POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN - POLÍTICA SEGURIDAD DIGITAL – POLITICA DE CIBERSEGURIDAD Y CIBERDEFENSA

TABLA DE CONTENIDO

1. OBJETIVOS

1.1 GENERAL

Establecer las políticas y directrices que se requieren en el IDIPRON, con la finalidad de asegurar y garantizar la disponibilidad, confidencialidad e integridad de los activos de información en todos los procesos del IDIPRON.

1.2 ESPECIFICOS

- Establecer e implementar el Modelo de Seguridad y Privacidad de la Información (MSPI).
- Definir, implementar y divulgar la Política de Seguridad y Privacidad de la Información y la Política de Seguridad Digital.
- Definir los roles y responsabilidades de Seguridad de la Información.
- Crear el Plan de Seguridad y Privacidad de la Información

2. ALCANCE

La presente política determina los lineamientos de obligatorio cumplimiento para todos los procesos del IDIPRON los cuales se crean dentro del marco legal y normativo que regula al Instituto, con la finalidad de establecer directrices para el adecuado uso, administración de los activos de información, seguimiento periódico y actualización de la Política. Así mismo determinar los instrumentos requeridos para evitar la materialización de los riesgos identificados con la finalidad de disminuir la probabilidad de ocurrencia de una amenaza en los activos de información y los datos del Instituto.

3. DEFINICIONES

TÉRMINO	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, 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 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

4. MARCO NORMATIVO

Las normas para considerar en lo referente al Instituto Distrital para la Protección de la Niñez y la Juventud, el Sistema Distrital de Información y a 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 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 rsonales”.
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 338 de 8 de Marzo de 2022	“Por el cual se adiciona el Titulo 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. Digital coma se crea el modelo y las instancias de gobernanza, de seguridad digital y se dictan otras disposiciones”
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”.
Norma Técnica Colombiana NTC-ISO-IEC-27001 Instituto Colombiano de Normas Técnicas y Certificación.	Sistema de Gestión de la Seguridad de la Información.

5. CONDICIONES GENERALES

El Área de Sistemas realizará el seguimiento y cumplimiento del Modelo de Seguridad y Privacidad de la Información aprobado por la Alta Dirección.

El equipo de trabajo de la Oficina Asesora de Planeación, el Área de Sistemas y el Área de 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.

El Área de Sistemas 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.

El Área de Sistemas definirá la declaración de aplicabilidad e implementará los controles de acuerdo al Anexo A de la NTC- ISO/IEC – 27001.

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 tenida en cuenta para el reporte de incidentes ante CSIRT o COLCERT.

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 funcionarios contratistas colaboradores y proveedores del IDIPRON sin importar su modo de vinculación

7. DECLARACION DE LA POLITICA DE CIBERSEGURIDAD Y CIBERDEFENSA

Con el fin de garantizar la ciberseguridad y ciberdefensa El IDIPRON, como responsable de la Política de Ciberseguridad y Ciberdefensa, se compromete a disponer de los recursos necesarios que permitan el seguimiento y control para la conservación de la información en su criterio de disponibilidad, confidencialidad e integridad, realizando las actividades que sean necesarias de acuerdo con lo establecido en la normatividad vigente. Esta política es de obligatorio cumplimiento para todos los funcionarios contratistas colaboradores y proveedores del IDIPRON sin importar su modo de vinculación

8. MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El IDIPRON deberá implementar y hacer seguimiento periódico del Sistema de Gestión de Seguridad de la Información en concordancia con la Norma Técnica NTC-ISO/IEC 27000 y la GTC-ISO/IEC 27003, con la finalidad conservar la información y los datos de manera integral, auténtica, fiable y disponible; así mismo mantener actualizado y controlado los activos de información físicos y digitales que posee en Instituto, con el fin de contar con una gestión adecuada en el manejo de riesgos y continuidad de la operación de la Entidad.

El desarrollo de cada una de sus fases permitirá y adoptará el Modelo de Seguridad y Privacidad de la Información establecido por el MINTIC, dando cumplimiento a las fases y ciclo de desarrollo del MSPI.

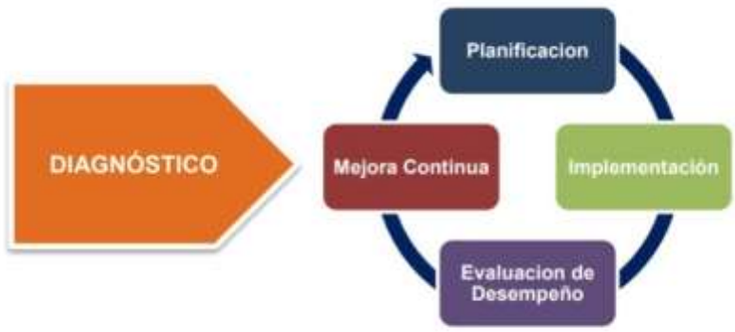

Figura No. 1. Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información

DIAGNOSTICO

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.

PLANEACION

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.

IMPLEMENTACION

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.

EVALUACION 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.

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

El Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, a través de la implementación del Modelo de Seguridad y Privacidad de la Información, enmarcado dentro del Sistema de Gestión de Seguridad de la información, realizara supervisión a protección y preservación de la información del Instituto, en cuanto a confidencialidad, integridad, disponibilidad, autenticidad y no repudio, mediante una adecuada identificación de los activos de información, un programa que garantiza la gestión de riesgos, la implementación y monitoreo permanente de controles físicos y digitales, con la finalidad de prevenir incidentes en los activos de Información del Instituto, con el objetivo primordial de cumplir con calidad al desarrollo de su misión, facilitando el acceso de la información, a los beneficiarios, grupos de interés, funcionarios y partes interesadas.

10. POLITICA DE CIBERSEGURIDAD Y CIBERDEFENSA

El Instituto Distrital para la Protección de la Niñez y la Juventud – IDIPRON, a través de la Política de Ciberseguridad y Ciberdefensa, realizará veeduría a la protección y preservación de la información del Instituto con el fin de minimizar el nivel de riesgo cibernético al que están expuesta nuestra Entidad en el área de protección a la información y propiedad intelectual con el fin de prevenir y contrarrestar cualquier incidente o amenaza cibernética que afecte el instituto. Recordemos que el uso de la internet también es con fines terroristas, actos de espionaje y guerra cibernética ya que la internet y las TIC se vuelven cada vez más esenciales para el desarrollo social y económico. Así mismo, crece la importancia por infraestructura de TIC y las amenazas cibernéticas evolucionan a un ritmo acelerado, de acuerdo con un informe de la Organización para la Cooperación y el Desarrollo Económicos (OCDE), por ende debemos tener una adecuada identificación de los activos de información, un programa que garantiza la gestión de riesgos, la implementación y monitoreo permanente de controles físicos y digitales, con la finalidad de prevenir incidentes en los activos de Información del Instituto, con el objetivo primordial de cumplir con calidad al desarrollo de su misión, facilitando el acceso de la información, a los beneficiarios, grupos de interés, funcionarios y partes interesadas.

Se deben establecer todas aquellas medidas organizativas, técnicas, físicas y legales destinadas a la identificación, protección, detección, respuesta y recuperación de los ciber activos críticos de tal forma que se logre el cumplimento de las leyes, reglamentos y regulación vigente que sean aplicables al IDIPRON, contra el acceso no autorizado, divulgación, duplicación, interrupción de la operación, modificación, destrucción, pérdida, robo, o mal uso, que se pueda producir en forma intencional o accidental, buscando garantizar la confiabilidad, confidencialidad, integridad y disponibilidad de las tecnologías de operación, para asegurar la sostenibilidad y seguridad de los negocios. A través de esta política se difunden los objetivos de ciberseguridad del IDIPRON, que se consiguen con la aplicación de controles de ciberseguridad, para gestionar un nivel de ciber riesgo aceptable. Sistemas es el responsable de realizar las acciones de sensibilización, comunicación, entrenamiento y socialización de la política de ciberseguridad y de los procesos de seguridad cibernética donde se incluyan como mínimo los siguientes objetivos:

- Identificación y documentación de la situación actual.
- Establecimiento de procedimientos de seguridad cibernética.
- Diseño de arquitecturas de seguridad aplicable a los ciber activos.
- Definición e implantación de controles legales, técnicos, organizativos y físicos.
- Implementación de un ciclo de mejora continua de la gestión de ciberseguridad.

Debemos tener en cuenta que la información y los sistemas asociados son activos críticos que deben ser protegidos para asegurar el correcto funcionamiento de la entidad. La Política de Ciberseguridad está orientada a gestionar eficazmente la seguridad de la información tratada por los sistemas informáticos de la empresa, así como los activos que participan en sus procesos. Reitero que esta Política tiene como objetivo garantizar la

confidencialidad, integridad, disponibilidad y privacidad de la información, y cumplir con las Leyes y Reglamentaciones vigentes en cada momento, manteniendo un equilibrio entre los niveles de riesgo y un uso eficiente de los recursos, con criterios de proporcionalidad. Esta política de ciberseguridad se aplica a todos los empleados, contratistas, directivos y administradores que integran el IDIPRON, incluyendo aquellas sociedades participadas sobre las que tenga un control efectivo, dentro de los límites previstos en la normativa aplicable.

11. ROLES Y RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN

Áreas 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.
Área de Sistemas	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.
Subdirección Técnica Administrativa y Financiera	Dirigir, orientar y hacer seguimiento de la Implementación del Modelo de Seguridad y Privacidad de la información.
Subdirección Técnica de Desarrollo Humano	Desarrollar junto a la Subdirección Técnica Administrativa y Financiera y el Área de Sistemas, 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 áreas involucradas. Revisar y validar las Políticas de Seguridad de la Información.
Oficina Asesora Jurídica	Identificar y asesorar en la legislación aplicable al cumplimiento de la Seguridad de la Información.
Subdirección de Métodos Educativos y Operativa	Sugerir, retroalimentar y dar cumplimiento de las Políticas de Seguridad en las Áreas misionales del IDIPRON.
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.

12. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Tema	Acciones a ejecutar	Tareas a realizar	Responsable	Programación de tareas			
				AÑO 2020	AÑO 2021	AÑO 2022	AÑO 2023
Activos de Información	Definición del Plan de Trabajo	Aprobación del documento Política de Seguridad y Privacidad de la Información.	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
		Definir el grupo de trabajo para el levantamiento de los activos de información.	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
	Levantamiento e identificación de los activos de información	Definir la metodología y el alcance para identificar los activos de información.	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
		Socializar y aplicar la guía para el levantamiento de los activos de Información.	Área de Sistemas				
		Realizar el levantamiento de los activos de información en el formato "ACTIVOS DE	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				

		INFORMACIÓN A-TIC-FT-007"., en cada dependencia					
	Publicación de los activos de información	Publicar en el sitio Web los activos de información según la Ley 1712 de 2014	Subdirección Técnica Administrativa y Financiera / Área de Sistemas /Área de Administración Documental y Área de Comunicaciones				
Gestión de Riesgos	Lineamientos para la valoración de riesgos	Establecimiento de la Metodología y el instrumento para la Valoración de Riesgo	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
	Valoración de riesgos	Identificación, análisis, y evaluación de riesgos.	Área de Sistemas / Responsable de cada proceso				
		Resultado de la valoración del Riesgo	Subdirección Técnica Administrativa y Financiera / Área de Sistemas /Área de Administración Documental y Oficina Asesora de Planeación / Oficina de Control Interno				
		Retroalimentación, verificación y ajustes de la valoración de riesgos.	Subdirección Técnica Administrativa y Financiera / Área de Sistemas /Área de Administración Documental y Oficina Asesora de Planeación / Oficina de Control Interno				
	Aceptación de Riesgos	Aceptación y aprobación de los riesgos identificados	Subdirección Técnica Administrativa y Financiera / Área de Sistemas /Área de Administración Documental				
	Plan de tratamiento y publicación	Plan de tratamiento de riesgos	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
		Publicación de la matriz de riesgos	Subdirección Técnica Administrativa y Financiera / Área de Comunicaciones				
	Evaluación de los riesgos residuales	Verificación y evaluación de los riesgos residuales	Subdirección Técnica Administrativa y Financiera / Área de Sistemas /Área de Administración Documental				
	Realizar y aprobar la Declaración de Aplicabilidad - SoA	Realizar la Declaración de Aplicabilidad	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
Gestión de incidentes	Mejoramiento continuo	Identificación de oportunidades de mejora acorde a los resultados obtenidos en evaluación de los riesgos residuales.	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Área de Administración Documental				
	Monitoreo y revisión de indicadores	Realización y monitoreo de indicadores de Riesgos de MSPI	Área de Sistemas				
	Elaboración de instrumento para la gestión de incidentes de Seguridad de la Información	Elaboración del procedimiento de gestión de incidentes	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
	Aprobación del Procedimiento de Gestión de Incidentes	Aprobación y publicación del procedimiento gestión de incidentes	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
	Publicación y Socialización del procedimiento de gestión de incidentes	Socialización del procedimiento a los funcionarios del Área de Sistemas	Área de Sistemas				
		Socialización del procedimiento a los funcionarios de las dependencias del IDIPRON	Área de Sistemas				
	Gestionar Incidentes de Seguridad de la Información	Gestionar los incidentes de seguridad de la información	Subdirección Técnica Administrativa y Financiera / Área de Sistemas				
	Gestionar incidentes al equipo de respuesta ante Emergencias Informáticas - CSIRT	Socializar los boletines informativos generados por CSIRT	Área de Sistemas				
Plan de Continuidad del Negocio	Planificación de la Continuidad del Negocio	Definir los requisitos de la continuidad de la operación	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Implementar la continuidad de la operación	Realizar los documentos, proceso y procedimientos para implementar la continuidad de la operación	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Fase: Análisis de Impacto - BIA	Documentación del Análisis de Impacto – BIA	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
		Ejecución del Análisis de Impacto - BIA	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
		Cálculos de MTPD, RTO, RPO	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
		Identificación y priorización de procesos críticos	Área de Sistemas / Responsable de cada proceso				
	Fase: Análisis y valoración de riesgos de interrupción	Identificación activos, análisis y valoración de riesgos de interrupción	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
		Publicación valoración de riesgos de interrupción	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Fase: Planes de continuidad documentados	Definición de escenarios de desastres	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
		diseño y documentación: Planes de continuidad - gestión de incidentes y planes de respuesta y recuperación	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Fase: Plan de Pruebas de continuidad	Pruebas, análisis de conclusiones y revisión de los planes documentados	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Fase Crisis	Gestión de incidente, activación de planes, análisis de conclusiones y revisión de los planes de Gestión de Crisis	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				

	Gestión de incidentes, no conformidades y acciones correctivas y preventivas	Registro, seguimiento y trazabilidad	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				
	Cuadro de mando	Gestión de indicadores, catálogo de indicadores métricas	Subdirección Técnica Administrativa y Financiera / Área de Sistemas / Equipo Continuidad del Negocio				

13. SEGUIMIENTO Y EVALAUCIÓN DE LA POLITICA

El IDIPRON realiza el seguimiento de la política a través del cumplimiento definido en su Plan de Seguridad y Privacidad de la Información, en las actividades definidas en el Plan de acción así como seguimiento de mejora continua y actividades de control de la Oficina de Control Interno de la Entidad.

14. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN DE CAMBIOS	FECHA (DD/MM/AAAA)	ELABORÓ
01	Se dio inicio a 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 maestro	29/07/2011	**JOSÉ VICENTE CASTRO ORDÓÑEZ** Profesional Universitario área de Sistemas
03	Se ajustó la Política y el Manual de acuerdo a 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 a 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	21/09/2022	**ORALIA FRANCO GOEZ** Profesional Universitario área de Sistemas **SONIA CONSTANZA NEIRA** Profesional Área de Sistemas **JONNY HIRLAN TORRES RUBIANO**

	del documento de conformidad con los lineamientos requeridos por MINTIC. 5. 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. 6. Se incluye la Política de Ciberseguridad y Ciberdefensa		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" 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. Se realiza cambio de código del documento del A-TIC-MA-001 (código original) al código E-GTIC-MA-001 (nuevo código)	04/10/2022	**NICOLLE CATALINA CARDENAS MARTINEZ** CONTRATISTA OFICINA ASESORA DE PLANEACIÓN

15. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA (DD/MM/AAAA)
REVISÓ	VIVIANA ANDREA SANCHEZ MORALES	PROFESIONAL ESPECIALIZADO CONTRATISTA	04/10/2022
APROBACIÓN LÍDER DE PROCESO	FABIAN ANDRES CORREA ALVAREZ	JEFE DE LA OFICINA ASESORA DE PLANEACIÓN	04/10/2022

RESOLUCIÓN No. 639 DE 2020

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, la Política de Tratamiento de Datos Personales, el Plan Estratégico de Tecnologías de la Información – PETI y se adopta la Política de Seguridad Digital, el Plan de Seguridad y Privacidad de la Información y se derogan las Resoluciones 435 de 2013 y 282 de 2015"

El Director General de entidad descentralizada Código 050 Grado 03, del Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON, en uso de sus facultades legales conferidas mediante el Artículo 7 del Acuerdo 80 de 1967 y el Artículo 59 del Decreto Ley 1421 de 1993

CONSIDERANDO

Que la Constitución Política de Colombia en su artículo 15, consagra que todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas.

Que el artículo 17 de la Ley Estatutaria 1581 de 2012, "Por medio de la cual se dictan disposiciones generales para la protección de datos personales", y el artículo 2.2.2.25.3.1. del Decreto 1074 de 2015, "Decreto Único Reglamentario del Sector Comercio Industria y Turismo", consagraron la necesidad de garantizar de forma integral la protección y el ejercicio del derecho fundamental de Habeas Data y estableció dentro de los deberes de los responsables del tratamiento de datos personales, desarrollar políticas para este derecho.

Que la Ley 1712 de 2014, "Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones", adiciona nuevos principios, conceptos y procedimientos para el ejercicio y garantía del referido derecho; junto con lo dispuesto en el Libro 2. Parte VIII, Título IV "Gestión de la Información Clasificada y Reservada" del Decreto 1080 de 2015, "por medio del cual se expide el Decreto Reglamentario Único del Sector Cultura", el cual establece las directrices para la calificación de información pública, en el mismo sentido, el Título V de la misma Parte y Libro, establecen los instrumentos de la gestión de información pública (1) Registro de Activos de Información; (2) Índice de Información Clasificada y Reservada; (3) Esquema de Publicación de Información; (4) Programa de Gestión Documental.

Que el artículo 2.2.9.1.1.3. del Decreto 1078 de 2015, subrogado por el artículo 1 del Decreto 1008 de 2018, determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través de este se busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Que igualmente, el artículo 1 del Decreto 1499 de 2017 sustituyo el Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015. El nuevo artículo 2.2.22.1.1 del Decreto 1083 de 2015, señala que el Sistema de Gestión, que integra los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad, es el conjunto de entidades y organismos del Estado, políticas, normas, recursos e información, cuyo objeto es dirigir la gestión pública al mejor desempeño institucional y a la consecución de resultados para la satisfacción de las necesidades y el goce efectivo de los derechos de los ciudadanos, en el marco de la legalidad y la integridad.

Que el artículo 2.2.22.2. del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de "11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital"

Que el Documento CONPES 3854 del 11 de abril de 2016, establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Que en el artículo 2.2.22.3.2. del Decreto 1499 de 2017 se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

Que de conformidad con lo establecido en el Decreto 1499 de 2017, el Comité Institucional de Gestión y Desempeño, debe incluir todos los temas que atiendan la implementación y desarrollo de las políticas de gestión definidas en el MIPG

Que el Comité Institucional de Gestión y Desempeño mediante acta de fecha 30 de diciembre de 2020 aprobó la actualización de la Política de Seguridad y Privacidad de la Información, Política de Tratamiento de Datos Personales, el Plan Estratégico de Tecnologías de la Información– PETI, aprobó la Política de Seguridad Digital y el Plan de Seguridad y Privacidad de la Información.

Que por otra parte se hace necesario derogar las Resoluciones 435 de 2013 y 282 de 2015.

En mérito de lo expuesto,

R E S U E L V E:

ARTÍCULO PRIMERO: Actualizar la Política de Seguridad y Privacidad de la Información, así como la definición de los roles y responsabilidades de la información.

ARTÍCULO SEGUNDO: Actualizar la Política de Tratamiento de Datos Personales, así como el establecimiento de las finalidades del tratamiento de datos y la protección de los datos de los denunciantes de posibles actos de corrupción.

ARTÍCULO TERCERO: Actualizar el Plan Estratégico de Tecnologías de la Información - PETI, para el cuatrienio 2020 – 2024 de acuerdo con la Plataforma Estratégica de la Entidad y el Plan de Desarrollo "UN NUEVO CONTRATO SOCIAL Y AMBIENTAL PARA LA BOGOTÁ DEL SIGLO XXI"

ARTÍCULO CUARTO: Adoptar la Política de Seguridad Digital en el marco del desarrollo de las Políticas de Gestión y Desempeño Institucional.

ARTÍCULO QUINTO: Adoptar el Plan de Seguridad y Privacidad de la Información, el cual define la ruta para el desarrollo del Modelo de Seguridad y Privacidad de la Información – MSPI, así como el cumplimiento de la implementación el Modelo de Seguridad y Privacidad de la Información.

"Por la cual se actualiza la Política General de Seguridad y Privacidad de la Información, la Política de Tratamiento de Datos Personales, el Plan Estratégico de Tecnología de la Información – PETI y se adopta la Política de Seguridad Digital, el Plan de Seguridad y Privacidad de la Información y se derogan las Resoluciones 435 de 2013 y 282 de 2015"

ARTÍCULO SEXTO: Las políticas y planes adoptados mediante la presente resolución serán actualizados en el momento que se requiera, para lo cual se procederá a realizar el procedimiento definido por la oficina asesora de planeación y los formatos establecidos para tal fin.

ARTÍCULO SEPTIMO: La presente Resolución rige a partir de su fecha de su publicación y deroga las Resoluciones 435 de 2013 y 282 de 2015 y todas aquellas disposiciones que le sean contrarias.

PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D. C., a los 31 días del mes de diciembre de 2020.

CARLOS ENRIQUE MARIN CALA
Director General de entidad descentralizada

Proyectó: Oralia Franco Gomez - Contratista -CPS
Revisó: Juan Gabriel Pérez Tobaría – Contratista CPS
Revisó: Manuel Ricardo Montenegro Zamora – Abogado Oficina Asesora Jurídica
Revisó y Aprobó: Luz Miriam Botero Serna – Jefe Oficina Asesora Juridica