Ambiente

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2026

Proceso

Gestión Estratégica de Tecnologías de la Información

Versión 4

28/01/2026

TABLA DE CONTENIDO

1. INTRODUCCIÓN

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Ambiente y Desarrollo Sostenible, establece las estrategias, acciones y medidas destinadas a mitigar los riesgos que puedan comprometer la confidencialidad, integridad, disponibilidad y privacidad de la información institucional. Su propósito es mantener los niveles de riesgo dentro de un rango residual aceptable, mediante la identificación, análisis, valoración, tratamiento y seguimiento de los riesgos asociados a los diferentes procesos de la Entidad.

Este Plan constituye una línea estratégica de fortalecimiento institucional, orientada a consolidar una cultura organizacional basada en la gestión preventiva del riesgo y en la comprensión de su contexto interno y externo. De esta forma, promueve la adopción de medidas proactivas frente a las nuevas modalidades de ciberataques que afectan a entidades públicas, privadas, proveedores de servicios tecnológicos y, en general, a los actores del ecosistema digital del Estado.

Asimismo, el Plan fomenta la conciencia y responsabilidad individual y colectiva frente al resguardo de la información y de los datos personales, impulsando la autoprotección, el cumplimiento normativo y la aplicación de buenas prácticas en materia de seguridad de la información. También busca fortalecer las capacidades institucionales para la detección temprana de vulnerabilidades, la respuesta oportuna a incidentes de seguridad y la recuperación frente a posibles afectaciones que puedan comprometer la continuidad de los servicios ofrecidos al ciudadano.

En concordancia con lo anterior, el Ministerio actualiza el presente Plan de Tratamiento de Riesgos de Seguridad de la Información para la vigencia 2026, en cumplimiento de lo dispuesto en el Decreto 612 de 2018, asegurando así la mejora continua de la gestión de seguridad de la información y su alineación con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y del Departamento Administrativo de la Función Pública.

2. OBJETIVO

Definir la estrategia y actividades del Plan de Tratamiento de Riesgos de Seguridad de la Información del Ministerio, alineado a la metodología de Gestión del Riesgo de la Entidad, conforme a los lineamientos y directrices emitidos por el Departamento Administrativo de la Función Pública (DAFP) y el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC), para la gestión y tratamiento de los riesgos de seguridad de la información, preservando la confidencialidad, integridad y disponibilidad.

3. OBJETIVOS ESPECÍFICOS

- Identificar y actualizar los riesgos de seguridad de la información del Ministerio.
- Tratar los riesgos de seguridad de la información, conforme al análisis, evaluación y valoración de estos, para preservar la integridad, disponibilidad y confidencialidad de los activos de información.
- Sensibilizar y reforzar la protección de los activos de información y sus riesgos de seguridad, por medio de charlas y socializaciones que cubran esta temática.
- Proponer e implementar controles que apunten a minimizar la probabilidad de ocurrencia de los riesgos identificados.

4. ALCANCE

El plan de tratamiento de riesgos de seguridad aplica a toda la Entidad, se enfoca en identificar, valorar, evaluar y tratar los riesgos de seguridad de la información, en especial los que se encuentran en la zona de riesgo Extremo, Alto o Moderado, los cuales superan el apetito de riesgo aceptable en el Ministerio, con la finalidad de generar mecanismos de tratamiento, así como fortalecer la toma de decisiones y la prevención frente a la materialización de incidentes de seguridad de la información que puedan afectar el logro de los objetivos institucionales.

Para el adecuado tratamiento y gestión de los riesgos se debe contar con la participación de todas las dependencias, oficinas y grupos de trabajo del Ministerio, con el fin de conocer, apropiar e implementar las directrices y lineamientos, realizar el seguimiento o monitoreo correspondiente de acuerdo con la Política de Riesgos de la Entidad.

5. DEFINICIONES

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

- **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.

- **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.

6. MARCO NORMATIVO

- **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".

- **Resolución 02277:** Junio de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones, por la cual se actualiza el Anexo 1 de la Resolución número 500 de 2021 y se derogan otras disposiciones relacionadas con la materia.

- **Guía para la administración del riesgo y el diseño de controles en entidades públicas -V6:** Noviembre 2022, **"**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".

- **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. Capitulo 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”.

7. GUÍA DE ADMINISTRACIÓN DEL RIESGO

El Ministerio de Ambiente y Desarrollo Sostenible, consciente de la responsabilidad e importancia del manejo de los riesgos asociados a los diferentes procesos definidos en el Sistema Integrado de Gestión, implementa la Guía de Administración del Riesgo, que valora y trata los riesgos, como herramienta estratégica y de gestión, que permita anticipar y responder oportunamente y óptimamente a la materialización de estos, identificados en el mapa, contribuyendo al cumplimiento de los objetivos misionales y la mejora continua.

8. OBJETIVOS DE LA POLÍTICA DE ADMINISTRACIÓN Y GESTIÓN DE RIESGOS

- 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, riesgos fiscales, riesgos ambientales, riesgos de seguridad de la información y riesgos para la integridad pública

- 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 los riesgos de gestión, riesgos fiscales, riesgos ambientales, riesgos de seguridad de la información y riesgos para la integridad pública.

- Fortalecer el comportamiento profesional y personal de los funcionarios del Ministerio de Ambiente y Desarrollo Sostenible.

9. ESTRATEGIA DE DESARROLLO DEL PLAN

El Plan de Tratamiento de Riesgos de Seguridad de la Información establece las actividades orientadas a gestionar, mitigar y controlar los riesgos que puedan afectar los activos de información institucional. Su finalidad es prevenir la materialización de los riesgos y asegurar que su valoración se mantenga dentro de niveles aceptables, procurando que los riesgos residuales se clasifiquen en niveles Moderado o Bajo, conforme a los criterios definidos por la Entidad.

La etapa de implementación se enfoca en la ejecución efectiva de las actividades y medidas de tratamiento definidas, garantizando el cumplimiento de los objetivos establecidos y considerando los roles y responsabilidades, así como los tiempos y lineamientos fijados en la Política de Administración del Riesgo. El resultado esperado de esta fase es la adecuada aplicación de los controles y la efectividad de las acciones previstas para reducir o mantener los riesgos en niveles tolerables.

Este Plan se fundamenta en las directrices de la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública, así como en la Guía de Administración del Riesgo del Ministerio, integrando buenas prácticas de gestión del riesgo, seguridad de la información y gestión institucional.

En el siguiente gráfico se presenta el modelo de gestión de riesgos de seguridad de la información, el cual integra los elementos esenciales para su adecuada identificación, análisis, valoración, tratamiento, seguimiento y mejora continua.

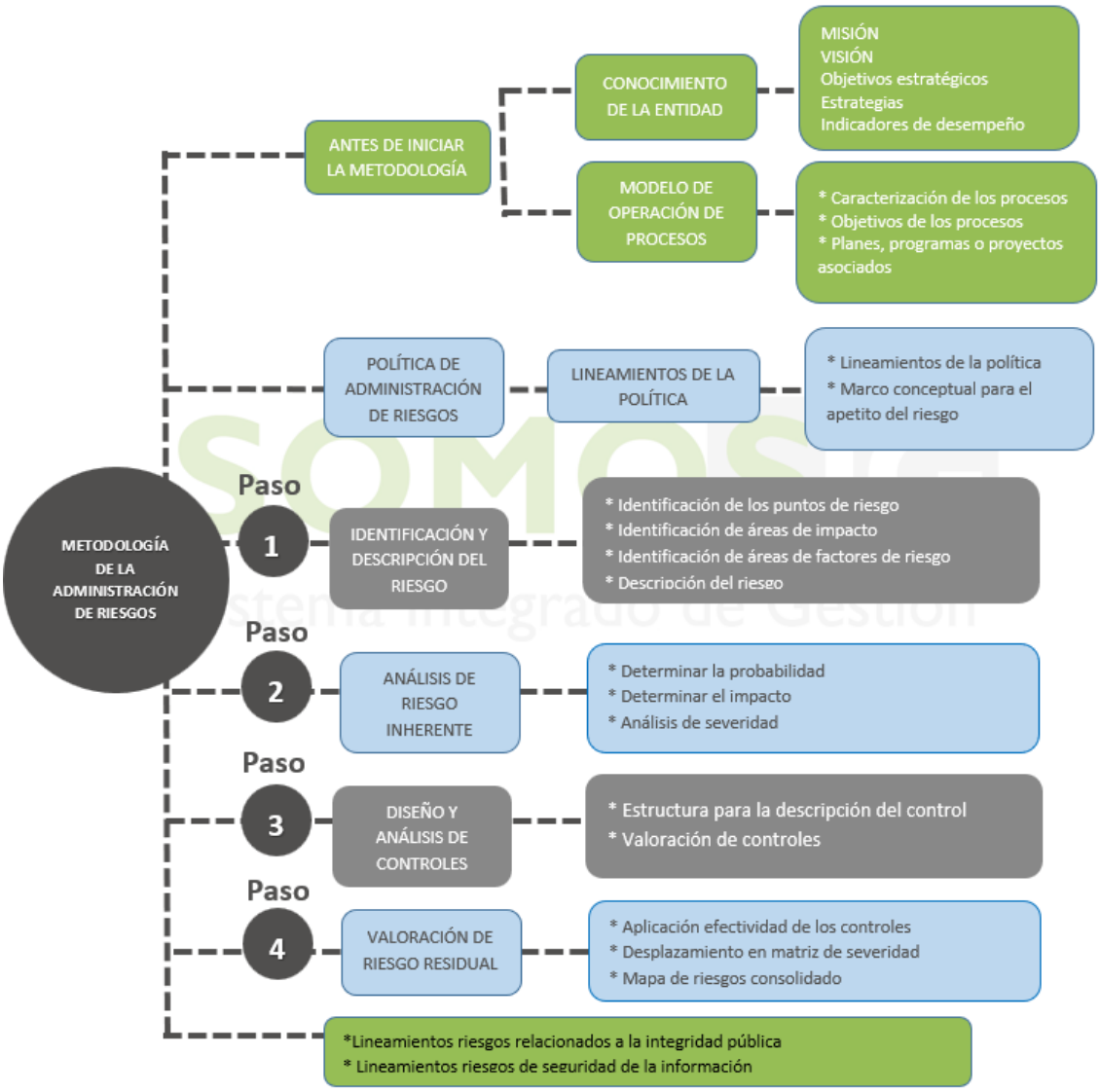

Ilustración 1. Metodología para la Administración del Riesgo. Adaptada fuente: DAFP. 2025.

10. DESARROLLO METODOLÓGICO

Teniendo en cuenta la aplicabilidad del ciclo PHVA (Planificar, Hacer, Verificar y Actuar) como base para la mejora continua de la gestión y tratamiento de riesgos de seguridad de la información, se definen las fases y actividades de la siguiente manera:

- **Planificar (Planear)**

Corresponde a las actividades previstas en la Fase 1 de la metodología de tratamiento de riesgos, en la cual se realiza el análisis inicial.

En esta etapa se adelantan actividades como:

  - Revisión y verificación de los riesgos identificados,
  - Análisis de su impacto y probabilidad,
  - Determinación de los controles aplicables,
  - Definición de los planes de tratamiento para los riesgos que superen el nivel de apetito o tolerancia definido por la Entidad.

- **Hacer (Ejecutar)**

Se relaciona con las actividades de la Fase 2, orientadas al desarrollo y ejecución de las medidas de tratamiento.

Incluye:

  - Determinar la medida de tratamiento más adecuada (mitigar, transferir, evitar o aceptar),
  - Asignar responsables,
  - Definir objetivos específicos por medida,
  - Implementar las acciones requeridas para la ejecución del tratamiento.

- **Verificar (Revisar y evaluar)**

Articulada con la Fase 3, comprende las actividades de seguimiento, validación y auditoría interna para revisar la eficacia del tratamiento aplicado.

Actividades clave:

- Validar la efectividad de los controles implementados,
- Verificar el cumplimiento de las acciones definidas,
- Evaluar la pertinencia y suficiencia de las medidas de mitigación o tratamiento.

- **Actuar (Mejorar)**

Corresponde a la Fase 4, donde se adoptan mejoras con base en los resultados del seguimiento, auditorías o revisiones.

Incluye:

- Actualización del plan de tratamiento,
- Ajustes a controles o estrategias que no resultaron efectivos,
- Definición de nuevas acciones para fortalecer la gestión de riesgos,
- Retroalimentación del ciclo para garantizar la mejora continua.

10.1. Fases Metodológicas del Tratamiento de Riesgos

Fase 1: Análisis de la información

Se revisan los insumos derivados de las mesas de trabajo con los procesos y se desarrolla:

- Verificación y análisis detallado de los riesgos identificados,
- Determinación de los controles vigentes y necesarios,
- Definición de los planes de tratamiento para riesgos que superen el nivel aceptable.

Fase 2: Desarrollo de las medidas de tratamiento de riesgos

Actividades orientadas a la ejecución:

- Selección de la medida de tratamiento (mitigación, eliminación, aceptación, transferencia),
- Definición de responsables,
- Establecimiento del objetivo de cada medida,
- Ejecución de las acciones requeridas para implementar cada medida.

Fase 3: Análisis de los riesgos y medidas aplicadas

Actividades orientadas a la evaluación y revisión:

- Validación de la eficacia de los controles y medidas aplicadas,
- Análisis de la pertinencia y aplicabilidad de las medidas de mitigación implementadas,
- Revisión de la evolución del riesgo residual.

Fase 4: Ciclo de vida del tratamiento de riesgos

Comprende todas las actividades transversales de seguimiento, mejora, retroalimentación y documentación del Plan de Tratamiento de Riesgos, asegurando su actualización continua y su alineación con los lineamientos institucionales y normativos vigentes.

11. ACTIVIDADES DEL PLAN

No.	ACTIVIDAD	EVIDENCIA	FECHA INICIO	FECHA FIN	RESPONSABLE
1	Apoyar la actualización de los Riesgos de Seguridad de la Información del Ministerio en articulación con el cronograma de la OAP	Mapa de riesgos	Mayo 2026	Agosto 2026	Equipo de Seguridad /OAP /Procesos
2	Consolidar el mapa de Riesgos de Seguridad de la Información	Mapa de riesgos consolidado	Agosto 2026	Septiembre 2026	Equipo de Seguridad
3	Gestionar la aprobación de los Riesgos de Seguridad de la Información y sus planes de tratamiento por parte de los procesos y el comité	Acta o correo de aprobación de riesgos – Acta del CIGD en donde sean aprobados	Septiembre 2026	Octubre 2026	Responsables de los procesos y dependencias de la entidad
4	Acompañar técnicamente a los procesos en el Seguimiento al mapa de riesgos de seguridad de la información (en caso de ser requerido)	Correo electrónico con la solicitud	Agosto 2026	Diciembre 2026	Equipo de Seguridad /Procesos

12. GESTIÓN DE LOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

Es un proceso cíclico que busca identificar los riesgos, vulnerabilidades, causas, amenazas, impacto, consecuencias, controles y el tratamiento según aplique para cada riesgo analizado y evaluado.

12.1. Identificación/Actualización del Riesgo

Para gestionar los riesgos hay que identificarlos o actualizarlos, incluyendo la determinación y análisis de los sucesos que pueden llegar a ocurrir y sus posibles consecuencias. Se debe considerar aspectos como infraestructura, áreas de trabajo, entorno, otros, para lo cual es necesario que cada proceso tenga identificados sus activos de información.

12.2. Valoración del Riesgo

Se establecen los criterios para analizar probabilidad e impacto del riesgo identificado y su nivel de severidad, con enfoque en la exposición al riesgo, análisis que permite a los líderes de proceso contar con elementos objetivos para definir, se consideran la afectación económica y reputacional como aspectos principales frente a la posible materialización de los riesgos, según la escala de severidad definida en (baja, moderada, alta y extrema), elementos que plantean un análisis de mayor profundidad según el entorno cambiante de la Entidad.

En mesas de trabajo con los procesos se identifican o actualizan 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.

12.3. Tratamiento Zona de Riesgo Final:

- **Zona de riesgo Baja:** Aceptar el riesgo.
- **Zona de riesgo Moderada:** Reducir el riesgo.
- **Zona de riesgo Alta:** Reducir el riesgo, evitar, transferir o compartir.
- **Zona de riesgo Extrema:** Reducir el riesgo, evitar, transferir o compartir.

Los riesgos que se encuentren en zona baja se aceptan (apetito del riesgo) y se continúa el monitoreo, con el fin de garantizar que las condiciones bajo las cuales han sido analizados no han cambiado, si las condiciones cambian, es necesario volver a valorar y si es el caso determinar el manejo correspondiente a través de los controles que sean necesarios. Así mismo, los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento.

Los riesgos que se encuentran en las zonas más altas o de mayor gravedad son los que se priorizan disminuyéndose para estos el nivel de aceptación, determinando en el plan de contingencia las actividades de control (correctivas) que ataquen las causas del riesgo, cuando éste se llegue a materializar.

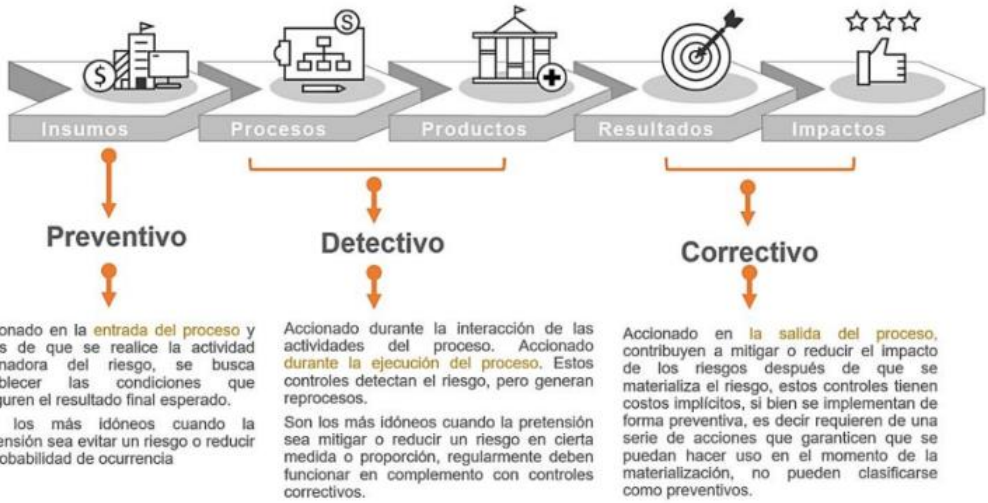

Ilustración 2. Metodología para la Administración del Riesgo - Controles. Adaptada fuente: DAFP. 2025.

Esto ayuda a la Entidad a mejorar su administración de riesgos, priorizando los esfuerzos y acciones sobre los riesgos potencialmente de mayor impacto.

12.4. Aprobación de Mapas de Riesgo

Una vez finalizadas las etapas de identificación, valoración, actualización y tratamiento de los riesgos de Seguridad de la Información, y tras completar los campos requeridos en la matriz y el Plan de Tratamiento de Riesgos (cuando aplique), los líderes de proceso deberán emitir su aprobación formal respondiendo al correo institucional mediante el cual se remite el acta de aprobación de riesgos y la matriz consolidada correspondiente. Este procedimiento garantiza la validación, trazabilidad y responsabilidad de cada proceso frente a la administración integral del riesgo.

13. MATERIALIZACIÓN DEL RIESGO

Cuando se detecte la materialización de un riesgo, deberán aplicarse las acciones determinadas según la línea de defensa que lo identifique:

a) Materialización de riesgos detectada por el líder del proceso (primera línea de defensa):

La primera línea es responsable de la operación y del control directo de los riesgos. En caso de materialización:

- Si el riesgo es de corrupción se deberá informar a la Oficina Asesora de Planeación como

representante del (la) Ministro(a) para el Sistema Integrado de Gestión (Resolución 2140 de 2017), sobre el hecho encontrado. De considerarlo necesario, realizar la denuncia ante el ente de control respectivo.

- Si el riesgo es de gestión o de seguridad de la información, se debe realizar el análisis de causas y determinar acciones, análisis y actualización correspondiente del mapa de riesgos.

b) Materialización de riesgos detectada por la Oficina Asesora de Planeación (segunda línea de defensa):

La segunda línea supervisa la gestión del riesgo, brinda directrices y verifica la correcta aplicación del Modelo de Control Interno.

- En los casos de riesgos de corrupción detectado por la segunda Línea de defensa, se debe:
  - Informar sobre el hecho encontrado a la Oficina de Control Interno, para lo de su competencia.
  - Informar al líder del proceso, para revisar el mapa de riesgos y sus controles asociados, verificar que se tomaron las acciones y que se actualizó el mapa de riesgo.
- En los casos de riesgos de Gestión detectado por la segunda Línea de defensa, se debe comunicar a la Oficina de Control Interno, para lo de su competencia y al líder del proceso sobre el hecho encontrado, para que realice la revisión, análisis y acciones correspondientes para resolver el hecho y verificar que se tomaron las acciones, que se actualizó el mapa de riesgos correspondiente e informar a la Alta Dirección sobre el hallazgo y las acciones tomadas.

c) Materialización de riesgos detectada por parte de la Oficina de Control Interno (tercera línea de defensa).

La tercera línea realiza evaluación independiente y verifica la eficacia del Sistema de Control Interno.

- Si el riesgo es de corrupción, se deberá convocar al Comité de Coordinación de Control Interno e informar sobre los hechos detectados, desde donde se tomarán las decisiones para iniciar la investigación de los hechos. Dependiendo del alcance (normatividad asociada al hecho de corrupción materializado), realizar la denuncia ante el ente de control respectivo. Facilitar el inicio de las acciones correspondientes con el líder del proceso, para revisar el mapa de riesgos y sus controles asociados. Verificar si se tomaron las acciones y si se actualizó el mapa de riesgos.

- Si el riesgo es de gestión, informar al líder del proceso sobre el hecho encontrado y orientarlo frente a la revisión, análisis y acciones correspondientes para resolver el hecho. Convocar al Comité de Coordinación de Control Interno e informar sobre la actualización realizada

14. OPORTUNIDAD DE MEJORA

La Entidad deberá identificar de manera continua brechas y oportunidades de mejora en la gestión de riesgos, considerando:

- Recomendaciones de la Oficina de Control Interno,
- Resultados de auditorías internas o externas,
- Lecciones aprendidas derivadas de la materialización de riesgos,
- Ajustes necesarios para fortalecer controles, acciones y medidas adoptadas.

15. RECURSOS

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

RECURSOS	DESCRIPCIÓN
Humanos	• La OTIC con su equipo de Seguridad de la Información es responsable de liderar, definir e implementar políticas y lineamientos de seguridad de la información, 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 y necesario para la identificación y gestión de riesgos de seguridad de la información.
Técnicos	• Guía de administración del riesgo (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 2026.