismos para restringir el uso de dispositivos USB en equipos de la entidad, permitiendo excepciones bajo procedimientos definidos. ✓ Los dispositivos móviles no deben almacenar información institucional sin la debida autorización y controles de seguridad.


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 10 de 42</p>

	<ul style="list-style-type: none"> ✓ Cualquier almacenamiento externo de información institucional debe estar cifrado según los estándares de la SDIS. ✓ Ante pérdida o robo de un dispositivo, debe notificarse de inmediato a la mesa de ayuda y seguirse los procedimientos de seguridad establecidos, incluyendo posibles bloqueos y cambios de claves. <p>Configuraciones y Actualizaciones:</p> <ul style="list-style-type: none"> ✓ Los dispositivos deben tener una configuración de seguridad base definida por la SII y estar siempre actualizados en términos de seguridad. ✓ Solo se permite la instalación de software autorizado, manteniendo una línea base estándar en la entidad. ✓ Los dispositivos deben usar únicamente la tarjeta SIM asignada por la entidad y no deben tener SIM o memorias adicionales. <p>Responsabilidades del Usuario:</p> <ul style="list-style-type: none"> ✓ Los usuarios no deben modificar la configuración de los dispositivos asignados ni instalar/desinstalar software sin autorización. ✓ Es responsabilidad del usuario evitar el uso de dispositivos móviles en zonas de alto riesgo y en lugares públicos. ✓ No conectar los dispositivos a redes o puertos USB de uso público. ✓ Los usuarios deben mantener desactivadas las funciones de redes inalámbricas (Wifi, Bluetooth, etc.) fuera de las instalaciones de la entidad y evitar el uso de redes inalámbricas públicas. <p>Medidas para Dispositivos Externos:</p> <ul style="list-style-type: none"> ✓ La Subdirección de Investigación e Información SII y los propietarios de sistemas deben definir configuraciones de seguridad para los dispositivos personales usados por funcionarios, contratistas o terceros para acceder, almacenar y transmitir información. ✓ Los dispositivos autorizados deben tener antivirus actualizado, protección por contraseñas o patrones de bloqueo y, preferiblemente, autenticación multifactor. ✓ Los dueños de dispositivos personales deben tomar nota del IMEI y aceptar que la entidad pueda ejecutar acciones de mitigación de riesgos sobre la información institucional en caso de pérdida o venta del dispositivo. ✓ Los funcionarios, contratistas y proveedores de la SDIS que utilicen equipos personales en el desempeño de sus funciones deben garantizar que, al finalizar sus contratos, toda la información sea entregada y cargada en los repositorios designados por la entidad, ya sean en la nube o físicos y sin claves de acceso. <p>Concientización y Entrenamiento:</p> <ul style="list-style-type: none"> ✓ La entidad debe ofrecer entrenamiento y sensibilización sobre los riesgos asociados al uso de dispositivos móviles para incrementar la concientización entre los colaboradores para mitigar la pérdida o uso indebido de la información.
--	--

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 11 de 42

7.1.4. Política de teletrabajo, trabajo en casa o trabajo remoto


Objetivo y definición	Garantizar la seguridad de la información durante el teletrabajo concienciando a todos los colaboradores sobre la importancia de cumplir con las medidas de seguridad establecidas, tanto dentro como fuera de la oficina, para asegurar la confidencialidad, integridad y disponibilidad de los datos.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de tráfico de red cifrado conforme a los lineamientos de la entidad. • Fórmula: $\text{Porcentaje de tráfico cifrado} = \frac{\text{Volumen de tráfico de red cifrado}}{\text{Volumen total de tráfico de red}} * 100$ • Fuente: Plataformas de Monitoreo de Redes (NAC): Herramientas que monitorizan el acceso y comportamiento de los dispositivos en la red, verificando que las conexiones estén cifradas conforme a las políticas de la organización.
Declaración de aplicabilidad	Se implementan medidas de seguridad para proteger la información durante el teletrabajo, asegurando que los colaboradores cumplan con las políticas establecidas.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	A.6.2.2 Teletrabajo
Lineamientos Generales	<ul style="list-style-type: none"> ✓ La Subdirección de Investigación e información -SII junto con la Subdirección de Gestión y Desarrollo del Talento Humano, personal de planta, provisional, contratistas y con los supervisores de contratos; desarrollarán y establecerán los respectivos protocolos de monitoreo sobre las actividades que desarrollan su trabajo en estas modalidades, para minimizar el riesgo de afectación sobre la integridad, disponibilidad, privacidad y confidencialidad de los activos de información a los cuales tiene acceso durante el teletrabajo o trabajo en casa o trabajo remoto, lo anterior según el aplique de acuerdo con la relación contractual o laboral. ✓ El líder del teletrabajador o supervisor del contratista; definirá la información a acceder, aplicaciones, sistemas de información o servicios de la Entidad que se utilizarán para la ejecución de las labores u obligaciones durante el teletrabajo o trabajo en casa o trabajo remoto según corresponda aplicando las tablas de control de acceso definidas por la entidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 12 de 42</p>


	<ul style="list-style-type: none"> ✓ En caso de requerirse conexión remota la Subdirección de Investigación e información -SII debe garantizar el uso de las conexiones VPN “Client to Site” y canales seguros para el acceso, procesamiento, almacenamiento y transporte de los datos. ✓ Los dispositivos usados para el teletrabajo, trabajo en casa o trabajo remoto deben tener un antivirus actualizado, sistema operativo licenciado y con las actualizaciones, en caso contrario y de manera preventiva se podrá denegar o inhabilitar la conexión remota a los servicios provistos por la SDIS. ✓ Se debe garantizar por parte de los colaboradores que toda la información generada debe almacenarse en los repositorios autorizados y controlados por la SDIS en caso de ser almacenado en el dispositivo móvil personal se traslada toda responsabilidad frente a los controles de acceso, respaldo, criptografía y demás controles indicados por la Entidad para garantizar la confidencialidad, integridad y disponibilidad de la información almacenada en el dispositivo. ✓ Todos los colaboradores en teletrabajo, trabajo en casa o trabajo remoto deben informar a la mesa de servicio las posibles anomalías en los dispositivos institucionales o en la información, así como eventos o incidentes de forma inmediata y seguir los lineamientos para la gestión de incidentes de seguridad de la información. ✓ Todos los colaboradores deberán acogerse y dar cumplimiento a las políticas y controles definidos para el cumplimiento del teletrabajo, trabajo en casa o trabajo remoto.
--	--

7.1.5. Política de seguridad para el talento humano

Objetivo	Asegurar que todos los colaboradores y terceros comprendan y cumplan con sus responsabilidades en materia de seguridad de la información, protegiendo los intereses de la organización durante los procesos de cambio de roles o terminación de empleo.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Gestión Corporativa • Subdirección de Gestión y Desarrollo del Talento Humano
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de colaboradores y contratistas capacitados en seguridad de la información. • Fórmula: (Número de colaboradores y contratistas capacitados en seguridad de la información / Total de colaboradores y contratistas) / 100. • Fuente: Registro de las bases de datos o sistemas de gestión de recursos humanos que registren la capacitación recibida por colaboradores y contratistas, especificando los cursos de seguridad de la información.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN	Código: LIN-TI-002
	LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 13 de 42


	<ul style="list-style-type: none"> • Meta: 100%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se establecen procesos de capacitación y concienciación en seguridad de la información para todos los colaboradores y terceros, garantizando su comprensión y cumplimiento de las responsabilidades.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	A.7.1.1 Investigación de antecedentes A.7.1.2 Términos y condiciones de contratación A.7.2.1 Responsabilidades de gestión A.7.2.2 Concientización, educación y capacitación en seguridad de la información A.7.2.3 Proceso disciplinario A.7.3.1 Cese o cambio de puesto de trabajo
Lineamientos Generales	<p>La Subdirección de Gestión y Desarrollo del Talento Humano, o quien haga sus veces, debe cumplir con los siguientes lineamientos:</p> <ul style="list-style-type: none"> ✓ Establecer y verificar los antecedentes de todos los candidatos, garantizando el cumplimiento de los requisitos legales, reglamentarios e internos antes de cualquier relación contractual o laboral. ✓ Definir una lista de verificación para la revisión de antecedentes y documentos del personal a vincular, conforme a la legislación y reglamentación aplicable, y archivar dicha lista junto con los soportes en la carpeta contractual para contratistas o en la hoja de vida para personal de planta. ✓ Establecer los términos y condiciones en materia de seguridad y privacidad de la información, considerando las leyes de propiedad intelectual, protección de datos personales, y transparencia y acceso a la información pública. ✓ Solicitar a funcionarios y contratistas la firma de acuerdos de confidencialidad y no divulgación de información institucional. ✓ Incluir temas de seguridad y privacidad de la información en los programas de inducción y capacitación. ✓ Establecer la documentación y entregables necesarios para la desvinculación de funcionarios. ✓ Informar a la gestión de soporte y mantenimiento tecnológico sobre el personal que no se encuentre en servicio activo por más de 5 días hábiles, una vez formalizadas las novedades. ✓ Comunicar los términos y condiciones de seguridad de la información desde el momento de la vinculación. ✓ Especificar las responsabilidades de seguridad y privacidad que permanecen válidas durante cambios de funciones, terminación de contrato o desvinculación, garantizando procesos ordenados y seguros. ✓ Comunicar a todos los colaboradores las consecuencias del incumplimiento de las políticas de seguridad y privacidad, y tomar las acciones pertinentes para documentar y escalar la situación si es necesario.

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 14 de 42


	<ul style="list-style-type: none"> ✓ Incluir en los contratos de prestación de servicios obligaciones referentes a las políticas y directrices de seguridad y privacidad de la información. ✓ Asignar y promover el uso del carné institucional, asegurándose de que se utilice de forma visible mientras se esté en las instalaciones de la SDIS o en representación de la entidad. ✓ Designar al supervisor del contrato o delegado la responsabilidad de consolidar la información de los contratistas en caso de terminación, investigación, o cambios de obligaciones, informar novedades para inhabilitar accesos y solicitar copias de respaldo de la información una vez termine la relación contractual. ✓ Todos los funcionarios, contratistas o proveedores de la SDIS deben asistir a las capacitaciones y eventos del plan de concientización en seguridad de la información, y abstenerse de divulgar información pública clasificada o reservada que pueda impactar operativamente o tener repercusiones legales para la entidad. ✓ Los supervisores de contrato deben informar a los subdirectores, oficial de seguridad o gestión de soporte y mantenimiento tecnológico sobre cualquier incumplimiento de las políticas y procedimientos de seguridad y privacidad de la información por parte de ellos mismos o de sus contratistas. ✓ Todos los supervisores de contratos deben informar a los subdirectores, oficial de seguridad o la gestión de soporte y mantenimiento tecnológico, el incumplimiento de las políticas y procedimientos de seguridad y privacidad de la información de la SDIS, por parte suya o de sus contratistas a cargo.
--	---

7.1.6. Política de gestión de activos de información


Objetivo y definición	Identificar los activos de información y definir las responsabilidades de protección adecuadas, asegurando que reciban el nivel apropiado de protección según su importancia para la entidad, y prevenir la divulgación, modificación, retiro o destrucción no autorizados de información almacenada en medios removibles.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Investigación e información - SII • Subdirección Administrativa y financiera
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de activos de información identificados y clasificados según su nivel de criticidad para aplicar controles de etiquetado y acceso. • Fórmula: $(\text{Número de activos de información identificados y clasificados} / \text{total de activos de información}) * 100$ • Fuente: Reporte de avance sobre la implementación de la guía de etiquetado sobre los documentos que hacen parte de la TRD

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 15 de 42

	<ul style="list-style-type: none"> • Meta: 100%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se identifican y clasifican los activos de información, implementando controles adecuados para proteger su confidencialidad, integridad y disponibilidad.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.8.1.1 Inventario de activos.</p> <p>A.8.1.2 Propiedad de los activos.</p> <p>A.8.1.3 Uso aceptable de los activos.</p> <p>A.8.1.4 Devolución de activos.</p> <p>A.8.2.1 Directrices de la clasificación.</p> <p>A.8.2.2 Etiquetado y manipulado de la información.</p> <p>A.8.2.3 Manipulación de los activos.</p> <p>A.8.3.1 Gestión de soportes extraíbles.</p> <p>A.8.3.2 Eliminación de soportes.</p> <p>A.8.3.3 Soportes físicos en tránsito.</p>
Lineamientos Generales	<p>La Subdirección de Investigación e Información (SII) o quien haga sus veces debe cumplir los siguientes lineamientos:</p> <ul style="list-style-type: none"> ✓ Los activos de la SDIS, incluidos información, sistemas, servicios y equipos (como estaciones de trabajo, equipos portátiles, impresoras, redes, servidores, aplicaciones, teléfonos, entre otros), se proporcionan a los funcionarios y contratistas para cumplir con los propósitos institucionales y desarrollo de sus funciones. ✓ Todos los activos deben estar inventariados y clasificados de acuerdo con los requisitos y criterios establecidos antes de ser asignados a un responsable. ✓ Custodiar los medios magnéticos y electrónicos, así como sus manuales y licencias de uso, siguiendo el tratamiento adecuado según su nivel de clasificación. ✓ Realizar una copia de respaldo de la información antes de destruir o eliminar de manera segura cualquier medio de almacenamiento, siguiendo el procedimiento establecido. ✓ Establecer lineamientos para el borrado seguro de la información institucional, detallando las herramientas, responsables y razones para su eliminación teniendo en cuenta además la disposición final establecida en las Tablas de Retención Documental de la entidad, y asegurar que, al cambiar de propósito, devolver por garantía, o finalizar la vida útil de los dispositivos tecnológicos y equipos de cómputo, la información institucional sea borrada, eliminada y destruida de manera segura. ✓ Verificar que los equipos de cómputo no contengan medios de almacenamiento antes de su disposición final, asegurando el uso de técnicas de borrado seguro para hacer la información irrecuperable. ✓ Definir lineamientos para el transporte seguro de medios que contengan información institucional, evitando accesos no autorizados y uso indebido. ✓ Implementar lineamientos para el etiquetado de la información en las herramientas tecnológicas de la entidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 16 de 42</p>


	<ul style="list-style-type: none"> ✓ Para equipos que manejan medios extraíbles, asegurar que tengan habilitado el escaneo automático de virus, bloqueo de reproducción automática de archivos ejecutables, y seguir los lineamientos para el ingreso, uso, y movilización de dispositivos de almacenamiento. ✓ Verificar y monitorear que la información que transita por la red cumpla con los protocolos de seguridad necesarios, garantizando su confidencialidad, disponibilidad e integridad. ✓ Implementar protocolos de seguridad para el cifrado de los datos. ✓ La SDIS deberá conformar un equipo interdisciplinario en el que participen miembros de las siguiente áreas: Dirección de Análisis y Diseño Estratégico – DADE, Dirección Territorial, Dirección Poblacional, Dirección para la Inclusión y las Familias, Dirección de Transferencias Monetarias, Subdirección de Diseño Evaluación y Sistematización – SDES, Oficina Asesora Jurídica, Dirección de Gestión Corporativa y la Subdirección Administrativa para: Definir, implementar, monitorear y socializar los lineamientos para el etiquetado de la información física, electrónica y digital Garantizar que a todos los colaboradores de la entidad se les asigne una cuenta de correo institucional, con el fin de mitigar fugas de información o uso indebido de la misma. ✓ Garantizar la integridad de la firma electrónica o digital para los documentos producidos en el cumplimiento de su misión y visión que requieran tener una firma. <p>Los funcionarios y contratistas deben:</p> <ul style="list-style-type: none"> ✓ Usar los activos de información de la SDIS exclusivamente para propósitos laborales. ✓ Tratar los activos de acuerdo con su nivel de clasificación. ✓ Utilizar solo programas y dispositivos autorizados por la SII. ✓ Abstenerse de almacenar información personal en los equipos de cómputo asignados. ✓ Solicitar requisitos de aplicativos, sistemas y equipos a través de la Mesa de Ayuda u otros canales autorizados. ✓ Usar la cuenta de correo electrónico exclusivamente para las funciones u obligaciones asignadas. ✓ No enviar información confidencial sin aplicar controles de seguridad o sin autorización. ✓ Evitar el uso de herramientas de mensajería instantánea no autorizadas para información pública clasificada o reservada. ✓ Usar Internet de manera ética y responsable, sin afectar la productividad ni la protección de la información. ✓ Generar requerimientos de borrado seguro de información con la debida autorización y en cumplimiento a la disposición establecida en las Tablas de Retención Documental de la entidad. ✓ Ejercer controles sobre la consulta de información pública reservada, clasificada o medios que la contienen para mantener un rastro de
--	--

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 17 de 42


	<ul style="list-style-type: none"> ✓ Devolver los activos de información al Director, Subdirector, líder de procesos o delegado al finalizar la vinculación. ✓ Asegurarse de no dejar documentos en equipos reprográficos tras su uso. ✓ Recoger documentos confidenciales de impresoras, escáneres y fotocopiadoras para evitar divulgación no autorizada. ✓ Proteger documentos y medios de almacenamiento de información sensible cuando se ausente del puesto de trabajo. <p>Los propietarios de los activos deben:</p> <ul style="list-style-type: none"> ✓ Establecer controles durante el ciclo de vida del activo, promover su uso y gestión adecuada, definir y revisar permisos, restricciones y clasificaciones, informar sobre requisitos de seguridad y monitorear actividades relacionadas con los activos. <p>Los custodios de los activos deben:</p> <ul style="list-style-type: none"> ✓ Implementar los controles definidos por el propietario, promover el uso adecuado de los activos, monitorear usuarios y permisos, y apoyar en el monitoreo de actividades realizadas en los activos. <p>Los Directores, Subdirectores y Líderes de Proceso deben:</p> <ul style="list-style-type: none"> ✓ Actuar como propietarios de los activos de información, aprobando o revocando accesos, asignando controles y custodios, y manteniendo actualizado el Registro de Activos de Información y el índice de información clasificada y reservada. ✓ Proteger los activos incluida la información clasificada y reservada aplicando controles para mantener su confidencialidad, integridad, disponibilidad y privacidad. ✓ Clasificar los activos según la Ley 1712 de 2014 o sus sustitutas, derogatorias o adiciones.
--	--

7.1.7. Política de control de acceso


Objetivo y definición	Gestionar el acceso a la información y a las instalaciones de procesamiento, estableciendo procedimientos que aseguren que solo los usuarios autorizados puedan acceder a sistemas y datos, al mismo tiempo que se previene el acceso no autorizado y se garantiza la responsabilidad de los usuarios en la protección de su información de autenticación.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Investigación e información - SII

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 18 de 42

Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de aplicaciones operativas e integradas con el Directorio Activo. • Fórmula: (Número de aplicaciones operativas e integradas con el Directorio Activo / Total de aplicaciones en el catálogo de SDIS) * 100 • Fuente: Registros de auditoría del Directorio Activo y el catálogo de aplicaciones disponible en SDIS. • Meta: 100%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se gestionan los accesos a sistemas y servicios mediante controles robustos, asegurando que solo los usuarios autorizados tengan acceso a la información crítica.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.9.1.1 Política de control de acceso.</p> <p>A.9.1.2 Control de acceso a las redes y servicios asociados.</p> <p>A.9.2.1 Gestión de altas/bajas en el registro de usuarios.</p> <p>A.9.2.2 Gestión de los derechos de acceso asignados a usuarios.</p> <p>A.9.2.3 Gestión de los derechos de acceso con privilegios especiales.</p> <p>A.9.2.4 Gestión de información confidencial de autenticación de usuarios.</p> <p>A.9.2.5 Revisión de los derechos de acceso a los usuarios.</p> <p>A.9.2.6 Retirada o adaptación de los derechos de acceso.</p> <p>A.9.3.1 Uso de información confidencial para la autenticación.</p> <p>A.9.4.1 Restricción de acceso a la información.</p> <p>A.9.4.2 Procedimientos seguros de inicio de sesión.</p> <p>A.9.4.3 Gestión de contraseñas de usuario.</p> <p>A.9.4.4 Uso de herramientas de administración de sistemas.</p> <p>A.9.4.5 Control de acceso al código fuente de los programas.</p>
Lineamientos Generales	<p>Controles Físicos y Ambientales</p> <ul style="list-style-type: none"> ✓ Controles de Acceso: Garantizar entornos seguros con controles de acceso adecuados en la Dirección General, sedes, entornos abiertos y dependencias que hacen parte de la estructura orgánica de la entidad y sus unidades operativas propias, arrendadas o cofinanciadas. ✓ Amenazas Físicas: Controlar amenazas externas y asegurar condiciones medioambientales óptimas para la plataforma tecnológica y la preservación de activos digitales y físicos. <p>Protección de Redes y Accesos</p> <ul style="list-style-type: none"> ✓ Establecer procedimientos de autorización para redes de datos. ✓ Asegurar redes inalámbricas con mecanismos de autenticación. ✓ Controlar la identificación y autenticación de usuarios externos a la SDIS. ✓ Proveer herramientas seguras para conexiones remotas. ✓ Proveer acceso limitado a información y sistemas solo según funciones y roles.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 19 de 42</p>


	<ul style="list-style-type: none"> ✓ Se deben definir mecanismos para solicitar, crear, inhabilitar y revisar accesos, incluyendo roles y privilegios, asegurando que se establezcan etiquetados adecuados y permisos asociados conforme al tipo de activos involucrados. <p>Gestión de Contraseñas</p> <ul style="list-style-type: none"> ✓ Longitud mínima de 12 caracteres, incluyendo mayúsculas, minúsculas, números y caracteres especiales. ✓ No usar información personal, secuencias básicas o el nombre de usuario. ✓ Cambiar contraseñas cada 30 días y después de divulgaciones accidentales. ✓ No almacenar contraseñas en navegadores ni en lugares accesibles. ✓ Cambiar contraseñas iniciales al primer uso y emplear autenticación segura. ✓ Las contraseñas de Administradores deben ser de al menos 14 caracteres, con una combinación de caracteres y deben ser cambiadas cada 60 días. ✓ Se debe mantener una política de historial de contraseñas que impida la reutilización de al menos las últimas 5 contraseñas para fortalecer la seguridad. <p>Gestión de Accesos de Usuarios Privilegiados</p> <ul style="list-style-type: none"> ✓ Revisar y autorizar privilegios especiales; registrar solicitudes y autorizaciones. ✓ Actualizar contraseñas inmediatamente después de cambios de personal y almacenar en lugares seguros. <p>Inicio de Sesión Seguro</p> <ul style="list-style-type: none"> ✓ Se deben garantizar conexiones seguras y proteger los sistemas contra intentos repetidos de acceso no autorizado, como aquellos que utilizan múltiples combinaciones de contraseñas de manera automatizada, asegurando el uso de términos claros y comprensibles. ✓ Registrar intentos exitosos y fallidos; asegurar terminación de sesiones inactivas después de 5 minutos. <p>Control de Acceso a Códigos Fuentes</p> <ul style="list-style-type: none"> ✓ Restringir el acceso al código fuente de aplicaciones a personal autorizado. ✓ Implementar herramientas para controlar cambios y retroceder versiones. <p>Uso Responsable y Cumplimiento</p> <ul style="list-style-type: none"> ✓ Custodiar, no divulgar y utilizar credenciales de forma responsable. No compartir cuentas ni contraseñas. ✓ Todos los usuarios deben autenticarse antes de usar los recursos tecnológicos y no proporcionar información de acceso a personal externo sin autorización.
--	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 20 de 42

	<p>Requisitos Adicionales</p> <ul style="list-style-type: none"> ✓ Todos los usuarios deben tener un ID único e intransferible. ✓ El área de tecnología debe custodiar y actualizar las contraseñas de administración, así como reemplazar aquellas que vienen por defecto.
--	---

7.1.8. Política de criptografía


Objetivo y definición	Asegurar el uso adecuado y eficaz de la criptografía en toda la organización para proteger la confidencialidad, autenticidad e integridad de la información.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Investigación e información – SII.
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de tráfico de red cifrado conforme a los lineamientos de la entidad. • Fórmula: $\text{Porcentaje de tráfico cifrado} = \frac{\text{Volumen de tráfico de red cifrado}}{\text{Volumen total de tráfico de red}} * 100$. • Fuente: Plataformas de Monitoreo de Redes (NAC): Herramientas que monitorizan el acceso y comportamiento de los dispositivos en la red, verificando que las conexiones estén cifradas conforme a las políticas de la organización.
Declaración de aplicabilidad	Se utiliza criptografía para proteger la confidencialidad e integridad de la información sensible, de acuerdo con las normativas y mejores prácticas aplicables.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<ul style="list-style-type: none"> • A.10.1.1 Política de uso de los controles criptográficos. • A.10.1.2 Gestión de claves.
Lineamientos Generales	<ul style="list-style-type: none"> ✓ La SDIS deberá usar e implementar controles criptográficos para proteger la confidencialidad, autenticidad o integridad de la información clasificada de la Entidad al momento de almacenarse o transmitirse. ✓ Proporcionar los mecanismos de cifrado necesarios para asegurar que la transmisión de información clasificada de forma interna o externa se realice de forma segura. ✓ La información pública reservada y pública clasificada debe almacenarse en repositorios cifrados de acuerdo con sus niveles de confidencialidad e integridad. ✓ Se debe disponer de los mecanismos de cifrado para el aseguramiento de las conexiones de acceso remoto a la red de la SDIS o recursos de la entidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 21 de 42


	<ul style="list-style-type: none"> ✓ Todas las llaves criptográficas de la Entidad deben estar resguardadas por los responsables y custodios protegiendo su confidencialidad, integridad y disponibilidad. ✓ La administración de llaves criptográficas y certificados digitales estarán a cargo de cargo de la Subdirección de Investigación o quien haga sus veces. ✓ Establecer mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas. ✓ Las llaves criptográficas serán deshabilitadas por la Subdirección de Investigación o quien haga sus veces, cuando estas se encuentren en riesgo de divulgación o cuando los colaboradores de la Entidad autorizados culminen la relación laboral o contractual con esta. <p>Todo funcionario, contratista de la SDIS y/o proveedores externos contratistas deben dar cumplimiento a los siguientes lineamientos:</p> <ul style="list-style-type: none"> ✓ Reportar mediante los canales autorizados, los incidentes o potenciales riesgos del sistema de cifrado o llaves criptográficas.
--	--

7.1.9. Política de seguridad física y del entorno


Objetivo y definición	Prevenir el acceso físico no autorizado y proteger la información y los activos de la entidad contra daños, robos, compromisos y la interrupción de las operaciones en las instalaciones de procesamiento de información.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Investigación e información - SII • Subdirección Administrativa y financiera
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de controles de acceso físico al datacenter implementados y operativos. • Fórmula: $(\text{Número de controles de acceso operativos} / \text{Total de controles de acceso planificados para el datacenter}) * 100$ • Fuente: Informes de auditoría de seguridad física y registros de acceso al datacenter. • Meta: 100%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se implementan controles físicos para proteger los activos de información contra el acceso no autorizado, daño y otras amenazas físicas.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.11.1.1 Perímetro de seguridad física.</p> <p>A.11.1.2 Controles físicos de entrada.</p> <p>A.11.1.3 Seguridad de oficinas, despachos y recursos.</p> <p>A.11.1.4 Protección contra las amenazas externas y ambientales.</p> <p>A.11.1.5 El Trabajo en áreas seguras.</p>

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 22 de 42

	<p>A.11.1.6 Áreas de acceso público, carga y descarga.</p> <p>A.11.2.1 Emplazamiento y protección de equipos.</p> <p>A.11.2.2 Instalaciones de suministro.</p> <p>A.11.2.3 Seguridad del cableado.</p> <p>A.11.2.4 Mantenimiento de los equipos.</p> <p>A.11.2.5 Salida de activos fuera de las dependencias de la empresa.</p> <p>A.11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.</p> <p>A.11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.</p> <p>A.11.2.8 Equipo informático de usuario desatendido.</p> <p>A.11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.</p>
Lineamientos Generales	<p>Gestión de Centros de Cableado y Data Centers</p> <p>Control de Temperatura y Humedad:</p> <ul style="list-style-type: none"> ✓ El administrador de los centros de cableado y/o del datacenter es responsable de mantener controles adecuados de temperatura y humedad en estos lugares, así como en los archivos que albergan información física. <p>Separación de Cables:</p> <ul style="list-style-type: none"> ✓ Los cables de energía eléctrica deben mantenerse separados de los cables de comunicaciones para evitar interferencias. Esta responsabilidad recae en el administrador de los centros de cableado y/o del datacenter. <p>Protección Contra Fallas Eléctricas:</p> <ul style="list-style-type: none"> ✓ Las dependencias responsables de los centros de cómputo y centros de cableado, en colaboración con la Subdirección Administrativa y Financiera, deben garantizar que los recursos tecnológicos estén protegidos contra fallas o interrupciones eléctricas. <p>Responsabilidades de la Subdirección Administrativa y Financiera</p> <ul style="list-style-type: none"> ✓ Proporcionar mecanismos tecnológicos para el registro de visitantes de la Entidad. ✓ Definir los perímetros de seguridad física basados en los activos de información de la Entidad y en las áreas seguras. ✓ Aplicar controles necesarios para mantener la seguridad en las instalaciones de procesamiento de información confidencial. ✓ Las áreas seguras deben permanecer bajo llave en ausencia de supervisión. ✓ Llevar un registro de entrada y salida de los visitantes, quienes deben ser supervisados a menos que su acceso haya sido previamente aprobado. ✓ Aplicar controles adecuados para evitar que actividades o información confidencial sean visibles y audibles desde el exterior. ✓ Mantener un control sobre la entrada y salida de equipos tecnológicos, los cuales deben ser retirados con la previa autorización del director o subdirector.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 23 de 42</p>


	<p>Lineamientos para Funcionarios, Contratistas y Proveedores Externos</p> <ul style="list-style-type: none"> ✓ Todo personal debe portar el carné o identificación en un lugar visible dentro de las instalaciones de la SDIS. ✓ Los colaboradores deben reportar al personal de seguridad cualquier visitante no acompañado y sin identificación visible. ✓ Está prohibido el uso de equipos fotográficos, de video o audio en áreas seguras sin autorización. ✓ No se permite el consumo de alimentos o bebidas en los puestos de trabajo. Conservar el escritorio o espacio de trabajo libre de información institucional al final del día, guardándola bajo llave. ✓ Los accesos físicos y lógicos se desactivarán o modificarán una vez terminados los vínculos contractuales o laborales. ✓ Las solicitudes para ingresar a centros de cómputo o centros de cableado deben ser dirigidas a la Subdirección de Investigación e Información. ✓ Los colaboradores deben realizar copias de seguridad locales o utilizar repositorios web para salvaguardar la información institucional en sus equipos de cómputo. ✓ Los lugares de trabajo deben ubicarse en áreas que no estén expuestas a personas externas. ✓ El equipo de cómputo para atención al público debe estar ubicado para evitar el acceso a la información por parte de los usuarios, y debe estar protegido y monitoreado por personal de seguridad. ✓ Documentos y dispositivos con información pública reservada, clasificada o reservada deben ser almacenados bajo llave y no dejarse a la vista. ✓ Los equipos deben ser bloqueados (en Windows, con las teclas Windows + L) y el monitor apagado cuando se ausente el personal. ✓ Los documentos con información reservada impresos deben ser recogidos inmediatamente. ✓ Implementar controles para asegurar físicamente los computadores portátiles, como guayas de seguridad. ✓ Al finalizar la jornada laboral, se deben cerrar todas las aplicaciones y apagar los equipos, salvo excepciones necesarias. ✓ No se deben publicar ni dejar a la vista documentos o datos críticos, como nombres de usuario, contraseñas, IP, números de cuentas, datos personales sensibles, etc. ✓ Las sesiones de escritorio remoto deben cerrarse inmediatamente después de su uso y requerir credenciales de acceso para cada conexión. ✓ La Subdirección de Investigación e Información y el Líder de Seguridad, establecerán controles para bloquear sesiones de equipos de cómputo tras un periodo de inactividad. ✓ La tecnología de la información aplicará un protector de pantalla que se active después de tres minutos de inactividad.
--	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 24 de 42


	<p>✓ Las estaciones de trabajo deben utilizar un protector de pantalla que se active automáticamente después de tres minutos de inactividad y solo pueda desbloquearse con la contraseña del usuario.</p>
--	---

7.1.10. Política de seguridad en las operaciones


Objetivo y definición	Asegurar el correcto funcionamiento de las instalaciones de procesamiento de información, protegiendo contra códigos maliciosos y pérdidas de datos, garantizando la integridad de los sistemas operacionales, registrando eventos para generar evidencia, previniendo el aprovechamiento de vulnerabilidades técnicas y minimizando el impacto de las actividades de auditoría sobre los sistemas.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Investigación en Información – SII. • Dirección de Análisis y Diseño Estratégico.
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de tiempo de disponibilidad de los sistemas críticos. • Fórmula: Porcentaje de disponibilidad = (Tiempo total de operación – tiempo de inactividad) / Tiempo total de operación *100. • Fuente: Informes de disponibilidad de la infraestructura. • Meta: 100%. • Frecuencia de medición: Mensual.
Declaración de aplicabilidad	Se aseguran procedimientos para la operación segura de sistemas y procesos, minimizando riesgos de seguridad y garantizando la integridad de los datos.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.12.1.1 Documentación de procedimientos de operación.</p> <p>A.12.1.2 Gestión de cambios.</p> <p>A.12.1.3 Gestión de capacidades.</p> <p>A.12.1.4 Separación de entornos de desarrollo, prueba y producción.</p> <p>A.12.2.1 Controles contra el código malicioso.</p> <p>A.12.3.1 Copias de seguridad de la información.</p> <p>A.12.4.1 Registro y gestión de eventos de actividad.</p> <p>A.12.4.2 Protección de los registros de información.</p> <p>A.12.4.3 Registros de actividad del administrador y operador del sistema.</p> <p>A.12.4.4 Sincronización de relojes.</p> <p>A.12.5.1 Instalación del software en sistemas en producción.</p> <p>A.12.6.1 Gestión de las vulnerabilidades técnicas.</p> <p>A.12.6.2 Restricciones en la instalación de software.</p> <p>A.12.7.1 Controles de auditoría de los sistemas de información.</p>
Lineamientos Generales	La Subdirección de Investigación e información -SII o quien haga sus veces debe:

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 25 de 42


	<ul style="list-style-type: none"> ✓ Documentar, formalizar, mantener actualizado y divulgar los procedimientos relacionados con la operación y administración de los servicios y componentes tecnológicos que garanticen la disponibilidad, integridad, confidencialidad y privacidad de la información, procedimientos como: copias de respaldo, mantenimiento de equipos, gestión de cambios, gestión de capacidad, gestión de eventos, entre otros. <p>Gestión de Cambios:</p> <ul style="list-style-type: none"> ✓ Establecer un procedimiento para la gestión de cambios donde se contemplen los mecanismos para las solicitudes de los cambios a nivel de infraestructura, aplicativos, sistemas de información, bases de datos, servicios tecnológicos de la entidad y en general a los activos de información tecnológicos y los recursos informáticos. ✓ Analizar los riesgos, impactos y requisitos de seguridad de la información de los cambios en los componentes tecnológicos, con el fin de no afectar la correcta operación de estos ni de otros servicios. ✓ Informar a los propietarios de los activos de información los cambios que se realicen a los servicios, componentes, sistemas de información y/o infraestructura a su cargo. <p>Gestión de Capacidad:</p> <ul style="list-style-type: none"> ✓ Establecer un procedimiento de gestión de capacidad que permita monitorear el uso y las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, así como la designación de responsables encargados de monitorear la capacidad de la infraestructura tecnológica. ✓ Supervisar continuamente el consumo, demanda y comportamiento de los recursos tecnológicos asignados, con el fin de realizar gestionar oportunamente los cambios y/o ajustes que se requieran y proyectar las futuras necesidades de capacidad. <p>Separación de Ambientes:</p> <ul style="list-style-type: none"> ✓ Definir los lineamientos para la separación de los ambientes: desarrollo, pruebas, preproducción y producción utilizados en el desarrollo de software y soporte de aplicaciones, con el fin de reducir los riesgos de acceso o cambios no autorizados que puedan afectar la confidencialidad, integridad y disponibilidad de los entornos productivos, teniendo en cuenta consideraciones como: <ul style="list-style-type: none"> • Controles para el intercambio de información entre los diferentes ambientes. • Estandarización de las herramientas utilizadas para los diferentes ambientes. • Gestión de accesos de acuerdo con roles, privilegios y ambientes. • Separación de redes, bases de datos e información.
--	--

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 26 de 42</p>


	<p>Protección contra códigos maliciosos:</p> <ul style="list-style-type: none"> ✓ Instalar, controlar y mantener actualizada en todos los equipos de cómputo y servidores de la entidad una herramienta de antivirus, que permita la gestión centralizada de las amenazas, eventos, estados de los equipos, entre otros. <p>Todos los funcionarios, contratistas y terceros:</p> <ul style="list-style-type: none"> ✓ Deben verificar que la información y los medios de almacenamiento, estén libres de cualquier tipo de código malicioso, para lo cual deben analizarlos con el software antivirus instalado en sus equipos de cómputo. ✓ Deben reportar inmediatamente ante la sospecha o evento de infección por virus, a la mesa de ayudas para que realice la revisión y eliminación del virus. ✓ No deben realizar modificaciones o eliminar las configuraciones de seguridad en Antivirus, Office 365, navegadores u otros programas, para detectar y prevenir la propagación de virus. <p>Lineamientos para Copias de Respaldo</p> <p>Los lineamientos aplican a todos los sistemas, aplicaciones y dispositivos de almacenamiento que manejan información pública reservada y clasificada en la SDIS. A continuación, se detallan las responsabilidades y procedimientos clave:</p> <ul style="list-style-type: none"> ✓ La Subdirección de Investigación e Información (SII) debe documentar, divulgar y mantener actualizado un procedimiento de respaldo de información. Este procedimiento incluirá la arquitectura de conectividad para respaldos y estrategias de generación, retención, rotación y periodicidad de las copias de seguridad. ✓ Junto con los propietarios de los activos de información y el Líder de Seguridad de la Información, se definirá la información pública reservada y clasificada a respaldar, y se cumplirán los tiempos de retención establecidos en las Tablas de Retención Documental de la entidad. ✓ El sistema de almacenamiento de copias de respaldo debe garantizar la seguridad física y protección de los medios de almacenamiento, tanto internos como externos. Las copias deben almacenarse en un lugar remoto para protegerlas de daños en el centro de datos principal. ✓ Se debe mantener un inventario de las copias de respaldo, y las cintas deben almacenarse externamente, asegurando los protocolos de seguridad en transporte y custodia. ✓ Las pruebas de restauración deben realizarse al menos cuatro veces al año en ambientes controlados. Los resultados de estas pruebas deben ser documentados y reportados.
--	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 27 de 42</p>

	<ul style="list-style-type: none"> ✓ La información pública clasificada debe estar protegida mediante cifrado, y no se deben almacenar datos personales, videos, fotos, música u otra información no relacionada con la misión y objetivos de la SDIS. ✓ Los procedimientos deben incluir registros exactos y completos de las copias de respaldo, frecuencia de backup (completos, diferenciales, incrementales) y estar alineados con los requisitos de seguridad y continuidad operativa. ✓ Definir los periodos de retención y eliminación de la información conforme a la normativa vigente y la Tabla de Retención Documental. ✓ Para sistemas críticos, las copias de respaldo deben permitir la recuperación completa en un centro de datos alterno, alineadas con el RPO (Recovery Point Objective) y RTO (Recovery Time Objective) del Plan de Continuidad del Negocio y Planes de Recuperación (DRP). ✓ La SII no es responsable de los respaldos de información en equipos de cómputo individuales o dispositivos de almacenamiento. Los respaldos solicitados deben ser autorizados por el Director, Subdirector o líder de proceso. ✓ Aplicar las estrategias de preservación digital a largo plazo con el fin de garantizar la disponibilidad, integridad y confidencialidad de los documentos y archivos que serán preservados; de igual forma, garantizar que las características de los medios de almacenamiento final sean las idóneas para tal fin, de acuerdo con lo establecido en el Plan de Preservación Digital a Largo Plazo de la Entidad. <p>Control de Eventos</p> <p>Las áreas operativas responsables de la gestión de sistemas de información, deben:</p> <ul style="list-style-type: none"> ✓ Generar y revisar periódicamente registros de auditoría que contengan actividades del usuario, excepciones, fallas y eventos de seguridad de la información de las actividades de los sistemas de información e infraestructura crítica. ✓ Implementar los controles necesarios por la custodia, confidencialidad, integridad y disponibilidad de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros. ✓ En conjunto con los responsables de los servicios, definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos de la entidad. ✓ Determinar los eventos que generarán registros de auditoría en los recursos tecnológicos y los sistemas de información. ✓ Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con el tipo de información y la criticidad de las operaciones.
--	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 28 de 42</p>


	<ul style="list-style-type: none"> ✓ Sincronizar los relojes de los servidores, sistemas de información, telefonía, CCTV, sistemas de información, estaciones de trabajo y todo componente de información; con una única fuente de referencia de tiempo con el fin de garantizar la exactitud de los registros de auditoría. <p>Control de Software</p> <p>La Subdirección de Investigación e información - SII, a través del equipo de infraestructura debe:</p> <ul style="list-style-type: none"> ✓ Documentar, actualizar y divulgar los procedimientos para controlar la instalación de software en los equipos de cómputo de la entidad, estableciendo las responsabilidades, restricciones y limitaciones. ✓ Garantizar que el software instalado en la plataforma tecnológica cuente con soporte en caso de ser necesario y con los proveedores según sea requerido. ✓ Gestionar oportunamente las actualizaciones sobre el software instalado. ✓ Validar los riesgos que genera la migración hacia nuevas versiones del software, realizando las correspondientes pruebas y contando con la aprobación del Comité de Cambios. <p>Gestión de Vulnerabilidades</p> <p>La Subdirección de Investigación e información – SII en conjunto con el equipo de infraestructura, revisará periódicamente (cada seis meses), los resultados de las pruebas de vulnerabilidades técnicas y ethical hacking sobre los recursos de la plataforma tecnológica.</p> <ul style="list-style-type: none"> ✓ Debe revisar cada seis meses o según se requiera, la aparición de nuevas vulnerabilidades técnicas y reportarlas a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de prevenir la exposición al riesgo de estos. ✓ Debe generar, ejecutar y monitorear planes de acción para la mitigación de las vulnerabilidades técnicas detectadas en la plataforma tecnológica cada tres meses. <p>Restricciones en la instalación del software</p> <p>La Subdirección de Investigación e información - SII, a través del equipo de gestión de soporte y mantenimiento tecnológico o quien haga sus veces:</p> <ul style="list-style-type: none"> ✓ Es la única dependencia autorizada para realizar la instalación de software o programas en los sistemas operativos de los equipos de cómputo y portátiles institucionales.
--	---

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN	Código: LIN-TI-002
	LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 29 de 42


	<ul style="list-style-type: none"> ✓ Debe realizar la instalación de software en los computadores suministrados por la SDIS, como función exclusiva de esta o a quienes ellos deleguen. ✓ Debe autorizar el software adicional que se requiera instalar en equipos de cómputo específicos de la SDIS. ✓ Debe definir, mantener y publicar la lista actualizada del software autorizado y no autorizado para instalar en los computadores la SDIS. ✓ Validar y controlar el uso de software libre teniendo en cuenta las limitaciones para el uso corporativo y validado por el Oficial de Seguridad de la Información. ✓ Controlar y validar la instalación y administración de las licencias de programas y software autorizado. <p>Auditorias de sistemas de información</p> <ul style="list-style-type: none"> ✓ Las áreas de cumplimiento, la segunda línea defensa y las responsables de la implementación de normativas, verificarán el cumplimiento de los requisitos de las normas ISO aplicables, la normatividad legal vigente y los requisitos propios de la organización, según sea necesario. ✓ Las áreas responsables y/o propietarias de los sistemas de información donde se encuentren desviaciones, deficiencias o no conformidades, deberán generar y darle cumplimiento, a un plan de mitigación o atención, con el apoyo de la Subdirección de Investigación e información, a través del equipo de infraestructura.
--	---

7.1.11. Política de seguridad de las comunicaciones

Objetivo	Garantizar la protección de la información durante su transmisión a través de redes de datos, tanto alámbricas como inalámbricas, que facilitan la comunicación y el intercambio de información dentro de la entidad y con entidades externas.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Análisis y Diseño Estratégico. • Subdirección de Investigación e información – SII. • Oficina Asesora de Comunicaciones. • Oficina Jurídica. • Subdirección Administrativa y Financiera.
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de tráfico de red cifrado conforme a los lineamientos de la entidad. • Fórmula: Porcentaje de tráfico cifrado = Volumen de tráfico de red cifrado / Volumen total de tráfico de red *100. • Fuente: Plataformas de Monitoreo de Redes (NAC): Herramientas que monitorizan el acceso y comportamiento de los dispositivos en la red, verificando que las conexiones estén cifradas conforme a las políticas de la organización.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 30 de 42


	<ul style="list-style-type: none"> • Meta: 95%. • Frecuencia de medición: Semestral.
Declaración de aplicabilidad	Se aplican medidas de seguridad para proteger la información durante su transmisión en redes, garantizando la confidencialidad y la integridad de los datos. Se aplican medidas de seguridad para proteger la información durante su transmisión en redes, garantizando la confidencialidad y la integridad de los datos.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.13.1.1 Controles de red.</p> <p>A.13.1.2 Mecanismos de seguridad asociados a servicios en red.</p> <p>A.13.1.3 Segregación de redes.</p> <p>A.13.2.1 Políticas y procedimientos de intercambio de información.</p> <p>A.13.2.2 Acuerdos de intercambio.</p> <p>A.13.2.3 Mensajería electrónica.</p> <p>A.13.2.4 Acuerdos de confidencialidad y secreto.</p>
Lineamientos Generales	<p>Gestión de la Seguridad de las Redes</p> <ul style="list-style-type: none"> ✓ Se deben identificar mecanismos de seguridad, niveles de servicio y requisitos de gestión para servicios de red, tanto internos como externos, e incluirlos en los acuerdos de servicio. ✓ Se deben adoptar medidas para asegurar la disponibilidad y minimizar riesgos de seguridad en redes de datos. ✓ Se debe mantener redes segmentadas y establecer controles para proteger información y minimizar riesgos, incluyendo la protección contra códigos maliciosos. ✓ Se debe instalar protección entre redes internas y externas y garantizar la confidencialidad de la información de direccionamiento y enrutamiento. ✓ Se debe bloquear accesos no corporativos y mantener configuraciones seguras en equipos inalámbricos. Garantizar que las redes inalámbricas tengan seguridad similar a las cableadas. ✓ Se debe proporcionar recursos para la administración segura del servicio de internet, monitorear el uso, y establecer procedimientos de continuidad y restablecimiento en caso de contingencias. ✓ Se debe implementar campañas de concientización sobre el uso seguro de internet. <p>Todo funcionario, contratista y/o proveedores externos contratistas de la SDIS:</p> <ul style="list-style-type: none"> ✓ Está prohibido enviar, retransmitir, o acceder a contenido ofensivo o ilegal, y evitar la instalación de software no autorizado. ✓ El uso del internet está limitado a actividades laborales, evitando el acceso a sitios no corporativos y el uso de servicios interactivos para intercambio de información confidencial. ✓ No se debe descargar ni compartir material que infrinja derechos de propiedad intelectual, ni ejecutar archivos que puedan comprometer o exponer la seguridad de la entidad.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 31 de 42


	<p>Transferencia de Información</p> <ul style="list-style-type: none"> ✓ Definir procedimientos de transferencia de información, establecer acuerdos de confidencialidad, y asegurar que se protejan la integridad y confidencialidad de la información. ✓ Incluir cláusulas de confidencialidad en contratos con terceros y definir controles de seguridad y responsabilidades. ✓ Usar controles criptográficos para la transferencia de información, con acuerdos específicos para garantizar la seguridad y el cumplimiento legal. <p>Mensajería Electrónica y Herramientas Colaborativas</p> <ul style="list-style-type: none"> ✓ Establecer procedimientos para la administración de cuentas de correo electrónico, proteger contra códigos maliciosos y evitar el envío de mensajes masivos no autorizados. ✓ Mantener la privacidad y seguridad de las cuentas de correo, evitar el uso de cuentas ajenas y no utilizar el correo para actividades no institucionales. ✓ Respetar el formato y estándares corporativos, no enviar correos maliciosos o SPAM, y reportar cualquier incidente de seguridad. <p>Almacenamiento en la Nube</p> <ul style="list-style-type: none"> ✓ Limitar el almacenamiento en la nube a fines institucionales y prohibir el almacenamiento de información reservada sin cifrar en nubes públicas. ✓ Realizar copias de seguridad de la información y usar únicamente herramientas institucionales para mensajería y reuniones virtuales. ✓ Para el almacenamiento de documentación en la nube se deben aplicar lineamientos de gestión documental como clasificación, ordenación y descripción de documentos y expedientes. <p>Administradores de Plataformas</p> <ul style="list-style-type: none"> ✓ Monitorear cuentas de correo sólo con la debida autorización y para investigaciones relevantes, siguiendo procedimientos establecidos. ✓ Se deben revisar periódicamente las cuentas inactivas y proceder con su eliminación, a menos que se solicite lo contrario.
--	---

7.1.12. Política de adquisición, desarrollo seguro y mantenimiento de sistemas


<p>Objetivo y definición</p>	<p>Garantizar que la seguridad de la información se aplique de forma integral en el ciclo de vida de todos los sistemas de información, incluyendo aquellos que operan en redes públicas, asegurando que se consideren requisitos de seguridad en cada fase de desarrollo y protegiendo los datos utilizados durante las pruebas.</p>
------------------------------	---

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 32 de 42

Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> Subdirección de Investigación e información – SII.
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> Directores, Subdirectores y Líderes de procesos Apoyos a la supervisión de contratos. Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> Indicador: Porcentaje de aplicaciones desarrolladas que han pasado las pruebas de vulnerabilidad. Fórmula: (Número de aplicaciones que superaron las pruebas de vulnerabilidad / Total de aplicaciones desarrolladas) * 100. Fuente: Informes de pruebas de penetración y análisis de vulnerabilidades. Meta: 60%. Frecuencia de medición: Anual por aplicación operativa.
Declaración de aplicabilidad	<p>Se implementan controles para asegurar que la seguridad de la información se integre en todas las fases del ciclo de vida de los sistemas. Esto incluye la evaluación de riesgos en la adquisición, el diseño seguro en el desarrollo, y la protección de datos durante las pruebas, garantizando la confidencialidad, integridad y disponibilidad de la información, incluso en sistemas que operan en redes públicas.</p>
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.14.1.1 Análisis y especificación de requisitos de los requisitos de seguridad.</p> <p>A.14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.</p> <p>A.14.1.3 Protección de transacciones por redes telemáticas.</p> <p>A.14.2.1 Política de desarrollo seguro de software.</p> <p>A.14.2.2 Procedimientos de control de cambios en los sistemas.</p> <p>A.14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.</p> <p>A.14.2.4 Restricciones en los cambios en los paquetes de software.</p> <p>A.14.2.5 Uso de principios de ingeniería en protección de sistemas.</p> <p>A.14.2.6 Seguridad en entornos de desarrollo.</p> <p>A.14.2.7 Externalización del desarrollo de software.</p> <p>A.14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.</p> <p>A.14.2.9 Pruebas de aceptación.</p> <p>A.14.3.1 Protección de los datos utilizados en pruebas.</p>
Lineamientos Generales	<p>La Subdirección de Investigación e Información (SII), junto con el grupo de Fábrica de Software y el Oficial de Seguridad CISO, es responsable de planificar, desarrollar y ejecutar actividades relacionadas con el ciclo de vida del software, asegurando la integración de los requisitos de seguridad y privacidad según las necesidades de la SDIS. Los lineamientos establecidos incluyen:</p> <ul style="list-style-type: none"> ✓ Asegurar que todo software, interno o externo, cumpla con los requisitos de seguridad y calidad de la SDIS.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p>	<p>Código: LIN-TI-002</p>
	<p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	<p>Versión: 1</p>
		<p>Fecha: Memo I2024030735 – 23/10/2024</p>
		<p>Página: 33 de 42</p>


	<ul style="list-style-type: none"> ✓ Definir metodologías que integren requisitos de seguridad y buenas prácticas durante el desarrollo. ✓ Establecer un entorno seguro en todas las fases del proyecto y entre diferentes ambientes (producción, pruebas, desarrollo). ✓ Liderar la definición de los requerimientos de seguridad, incluyendo autenticación y control de acceso. ✓ Documentar criterios de aceptación y pruebas de funcionalidad y seguridad, asegurando la trazabilidad de los requerimientos. ✓ Garantizar la inclusión de requisitos de seguridad en todas las fases del ciclo de vida del software. ✓ Realizar pruebas de seguridad en el código fuente y la aplicación en cada fase del desarrollo. ✓ Certificar que se utilicen herramientas de desarrollo licenciadas y actualizadas. ✓ Implementar mecanismos de seguridad en todas las fases del desarrollo y proteger datos personales en pruebas. ✓ Evitar el uso de información confidencial en pruebas y anonimizar datos de producción en entornos de desarrollo. ✓ Generar registros de auditoría para todas las operaciones importantes en los sistemas. ✓ Formalizar la solicitud de nuevos desarrollos o modificaciones siguiendo los procedimientos institucionales. ✓ Documentar cualquier excepción a los mecanismos mínimos de seguridad con la debida justificación. ✓ Cada sistema debe contar con manuales de uso, técnicos y administrativos. ✓ Documentar los requerimientos y definir la arquitectura de software adecuada. ✓ Utilizar canales seguros y cifrados para la transmisión de pagos o transacciones en línea. ✓ Obtener aprobación de la SII para la adquisición de software, siguiendo políticas de seguridad. ✓ Establecer procedimientos para la adquisición o desarrollo de sistemas, asegurando el cumplimiento de los requerimientos de seguridad. ✓ Definir y solicitar la eliminación de información pública clasificada o reservada de los sistemas. ✓ Planificar y ejecutar pruebas funcionales y de aceptación para nuevos desarrollos o modificaciones. <p>Aseguramiento de Código Fuente:</p> <ul style="list-style-type: none"> ✓ Limitar la entrada y salida de datos y gestionar errores sin comprometer la seguridad. ✓ No almacenar credenciales en el código e implementar módulos de seguridad. ✓ Usar protocolos seguros para la transferencia de datos y gestionar sesiones y cookies.
--	--

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 34 de 42


	<ul style="list-style-type: none"> ✓ Implementar controles según el top 10 de OWASP y evitar exponer información sensible en el código o logs. ✓ Mantener separados los ambientes de desarrollo, pruebas y producción. ✓ Llevar control de versiones del código y documentación. ✓ Deshabilitar funcionalidades innecesarias y cerrar sesiones y conexiones inactivas. <p>Desarrollo Seguro:</p> <ul style="list-style-type: none"> ✓ Garantizar que el desarrollo cumpla con los requerimientos de seguridad y buenas prácticas. ✓ Realizar pruebas de aceptación y asegurar la correcta migración entre ambientes. ✓ Administrar cambios y mantener actualizadas las plataformas tecnológicas. ✓ Proporcionar soporte adecuado y validar datos de entrada y salida. <p>Desarrollo Externo:</p> <ul style="list-style-type: none"> ✓ Definir procesos para administración de parches y acuerdos de confidencialidad con proveedores. ✓ Solicitar acuerdos de licenciamiento y definir requisitos de seguridad en los pliegos de contratación. ✓ Implementar protocolos cifrados para la comunicación de datos y transferencia de los desarrollos cuando aplique. <p>Datos de Prueba:</p> <ul style="list-style-type: none"> ✓ Proteger los datos de prueba, garantizar que no revelen información confidencial y anonimizar datos de producción. ✓ Eliminar la información de los ambientes de prueba al finalizar las pruebas.
--	---

7.1.13. Política de relación con los proveedores


Objetivo	Garantizar la protección de los activos de la organización accesibles a los proveedores, asegurando que mantengan el nivel acordado de seguridad de la información y la calidad en la prestación del servicio conforme a los acuerdos establecidos.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Subdirección de Contratación • Subdirección de Investigación e información - SII • Oficina Jurídica
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 35 de 42

Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de proveedores que cumplen con los requisitos de seguridad de la información establecidos en los acuerdos de servicio. • Fórmula: Porcentaje de proveedores en cumplimiento = (Número de proveedores que cumplen con los requisitos de seguridad / Número total de proveedores evaluados) /100 • Fuente: Revisar los contratos y acuerdos de servicio que establecen los requisitos de seguridad de la información. • Meta: 90%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se establecen criterios de seguridad en la gestión de relaciones con proveedores, asegurando que se mantenga un nivel adecuado de protección de la información.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.15.1.1 Política de seguridad de la información para las relaciones con proveedores.</p> <p>A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores.</p> <p>A.15.1.3 Cadena de suministro de Tecnología de información y comunicación.</p> <p>A.15.2.1 Seguimiento y revisión de los servicios de los proveedores.</p> <p>A.15.2.2 Gestión de cambios en los servicios de los proveedores.</p>
Lineamientos Generales	<p>La SDIS implementará mecanismos de control en sus relaciones con proveedores para asegurar que la información y los servicios accedidos cumplan con las políticas y procedimientos de seguridad y privacidad de la información. Los proveedores deben:</p> <ul style="list-style-type: none"> ✓ Contar con planes de contingencia y procedimientos de buenas prácticas en un Sistema de Gestión de Seguridad de la Información (SGSI). ✓ Definir procedimientos para la gestión de eventos, incidentes, contingencia y recuperación de la información asignada, alineados con los controles de seguridad y privacidad de SDIS. ✓ Devolver activos físicos y lógicos generados o almacenados en sistemas no autorizados por SDIS. ✓ Cumplir con los requisitos legales para la protección de datos, derechos de propiedad intelectual y autor. ✓ Mantener la confidencialidad de los datos personales privados y sensibles conforme a la ley 1581 de 2012 y las políticas institucionales. ✓ Utilizar la información recibida solo para los fines contractuales establecidos. <p>Responsabilidades de los Supervisores de Contrato:</p>


 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 36 de 42

	<ul style="list-style-type: none"> ✓ Definir controles de seguridad para el acceso del proveedor a la información, cumpliendo con la Política de Seguridad y Privacidad de SDIS. ✓ Divulgar las políticas y procedimientos de seguridad y privacidad a los proveedores. ✓ Evaluar riesgos de seguridad y privacidad asociados a la información manejada por proveedores. ✓ Revisar, con el apoyo del Líder de Seguridad, que los contratos incluyan acuerdos de confidencialidad y cumplimiento de políticas de seguridad. ✓ Las áreas de cumplimiento, la segunda línea de defensa y los responsables de la implementación de normativas, verificarán el cumplimiento de los requisitos de las normas ISO aplicables, la normatividad legal vigente y los requisitos propios de la organización según sea necesario. <p>Responsabilidades de la Subdirección Administrativa y Financiera y la Oficina Jurídica:</p> <ul style="list-style-type: none"> ✓ Incluir requisitos de seguridad en los procesos de adquisición de productos y servicios tecnológicos. ✓ Solicitar la firma de acuerdos de confidencialidad en contratos que impliquen el intercambio o procesamiento de información de SDIS. ✓ Asegurar que los acuerdos de confidencialidad formen parte integral de los contratos. ✓ Establecer protocolos de intercambio de información en acuerdos o anexos técnicos, especificando las condiciones y controles de seguridad necesarios. <p>Responsabilidades de la Subdirección de Investigación e Información - SII:</p> <ul style="list-style-type: none"> ✓ Establecer condiciones adecuadas para la conexión de equipos de terceros a la red de datos de SDIS. ✓ Identificar y mitigar riesgos asociados a terceros con acceso a los sistemas de información de SDIS. <p>Responsabilidades de la Subdirección de Gestión y Desarrollo de Talento:</p> <ul style="list-style-type: none"> ✓ Con el apoyo del Líder de Seguridad y la Subdirección de Investigación e Información - SII, desarrollar y divulgar una guía para Acuerdos de Niveles de Servicio y requisitos de seguridad informática para proveedores. ✓ Elaborar modelos de Acuerdos de Confidencialidad y de Intercambio de Información, con responsabilidades civiles y penales para las partes contratadas.
--	--

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 37 de 42

7.1.14. Política de gestión de incidentes de seguridad de la información


Objetivo y definición	Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluyendo la comunicación sobre eventos y debilidades en la seguridad.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> Subdirección de Investigación e información - SII
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> Directores, Subdirectores y Líderes de procesos Apoyos a la supervisión de contratos. Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> Indicador: Tiempo promedio de respuesta a incidentes de seguridad de la información. Fórmula: $\text{Tiempo promedio de respuesta} = (\text{Suma de tiempos de respuesta a todos los incidentes}) / (\text{Número total de incidentes reportados})$ Fuente: Incidentes de seguridad registrados por la herramienta de gestión Aranda Meta: Reducir el tiempo promedio de respuesta de incidentes. Frecuencia de medición: Mensual.
Declaración de aplicabilidad	Se implementan procedimientos para la gestión de incidentes, garantizando que los eventos de seguridad sean comunicados y tratados de manera efectiva.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.16.1.1 Responsabilidades y procedimientos.</p> <p>A.16.1.2 Reporte de eventos de seguridad de la información.</p> <p>A.16.1.3 Reporte de debilidades de seguridad de la información.</p> <p>A.16.1.4 Evaluación de eventos de seguridad de la información y decisiones sobre ellos.</p> <p>A.16.1.5 Respuesta a incidentes de seguridad de la información.</p> <p>A.16.1.6 Aprendizaje obtenido de los incidentes de seguridad de la información.</p> <p>A.16.1.7 Recolección de evidencia.</p>
Lineamientos Generales	<p>Colaboradores:</p> <ul style="list-style-type: none"> ✓ Reportar inmediatamente a través de la mesa de ayuda cualquier evento o incidente relacionado con la seguridad de la información o los recursos tecnológicos. ✓ El reporte debe incluir datos mínimos para evidenciar y respaldar las acciones realizadas, siguiendo el procedimiento definido y alineado con la política de seguridad de la información. <p>Subdirección de Investigación e Información - SII:</p> <ul style="list-style-type: none"> ✓ Detectar incidentes a través de alertas, colaboradores, proveedores o entidades externas relacionadas con aspectos técnicos, físicos o procedimentales.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 38 de 42

	<ul style="list-style-type: none"> ✓ Gestionar el seguimiento y tratamiento de los incidentes, asignando responsables para investigar y solucionar los problemas, y escalando según su criticidad. ✓ Solo los Directores, Subdirectores o el Líder de Seguridad están autorizados para reportar incidentes a las autoridades y hacer pronunciamientos oficiales. ✓ Establecer responsabilidades y procedimientos para una respuesta rápida y efectiva a los incidentes. ✓ Documentar una base de conocimiento con incidentes y soluciones para mejorar tiempos de respuesta futuros. ✓ Comunicar a los colaboradores sobre la gestión de incidentes y buenas prácticas para minimizar su ocurrencia. <p>Subdirección de Investigación e Información:</p> <ul style="list-style-type: none"> ✓ Documentar todos los incidentes en la herramienta designada, detallando claramente el seguimiento, análisis y control. ✓ Definir mecanismos para el análisis, contención y erradicación eficiente de los incidentes de seguridad. ✓ Identificar y registrar riesgos materializados para su reevaluación en la gestión de riesgos. ✓ Investigar incidentes causados por acciones, omisiones o exralimitaciones que contravengan la seguridad de la información.
--	---

7.1.15. Política de Seguridad en la gestión de continuidad de negocio


Objetivo y definición	Integrar la seguridad de la información en los sistemas de gestión de continuidad de negocio de la organización para asegurar la disponibilidad de las instalaciones de procesamiento de información y garantizar la continuidad de los servicios y operaciones en caso de incidentes.
Responsable(s) de la ejecución de la política – Alta Dirección	<ul style="list-style-type: none"> • Dirección de Análisis y Diseño Estratégico • Subdirección de Investigación e información - SII • Subdirección de Diseño, Evaluación y Sistematización
Responsable(s) del cumplimiento de la política	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos. • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
Indicador	<ul style="list-style-type: none"> • Indicador: Porcentaje de pruebas DRP realizadas con éxito. • Fórmula: $\text{Porcentaje de pruebas exitosas} = \frac{\text{Número de pruebas exitosas}}{\text{Número total de pruebas realizadas}} \times 100$ • Fuente: Mantener un registro detallado de todas las pruebas de DRP realizadas, incluyendo fechas, tipos de pruebas y resultados. • Meta: 90%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se integran controles de seguridad en los planes de continuidad de negocio, asegurando que se mantenga la disponibilidad de servicios críticos.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 39 de 42


<p>Controles que abarca la norma NTC-ISO-27001:2013 Anexo A</p>	<p>A.17.1.1 Planificación de la continuidad de la seguridad de la información. A.17.1.2 Implementación de la continuidad de la seguridad de la información. A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información. A.17.2.1 Disponibilidad de instalaciones de procesamiento de información.</p>
<p>Lineamientos Generales</p>	<p>La Dirección de Análisis y Diseño Estratégico debe:</p> <ul style="list-style-type: none"> ✓ Realizar regularmente el Análisis de Impacto de Negocio (BIA) para identificar la criticidad de los productos o servicios críticos de la entidad. ✓ Asegurar la continuidad de la seguridad de la información mediante un Plan de Continuidad de Negocio y un Plan de Recuperación de Desastres, gestionados por Tecnologías de la Información y Soporte Técnico. ✓ Establecer y ejecutar pruebas periódicas del Plan de Continuidad de Negocio para evaluar la recuperación, requisitos de seguridad, funciones y responsabilidades. ✓ Asignar roles y responsabilidades detallados en el Plan de Continuidad a personal capacitado para manejar incidentes de continuidad. ✓ Incluir en el plan de concientización información sobre Continuidad del Negocio para asegurar una reacción eficiente de los colaboradores ante incidentes. ✓ Gestionar el manejo de crisis y comunicación adecuada durante incidentes significativos que interrumpan los servicios. ✓ Exigir que los procesos desarrollados por terceros cuenten con planes de continuidad y sean probados regularmente. ✓ Garantizar que los planes de continuidad se ejecuten de manera segura, protegiendo la información de la entidad.

7.1.16. Política de Cumplimiento

<p>Objetivo y definición</p>	<p>Asegurar el cumplimiento de las obligaciones legales, estatutarias, reglamentarias y contractuales relacionadas con la seguridad de la información, garantizando que su implementación se realice conforme a las políticas y procedimientos organizacionales establecidos.</p>
<p>Responsable(s) de la ejecución de la política – Alta Dirección</p>	<ul style="list-style-type: none"> • Oficina Jurídica • Oficina de Control Disciplinario Interno • Subdirección de Investigación e información - SII • Dirección de Análisis y Diseño Estratégico • Subdirección Administrativa y Financiera
<p>Responsable(s) del cumplimiento de la política</p>	<ul style="list-style-type: none"> • Directores, Subdirectores y Líderes de procesos • Apoyos a la supervisión de contratos. • Todos los colaboradores de la SDIS.
<p>Indicador</p>	<ul style="list-style-type: none"> • Indicador: Porcentaje de políticas y procedimientos de seguridad revisados y actualizados.

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 40 de 42

	<ul style="list-style-type: none"> • Fórmula: (Número de políticas y procedimientos revisados / Total de políticas y procedimientos de seguridad) * 100. • Fuente: Informe de implementación del MSPI. • Meta: 100%. • Frecuencia de medición: Anual.
Declaración de aplicabilidad	Se aplican controles para asegurar el cumplimiento con las obligaciones legales y reglamentarias, garantizando que la seguridad de la información sea parte integral de las operaciones organizacionales.
Controles que abarca la norma NTC-ISO-27001:2013 Anexo A	<p>A.18.1.1 Identificación de la legislación aplicable y de los requisitos Contractuales.</p> <p>A.18.1.2 Derechos de propiedad intelectual.</p> <p>A.18.1.3 Protección de registros.</p> <p>A.18.1.4 Privacidad y protección de información de datos personales.</p> <p>A.18.1.5 Reglamentación de controles criptográficos.</p> <p>A.18.2.1 Revisión independiente de la seguridad de la información.</p> <p>A.18.2.2 Cumplimiento con las políticas y normas de seguridad.</p> <p>A.18.2.3 Revisión del cumplimiento técnico.</p>
Lineamientos Generales	<p>Colaboradores, Contratistas y Proveedores Externos:</p> <ul style="list-style-type: none"> ✓ Está prohibida la descarga, instalación o uso de software no autorizado por la Subdirección de Investigación e Información (SII), así como la utilización de software ilegal o no autorizado, lo cual puede acarrear consecuencias disciplinarias para los funcionarios. ✓ Se debe cumplir con la Política de Protección de Datos Personales, el manual de protección de datos y sus procedimientos. <p>Subdirección de Investigación e Información (SII):</p> <ul style="list-style-type: none"> ✓ Adquirir software respetando derechos de autor y verificar licencias y términos de uso. ✓ Asegurar que todo software en la institución esté licenciado o sea de libre distribución. ✓ Designar personal para instalar, configurar y dar soporte a equipos de cómputo. ✓ Mantener un listado actualizado de software permitido y controlar su instalación y uso. ✓ Implementar controles para la instalación y uso adecuado de programas y software. ✓ Realizar verificaciones periódicas para asegurar que los sistemas cumplan con los lineamientos de seguridad. <p>Oficina de Control Disciplinario Interno:</p> <ul style="list-style-type: none"> ✓ Estudiar y evaluar procesalmente las quejas e informes con connotación disciplinaria derivados de los eventuales incumplimientos en la política de seguridad y privacidad. <p>Área de Gestión Documental:</p>

 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL</p>	<p>PROCESO TECNOLOGÍAS DE LA INFORMACIÓN</p> <p>LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL</p>	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 41 de 42


	<ul style="list-style-type: none"> ✓ Establecer controles para conservar la información física, electrónica y digital en condiciones adecuadas y cumplir con los lineamientos del Archivo General de la Nación. <p>Dirección de Análisis y Diseño Estratégico:</p> <ul style="list-style-type: none"> ✓ Documentar, publicar e implementar la política de Protección de Datos Personales en cumplimiento de la normativa vigente. ✓ Definir lineamientos para el Sistema de Gestión de Seguridad de la Información (SGSI) y protección de datos personales. ✓ Hacer seguimiento y validar el cumplimiento de políticas y procedimientos del SGSI. ✓ Articular procesos del SGSI con la alta consejería TIC del distrito. <p>Oficina de Control Interno:</p> <ul style="list-style-type: none"> ✓ Realizar evaluación independiente en atención a sus funciones y roles como tercera línea de defensa. <p>Oficina Jurídica:</p> <ul style="list-style-type: none"> ✓ Identificar y mantener actualizados los requisitos legales, reglamentarios y contractuales relacionados con la seguridad de la información. ✓ Asesorar en la propiedad intelectual y establecer lineamientos para el cumplimiento de derechos de autor. <p>Subdirección Administrativa y Financiera y Oficina Jurídica:</p> <ul style="list-style-type: none"> ✓ Identificar legislación y requisitos aplicables a los procesos contractuales. ✓ Incluir cláusulas de seguridad y privacidad en los contratos y definir directrices para la protección de información institucional. <p>Directores, Subdirectores, Líderes de Proceso, TI, Soporte y Líder de Seguridad:</p> <ul style="list-style-type: none"> ✓ Apoyar las revisiones del cumplimiento de políticas de seguridad y privacidad de la información.
--	---

8. Evaluación del lineamiento o Política interna

La evaluación del lineamiento se realizará de manera trimestral a través de la aplicación de la herramienta de verificación de controles implementados, MSPI, conforme a la Política de Seguridad de la Información. Los resultados de los seguimientos serán presentados a la Subdirección de Investigación e instancias que lo soliciten, para su revisión y análisis, con el fin de asegurar el cumplimiento de los controles establecidos y proponer mejoras continuas.

9. Responsabilidades y competencias

Las responsabilidades de ejecutar este lineamiento, cumplirlo a cabalidad y sin excepciones son todos los funcionarios, contratistas y visitantes de la Secretaría de Integración Social, de acuerdo

 ALCALDÍA MAYOR DE BOGOTÁ D.C. SECRETARÍA DE INTEGRACIÓN SOCIAL	PROCESO TECNOLOGÍAS DE LA INFORMACIÓN LINEAMIENTOS ESPECÍFICOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL	Código: LIN-TI-002
		Versión: 1
		Fecha: Memo I2024030735 – 23/10/2024
		Página: 42 de 42

con lo descrito en los numerales de responsable(s) del cumplimiento de cada una de las políticas definidas.

10. Comunicación de las políticas

Se establecerán los mecanismos necesarios para la comunicación efectiva de la Política de Seguridad de la Información, asegurando su difusión tanto a nivel interno de la entidad como a las partes interesadas externas, según corresponda. Esto permitirá que todos los colaboradores, contratistas y demás actores relevantes comprendan los objetivos, lineamientos y responsabilidades establecidos en la política, fomentando un entorno de trabajo seguro y alineado con los principios de protección de la información.

11. Administración del lineamiento

Subdirección de Investigación e Información

12. Aprobación del documento

	Elaboró	Revisó	Aprobó
Nombre	Edna Rocio Univio Amaya	Mayra Andrea Ruiz Bello Claudia Patricia Guerrero Johanna Paola Caicedo Murcia Carolina Sarasty Manotas Inés Francy Medina Peña Deysi Yolima Gutiérrez Liliana Niño Montoya Diego Felipe Bustos	Iván Osejo Villamil Comité de gestión y desempeño institucional
Cargo/Rol	Contratista – Subdirección de Investigación e información	Gestora SG - proceso Tecnologías de la información Contratista – Subdirección de Investigación e Información Dirección de Análisis y Diseño Estratégico Subdirección de Diseño Evaluación y Sistematización Gestión Documental Subdirección Administrativa y Financiera Oficina Asesora de Comunicaciones Jefe Oficina de Control Disciplinario Interno	Subdirector de Investigación e información (E)