Firma de Autorizaciones		
Elaboró	**Revisó**	**Aprobó**
Maria Alejandra Suarez	Lira Pineda	Comité Institucional de Gestión y Desempeño
Control de Cambios		
Fecha	**Descripción**	
28/06/2024	Se alinea el plan a la estructura documental de la entidad, estableciendo actividades mediables y ejecutables para la vigencia 2024	

TABLA DE CONTENIDO

1 OBJETIVO

Gestionar de manera efectiva y proactiva los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de la información en el IDEP.

2. ALCANCE

El alcance de este plan de tratamiento de riesgos de seguridad de la información incluye la identificación, análisis valoración y definición de controles de los riesgos que puedan afectar la confidencialidad, integridad y disponibilidad de los activos de información del IDEP.

3. REFERENCIAS NORMATIVAS

Normatividad	Entidad	Descripción
Acuerdo 002 de 2023	Comisión Distrital de Transformación Digital	Por la cual se adopta el lineamiento para el desarrollo de evaluaciones de impacto a la privacidad.
Resolución 500 de 2021	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.
Decreto 620 de 2020	Ministerio de Tecnologías de la información y las comunicaciones - MINTIC	Establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Directiva 002 de 2020	Presidencia de la Republica	Medidas para atender la contingencia generada por el covid-19, a partir uso de las tecnologías la información y las telecomunicaciones - TIC
CONPES 3995 de 2020.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política Nacional de Confianza y Seguridad Digital.
Decreto 612 de 2018	Presidencia de la Republica	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado
CONPES 3854 de 2016.	Consejo Nacional de Política Económica y Social República de Colombia Departamento Nacional de Planeación	Política de Seguridad Digital del Estado Colombiano

4. DOCUMENTOS ASOCIADOS

- Política de Seguridad y Privacidad de la Información
- Plan Estratégico de Tecnologías de la Información y las Comunicaciones

5. DEFINICIONES

- **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 (materializar el riesgo).

- **Control:** Medida que permite reducir o mitigar un riesgo

- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo

- **Probabilidad**: se entiende 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 explotar 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).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

6. DESARROLLO

En el IDEP, el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información, y Seguridad Digital se fundamenta en una orientación estratégica que promueve una cultura preventiva. Esta estrategia implica comprender el concepto de riesgo y el contexto específico, permitiendo la planificación de acciones anticipativas para mitigar los impactos adversos en caso de materialización.

Este enfoque está alineado con la normativa colombiana, como el CONPES 3995 de 2020, el Modelo de Seguridad y Privacidad de MINTIC, y el decreto 1008 de 2018. Además, adopta los estándares de la Resolución 500 de 2021, que establece directrices y estándares para la estrategia de seguridad digital y adopta el modelo de seguridad y privacidad como facilitador de la política de Gobierno Digital. Implementando buenas prácticas y lineamientos de normas como ISO 27001, ISO 31000:2018, y la guía para la administración del riesgo y diseño de controles en entidades públicas, integrados en el Modelo Integrado de Planeación y Gestión.

Para lograr esto, se ha diseñado un plan que incluye:

ESTRATEGIA	ACTIVIDAD	ENTREGABLE
Documentar estrategia	Identificar y documentar la gestión de riesgos de seguridad, alineándola con la política de gestión de riesgos institucional.	Actas de sesión O Actualización de la documentación existente en donde se relacionen los riesgos de seguridad digital
Identificación, consolidación de riesgos de seguridad de la información y seguridad digital	**Fase I** Identificar, analizar y evaluar los riesgos de aquellos activos de información tecnológicos identificados con criticidad alta	Matriz con riesgos identificados, valorados
	Establecer controles y planes de tratamiento sobre los riesgos	
Gestión de Vulnerabilidades	Gestionar vulnerabilidades relacionadas con la red institucional	Documento con las acciones realizadas
	Gestionar vulnerabilidades relacionadas con la página web institucional	
	Validar y actualizar los parches de seguridad relacionados con la infraestructura tecnológica.	

Fuente: Elaboración propia