MINISTERIO DE AMBIENTE Y DESARROLLO SOSTENIBLE

PLAN DE TRATAMIENTO DE RIESGOS - 2023

PROCESO

Gestión Estratégica de Tecnologías de la Información

Versión 1

30/01/2023

MADSIG
Sistema Integrado de Gestión

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio se basa en la generación de actividades y acciones preventivas para la mitigación de los riesgos y de esta manera mantener su valoración en un residual aceptable para el Ministerio, a través de estrategias de identificación, análisis, tratamiento, evaluación y seguimiento periódico de los riesgos de seguridad de la información en cada uno de los procesos de la Entidad.

Este plan de tratamiento, es una acción estratégica que pretende desarrollar una cultura de prevención, entendiendo y comunicando de forma objetiva el contexto de los riesgos que podrían comprometer el cumplimiento de los objetivos de la Entidad y buscando fortalecer la cultura de participación de todas las áreas del Ministerio, con el fin de entender la metodología y la forma de gestionar los riesgos, así como la importancia de la protección de los activos de información.

2. OBJETIVO

Definir el Plan de Tratamiento de Riesgos de Seguridad de la Información alineado a la metodología de Gestión del Riesgo del Ministerio y del Departamento Administrativo de la Función Pública - DAFP, que permita a los responsables de los procesos gestionar los riesgos en materia de seguridad de la información, identificados a partir del inventario de activos de información y valorados de acuerdo con el nivel de criticidad frente a su confidencialidad, integridad y disponibilidad.

2.1. OBJETIVOS ESPECÍFICOS

- Identificar los riesgos de seguridad de la información en cada uno de los procesos del Ministerio mediante la metodología definida por la Oficina de Planeación para este fin
- Gestionar los riesgos de seguridad de la información mediante ejercicios de análisis, evaluación y valoración periódica para preservar la integridad, disponibilidad y confidencialidad d ellos activos de información de cada uno de los procesos
- Sensibilizar y reforzar el conocimiento del tratamiento de los activos de información y sus riesgos de seguridad de la información asociados para su adecuada gestión a través de capacitaciones y talleres que cubran esta temática.

3. ALCANCE

Este plan de tratamiento se enfocará en gestionar y tratar los riesgos identificados y valorados como Muy Alto o Altos, que superan el nivel de riesgo aceptable en los diferentes procesos del Ministerio, con el fin de generar mecanismos para la mitigación de riesgos, toma de decisiones y prevención de incidentes asociados a la seguridad de la información.

El tratamiento de los riesgos debe contar con la participación activa de todas las áreas del Ministerio, con el fin de apropiar las directrices y lineamientos definidos en este plan y efectuar el monitoreo eficiente de los riesgos.

4. DEFINICIONES

• **Alta dirección:** persona o grupo de personas que dirige y controla una organización, al nivel más alto (ISO/IEC 27001:2013).

• **Activo de Información:** un activo de información es, cualquier elemento que contenga, genere, adquiera, gestione y/o procese información, que tiene valor para uno o más procesos de la organización y debe protegerse (ISO/IEC 27001:2013).

• **Aceptación de riesgo:** decisión de asumir un riesgo Amenazas: situación potencial de un incidente no deseado, el cual puede ocasionar daño a un sistema o a una organización.

• **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).

Análisis de Riesgo: uso sistemático de la información para identificar fuentes y estimar el riesgo (Guía ISO/IEC 73:2002).

• **Apetito al riesgo:** magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

• **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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 de una entidad.

• **Evaluación del riesgo:** proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo.

• **Gestión de riesgos:** actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y su tratamiento. (ISO 27000, Glosario de términos y definiciones).

• **Impacto:** son las consecuencias que genera un riesgo una vez se materialice.

• **Mapa de riesgos:** documento con la información resultante de la gestión del riesgo.

• **Probabilidad:** es la posibilidad de 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:** combinación de amenazas y vulnerabilidades en el entorno 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. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

• **Riesgo inherente:** nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

• **Riesgo residual:** nivel restante de riesgo después del tratamiento del riesgo.

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

5. MARCO NORMATIVO

El presente es el marco normativo en el que se basa el Plan de Tratamiento de Riesgos de Seguridad de la información del Ministerio para la vigencia 2023.

MARCO LEGAL	*FECHA*	*CONTEXTO*
Directiva Presidencial 02	Febrero 24 de 2022	"Para garantizar la implementación segura de la Política de Gobierno Digital liderada por el Ministerio de Tecnologías de la Información y las comunicaciones (MinTIC)"

Decreto 338	Marzo 8 de 2022	"Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los 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"
Resolución 746	Marzo 11 de 2022	"Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021".
Decreto 767	Mayo 16 de 2022	"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"
Directiva Presidencial 03	Marzo 15 de 2021	Lineamientos para el uso de Servicios en la Nube, Inteligencia Artificial, Seguridad digital y Gestión de Datos.
Resolución 500	Marzo 10 de 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".
Conpes 3995	Julio 1 de 2020	Política Nacional de Confianza y Seguridad Digital "Establecer medidas para desarrollar la confianza digital a través de la mejora la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías"
Resolución 1519	Agosto 24 de 2020	"Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos en materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos"
Guía para la administración del riesgo y el diseño de controles en entidades públicas -V5	Diciembre 2020	Establece la metodología para la administración del riesgo, los criterios para el análisis de probabilidad e impacto identificado y su respectivo nivel de severidad. En la versión 5 se actualizaron y precisaron algunos elementos metodológicos para mejorar el ejercicio de identificación y valoración del riesgo.
Decreto 612	Abril 4 de 2018	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.

Decreto 1008	Junio 14 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el Capítulo 1 del Tí-tulo 9 de la Parte 2 del Libro 2 del Decreto número 1078 de 2015, Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Ley 1915	Julio 12 de 2018	Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.
Resolución 2140	Octubre 19 de 2017	"Por la cual adopta el Modelo Integrado de Planeación y Gestión y se crean algunas instancias administrativas al interior del Ministerio de Ambiente y Desarrollo Sostenible y del Fondo Nacional Ambiental, y se dictan otras disposiciones"
Conpes 3854	Abril 11 de 2016	Política Nacional de Seguridad Digital. Busca fortalecer 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, en un marco de cooperación, colaboración y asistencia.
Decreto 103 de 2015	Enero 20 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
Decreto 1068	Mayo 26 de 2015	Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Capítulo 26.
Ley 1712	Marzo 06 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.
Decreto 886	Mayo 13 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 1377	Junio 23 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1581	Octubre 17 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Reglamentada parcialmente por el Decreto Nacional 1377 de 2013.

Ley 1273	Enero 05 de 2009	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.

6. POLÍTICA DE AMINISTRACIÓN Y GESTION DE RIESGOS DEL MINISTERIO

"La Alta Dirección del Ministerio de Ambiente y Desarrollo Sostenible en conocimiento de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos del Sistema Integrado de Gestión, implementa la Política de Administración y Gestión del Riesgo, por medio de la cual se valoran y se hace tratamiento a los riesgos por procesos como herramienta estratégica y de gestión, que permita anticipar y responder de manera oportuna y óptima a la materialización de los riesgos identificados en la matriz, contribuyendo al cumplimiento de los objetivos misionales y la mejora continua del sistema. Así mismo, la Política de Administración y Gestión de Riesgos será publicada y comunicada a todos los funcionarios y colaboradores del Ministerio de Ambiente y Desarrollo Sostenible a través de los diferentes medios con que cuenta la entidad."

6.1. OBJETIVOS DE LA POLÍTICA

- Controlar a través del Mapa de Riesgos todo el proceso relacionado con el manejo de los riesgos asociados al Sistema Integrado de Gestión.
- Proporcionar al Ministerio las directrices para la administración de los riesgos asociados a los procesos de la entidad, con el propósito de contribuir a la adecuada identificación, análisis, valoración (riesgos y controles) y tratamiento de estos.
- Integrar el manejo de los riesgos de gestión, corrupción, ambientales y seguridad de la información.
- Establecer la responsabilidad de los diferentes líderes de los procesos del ministerio.
- Establecer el rol de las diferentes dependencias del Ministerio.
- Dar cumplimiento a los requerimientos legales que apliquen al manejo de riesgos de gestión, corrupción, ambientales y de seguridad de la información.
- Fortalecer el comportamiento profesional y personal de los funcionarios del Ministerio.

7. ROLES Y RESPONSABILIDADES

7.1. Oficina de Planeación

- Responsable de realizar seguimiento a los Riesgos de Gestión, Corrupción y Seguridad de la Información.

7.2. Oficina de Tecnología de la Información y la Comunicación

- El Plan de Tratamiento de Riesgos de Seguridad de la Información se encuentra bajo el liderazgo de la Oficina de Tecnología de la Información y la Comunicación, quien establece los lineamientos y directrices, necesarios para realizar el apoyo en la identificación de los riesgos, implementación de controles y acciones que servirán para el tratamiento y mitigación de los riesgos de Seguridad de la Información.
- Responsable de definir y ejecutar el plan de comunicación, sensibilización y capacitación en seguridad de la información, cuyo objetivo es concientizar a las servidoras, servidores y contratistas, en lo relacionado con el tratamiento de los riesgos de seguridad de la información en la Entidad.
- Responsable de apoyar a los procesos que lo requieran, en las actividades conducentes a la identificación de los riesgos de seguridad de la información.

7.3. Responsables de Procesos y Dependencias

- Son responsables de identificar los riesgos, establecer y ejecutar acciones y/o controles para mitigarlos y aprobar los mapas de riesgos.
- Realizar seguimiento a la oportuna identificación, gestión y reporte de los riesgos de seguridad de la información de acuerdo con los lineamientos establecidos en el Ministerio. Cabe aclarar que, para cumplir con la implementación y cumplimiento de las actividades previstas en el Plan de Tratamiento de Riesgos de Seguridad de la Información es indispensable contar con el apoyo y el compromiso de los líderes de los procesos, el personal designado para tal fin (enlace - facilitador) y de la alta dirección.

8. ESTRATEGIA DE DESARROLLO DEL PLAN

En este Plan de Tratamiento de Riesgos de Seguridad de la Información se definen actividades y tareas encaminadas a gestionar los riesgos con el fin de obtener una valoración aceptable disminuyendo su calificación de Extrema o Alta a una calificación Moderada o Baja.

La etapa de implementación, se centra en la ejecución y cumplimiento de las actividades y objetivos acordados y aprobados, de la misma forma se tienen en cuenta los roles y responsabilidades y los tiempos establecidos por la Entidad en la Política de Administración del Riesgo. El resultado esperado de esta fase, es la adecuada implementación y cumplimiento de las actividades previstas en el Plan de Tratamiento de Riesgos de Seguridad de la Información.

El Plan de Tratamiento de Riesgos de Seguridad de la Información, está basado en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitido por el Departamento Administrativo de Función Pública - DAFP (V5), en la Política de Administración de Riesgos del Ministerio.

En el siguiente gráfico se presenta el modelo de gestión de riesgos de seguridad de la información para la adecuada administración de riesgos, los elementos que lo componen son:

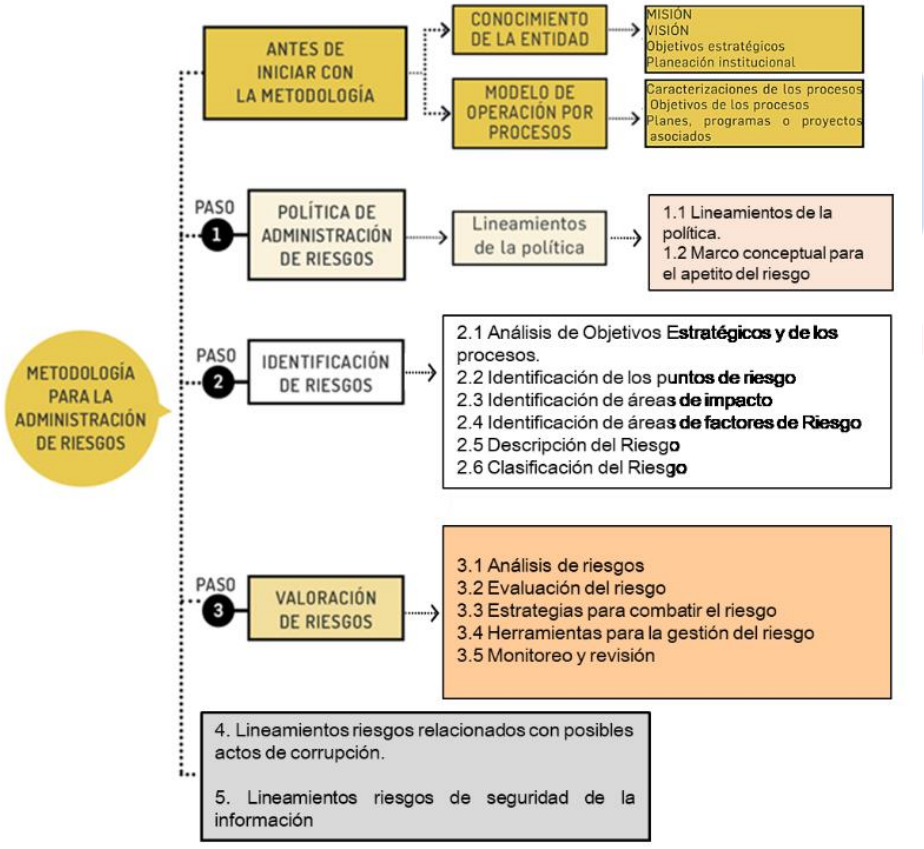

Ilustración 1. Metodología administración del riesgo
Fuente: Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas V5

9. DESARROLLO METODOLÓGICO

Fase 1: Análisis de la información

En esta fase se revisan los resultados de las mesas de trabajo con los diferentes procesos de la Entidad para desarrollar siguientes actividades:

- Verificar y analizar los riesgos identificados.
- Determinar los controles aplicables a cada riesgo.
- Definir los planes de tratamiento de los riesgos que superen al apetito de riesgo aceptable.

Fase 2: Desarrollo de las medidas de tratamiento de riesgos

En esta fase se realizarán las siguientes actividades.

- Determinar la medida de tratamiento.
- Definir los responsables de cada medida.
- Establecer el objetivo de cada medida.
- Desarrollar las actividades de ejecución de cada medida.

Fase 3: Análisis de los riesgos y medidas aplicadas

- Validar la eficacia de los controles y medidas de mitigación y tratamiento.
- Análisis de la aplicabilidad de las medidas de mitigación y tratamiento.

Fase 4: Ciclo de vida del tratamiento de riesgos

- Definir las actividades dentro 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 y revisiones a los riesgos de seguridad de la información.

9.1. ACTIVIDADES DEL PLAN

No.	ACTIVIDAD	EVIDENCIA	FECHA INICIO	FECHA FIN	RESPONSABLE
1	**PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**				
1.1	Definir el Plan de Tratamiento de Seguridad de la Información	Plan de tratamiento publicado/URL de publicación	18 Enero	27 Enero	Equipo de seguridad
1.2	Publicar el Plan de Tratamiento de Seguridad de la Información	Plan de Tratamiento de Seguridad de la Información publicado	27 Enero	31 Enero	Equipo de seguridad / OAP
2	**IDENTIFICACIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN**				
2.1	Socialización metodología de identificación de Riesgos de Seguridad de la Información	Correo electrónico masivo, listados de asistencia	1/06/2023	30/11/2023	Equipo de Seguridad
2.2	Apoyar la identificación de riesgos para 9/18 procesos	Mapa de riesgos por proceso	3/04/2023	30/11/2023	Equipo de Seguridad
2.3	Consolidar mapa de riesgos de seguridad de la información del Ministerio para 9/18 procesos	Mapa de riesgos por proceso	1/06/2023	30/11/2023	Oficina Asesora de Planeación
2.4	Aprobación de riesgos de seguridad de la información	Acta o correo de aprobación de riesgos - Mapa de riesgos de seguridad de la información	1/06/2023	30/11/2023	Responsables de los procesos y dependencias de la entidad
2.5	Seguimiento a los riesgos de seguridad de la información	Mapa de riesgos de seguridad de la información	1/06/2023	30/11/2023	Responsables de los procesos y dependencias de la entidad
3	**PLAN DE SENSIBILIZACIÓN SEGURIDAD DE LA INFORMACIÓN**				
3.1	Revisión y actualización del plan de sensibilización y capacitación	Documento actualizado en el MADSIGESTION/ URL de publicación	1/02/20223	15/03/2023	Equipo de Seguridad
3.2	Publicación y divulgación del plan de sensibilización y capacitación	Correo electrónico masivo y/o publicación en el MADSIG/ URL de publicación	15/03/2023	31/03/2023	Equipo de Seguridad
3.3	Ejecutar las	Correo electrónico	3/04/2023	30/11/2023	Equipo de Seguridad

No.	ACTIVIDAD	EVIDENCIA	FECHA INICIO	FECHA FIN	RESPONSABLE
	actividades del plan de sensibilización, por medio de reuniones, socializaciones, correos electrónicos, pantallas, carteleras, otros.	masivo, listados de asistencia			

9.2. TRATAMIENTO DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Una vez se han identificado los riesgos, se debe definir el tratamiento para cada uno de los riesgos analizados y evaluados. Este es un proceso cíclico, el cual involucra una selección de opciones para modificarlos, por lo tanto, se tendrán en cuenta las opciones planteadas en la "Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V5) – DAFP.

9.3. IDENTIFICACIÓN DEL RIESGO

Para poder gestionar los riesgos de la mejor forma posible es absolutamente necesario realizar una identificación previa de estos, que incluya la determinación y análisis de los sucesos que pueden llegar a ocurrir, así como sus posibles consecuencias. Se debe tener en cuenta diferentes aspectos como infraestructura, áreas de trabajo, entorno y ambiente en general, para lo cual se hace indispensable que cada uno de los procesos tenga identificados los activos de información.

9.4. VALORACIÓN DEL RIESGO

Se realizará acorde a la metodología para la administración de riesgos mencionada en la Guía para la administración del riesgo y el diseño de controles en entidades públicas emitida por el Departamento Administrativo de la Función Pública y adoptada por el Ministerio para la gestión del riesgo.

Se establecen los criterios para el análisis de probabilidad e impacto del riesgo identificado y su respectivo nivel de severidad, con un enfoque en la exposición al riesgo, análisis que le permite a los líderes de proceso contar con elementos objetivos para su definición, se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos,

en tal sentido, de acuerdo con la escala de severidad definida en 5 zonas (baja, moderada, alta y extrema), elementos que, en su conjunto, plantean un análisis de mayor profundidad teniendo en cuenta el entorno cambiante de la Entidad.

En mesas de trabajo con los procesos se analiza el contexto, se identifican los riesgos y se realiza el análisis de la probabilidad e impacto como valoración preliminar para identificar el nivel del riesgo inherente, asociando sus vulnerabilidades e identificando los controles para mitigarlas.

9.5. APROBACIÓN DE MAPAS DE RIESGO

Finalizada las etapas de la administración de riesgos y se obtenga la valoración de los riesgos de Seguridad y Privacidad de la Información, los líderes de los procesos deberán emitir un correo electrónico o acta de aprobación de los mapas de riesgos y planes de tratamiento con las actividades, cuando haya lugar a ello.

9.6. TRATAMIENTO ZONA DE RIESGO FINAL:

- Muy Alta: Evitar
- Alta: Reducir el riesgo - Mitigar
- Media: Compartir
- Baja, Muy Baja: Aceptar

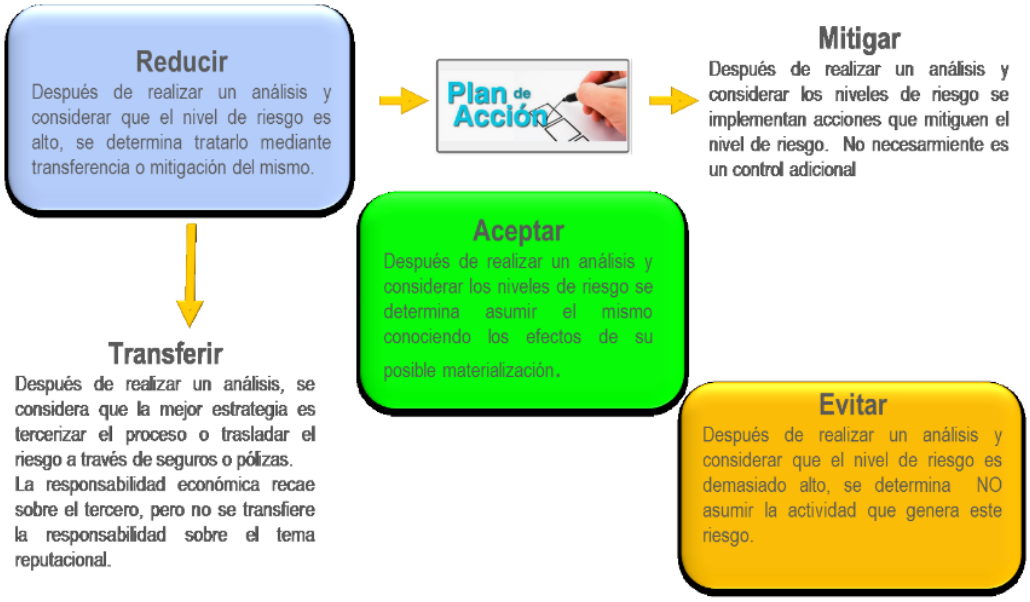

Ilustración 2 - Estrategias para combatir el riesgo
Fuente: Tomado de Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas (V5)

9.7. MATERIALIZACIÓN DEL RIESGO

En el caso de materializarse un riesgo, este debe ser reportado de acuerdo con el procedimiento establecido por la Oficina Asesora de Planeación. En caso de que se materialice un riesgo que no esté identificado, deberá ser reportado para que se inicie su correspondiente identificación en el mapa de riesgos.

10. OPORTUNIDAD DE MEJORA

Se deben identificar brechas y oportunidades de mejora en la gestión de los riesgos teniendo en cuenta las apreciaciones de la Oficina de Control Interno y/o las auditorias con el fin de optimizar la gestión de riesgos.

11. RECURSOS

El Ministerio dispondrá de los siguientes recursos para gestionar los riesgos de seguridad de la información.

RECUROS	DESCRIPCION
Humanos	• El grupo de Seguridad de la Información es responsable de definir e implementar las Políticas y lineamientos de seguridad de la información, así como su seguimiento y monitoreo, estableciendo estrategias y procedimientos que contribuyan a la mejora continua de la seguridad y privacidad de la información. • Los responsables de los procesos y dependencias, deben designar el personal idóneo para la identificación y gestión de riesgos de seguridad de la información.
Técnicos	• Política de administración y gestión de riesgos del Ministerio • Herramienta para la gestión de riesgos

Logísticos	• Recursos y logística para la transferencia de conocimiento, socializaciones y seguimiento a la gestión de riesgos.
Financieros	• Recursos asignados a Seguridad de la Información en la vigencia presupuestal del 2023.

12. 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.