PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2021

TC-PL-02

Oficina de Tecnologías de la Información y las Comunicaciones

12/01/2021

Versión 2

ALCALDÍA MAYOR DE BOGOTÁ D.C.

INSTITUTO DISTRITAL DE GESTIÓN DE RIESGOS Y CAMBIO CLIMÁTICO

BOGOTÁ

Control de Cambios		
Versión	Fecha	Descripción de la Modificación
1	28/12/2020	Versión inicial
2	12/01/2021	Se adhiere al documento la normatividad aplicable y se establece un cronograma

Elaboró	Revisó	Aprobó
José Alejandro Suárez Profesional Especializado Infraestructura Oficina TICS	Paula Contreras Jefe Oficina TICS	Comité Gestión y Desempeño

CONTENIDO

1. INTRODUCCIÓN

Mediante la definición del Plan de Tratamiento de Riesgos se busca mitigar los riesgos presentes en el análisis de riesgos (Pérdida de la Confidencialidad, Integridad y Disponibilidad de los activos) evitando aquellas situaciones que impidan el cumplimiento de los objetivos del Instituto Distrital de Gestión del Riesgo y Cambio Climático (IDIGER).

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, estas acciones son organizadas en forma de medias de seguridad, 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 definieron teniendo en cuenta la información del análisis de riesgos, el cual brindó información acerca de las necesidades del Proceso de Tic´s para la Gestión del Riesgo, en cuanto a la seguridad de la información y proporcionó las herramientas necesarias para definir cada una de las características de las medidas y la definición de los pasos a seguir para su ejecución.

El plan de tratamiento de riesgos de Seguridad y Privacidad de la información se basa en una orientación estratégica que requiere el desarrollo de una cultura de carácter preventivo, de manera que, al comprender el concepto de riesgo, así como el contexto, se planean acciones que reduzcan la afectación a la entidad en caso de materialización del mismo.

2. OBJETIVOS

- Definir y aplicar los lineamientos para tratar de manera integral los riesgos de Seguridad y Privacidad de la Información del Instituto Distrital de Gestión de Riesgos y Cambio Climático IDIGER.

- Gestionar riesgos de Seguridad y Privacidad de la información, de acuerdo al contexto del Instituto Distrital de Gestión de riesgos y Cambio Climático IDIGER.

- Fortalecer y apropiar conocimientos referentes a la gestión de Riesgos Seguridad y Privacidad de la información.

3. ALCANCE

Realizar una eficiente gestión de riesgos de Seguridad y Privacidad de la información, que permita integrar en los procesos del Instituto, buenas prácticas que contribuyan a la toma de decisiones y prevenir incidentes que puedan afectar el logro de los objetivos.

El Plan de Tratamiento de Riesgo tendrá en cuenta los riesgos que se encuentren en los niveles Medio y Alto acorde con los lineamientos definidos por el Ministerio TIC, los riesgos que se encuentren en niveles inferiores serán aceptados por la Entidad.

4. RESPONSABLES

Oficina 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 o Medida:** Acciones o mecanismos definidos para prevenir o reducir el impacto de los eventos que ponen en riesgo, la adecuada ejecución de las actividades y tareas requeridas para el logro de objetivos de los procesos del Instituto.
- **Impacto:** Son las consecuencias que genera un riesgo una vez se materialice.
- **Probabilidad:** Es la posibilidad de que la amenaza aproveche la vulnerabilidad para materializar el riesgo.
- **Riesgo:** Es un escenario bajo el cual una amenaza puede explotar una vulnerabilidad generando un impacto negativo al negocio evitando cumplir con sus objetivos.
- **Riesgo de seguridad de la información:** Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información (estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información).
- **Seguridad de la Información:** Este principio 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

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

6. MARCO REFERENCIAL

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

A través de la Política de Seguridad y Privacidad de la Información, el Instituto Distrital de Gestión de Riesgos y Cambio Climático (Aprobada con la Resolución 214 de 2019), se ha comprometido con la Implementación, mantenimiento y mejora continua del Modelo se Seguridad y Privacidad de la información – MSPI alineado con el Sistema de Gestión de Seguridad de la Información SGSI, aplicando la administración y gestión de riesgos para prevenir o minimizar el impacto generado sobre los activos de la información.

Se deben tener en cuenta alguna de las siguientes opciones, las cuales pueden considerarse independientemente, interrelacionadas o en conjunto:

• Evitar: Es eliminar la probabilidad de ocurrencia o disminuir totalmente el impacto, lo que requiere la eliminación de la actividad o fuente de riesgo, eliminar la exposición y su expresión máxima es dejar una actividad. Por ejemplo, para evitar pérdida de documentación se prohíbe el ingreso a un área.

• Prevenir: Corresponde al área de planeación, esto es, planear estrategias conducentes a que el evento no ocurra o que disminuya su probabilidad. Un ejemplo de ello son las inspecciones el mantenimiento preventivo, las políticas de seguridad o las revisiones periódicas a los procesos

• Reducir o mitigar: Corresponde a la protección en el momento en que se presenta el riesgo se encuentra en esta categoría los planes de emergencia, planes de continencia, equipos de protección personal, ambiental, de acceso y mantener copias de respaldo.

• Dispersar: Es dividir una actividad en diferentes componentes operativos, de manera que las actividades no se concentren en un mismo sitio o bajo una sola responsabilidad. Este es el caso de los contratos de suministro de partes, la ubicación de nodos, plantas alternas, equipos paralelos, contratar obras por tramos

• Compartir: es involucrar a un tercero para que responda en todo o en parte por el riesgo que genera una actividad. Dentro de los mecanismos de transferencia se encuentran los siguientes: contratos de seguro, transferencia explícita por medio de cláusulas contractuales, derivados financieros.

Los riesgos detectados deberán ser analizados de tal forma que se pueda determinar cuál va a ser su tratamiento.

7. METODOLOGÍA

El Plan de Tratamiento de Riesgos contempla la definición de las actividades a desarrollar en aras de mitigar los riesgos sobre los activos, estas actividades se estructuraron de acuerdo al Cronograma anexo, siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información (MinTIC:2016)2:

Los controles seleccionados serán confrontados con los estándares ISO 27001:2013 y su anexo A; a fin de determinar las falencias del Instituto Distrital de Gestión de Riesgo y Cambio Climático IDIGER.

7.1. DESARROLLO METODOLÓGICO

• Fase 1: Análisis de la información. En esta etapa se evaluarán los resultados de las entrevistas con los colaboradores del proceso de TI, se desarrollarán las siguientes actividades:

- Aplicar las políticas de tratamiento de riesgos.
- Determinar los controles (se desprenden de las medidas) aplicados en el Instituto de Gestión de Riesgos y Cambio Climático IDIGER.
- Determinar los riesgos que van a ser incluidos en el Plan de Tratamiento de Riesgos.

• Fase 2: Desarrollo de los proyectos En esta fase se realizarán las actividades que permitan la estructuración de las medidas.

- Determinar el nombre de la medida.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Elaborar la justificación de la medida.
- Definir las actividades a realizar para el desarrollo de la medida.

• Fase 3: Análisis de los proyectos

- Definición de los controles relacionados con cada medida.
- Validar los riesgos mitigados por cada medida.
- Análisis de la aplicabilidad de las medidas.
- Priorización de las medidas.

• Fase 4: Definición del organigrama de responsabilidad. En esta fase se realizará un organigrama y se definirán responsabilidades respecto a la administración y gestión del riesgo, esta etapa deberá ser definida por el Instituto teniendo en cuenta su estructura organizacional para la gestión de riesgos.

- Identificación de las funciones del Instituto en materia de seguridad de la información.

- Definición del grupo de trabajo de gestión de riesgo por parte del Instituto.
- Definición de las funciones del grupo de trabajo referentes a la aplicación y gestión de las medidas.

• Fase 5: Ciclo de vida del tratamiento de riesgos Definir las actividades a realizar por cada uno de los elementos del ciclo de vida del Plan de Tratamiento de Riesgos.

Planear: Dentro de esta etapa se desarrollan las actividades definidas en la fase 1 de la metodología de tratamiento de riesgos.

Hacer: En este paso del ciclo de vida se desarrollarán las actividades enmarcadas en la fase 2 de la metodología del tratamiento de riesgos.

Verificar: En esta etapa se desarrollarán las actividades que permiten hacer seguimiento o auditorías a la ejecución de cada una de las medidas.

Actuar: Dentro de esta etapa se realizarán las mejoras teniendo en cuenta el seguimiento y los resultados de las auditorías de la ejecución de los proyectos.

7.2. OPORTUNIDAD DE MEJORA

El Instituto Distrital de Gestión de Riesgos y Cambio Climático IDIGER, no sólo deberá centrarse en los riesgos identificados, sino que este análisis o apreciación del riesgo debe ser la base para identificar oportunidades. Por lo anterior la oportunidad deberá entenderse como la consecuencia positiva frente al resultado del tratamiento del Riesgo.

8. RECURSOS

El Instituto Distrital de Gestión de Riesgos y Cambio Climático IDIGER, en el marco de la gestión de riesgos de seguridad y Privacidad de la información, dispone de los siguientes recursos.

Humanos
La Oficina de Tecnologías de la información a través de seguridad de la información es responsable de coordinar, implementar, modificar y realizar seguimiento a las políticas, estrategias y procedimientos en la Entidad en lo concerniente a la seguridad y privacidad de la información lo cual contribuye a la mejora continua.

Técnicos
Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital - Versión 4 -

Octubre de 2018 del DAFP. Herramienta para la gestión de riesgos (Matriz de Riesgos SGSI)

Logísticos
Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos.

Financieros
Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías.

9. PRESUPUESTO

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la información identificados en la entidad, corresponderá al dueño del riesgo, quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos en el plan de tratamiento.

10. MEDICIÓN DEL PLAN DE TRATAMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La medición se realiza con un indicador de gestión que está orientado principalmente a determinar el porcentaje de implementación de los controles definidos en el tratamiento de riesgos de seguridad y privacidad de la información.

11. NORMATIVIDAD APLICABLE

NORMA	DESCRIPCIÓN
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1008 de 2018	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.
CONPES 3854 de 2016	Política Nacional de Seguridad Digital
Manual para la Implementación de la Política de Gobierno Digital	Implementación de la política de Gobierno Digital. Decreto 1008 de 2018 (Compilado en el Decreto 1078 de 2015, capítulo 1, título 9, parte 2, libro 2) Versión 7, abril de 2019

Modelo de Seguridad y privacidad de la información - MSPI	Se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital, TIC para el Estado y TIC para la Sociedad. TIC, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales
NTC / ISO 27001:2013	Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
NTC/ISO 31000:2009	Gestión del Riesgo. Principios y directrices.
Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 4	Riesgos de Gestión, Corrupción y Seguridad Digital Función Pública octubre 2018

12. CRONOGRAMA PRELIMINAR

GESTION	ACTIVIDAD	TAREA	RESPONSABLE	FECHA DE INICIO	FECHA DE FIN
	Identificación de Riesgos de Seguridad y Privacidad de la Información	Identificación, análisis y evaluación de Riesgos	Equipo de TICs	11 de enero de 2021	15 de febrero de 2021
	Aceptación de Riesgos Identificados	Aceptación, Aprobación de Riesgos Identificados y Planes de Mejoramiento	Equipo de TICs	16 de febrero de 2021	28 de febrero de 2021
	Publicación	Publicación de Matriz de Riesgos	Equipo de Planeación	1 de marzo de 2021	15 de marzo de 2021
	Seguimiento Fase de Tratamiento	Seguimiento estado planes de tratamiento de riesgos identificados y verificación de evidencias	Equipo de TICs	01 de julio de 2021	31 de diciembre de 2021
	Evaluación de Riesgos Residuales	Evaluación de Riesgos Residuales	Equipo de Planeación	02 de noviembre 2021	30 de noviembre de 2021

	Mejoramiento	Identificación de oportunidades de Mejora acorde a los resultados obtenidos durante la evaluación de riesgos residuales	Equipo de TICs Equipo de Planeación	01 de diciembre 2021	10 de diciembre 2021
	Monitoreo y Revisión	Generación, Presentación y Reporte de Indicadores	Equipo de TICs	13 de diciembre de 2021	23 de diciembre de 2021