 <p>ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL <small>Instituto Distrital para la Protección de la Niñez y la Juventud</small></p>	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	1 de 13
		VIGENTE DESDE	04/03/2025



**POLÍTICA DE SEGURIDAD Y
PRIVACIDAD DE LA INFORMACIÓN
- POLÍTICA SEGURIDAD DIGITAL -
POLÍTICA DE CIBERSEGURIDAD Y
CIBERDEFENSA**


 ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Distrital para la Protección de la Niñez y la Juventud	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	2 de 13
		VIGENTE DESDE	04/03/2025

TABLA DE CONTENIDO

1. OBJETIVO GENERAL 3

1.1. Objetivos específicos3

2. ALCANCE 3

3. CONDICIONES GENERALES..... 3

4. GLOSARIO 3

5. MARCO NORMATIVO 5

6. DECLARACIÓN DE LA POLÍTICA..... 7

7. DECLARACIÓN DE LA POLÍTICA DE CIBERSEGURIDAD Y CIBERDEFENSA..... 7

8. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 7

8.1. Diagnóstico8

8.2. Planeación8

8.3. Implementación.....8

8.4. Evaluación de desempeño.....8

8.5. Mejora continua8

9. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL 8

10. POLÍTICA DE CIBERSEGURIDAD Y CIBERDEFENSA 9

11. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN..... 9


11.1. Colaboradores(as)9

11.2. Dependencias 10

12. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA 10

13. CONTROL DE CAMBIOS 10

14. REVISIÓN Y APROBACIÓN 13

 ALCALDÍA MAYOR DE BOGOTÁ D.C. INTEGRACIÓN SOCIAL Instituto Distrital para la Protección de la Niñez y la Juventud	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	3 de 13
		VIGENTE DESDE	04/03/2025

1. OBJETIVO GENERAL

Dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a las normas técnicas aplicables en Colombia en materia de seguridad y privacidad de la información, seguridad digital y protección de datos personales que correspondan al IDIPRON.

1.1. Objetivos específicos

- 1. Definir y formalizar los elementos normativos sobre los temas de protección de la información del IDIPRON.
- 2. Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información, seguridad digital y ciberseguridad y ciberdefensa.
- 3. Mitigar el impacto de los incidentes de seguridad y privacidad de la información, así como los relacionados con seguridad digital, de forma efectiva, eficaz y eficiente en el contexto de los procesos institucionales del IDIPRON.
- 4. Establecer los mecanismos de aseguramiento físico y digital para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información del IDIPRON.
- 5. Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información adaptada a las necesidades del IDIPRON.

2. ALCANCE

La presente política aplica a todo el modelo de operación del IDIPRON, en cumplimiento de lo establecido en el marco legal y normativo vigente, incluyendo el Decreto 1083 de 2015, el Decreto 1078 de 2015 sobre la Política de Gobierno Digital, y la Resolución 500 de 2021, alineado con la NTC/IEC ISO 27001 de 2022. Este documento establece lineamientos de obligatorio cumplimiento para el adecuado uso, administración y protección de los activos de información del Instituto, incorporando directrices para su gestión responsable, el seguimiento periódico y la actualización de la política. Asimismo, define los instrumentos necesarios para mitigar riesgos, prevenir amenazas y garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

3. CONDICIONES GENERALES

La Oficina de Tecnologías de la Información y las Comunicaciones - TIC realizará el seguimiento y cumplimiento del Modelo de Seguridad y Privacidad de la Información aprobado por la Dirección de la Entidad.

El equipo de trabajo de la Oficina Asesora de Planeación, Oficina de TIC y la Gerencia Administrativa “Gestión Documental”, realizará el acompañamiento a los procesos para actualizar el inventario de activos de información para que estos realicen la clasificación de cada uno de ellos de acuerdo con su naturaleza.


La Oficina de TIC realizará el análisis de riesgos de seguridad de la información y seguridad digital, de acuerdo con la línea de defensa y con la metodología dispuesta por el DAFP, MINTIC y la Alta Consejería de las TIC.

La Oficina de TIC definirá la declaración de aplicabilidad e implementará los controles de acuerdo con el Anexo A de la NTC- ISO/IEC – 27001 de 2022.


El proceso de Gestión Tecnológica y de la Información desarrollará y documentará el procedimiento de Gestión de Incidentes de Seguridad de la Información y establecerá la documentación que deberá ser tomada en cuenta para el reporte de incidentes ante CSIRT o COLCERT.

4. GLOSARIO

Termino	Definición
Activos de Información	En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga,

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	4 de 13
		VIGENTE DESDE	04/03/2025

Termino	Definición
	adquiera, transforme o controle en su calidad de tal. Modelo de Seguridad Privacidad – MINTIC.
Amenaza	Posible violación de la seguridad digital que tiene el potencial de ocurrir total o parcialmente en el entorno digital. Se caracteriza por la aparición de una situación donde uno o más actores (externos o internos) adelantan una o varias acciones con la capacidad de alterar una infraestructura física, un sistema de información o la integridad de la información en sí. (Tomado del Documento CONPES 3995).
Ataque	Amenaza intencional que se concreta. (Tomado del Documento CONPES 3995).
Ataque cibernético	Acción organizada y/o premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia)
Ciberseguridad	Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguras y tecnologías que puedan utilizarse buscando la disponibilidad, autenticación confidencialidad y no repudio, con el fin de proteger a los usuarios y activos de la organización en el ciberespacio. (Tomado del Documento CONPES 3854).
Confidencialidad	Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados. Tomado de NTC ISO/IEC 27000:2013.
Disponibilidad	Propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada, cuando ésta así lo requiera. NTC ISO/IEC 27000:2013
Gestión de Riesgo	Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. GTC 137 ISO Guía 73:2009
Hacking	Es el ingreso ilegal a computadores, páginas y redes sociales con el objetivo de robar información, suplantar la identidad del dueño, beneficiarse económicamente o protestar. MINTIC.
Incidente	Cualquier evento adverso real o sospechado, intencionado o no intencionado, que puede cambiar el curso esperado de una actividad en el entorno digital. (Tomado del Documento CONPES 3995).
IP (Internet Protocol)	Etiqueta numérica que identifica, de manera lógica y jerárquica, a una interfaz (elemento de comunicación/conexión) de un dispositivo (habitualmente una computadora) dentro de una red que utilice el protocolo IP. (http://www.iso.org)
Integridad	Propiedad de salvaguardar la exactitud y estado completo de los activos. NTC ISO/IEC 27000:2013
Modelo de Seguridad y Privacidad de la Información (MSPI):	El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital - MINTIC
No Repudio	Servicio de seguridad que previene que un emisor niegue haber remitido un mensaje (cuando realmente lo ha emitido) y que un receptor niegue su recepción (cuando realmente lo ha recibido. (ISO-7498-2)
Riesgo Informático	Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. (ISO Guía 73:2002)
Riesgos de Seguridad Digital	Es la expresión usada para describir una categoría de riesgo relacionada con el desarrollo de cualquier actividad en el entorno digital. Este riesgo puede resultar de la combinación de amenazas y vulnerabilidades en el ambiente digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. El riesgo de seguridad

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	5 de 13
		VIGENTE DESDE	04/03/2025

Termino	Definición
	digital es de naturaleza dinámica. Incluye aspectos relacionados con el ambiente físico y digital, las personas involucradas en las actividades y los procesos organizacionales que las soportan. (Tomado del Documento CONPES 3854)
Sistema de Gestión de Seguridad de la Información SGSI	Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).
Seguridad de la Información	Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas. Guía # 1 Metodológica de Pruebas de Efectividad - MINTIC

Fuente: Creación Propia Oficina TIC


5. MARCO NORMATIVO

Las normas para considerar respecto al Instituto Distrital para la Protección de la Niñez y la Juventud - IDIPRON, el Sistema Distrital de Información y la Comisión Distrital de Sistemas son las siguientes:

Tipo de norma	Descripción
Constitución Política de Colombia Del 04 de julio de 1991 Congreso de la República	Artículo 15 que reconoce el derecho a la intimidad personal y familiar y al buen nombre, y la obligación del Estado de respetarlos y hacerlos respetar. Artículo 20 en donde se garantiza a toda persona la libertad de expresar y difundir su pensamiento y opiniones, la de informar y recibir información veraz e imparcial, y la de fundar medios de comunicación masiva. Artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano. Artículo 217 que establece que las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional entre otros”.
Directiva 5 del 12 de agosto de 2005 Alcaldía Mayor de Bogotá D.C.	“Políticas Generales de Tecnologías de Información y Comunicaciones aplicables a las entidades del Distrito Capital” Alcaldía Mayor de Bogotá D.C. Gestión Tecnológica y de la Información.
Resolución 305 del 20 de octubre de 2018 Secretaría General Alcaldía Mayor de Bogotá D.C. – Comisión Distrital de Sistemas – CDS	“Por la cual se expiden políticas públicas para las entidades, organismos y órganos de control del Distrito Capital, en materia de Tecnologías de la Información y Comunicaciones respecto a la planeación, seguridad, democratización, calidad, racionalización del gasto, conectividad, infraestructura de Datos Espaciales y Software Libre”
Ley 1266 del 31 de diciembre de 2008 Congreso de la República	“Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones”
Ley 1273 del 5 de enero de 2009 Congreso de la República	“Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado “de la protección de la información y de los datos”- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”
Ley 1341 del 30 de julio de 2009 Congreso de la República	Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional del Espectro y

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	6 de 13
		VIGENTE DESDE	04/03/2025

Tipo de norma	Descripción
	se dictan otras disposiciones"
Decreto 235 del 28 de enero de 2010 Ministerio del Interior y Justicia	“Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas”
CONPES 3701 del 14 de julio de 2011 Ministerio del Interior y Justicia	Lineamientos de Política para ciberseguridad y ciberdefensa
Ley 1581 del 17 de octubre de 2012 Congreso de la República	“Por la cual se dictan disposiciones generales para la protección de datos personales”.
Decreto 1377 del 27 de junio de 2013 Ministerio de Comercio, Industria y Turismo	“Por el cual se reglamenta parcialmente la Ley 1581 de 2012”
Ley 1712 del 6 de marzo de 2014 Congreso de la República	“Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”
Decreto 103 del 20 de enero de 2015 Presidencia de la República	"Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones”
Decreto 1083 del 26 de mayo de 2015 Presidencia de la República	“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública.”
Decreto 1078 del 26 de mayo de 2015 Presidencia de la República	“Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones”
CONPES 3854 del 11 de abril de 2016 MINTIC	Política Nacional de Seguridad Digital
Decreto 1413 del 25 de agosto de 2017 MINTIC	“Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título 111 de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales”
Resolución 4 del 28 de noviembre de 2017 Secretaría General Alcaldía Mayor de Bogotá D.C. – Comisión Distrital de Sistemas – CDS	“Por la cual se modifica la Resolución 305 de 2008 de la CDS”
CONPES 3920 del 17 de abril de 2018 Departamento Nacional de Planeación	Política Nacional de Explotación de Datos (BiG Data)
Acuerdo 702 del 23 de abril de 2018 Consejo de Bogotá	“Por el cual se adoptan lineamientos para la definición de estrategias de prevención frente a la ocurrencia de crímenes cibernéticos que amenazan o vulneran los derechos de las niñas, niños, adolescentes y Jóvenes del Distrito Capital”.
Decreto 1008 del 14 de junio de 2018 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”.
Resolución 500 de marzo 10 de 2021 Ministerio de Tecnologías de la Información y las Comunicaciones	“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“
Acuerdo 822 de 2021 Concejo de Bogotá, D.C	“Por medio del cual se dictan los lineamientos para la promoción del ciclo virtuoso de la seguridad, el uso y aprovechamiento de los datos en Bogotá”
Decreto 338 de 8 de marzo de 2022	“Por el cual se adiciona el Título 21 a la Parte 2 del Libro del Decreto Único 1078 de 2015, Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad.

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	7 de 13
		VIGENTE DESDE	04/03/2025

Tipo de norma	Descripción
	Digital coma se crea el modelo y las instancias de gobernanza, de seguridad digital y se dictan otras disposiciones”
Norma Técnica Colombiana NTC-ISO- IEC-27001 del 2022 Instituto Colombiano de Normas Técnicas y Certificación.	Sistema de Gestión de la Seguridad de la Información.
Acuerdo 002 de 2023 Alcaldía Mayor de Bogotá, D.C.	“Por el cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad LA COMISIÓN DISTRITAL DE TRANSFORMACIÓN DIGITAL”.

Fuente: Creación Propia Oficina TICS

6. DECLARACIÓN DE LA POLÍTICA

Con el fin de garantizar la disponibilidad confidencialidad e integridad de la información. El IDIPRON, como responsable de la Política de Seguridad y Privacidad de la Información y Seguridad Digital; se compromete a disponer de los recursos necesarios que permitan el seguimiento y control para la conservación de la información en sus criterios de disponibilidad, confidencialidad e integridad, realizando las actividades que sean necesarias de acuerdo con lo establecido en la normatividad vigente en especial al modelo de seguridad y privacidad y la información MSPI.

Esta política es de obligatorio cumplimiento para todos los (as) funcionarios(as) contratistas colaboradores(as) y proveedores del IDIPRON sin importar su modo de vinculación.

7. DECLARACIÓN DE LA POLÍTICA DE CIBERSEGURIDAD Y CIBERDEFENSA

Con el propósito de garantizar la ciberseguridad y la ciberdefensa el IDIPRON, como responsable de la Política de Ciberseguridad y Ciberdefensa, se compromete a disponer de los recursos necesarios para asegurar el seguimiento y control de la conservación de la información bajo los criterios de disponibilidad, confidencialidad e integridad. Para ello, llevará a cabo las actividades necesarias conforme a la normatividad vigente.

Esta política es de obligatorio cumplimiento para todos los (as) funcionarios (as), contratistas, colaboradores (as) y proveedores del IDIPRON, sin importar su modalidad de vinculación.

8. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IDIPRON deberá implementar y realizar un seguimiento periódico del Sistema de Gestión de Seguridad de la Información, en concordancia con la Norma Técnica NTC-ISO/IEC 27000 de 2016 y la GTC-ISO/IEC 27003 de 2017, con el propósito de conservar la información y los datos de manera íntegra, auténtica, fiable y disponible. Asimismo, deberá mantener actualizados y controlados los activos de información, tanto físicos como digitales, que posee el Instituto, garantizando una adecuada gestión de riesgos y la continuidad de la operación de la Entidad.

El desarrollo de cada una de las fases permitirá adoptar el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el MINTIC, asegurando el cumplimiento de las etapas y el ciclo de desarrollo del modelo.


	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	8 de 13
		VIGENTE DESDE	04/03/2025



Figura No. 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

8.1. Diagnóstico

El diagnóstico del Modelo de Seguridad y Privacidad de la Información es elaborado con base a un instrumento que brinda El Ministerio y las Tecnologías de Información y Comunicaciones MinTIC, llamado autodiagnóstico, donde se enumeran cada uno de los controles que tiene la norma ntc 27001. Con este tipo de controles administrativos y técnicos se puede mostrar el avance que se tiene en el sistema de gestión de seguridad de la información, que en adelante llamaremos, Modelo De Seguridad Y Privacidad De La Información MSPI.

8.2. Planeación

Como parte de la planeación el autodiagnóstico, es la primera herramienta que se utiliza para analizar el contexto de la entidad y la cantidad de elementos, que se encuentran para la gobernanza del Modelo De Seguridad Y Privacidad La Información. En su primera etapa la planeación, busca encontrar los roles y responsabilidades de cada uno de los directivos, que serán las personas indicadas, para propiciar la creación del Modelo De Seguridad Y Privacidad En El Instituto.

8.3. Implementación

La implementación del Modelo De Seguridad Y Privacidad De La Información, en el Instituto, se hará de acuerdo con lo estipulado en las guías contenidas para tal fin, que dicta El Ministerio de las Tecnologías de Información y Comunicaciones MinTIC.

8.4. Evaluación de desempeño


La evaluación de desempeño se tomará basados, en las brechas que se encuentren en el autodiagnóstico de seguridad y privacidad la información, de donde se tomará el insumo de aquellas vulnerabilidades para continuar con la implementación de los desfases encontrados.

8.5. Mejora continua

La mejora continua del sistema de seguridad información y/o modelo de seguridad y privacidad la información, será constante, los elementos para realizar esta mejora se tomarán siempre del análisis del autodiagnóstico de la entidad, versus el estado de sus brechas que nos muestra el autodiagnóstico.

9. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN Y SEGURIDAD DIGITAL

El IDIPRON, mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado en el Sistema de Gestión de Seguridad y Privacidad de la Información, protege, preserva y administra

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	9 de 13
		VIGENTE DESDE	04/03/2025

la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información que circula en el mapa de operación por procesos.

Esto se realiza a través de una gestión integral de riesgos y la implementación de controles físicos y digitales para prevenir incidentes, garantizar la continuidad de la operación de los servicios misionales y dar cumplimiento a los requisitos legales, reglamentarios, regulatorios y a las normas técnicas aplicables en Colombia.

Es así como, la política está orientada a la mejora continua y al alto desempeño del Sistema de Gestión de Seguridad y Privacidad de la Información del IDIPRON, promoviendo el acceso y uso efectivo de las tecnologías de información y comunicación. contribuyendo al desarrollo integral de la niñez, adolescencia y juventud del Instituto.

10. POLÍTICA DE CIBERSEGURIDAD Y CIBERDEFENSA

El Instituto Distrital para la Protección de la Niñez y la Juventud (IDIPRON), mediante la adopción e implementación de la Política de Ciberseguridad y Ciberdefensa, protege, preserva y administra la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información institucional.

Esto se logra a través de una adecuada gestión de riesgos cibernéticos y la implementación de controles legales, técnicos, organizativos, físicos y digitales que permitan prevenir y contrarrestar incidentes o amenazas cibernéticas que puedan afectar al Instituto. La política está orientada a mitigar los riesgos asociados al uso de las Tecnologías de la Información y las Comunicaciones (TIC), garantizar la continuidad de los servicios misionales y asegurar la sostenibilidad y seguridad de los procesos institucionales.

Reconociendo que las TIC son esenciales para el desarrollo social y económico, pero que también pueden ser utilizadas con fines ilícitos como terrorismo, espionaje o guerra cibernética, el IDIPRON implementará medidas para proteger sus ciber activos críticos frente a accesos no autorizados, divulgación indebida, interrupción, modificación, destrucción, pérdida o mal uso. Esto se logrará mediante un programa integral de gestión de riesgos, la identificación de activos de información críticos y el monitoreo constante de sistemas para garantizar su confiabilidad.

La política fomenta la mejora continua en la gestión de ciberseguridad, contribuyendo al cumplimiento de los requisitos legales, regulatorios y normativos aplicables en Colombia. A través de acciones de sensibilización, capacitación y socialización lideradas por la Oficina de TIC, se busca garantizar la confidencialidad, integridad, disponibilidad y privacidad de la información institucional, fundamentales para el desarrollo integral de la niñez, juventud y demás beneficiarios del Instituto.


Esta política es de obligatorio cumplimiento para todos los(as) funcionarios(as), contratistas, colaboradores(as) y proveedores del IDIPRON, sin importar su modalidad de vinculación, asegurando así la sostenibilidad y seguridad de sus procesos misionales.

11. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

11.1. Colaboradores(as)

Todos(as) los(as) empleados(as) públicos(as) o contratistas que hagan uso de los recursos tecnológicos del Instituto Distrital para la Protección de la Niñez y la Juventud (IDIPRON) tienen la responsabilidad de cumplir cabalmente las políticas establecidas para su uso aceptable, entendiendo que el uso no adecuado de los recursos pone en riesgo la continuidad de la operación de los servicios y, por ende, el cumplimiento de la misión institucional. Para ello, deben acatar las siguientes disposiciones:

- 1. **Del uso del correo electrónico:** El correo electrónico institucional es una herramienta de apoyo para la ejecución de funciones y obligaciones de los(las) empleados(as) públicos(as) y contratistas del IDIPRON. El uso debe estar alineado con las políticas de seguridad de la información y únicamente para fines relacionados con la misión del Instituto.
- 2. **Del uso de Internet:** Será responsabilidad de los(as) colaboradores(as) respetar estas políticas y evitar actividades que comprometan la seguridad de la información o la continuidad de los servicios.

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	10 de 13
		VIGENTE DESDE	04/03/2025

3. **Del uso de los recursos tecnológicos:** Los recursos tecnológicos del IDIPRON son herramientas de apoyo a las labores, responsabilidades y obligaciones de los(as) empleados(as) públicos(as) y contratistas. Es deber de los(as) usuarios(as) utilizarlos de manera ética, eficiente y alineada con las políticas institucionales, evitando cualquier acción que pueda comprometer su seguridad o disponibilidad.
4. **Del uso de los sistemas, herramientas de información y sistemas de almacenamiento institucionales:** Todos(as) los(as) empleados(as) públicos(as) y contratistas del IDIPRON son responsables de la protección de la información a la que acceden y procesan, garantizando que no se pierda, altere, destruya o use indebidamente. Los(as) usuarios(as) deben cumplir con los lineamientos establecidos para el uso adecuado de los sistemas institucionales, asegurando la confidencialidad, integridad y disponibilidad de la información.

11.2. Dependencias

Dependencias encargadas		Roles y responsabilidades
Comité Institucional de Gestión y Desempeño		Responsable de aprobar la Política de Seguridad y Privacidad de la Información, Seguridad Digital y seguimiento al cumplimiento del MSPI.
Oficina de TIC		Liderar la implementación del Modelo de Seguridad y Privacidad de la Información, así mismo adelantar las acciones y los mecanismos necesarios para implementar los controles y mitigar los riesgos identificados; actualizar el manual de controles básicos y específicos para el manejo de los activos de información y los datos del Instituto.
Dirección General		Dirigir, orientar y hacer seguimiento de la Implementación del Modelo de Seguridad y Privacidad de la información.
Gerencia de Talento Humano		Desarrollar junto a la Oficina de TIC, el plan de formación y sensibilización de la entidad en temas de seguridad de la información.
Oficina Asesora de Planeación		Asesorar planear, avalar, aprobar, acompañar e impulsar el desarrollo de proyectos de Seguridad y Privacidad de la Información con las dependencias involucradas. Revisar y validar las Políticas de Seguridad de la Información.
Oficina Jurídica		Identificar y asesorar en la legislación aplicable al cumplimiento de la Seguridad de la Información.
Subdirección Técnica Poblacional		Sugerir, retroalimentar y dar cumplimiento de las Políticas de Seguridad en el ámbito misional de el IDIPRON.
Gerencia Administrativa “Administración Documental”		Establecer, proponer y verificar los controles requeridos para prevenir los riesgos que puedan afectar la información almacenada en el Archivo Central.
Oficina de Control Interno		Verificar y hacer seguimiento de la mejora continua en la Implementación del Modelo de Seguridad y Privacidad de la Información.


Fuente: Creación Propia Oficina TICS

12. SEGUIMIENTO Y EVALUACIÓN DE LA POLÍTICA


El IDIPRON realiza el seguimiento de la política mediante el cumplimiento de las actividades definidas en su Plan de Seguridad y Privacidad de la Información y en el Plan de Acción, así como a través del monitoreo continuo y las actividades de control realizadas por la Oficina de Control Interno de la Entidad.

13. CONTROL DE CAMBIOS


VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se dio inició la creación del manual	20/11/2009	ORALIA FRANCO GOEZ Profesional Universitario área de Sistemas
02	Se ajustó el manual según la nueva presentación de la documentación; y a su vez su nueva codificación en el listado	29/07/2011	JOSÉ VICENTE CASTRO ORDÓÑEZ Profesional Universitario área de

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	11 de 13
		VIGENTE DESDE	04/03/2025

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
	maestro		Sistemas
03	Se ajustó la Política y el Manual de acuerdo con los lineamientos de la Resolución 305 de 2008 y a las recomendaciones del Comité de Sistemas de Tecnología y Seguridad de la Información.	12/06/2013	BLEIDYS YEANA POLO URRUTIA Profesional Universitario área de Sistemas
04	Se pasa al proceso Gestión Tecnológica y de la Información, en versión 04; anteriormente se encontraba en el proceso Tecnología de la Información y Comunicaciones, con código A-TIC-MA-001, en versión 03 y vigente desde 21 JUNIO 2013. Se adecúa el encabezado a la plantilla vigente.	09/12/2014	ORALIA FRANCO GOEZ Profesional Universitario área de Sistemas
05	Se ajustó la Política y el Manual de acuerdo con la inclusión de los dominios de control de la norma NTC-ISO-IEC 27001:2013 y la NTC-ISO-IEC 27002:2013 y de los parámetros de configuración del correo electrónico en el Instituto.	30/03/2015	ORALIA FRANCO GOEZ Profesional Universitario área de Sistemas
06	Para la presente versión el manual se actualizó a la plantilla vigente de manual.	2/04/2019	SANDRA LUCIA BADLISSI TAJAN Profesional Área de Sistemas
07	Se realizó las siguientes modificaciones al documento: 1. Actualiza el documento a la plantilla vigente. 2. Se migra el documento de Manual a documento interno. 3. Se cambia el nombre al documento de acuerdo con su contenido. 4. Se modifica la estructura del documento con la finalidad de ampliar los requisitos y la vigencia del documento de conformidad con los lineamientos requeridos por MINTIC. 5. Se modifica la redacción de las condiciones generales. 6. Se modifica la estructura del documento con la finalidad de ampliar los requisitos y la vigencia del documento de conformidad con los lineamientos requeridos por MINTIC. 7. Se incluye la Política de Ciberseguridad y Ciberdefensa	21/09/2022	ORALIA FRANCO GOEZ Profesional Universitario área de Sistemas SONIA CONSTANZA NEIRA Profesional Área de Sistemas KHAANKO NORBERTO RUIZ RODRIGUEZ Profesional Área de Sistemas
08	Se realiza la actualización de las áreas / dependencias y cargos mencionados en el documento con el fin de dar cumplimiento a lo establecido en el Acuerdo “Por el cual se modifica la Estructura Organizacional del INSTITUTO DISTRITAL PARA LA PROTECCIÓN DE LA NIÑEZ Y LA JUVENTUD IDIPRON, se establecen las funciones de sus dependencias y se dictan otras disposiciones”.	04/10/2022	NICOLLE CATALINA CARDENAS MARTINEZ Contratista oficina asesora de planeación

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	12 de 13
		VIGENTE DESDE	04/03/2025

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
	<p>Se realiza el ajuste de la codificación de los formatos y documentos mencionados en el manual de acuerdo con los ajustes realizados a los códigos de los documentos del Sistema Integrado de Gestión producto del rediseño institucional.</p> <p>Se realiza cambio de código del documento del A-TIC-MA-001 (código original) al código E-GTIC-MA-001 (nuevo código)</p>		
09	<p>Se realizaron las siguientes modificaciones al documento:</p> <ol style="list-style-type: none">.Se ajusta a lo largo del documento, el cambio de el “área de sistemas” por el de “Oficina de TIC”, así mismo el remplazo de “Subdirección técnica administrativa y financiera” por “Gerencia administrativa “Gestión Documental””; "Subdirección Técnica de Desarrollo Humano" por "Gerencia del Talento Humano"; Oficina Asesora jurídica por Oficina Jurídica; Subdirección Técnica de Métodos Educativos y Operativa por Subdirección Técnica Poblacional, debido al proceso de rediseño institucional en la entidad.Se realiza actualización de la tabla de contenido.Se modifica la sección de objetivos con el fin de ampliar y establecer objetivos alcanzables, específicos y controlables.Se modifica la sección de alcance, con el fin de lograr mayor claridad y alineación normativa, posicionando la política dentro de un maro más sólido y explícito.Se modifican la redacción de las condiciones generales.Se añade nueva normativa en la sección de marco normativo, con el fin de incluir decretos y resoluciones faltantes, las cuales complementan la política.Se modifica la sección de política de seguridad y privacidad de la información y seguridad digital, con el fin de poder pasar de un compromiso conceptual, a un plan de acción concreto orientado a resultados.Se modifica la sección de política de ciberseguridad y	04/03/2025	<p>YEIMMY ROCIO CARDENAS CRUZ</p> <p>Técnico Operativo Código 314 Grado 03 Oficina de TIC</p>

	GESTIÓN DE TICS	CÓDIGO	E-GTIC-MA-001
		VERSIÓN	09
	POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - SEGURIDAD DIGITAL - POLITICA - CIBERSEGURIDAD Y CIBERDEFENSA	PÁGINA	13 de 13
		VIGENTE DESDE	04/03/2025

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
	<p>ciberdefensa, con el fin de poder pasar de un compromiso conceptual, a un plan de acción concreto orientado a resultados.</p> <p>9. Se agrega el apartado los/los colaboradores(as) en la sección de roles y responsabilidades de la seguridad de la información, con el fin de garantizar el uso adecuado de los recursos tecnológicos de el IDIPRON, protegiendo la seguridad de la información y asegurando la continuidad de los servicios.</p> <p>10. Se complemento el lenguaje incluyente.</p> <p>11. Se actualiza la plantilla actual del documento.</p> <p>12. Se reorganiza el orden de la información al interior del documento y se ajusta la numeración de los títulos del documento.</p>		

14. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	SANDRA PATRICIA GUERRERO RAMÍREZ	PROFESIONAL CONTRATISTA OFICINA DE TIC - GOBIERNO DIGITAL	04/03/2025
APROBACIÓN LÍDER DE PROCESO	LUIS CARLOS OCAMPO RAMOS	JEFE DE OFICINA DE TECNOLOGÍAS DE INFORMACIÓN Y LAS COMUNICACIONES	04/03/2025