	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	1 de 13
		VIGENTE DESDE	25/11/2024



**PLAN DE TRATAMIENTO DE RIESGOS
DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN
AÑO 2024 -2028**



	GESTION TECNOLÓGICA Y DE LA INFORMACION	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	2 de 13
		VIGENTE DESDE	25/11/2024

TABLA DE CONTENIDO

1.	INTRODUCCIÓN	3
2.	OBJETIVO	4
3.	ALCANCE.....	4
4.	CONDICIONES GENERALES.....	4
5.	NORMATIVIDAD	5
6.	GLOSARIO.....	6
7.	PLAN DE TRATAMIENTO DE RIESGOS	7
	7.1. Factores de riesgo	7
	7.2 Valoración del riesgo	7
	7.2.1. Guía para la administración de riesgos.....	8
	7.3 Estrategia de tratamiento de riesgos	8
8.	ESTRATEGIA DE CONTROL DE RIESGOS 2024-2028	9
	8.1. Estrategias orientadas al conocimiento	9
	8.2. Estrategias orientadas al control de acceso.....	10
	8.3. Estrategias de fortalecimiento de controles técnicos.....	10
9.	RECURSOS	10
10.	MEDICIÓN	11
	10.1. Criterios de clasificación	12
	10.2. Niveles de clasificación	12
11.	BIBLIOGRAFIA.....	12
12.	CONTROL DE CAMBIOS	13
13.	REVISIÓN Y APROBACIÓN	13

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	3 de 13
		VIGENTE DESDE	25/11/2024


1. INTRODUCCIÓN

El Instituto Distrital para la Protección de la Niñez y la Juventud -IDIPRON, presenta a los grupos de interés, y a la ciudadanía en general, el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la vigencia 2024-2028, donde se establece un conjunto de actividades basadas en el ciclo PHVA (Planificar- Hacer-Verificar-Actuar), para crear condiciones de uso confiable en el entorno digital y físico de la información, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad, privacidad y disponibilidad de la información de la entidad para mitigar las posibles afectaciones a los activos críticos que presenten riesgos de seguridad de la información.

El análisis de riesgos de los activos de información nos permite entender de una manera efectiva y eficiente los riesgos de pérdida de confidencialidad, integridad, privacidad y disponibilidad sobre cada uno de los activos definidos como parte del alcance del análisis. Los escenarios de riesgo presentes en nuestra época obligan a que las entidades como el IDIPRON, cuenten con un proceso integral de gestión de riesgos orientado a darle la confianza necesaria a la ciudadanía, para contar con instituciones seguras, confiables y que estas tienen resiliencia frente a los diferentes factores externos causantes de inestabilidad política, afectación de la información y conflictos sociales.

Mediante la definición del Plan de Tratamiento de Riesgos, el Instituto Distrital Para la Protección de la Niñez y la Juventud -IDIPRON busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad, Pérdida de Integridad y Pérdida de Disponibilidad), en la información digital, evitando aquellas situaciones que impidan el logro de los objetivos Estratégicos del IDIPRON. El Plan de Tratamiento de Riesgo se define con el fin de evaluar las posibles acciones que se deben tomar para mitigar los riesgos existentes en los activos de información de la entidad, estas acciones son organizadas en forma de medidas de seguridad denominados controles, y para cada una de ellas se define el nombre de la medida, objetivo, justificación, responsable de la medida y su prioridad.

Las anteriores medidas se definen teniendo en cuenta la información del análisis de riesgos, sobre la plataforma informática y las necesidades del Proceso de Gestión de la Infraestructura de TIC de la entidad, en cuanto a la seguridad de la información y proporciona las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	4 de 13
		VIGENTE DESDE	25/11/2024

2. OBJETIVO

Determinar las acciones relacionadas con el tratamiento de riesgos de seguridad y privacidad de la información, mediante la identificación, análisis, valoración y tratamiento de los riesgos de pérdida de confidencialidad, disponibilidad e integridad de la información, así como la protección de la privacidad para prevenir su materialización y/o reducir los impactos negativos en la gestión institucional. Para lo cual se realizará seguimiento según el alcance de este documento.

3. ALCANCE


El presente documento tiene como finalidad, realizar una efectiva gestión de riesgos de seguridad y privacidad de la información, seguridad digital y continuidad de la operación de los servicios (riesgos de interrupción), de la Oficina de Tecnología de las Comunicaciones TIC; que permitan las buenas prácticas, contribuyendo así a la toma de decisiones y de esta manera prevenir incidentes que puedan afectar el cumplimiento del logro de los objetivos, así como dar a conocer los lineamientos, roles y responsabilidades, que permitan identificar, analizar evaluar y monitorear los riesgos de seguridad y privacidad de la información de la Oficina de Tecnologías de la Información y las Comunicaciones TIC-IDIPRON.

El plan de tratamiento de riesgos tendrá en cuenta aquellos riesgos que se encuentran en el nivel Alto y extremo, teniendo en cuenta los lineamientos establecidos por el Ministerio de TIC y DAFP.

Inicia con el diligenciamiento de la matriz de identificación de riesgos y finaliza con la formulación de controles para mitigar el impacto o probabilidad de materialización del riesgo con el análisis de los riesgos identificados.

Este tendrá seguimiento mediante el cronograma establecido por el procedimiento **MANUAL PARA LA ADMINISTRACION DE LOS RIESGOS E-DES-MA-003** en el literal 7.4.5 “Monitoreo, seguimiento y evaluación de la gestión del riesgo”.

4. CONDICIONES GENERALES

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	5 de 13
		VIGENTE DESDE	25/11/2024


Desde la Oficina de TICS, se propone, la matriz de riesgos de seguridad de la información; con la finalidad de que los/las responsables de los procesos, Líderes de Oficina, y gerentes, diligencien la matriz y ubiquen los activos de mayor valor para identificar controles, con el fin de mitigar la materialización de riesgos de seguridad de la información.

Es un deber de los/las responsables de los procesos, líderes de oficina y gerentes, como primera línea de defensa, diligenciar la matriz e identificar los controles y riesgos inherentes y residuales para el tratamiento de los riesgos de seguridad de la información.

5. NORMATIVIDAD

El plan de tratamiento de riesgos en Colombia se encuentra establecido en el siguiente marco normativo:

NORMA	FECHA	DESCRIPCION
Decreto 612 de 2018	2018	Artículo 1. Adicionar al Capítulo 3 del Título 22 de la Parte 2 del Libro 2 del Decreto 1083 de 2015, Único Reglamentario del Sector de Función Pública, los siguientes artículos:
Decreto 1008	14/06/2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital.
CONPES 3995	2020	Por medio del cual se establecen los lineamientos de política nacional de confianza y seguridad digital.
Resolución 500	2021	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 1494	2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 2573	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.


	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	6 de 13
		VIGENTE DESDE	25/11/2024

NORMA	FECHA	DESCRIPCION
Decreto 1377 de 2013	2013	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 338 de 2022	2022	Por medio del cual se establecen lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el modelo y las instancias de Gobernanza de seguridad Digital y se dictan otras disposiciones.
Ley estatutaria 1581 de 2012.	2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley 1474 de 2011	2011	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República.
Norma técnica colombiana NTC - ISO/IEC 27001	2013	Estándar para la seguridad de la información, describe cómo gestionar la seguridad de la información en una empresa
Manual Para la Administración de los riesgos E-DES-MA-003	2023	Lineamiento riesgos de seguridad de la información

Fuente: Creación Propia Oficina TICS

6. GLOSARIO

TERMINOS	DEFINICIÓN
Amenaza	Es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la Institución logrando con ello materializar el riesgo.
Control o medida	Se define como las acciones que permiten reducir o mitigar el riesgo.
Impacto	Consecuencias que puede ocasionar a la organización la materialización del riesgo.

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	7 de 13
		VIGENTE DESDE	25/11/2024

TERMINOS	DEFINICIÓN
Probabilidad	Se define como la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.
Riesgo	Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales
Riesgo de Seguridad de la Información	Posibilidad de que una amenaza concreta pueda materializarse, una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000)
TICS	Tecnologías de la Información y Comunicaciones.
Vulnerabilidad	Es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

Fuente: Creación Propia Oficina TICS


7. PLAN DE TRATAMIENTO DE RIESGOS

7.1. Factores de riesgo

Para la vigencia 2024-2028 se priorizan los siguientes factores de riesgo digital en nuestro plan de tratamiento de riesgos:

- Nivel de conocimiento del personal en amenazas digitales, políticas y controles de seguridad.
- Disponibilidad permanente de servicios esenciales como telecomunicaciones, energía e infraestructura.
- Identificación y protección de los datos de carácter personal.
- Adecuada clasificación de la información bajo custodia de la Oficina de Tecnología de las Comunicaciones TIC de acuerdo con el marco legal vigente.
- Entorno global digital inseguro.
- Asignación apropiada de roles y privilegios en todos los sistemas de información.

7.2 Valoración del riesgo

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	8 de 13
		VIGENTE DESDE	25/11/2024

El análisis del riesgo busca establecer la probabilidad de ocurrencia de los riesgos y el impacto de sus consecuencias, calificándolos y valorándolos con el fin de obtener información para establecer el nivel de riesgo y las posibles acciones preventivas y correctivas a implementar.

Para el análisis de los riesgos se incluyen las fuentes, así como los factores que generan las consecuencias y aumentan la probabilidad de que ocurran. En la etapa de análisis se identifican los controles existentes ya sea de carácter administrativos, técnicos y/o procedimientos implementados en la Oficina de Tecnología de las Comunicaciones TIC. Por lo tanto, se hace necesario analizar el riesgo combinando con las estimaciones de impacto y probabilidades en el contexto de las medidas de control existente.

La aplicación de análisis cualitativo facilita la calificación y evaluación de los riesgos al aplicar formas descriptivas para presentar la magnitud de las consecuencias potenciales (consecuencia) y la posibilidad de ocurrencia (probabilidad). La siguiente tabla describe la valoración de los riesgos definidos por la Oficina de Tecnología de las Comunicaciones TIC del Instituto Distrital Para la Protección de la Niñez y la Juventud -IDIPRON.

7.2.1. Guía para la administración de riesgos


	Frecuencia de la Actividad	Probabilidad
Muy baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces al año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año.	100%

Fuente: Creación Propia Oficina TICS

7.3 Estrategia de tratamiento de riesgos

Las estrategias tendientes al tratamiento de riesgos se encuentran relacionadas con minimizar la probabilidad de ocurrencia del riesgo, para lo cual se establecen las siguientes opciones:

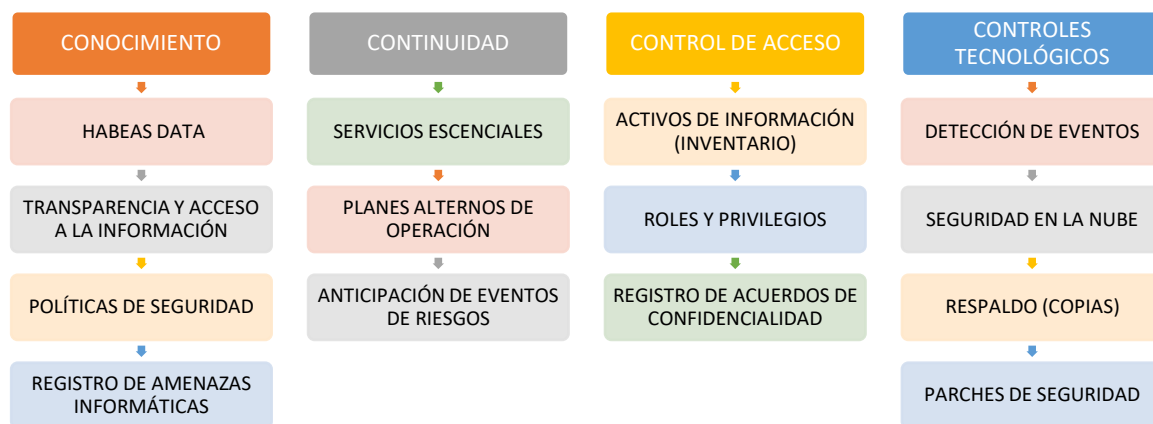
- Transferir: se encuentra relacionado con la transferencia del riesgo por medio de la

	GESTION TECNOLÓGICA Y DE LA INFORMACION	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	9 de 13
		VIGENTE DESDE	25/11/2024

asignación a la dependencia o proceso responsable.

- **Mitigar:** permite reducir la probabilidad de ocurrencia del riesgo o reducir sus consecuencias. La probabilidad de ocurrencia de un riesgo puede reducirse a través de controles de gestión, políticas y procedimientos encaminados a reducir la materialización del riesgo.
- **Evitar:** puede evitarse el riesgo no procediendo con la actividad que incorporaría el riesgo, o escoger medios alternativos para la actividad que logren el mismo resultado y no incorporen el riesgo detectado.
- **Aceptar:** consiste en hacer frente a un riesgo (positivo o negativo) o porque no se ha identificado ninguna otra estrategia de respuesta adecuada.

8. ESTRATEGIA DE CONTROL DE RIESGOS 2024-2028




Fuente: Creación Propia Oficina TICS

8.1. Estrategias orientadas al conocimiento

Mediante el proceso de capacitación, inducción, sensibilización periódica se busca que todos los/las servidores/as, contratistas apropien conocimientos en materia de:

- Ley de protección de datos personales;
- Ley de transparencia y acceso a la información;
- Políticas institucionales de seguridad digital;
- Modalidades y control de ataques informáticos;

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	10 de 13
		VIGENTE DESDE	25/11/2024

- Uso seguro de los recursos informáticos.

8.2. Estrategias orientadas al control de acceso

Con el ánimo de prevenir y controlar el acceso no autorizado a activos de información clasificados y reservados, la Oficina de Tecnología de las Comunicaciones TIC emprenderá en la vigencia 2024 -2028 acciones específicas para:

- Actualizar los instrumentos de acceso a la información pública;
- Reforzar los controles de acceso a activos de información con roles y privilegios más precisos;
- Reforzar el cumplimiento de los acuerdos de confidencialidad y los acuerdos de intercambio seguro de información.

8.3. Estrategias de fortalecimiento de controles técnicos


Ante el aumento inminente del tipo y complejidad de amenazas informáticas en la Oficina de Tecnología de las Comunicaciones TIC implementará estrategias específicas en:

- Identificación de eventos potencialmente nocivos;
- Reforzamiento de controles de acceso a servicios en la nube;
- Verificación y control de copias de respaldo;
- Control de cambios en plataformas tecnológicas;
- Aplicación de parches de seguridad y actualización de equipos de procesamiento de datos.

9. RECURSOS

La Oficina de Tecnología de las Comunicaciones TIC/Instituto Distrital Para la Protección de la Niñez y la Juventud IDIPRON, en el marco de la Gestión de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la Operación de los Servicios (riesgos de interrupción) dispone de los siguientes recursos para su operación:

Vr. 09; 13/03/2024

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	11 de 13
		VIGENTE DESDE	25/11/2024


RECURSOS	VARIABLES
FINANCIEROS	Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías en el GIT de Seguridad y Privacidad de la Información TIC.
HUMANOS	<ul style="list-style-type: none"> • Equipo de trabajo de seguridad y privacidad de la información. • Profesional de Riesgos de Seguridad y Privacidad de la Información. • Líder de proceso TIC
LOGÍSTICOS	Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos de la Oficina de Tecnología de las Comunicaciones TIC.
TÉCNICOS	<p>Guía para la administración del riesgo y el diseño de controles en entidades públicas – Riesgos de gestión, corrupción y seguridad digital del DAFP.</p> <p>Manual para la Administración de los Riesgos E-DES-MA-003.</p> <p>Mapa de riesgos de Seguridad de la Información</p>

Fuente: Creación Propia Oficina TICS

10. MEDICIÓN

El proceso de medición y seguimiento, de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) de la Oficina de Tecnología de las Comunicaciones TIC/Instituto Distrital Para la Protección de la Niñez y la Juventud – IDIPRON, aprobados por la Oficina TIC, así como de sus controles y planes de tratamiento, se realiza por parte del equipo del Grupo Interno de Trabajo de la oficina de las TIC, teniendo en cuenta la periodicidad y fechas de cumplimiento establecidas, validando los resultados de los seguimientos realizados así como el cargue de los soportes correspondientes a los controles definidos.

Una vez la Oficina de Tecnología de las Comunicaciones TIC realice el reporte de cumplimiento de sus planes de tratamiento y controles, los/las profesionales de la Oficina de

	GESTION TECNOLÓGICA Y DE LA INFORMACION	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	12 de 13
		VIGENTE DESDE	25/11/2024

Seguridad y Privacidad de la Información realizarán la revisión y validación de esta información, con el fin de reportar la medición de la gestión del riesgo a través de la matriz que tiene como propósito medir el nivel de implementación de los controles de los riesgos de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de la operación de los Servicios (riesgos de interrupción) de la Oficina de Tecnología de las Comunicaciones TIC/Instituto Distrital para la Protección de la Niñez y la Juventud IDIPRON.

La medición se realizará según lo establecido en el Manual para la Administración de Riesgos E-DES-MA-003 y el mapa de riesgos de Seguridad de la Información, en cual se podrá determinar el porcentaje de ejecución de los controles definidos para mitigar los riesgos identificados en los sistemas de gestión de TIC.

10.1. Criterios de clasificación

CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (1)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (2)
INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (3)
NO CLASIFICADA	NO CLASIFICADA	NO CLASIFICADA


Fuente: Creación Propia Oficina TICS

10.2. Niveles de clasificación

ALTA	Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.
MEDIA	Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Fuente: Creación Propia Oficina TICS

11. BIBLIOGRAFIA

	GESTION TECNOLÓGICA Y DE LA INFORMACIÓN	CÓDIGO	E-GTIC-MA-007
		VERSIÓN	01
	PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN	PÁGINA	13 de 13
		VIGENTE DESDE	25/11/2024

https://www.mintic.gov.co/gestionti/615/articles5482_G7_Gestion_Riesgos.pdf

Guía de gestión de riesgos, seguridad y privacidad de la Información – MinTIC

https://www1.funcionpublica.gov.co/documents/28587410/34299967/Guia_administracion_riesgos_capitulo_riesgo_fiscal.pdf

12. CONTROL DE CAMBIOS

VERSIÓN	DESCRIPCION DE CAMBIOS	FECHA	ELABORÓ
01	Se crea el Plan de Tratamiento de Riesgos el cual define las medidas de seguridad y privacidad de la información necesarias en el Instituto Distrital Para la Protección de la Niñez y la Juventud IDIPRON/Oficina de TICS para la Vigencia 2024-2028, según lo establecido en el decreto 612 de 2018 y en el Decreto 500 de 2020 Por medio del 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.	25/11/2024	YEIMMY ROCIO CARDENAS CRUZ Técnico Operativo Código 314 Grado 03 (E)

13. REVISIÓN Y APROBACIÓN

	NOMBRE	CARGO	FECHA
REVISÓ	NORBERTO RUIZ RODRIGUEZ	PROFESIONAL ESPECIALIZADO CONTRATISTA TIC	25/11/2024
APROBÓ	LUIS CARLOS OCAMPO RAMOS	JEFE OFICINA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES	25/11/2024