Manual

SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS

Gestión Integral de Riesgos

Contenido

1. INTRODUCCIÓN 5
2. OBJETIVO GENERAL DE LA GESTIÓN INTEGRAL DE RIESGOS 5
2.1. OBJETIVOS ESPECÍFICOS 6
3. ALCANCE 6
4. MARCO LEGAL Y DE REFERENCIA 7
5. DEFINICIONES 8
6. PRINCIPIOS Y POLÍTICAS 12
6.1. PRINCIPIOS DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS 12
6.2. POLÍTICAS GENERALES 13
6.3. POLÍTICAS ESPECÍFICAS 20
6.3.1. De los elementos 20
6.3.2. De las etapas 23
6.4. PRINCIPIOS Y POLÍTICAS GESTIÓN DE RIESGO DE TERCERAS PARTES 27
7. ESTRUCTURA ORGANIZACIONAL 28
7.1. ROLES Y FUNCIONES 31
7.1.1. JUNTA DIRECTIVA 31
7.1.2. REPRESENTANTE LEGAL 33
7.1.3. COMITÉS DE RIESGOS 35
7.1.4. ALTA DIRECCIÓN (PRESIDENTE, VICEPRESIDENTES, JEFES DE OFICINA, GERENTES, DIRECTORES) 35
7.1.5. VICEPRESIDENCIA DE SEGURIDAD Y RIESGOS EMPRESARIALES 36
7.1.6. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN 38
7.1.7. OFICIAL DE CUMPLIMIENTO 39
7.1.8. UNIDAD DE PREVENCIÓN DEL RIESGO LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (LAFT) 41
7.1.9. LÍDERES DE PROCESOS 42
7.1.10. GESTORES INTEGRALES 44
7.1.11. DEBERES DE CUMPLIMIENTO DE LOS SERVIDORES PÚBLICOS Y COLABORADORES DE COLPENSIONES 45

7.1.12. ÓRGANOS DE CONTROL 46
8. CLASIFICACIÓN DE RIESGOS 47
9. MARCO INTEGRAL DE APETITO DE RIESGOS Y AGREGACIÓN DE RIESGOS 49
9.1. MARCO INTEGRAL DE APETITO DE RIESGO 49
9.1.1. Objetivo del Marco Integral de Apetito de Riesgo 50
9.1.2. Alcance del Marco Integral de Apetito de Riesgo 50
9.1.3. Funciones y Responsabilidades en el Marco Integral de Apetito de Riesgo 50
9.1.4. Definición del Marco Integral de Apetito de Riesgo 51
9.1.5. Lineamientos para el Seguimiento al Comportamiento del Apetito de Riesgo 62
9.1.6. Comunicación Marco Integral de Apetito de Riesgo 62
9.2. AGREGACIÓN DE RIESGOS 63
10. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS 65
10.1. ESTABLECIMIENTO DEL CONTEXTO 67
10.1.1. Establecimiento del Contexto de la Gestión de Riesgo 68
10.1.2. Establecimiento del Contexto a Nivel Estratégico 68
10.1.3. Establecimiento del Contexto a Nivel Táctico 72
10.1.4. Establecimiento del Contexto a Nivel de Procesos 73
10.2. EVALUACIÓN DE RIESGOS 74
10.2.1. Identificación de Riesgos 74
10.2.2. Análisis de Riesgos 83
10.2.3. Valoración de Riesgos 100
10.3. TRATAMIENTO DE RIESGOS 101
10.4. SEGUIMIENTO Y REVISIÓN 104
10.4.1. Eventos de Riesgo 105
10.4.2. Autoevaluación de Riesgos y Controles 109
10.4.3. Monitoreo a riesgos a través de indicadores 110
10.4.4. Evaluación de Riesgos en Terceras Partes 112
10.4.5. Seguimiento a los planes de mejoramiento 117

10.5. METODOLOGÍA PARA LA GESTIÓN DE LAS OPORTUNIDADES 118
10.6. COMUNICACIÓN Y CONSULTA 119
10.7. REGISTRO E INFORME 119
11. DOCUMENTACIÓN Y REGISTRO DE LA GESTIÓN INTEGRAL DE RIESGOS 120
12. PLATAFORMA TECNOLÓGICA 120
13. CAPACITACIÓN Y SENSIBILIZACIÓN 121
13.1 DISEÑO 122
13.2 DESARROLLO 123
13.3 IMPLEMENTACIÓN 124
13.4 EVALUACIÓN Y MEJORAMIENTO CONTINUO DEL PLAN 125
14. ANEXOS 126
15. CONTROL DE CAMBIOS DEL DOCUMENTO 127

TÍTULO I. DISPOSICIONES GENERALES

1. INTRODUCCIÓN

En un entorno de constante evolución y cambio, identificar, valorar y gestionar los riesgos y oportunidades a los que se enfrenta una empresa, es fundamental para su desarrollo y crecimiento.

Es por ello que, para Colpensiones, la Gestión Integral de Riesgos es un eje fundamental para el logro de sus objetivos estratégicos, tácticos y por procesos. Bajo esta premisa, se ha definido el marco de actuación sobre el cual se gestionan los riesgos en la entidad, estableciendo políticas, responsabilidades, procedimientos y metodologías, que deberán ser consideradas por todos sus grupos de interés, (colaboradores, proveedores, órganos de control, ciudadanos, etc), para una adecuada administración de los diferentes riesgos a los que se enfrenta la entidad en la búsqueda de sus objetivos estratégicos, en el cumplimiento del plan de acción institucional y en el desarrollo de sus procesos.

Para la definición de este marco de actuación y en línea con los objetivos estratégicos de Colpensiones, se consideraron las mejores prácticas en materia de gestión de riesgos, tomando como referencias principales el marco de normas ISO, en especial la norma técnica colombiana NTC-ISO 31000, el Modelo Integrado de Administración de Riesgo emitido por el Committee of Sponsoring Organizations of the Treadway Commission - COSO ERM, los acuerdos emitidos por el Comité de Basilea, 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 las recomendaciones en materia de gestión de riesgo de la Organización Internacional de Supervisores de Pensiones y la Organización para la Cooperación y el Desarrollo Económico OCDE.

De igual forma, y como entidad vigilada por la Superintendencia Financiera de Colombia, se consideró el marco normativo emitido por dicha entidad, en materia de Gestión de Riesgos.

2. OBJETIVO GENERAL DE LA GESTIÓN INTEGRAL DE RIESGOS

Crear y proteger el valor para Colpensiones dentro del apetito de riesgo definido, a través de un marco claro de políticas, lineamientos, responsabilidades, procedimientos y metodologías que permitan la identificación, valoración, tratamiento, seguimiento y comunicación eficiente y eficaz de los riesgos a los que se ve expuesta la entidad a nivel estratégico, táctico y por proceso, promoviendo la cultura de gestión de riesgos en todos los niveles de la organización, reduciendo los efectos no deseados, potenciando las oportunidades y contribuyendo al cumplimiento de los objetivos y metas institucionales.

2.1. OBJETIVOS ESPECÍFICOS

a. Establecer y divulgar el marco de políticas y lineamientos para la gestión de riesgos, considerando el conocimiento y puntos de vista de todas las partes interesadas.

b. Establecer y divulgar el marco integral de apetito de riesgo de la entidad, abarcando las diferentes tipologías de riesgo a las que se ve expuesta Colpensiones, con el fin de que el mismo sea considerado por la organización en la toma de decisiones y asignación de recursos.

c. Definir con claridad el marco de gobierno y las responsabilidades de todos los roles presentes en la gestión de riesgos y en todos los niveles de la organización.

d. Definir e implementar metodologías, procedimientos y herramientas que permitan gestionar los diferentes componentes del sistema de administración de riesgos de manera integral para las diferentes tipologías de riesgo y de manera integrada a todas las actividades de la organización

e. Establecer los mecanismos de seguimiento a los riesgos a los que se ve expuesta la entidad con el fin de generar alertas tempranas, corregir tendencias negativas que impliquen el asumir un mayor riesgo al permitido y mejorar los procesos y el control interno de la entidad.

f. Determinar los criterios, parámetros y alcance a considerar en el establecimiento de un plan de capacitación sobre la administración de riesgos que permita profundizar los conocimientos, desarrollar nuevas habilidades y mantener las existentes.

g. Definir e implementar un proceso de comunicación eficaz sobre la gestión de riesgos que apoye el proceso de toma de decisiones y al mejoramiento continuo.

h. Asegurar el cumplimiento del marco normativo en materia de gestión de riesgos, aplicable a Colpensiones.

3. ALCANCE

La administración integral de riesgos es responsabilidad de todos los servidores públicos y colaboradores de Colpensiones, así como, de los terceros que apoyan el cumplimiento de sus objetivos.

Tiene alcance sobre el direccionamiento estratégicos de la entidad (Riesgos Estratégicos), los proyectos desarrollados para alcanzar sus metas (Riesgos Tácticos) y los procesos empleados para el cumplimiento de su objeto social (Riesgos por procesos).

Por lo anterior, es de vital importancia para Colpensiones sensibilizar a todos sus colaboradores respecto de la importancia de contar con una visión integral y estratégica sobre la identificación, el

análisis, la evaluación, el tratamiento, monitoreo y comunicación de los riesgos de forma que se dé cumplimiento a la misión y objetivos de Colpensiones.

Este manual describe la administración de riesgos de forma integrada, basado en una metodología estandarizada para los diferentes riesgos que afectan a la entidad, incluyendo: operacional, continuidad del negocio, fraude y corrupción, seguridad de la información y ciberseguridad, financieros, lavado de activos y financiación del terrorismo.

4. MARCO LEGAL Y DE REFERENCIA

El presente Manual se establece conforme al marco regulatorio vigente aplicable a Colpensiones expedido por la Superintendencia Financiera de Colombia en lo relativo a los Sistemas de Administración de Riesgos (Operacional, Continuidad del Negocio, Lavado de Activos y Financiación del Terrorismo, Seguridad de la información y Ciberseguridad, Financieros) y el Sistema de Control Interno; los documentos establecidos por el Departamento Administrativo de la Función Pública con relación al Modelo Integrado de Planeación y Gestión-MIPG– y la Guía para la administración del riesgo y el diseño de controles en entidades públicas.

Adicional a lo anterior, y con el objetivo de adoptar las mejores prácticas en materia de gestión de Riesgos, Colpensiones ha considerado los siguientes marcos de referencia:

- Marco de normas establecidas por el Organismo Internacional de Estandarización (ISO), entre las que se encuentran:
  - ISO 9001 - Sistema de Gestión de Calidad – Requisitos
  - ISO 31000 - Gestión de Riesgos – Directrices
  - ISO 27001 – Seguridad de la Información
  - ISO 27005 – Gestión de Riesgos de Seguridad de la Información
  - ISO22301 – Continuidad del Negocio
- El Marco Integrado para la Gestión de Riesgos Corporativos emitido por el Committe Of Sponsoring Organizations of the Treadway Commission – COSO ERM.
- Las recomendaciones en materia de riesgos definidas en los acuerdos de supervisión bancaria emitidos por el Comité de Basilea.
- Las recomendaciones dadas en materia de riesgos por la Organización Internacional de Supervisores de Pensiones (IOPS) y la Organización para la Cooperación y el Desarrollo Económico (OECD).

5. DEFINICIONES

Activos de información: Cualquier elemento que contenga, datos que tienen valor para uno o más procesos de la organización y debe protegerse. (ISO/IEC 27001:2013).

Amenaza: Son los eventos que pueden causar la afectación de la confidencialidad, integridad o disponibilidad de la información y se deben clasificar de acuerdo con los tipos de contenedores de los activos de información.

Ciberseguridad: Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio que son esenciales para la operación de la entidad. (Circular Básica Jurídica, Parte I, Título IV, Capítulo V "Requerimientos mínimos para la gestión del riesgo de ciberseguridad" agregado por la Circular Externa 008 de 2018).

Corrección: Acción para eliminar una no conformidad detectada.

Corrupción: Cualquier acción u omisión cometida por un servidor, colaborador o tercero de la entidad, usando las facultades o funciones del cargo confiado por la entidad para su desarrollo, con el fin de desviar la gestión hacia un beneficio particular.

De acuerdo con las definiciones establecidas, la corrupción es una clasificación del fraude, que implica una calificación del sujeto que realiza el acto, teniendo en cuenta que son personas con poder o incidencia en la toma de decisiones y la administración de los recursos de Colpensiones.

Declaración de apetito por el riesgo (DAR): Informe escrito en donde la Junta Directiva y la Presidencia informan los diferentes tipos de riesgo en los que Colpensiones está dispuesta a aceptar, asumir o evitar para lograr sus objetivos estratégicos.

Evento: Incidente o situación que ocurre en un lugar particular durante un intervalo de tiempo determinado.

Eventos de pérdida: Son aquellos incidentes que generan pérdidas por riesgo a la entidad.

Factores de riesgo: Se entiende por factores de riesgo, las fuentes generadoras de riesgos que pueden o no generar pérdidas.

Fraude: Cualquier acción u omisión intencional realizada con el fin de obtener un provecho económico ilícito o de cualquier otra índole, en detrimento de los intereses de la entidad o de un tercero.

Gestión del Riesgo: Proceso efectuado por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Límites: Medidas cuantitativas desarrolladas con base en supuestos, utilizadas para la definición del apetito de riesgos de la Entidad e incorporadas en la declaración del apetito de riesgos.

Manual de Riesgo: Es el documento que contiene las políticas, objetivos, estructura organizacional, estrategias, los procesos y procedimientos aplicables en el desarrollo, implementación y seguimiento del Sistema Integral de Administración de Riesgos.

Mapa de Riesgos: Instrumento que permite representar gráficamente la información resultante de la gestión de riesgos.

Marco de apetito de riesgo (MAR): Conjunto de Políticas, metodologías, procedimientos y controles a partir del cual Colpensiones establece, comunica y monitorea el apetito de riesgo. Debe tener en consideración los riesgos tanto financieros, como no financieros, así como los que afectan la reputación de la entidad.

Pérdida: Cuantificación económica de la ocurrencia de un evento, así como los gastos derivados de su atención.

Pérdida Bruta: Se entiende una pérdida antes de recuperaciones de cualquier tipo.

Pérdida Neta: Se entiende la pérdida después de tener en consideración los efectos de las recuperaciones. La recuperación es un hecho independiente, relacionado con el evento de pérdida bruta, que no necesariamente se efectúa en el mismo periodo por el que se perciben fondos o flujos económicos.

Perfil de riesgo: Resultado consolidado de la medición permanente de los riesgos a los que se ve expuesta la entidad.

Plan de contingencia: Conjunto de acciones y recursos para responder a las fallas e interrupciones específicas de un sistema o proceso.

Plan de continuidad del negocio: Conjunto detallado de acciones que describen los procedimientos, los sistemas y los recursos necesarios para retornar y continuar la operación, en caso de interrupción.

Riesgo: El riesgo es el efecto de la incertidumbre y dicha incertidumbre puede tener efectos positivos o negativos. Una desviación positiva que surge de un riesgo puede proporcionar una oportunidad, pero no todos los efectos positivos del riesgo tienen como resultado oportunidades.

Riesgo de cumplimiento: Es la posibilidad de incurrir en sanciones administrativas, legales y financieras o en dado caso en la pérdida de reputación por el incumplimiento de las normas, disposiciones legales o regulatorias, código de conducta y estándares adoptados por la Entidad.

Riesgo de contagio: Es la posibilidad de pérdida que una entidad puede sufrir, directa o indirectamente, por una acción o experiencia de un vinculado. El vinculado es el relacionado o asociado e incluye personas naturales o jurídicas que tienen posibilidad de ejercer influencia sobre la entidad.

Riesgo de terceras partes: Se entiende como la posibilidad de ocurrencia de sucesos (positivos o negativos), a raíz de la relación u arreglo de negocios que la entidad tiene con una tercera parte. Estos sucesos inciertos pueden afectar los objetivos y metas de la entidad contratante.

Riesgo Emergente: Los riesgos emergentes son eventos nuevos e imprevistos y/o la evolución de riesgos conocidos previamente que la entidad no ha comprendido o permitido.

Riesgo inherente: Nivel de riesgo propio de la actividad, sin tener en cuenta el efecto de los controles. El riesgo inherente puede reducirse de acuerdo con la gestión operativa de la entidad, lo cual se hace a través de la adopción de políticas, procesos, procedimientos, y definición de perfiles de los funcionarios, previo a su contratación entre otros.

Riesgo legal: Es la posibilidad de pérdida en que incurre una entidad al ser sancionada u obligada a indemnizar daños como resultado del incumplimiento de normas o regulaciones y obligaciones contractuales.

El riesgo legal surge también como consecuencia de fallas en los contratos y transacciones, derivadas de actuaciones malintencionadas, negligencia o actos involuntarios que afectan la formalización o ejecución de contratos o transacciones. Aplica a todas las actividades e incluye a terceros que actúen en representación de la entidad respecto de los procesos y/o actividades tercerizadas.

Riesgo reputacional: Es la posibilidad de pérdida en que incurre una entidad por desprestigio, mala imagen, publicidad negativa, cierta o no, respecto de la institución y sus prácticas de negocios, que cause pérdida de clientes, disminución de ingresos o procesos judiciales.

Riesgo residual: Es el nivel resultante del riesgo después de aplicar los controles.

Tercera parte: Organización / Entidad (Persona Natural o Jurídica), que tiene un acuerdo, relación contractual o no contractual, con el propósito de proveer o suministrar un bien, servicio o producto, o un beneficio a Colpensiones. Ejemplos de Terceras Partes: contrapartes, proveedores de servicios y productos, entidades sin ánimo de lucro, consultores, firmas de abogados, entidades de servicios públicos, distribuidores, etc.

Tipo de riesgo: Se refiere a los diferentes riesgos a los cuales se enfrenta la entidad, según corresponda que con carácter enunciativo y no limitativo pueden corresponder a los riesgos operacionales, de continuidad del negocio, de seguridad de la información y ciberseguridad, financieros, de fraude y corrupción, de lavado de activos y financiación del terrorismo.

Tratamiento al riesgo: Es la acción que la entidad toma para prevenir o mitigar los impactos de eventos que afectaría el logro de objetivos, mediante una apropiada definición e implementación de controles, de manera que los riesgos se sitúen en un nivel tolerable por la institución.

Vulnerabilidad: Son las debilidades identificadas en los procesos, tecnología, personas y/o la infraestructura con la que se realiza el procesamiento de la información y que son aprovechadas por las amenazas contra la confidencialidad, integridad y/o disponibilidad de la información.

TÍTULO II. GESTIÓN INTEGRAL DE RIESGOS

6. PRINCIPIOS Y POLÍTICAS

6.1. PRINCIPIOS DEL SISTEMA INTEGRAL DE ADMINISTRACIÓN DE RIESGOS

Propendiendo por la eficacia de los procesos de Colpensiones, la gestión de riesgos está basada en los siguientes principios:

✓ *La gestión de riesgos crea y protege el valor:*

La gestión de riesgos en Colpensiones contribuye al logro de los objetivos estratégicos y a la mejora del desempeño organizacional.

✓ *La gestión de riesgos es una parte integral de todos los procesos de la entidad:*

La gestión de riesgos en Colpensiones hace parte de las actividades de todos los procesos de la entidad, incluyendo la planeación estratégica y la gestión de proyectos.

✓ *La gestión de riesgos es parte de la toma de decisiones:*

La gestión de riesgos hace parte fundamental en la toma de decisiones.

✓ *La gestión de riesgos aborda explícitamente la incertidumbre:*

La gestión de riesgos considera eventos internos o externos que se pueden llegar a presentar, así como su naturaleza y la forma en que se pueden mitigar.

✓ *La gestión de riesgos es sistemática, estructurada y oportuna:*

La gestión de riesgos está orientada a apoyar el cumplimiento en la promesa de servicio y se basa en un enfoque estructurado y establecido, aprobado por la Alta Dirección.

✓ *La gestión de riesgos se basa en la mejor información disponible:*

El proceso de gestión de riesgos se basa en fuentes de información tales como datos históricos, experiencia, retroalimentación de las partes involucradas, observación, previsiones, eventos de riesgos, juicio de expertos.

✓ *La gestión de riesgos está adaptada.*

La gestión de riesgos se alinea con el contexto externo e interno y del perfil de riesgo de la entidad.

✓ *La gestión de riesgos toma en consideración los factores humanos y culturales*:

La gestión de riesgos reconoce las capacidades, percepciones e intenciones de individuos externos e internos, los cuales pueden facilitar o dificultar el logro de los objetivos de la entidad.

✓ *La gestión de riesgos es transparente e inclusiva:*

La correcta y oportuna intervención de las partes involucradas y, en particular, de aquellos que toman las decisiones en todos los niveles de la organización, está orientada a que la gestión de riesgos sea dinámica.

✓ *La gestión de riesgos es dinámica, reiterativa y receptiva al cambio:*

La gestión de riesgos responde al cambio. En la medida en que se presenten eventos externos e internos, de su análisis y monitoreo pueden surgir riesgos nuevos y cambios en los ya existentes.

✓ *La gestión de riesgos facilita la mejora continua de la organización:*

La gestión de riesgos involucra la identificación de oportunidades de mejora y se realiza con el fin de contribuir al logro de los objetivos de Colpensiones, por lo tanto, facilita la mejora continua de la entidad.

6.2. POLÍTICAS GENERALES

El marco de políticas generales para la administración de riesgos se establece considerando los 5 componentes del Marco Integrado para la Gestión de Riesgos Corporativos emitido por el Committe Of Sponsoring Organizations of the Treadway Commission – COSO ERM, así:

- ***Gobierno de Riesgo y Cultura***

a. El máximo órgano de supervisión de los riesgos es la Junta Directiva de la organización, es por ello por lo que es su responsabilidad, el aprobar las políticas, estructuras, líneas de reporte y responsabilidades en materia de gestión de riesgos, contenidas en el presente documento, apoyándose en los conceptos de los comités de apoyo que considere pertinentes.

b. Dado lo anterior, es fundamental el desarrollo y mantenimiento de habilidades, experiencia y conocimiento en el negocio y en materia de administración de riesgos, en esta instancia y en la Alta Dirección de Colpensiones.

c. La Junta Directiva de la entidad asume el compromiso de impulsar a nivel institucional la cultura en materia de gestión integral de riesgos, definiendo con claridad los comportamientos y valores institucionales y su compromiso con la integridad y los valores éticos.

d. La cultura de Gestión de Riesgos de Colpensiones debe incluir la incorporación del análisis de riesgos en el proceso de toma de decisiones de la Junta Directiva y la Alta Gerencia, analizando los diferentes escenarios que pueden presentarse y su impacto sobre los objetivos trazados.

e. La Junta Directiva realiza, como mínimo una vez al año, seguimiento a la estrategia considerando en dicho seguimiento el estado de los riesgos estratégicos y emergentes identificados.

f. La Alta Dirección tiene atribuciones delegadas por la Junta Directiva para dirigir la gestión de Colpensiones, administrando los recursos disponibles para la administración de riesgos, enfocándose en la creación y mantenimiento de la cultura de autogestión, autocontrol y autorregulación.

g. La participación de la Alta Dirección (Presidente, Jefes de Oficina, Vicepresidentes y Gerentes) en la definición del marco de políticas de la gestión de riesgos, del apetito de riesgo y de la identificación y evaluación de riesgos a nivel estratégico, constituyen una práctica fundamental en la generación de cultura de gestión de riesgos.

h. La definición de los roles y responsabilidades en materia de administración integral de riesgos, debe realizarse bajo el modelo de las tres línea de defensa, logrando la apropiación y gestión de los riesgos desde la primera línea de defensa (Unidades de negocios), bajo el marco de las políticas y metodologías establecidas por la segunda línea de defensa (Unidades de riesgo), que adicionalmente complementa la gestión de riesgos con una visión agregada de los mismos y monitorea su comportamiento; y logrando una evaluación independiente de la tercera línea de defensa (Unidades de Auditoría Interna).

i. Colpensiones promueve la integración de las diferentes tipologías de riesgo a la cultura institucional, a partir de la divulgación y formación en los temas que componen la administración de riesgos y en las herramientas que se emplean para su gestión.

j. Se consagra como mecanismo fundamental para la prevención y control de los riesgos, la capacitación permanente de los servidores públicos, colaboradores y terceros críticos de

Colpensiones. Para el efecto, la entidad desarrolla un programa anual de sensibilización, difusión y capacitación en gestión de riesgos, que incluya cada una de las tipologías de riesgo definidas en el presente manual.

k. Adicional a las capacitaciones, Colpensiones debe considerar otro tipo de actividades para concientizar y difundir los principales aspectos de la gestión de riesgos, en cada una de sus tipologías.

l. La buena conducta y la ética en las operaciones diarias son política esencial en la Entidad. Los miembros de la Junta Directiva, la administración, los servidores públicos, y colaboradores deben mantener los más altos estándares éticos en sus actuaciones diarias, dentro y fuera de la Entidad.

m. Colpensiones considera a su talento humano, como el principal factor para mantener y fortalecer su cultura organizacional. Dado lo anterior, desarrolla procesos eficientes para atraer, desarrollar y retener personal competente de acuerdo con sus funciones.

n. Colpensiones propenderá por el autocontrol, entendido como la capacidad de los colaboradores de considerar el control como parte inherente de sus responsabilidades, campos de acción y toma de decisiones asegurando que se tengan implementados y documentados los controles para mitigar los riesgos a los que se encuentren expuesta la Entidad.

Dado lo anterior, es responsabilidad de las tres líneas de defensa, promover la cultura del autocontrol.

p. La gestión de riesgos incluirá las actualizaciones presentadas por cambios en el tipo de relación con terceros vigentes y en la iniciación de relaciones con nuevos terceros; así como eventos de riesgo, auditorías, informes de entes de control, relacionados con las terceras partes.

- ***Estrategia y Objetivos***

a) Colpensiones debe considerar los riesgos estratégicos al tiempo que desarrolla o actualiza su Direccionamiento Estratégico. Las estratégicas definidas en dicho proceso, deben ser respuesta a los riesgos y oportunidades identificados en el marco de este ejercicio.

b) De acuerdo con lo anterior, en los procesos de actualización e identificación de riesgos, Colpensiones debe entender el contexto interno y externo del negocio, y como este afecta el cumplimiento de sus objetivos de corto, mediano y largo plazo.

c) En el entendimiento del contexto externo, es de vital importancia la identificación de los riesgos emergentes que puedan impactar a futuro el negocio.

d) La Junta Directiva de Colpensiones debe fijar las políticas y directrices para la implementación del Sistema Integral de Administración de Riesgos y disponer de los recursos necesarios para garantizar la adecuada gestión y actualización de los riesgos que afectan el cumplimiento de los objetivos de la Entidad, dando cumplimiento a las regulaciones y requerimientos definidos por la Superintendencia Financiera de Colombia y demás entidades de control que sean aplicables a Colpensiones.

e) En el marco de establecimiento del contexto de la gestión integral de riesgos de Colpensiones, es indispensable la definición clara del nivel de apetito de riesgos y el nivel de tolerancia sobre el mismo. Dicho apetito debe establecerse en función de declaraciones cualitativas y mediciones cuantitativas que permitan establecer con precisión, si las decisiones que se toman en cada nivel de la organización, se encuentran dentro de la cantidad de riesgo que la entidad está dispuesta a asumir para el logro de sus objetivos.

- **Desempeño – Identificación y evaluación del riesgo**

a) El sistema Integral de Administración de Riesgos de Colpensiones debe identificar y evaluar los riesgos a nivel estratégico (Análisis del contexto, Misión, Visión, Objetivos Estratégicos), táctico (Riesgos sobre proyectos) y por procesos (Riesgos sobre los procesos), abarcando los riesgos operacionales, de continuidad del negocio, de seguridad de la información y ciberseguridad, de fraude y corrupción, de lavado de activos y financiación del terrorismo y los riesgos financieros de mercado, liquidez y contraparte.

b) La valoración de los riesgos debe realizarse considerando la probabilidad de ocurrencia de estos, así como el impacto que podrían llegar a tener sobre los objetivos estratégicos, de los proyectos o de los procesos.

c) En dicha valoración, se deben considerar variables cualitativas y cuantitativas, buscando que dicho proceso sea cada vez más objetivo.

d) Una vez analizados y definidos las variables y criterios de valoración para establecer el nivel de apetito de riesgo de Colpensiones, se procederá a socializar con las Gerencias participes en esta definición (Gerencia Administrativa, Gerencia de Planeación Institucional, Gerencia de Determinación del Derecho, Gerencia de Financiamiento e Inversiones, entre otras) y que de acuerdo con su conocimiento e información administrada pueden brindar soporte a la adecuada definición del nivel de apetito de riesgo.

e) El proceso de evaluación del riesgo debe permitir priorizar los riesgos a los que se ve expuesta la organización, enfocando sus esfuerzos en primera instancia a los riesgos estratégicos sin

olvidar los riesgos a nivel táctico y por procesos, que presenten señales de alerta o desviaciones.

f) Para una adecuada identificación y evaluación de riesgos, la Vicepresidencia de Seguridad y Riesgos Empresariales tiene la responsabilidad de definir metodologías claras y comprensibles para el desarrollo de la gestión integral de riesgos, buscando su mejora continua a través de estándares nacionales e internacionales. En este marco, es responsabilidad de la Vicepresidencia de Seguridad y Riesgos Empresariales el desarrollar las habilidades necesarias para que las tres líneas de defensa apliquen dichas metodologías de forma adecuada.

g) La metodología definida para la gestión integral de riesgos, es aplicable a cualquier otro sistema de administración de riesgos, sistema de gestión o marcos de referencia, que llegaren a resultar aplicables para Colpensiones. En este entendido, es responsabilidad del líder asignado a cada sistema de gestión, adoptar la metodología y ajustar acorde con los criterios particulares que se definan en la respectiva normativa o marco de referencia, para su ejecución.

h) La Junta Directiva, el Vicepresidente de Seguridad y Riesgos Empresariales, el Oficial de Cumplimiento, los órganos de dirección y control, los servidores públicos y colaboradores de Colpensiones, deben velar por el efectivo cumplimiento de los reglamentos internos de la entidad y de la normatividad vigente en materia de administración integral de riesgos.

i) De acuerdo con la evaluación del riesgo, y considerando los niveles de apetito y tolerancia al riesgo aprobado por la Junta Directiva, la Alta Dirección de Colpensiones (Presidente, Vicepresidentes, Jefes de Oficinas, Gerentes y Directores), Líderes de Proyectos y Líderes de Procesos, son los responsables de definir las medidas de tratamiento a los riesgos priorizados, así como de asegurar su eficacia.

j) Los riesgos en Colpensiones pueden ser aceptados, evitados, mitigados, transferidos o monitoreados. Al establecer la medida de tratamiento a emplear, se deberá considerar el contexto interno, el contexto externo y la relación beneficio costo de la decisión adoptada.

- ***Revisión y Monitoreo***

a) De acuerdo con el nivel de riesgo (Estratégico, Táctico y por Procesos), su evaluación y el nivel de apetito de riesgo de Colpensiones, se debe establecer un periodo mínimo de revisión y seguimiento, que en todo caso no podrá ser superior a 6 meses.

b) Para el seguimiento y monitoreo de los riesgos, Colpensiones debe definir mecanismos que le permitan generar alertas tempranas sobre los principales riesgos de la entidad, con el fin de anticiparse a las desviaciones que en los mismos se puedan presentar.

c) El reporte oportuno y completo de los eventos de riesgo que se materializan en la entidad es fundamental para el seguimiento al comportamiento de los riesgos y para el mejoramiento continuo del negocio, los proyectos y sus procesos. Dado lo anterior, es responsabilidad de la Alta Dirección fortalecer en sus equipos la cultura del reporte bajo los procedimientos y metodologías eficientes definidas desde la Vicepresidencia de Seguridad y Riesgos Empresariales.

d) Para los riesgos que cuenten con información histórica y permitan su medición cuantitativa, se debe dar preferencia al establecimiento de indicadores o métricas que permitan mantenerlos monitoreados y alerten sobre la desviación de estos.

e) La primera línea de defensa tendrá un esquema de monitoreo y tratamiento consistente y periódico sobre los riesgos generados de terceras partes. De acuerdo con esto se establecerán flujos de información oportunos y precisos, para propender por una gestión proactiva del riesgo.

- ***Información, Comunicación y Reporte***

a) En el marco de la gestión integral de riesgos, Colpensiones debe establecer la información requerida para el desarrollo de sus diferentes etapas, contemplando fuentes internas y externas.

b) En la búsqueda de las fuentes de información, la Gestión Integral de Riesgos en Colpensiones, debe analizar los sistemas de información con los que cuenta la entidad y debe buscar el máximo aprovechamiento de la información que ellos generan y las funcionalidades que utilizan para fortalecer los mecanismos de seguimiento, comunicación y reporte de riesgos al interior de la entidad.

c) La Gestión Integral de Riesgos debe contemplar una estrategia de comunicación y reporte que incluya a todos los grupos de interés, incluyendo al menos a la Junta Directiva, la Alta Dirección, los líderes de proceso, los gestores integrales, los servidores públicos y colaboradores de la entidad, los terceros críticos, las áreas especiales de riesgo, los órganos de control, la Superintendencia Financiera de Colombia y los ciudadanos.

d) La Vicepresidencia de Seguridad y Riesgos Empresariales, con base en la información disponible, debe proporcionar información relevante en materia de riesgos, a las diferentes instancias de gobierno de la entidad, con el fin de que con base en la misma se tomen decisiones acertadas para el cumplimiento de los objetivos del negocio.

- ***Prevención y resolución de conflictos de interés en la recolección de información en las diferentes etapas del Sistema Integral de Administración de Riesgos.***

  a. Todo lo relacionado con la prevención y resolución de conflictos de interés se encuentra contenido en el Código de Ética de Colpensiones.

     Para COLPENSIONES, un conflicto de interés es la situación en la que un colaborador realiza sus funciones, trabajos u otras actividades propias de la Entidad influenciado por consideraciones personales, con lo que puede afectar su imparcialidad, objetividad e independencia.

     En materia de Lavado de Activos y Financiación del Terrorismo – LA/FT, además de poner en conocimiento del superior jerárquico el presunto conflicto de interés, como lo establece la normatividad general, se debe poner en conocimiento del Oficial de Cumplimiento.

  b. Los líderes de los procesos deben dar cumplimiento a los mecanismos establecidos para evitar y resolver conflictos de interés en la administración de los riesgos de Colpensiones, especialmente para el registro de eventos de riesgo materializados.

  c. Los mecanismos para la prevención y resolución de conflictos de interés están implícitos dentro del Sistema Integral de Administración de Riesgos, los cuales se basan en la consecución de un consenso basado en la discusión entre expertos conformado por el Comité Integral de Riesgos.

- ***Sanciones por el incumplimiento del Sistema Integral de Administración de Riesgos***

  a. Todos los servidores públicos y colaboradores de Colpensiones tienen la obligación institucional y personal de cumplir con la totalidad de las políticas, obligaciones y procedimientos contenidos en el presente manual, sus partes y anexos, y en las normas legales vigentes, pues se entiende que el no hacerlo expone a Colpensiones a riesgos de cumplimiento, legales, de reputación, financieros, operacionales, entre otros.

     El incumplimiento de las políticas y procedimientos establecidos en el Sistema Integral de Administración de Riesgos dará lugar a las sanciones previstas en la ley, los reglamentos y el contrato laboral.

6.3. POLÍTICAS ESPECÍFICAS

6.3.1. De los elementos

- ***Procedimientos***

a. Los lineamientos y actividades en materia de administración de riesgos deben estar documentados acorde con cada uno de los niveles establecidos: Estratégico, Táctico y por Procesos y deben ser actualizados conforme a la evolución de los mismos.

b. Todos los procesos documentados a través del Sistema Integrado de Gestión (mapa de procesos), deben contemplar las actividades de control que permitan mitigar los riesgos identificados y contemplados en la matriz de evaluación de riesgos del proceso, y su revisión y evaluación se debe realizar con base en la metodología establecida para tal fin.

- ***Documentación***

a. El Manual del Sistema Integral de Administración de Riesgos es elaborado, revisado y actualizado por la Gerencia de Riesgos y Seguridad de la Información, bajo la supervisión de la Vicepresidencia de Seguridad y Riesgos Empresariales, por lo menos una vez al año. La actualización que se genere de esta revisión debe surtir las etapas de validación establecidas en el marco de la elaboración y control de documentos del Sistema Integrado de Gestión.

b. Las modificaciones realizadas al Manual del Sistema Integral de Administración de Riesgos o sus Partes, deben ser presentadas por la Vicepresidencia de Seguridad y Riesgos Empresariales a los Comités competentes, según corresponda, para validación y posterior presentación y aprobación de la Junta Directiva.

c. El Manual del Sistema Integral de Administración de Riesgos debe ser publicado en el aplicativo definido para la administración de documentos del Sistema Integrado de Gestión - SIG, para consulta y conocimiento de los servidores públicos y colaboradores de la Entidad.

d. Cada actualización del Manual del Sistema Integrado de Administración debe estar acompañada por una estrategia de capacitación y comunicación que permita asegurar el conocimiento del marco general de riesgos definido en el mismo, involucrando a todas las partes interesadas.

e. Para la implementación de la administración de riesgos, ante la presencia de nuevos sistemas de gestión o marcos de referencia, se adoptará la metodología de gestión integral de riesgos en lo que respecta a su marco general (ej. Mapa de riesgos y sus niveles), y en lo particular, el responsable del sistema respectivo, debe contar con un documento que lo soporte.

- ***Registro de Eventos de Riesgo***

  a. Los eventos de riesgo deben ser reportados en el momento de su identificación, a través del formato, canales o herramientas tecnológicas establecidas para tal fin.

  b. En caso de presentarse un evento de riesgo cuya materialización afecte de manera crítica el desarrollo normal de uno o varios procesos o que su impacto tenga repercusiones financieras para la entidad, éste debe ser reportado e informado a la Vicepresidencia de Seguridad y Riesgos Empresariales, a través de los mecanismos definidos por la Entidad para este fin y de acuerdo con el instructivo vigente.

  c. Es responsabilidad de todos los servidores públicos, colaboradores, contratistas y terceros que desarrollen actividades para Colpensiones, reportar los eventos de riesgos que en el desarrollo de sus actividades se presenten. El no reporte se considera como una falta disciplinaria o un incumplimiento contractual según corresponda.

  d. El análisis de causa raíz en la gestión de eventos de riesgo, es fundamental para que dicho mecanismo sea una herramienta eficaz en el mejoramiento continuo de la organización, siendo responsabilidad de los líderes de proceso; este se desarrollará en el marco de la metodología de formulación, seguimiento y evaluación de planes de mejoramiento, establecida en el proceso de Gestión de Procesos.

  e. La calidad e integridad de la información suministrada para el registro contable de los eventos de riesgo con pérdida económica, es responsabilidad del área y líder del proceso fuente de la información.

- ***Plataforma Tecnológica***

  a. Colpensiones debe contar con herramientas tecnológicas que le permitan la adecuada gestión de riesgos, soportando el cumplimiento de las políticas y procedimientos establecidos por la Entidad.

- ***Divulgación de la Información***

  a. Colpensiones debe divulgar a través de su página web la información relevante y necesaria, con el fin que los ciudadanos puedan conocer las estrategias de gestión integral de riesgos.

  b. El vocero único de Colpensiones es el Presidente o su delegado, ningún servidor público, colaborador o contratista se encuentra autorizado para divulgar información de la entidad, sin su previa autorización.

c. La divulgación interna y externa en materia de riesgos debe cumplir con los lineamientos establecidos por Colpensiones en cuanto a mantener la seguridad, calidad y confidencialidad de la información.

d. La revelación contable se debe realizar en los términos de Ley y bajo los correspondientes principios contables que regulan la materia. Al cierre de cada ejercicio contable, la administración debe incluir en el informe de gestión, los aspectos destacados de la administración integral de los riesgos.

e. Para efectos de divulgación de la información interna, se deben utilizar como medios de comunicación el correo institucional, la intranet y las herramientas tecnológicas que soporten la administración del Sistema Integrado de Gestión - SIG, en lo que respecta a la publicación de los manuales, procesos y demás documentos relacionados con el Sistema Integral de Administración de Riesgos, sus partes y anexos.

- ***Capacitación***

a. Todos los servidores públicos y colaboradores de Colpensiones durante el proceso de inducción deben recibir capacitación sobre la gestión integral de riesgos, y son responsables de su adecuado funcionamiento. Dicho proceso de inducción deberá surtirse acorde con los lineamientos y tiempos establecidos por la Gerencia de Talento Humano y Relaciones Laborales.

b. La capacitación de gestión integral de riesgos está contenida en la inducción corporativa, la cual es liderada por la Gerencia de Talento Humano y Relaciones Laborales.

c. La formación en materia de gestión integral de riesgos es obligatoria para todos los servidores públicos y colaboradores de la Entidad.

d. Los cargos Directivos (Presidente, Vicepresidentes, Jefes de Oficinas, Gerentes y Directores) y los roles de Líderes de Proceso, Gestores Integrales y Gestores Regionales, son considerados de un alto impacto e influencia en la cultura de riesgos de Colpensiones. Por lo anterior, ante el cambio de colaboradores en estos cargos o roles, se les debe impartir inducción particular sobre su rol en el Sistema Integral de Administración de Riesgos en un término máximo de dos meses a partir de su llegada al cargo o rol.

Es responsabilidad de los líderes de proceso y directores regionales, informar de manera oportuna cualquier cambio que se presente en la asignación del rol de gestor integral o gestor regional.

e. Los programas de capacitación se deben realizar mínimo una vez al año. En caso de las áreas con roles específicos en alguno de los Sistemas de Administración de Riesgos que componen

el Sistema Integral de Administración de Riesgos, las mismas deben recibir capacitación específica sobre sus responsabilidades en materia de gestión de riesgos.

f. Los programas de capacitación específicos en gestión integral de riesgos, dirigida a los proveedores considerados como críticos para el negocio, se deben realizar como mínimo una vez al año.

6.3.2. De las etapas

- ***Identificación de riesgos***

a. En el proceso de identificación y actualización de riesgos, debe considerarse la identificación de riesgos a nivel estratégico (Riesgos estratégicos y emergentes sobre su direccionamiento estratégico y la influencia del entorno sobre el mismo), Táctico (Riesgos tácticos sobre el Plan de Acción Institucional y los proyectos) y Por Procesos (Riesgos sobre los procesos)

b. Los eventos de riesgos identificados por los órganos de control en el desarrollo de sus actividades y los eventos de riesgos materializados reportados en las herramientas establecidas por la entidad para tal fin deben ser valorados por el responsable del proceso para ser considerados en la actualización de la matriz evaluación de riesgos.

c. La identificación y evaluación de los riesgos debe ser realizada por los líderes de los procesos y los proyectos, de acuerdo con la metodología establecida en el presente manual, considerando las diferentes tipologías de riesgos (operacional, continuidad del negocio, financieros, lavado de activos y financiación del terrorismo, fraude y corrupción, seguridad de la información y ciberseguridad, y cualquier otra tipología de riesgos, sistema de gestión o marco de referencia que se llegue a establecer).

d. La Gerencia de Riesgos y Seguridad de la información, debe establecer los procesos de validación sobre la identificación y evaluación de riesgos realizada por los líderes de los procesos y los proyectos, con el fin de asegurar la adecuada aplicación de las metodologías definidas en la materia.

e. En el lanzamiento de un nuevo producto, incursión en un nuevo mercado, adopción de nuevas tecnologías, uso de nuevos canales de comunicación y modificaciones sobre los procesos, es indispensable la identificación y evaluación de los riesgos que este cambio implica, previo a la puesta en operación de este.

f. En la identificación de los riesgos, los líderes de los procesos deben establecer el objetivo de control asociado al riesgo, a saber: objetivo de cumplimiento, objetivo de información u objetivo operativo; con el fin de establecer los riesgos de cumplimiento que pueden impactar

de manera significativa a la Entidad, asegurando el cumplimiento de las normas legales y los reglamentos que le sean aplicables.

- ***Análisis de riesgos***

a. El análisis de los riesgos identificados debe ser realizado por los líderes de los procesos de acuerdo con la metodología establecida en el presente manual, considerando las diferentes clasificaciones (Estratégico, Táctico y por Procesos) y tipologías de riesgos (operacional, financieros, lavado de activos y financiación del terrorismo, fraude y corrupción, continuidad del negocio, seguridad de la información y ciberseguridad, y cualquier otra tipología de riesgos).

b. Para la evaluación de los riesgos se deben emplear mediciones cualitativas o cuantitativas, con base en la información estadísticas obtenida y acorde con la metodología establecida en el presente manual y la documentación que lo soporta.

c. Los responsables de los procesos y/o proyectos deben diseñar y documentar los controles para mitigar los riesgos identificados en los procesos y valorar su efectividad, de acuerdo con la metodología establecida en el presente manual.

- ***Valoración de riesgos***

a. El control de los riesgos se debe efectuar mediante la verificación del cumplimiento de los límites aprobados por la Junta Directiva, los cuales mantienen los niveles de exposición dentro de intervalos tolerables según lo definido por Colpensiones.

b. La Gerencia de Riesgos y Seguridad de la Información y el Oficial de Cumplimiento son los responsables de verificar el cumplimiento de los límites que han sido formulados para el control de los riesgos y de reportar oportunamente cualquier incumplimiento.

c. Los planes de mejoramiento para mitigar los riesgos identificados en un nivel de exposición no tolerado deben ser definidos y liderados por los responsables de los procesos, siendo estos objetos de seguimiento por las áreas de control y la Gerencia de Riesgos y Seguridad de la Información.

- ***Tratamiento de riesgos***

a. Colpensiones, acepta como medida de tratamiento de riesgos la tercerización de operaciones, bajo el entendido de que dicha medida, genera otros riesgos que deben ser identificados y evaluados.

b. Dicha tercerización debe realizarse bajo criterios de seguridad y análisis de costo beneficio para la entidad.

c. La tercerización de actividades y/o procesos implica el desarrollo de al menos las siguientes actividades sobre los proveedores clasificados como críticos:

- Realizar un análisis de riesgo para determinar los procesos y/o actividades a tercerizar.
- Comprender el riesgo asociado a los procesos y/o actividades tercerizadas.
- Contar con políticas eficaces para incorporar en su estrategia de riesgos, aquellos derivados de la tercerización.
- Deben establecerse criterios claros y objetivos, así como los procedimientos para la selección.
- Desarrollar modelos de monitoreo permanente por parte de las tres líneas de defensa.
- Identificar claramente los activos de información involucrados y establecer las condiciones de protección y uso aceptable.
- Definir estrategias de capacitación y comunicación en materia de gestión de riesgos.
- Respecto al SARLAFT, la capacitación con terceros es obligatoria únicamente con los terceros (no empleados de la entidad) cuando sea procedente su contratación en los términos de la Parte I, Título IV, Capítulo IV.
- Establecer acuerdos de servicio claros y sanciones por su incumplimiento.
- Se deben establecer desde la etapa precontractual, las condiciones sobre cómo se puede finalizar el acuerdo, y las disposiciones de continuidad o traspaso de la operación a otro tercero.
- Gestionar los riesgos que se derivan por la prestación del servicio de estos.

d. De igual forma, Colpensiones reconoce en la gestión de seguros, un mecanismo adicional para el tratamiento de los riesgos y la reducción de su impacto sobre los estados financieros de la entidad.

Dado lo anterior, en el establecimiento de un programa de seguros se deben considerar los riesgos de la entidad que son asegurables, las condiciones actuales que ofrece el mercado asegurador y el comportamiento histórico de los riesgos materializados.

e. Colpensiones debe tomar las medidas necesarias para asegurar que los controles asociados al cumplimiento de las condiciones pactadas en las pólizas de seguro se cumplan.

- ***Registro e Informe***

a. El resultado de la etapa de evaluación de riesgos debe quedar documentado y registrado en la matriz de evaluación de riesgos, en sus diferentes niveles: estratégico, táctico y por procesos, esta última establecida para cada uno de los procesos contemplados en la cadena de valor, conservando la trazabilidad y versionamiento de las mismas.

b. El registro de eventos de riesgo se administrará a través de una base de datos consolidada utilizando las herramientas establecidas por Colpensiones, permitiendo la generación de estadísticas e información relevante para la toma de decisiones tanto de los procesos, como de la Entidad.

c. La Gerencia de Riesgos y Seguridad de la Información, la Gerencia de Prevención de Fraude y el Oficial de Cumplimiento deben elaborar reportes periódicos sobre el monitoreo de riesgos realizado.

d. La Vicepresidencia de Seguridad y Riesgos Empresariales, debe generar información periódica sobre la gestión y evolución del perfil de riesgos de Colpensiones a la Alta Dirección y Junta Directiva.

e. La Vicepresidencia de Seguridad y Riesgos Empresariales, debe generar información sobre la gestión integral de riesgos, cuando esta sea requerida, como parte de la rendición de cuentas de Colpensiones a la ciudadanía; así como, a través de los Estados Financieros, en lo que respecta a la revelación contable de eventos de riesgo materializados.

f. La información debe permitir que la Alta Dirección involucre al conjunto de la Entidad en las actividades tanto estratégicas, como tácticas y por procesos, resaltándose su responsabilidad ante la gestión de riesgos y la definición de controles.

g. Los reportes y mecanismos de comunicación que se generen deben permitir que los colaboradores de Colpensiones entiendan su papel en la gestión de riesgos y la identificación de controles, así como su contribución individual en relación con el trabajo de otros.

- ***Seguimiento y Revisión***

a. El monitoreo de los riesgos, los planes de mejoramiento y los indicadores de Colpensiones, deben ser realizados por: - los responsables de los procesos, - la Gerencia de Riesgos y Seguridad de la Información, la Gerencia de Prevención del Fraude, el Oficial de Cumplimiento, la Oficina de Control Interno y por los órganos de control de acuerdo con las funciones y estrategias definidas.

b. La Gerencia de Riesgos y Seguridad de la Información, la Gerencia de Prevención del Fraude y el Oficial de Cumplimiento, deben realizar un análisis de los eventos de riesgo registrados en las herramientas establecidas por la entidad para tal fin. Estos análisis podrán ser empleados como insumos para la toma de decisiones en la mejora de los procesos.

c. Durante las sesiones de trabajo con los líderes de los procesos o sus delegados, se debe realizar seguimiento a la evolución del perfil de riesgo del proceso y los riesgos asociados.

d. La Oficina de Control Interno, como parte de sus funciones de auditoría, debe realizar evaluaciones independientes, relacionadas con el diseño, implementación y efectividad de los controles identificados para los riesgos.

e. La Vicepresidencia de Seguridad y Riesgos Empresariales debe establecer la metodología para evaluar la efectividad de los controles.

f. Colpensiones debe contar con los mecanismos necesarios tales como: herramientas informáticas, políticas y procedimientos para monitorear los cambios en los controles y perfiles de riesgo, y mantener actualizados las matrices y mapas de riesgo y su nivel de exposición.

6.4. PRINCIPIOS Y POLÍTICAS GESTIÓN DE RIESGO DE TERCERAS PARTES

La Entidad ha adoptado como premisa fundamental en el desarrollo de las relaciones con terceras partes un perfil acorde con los objetivos de riesgo / rentabilidad; es por esto, la importancia de contar con una gestión de los riesgos de terceras partes, que esté alineada con los objetivos del negocio y permita mantener continuamente informada a la estructura funcional y administrativa sobre los riesgos que se pueden llegar a materializar por mantener estas relaciones.

Por tal motivo se establecen seis (6) lineamientos los cuales servirán como pilares para el desarrollo de toda la gestión de riesgo de terceras partes:

a. **Implementar la evaluación de riesgo de terceras partes:** La administración fomentará la implementación de un mecanismo de evaluación de riesgo de terceras partes de forma estructurada en toda la Entidad para que su gestión sea consistente con los objetivos estratégicos. Para ello la evaluación de riesgo de terceras partes estará bajo el alcance del Sistema Integral de Administración de Riesgos de Colpensiones.

b. **Definir la estructura organizacional para la gestión de riesgo de terceras partes**: La administración establecerá una estructura organizacional clara, eficaz y robusta, con líneas de responsabilidad bien definidas, transparentes y coherentes. La estructura establecida seguirá el modelo de las tres líneas de defensas.

c. **Gestionar el riesgo de terceras partes:** La administración determinará y administrará el perfil de riesgo de terceras partes de manera precisa, oportuna y eficaz. El perfil incluirá las actualizaciones presentadas por cambios en el tipo de relación con terceros vigentes y en la iniciación de relaciones con nuevos terceros; así como eventos de riesgo, auditorías, informes de entes de control, relacionados con las terceras partes.

d. **Definir el esquema de seguimiento y supervisión al riesgo de terceras partes:** La administración implementará un esquema de monitoreo y tratamiento consistente y periódico sobre el perfil de riesgo de terceras partes. De acuerdo con esto se establecerán flujos de información oportunos y precisos, para propender por una gestión proactiva del riesgo. El Comité Integral de Riesgos, Comité de Auditoría y Comité Institucional de Control Interno, supervisarán la gestión realizada por la administración.

e. **Sensibilización en la gestión de riesgos de terceras partes:** La administración fomentará de manera permanente una cultura en gestión de riesgo en terceras partes que permee en todos los niveles de la entidad. Para ello fomentará un esquema de divulgación sobre los avances en la gestión realizada y definirá e impulsará una comunicación veraz, comprensible y completa entre las áreas de la entidad.

f. **Autocontrol para aplicar el modelo con la debida responsabilidad**: La administración propenderá por el autocontrol, entendido como la capacidad de las personas de considerar el control como parte inherente de sus responsabilidades, campos de acción y toma de decisiones asegurando que se tengan implementados y documentados los controles para mitigar los riesgos de terceros a los que se encuentren expuesta la Entidad.

7. ESTRUCTURA ORGANIZACIONAL

La Junta Directiva provee los recursos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente una estructura organizacional para administrar integralmente los riesgos, asegurando la disponibilidad oportuna de los recursos para el correcto funcionamiento del Sistema.

En Colpensiones la adopción de las políticas para la gestión integral de riesgos inicia desde la Junta Directiva, a través de la cual se define el marco de gestión, los niveles de apetito de riesgos y su estructura.

Las responsabilidades en la gestión integral de riesgos en Colpensiones se establecen bajo el concepto de las tres líneas de defensa como se muestra a continuación:

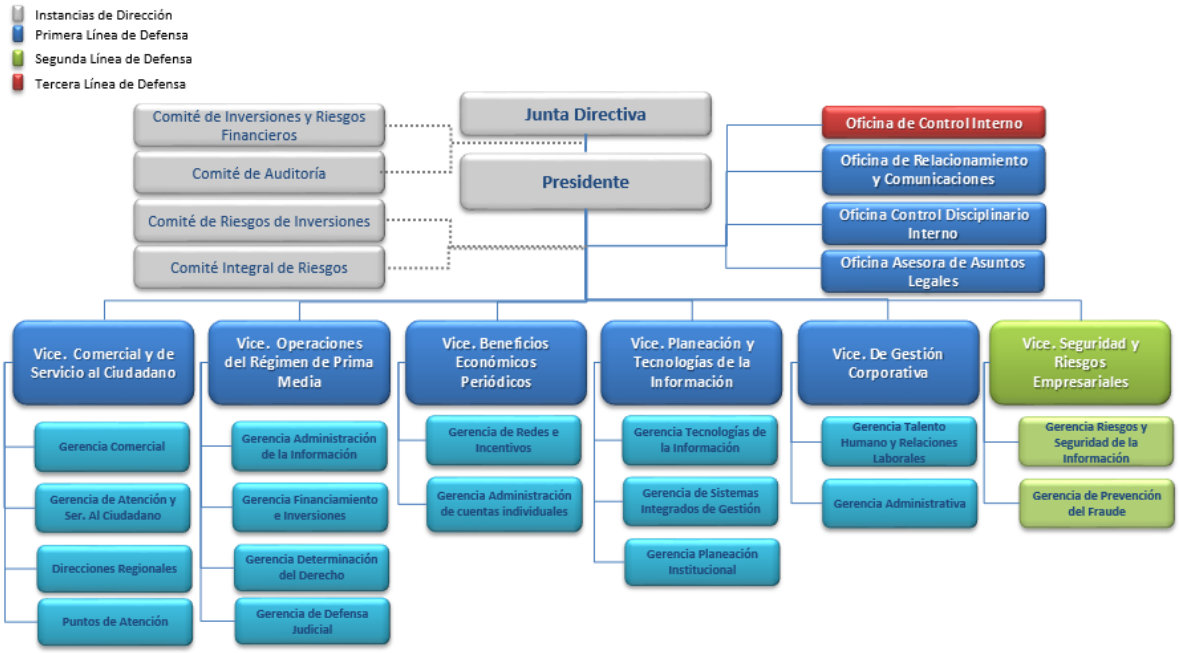


Ilustración 1. Esquema Organizacional Tres Líneas de Defensa

- **Primera Línea de Defensa**

La primera línea de defensa está conformada por las cinco vicepresidencias misionales y de apoyo, y las tres Oficinas, las cuales son las áreas originadoras y propietarias de los riesgos y las primeras llamadas a definir y tomar decisiones en cómo gestionarlos. Estas vicepresidencias son responsables de la implementación de acciones preventivas y correctivas para hacer frente a deficiencias de proceso y control.

Son las áreas responsables de mantener un control interno efectivo y de ejecutar actividades de control sobre los riesgos de manera permanente. Esta línea de defensa es la encargada de identificar, evaluar, analizar y tratar los riesgos a los que se ven expuestos en el desarrollo de sus funciones.

- **Segunda Línea de Defensa**

Función a cargo de la Vicepresidencia de Seguridad y Riesgos Empresariales. Esta línea de defensa busca ayudar a crear y/o monitorear los controles de la primera línea de defensa. Su función se concentra principalmente en los siguientes aspectos:

- Dirigir y coordinar, con las dependencias, la identificación de riesgos por procesos, tácticos, emergentes y estratégicos, evaluando y midiendo la exposición de la Entidad frente a ellos.
- Desarrollar e implementar el marco de gobierno del riesgo en toda la Entidad, que incluye la cultura de riesgo de Colpensiones, políticas, metodologías, su apetito y límites sobre riesgos.
- Realizar un seguimiento continuo de las actividades con aceptación y exposiciones al riesgo en consonancia con el apetito al riesgo, la capacidad de riesgo y el correspondiente marco definido por la Junta Directiva
- Generar indicadores para desarrollar un sistema para monitoreo y activación de alertas tempranas de desviaciones del apetito o la capacidad de riesgo definido en Colpensiones.
- Generar mecanismos de comunicación al interior Colpensiones que permitan informar a Alta Dirección y la Junta Directiva de los riesgos de la Entidad.

- **Tercera Línea de Defensa**

Rol desempeñado por la Oficina de Control Interno. La tercera línea de defensa tiene como principal función, verificar de manera independiente a la primera y segunda línea de defensa, la adecuada gestión de riesgos dentro de la entidad.

De acuerdo con la Circular Externa 038 de 2009 emitida por la Superintendencia Financiera de Colombia, frente a la naturaleza del trabajo de la auditoría interna como tercera línea de defensa, define:

- Gestión de Riesgos: El auditor interno debe evaluar la eficacia del sistema de gestión de riesgos de la organización y las exposiciones al riesgo referidas a gobierno, operaciones y sistemas de información de la organización.
- Sistema de Control Interno: La actividad de auditoría interna debe asistir a la organización en el mantenimiento de controles efectivos, mediante la evaluación de la eficacia y eficiencia de los mismos y promoviendo la mejora continua, sin perjuicio de la autoevaluación y el autocontrol que corresponden a cada funcionario de la organización.

De igual forma, Colpensiones tiene como principio la separación organizacional y funcional de los procesos de negociación (front office), identificación, monitoreo, control y administración de los riesgos (middle office) y cumplimiento y registro contable de las operaciones (back office). Las funciones de cada instancia se encuentran detalladas en la PARTE IV - Sistema de Administración de Riesgo Financieros.

7.1. ROLES Y FUNCIONES

Colpensiones definió la siguiente estructura organizacional, con sus respectivos roles y funciones, para la administración integral de riesgos, así:

7.1.1. JUNTA DIRECTIVA

a. Establecer las políticas relativas al Sistema Integral de Administración de Riesgos, así como las políticas que le aplica de manera particular a cada uno de los sistemas de administración de riesgos que lo componen.

b. Aprobar el Manual del Sistema Integral de Administración de Riesgos, sus partes y actualizaciones.

c. Hacer seguimiento y pronunciarse sobre el perfil de riesgos integral de la entidad, así como el perfil de cada una de las tipologías de riesgos que lo componen.

d. Aprobar las actuaciones, medidas, acciones correctivas, planes de mejoramiento y planes de contingencia establecidos en caso de sobrepasar el nivel de tolerancia o exceder los límites de exposición al riesgo, fijados por la misma Junta Directiva.

e. Hacer seguimiento a las medidas, acciones correctivas o planes de mejoramiento aplicados, para que se cumplan los límites y perfil de riesgo tolerado.

f. Pronunciarse respecto de cada uno de los puntos que contengan los informes periódicos que presente el Representante Legal, el Oficial de Cumplimiento y la Vicepresidencia de Seguridad y Riesgos Empresariales, dejando expresa constancia en la respectiva acta.

g. Pronunciarse sobre los informes presentados por la Revisoría Fiscal y la Oficina de Control Interno, sobre el sistema integral de administración de riesgos, así como de los sistemas que lo componen, y hacer seguimiento a las observaciones o recomendaciones adoptadas, dejando la expresa constancia en la respectiva acta.

h. Ordenar los recursos técnicos y humanos necesarios para implementar y mantener en funcionamiento, de forma efectiva y eficiente, el Sistema Integral de Administración de Riesgos y los sistemas que lo componen.

i. Aprobar y adoptar el Código de Ética y Código de Gobierno Corporativo de Colpensiones.

j. Realizar el nombramiento de los comités de riesgos, definir sus funciones y aprobar su reglamento, de acuerdo con las normas legales que les apliquen.

k. Aprobar la metodología que elabora la Vicepresidencia de Seguridad y Riesgos Empresariales para administrar el riesgo.

l. Efectuar un monitoreo periódico al cumplimiento de los lineamientos del Sistema de Administración de Riesgos financieros y comportamiento del riesgo de mercado.

m. Designar al Oficial de Cumplimiento y su respectivo suplente.

n. Aprobar el procedimiento para la vinculación de los clientes que pueden exponer en mayor grado a la entidad al riesgo de Lavado de Activos y Financiación del Terrorismo - LA/FT, así como las instancias responsables, atendiendo que las mismas involucran funcionarios de la Alta Dirección.

o. Aprobar los criterios objetivos y establecer los procedimientos y las instancias responsables de la determinación y reporte de las operaciones sospechosas.

p. Establecer y hacer seguimiento a las metodologías para la realización de entrevistas no presenciales y/o la realización de entrevistas por personal que no tenga la condición de empleado de la entidad.

q. Aprobar las metodologías de segmentación, identificación, medición y control del SARLAFT.

r. Designar la(s) instancia(s) responsable(s) del diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.

s. Aprobar el Marco de Apetito de Riesgo para Colpensiones y asegurarse que es coherente con los objetivos estratégicos, el modelo de negocio y la capacidad de riesgo.

t. Considerar el apetito de riesgo en el marco de las decisiones y aprobaciones que tome.

u. Evaluar y supervisar, al menos de forma anual, los límites de riesgos y los riesgos asumidos comparándolos con los niveles aprobados.

v. Supervisar el marco de apetito de riesgo con el objetivo de asegurar que se tomen las medidas adecuadas con respecto a niveles no aceptables o de potenciales incumplimientos en los límites de apetito, tolerancia y capacidad de riesgo.

w. Asegurar los recursos adecuados para la función de Gestión Integral de Riesgos, así como para la Auditoría Interna con el fin de dar garantías independientes a la Junta Directiva y la Presidencia de que Colpensiones está operando dentro de marco de apetito de riesgo aprobado.

x. Garantizar que la función de supervisión de Gestión Integral de Riesgos este apoyada en adecuados y sólidos sistemas de información y sistemas de gestión de información para permitir la identificación, medición, evaluación y comunicación de los riesgos de manera oportuna y precisa.

7.1.2. REPRESENTANTE LEGAL

a. Diseñar y someter a aprobación de la Junta Directiva u órgano que haga sus veces, el Manual del Sistema Integral de Administración de Riesgos, sus partes y actualizaciones.

b. Establecer y garantizar el efectivo cumplimiento de las políticas definidas por la Junta Directiva.

c. Adelantar un seguimiento permanente de las etapas y elementos constitutivos del Sistema Integral de Administración de Riesgos.

d. Designar el área o cargo que actuará como responsable de la implementación y seguimiento del Sistema Integral de Administración de Riesgos.

e. Desarrollar y velar porque se implementen las estrategias con el fin de establecer el cambio cultural que la administración integral de riesgos implica para la entidad.

f. Adoptar las medidas relativas al perfil de riesgos, teniendo en cuenta el nivel de tolerancia al riesgo, fijado por la Junta Directiva.

g. Velar por la correcta aplicación de los controles del riesgo inherente, identificado y medido.

h. Recibir y evaluar los informes presentados por la Vicepresidencia de Seguridad y Riesgos Empresariales y Oficial de Cumplimiento, de acuerdo con los términos establecidos en la normatividad vigente.

i. Velar porque las etapas y elementos del Sistema Integral de Administración de Riesgos cumplan, como mínimo, con las disposiciones señaladas en la normatividad vigente.

j. Velar porque se implementen los procedimientos para la adecuada administración integral de riesgos a los que se vea expuesta la entidad en desarrollo de su actividad.

k. Aprobar los planes de contingencia y de continuidad del negocio y disponer de los recursos necesarios para su oportuna ejecución.

l. Presentar un informe periódico, como mínimo semestral, a la Junta Directiva sobre la evolución y aspectos relevantes del Sistema Integral de Administración de riesgos, incluyendo, entre otros, las acciones preventivas y correctivas implementadas o por implementar y el área responsable.

m. Establecer un procedimiento para alimentar el registro de eventos de riesgo, de acuerdo con lo previsto en la normatividad vigente.

n. Velar porque el registro de eventos de riesgos cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

o. Informar oportunamente a la Superintendencia Financiera de Colombia sobre cualquier evento importante que afecte el riesgo operacional de la entidad.

p. Garantizar que las bases de datos y la plataforma tecnológica cumplan con los criterios y requisitos establecidos en la normatividad vigente.

q. Proveer los recursos técnicos y humanos necesarios para implementar y mantener en funcionamiento el Sistema Integral de Administración de Riesgos.

r. Prestar efectivo, eficiente y oportuno apoyo al Oficial de Cumplimiento.

s. Garantizar que los registros utilizados en el SARLAFT cumplan con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

t. Aprobar los criterios, metodologías y procedimientos para la selección, seguimiento y cancelación de los contratos celebrados con terceros para la realización de aquellas funciones relacionadas con el SARLAFT que pueden realizarse por éstos, de acuerdo con lo señalado en la normativida1d vigente.

u. Adelantar un seguimiento permanente del cumplimiento de las funciones de la Vicepresidencia de Seguridad y Riesgos Empresariales con respecto a la gestión de riesgo de mercado y de sus funcionarios y mantener informada a la Junta Directiva.

v. Definir procedimientos a seguir en caso de sobrepasar o exceder los límites de exposición frente al riesgo de mercado, así como los planes de contingencia a adoptar respecto de cada escenario extremo.

w. Hacer seguimiento y pronunciarse respecto de los informes diarios que presente la Vicepresidencia de Seguridad y Riesgos Empresariales sobre las posiciones en riesgo y los resultados de las negociaciones, referente al riesgo de mercado.

x. Hacer seguimiento y pronunciarse respecto de los informes que presente el Revisor Fiscal.

y. Vigilar cuidadosamente las relaciones de los empleados de la Dirección de Inversiones con los clientes o intermediarios, controlando de manera eficiente los conflictos de interés que puedan presentarse.

7.1.3. COMITÉS DE RIESGOS

En concordancia con los Acuerdos y Resoluciones respectivas y todas aquellas normas que las modifiquen, adicionen o complementen, se establecen como comités de apoyo a la gestión integral de riesgos el Comité de Auditoría y el Comité de Inversiones y Riesgos Financieros, como especializados de la Junta Directiva; y el Comité Integral de Riesgos, y el Comité de Riesgos de Inversiones, como Comités de la Alta Dirección. La reglamentación, funciones y demás aspectos inherentes a los mencionados comités se encuentran consagrados en los citados Resoluciones y Acuerdos.

El objetivo de estos Comités es apoyar a la Junta Directiva y a la Presidencia de Colpensiones en la definición, seguimiento, control e implementación de las políticas y lineamientos de la administración integral de los riesgos.

7.1.4. ALTA DIRECCIÓN (PRESIDENTE, VICEPRESIDENTES, JEFES DE OFICINA, GERENTES, DIRECTORES)

a. Establecer un marco de apetito de riesgo adecuado para Colpensiones, consistente con los objetivos estratégicos, el modelo de negocio, así como de los programas de compensación. El marco de apetito de riesgo debe establecer una evaluación prospectiva del perfil de riesgo.

b. Ser responsable de la integridad del marco de apetito de riesgo, incluyendo la identificación oportuna y los protocolos de escalamiento de toma de decisión cuando se deban aumentar los límites de riesgo y de exposiciones materiales.

c. Asegurar, en conjunto con las funciones de Gestión de Riesgos y planeación institucional, que el apetito de riesgos se traduzca adecuadamente en límites de riesgos para los procesos, además que el apetito de riesgos se incorpore en los procesos de toma de decisiones y planeación estratégica.

d. Asegurarse que el marco de apetito de riesgo es implementado por los líderes de procesos a través de la declaración de apetito de riesgos, la cual debe ser consistente con los límites de riesgo específicos.

e. Implementar canales de comunicación del marco de apetito de riesgo a los interesados internos y externos, así como ayudar a crear una cultura de riesgos al interior de Colpensiones.

f. Apoyar a las funciones de Gestión de Riesgos y planeación estratégica en las responsabilidades e incorporación efectiva del marco de apetito de riesgo en los procesos de toma de decisión.

g. Asegurar que la Gestión Operativa tenga procesos adecuados que permita efectivamente, monitorear e informar sobre el perfil de riesgos en relación con los límites de riesgos.

h. Asegurar recursos suficientes para las funciones de Gestión de Riesgos y Auditoría Interna, así como para desarrollar y mantener la infraestructura tecnológica que ayude a proporcionar una supervisión del marco de apetito de riesgo.

i. Actuar de manera oportuna para asegurar la gestión eficaz y el estado de mitigaciones necesarias de las exposiciones de riesgo materiales, en particular los que están cerca o superan el marco de apetito de riesgo aprobado y/o los límites de riesgo.

j. Establecer una política para la notificación de la Junta Directiva y de los supervisores en materia de incumplimientos de los límites de riesgo y exposiciones de riesgo material.

7.1.5. VICEPRESIDENCIA DE SEGURIDAD Y RIESGOS EMPRESARIALES

a. Definir los instrumentos, metodologías y procedimientos tendientes a que la entidad administre efectivamente sus riesgos, en concordancia con los lineamientos, etapas y elementos mínimos previstos en la normatividad vigente.

b. Asesorar a la Junta Directiva y al Representante Legal, en materia de gestión de riesgos por medio de la realización de capacitaciones, informes periódicos, documentos de sensibilización, entre otros.

c. Desarrollar e implementar el sistema de reportes, internos y externos, de los riesgos de la entidad.

d. Administrar el registro de eventos de riesgo.

e. Coordinar la recolección de la información para alimentar el registro de eventos de riesgo.

f. Evaluar la efectividad de las medidas de control potenciales y ejecutadas para los riesgos medidos.

g. Establecer y monitorear el perfil de riesgo de la entidad e informarlo al órgano correspondiente, en los términos del presente manual.

h. Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con la administración integral de riesgos y proponer sus correspondientes actualizaciones y modificaciones.

i. Desarrollar y actualizar los modelos de medición de los riesgos.

j. Desarrollar los programas de capacitación de la entidad relacionados con el Sistema Integral de Administración de Riesgos.

k. Realizar seguimiento a las medidas adoptadas para mitigar el riesgo inherente, con el propósito de evaluar su efectividad.

l. Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados y el monitoreo que se realice sobre el mismo, en los términos de la normatividad vigente.

m. Evaluar los límites de riesgo de mercado por líneas de negocios (RPM, BEPS, Administradora), operaciones y funcionarios, y presentar al comité de riesgos de inversiones o, en su defecto, a la Junta Directiva, las observaciones o recomendaciones que considere pertinentes.

n. Objetar la realización de aquellas operaciones que no cumplan con las políticas y/o límites de riesgo establecidas por la entidad, en lo referente a la gestión de riesgo de mercado.

o. Informar al comité de riesgos de inversiones o en su defecto a la Junta Directiva sobre los siguientes aspectos de la gestión de riesgo de mercado:

- La exposición al riesgo de manera global de la entidad, así como la específica de cada línea de negocio. Los informes sobre la exposición de riesgo incluyen un análisis de sensibilidad y pruebas bajo condiciones extremas.
- Las desviaciones presentadas con respecto a los límites de exposición de riesgo establecidos.
- Operaciones objetadas teniendo en cuenta lo establecido en el literal n)) del presente numeral.

p. Informar diariamente al Representante Legal y a los responsables de las líneas de negocios, sobre el comportamiento del riesgo de mercado de la entidad, así como las operaciones objetadas de que trata el literal m) del presente numeral.

q. Informar semanalmente al Representante Legal y a los responsables de las líneas de negocios sobre los niveles de riesgo y condiciones de las negociaciones realizadas y, en particular, reportar incumplimientos sobre los límites, operaciones poco convencionales o por fuera de las condiciones de mercado. Este mismo reporte se presenta mensualmente a la Junta Directiva.

r. Definir y ejecutar un plan de visita a terceros críticos de la entidad con el ánimo de determinar si el ambiente de control empleado por los mismos mitiga adecuadamente los riesgos a los que se

podría enfrentar Colpensiones por un desarrollo inadecuado de las actividades ejecutadas por estos.

s. Desarrollar un marco de apetito de riesgo adecuado para Colpensiones en colaboración con la Presidencia acorde a las necesidades y objetivos estratégicos.

t. Obtener la aprobación de la Junta Directiva sobre el marco de apetito de riesgo e informar al menos una vez al semestre sobre el perfil de riesgo de Colpensiones.

u. Monitorear de forma activa el perfil de riesgo de Colpensiones en relación con el marco de apetito de riesgo, estrategia, tolerancia y capacidad de riesgos.

v. Establecer un proceso para informar sobre la evolución del perfil de riesgo, cultura de riesgo y su alineación con el apetito de riesgo.

w. Garantizar las técnicas de medición de riesgos y del sistema de información gerencial utilizados para controlar el perfil de riesgo de Colpensiones en relación con su marco de apetito de riesgo.

x. Establecer y aprobar, en colaboración con la Presidencia, la Vicepresidencia de Planeación y Tecnología y líderes de procesos los límites de riesgo apropiados para los procesos, los cuales sean consistentes con la declaración de apetito de riesgo.

y. Monitorear de forma independiente los límites de riesgo de los procesos, además del perfil de riesgo agregado de Colpensiones para garantizar que sean consistentes con el marco de apetito de riesgo.

z. Actuar de manera oportuna para garantizar la gestión efectiva y, cuando sea necesario, la mitigación de las exposiciones de riesgo importantes, en particular los que se acerquen o superen el apetito de riesgo y/o los límites de riesgo aprobados.

aa. Escalar a la Junta Directiva y a la Presidencia cualquier incumplimiento de los límites de riesgos, que coloquen a Colpensiones en riesgo de exceder su apetito de riesgo.

7.1.6. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

a. Proponer y ejecutar la metodología de gestión de riesgos de seguridad de la información y Ciberseguridad, alineada con la metodología integral de gestión de riesgos de Colpensiones.

b. Realizar el perfil de riesgos de Seguridad de la Información y Ciberseguridad en Colpensiones.

c. Definir los mecanismos de control y seguimiento que permitan medir el nivel de cumplimiento de las Políticas de Seguridad de la Información y Ciberseguridad.

d. Definir las necesidades de formación y capacitación de los servidores de la empresa en referencia con la seguridad de la información y la ciberseguridad.

e. Realizar seguimiento a los eventos de seguridad internos y externos, con el propósito de identificar posibles ataques cibernéticos contra la entidad.

f. Reportar al menos semestralmente a la Junta Directiva a través del Comité Integral de Riesgos los resultados de la Gestión de Seguridad de la Información y Ciberseguridad, especialmente en la identificación de riesgos y ciberamenazas, resumen de la gestión a incidentes de ciberseguridad y propuestas de mejora en materia de Seguridad de la Información y Ciberseguridad.

g. Asesorar a la Junta Directiva en temas que considere necesarios sobre seguridad de la información y ciberseguridad para que pueda hacer seguimiento y tomar las decisiones adecuadas en esta materia.

Este Rol estará a cargo del Vicepresidente de Seguridad y Riesgos Empresariales, y su suplente es el Gerente de Riesgos y Seguridad de la Información.

7.1.7. OFICIAL DE CUMPLIMIENTO

a. Velar por el efectivo, eficiente y oportuno funcionamiento de las etapas que conforman el SARLAFT.

b. Presentar, cuando menos en forma trimestral, informes presenciales y escritos a la junta directiva u órgano que haga sus veces, en los cuales debe referirse como mínimo a los siguientes aspectos:

Los resultados de la gestión desarrollada.

- El cumplimiento que se ha dado en relación con el envío de los reportes a las diferentes autoridades.
- La evolución individual y consolidada de los perfiles de riesgo de los factores de riesgo y los controles adoptados, así como de los riesgos asociados.
- La efectividad de los mecanismos e instrumentos establecidos en el presente Capítulo, así como de las medidas adoptadas para corregir las fallas en el SARLAFT.
- Los resultados de los correctivos ordenados por la junta directiva u órgano que haga sus veces.
- Los documentos y pronunciamientos emanados de las entidades de control y de la UIAF.

c. Promover la adopción de correctivos al SARLAFT.

d. Coordinar el desarrollo de programas internos de capacitación.

e. Proponer a la administración la actualización del manual de procedimientos y velar por su divulgación a los funcionarios.

f. Colaborar con la instancia designada por la junta directiva en el diseño de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico para la oportuna detección de las operaciones inusuales.

g. Evaluar los informes presentados por la auditoría interna o quien ejecute funciones similares o haga sus veces, y los informes que presente el revisor fiscal y adoptar las medidas del caso frente a las deficiencias informadas.

h. Diseñar las metodologías de segmentación, identificación, medición y control del SARLAFT.

i. Elaborar y someter a la aprobación de la junta directiva o el órgano que haga sus veces, los criterios objetivos para la determinación de las operaciones sospechosas, así como aquellos para determinar cuáles de las operaciones efectuadas por usuarios serán objeto de consolidación, monitoreo y análisis de inusualidad.

j. Realizar y garantizar la reserva de los reportes de operaciones sospechosas remitidos a la UIAF.

k. Cumplir las obligaciones relacionadas con sanciones financieras dirigidas, establecidas en el Capítulo de la Circular Básica Jurídica.

No pueden contratarse con terceros las funciones asignadas al Oficial de Cumplimiento, ni aquellas relacionadas con la identificación y reporte de operaciones inusuales, así como las relacionadas con la determinación y reporte de operaciones sospechosas.

Este rol estará a cargo de quién designe la Junta Directiva y autorice la Superintendencia Financiera de Colombia, previa verificación del cumplimiento de los siguientes requisitos:

a. Ser como mínimo de segundo nivel jerárquico dentro de la entidad.

b. Tener capacidad decisoria.

c. Acreditar conocimiento en materia de administración del riesgo de LA/FT de mínimo ciento cincuenta (150) horas a través de especialización, cursos, diplomados, seminarios, congresos o cualquier otra similar, incluyendo pero sin limitarse a cualquier programa de entrenamiento que sea o vaya a ser ofrecido por la UIAF a los actores del sistema nacional antilavado de activos y contra la financiación del terrorismo, en los términos que señale la entidad.

d. Acreditar un título profesional.

e. Demostrar experiencia mínima de veinticuatro (24) meses en el desempeño de cargos relacionados con la administración de riesgos.

f. Estar apoyado por un equipo de trabajo humano y técnico, de acuerdo con el riesgo de LA/FT y el tamaño de la entidad.

g. No pertenecer a órganos de control ni a las áreas directamente relacionadas con las actividades previstas en el objeto social principal.

h. Ser empleado de la entidad.

i. Estar posesionado ante la Superintendencia Financiera de Colombia.

El oficial de cumplimiento suplente debe cumplir como mínimo, los requisitos establecidos en los literales del b. al i.

7.1.8. UNIDAD DE PREVENCIÓN DEL RIESGO LAVADO DE ACTIVOS Y FINANCIACIÓN DEL TERRORISMO (LAFT)

La Junta Directiva provee los recursos humanos que conformarán la Unidad de Prevención del riesgo de Lavado de Activos y Financiación del Terrorismo (LAFT).

Esta Unidad tiene, entre otras, las siguientes funciones:

a. Liderar el Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo –SARLAFT- a nivel institucional, en los aspectos normativos, metodológicos y tecnológicos, proponiendo las acciones requeridas para el mejoramiento continuo del Sistema.

b. Analizar las señales de alerta, las operaciones inusuales y presentar al Oficial de Cumplimiento las razones objetivas para la determinación de operaciones sospechosas.

c. Proponer al Oficial de Cumplimiento la definición de señales de alerta, tipologías de lavado de activos y financiación del terrorismo, criterios objetivos para la determinación de operaciones inusuales y sospechosas.

d. Proponer al Oficial de Cumplimiento el diseño de las metodologías de segmentación y los mecanismos para el conocimiento del mercado y la consolidación electrónica de operaciones.

e. Acompañar a los responsables de los procesos, en conjunto con la Gerencia de Riesgos y Seguridad de la Información, en la identificación de riesgos, causas, diseño de controles y evaluación o medición de los riesgos de lavado de activos y financiación del terrorismo asociados a los procesos.

f. Atender los requerimientos de las autoridades y auditorías de los entes de control interno y externo relativas al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo –SARLAFT-, proponiendo los planes de acción o mejoramiento, cuando haya lugar.

g. Elaborar los informes relativos al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo –SARLAFT-.

h. Diseñar e implementar las estrategias de capacitación relativas al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo –SARLAFT-.

7.1.9. LÍDERES DE PROCESOS

a. Aplicar los instrumentos, metodologías y/o procedimientos definidos en el presente manual, sus partes y anexos, administrando efectivamente los riesgos en cada uno de los procesos a su cargo.

b. Identificar, analizar, evaluar, tratar y monitorear los riesgos en cada uno de los procesos a su cargo, a través de la metodología y herramientas establecidas para tal fin, con el apoyo de la Vicepresidencia de Seguridad y Riesgos Empresariales.

c. Diseñar y documentar los controles existentes para mitigar los riesgos de sus procesos, asegurando la efectividad de los mismos.

d. Generar mecanismos [1] periódicos que le permitan evaluar:

- Si el diseño del control es el adecuado para cumplir con los objetivos del proceso
- Si el control se ejecuta de la manera en que fue diseñado y logra su objetivo.

e. Establecer las acciones correctivas o preventivas necesarias, que permitan mitigar los riesgos y dar cumplimiento a los objetivos establecidos en el proceso.

f. Promover y gestionar al interior de sus procesos el adecuado registro de los eventos de riesgo, así como el reporte de las pérdidas generadas de los mismos, de acuerdo con la metodología definida y en las herramientas establecidas para este fin.

[1] Los mecanismos puedes ser: Comités primarios, Análisis de los indicadores del proceso, Análisis de los eventos de riesgo presentados, Grupos de calidad, entre otros.

g. Asegurar la calidad e integridad de la información fuente para el registro contable de los eventos de riesgo con pérdida económica.

h. Divulgar y socializar al interior de sus áreas los mapas de riesgo de sus procesos.

i. Ser responsable de la gestión eficaz del apetito de riesgo dentro de su proceso.

j. Asegurar la alineación entre el apetito de riesgo, objetivos estratégicos y los procesos de toma de decisiones.

k. Integrar el marco de apetito de riesgo y los límites de apetito de riesgo en sus actividades con el fin de integrar la cultura de gestión de riesgos en la gestión diaria de riesgos.

l. Establecer y supervisar activamente el engrane e implementación a los límites de riesgo aprobados para Colpensiones.

m. Cooperar con la Vicepresidencia de Seguridad y Riesgos Empresariales, cuando se requiera evaluar como el marco de apetito de riesgo ha sido incorporado en la gestión de sus procesos.

n. Aplicar controles y procesos para poder identificar con eficacia, monitorear e informar los incumplimientos de los límites de riesgo asignados.

o. Actuar de manera oportuna para asegurar una gestión eficaz, y cuando sea necesario, la mitigación de las exposiciones a riesgos, en particular los que superan o tienen el potencial de sobrepasar el nivel de apetito de riesgo aprobado y/o los límites de niveles de riesgo.

p. Escalar de forma oportuna los incumplimientos en los límites de riesgo y las exposiciones importantes a la Vicepresidencia de Seguridad y Riesgos Empresariales y al Presidente, si diera lugar.

q. Realizar un análisis de riesgo para determinar los procesos y/o actividades a tercerizar.

r. Comprender el riesgo asociado a los procesos y/o actividades tercerizadas.

s. Contar con políticas eficaces para incorporar en su estrategia de riesgos, aquellos derivados de la tercerización.

t. Administrar los riesgos identificados para los terceros con los que el proceso maneja alguna relación contractual.

u. Verificar la ejecución de planes de tratamiento y mejora de los controles definidos para mitigar los riesgos identificados de terceros.

v. Aplicar el modelo de gestión de riesgos de Terceras Partes cuando se esté en proceso de consecución, selección y vinculación de un nuevo tercero.

w. Reportar a través del mecanismo de registro de eventos de riesgo establecido por la entidad, toda situación que pueda desviar el cumplimiento del objeto contractual, en la administración de terceras partes.

7.1.10. GESTORES INTEGRALES

El rol de Gestor Integral deberá cumplir con las siguientes competencias:

- Conocer el contexto completo de los procesos a gestionar.
- Contar con la capacidad de comunicación, para relacionarse con miembros del equipo u otros equipos para llevar a cabo la gestión.

El rol de Gestor Integral designado para cada proceso debe cumplir con las siguientes actividades, sin que esto exima la responsabilidad que le compete al Líder del Proceso en la gestión de riesgos:

a. Soportar al líder del proceso en el análisis, identificación y evaluación de los riesgos a los cuales están expuestos los procesos a cargo y su permanente actualización.

b. Realizar la documentación, monitoreo y evaluación de la efectividad de los controles diseñados, aplicando la metodología establecida por la Entidad.

c. Analizar y hacer el seguimiento del perfil de riesgo del proceso, escalando de forma oportuna los incumplimientos en los límites de riesgo y las exposiciones importantes al responsable del proceso y a la Vicepresidencia de Seguridad y Riesgos Empresariales.

d. Participar de la formulación de los indicadores de riesgo y coordinar la medición y seguimiento al reporte de los mismos.

e. Revisar periódicamente las exposiciones al riesgo con los terceros contratistas que soporten la operación del proceso.

f. Liderar la documentación y actualización de las herramientas de continuidad del negocio al interior de los procesos.

g. Liderar la documentación y actualización de las herramientas de seguridad de la información al interior de los procesos a cargo.

h. Articular y fomentar en el equipo de trabajo el reporte de situaciones conocidas que expongan al proceso y a la Entidad a potenciales riesgos, como: eventos de riesgo (operacional, seguridad de la información, continuidad del negocio), presuntos hechos de fraude y corrupción, señales de alerta de lavado de activos y financiación del terrorismo, entre otros.

i. Monitorear y reportar la gestión de los eventos de riesgo relacionados con los procesos a cargo, a través de las herramientas establecidas en la Entidad.

j. Soportar al líder del proceso en la documentación, seguimiento y reporte de los planes de mejoramiento establecidos en función de la gestión de riesgos.

k. Ser multiplicador y coordinar el plan de capacitación anual en Gestión Integral de Riesgos, para los servidores y colaboradores que soportan la ejecución de los procesos asignados.

l. Cooperar con la Vicepresidencia de Seguridad y Riesgos Empresariales en el mejoramiento continuo y efectivo de la gestión de riesgos.

7.1.11. DEBERES DE CUMPLIMIENTO DE LOS SERVIDORES PÚBLICOS Y COLABORADORES DE COLPENSIONES

Todos los servidores públicos y colaboradores de Colpensiones deben cumplir con:

a. El Código de Ética de Colpensiones.

b. El Manual del Sistema Integral de Administración de Riesgos, sus partes y anexos.

c. Comunicar cualquier problema que se presente en la ejecución de sus actividades, en cumplimiento de normas o posibles faltas al Código de Ética, así mismo, ejecutar las actividades asignadas en el Manual de Perfiles y Funciones tomando acciones necesarias para su control.

d. Reportar los eventos de riesgo una vez ocurridos o conocidos en el desarrollo de sus actividades, de acuerdo con la metodología definida y en las herramientas establecidas para este fin.

e. Informar al Oficial de Cumplimiento sobre cualquier señal de alerta de Lavado de Activos y Financiación del Terrorismo - LA/FT que evidencien en el desarrollo de sus funciones, o cualquier modalidad que se esté utilizando con el fin de realizar operaciones ilícitas y proponer nuevos mecanismos de control.

f. Informar al Oficial de Cumplimiento sobre cualquier operación inusual de la que tengan conocimiento.

g. Atender los requerimientos y solicitudes que les haga el Oficial de Cumplimiento y la Vicepresidencia de Seguridad y Riesgos Empresariales, y colaborar para el buen funcionamiento del Sistema Integral de Administración de Riesgos.

h. Participar activamente en los programas de formación establecidos, en el ámbito de la gestión de riesgos de Colpensiones.

7.1.12. ÓRGANOS DE CONTROL

Los órganos de control son los responsables de la evaluación del Sistema Integral de Administración de Riesgos. Estas instancias informan de manera oportuna los resultados a los órganos competentes.

7.1.12.1. Revisoría Fiscal

a. Realizar un reporte al cierre de cada ejercicio contable, en el que informe las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el Sistema Integral de Administración de Riesgos.

b. Poner en conocimiento del Representante Legal los incumplimientos del Sistema Integral de Administración de Riesgos, sin perjuicio de informar sobre ellos a la Junta Directiva u órgano que haga sus veces.

c. Elaborar un reporte trimestral dirigido a la junta directiva u órgano que haga sus veces, en el que informe acerca de las conclusiones obtenidas en el proceso de evaluación del cumplimiento de las normas e instructivos sobre el SARLAFT. Además, debe poner en conocimiento del oficial de cumplimiento las inconsistencias y fallas detectadas en el SARLAFT y, en general, todo incumplimiento que detecte a las disposiciones que regulan la materia.

d. Reportar operaciones sospechosas a la UIAF, en cumplimiento de lo establecido en la Parte I, Título IV, Capítulo IV de la Circular Básica Jurídica de la Superintendencia Financiera de Colombia. Para tal efecto, debe registrarse en la plataforma Sistema de Reporte en Línea (SIREL), administrado por la UIAF o cualquier otro sistema que dicha entidad desarrolle para el reporte de operaciones sospechosas.

e. Las demás definidas en el marco normativo actual.

7.1.12.2. Oficina de Control Interno

a. Evaluar periódicamente la efectividad y cumplimiento de todas y cada una de las etapas y los elementos del Sistema Integral de Administración de Riesgos con el fin de determinar las deficiencias y sus posibles soluciones. El resultado de su evolución se informa a la Junta Directiva, al Representante Legal, a la Vicepresidencia de Seguridad y Riesgos Empresariales, y al Oficial de

Cumplimiento, según sea el caso y acorde con la normatividad aplicable a cada uno de los Sistemas de Administración de Riesgos.

b. La Oficina de Control Interno, debe realizar una revisión periódica de los procesos relacionados con las exoneraciones y parametrizaciones de las metodologías, modelos e indicadores cualitativos y/o cuantitativos de reconocido valor técnico.

c. Realizar una revisión periódica del registro de eventos de riesgo, mínimo una vez al año, e informar al Representante Legal sobre el cumplimiento de las condiciones señaladas en la normatividad vigente.

d. Incluir en los planes de auditoria las evaluaciones del marco de apetito de riesgo, así como en los procesos analizados.

e. Identificar si los incumplimientos en los límites de riesgo están siendo debidamente identificados y reportados, e informar sobre la aplicación del marco de apetito de riesgo a la Junta Directiva y a la Presidencia, según corresponda.

f. Evaluar de forma independiente y periódicamente el diseño y la eficacia del marco de apetito de riesgo y su alineación con los objetivos estratégicos de Colpensiones.

g. Evaluar la eficacia en la aplicación del marco de apetito de riesgo, incluyendo la vinculación con la cultura de riesgos, así como en la planificación estratégica y en los procesos de toma de decisiones.

h. Evaluar el diseño y la efectividad de las técnicas de medición de riesgos y del sistema de gestión de la información usado para monitorear el perfil de riesgo en relación con su apetito por el riesgo.

i. Las demás definidas en el marco normativo actual.

8. CLASIFICACIÓN DE RIESGOS

El Sistema Integral de Administración de Riesgos de Colpensiones, clasifica sus riesgos desde dos puntos de vista así:

- Considerando el contexto sobre el cual se identifican y evalúan los riesgos:

    - **Riesgos estratégicos:** Corresponde a toda situación o evento actual o futuro, ya sea ocasionado por las debilidades internas (Riesgos Estratégicos Internos) o las amenazas externas (Riesgos Estratégicos Externos o Emergentes) que afecte o pueda afectar el logro de los objetivos institucionales.

- **Riesgos Tácticos**: Corresponde a los eventos o situaciones que pueden afectar de forma adversa el cumplimiento de los objetivos de los proyectos y planes de acción definidos para alcanzar metas de corto plazo.

- **Riesgos Por Procesos:** Corresponden a los eventos o situaciones que pueden afectar a el cumplimiento de los objetivos de los procesos del negocio.

- Considerando la tipología de riesgos y los factores que los materializan:

Riesgo Operacional	Posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuado funcionamiento de los procesos, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos. Esta definición incluye el riesgo legal asociado a tales factores.
Riesgo de Continuidad del Negocio	Interrupción del negocio a causa de la Indisponibilidad del recurso humano, la infraestructura tecnológica o infraestructura física necesaria para el normal desarrollo de las operaciones.
Riesgo de Fraude y Corrupción	**Riesgo de Corrupción**: Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. **Riesgo de Fraude**: Posibilidad de pérdida a causa de una acción u omisión intencional realizada con el fin de obtener un provecho económico ilícito y/o beneficio, en detrimento de los intereses de la entidad o de un tercero.
Riesgo de Seguridad de la Información y Ciberseguridad	Posibilidad que los activos de información de la entidad se vean afectados por la ocurrencia de eventos que comprometan la confidencialidad, integridad y disponibilidad de la información, mediante la explotación de vulnerabilidades producto de la inexistencia o ineficacia de los controles implementados para la protección y resguardo de ésta, incluyendo los activos expuestos al ciberespacio.
Riesgo de Lavado de Activos y Financiación del Terrorismo	Posibilidad de pérdida o daño que puede sufrir la entidad por su propensión a ser utilizada directamente o a través de sus operaciones como instrumento para el lavado de activos y/o canalización de recursos hacia la realización de actividades terroristas, o cuando se pretenda el ocultamiento de activos provenientes de dichas actividades.
Riesgos Financieros	Los riesgos financieros los que está expuesta Colpensiones se clasifican en tres tipologías, así: • **Riesgos de Mercado**: Es la posibilidad de que Colpensiones incurran en pérdidas asociadas a la disminución del valor de sus portafolios, por efecto de cambios en el precio de los

	instrumentos financieros en los cuales se mantienen posiciones dentro o fuera del balance. • **Riesgos de Liquidez:** Es la contingencia de no poder cumplir plenamente, de manera oportuna y eficiente los flujos de caja esperados e inesperados, vigentes y futuros, sin afectar el curso de las operaciones diarias o la condición financiera de la entidad. Esta contingencia (riesgo de liquidez de fondeo) se manifiesta en la insuficiencia de activos líquidos disponibles para ello y/o en la necesidad de asumir costos inusuales de fondeo. A su turno, la capacidad de las entidades para generar o deshacer posiciones financieras a precios de mercado, se ve limitada bien sea porque no existe la profundidad adecuada del mercado o porque se presentan cambios drásticos en las tasas y precios (riesgo de liquidez de mercado). • **Riesgo de Contraparte:** Es la posibilidad de que Colpensiones incurra en pérdidas y disminuya el valor de sus activos como consecuencia del incumplimiento de un Emisor o una Contraparte, eventos en los cuales deberá atender el incumplimiento con sus propios recursos o materializar una pérdida en su balance.

Tabla 1. Tipologías de Riesgos

9. MARCO INTEGRAL DE APETITO DE RIESGOS Y AGREGACIÓN DE RIESGOS

9.1. MARCO INTEGRAL DE APETITO DE RIESGO

El marco de apetito de riesgo definido es la guía de actuación y toma de decisiones por parte de la Junta Directiva y de la Alta Dirección, influyendo en la forma de operar de Colpensiones y en la cultura respecto a la gestión de los riesgos. Este marco contempla el conjunto de políticas, metodologías, procedimientos, controles y límites a partir del cual Colpensiones establece, comunica y monitorea el nivel de apetito por el riesgo.

El apetito de riesgo es parte de la gestión integral de riesgos, es un elemento esencial que permite alinear las acciones de la planeación estratégica, el modelo de negocio, el sistema integrado de gestión y la gestión de riesgos, contrastando los riesgos a los que Colpensiones se ve expuesta con aquellos que desea asumir.

En este sentido, se desarrolla en el presente numeral el marco de apetito de riesgo de Colpensiones, el cual contempla los lineamientos, roles y responsabilidades y desarrollo metodológico, lo cual permitirá facilitar la toma de decisiones por parte de la Junta Directiva y la Alta Dirección, en una adecuada comunicación y fortaleciendo la cultura en gestión de riesgos.

9.1.1. Objetivo del Marco Integral de Apetito de Riesgo

El objetivo del Marco de Apetito de Riesgo es ser el enlace entre el marco estratégico, el modelo de negocio, el sistema integral de administración de riesgos y la gestión operativa. Este marco proporciona un conjunto integrado de principios y medidas que le permiten a Colpensiones determinar los tipos de riesgos que desea asumir y el tratamiento.

9.1.2. Alcance del Marco Integral de Apetito de Riesgo

Dentro de la estructura de gestión integral de riesgo, el sistema contempla consideraciones estratégicas, cualitativas y cuantitativas en la determinación de los niveles de apetito, tolerancia y capacidad de riesgo, donde se tendrán en cuenta algunos aspectos.

a. Ser consistente con los objetivos estratégicos de Colpensiones, así como con la identificación, medición, control y monitoreo de riesgos y de la operación diaria.
b. Asegurar que las exposiciones a los niveles de riesgos sean consistentes con el apetito de riesgo y sus correspondientes límites.
c. Ser transversal a toda la entidad, entendido desde un punto de vista de administración de riesgos y gestión operativa, con el objetivo de ajustarse a las actividades y operaciones.
d. Definir objetivos, metodologías, modelos, controles, límites y procedimientos frente a los niveles y tipos de riesgo que Colpensiones está dispuesta a asumir a nivel agregado y por cada una de las actividades que desarrolle.
e. Incluir mediciones cualitativas y cuantitativas de los niveles de riesgo que Colpensiones está dispuesta a asumir y aquellos que esté dispuesto a evitar y/o transferir.
f. Incluir en el análisis mediciones prospectivas que permitan a Colpensiones evaluar la capacidad de gestionar riesgos emergentes.
g. Ser parte integral del proceso de toma de decisiones y de la evaluación y seguimiento de los niveles riesgo que realiza la entidad.
h. Ser difundido y comprendido por toda la organización y estar inmerso en la cultura de riesgo de Colpensiones.
i. Contar con adaptabilidad ante cambios en las condiciones financieras y operativas de Colpensiones, el entorno macroeconómico y los mercados, considerando escenarios normales y adversos.
j. Contar con una declaración de apetito de riesgo, adecuadamente soportada y documentada.

9.1.3. Funciones y Responsabilidades en el Marco Integral de Apetito de Riesgo

Los órganos que hacen parte integral de la estructuración, definición y seguimiento de los niveles de apetito, tolerancia y capacidad de riesgo en Colpensiones son la Junta Directiva, la Presidencia, el Vicepresidente de Planeación y Tecnologías de la Información y el Vicepresidente de Seguridad y Riesgos Empresariales. Las responsabilidades en la definición, implementación y seguimiento de

Marco de Apetito de Riesgo se encuentran contempladas en el numeral 7.1. – ROLES Y FUNCIONES, del presente Manual.

9.1.4. Definición del Marco Integral de Apetito de Riesgo

El Sistema Integral de Administración de Riesgos tiene como base fundamental el Plan Estratégico Institucional - PEI, sobre el cual se establece y define el Marco Integral de Apetito de Riesgo, contemplando las diferentes tipologías de riesgos: operacional, continuidad del negocio, fraude y corrupción, financieros, seguridad de la información y ciberseguridad, lavado de activos y financiación del terrorismo.

En la definición del apetito de riesgo en Colpensiones, se evalúan aspectos tanto cualitativos, como cuantitativos, así:

9.1.4.1. Declaración Cualitativa de Apetito de Riesgos

La declaración de apetito de riesgo corresponde a las afirmaciones cualitativas que enmarcan el actuar de Colpensiones en el desarrollo de sus actividades y definen con claridad, al menos los siguientes aspectos:

- Los riesgos que está dispuesta asumir en el desarrollo de su objeto.
- Las consideraciones de riesgos que se deberán tener en cuenta en los diferentes tipos de decisiones.
- Los aspectos que prevalecen sobre otros cuando ellos se vean enfrentados.

De forma general, Colpensiones tiene como objetivo mantener como máximo nivel de exposición un perfil de riesgo residual en nivel “Medio Bajo” de acuerdo con su metodología de valoración. Considerando lo anterior, sobre los riesgos que, una vez aplicados los controles, permanecen en los niveles de severidad “Alto” y “Medio Alto”, los responsables de los procesos deben implementar medidas de tratamiento para mantener los controles en los límites aceptados. Los riesgos ubicados en niveles “Medio Bajo “y “Bajo”, deben ser objeto de monitoreo y seguimiento dentro de la gestión normal del proceso.

Así las cosas, y partiendo del Plan Estratégico Institucional de la entidad y de su modelo de negocio, a continuación, se presentan las afirmaciones cualitativas que deberá considerar la Junta Directiva, la Alta Dirección, los líderes de proceso y en general, todos los colaboradores de la entidad, en la toma de decisiones y en el desarrollo de las actividades de Colpensiones:

Con relación a los ciudadanos:

- Los ciudadanos son la principal razón de ser de la entidad. Es por lo que se debe prestar especial atención a aquellos riesgos que los puedan impactar de forma directa, dando prioridad a la identificación, valoración y monitoreo de estos.
- Se deberán diseñar controles eficaces con relación a toda la información que se divulgue a los ciudadanos buscando:

  - Asegurar la completitud y claridad de esta, con el fin de que el ciudadano pueda tomar decisiones suficientemente informado.
  - Proteger su integridad y confidencialidad, en los casos en que se requiera.
  - Debe ser informada y divulgada oportunamente.

  Dichos controles deben mantenerse sea que la misma sea suministrada por canales propios o a través de terceros.

- Las denuncias de fraude y corrupción que sean reportadas por los ciudadanos deberán ser atendidas de manera diligente, estableciendo tiempos máximos para su gestión e investigación.

En el desarrollo de sus operaciones:

- Colpensiones analiza e identifica los riesgos que pueden afectar el normal desempeño de sus operaciones, implementando controles que mitiguen su materialización.
- La oportunidad y la calidad en el desarrollo de las operaciones de Colpensiones son características esenciales. Es por ello, que estas dos características deben ser monitoreadas permanentemente informando oportunamente a los líderes de proceso, Alta Dirección y Junta Directiva, según corresponda, las desviaciones que se presenten frente al estándar definido por la entidad.
- Colpensiones espera que sus colaboradores reporten, todos aquellos eventos que puedan comprometer el desarrollo normal de sus operaciones, en especial, aquellos que puedan o generar pérdida económica para la misma. Ocultar información al respecto, se considera una falta grave por parte del colaborador que lo realice.
- La seguridad de los sistemas de información utilizados en los procesos misionales debe ser tratada con especial atención para preservar la integridad, confidencialidad y disponibilidad de la información administrada a través de los mismos.
- Se considera como una actividad altamente riesgosa la modificación directa a las bases de datos de los procesos misionales. Dado lo anterior, esta práctica debe utilizarse sólo en los casos estrictamente necesarios, y el análisis de su necesidad debe quedar adecuadamente documentado. En todo caso, esta práctica debe tender a ser eliminada.
- La entidad reconoce como alternativa para mejorar su eficiencia y administrar sus riesgos, la tercerización de operaciones. Sin embargo, es consciente de que esto le genera nuevos

riesgos. Dado lo anterior, cuando contemple la posibilidad de desarrollar alguna de sus operaciones a través de un tercero, deberá tener claro:

- La identificación de los riesgos que debe administrar y los controles mínimos que debe tener el tercero para el desarrollo de la actividad.
- La revisión periódica de que los mecanismos de control exigidos se mantienen.
- Debe contemplar con claridad las condiciones sobre cómo se puede finalizar el acuerdo, y las disposiciones de continuidad de la operación.
- Previa a la contratación con un tercero, debe realizarse las verificaciones necesarias para validar que el mismo, no haya sido cuestionado ni se encuentre inmerso en investigaciones de fraude, corrupción, lavado de activos o financiación del terrorismo.
- Estos terceros deben ser monitoreados de manera permanente, y el contrato debe incluir claros requisitos de servicios y detalles sobre cómo y cuán frecuentemente éstos serán medidos.

En la innovación de sus procesos

- Como eje principal de desarrollo, Colpensiones se apalanca en la innovación de sus procesos.
- La innovación trae consigo nuevos riesgos que deben ser cuidadosamente analizados bajo la premisa de encontrar la manera de administrarlos. Sólo luego de un análisis profundo de los mismos, se puede llegar a la conclusión de evitar los riesgos producto de la innovación.
- Previo a la entrada de cambios en los procesos, se deben haber identificado y evaluado los riesgos y definido sus actividades de control o tratamiento. Sin esta identificación, no deben ser implementados los cambios.

En la adopción de nuevas tecnologías

- Como eje principal de su desarrollo, Colpensiones se apalanca en la adopción de nuevas tecnologías.
- Las nuevas tecnologías traen consigo nuevos riesgos que deben ser cuidadosamente analizados bajo la premisa de encontrar la manera de administrarlos. Sólo luego de un análisis profundo de los mismos, se puede llegar a la conclusión de evitar los riesgos.
- Previo a la adopción de nuevas tecnologías, se deben haber identificado y evaluado los riesgos y definido sus actividades de control o tratamiento.

Con relación a la prevención del fraude y la corrupción:

- Colpensiones establece como principio rector de su cultura institucional y de operación, la posición de "**Cero Tolerancia"** frente al fraude y la corrupción, siendo consecuentes con los valores institucionales de la Entidad.

- En este sentido, cualquier riesgo de fraude o corrupción materializado, debe ser informado a la Junta Directiva y a la Oficina de Control Interno, sin importar su cuantía.
- Colpensiones establece como prioridad en la administración del riesgo de fraude y corrupción la prevención, detección y disuasión, que permitan a la Entidad evitar la materialización de eventos en esta materia.
- Colpensiones garantiza la implementación de canales de reporte interno y externo de presuntos hechos de fraude y corrupción, en los que se asegura la reserva y confidencialidad del denunciante y de los hechos puestos en conocimiento. Así mismo, se garantiza la posibilidad de realizar reportes de forma anónima y la protección al denunciante, con el fin de evitar retaliaciones.

Con relación a la protección de su imagen:

- En sus actuaciones, Colpensiones respeta a su competencia y no utiliza sus canales de comunicación para hablar mal de ella.
- Colpensiones reconoce la importancia de las redes sociales para el posicionamiento y protección de su imagen y como canal para generar confianza. En la utilización de este canal, debe tener claramente identificados sus riesgos y la forma de administrarlos.
- El vocero único de Colpensiones es el Presidente, ningún servidor público, colaborador o contratista se encuentra autorizado para divulgar información de la entidad, sin su previa autorización.

Con relación al cumplimiento legal:

- Para Colpensiones es inaceptable las sanciones económicas por incumplimiento de las normas establecidas por los entes reguladores. Dado lo anterior, es deber de la Alta Dirección el comunicar a la Junta Directiva la apertura de procesos sancionatorios, disciplinarios o fiscales contra la entidad.
- Así mismo, para Colpensiones el cumplimiento normativo interno y externo, y el código de ética, están alineados con los objetivos estratégicos y, consecuentemente, la no tolerancia de conductas que puedan constituir incumplimientos.

Con relación a sus colaboradores:

- Todos los servidores públicos y colaboradores de Colpensiones, durante el proceso de inducción, deben recibir capacitación sobre la administración integral de riesgos, y son responsables de su adecuado funcionamiento.
- La formación en materia de administración integral de riesgos es obligatoria para todos los servidores públicos y colaboradores de la Entidad.
- Colpensiones es consciente que el recurso humano es un factor de riesgo relevante en el desarrollo de sus operaciones. Es por ello, que tratará con especial atención los procesos de selección y capacitación del mismo.

9.1.4.2. Declaración Cuantitativa del Apetito de Riesgo

Las declaraciones cualitativas del apetito de riesgo son complementadas con métricas que le permiten a la entidad, medir objetivamente el nivel de riesgo en el cual se encuentra, y así, establecer los niveles tolerados y su capacidad de asumir nuevos riesgos.

En cuanto a la definición del apetito de riesgo bajo criterios cuantitativos, se tendrán en cuenta las siguientes definiciones:

Apetito al Riesgo	Es la exposición al riesgo que una entidad está dispuesta a asumir en el desarrollo de su actividad con el fin de alcanzar sus objetivos estratégicos y cumplir con su plan de negocios.
Tolerancia al Riesgo	Es el nivel aceptable de variación o desviación frente al apetito de riesgo que la Entidad está dispuesta a aceptar en la búsqueda del logro de sus objetivos.
Capacidad de Riesgo	Nivel máximo que la empresa es capaz de soportar en el logro de los objetivos estratégicos establecidos en su misión y visión.

Ilustración 2. Criterios Cuantitativos del MAR

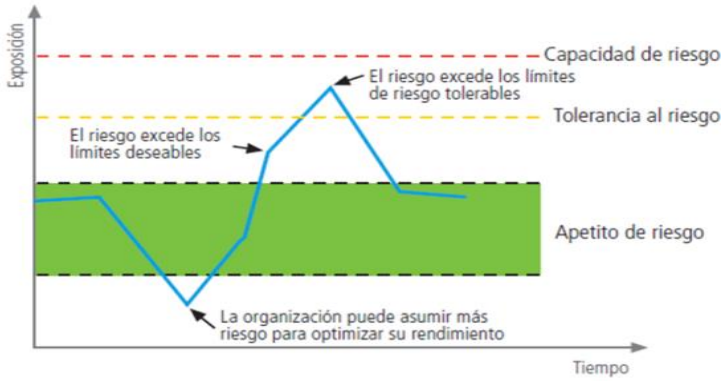


Ilustración 3. Esquema Criterios Cuantitativos del MAR
Fuente: Marco de Apetito de Riesgo - SFC

El desarrollo de estos conceptos se realizará a través de la definición de métricas que permitan la definición de niveles aceptados y límites tolerados, para lo cual se llevará a cabo la articulación de indicadores para medir sistemáticamente, y de forma continua en el tiempo, los resultados obtenidos y la comparación con resultados deseados o planeados.

Así las cosas, y analizando cada una de las tipologías de riesgo a las que se ve expuesta Colpensiones en el desarrollo de sus actividades, el apetito cuantitativo de riesgo se medirá considerando lo siguiente:

I. **Riesgo Operacional, Fraude y Corrupción, Seguridad de la información y Ciberseguridad y de Continuidad del Negocio**: Se medirá a través de la siguiente metodología:

i. Metodología para el Cálculo del Apetito

Se calculará a través de la metodología de IBNR (Siniestros Ocurridos, pero No Avisados). Utiliza datos de pérdidas reales por eventos de riesgo operacional y fraude, y calcula los perfiles históricos de desarrollo de eventos no descubiertos desde los más antiguos hasta los más recientes, es decir, se define una distribución de la evolución de los eventos basado en dos variables:

- Tiempo que se tarda (en años) en ser descubierto un evento de riesgo después de su materialización.
- Valor de los eventos de riesgo operacional para cada uno de los años posterior a la materialización.

De esta forma, se establece una proyección del valor de los eventos de riesgo esperado para un horizonte de tiempo definido.

A continuación, se describen los pasos para realizar el cálculo:

- **Cálculo Triángulo de Obligaciones Conocidas Pagadas**

Contiene la distribución por periodo de prestación (año de materialización) y periodo de desarrollo (año de contabilización del evento) del valor de las obligaciones pagadas a la fecha de corte de la información:

Triángulo de obligaciones conocidas pagadas							
Periodo de prestación (I)	Periodo de desarrollo (j)						
	1	2	…	K	…	n−1	N
1	$P_{1,1}$	$P_{1,2}$	…	$P_{1,k}$	…	$P_{1,n-1}$	$P_{1,n}$
2	$P_{2,1}$	$P_{2,2}$	…	$P_{2,k}$	…	$P_{2,n-1}$	
…	…	…	…	…	…		
K	$P_{k,1}$	$P_{k,2}$	…	$P_{k,k}$			
…	…	…					
N	$P_{n,1}$						

Tabla 2. Triángulo de Obligaciones Conocidas Pagadas

Los eventos contabilizados se pueden expresar como Pij y corresponde al valor de los eventos materializados en el periodo de prestación i que se contabilizaron en el periodo de desarrollo j.

- **Cálculo Triángulo de Obligaciones Conocidas Acumuladas**

Contiene la distribución por periodo de prestación (materialización) y periodo de desarrollo (contabilización) del valor acumulado de los eventos de riesgo contabilizados a la fecha de corte de la información. Es decir, para cada periodo de desarrollo, se muestra el valor acumulado de eventos de riesgo de un año de materialización específico:

Triángulo de Obligaciones Conocidas Acumuladas							
Periodo de prestación (i)	Periodo de desarrollo (j)						
	1	2	…	K	…	n–1	N
1	$P_{1,1}$	$PA_{1,2}$	…	$PA_{1,k}$	…	$PA_{1,n-1}$	$PA_{1,n}$
2	$P_{2,1}$	$PA_{2,2}$	…	$PA_{2,k}$	…	$PA_{2,n-1}$	
…	…	…	…	…	…		
K	$P_{k,1}$	$PA_{k,2}$	…	$PA_{k,k}$			
…	…	…					
N	$P_{n,1}$						

$$PA_{ij} = \sum_{k=1}^{j} P_{i,k}$$

Tabla 3. Triángulo de Obligaciones Conocidas Acumuladas

- **Cálculo Factores de Desarrollo**

Los factores de desarrollo sirven para medir la evolución del valor de eventos de riesgo de un periodo de prestación definido (año de materialización específico) desde un periodo de desarrollo al siguiente y se utilizan como base para seleccionar los factores de desarrollo más apropiados para proyectar las contabilizaciones de los periodos futuros.

Se calcula como el cociente entre las Obligaciones Conocidas Acumuladas de dos periodos de desarrollo sucesivos (calculados en el punto anterior):

Factores de Desarrollo						
Periodo de desarrollo (j)						
1	2	…	K	…	n–1	
FD_1	FD_2	…	FD_k	…	FD_{n-1}	FD_n

$$FD_j = \frac{\sum_{i=1}^{n-j+1} PA_{i,j+1}}{\sum_{i=1}^{n-j+1} PA_{i,j}}$$

Tabla 4. Factores de Desarrollo

- **Cálculo de IBNR**

Si bien, la Metodología del IBNR calcula la pérdida esperada para los años posteriores al presente, para el caso puntual de apetito al riesgo, se tomará únicamente el cálculo de perdida esperada para el año más próximo, es decir, la pérdida esperada con un horizonte de un año. Esto se fundamenta debido a que el cálculo del apetito al riesgo se realiza con un horizonte anual.

De esta forma, la fórmula del IBNR con un horizonte a un año, para cada uno de los periodos de prestación *i,* quedaría de la siguiente forma:

$$IBNR_i = PA_{ij} * (FD_j - 1)$$

- **Cálculo de Apetito**

El cálculo del apetito al riesgo operacional resultará de la suma del IBNR con un horizonte a un año de todos los periodos de prestación definidos.

$$Apetito = \sum_{i=1}^{N} IBNR_i$$

ii. Metodología para el Cálculo de la Tolerancia

Basado en el cálculo de apetito al riesgo, se estresan los factores de desarrollo (FD_j) de la metodología IBNR. De esta forma, se tendrá un cálculo de IBNR estresado con un horizonte de un año. Es decir, se calcula un nivel de IBNR asumiendo que se repiten de manera sostenida, de un año a otro, los mayores factores de crecimiento de los eventos de riesgo operacional.

- **Determinación del nivel de estrés**

Para definir un nivel de estrés del IBNR calculado en la formulación de apetito al riesgo, se suma a cada factor de desarrollo (FD_j) una desviación estándar de los factores de desarrollo individuales (FD_{ij}) calculados para cada periodo de prestación (periodo de materialización) agrupado por periodo de desarrollo (periodo de contabilización). Es decir, se recogen los mayores valores de variación históricos para los eventos de riesgo entre dos periodos de desarrollo consecutivos y se calcula la pérdida esperada basada en los mayores valores de la distribución histórica.

La fórmula para el cálculo de los factores de desarrollo individuales por cada periodo de prestación y cada periodo de desarrollo será la siguiente:

$$FD_{ij} = \frac{PA_{i,j+1}}{PA_{i,j}}$$

- **Factores de Desarrollo Estresados**

Paso seguido, se calcula el factor de desarrollo estresado (FDE) para cada uno de los factores de desarrollo así:

$$FDE_j = (\mathrm{FDj}) + Desviación\ Estandar\ \left(FD_{ij}\right)\ para\ 1 \leq i \leq N$$

- **Cálculo de IBNR Estresado**

Para el caso puntual de tolerancia al riesgo, se tomará únicamente el cálculo de pérdida esperada estresado para el año más próximo, es decir, la pérdida esperada con un horizonte de un año. Esto se fundamenta debido a que el cálculo de tolerancia al riesgo se realiza con un horizonte anual.

De esta forma, la fórmula del IBNR estresado (IBNRE) con un horizonte a un año, para cada uno de los periodos de prestación i, quedaría de la siguiente forma:

$$IBNRE_i = PA_{ij} * (FDE_j - 1)$$

- **Cálculo de Tolerancia**

El cálculo de tolerancia al riesgo operacional resultará de la suma del IBNRE con un horizonte a un año de todos los periodos de prestación definidos:

$$Tolerancia = \sum_{i=1}^{N} IBNRE_i$$

iii. Metodología para el Cálculo de la Capacidad

El objetivo de esta formulación, es establecer la relación de equilibrio entre ingresos y egresos que solvente el riesgo máximo que puede asumir la entidad frente a eventos de riesgo operacional. Es decir, se busca determinar el máximo nivel de eventos de riesgo operacional que podría asumir la entidad, sin entrar en un escenario de utilidades negativas y manteniendo el nivel patrimonial estable.

- **Cálculo de ingresos estresados**

Como insumo para el cálculo de la capacidad, se requiere tener un escenario de estrés para el nivel de ingresos totales de la entidad. Para ello, se toma como base la proyección de ingresos de la Administradora para un año determinado aprobado por la Junta Directiva y se proyecta un escenario bajo el cual se obtengan ingresos un 10% por debajo de lo esperado:

$$Ingresos\ Estresados = Proyección\ de\ Ingresos\ Anual * 90\%$$

- **Cálculo de egresos estresados**

Se define el escenario de estrés para los egresos de la entidad, tomando como base la ***Proyección de Gastos Anual*** de la Administradora para un periodo determinado aprobado por la Junta Directiva (diferentes a riesgo operacional), y se proyecta un escenario de gastos bajo el cual se materialicen eventos de riesgo operacional por encima de lo esperado, al cual se le denominará Capacidad por Riesgo Operacional:

$$Egresos\ Estresados = Proyección\ de\ Gastos\ Anual\ + Capacidad\ Riesgo\ Operacional$$

- **Cálculo de la Capacidad por Riesgo Operacional**

Se busca el Estrés Máximo de Riesgo Operacional que iguale el valor de Ingresos Estresados con el valor de Egresos Estresados:

$$Ingresos\ Estresados = Egresos\ Estresados$$

Es decir, el cálculo de la Capacidad por Riesgo Operacional resultará de la siguiente expresión:

$$Capacidad\ Riesgo\ Operacional = Ingresos\ Estresados - Proyección\ de\ Gastos\ Anual$$

II. ***Riesgos de Fraude y Corrupción:*** La medición del apetito de riesgo de fraude y corrupción señalada en el punto anterior, se realiza considerando la necesidad de realizar una medición agregada de riesgos que permita alertar a la entidad frente a su capacidad financiera de asumir riesgos. Sin embargo, la tolerancia al riesgo de fraude para Colpensiones es cero. Esto implica que, sin importar la cuantía del evento, Colpensiones debe definir medidas de mitigación que disminuyan la probabilidad de que el mismo vuelva a ocurrir o que sea oportunamente identificado.

De igual forma, esta declaración implica que todos los eventos que materialicen un riesgo de fraude y corrupción, sin importar su cuantía, tendrán el siguiente tratamiento:

- Análisis tipología, causas y medidas de control a implementar
- Recursos necesarios para su implementación.
- Informe a Comité de Riesgos Operativo y Seguridad de la Información, Comité de Auditoria y Junta Directiva.

III. ***Riesgos de Lavado de Activos y Financiación del Terrorismo***: La medición cuantitativa del apetito de esta tipología de riesgo, no aplica, considerando el nivel de tolerancia Cero, establecido por el marco normativo actual.

Al igual que en el riesgo de Fraude y Corrupción, la declaración de que el apetito de riesgo para esta tipología es cero, implica que, sin importar la cuantía del evento Colpensiones debe definir medidas de mitigación que disminuyan la probabilidad de que el mismo vuelva a ocurrir o que sea oportunamente identificado.

De igual forma, esta declaración implica que todos los eventos que materialicen este tipo de riesgo, sin importar su cuantía, tendrán el siguiente tratamiento:

- Análisis tipología, causas y medidas de control a implementar
- Recursos necesarios para su implementación.
- Informe a Comité de Riesgos Operativo y Seguridad de la Información, Comité de Auditoria y Junta Directiva.

IV. ***Riesgo de Mercado***: El apetito y tolerancia al riesgo de mercado, está definido de acuerdo con el indicador de valor en riesgo y a los límites establecidos para dicho indicador en el Manual del Sistema Integral de Riesgos, Parte IV - Sistema de Administración de Riesgo de Mercado y Contraparte.

- VAR por portafolio

- Límites de VAR:
  - Apetito – Limite 1
  - Tolerancia – Limite 2

9.1.5. Lineamientos para el Seguimiento al Comportamiento del Apetito de Riesgo

- Todos los eventos de riesgo individual o que de forma agrupada (eventos de alta frecuencia y bajo impacto) superen el apetito de riesgo, deberán ser presentados al Comité Integral de Riesgos con su respectivo análisis de causas y los planes de acción para mitigar sus efectos y recuperar los recursos.

- Todos los eventos de riesgo individual o que de forma agrupada (eventos de alta frecuencia y bajo impacto) superen el nivel de tolerancia al riesgo, deberán ser presentados al Comité Integral de Riesgos, Comité de Auditoria y Junta Directiva, con su respectivo análisis de causas y los planes de acción para mitigar sus efectos y recuperar los recursos.

- La Gerencia de Riesgos y Seguridad de la Información, monitoreará la tendencia de los eventos de riesgo con pérdida para alertar de manera oportuna si, de acuerdo con dicho análisis, existe el riesgo de sobrepasar el apetito de riesgo o el nivel de tolerancia.

- Es responsabilidad de la Vicepresidencia de Seguridad y Riesgos Empresariales, presentar de forma anual, o cuando la tendencia de los eventos de riesgo genere señales de alerta, un análisis sobre el apetito cuantitativo de riesgo operativo de la entidad, señalando si los límites establecidos se mantienen, disminuyen o deben incrementarse.

9.1.6. Comunicación Marco Integral de Apetito de Riesgo

El marco de apetito de riesgo debe ser adecuadamente comunicado en todos los niveles de la organización. Esto con el fin de que sea considerado en el marco de la toma de decisiones. Así las cosas, los grupos de interés a los que se debe comunicar dicho marco son:

- Junta Directiva
- Alta Dirección, conformada por el Presidente, los Vicepresidentes y los Jefes de Oficinas.
- Áreas Especiales. Dentro de este grupo se encuentran las siguientes áreas:
  - Gerencia de Financiamiento e Inversiones.
  - Gerencia de Determinación del Derecho.
  - Gerencia Administrativa
  - Gerencia de Talento Humano y Relaciones Laborales
  - Gerencia de Tecnologías de la Información.
  - Gerencia de Prevención del Fraude
  - Gerencia de Defensa Judicial

- Oficina Asesora de Asuntos Legales
- Oficina de Comunicaciones y Relacionamiento.
- Gerencia de Sistemas Integrados de Gestión.
- Gerencia de Planeación Institucional.

- Servidores públicos y colaboradores de Colpensiones. Para el efecto, se debe considerar en el marco de las capacitaciones anuales sobre el sistema integral de administración de riesgos.

9.2. AGREGACIÓN DE RIESGOS

9.2.1. Objetivos

i) Definir una metodología que integre las mediciones de las diferentes tipologías de riesgos y que permita establecer la exposición consolidada de los riesgos que podrían afectar la sostenibilidad financiera de la entidad

ii) Establecer señales de alerta frente a riesgos de sostenibilidad financiera.

9.2.2. Metodología de Integración de Riesgos

La metodología para realizar la integración de riesgos será el Cálculo de Solvencia, la cual estará formulada de la siguiente forma:

$$Relación\ de\ Solvencia = \frac{Patrimonio\ Técnico}{APNR + \frac{100}{9} * RM + \frac{100}{9} * Riesgo\ Operativo}$$

DEFINICIONES	
RM: Exposición al Riesgo de Mercado	Para este cálculo, se tomará el valor en riesgo calculado a través del modelo interno de Colpensiones aprobado por la Junta Directiva y descrito en la Parte IV del Manual SIAR.
Exposición al Riesgo de Operativo	Se tomará el Valor aprobado por la Junta Directiva de Apetito al Riesgo Operacional definido dentro del Marco Integral de Apetito al Riesgo. Metodología definida en el Numeral 9.1.4.2. del presente Manual.
APNR: Activos Ponderados por Nivel de Riesgo	Corresponde a las posiciones activas del Balance de la entidad, computadas en un 0%, 20% según el riesgo de crédito al que se encuentren expuestos los activos.
Relación de Solvencia	Corresponde a la relación adecuada de patrimonio técnico (PT) y activos ponderados por nivel de riesgo (APNR) destinado a cubrir los riesgos a los que se expone Colpensiones por la administración de recursos de terceros.

Tabla 5. Definiciones de Relación de Solvencia

Categorías APNR		%
Categoría I.	Activos de máxima seguridad, tales como caja, depósitos a la vista en entidades sometidas a la inspección y vigilancia de la Superintendencia Financiera de Colombia, inversiones en títulos o valores de la Nación, del Banco de la República, o emitidos para el cumplimiento de inversiones obligatorias y los créditos a la Nación o garantizados por esta.	0%
Categoría II	Activos de alta seguridad, tales como los títulos o valores emitidos por entidades públicas del orden nacional, los depósitos a término en otros establecimientos de crédito, las operaciones relacionadas con fondos interbancarios vendidos, y los créditos garantizados incondicionalmente con títulos o valores emitidos por la Nación o por el Banco de la República o de Gobiernos o Bancos Centrales de países que autorice expresamente la Superintendencia Financiera de Colombia.	20%

Tabla 6. Categorías de Activos Ponderados por Nivel de Riesgo

9.2.3. Fuentes de Información Cálculo de Solvencia

Cálculo de Patrimonio Técnico:

Se tomarán las siguientes cuentas contables de la Administradora:

3105	CAPITAL FISCAL
3110	RESULTADO DEL EJERCICIO

Cálculo de Activos Ponderados por Nivel de Riesgo:

Con base en la composición de los activos de Colpensiones y a las categorías I y II descritas en la Tabla 6 de Categorías de APNR, se tomarán las siguientes cuentas contables de la Administradora y ponderadores:

		Ponderación
1110	DEPÓSITOS EN INSTITUCIONES FINANCIERAS	0%
1200	INVERSIONES E INSTRUMENTOS DERIVADOS	20%
1908	RECURSOS ENTREGADOS EN ADMINISTRACIÓN	20%

Exposición al Riesgo Operacional:

Nivel de apetito definido por la Junta Directiva dentro del Marco de Apetito de Riesgos.

Exposición al Riesgo de Mercado:

Para calcular la exposición al riesgo de mercado se tomará el Modelo Interno de Valor en Riesgo aprobado por la Junta Directiva de Colpensiones, el cual se describe en la Parte IV del Manual SIAR. Este cálculo es realizado por la Gerencia de Riesgos y Seguridad de la Información sobre el portafolio de inversiones perteneciente a la Administradora.

9.2.4. Generación de Alertas por Indicador de Solvencia:

Se propende por tener una relación de Solvencia igual o superior al 9%, con el objetivo de establecer una relación óptima entre el riesgo asumido por la entidad, y el patrimonio y activos que lo soportan. Los niveles de Solvencia por debajo del 9% serán informados al Comité de Riesgos de Inversiones para generar un plan de acción.

10. METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS

Teniendo en cuenta que la administración de riesgos es un aspecto fundamental en la estructura del gobierno corporativo, que consiste en la aplicación sistemática de políticas, procedimientos y prácticas que permitan desarrollar cada una de las etapas de la gestión de riesgos; y tomando como referencia la normatividad vigente establecida por la Superintendencia Financiera de Colombia, las guías del Departamento Administrativo de la Función Pública y las mejores prácticas, Colpensiones cuenta con una metodología para la gestión integral de riesgos que incluye etapas y actividades, que a su vez, deben ser parte del Sistema de Control Interno y del Sistema Integrado de Gestión de Colpensiones y estar incluida en la cultura y prácticas institucionales.

En este entendido, la metodología de gestión integral de riesgos, contempla las siguientes dimensiones para su administración:

Niveles: Gestión de riesgos estratégicos, tácticos y por procesos.

Tipologías de Riesgo: Riesgos operacionales, de continuidad del negocio, de seguridad de la información y ciberseguridad, de fraude y corrupción, de lavado de activos y financiación del terrorismo y los riesgos financieros (mercado, liquidez y contraparte).

Objetivos de Control: Objetivo de cumplimiento, operativo y de información.

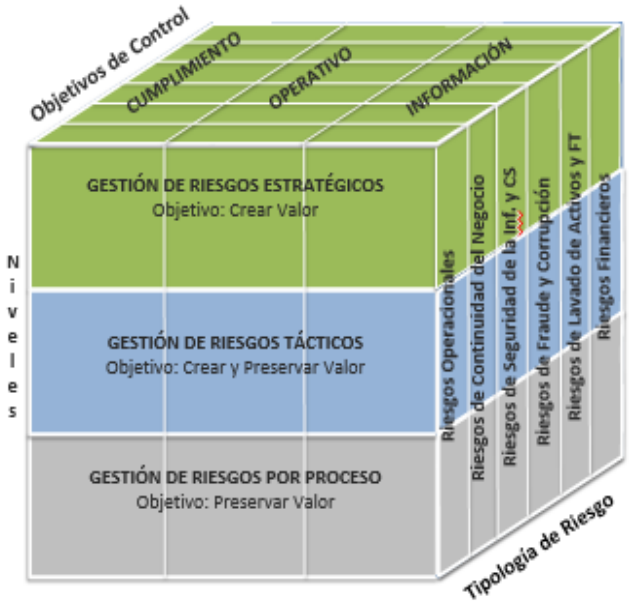


Ilustración 5. Dimensiones de la Gestión Integral de Riesgos

Para el establecimiento del proceso de Gestión Integral de Riesgos, Colpensiones adopta como metodología base, la definida por la norma ISO 31000, desarrollando las etapas que se muestran a continuación:

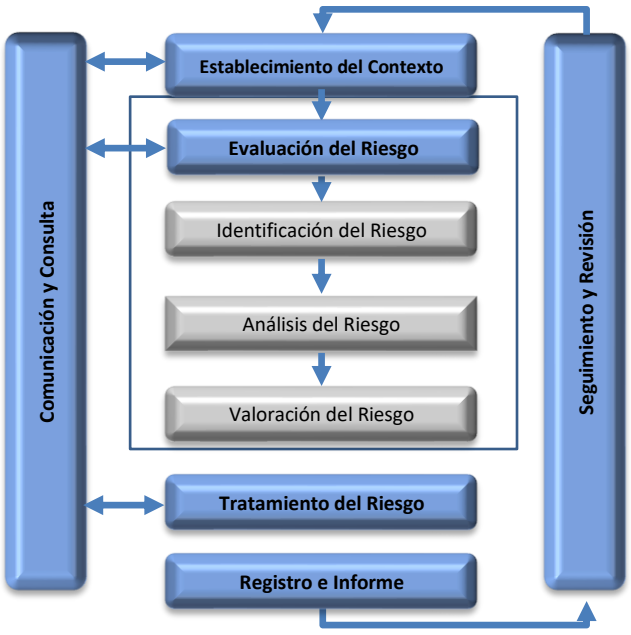


Ilustración 6. Etapas en la Gestión Integral de Riesgos
Fuente de Información: Norma ISO 31000_2018

Sin perjuicio de lo anterior, Colpensiones incorpora elementos adicionales de otros estándares de gestión de riesgos, que complementan el modelo y la eficacia de este, reconociendo así, las mejores prácticas en la gestión de cada una de las tipologías de riesgo. Así las cosas, incorpora elementos adicionales relacionados con:

- La gestión de riesgos estratégicos bajo lo señalado en la norma ISO 9001 – Sistema de Gestión de Calidad, y el Marco Integrado para la Gestión de Riesgos Corporativos emitido por el Committe Of Sponsoring Organizations of the Treadway Commission - COSO ERM
- La gestión de riesgos tácticos, considerando los lineamientos definidos por el Project Management Institute.
- La gestión de riesgos de Seguridad de la Información y Ciberseguridad, tomando como referencias componentes de ISO 27005 e ISO 27032.
- La gestión de riesgos de continuidad del negocio, tomando elementos del marco internacional señalado en la norma ISO 22301.
- Los lineamientos y metodologías de identificación y valoración de riesgos de corrupción, definidos por la Guía del Departamento Administrativo de la Función Pública.
- La gestión de riesgos de cumplimiento, con base en la normatividad emitida por la Superintendencia Financiera de Colombia, del Sistema de Control Interno. Es así, como se incorporan los objetivos de control en la identificación de riesgos.

10.1. ESTABLECIMIENTO DEL CONTEXTO

La administración de riesgos se desarrolla dentro del marco estratégico de Colpensiones[2] e integrado al sistema de gestión, determinando las características del entorno externo e interno en el cual opera Colpensiones.

El establecimiento del contexto se establece considerando las siguientes 4 instancias:

[2] Ver Plan Estratégico Institucional de Colpensiones.

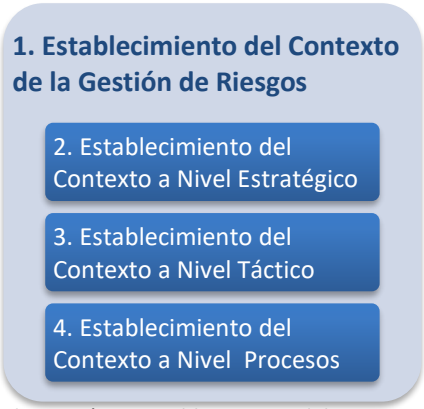


Ilustración 7. Establecimiento del Contexto

10.1.1. Establecimiento del Contexto de la Gestión de Riesgo

El establecimiento del contexto de la gestión de riesgos es el marco de actuación general, que los servidores públicos, Colaboradores, Proveedores y en general sus partes interesadas, deberán considerar para gestionar cualquier riesgo al que se enfrenten en el desarrollo de sus responsabilidades.

La definición de este contexto incluye:

- La definición de objetivos, alcance y principios de la Gestión Integral de Riesgos en Colpensiones.
- El establecimiento de políticas que deberán ser consideradas e incorporados en los procesos de toma de decisiones de la organización.
- El establecimiento de un marco integral de apetito de riesgo alineado a los criterios de valoración de los riesgos en sus diferentes clasificaciones de riesgo.
- La definición de responsabilidades y roles en la gestión de riesgos.
- El establecimiento de marcos de referencia para el desarrollo y fortalecimiento de las metodologías utilizadas en la gestión integral de riesgos.

Los anteriores componentes ya han sido expuestos en el desarrollo del presente documento.

10.1.2. Establecimiento del Contexto a Nivel Estratégico

En el marco de la gestión de riesgos estratégicos, es necesario identificar los factores internos y externos que afectan o pueden afectar las estrategias definidas por la entidad para alcanzar sus objetivos de largo plazo. Los riesgos estratégicos pueden afectar la continuidad del negocio, el cumplimiento de sus estrategias o impactar de manera significativa su desempeño. Pero de igual forma pueden evidenciar nuevas oportunidades para el desarrollo de la entidad.

Así las cosas, el establecimiento del contexto debe realizarse bajo dos líneas, así:

- **Establecimiento del Contexto Interno**

Para el análisis de contexto interno, Colpensiones ha establecido como metodología principal, el Perfil de Capacidad Interna (PCI) que se utiliza para analizar las fortalezas y debilidades en relación con las oportunidades y amenazas que presenta el medio externo.

La metodología de Perfil de Capacidad considera los siguientes factores de riesgo interno:

Capacidad Directiva	Capacidad Competitiva	Capacidad Financiera	Capacidad Técnica y Tecnológica	Capacidad de Talento Humano
Imagen Corporativa Comunicación y Control Gerencial Sistema de Control Interno Gobierno Corporativo Modelos de evaluación de la gestión	Calidad del producto Participación en el mercado. Canales de distribución Investigación y Desarrollo Lealtad de los clientes Calidad en los procesos de servicio. Modelo operativo	Comportamiento de indicadores financieros Fortaleza patrimonial Estabilidad de los ingresos y los costos Sostenibilidad financiera.	Habilidades Técnicas Capacidad de innovación Desarrollo Tecnológico Demanda tecnológica delos procesos Actualización tecnológica	Nivel Académico Experiencia técnica Estabilidad y Rotación. Niveles de remuneración Clima Organizacional Programas de desarrollo Motivación Pertenencia

Ilustración 8. Factores de Riesgo Interno

Para el establecimiento del perfil de capacidad interna, la Gestión Integral de Riesgos puede apoyarse en las siguientes fuentes de información:

- Informes de órganos de control.
- Comportamiento de eventos de riesgo e incidentes de seguridad.
- Encuestas realizadas a los grupos de interés.
- Comportamiento de los indicadores estratégicos, tácticos u operativos.
- Informes de análisis generados por las diferentes áreas de la entidad.
- Evaluaciones especiales de riesgos.
- Perfil de riesgos estratégicos, tácticos y por procesos.

Como base en esta información se definen y priorizan las oportunidades de mejora y las fortalezas de la entidad frente a su contexto interno; que, a su vez, corresponderá a acciones que permiten la mitigación a la exposición de potenciales riesgos.

- **Establecimiento del Contexto Externo**

Para el establecimiento del contexto externo, Colpensiones realiza una identificación de factores de riesgo que puedan materializar riesgos estratégicos y emergentes a través de la metodología PESTAL. Esta metodología permite analizar el entorno macroeconómico en el que opera la empresa, considerando las variables Políticas, Económicas, Sociales, Tecnológicas, Ambientales y Legales a las que se enfrenta o se puede enfrentar Colpensiones en búsqueda de su visión y objetivos estratégicos. Es una herramienta fundamental para calcular los riesgos emergentes y oportunidades que muestra el entorno.

Esta metodología evalúa 5 factores de riesgo, así:

- **Políticos.** Los factores políticos se centran en la intervención del gobierno en la economía. Dentro de los factores políticos, hay que analizar los impuestos, las leyes laborales, leyes medioambientales, tarifas y estabilidad política.

  Las decisiones gubernamentales que tienen más impacto son las basadas en salud, educación e infraestructuras de un país. El cambio de gobierno a corto plazo también es un factor a tener en cuenta, analizando las encuestas de popularidad de los distintos posibles gobiernos futuros, al igual que sus programas electorales.

- **Económicos.** Dentro de los factores económicos para el análisis del entorno empresarial, podemos hacer una pequeña división, entre los factores económicos permanentes, los temporales a nivel nacional y los temporales internacionales.

En los factores económicos permanentes podemos incluir el nivel de desarrollo económico de la región, el índice de crecimiento de la población, los niveles salariales y la disponibilidad de las materias primas. Estos factores suelen ser estables a lo largo del tiempo y sus modificaciones son mínimas con el paso del tiempo.

Dentro de los factores temporales a nivel nacional, hay que centrarse en la situación de la balanza de pagos y los tipos de interés presentes en el mercado. En definitiva, los elementos de la situación de un país en relación con la actividad económica del mismo.

En los factores temporales a nivel internacional, hay que tener en cuenta la competencia entre empresas en otras regiones y el nivel de proteccionismo de los mercados.

La coyuntura económica mundial también es un factor a tener en cuenta, ya que la posibilidad de guerras cercanas o posibles crisis puede incidir en la economía de otro país si se trata de naciones interdependientes.

- **Sociales.** Es importante tener en cuenta las necesidades de los ciudadanos de la entidad; sus gustos, sus preferencias, valores y creencias. Hay que valorar si los clientes a los que nos dirigimos viven en una gran ciudad o sin embargo habitan en zona rural, ya que esto modifica sus hábitos de consumo.

  Entre los factores que se pueden destacar en el análisis de los factores sociales hay que incluir la migración de la población, el nivel de educación, la tasa de natalidad y las nuevas formas de estructura familiar.

  En una era globalizada, hay que tener en cuenta la comunicación disponible para los consumidores. Esta comunicación proporciona a los consumidores información de productos y servicios de otros países, que competirán directamente con el mercado nacional.

- **Tecnológicos.** En cualquier tipo de negocio la tecnología es el punto clave de su éxito. Dentro de los factores tecnológicos, hay que tener en cuenta los incentivos a la tecnología que ofrece el gobierno, la automatización, el ritmo de los cambios tecnológicos y las actividades de Investigación y Desarrollo. En este marco también es importante analizar el impacto de la evolución tecnológica a los temas de seguridad de la información, por esta razón se consideran los riesgos cibernéticos como un aspecto a considerar, los cuales se pueden ver reflejados en ataques cibernéticos, como lo son; el fraude masivo de datos, ataques de denegación del servicio, programas de secuestro cibernético, instalación de programas maliciosos, colapso de la infraestructura critica de información y redes , difusión de información errónea, efectos adversos de los avances tecnológicos.

- **Ambientales.** Dentro de los factores ambientales que afectan al desarrollo de la actividad económica de una empresa, encontramos los aspectos ecológicos y de medio ambiente. En la actualidad, ha aumentado la preocupación por el cambio climático. Esta no solo afecta a las políticas que puedan adoptar los determinados organismos gubernamentales, sino que los clientes valoran si las empresas generan su actividad económica, a través de prácticas que no sean nocivas para el medio ambiente.

- **Legales.** Dentro del análisis PESTEL, se hace distinción entre los factores políticos y los legales. Dentro del marco del análisis legal, se valorará los proyectos de ley que puedan afectar al desarrollo de la actividad económica.

A continuación, se ilustran, algunas variables consideradas en cada factor de riesgo:

Políticos	Económicos	Sociales	Tecnológicos	Ambientales	Legales
Política económica e iniciativas de Gobierno. Política Fiscal. Leyes Laborales. Estabilidad Política. Decisiones gubernamentales sobre el sistema pensional Tendencias políticas en épocas de elecciones.	Perspectivas Económicas. Flujos de Capital Extranjero. Comportamiento económico de socios comerciales. Percepción del Riesgos País.	Tendencias de los ciudadanos. Migración poblacional. Evolución de la educación. Tasa de natalidad y envejecimiento de la población. Estructuras familiares. Salud de la población. Mercado Laboral. Seguridad Rural.	Evolución de la tecnología Ritmo de cambios tecnológicos Comportamiento de fraudes sobre nuevas tecnologías. Vulnerabilidades de nuevas tecnologías.	Cambio climático. Impacto de la actividad económica sobre el medio ambiente. Posibilidad de desastres naturales.	Cambios normativos esperados. Interpretación de normas por parte de partes relacionadas y grupos de interés.

Ilustración 9. Factores de Riesgo Externo

Producto de este análisis, se genera un listado de amenazas y oportunidades del entorno las cuales son priorizadas y consideradas en la identificación de riesgos emergentes y en el establecimiento de los objetivos que permitan potencializar esas oportunidades.

El análisis del contexto en el marco de la gestión de riesgos estratégicos es liderado por la Vicepresidencia de Seguridad y Riesgos Empresariales en Coordinación con la Vicepresidencia de Planeación y Tecnologías de la información.

10.1.3. Establecimiento del Contexto a Nivel Táctico

El nivel táctico en la gestión de riesgos hace referencia al análisis del contexto de los proyectos institucionales, definidos para avanzar en el cumplimiento de sus objetivos estratégicos.

De acuerdo con lo anterior, las siguientes son las variables, que, desde el punto de vista del proyecto deberán ser consideradas para analizar el contexto del mismo:

- Objetivo estratégico al cual contribuye.
- Objetivo del proyecto.
- Presupuesto asignado.
- Procesos que impacta el proyecto.
- Actividades críticas de continuidad del negocio que impacta el proyecto.
- Indicadores que miden los avances de las actividades.
- Fechas y entregables claves.
- Personal y áreas que participarán en el proyecto.
- Activos de información de los procesos que serán utilizados en el marco del proyecto.
- Proveedores involucrados.
- Marco normativo a considerar.

10.1.4. Establecimiento del Contexto a Nivel de Procesos

Para el análisis del contexto, se tiene en cuenta como base de información, adicional al marco estratégico y a sus factores internos y externos, la caracterización de cada uno de los procesos, contemplando el objetivo, alcance, subprocesos, herramientas tecnológicas, terceros que lo soportan y responsables del proceso. Por lo cual es importante que los Líderes de Procesos, con el apoyo de sus Gestores Integrales y bajo la coordinación de la Gerencia de Sistemas Integrados de Gestión, aseguren que estos se encuentren documentados y actualizados para aplicar la metodología de gestión de riesgos.

Así las cosas, los siguientes son los elementos mínimos que se deberán considerar y documentar en el establecimiento del contexto en cada uno de los procesos del mapa de procesos de Colpensiones:

- Objetivos estratégicos vinculados al proceso.
- Objetivo del procesos y características claves.
- Actividades claves utilizadas por el proceso para el cumplimiento del objetivo.
- En el marco del Sistema de Gestión de Continuidad del Negocio, y de acuerdo con la Matriz de Análisis de Impacto del Negocio – Matriz BIA, identificar las actividades críticas en materia de continuidad del negocio.
- En el marco del Sistema de Gestión de Seguridad de la Información y Ciberseguridad y de acuerdo con la información contenida en la Matriz de Activos de Información – Matriz MAI, identificar los activos de información clasificados en crítico en alguno de los pilares de seguridad de la información (Integridad, Confidencialidad y Disponibilidad).
- Sistemas de información utilizados en la operación.
- Estructura Organizacional que soporta el proceso.
- Proveedores o terceros que soportan el proceso.
- Marco Legal.
- Los eventos de riesgo materializados en el último año.
- Las tipologías de fraude y corrupción identificadas.

Para el establecimiento del contexto son claves, las siguientes fuentes de información:

- Direccionamiento Estratégico.
- Caracterización del proceso.
- Matriz de Activos de Información – MAI
- Matriz de Análisis de Impacto del Negocio – BIA
- El Manual de Funciones.
- La relación de contratos o convenios que soportan el proceso.
- El Normograma.
- La base consolidada de eventos de riesgo.

La información del contexto es clave en la siguiente etapa del proceso de gestión de riesgos, ya que con ella se asegura la correcta y completa identificación de riesgos en cada una de las tipologías alcanzadas por el Sistema Integral de Administración de Riesgos, y que permitirán establecer los planes de mejora.

10.2. EVALUACIÓN DE RIESGOS

La evaluación de riesgos es un proceso dinámico e interactivo que le permite a la entidad identificar, analizar y valorar el riesgo y las oportunidades, gestionando aquellos eventos tanto internos, como externos, que puedan afectar el logro de los objetivos estratégicos, de proyectos y de procesos o que puedan potenciar sus efectos positivos.

Con el establecimiento de los niveles de riesgo se dispondrá de una base para definir la prioridad de tratamiento para los riesgos y oportunidades identificadas.

10.2.1. Identificación de Riesgos

La identificación de riesgos y oportunidades es permanente y parte de los objetivos estratégicos de la Entidad y de su adecuado despliegue descendente a los objetivos de los macroprocesos y/o procesos, diferenciando entre el riesgo que afecta el cumplimiento de los objetivos, las oportunidades y las causas que lo generan

Los riesgos y oportunidades son identificados en tres niveles:

- **Riesgos Estratégicos y Emergentes**: La gestión de riesgos estratégicos busca crear valor. Los riesgos estratégicos se identifican con base en el análisis del contexto interno (Riesgos Estratégicos Internos) y el contexto externo (Riesgos Emergentes), considerando las debilidades y fortalezas de la entidad, y las amenazas y oportunidades de su entorno. El ejercicio de identificación de riesgos estratégicos es liderado por la Vicepresidencia de Seguridad y Riesgos Empresariales.

- **Riesgos Tácticos**: La gestión de riesgos tácticos busca crear y proteger, ya que debe asegurar el avance en el cumplimiento del plan estratégico, manteniendo los niveles de riesgo de los procesos impactados. Son riesgos identificados sobre los proyectos de la entidad, considerando el objetivo del mismo, sus entregables claves, los costos y tiempos del mismo, los procesos y sistemas de información que afecta, los activos de información que utilizará y las actividades críticas a nivel de continuidad del negocio.

  El ejercicio de identificación de riesgos es responsabilidad de la primera línea de defensa, en cabeza del líder del proyecto, complementando la visión de riesgos con el concepto de la segunda línea de defensa.

- **Riesgos por Proceso**: La gestión de riesgos sobre procesos busca proteger valor. La identificación de los riesgos por procesos se basa en el análisis del contexto de los procesos establecidos en el mapa de procesos de la Entidad. La identificación de este tipo de riesgos es responsabilidad de los líderes de proceso en coordinación con los gestores integrales y con la participación de los colaboradores del proceso. Sin perjuicio de lo anterior, es responsabilidad de la Gerencia de Riesgos y Seguridad de la información, implementar controles de calidad sobre la labor desempeñada por la primera línea de defensa, con el fin de poder identificar oportunamente deviaciones y así poder tomar las acciones respectivas.

En el marco del proceso de identificación de riesgos se debe:

- Identificar los eventos que pueden impactar positiva o negativamente el logro de los objetivos estratégicos, del plan o proyecto o de los procesos.
- Identificar las causas que lo pueden originar y el factor de riesgo asociado.
- Identificar la línea o líneas de negocio a la que aplica el riesgo.

Esta etapa debe permitir la identificación de los riesgos asociados a cada una de las tipologías establecidas.

En la identificación y redacción del riesgo se deberán tener presentes las siguientes premisas:

- En los riesgos estratégicos se deben identificar riesgos para todas las tipologías de riesgos.
- Para los riesgos tácticos y por proceso, es importante considerar que no todas las tipologías de riesgos aplican a todos los proyectos o procesos, esto dependerá del análisis del contexto realizado.
- Los riesgos y sus causas no se redactan como la ausencia de un control, Ejemplo: No realizar las conciliaciones bancarias, error de consulta en listas.
- La descripción del riesgo no debe iniciar con términos negativos "*No…, ausencia de, falta de, debilidades en*", entre otras, entendiéndose estas como causas generadoras del riesgo.
- Los riesgos de fraude y corrupción deben contemplar en su descripción los componentes de su definición: Acción u omisión + Uso del poder + Desviación de la gestión de lo público + el beneficio privado, es decir: "*Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio para terceros…".*

10.2.1.1. Identificación de Riesgos Estratégicos y Emergentes

El ejercicio de identificación de Riesgos Estratégicos y Emergentes de realiza de forma anual con validación semestral. El ejercicio es liderado por la Vicepresidencia de Seguridad y Riesgos Empresariales y comprende la información de las siguientes partes Interesadas:

- Gobierno y Ministerio del Trabajo, a través de los informes y perspectivas publicadas sobre variables que se pueden afectar a Colpensiones.
- Junta Directiva a través del ejercicio de planeación estratégica y los pronunciamientos realizados a través de sus sesiones.
- Alta Dirección (Presidente, Vicepresidentes, Jefes de Oficinas, Gerentes y Directores)
- Órganos de Control, tales como la Oficina de control Interno y Revisoría Fiscal a través de los informes de auditorías realizados.
- Entidades de Supervisión como la Superintendencia Financiera de Colombia a través de los informes y publicaciones realizadas.

Con base en esta información, la identificación de riesgos estratégicos y emergentes se realiza a través de elementos del método Delphi. Esta técnica permite llegar a un consenso de la opinión de un grupo de expertos. La característica principal es que los expertos formulan sus opiniones de forma individual, y conocen las opiniones de los otros expertos a medida que el proceso avanza.

Así las cosas, la identificación de riesgos estratégicos y emergentes se realiza en tres fases, así:

- Fase I: Propuesta de Riesgos Estratégicos y Emergentes realizada por la Vicepresidencia de Seguridad y Riesgos Empresariales.

- Fase II: Validación de áreas especiales: Esta descripción es puesta en consideración de los Vicepresidentes, Gerentes y Directores de las siguientes áreas claves:

    - Vicepresidencia de Gestión Corporativa, riesgos Vinculados al factor humano.
    - Vicepresidencia de Planeación y Tecnologías de la Información, riesgos vinculados a los factores de riesgo Político y Tecnológico.
    - Vicepresidencia de Comercial y de servicio al Ciudadano, los riesgos asociados a factores de riesgo social y Competitivo.
    - Vicepresidencia de Operaciones de RPM y Vicepresidencia de Beneficios Económicos los riesgos asociados a los factores de riesgos económicos, financieros y legales.
    - Oficina Asesora de Asuntos Legales, los riesgos asociados al factor de riesgo Legal.

  De acuerdo con las observaciones realizadas por estas áreas, la Vicepresidencia de Seguridad y Riesgos Empresariales actualiza la propuesta de riesgos estratégicos y emergentes.

- Fase III: Validación de la Alta Dirección: Finalmente se realiza una validación de los riesgos, poniendo en conocimiento de todos los Vicepresidentes, Jefes de Oficinas, Gerentes y Directores, la propuesta de riesgos para conocer sus observaciones o identificación adicional de nuevos riesgos.

El resultado de esta identificación se registra en la matriz de riesgos estratégicos que describe al menos la siguiente información:

- Factor de Riesgo
- Descripción del Riesgo
- Objetivo Estratégico Asociado.

10.2.1.2. Identificación de Riesgos Tácticos

La identificación de Riesgos Tácticos hace referencia a la identificación de riesgos sobre los proyectos institucionales que buscan cumplir el plan estratégico de Colpensiones.

La identificación de riesgos tácticos es realizada para cada uno de los planes o proyectos de la entidad, y bajo la responsabilidad del líder del proyecto con el acompañamiento de su equipo de trabajo, como primera línea de defensa, y con la orientación de los articuladores de riesgos de proyecto, adscritos a la Gerencia de Riesgos y Seguridad de la Información.

De acuerdo con el alcance del proyecto, se deberán identificar riesgos considerando las tipologías que le apliquen, ya sean riesgos operacionales, de seguridad de la información y ciberseguridad, de fraude y corrupción, de continuidad del negocio, de lavado de activos y financiación del terrorismo o financieros.

Como fuentes de información para la identificación de riesgos se deberán considerar las siguientes:

- Riesgos materializados en proyectos pasados o en curso similares.
- Informes de Auditoría realizados sobre proyectos similares.
- Eventos de riesgos materializados sobre proyectos.

En los proyectos se debe realizar la identificación de los riesgos teniendo en cuenta cada una de las etapas del ciclo de vida del proyecto, el objetivo, el alcance, los grupos de interés, los activos de información utilizados en el proyecto, los factores externos y las actividades claves en su implementación y las amenazas que puedan influir de manera significativa en el logro del objetivo del proyecto.

La línea base de riesgos tácticos que pueden afectar el cumplimiento del objetivo del proyecto están asociados a atributos como de oportunidad, calidad, alcance, integridad, confidencialidad y disponibilidad de la información; razón por la cual se debe tener en cuenta las actividades claves para el desarrollo del proyecto e identificar los riesgos asociados a:

- Oportunidad: Retraso en la ejecución de las actividades del proyecto.
- Calidad: Deficiencias en la ejecución de las actividades/entregables del proyecto.

- Completitud: Cambios en el alcance del proyecto
- Integridad: Debilidades en la precisión, coherencia y completitud de la información utilizada en el proyecto
- Confidencialidad: Divulgación o entrega de información no autorizada
- Disponibilidad: Falta de acceso a la información requerida en el proyecto.

La identificación de riesgos sobre los proyectos se realizará en las siguientes etapas:

- Etapa I: Entrenamiento y preparación: La Gerencia de Riesgos y Seguridad de la Información, realiza una sesión de entrenamiento y preparación del equipo de trabajo del proyecto, incluyendo al líder del mismo, entregando la siguiente información:

    - Lineamientos para la identificación de riesgos tácticos o sobre proyectos.
    - Línea base de riesgos sobre proyectos.
    - Tipologías de Gestión de Riesgos en Colpensiones.
    - Técnica de lluvia de ideas, que es, y como aplicarla.
    - Explicación del procedimiento a seguir para la identificación de riesgos.

- Etapa II: Identificación de riesgos por la primera línea de defensa: El líder el proyecto, de acuerdo con la información recolectada en la etapa de Evaluación del contexto del proyecto, en conjunto con el equipo del proyecto, realizará la identificación de riesgos y causas del mismo, considerando la línea base de riesgos tácticos, los riesgos particulares del proyecto por cada una de las tipologías de riesgo establecidas y los riesgos del proyecto sobre los procesos de la entidad. Para ello utilizará la técnica de lluvia de ideas. Los riesgos identificados, serán registrados en la matriz de riesgos del proyecto, considerando al menos la siguiente información:

    - Descripción del riesgo
    - Causas que lo originan
    - Factor del riesgo
    - Tipología del riesgo

- Etapa III: Validación de Riesgos por la segunda línea de defensa: El líder del plan o proyecto debe remitir la matriz de riesgos del proyecto diligenciada en su etapa de identificación de riesgos al articulador de riesgos de la Gerencia de Riesgos y Seguridad de la Información, quien tendrá la responsabilidad de:

    - Analizar la información del contexto del proyecto.
    - Validar la correcta descripción del riesgo y sus causas asociadas, solicitando ajustes sobre la misma.
    - Complementar la visión de la primera línea de defensa sobre los riesgos del proyecto.

- Etapa IV: Aprobación de Riesgos del Proyecto: Con la visión adicional de los riesgos del proyecto por parte de la segunda línea de defensa, el líder del proyecto confirmará o ajustará la matriz de riesgos del proyecto y dará paso a las etapas siguientes de construcción de la misma.

Es importante señalar, que la identificación de los riesgos sobre el plan o proyecto es un proceso dinámico. Es decir, en la medida en que avance el proyecto, pueden identificarse nuevos riesgos que deben ser incorporados bajo la responsabilidad del líder del proyecto en la matriz de riesgos del mismo.

10.2.1.3. Identificación de Riesgos Por Proceso

La identificación de riesgos por proceso es una actividad que debe ser validada por el líder del proceso en coordinación con su gestor integral, por lo menos una vez cada seis meses, y debe tener en cuenta:

- Los cambios realizados al proceso
- Los nuevos marcos normativos o la modificación a los existentes
- La implementación de nuevas tecnologías
- Los eventos de riesgo materializados
- El desarrollo de nuevos productos o servicios
- La inclusión de nuevos procesos en el mapa del proceso de la entidad
- La inclusión en nuevos mercados
- Las auditorías o seguimientos realizados al proceso

Con base en la información del contexto y considerando las tipologías de riesgos que componen el sistema integral de administración de riesgos, los riesgos por proceso se identifican considerando la siguiente información:

Tipología de Riesgo	Información mínima del Contexto a utilizar	Características claves para identificar el riesgo	Factores de Riesgos a Evaluar
Operacional	• Objetivo del proceso • Actividades Claves • Marco legal • Proveedores o terceros que soportan el proceso • Eventos de Riesgo • Sistemas de Información	• Oportunidad • Calidad • Incumplimiento Legal	• Recurso Humano • Tecnología • Infraestructura • Procesos • Acontecimientos Externos
Seguridad de la Información y Ciberseguridad	• Objetivo del proceso • Activos de Información • Las necesidades del proceso para el procesamiento,	• Confidencialidad • Integridad • Disponibilidad	• Recurso Humano • Tecnología • Infraestructura • Procesos

	almacenamiento y comunicación de la información • Marco legal • Proveedores o terceros que soportan el proceso • Incidentes de Seguridad		• Acontecimientos Externos
Continuidad del Negocio	• Objetivo del proceso • Actividades Críticas de acuerdo con el análisis de impacto del negocio BIA. • Marco legal • Proveedores o terceros que soportan el proceso	• Indisponibilidad de recursos (Tecnológicos, Humanos o de Infraestructura) para el desarrollo de la actividad.	• Recurso Humano • Tecnología • Infraestructura • Procesos • Acontecimientos Externos
Fraude y Corrupción	• Objetivo del proceso • Actividades Claves • Activos de Información • Marco legal • Proveedores o terceros que soportan el proceso • Tipología de Fraude	• Acción u omisión • Uso del poder • Desviación de la gestión de lo público • Beneficio Privado	• Recurso Humano • Tecnología • Infraestructura • Procesos • Acontecimientos Externos.
Lavado de Activos y Financiación del Terrorismo	• Objetivo del proceso • Actividades Claves • Marco legal • Proveedores o terceros que soportan el proceso • Tipologías de LA/FT • Señales de Alerta de LA/FT	• Apariencia de origen licito de recursos o bienes. • Financiar actividades delictivas	• Jurisdicción • Canales • Clientes • Productos • Usuarios
Riesgos Financieros	• Objetivo del proceso • Actividades clave • Marco legal • Proveedores o terceros que soportan el proceso	• Pérdidas Económicas asociadas al comportamiento de los portafolios administrados. • Pérdidas Económicas a raíz de indisponibilidad de recursos.	• Tasas de Interés • Valor de la UVR

Tabla 7. Criterios del Análisis de Contexto por Proceso

Tal como se señala en la tabla anterior, para identificar riesgos en las diferentes tipologías, se deberá considerar:

- Para la identificación de los riesgos de seguridad de la información y ciberseguridad, se tendrán en cuenta los principales activos de la información contemplados en la Matriz de Activos de la Información – MAI y la valoración de su criticidad.
- Para la identificación de los riesgos de continuidad del negocio, se tendrán en cuenta las actividades críticas establecidas en la matriz de análisis de impacto del negocio – BIA. Para lo cual, se debe tener presente aspectos que afecten la disponibilidad del proceso; hacerse

preguntas como: - el proceso se ve afectado por indisponibilidad de la infraestructura de tecnología? - del lugar físico de operación? - del personal del proceso? - de contratistas que apoyan el proceso?, entre otros.

- Para la identificación de los riesgos de lavado de activos y financiación del terrorismo, se deben analizar los procesos y aquellas actividades que se ejecuten y respondan a las preguntas: ¿el proceso vincula clientes o usuarios? - ¿El proceso recibe recursos de clientes o usuarios? - ¿El proceso reconoce alguna prestación económica? - ¿El proceso gira recursos a clientes o usuarios?
- Para la identificación de los riesgos financieros se contemplarán los procesos que en sus actividades administren y gestionen recursos financieros.
- Si el objetivo del proceso o sus actividades son soportadas a través de un contrato con terceros, deberán identificarse los riesgos y causas, asociados a este proveedor.

De igual manera, en la identificación de los riesgos para las diferentes tipologías, se debe considerar la identificación de los objetivos de control asociados a cada uno de estos.

Objetivos de Cumplimiento: Están relacionados con el cumplimiento de las leyes y regulaciones a las que está sujeta la entidad. La entidad debe desarrollar sus actividades en función de las leyes y normas específicas.

Objetivos Operativos: Se relacionan con el cumplimiento de la misión y visión de la entidad. Hacen referencia a la efectividad y eficiencia de las operaciones, incluidos sus objetivos de rendimiento financiero y operacional, y la protección de sus activos frente a posibles pérdidas.

Objetivos de Información: Se refieren a la preparación de reportes para uso de la organización y los accionistas, teniendo en cuenta la veracidad, oportunidad y transparencia. Estos reportes relacionan la información financiera y no financiera interna y externa y abarcan aspectos de confiabilidad, oportunidad, transparencia y demás conceptos establecidos por los reguladores, organismos reconocidos o políticas de la entidad.

Esta identificación permitirá a la Organización establecer los riesgos de cumplimiento asociados a la Legislación, Normatividad, Reglamentos y el Código de ética; así como establecer medidas de mitigación ante los riesgos que se puedan presentar en un momento dado por un posible incumplimiento de una norma, ya sea externa o interna. En este sentido, también le permite establecer el perfil de riesgo de cumplimiento, tanto en cada uno de los procesos, como a nivel institucional.

Autoevaluación de Riesgos y Controles:

La identificación o actualización de riesgos a nivel de procesos se realiza a través del ejercicio de Autoevaluación de Riesgos y Controles, cumpliendo las siguientes etapas:

- Etapa I: Lanzamiento del ejercicio de Autoevaluación de Riesgos y Controles: El lanzamiento semestral del ejercicio es realizado por la Gerencia de Riesgos y Seguridad de la información, área que suministrará al menos la siguiente información:

    - Avances en la gestión de riesgos durante el último semestre.
    - Lineamientos y principales enfoques del ejercicio
    - Eventos de Riesgo, incidentes de seguridad, tipologías de fraude, señales de alerta de LA/FT acaecidos en el último año.
    - Resultados de los indicadores que permiten monitorear los riesgos de los procesos.
    - Principales hallazgos de los órganos de control en materia de gestión de riesgos.
    - Debilidades y oportunidades de mejora a considerar.

- Etapa II: Actualización de Riesgos y Controles: Etapa liderada por la primera línea de defensa en cabeza de los Gerentes y Directores en coordinación con el gestor integral del proceso y demás funcionarios del área. En esta etapa, se considerará la información suministrada por la Gerencia de Riesgos y Seguridad de la información, los cambios en el proceso y demás información que actualice el contexto del proceso. Con base en ello, se actualizarán los riesgos del proceso y sus causas asociadas, ya sea, modificando los existentes o adicionando nuevos riesgos identificados. En esta etapa, se deberán considerar todas las tipologías de riesgos aplicables al proceso. Como resultado de esta etapa, el líder del proceso remitirá a la Gerencia de Riesgos y Seguridad de la Información la matriz de evaluación de riesgos actualizada.

- Etapa III: Validación de Riesgos por parte de la Segunda Línea de Defensa: En esta etapa, La Gerencia de Riesgos y Seguridad de la Información, con el fin de validar el ejercicio realizado por la primera línea de defensa, realizará las siguientes actividades:

    - Tomará una muestra de los riesgos actuales y verificará que los mismos conserven su adecuada descripción e identificación.
    - Validará que todos los nuevos riesgos incorporados, cumplan con los lineamientos del presente manual.
    - Calificará la gestión de riesgos de la primera línea de defensa con relación a dos criterios:
        - Oportunidad en la entrega de la Información.
        - Calidad de la actualización realizada, considerando. La adecuada descripción de los riesgos, la adecuada descripción de las causas y el cumplimiento de la metodología.
        - Completitud de la información actualizada: de acuerdo con la validación de los eventos de riesgo del proceso y de los conceptos emitidos desde la Gerencia de Riesgos y Seguridad de la Información, se validará si la actualización se realizó de forma completa.

Finalmente, la Gerencia de Riesgos y Seguridad de la Información, remitirá su concepto y observaciones a los Gerentes, Directores y gestor Integral, para los ajustes respectivos.

- Etapa IV: Aprobación Matriz de Evaluación de Riesgos: Con la visión adicional de los riesgos del proceso por parte de la segunda línea de defensa, el gestor Integral realizará los ajustes en la matriz de Evaluación de Riesgos y solicitará la aprobación de la misma por parte de los Gerentes y Directores. Una vez aprobada la matriz, la misma deberá ser actualizada en la herramienta ISOTOOLS, surtiendo el flujo de actualización de documentos definido (revisión y aprobación).

10.2.2. Análisis de Riesgos

El análisis de riesgos para los diferentes niveles (Estratégico, Táctico y por Proceso), tiene como objetivo realizar un entendimiento del riesgo, analizando sus causas originadoras, la probabilidad de que las mismas ocurran y los impactos que podría tener su materialización.

Así las cosas, el análisis de riesgos se realiza en tres instancias a saber:

- Análisis de Riesgos Inherente
- Análisis de Estrategias, Controles medidas mitigantes o para aumentar los efectos deseables.
- Análisis de Riesgo Residual

Los riesgos estratégicos no son mitigados a través de controles. El análisis de riesgo de este nivel se realiza considerando las estrategias definidas por la entidad en el marco de su direccionamiento estratégico.

10.2.2.1. <u>Análisis de Riesgo Inherente</u>

El análisis de riesgos inherente implica el desarrollo y la comprensión del riesgo sin considerar la existencia de controles. Busca identificar la probabilidad de ocurrencia de los riesgos y su impacto en caso de materializarse, a través de los criterios de evaluación definidos.

Criterios de Evaluación del Riesgo

La definición de los criterios de evaluación del riesgo debe considerar los siguientes aspectos:

- Es un ejercicio dinámico que debe validarse por lo menos una vez al año.
- El establecimiento de criterios debe estar alineado con el marco integral de apetito de riesgo definido.
- Debe emplear variables cuantitativas y cualitativas con el fin de maximizar la objetividad en la evaluación del riesgo.

- Debe reconocer las particularidades de los diferentes niveles de riesgo (Estratégico, Táctico y Por Procesos) y las particularidades de las diferentes tipologías alcanzadas por el sistema integral de administración de riesgos (Operacional, Continuidad del Negocio, Fraude y Corrupción, Seguridad de la Información y Ciberseguridad, Lavado de Activos y Financiación del Terrorismo y Riesgos Financieros).
- Deben estar definidos en función a la probabilidad de ocurrencia del riesgo y su impacto.

El resultado de la aplicación de dichos criterios se representará gráficamente a través de un mapa de calor conformado por una escala de cinco niveles, tanto para probabilidad, como impacto con la estructura que se muestra a continuación:

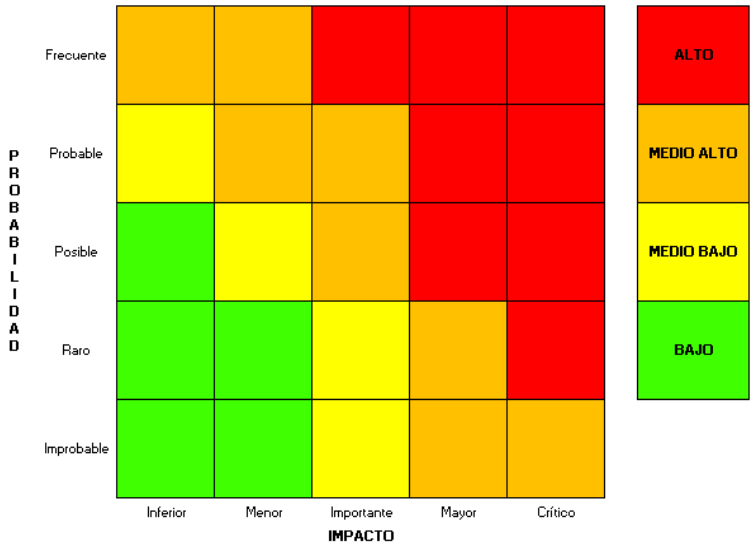


Ilustración 10. Mapa de Riesgos

Criterios de Probabilidad

La probabilidad se define como la posibilidad de ocurrencia del riesgo, la cual puede ser medida con criterios de frecuencia, si se ha materializado o de factibilidad, cuando se tiene en cuenta la presencia de factores internos y externos que pueden propiciar el riesgo, aunque este no se haya materializado.

Colpensiones ha determinado, los siguientes criterios mínimos de calificación del riesgo de acuerdo con la tipología del riesgo:

- ***Criterios para el análisis de Riesgos Estratégicos***

Tomando elementos de la metodología utilizada por el Word Economic Forum para la elaboración de su informe de riesgos mundiales, se utilizarán el siguiente criterio de probabilidad para el análisis de riesgos en este nivel:

Nivel	Frecuencia	Tipología de riesgo que le aplica
Frecuente	Se puede presentar más de una vez en al año.	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo. • Riesgos Financieros
Probable	Se puede presentar una vez al año.	
Posible	Se puede presentar una vez en dos años	
Raro	Se puede presentar una vez en cinco años	
Improbable	Sin probabilidad de ocurrir en los próximos 5 años.	

Tabla 8. Criterios de Probabilidad Riesgo Estratégico

Es importante considerar que de acuerdo con la metodología establecida para la identificación de riesgos a nivel estratégico (Metodología Delphi o Juicio de Expertos), esta valoración se realiza con base en el criterio cualitativo de cada experto, siguiendo las mismas etapas descritas en la identificación de riesgos.

- ***Criterios para el análisis de Riesgos Tácticos***

Para el análisis de riesgos tácticos se considerarán los siguientes criterios de probabilidad:

Nivel	Criterio	Tipología de riesgo a la que le aplica
Frecuente	Más de 12 eventos	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo. • Riesgos Financieros
	En más del 20% de los casos, transacciones o actividades	
Probable	Entre 6 y 12 eventos	
	Entre el 15% y el 20% de los casos, transacciones o actividades	
Posible	Entre 3 y 5 eventos	
	Entre el 10% y el 14.99% de los casos, transacciones o actividades	
Raro	Entre 1 y 3 eventos	
	Entre el 3% y el 9.99% de los casos, transacciones o actividades	

Improbable	No se han presentado	
	En menos del 3% de los casos, transacciones o actividades	

Tabla 9. Criterios de Probabilidad Riesgo Táctico

Para el Análisis de Riesgos, se siguen las mismas etapas descritas en la identificación de riesgos.

- ***Criterios para el análisis de Riesgos por Proceso***

Para el análisis de riesgos por proceso, se considerarán los siguientes criterios:

No.	Criterio	Nivel	Frecuencia	Tipología de riesgo que le aplica
1.	Frecuencia de ejecución de la actividad que puede materializar el riesgo	Frecuente	De forma diaria	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo. • Riesgos Financieros
		Probable	Por lo menos una vez al mes	
		Posible	Por lo menos una vez al trimestre	
		Raro	Por lo menos una vez al semestre	
		Improbable	Por lo menos una vez al año	
2.	Eventos de riesgos presentados en el último año	Frecuente	Más de 12 eventos	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo. • Riesgos Financieros
		Probable	Entre 6 y 12 eventos	
		Posible	Entre 3 y 5 eventos	
		Raro	Entre 1 y 3 eventos	
		Improbable	No se han presentado	
3.	Frecuencia en que podría presentarse el riesgo en función del volumen de operaciones en un año.	Frecuente	En más del 20% de los casos, transacciones o actividades	• Operacional
		Probable	Entre el 15% y el 20% de los casos, transacciones o actividades	
		Posible	Entre el 10% y el 14.99% de los casos,	

			transacciones o actividades	
		Raro	Entre el 3% y el 9.99% de los casos, transacciones o actividades	
		Improbable	En menos del 3% de los casos, transacciones o actividades	
4.	Cambios sobre el proceso o su tecnología	Frecuente	En el último mes	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo.
		Probable	En los últimos 3 meses	
		Posible	En los últimos 6 meses	
		Raro	En el último año	
		Improbable	No se han presentado cambios	
5.	Permanencia del personal	Frecuente	Más del 30% tiene menos de 6 meses	• Operacional • Continuidad del Negocio • Seguridad de la Información y Ciberseguridad • Fraude y Corrupción • Lavado de Activos y Financiación del Terrorismo.
		Probable	Entre el 20% y el 30% tiene menos de 6 meses	
		Posible	Entre el 10% y el 19.9% tiene menos de 6 meses	
		Raro	Menos del 10% tiene menos de 6 meses	
		Improbable	Todos los colaboradores tienen más de 6 meses	

Tabla 10. Criterios de Probabilidad Riesgo por Proceso

Reconociendo las particularidades que se presentan en las diferentes tipologías de riesgo, pueden existir criterios de probabilidad adicionales en cada tipología. Estos criterios se detallan en cada una de las partes del presente manual.

Para el Análisis de Riesgos, se siguen las mismas etapas descritas en la identificación de riesgos.

Criterios de Impacto

Como impacto se entiende la consecuencia que puede ocasionar la materialización del riesgo.

Para determinar el impacto que puede ocasionar cada uno de los riesgos identificados tanto a nivel estratégico, táctico y por proceso, se debe considerar las declaraciones cualitativas y las mediciones cuantitativas del marco integral de apetito de riesgo.

A continuación, se mencionan los criterios mínimos a considerar en la evaluación del impacto de los riesgos identificados:

	Descripción
Crítico	**Económico:** Pérdida igual o superior al 8% de los ingresos operacionales de la Administradora. - Pérdida superior al 0,40% del valor del portafolio de la Administradora. **Legal:** Intervención por parte de los órganos de control Superintendencia Financiera de Colombia por incumplimientos legales y/o contractuales. **Ciudadanos:** Incremento de más del 40% del número de reclamos formulados por los clientes**.** **Continuidad del negocio:** Interrupción de las operaciones por más de 2 días. **Reputacional:** Imagen negativa en el mercado por mal servicio, prácticas inseguras y/o irregulares. Mala reputación generalizada debido a comentarios adversos ampliamente difundidos a través de medios masivos de comunicación.
Mayor	**Económico:** Pérdida igual o superior al 3% y menor al 8% de los ingresos operacionales de la Administradora. Pérdida entre el 0,30% y el 0,40% del valor del portafolio de la Administradora **Legal:** Sanciones económicas por incumplimiento de las normas establecidas por los entes reguladores. Apertura de procesos sancionatorios, disciplinarios o fiscales. **Ciudadanos:** Incremento entre el 31% y el 40% del número de reclamos formulados por los clientes. **Continuidad del negocio:** Interrupción de las operaciones entre 1 y 2 días. **Reputacional:** Imagen negativa generalizada a través de las redes sociales a consecuencia de las ineficiencias operativas en los servicios, atención ineficaz o inoportuna.
Importante	**Económico:** Pérdida igual o superior al 2% y menor al 3% de los ingresos operacionales de la Administradora. Pérdida entre el 0,20% y el 0,29% del valor del portafolio de la Administradora. **Legal:** Llamados de atención o requerimientos realizados por los entes reguladores a nivel nacional. **Ciudadanos:** Incremento entre el 21% y el 30% del número de reclamos formulados por los clientes. **Continuidad del negocio:** Interrupción de las operaciones entre 8 horas y 24 horas. **Reputacional:** Imagen negativa por mal servicio y/o irregulares difundidos a través de medios masivos de comunicación regionales.
Menor	**Económico:** Pérdida igual o superior al 1% y menor al 2% de los ingresos operacionales de la Administradora. Pérdida entre el 0,10% y el 0,19% del valor del portafolio de la Administradora. **Legal:** Llamados de atención o requerimientos realizados por los entes reguladores a nivel local o regional.

	Ciudadanos: Incremento entre el 10% y el 20% del número de reclamos formulados por los clientes. **Continuidad del negocio:** Interrupción de las operaciones menor a 8 horas. **Reputacional:** Imagen negativa por mal servicio y/o irregulares difundidos a través de medios masivos de comunicación locales (municipal).
Inferior	**Económico:** Pérdida inferior al 1% de los ingresos operacionales de la Administradora. Pérdida inferior al 0,10% del valor del portafolio de la Administradora. **Legal:** No genera incumplimientos legales. **Ciudadanos:** No incrementa significativamente el número de reclamos formulados por los clientes. No afecta las relaciones con los clientes. **Continuidad del negocio:** No hay interrupción de las operaciones. **Reputacional:** No afecta la imagen de la entidad

Tabla 11. Criterios de Impacto en Riesgos

Reconociendo las particularidades que se presentan en las diferentes tipologías de riesgo, pueden existir criterios de impacto adicionales en cada tipología. Estos criterios se detallan en cada una de las partes del presente manual. En particular, para el riesgo de corrupción se contemplan criterios acordes con lo definido en la Guía del Departamento Administrativo de la Función Pública.

La metodología define la opción de hasta 5 criterios de probabilidad e impacto, con 5 niveles de calificación por cada criterio. Cada uno de los criterios cuenta con un valor ponderado, cuya sumatoria de todos los criterios generados por cada tipología de riesgos, debe ser el 100%. Con base en esta ponderación la calificación se ubicará en un rango de 1 a 5 así:

Escala	Rango	
	igual a	menor a
Improbable	1	1,8
Raro	1,8	2,6
Posible	2,6	3,4
Probable	3,4	4,2
Frecuente	4,2	igual a 5

Tabla 12. Rangos de Ponderación Probabilidad

Una vez evaluados los criterios de probabilidad e impacto para cada riesgo, se ubicará en el mapa de riesgos acorde con cada una de las escalas de calificación definidas, estableciendo así, el nivel de riesgo inherente:

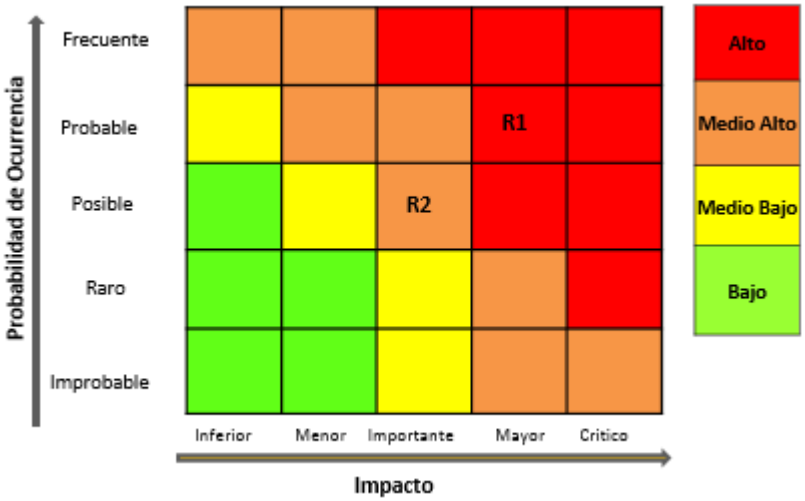


Ilustración 11. Mapa de Riesgos Inherente

10.2.2.2. Análisis de Estrategias, Controles y Medidas Mitigantes

- Análisis de Estrategias – Gestión de Riesgos Estratégicos

Los riesgos estratégicos y emergentes son mitigados a través de las estrategias planteadas por la organización en el marco de la planeación estratégica.

Dichas estrategias pueden tener dos objetivos:

- Mitigar los efectos no deseados de la materialización de un riesgo
- Aumentar los efectos deseados para el aprovechamiento de una oportunidad.

Considerando la metodología definida para la identificación y valoración de los riesgos estratégicos, las estrategias definidas se valoran bajo tres criterios:

- La estrategia mitiga impacto, probabilidad o ambas.
- Se considera que la estrategia mitiga el riesgo:
  - De forma adecuada
  - De forma moderada
  - De forma débil

Bajo estos componentes los expertos valoran la mitigación de los riesgos estratégicos.

- Análisis de Controles y Medidas Mitigantes – Gestión de Riesgos Tácticos y Por proceso

Las actividades de control se llevan a cabo en todos los niveles de la organización, en las diferentes etapas de los procesos de negocio y en el entorno tecnológico. Según su naturaleza, pueden ser preventivos, detectivos o correctivos, e incluye actividades manuales y automatizadas, tales como, pero sin limitarse a: autorizaciones y aprobaciones, verificaciones, conciliaciones, y revisiones de calidad que deben estar integradas con una adecuada segregación de funciones.

La documentación de las medidas de tratamiento (actividades de control), tendrá en cuenta los atributos asociados al diseño y ejecución establecidos en el presente documento.
En cuanto al diseño del control, su descripción debe contener los siguientes elementos:

Elemento	Descripción
No. Control	Corresponde al número consecutivo de los controles identificados y documentados en la matriz integral de riesgos. Su composición es: C-*XXX--001* XXX – Código definido para cada proceso, según la estructura del SIG. C – Letra equivalente a Control 001 – Tres números correspondiente al consecutivo.
¿Quién ejecuta el control?	Responsable de realizar la actividad del control (Rol / Cargo); para los controles automáticos se define el aplicativo en el cual se lleva a cabo el control
¿Con qué periodicidad ejecuta el control?	Frecuencia del Control (Cada cuanto se realiza)
¿Qué Hace?	Objetivo del control, define el para qué se realiza la actividad de control
¿Cómo lo hace?	Procedimiento llevado a cabo para cumplir con el objetivo del control
¿Qué pasa con las observaciones o desviaciones al control?	Establece el paso a seguir ante las observaciones encontradas en la ejecución del control, también debe contemplar si se realiza seguimiento a la actividad.
¿Cuál es la evidencia de la ejecución del control?	Registro soporte de la ejecución del control, que permita validar en algún momento su efectividad.

Tabla 13. Criterios Diseño del Control

En la identificación y documentación de los controles, también se deben tener en cuenta los siguientes atributos de control:

Criterio	Descripción
Nivel de responsable del control	Contempla la selección de los diferentes niveles de cargos establecidos en la estructura organizacional de Colpensiones. (ej. Director, Profesional, Jefe, etc)
Tipo de control	Por su oportunidad: *Preventivo*: Evitan que se materialicen los riesgos. *Detectivo*: Identifican los eventos de riesgo en el momento en que se presentan. *Correctivo*: Corrigen un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la causa ya se ha materializado pero que se corrige.
Forma de ejecución del control	Por su naturaleza: *Manual*: Son los que son desarrollados por una o más personas, y no requieren de tecnología o sistemas. *Automático*: Ejercido únicamente a través de sistemas o herramientas tecnológicas. *Dependiente de TI*: Se realiza con el apoyo de un sistema o herramienta tecnológica, pero no es totalmente automático.
Aplicación donde se ejecuta el Control	Para los controles automáticos y dependientes de tecnología de la información, corresponde a la herramienta tecnológica - software donde se ejecuta el control.
Referencia Documental	Documento oficializado en el Sistema Integrado de Gestión, donde se encuentra documentada la actividad de control descrita.

Tabla 14. Atributos del Control

Para mitigar los riesgos identificados en los procesos, hay causas que requieren documentar controles que pueden ser ejecutados por otras áreas o dependencias en razón a que un control puede mitigar una causa y un riesgo de un proceso, aunque éste no sea ejecutado por la misma área funcional.

Evaluación del diseño y ejecución de controles

En la evaluación de los controles se tienen en cuenta dos criterios, el diseño y la ejecución:

Diseño: Hace referencia a que los controles mitiguen de manera adecuada las causas internas o externas que puedan materializar los riesgos.

Ejecución: Busca asegurar que ésta se realice tal y como se diseñó.

Como resultado de la combinación de estos criterios se determina la solidez individual de cada control. A continuación, se presenta el detalle de los criterios utilizados para la evaluación de controles, así como, las ponderaciones dadas a cada una de ellas.

Criterios para la Evaluación del Diseño del Control: Criterio		Respuesta	Valor Diseño
Evaluación con respecto al Riesgo/Causa	¿El control permite mitigar la causa para la cual fue diseñado?	Si No	1 2
Evaluación con respecto al responsable	¿Se encuentra claramente identificado el responsable del control?	Si No	1 2
	¿El cargo que ejecuta el control es un cargo par o superior al que ejecuta la actividad que puede materializar el riesgo?	Si No	Informativo
	¿El responsable del control es diferente al responsable de ejecutar la actividad?	Si No	1 2
Evaluación con respecto a la frecuencia	¿Se encuentra claramente definida la frecuencia con la que se ejecuta el control?	Si No	1 2
	¿Con qué periodicidad se ejecuta el control versus la actividad que puede materializar el riesgo?	- Con la misma periodicidad en la que se ejecuta la actividad que puede materializar el riesgo - Con una periodicidad menor a la que se ejecuta la actividad que puede materializar el riesgo - Con una periodicidad mayor a la que se ejecuta la actividad que puede materializar el riesgo	1 2 3

Criterio		Respuesta	Valor Diseño
Evaluación con respecto a las actividades que componen el control	¿El control contempla la descripción del qué y el cómo se realiza?	Si No	1 2
	¿El control se ejecuta sobre una muestra o sobre cada operación/actividad?	- Cada operación/actividad - Muestra definida y documentada en el proceso - Muestra a criterio del funcionario	1 2 3
	¿El control se ejecuta de forma manual, dependiente de TI o automática?	- Automática - Dependiente de TI - Manual	1 2 3
	¿El control se realiza de forma preventiva, detectiva o correctiva?	- Preventiva - Detectiva - Correctiva	1 2 3
	¿El control describe la forma en que se manejan las excepciones?	Si No	1 2
Evaluación con respecto a las evidencias del control	¿El control describe de forma clara el soporte documental que se deja como evidencia de la ejecución del control?	Si Parcial No	1 2 3
	¿La evidencia se deja en todo momento sin importar el resultado de la ejecución del control?	Si No	1 2
	¿Cuál es el nivel de documentación del control?	- Documentado / revisado o actualizado en el último año - Documentado / no revisado o actualizado en el último año - No Documentado	1 2 3

Tabla 15. Criterios de Calificación del Diseño del Control

Calificación del Diseño del Control:

Con base en la evaluación de cada uno de los criterios de diseño del control, mencionados anteriormente, se obtiene una calificación de 1 a 3, la cual se ubica en una de las siguientes escalas:

Calificación del Diseño del Control		
Escala	Rango	
	igual a	menor a
Fuerte	1	1,67
Moderado	1,67	2,33
Débil	2,33	Igual a 3

No. Criterios Diseño Control	13

Tabla 16. Calificación del Diseño del Control

A partir de la calificación de este conjunto de variables se determina la evaluación del diseño de cada control y se establece si hay o no lugar a observaciones frente al diseño:

- Fuerte: El control está bien diseñado para mitigar el riesgo.
- Moderado: El control tiene oportunidades de mejora en el diseño.
- Débil: El control tiene debilidades significativas en su diseño para mitigar en forma adecuada la causa o falla.

Criterios para la Evaluación de la Ejecución del Control Criterio		Respuesta	Valor Diseño
Ejecución actual	¿El control es ejecutado siguiendo las actividades descritas en el mismo?	SI No	1 2
Responsable	¿El control es ejecutado por el cargo/rol definido en su diseño?	SI No	1 2
Frecuencia	¿El control es ejecutado con la frecuencia definida en su diseño?	SI No	1 2
Actividades	¿Las excepciones del control son ejecutadas acorde con lo establecido en el diseño?	SI No	1 2
Evidencia	¿Se conservan los registros soportes de la ejecución del control?	SI No	1 2
Divulgación	¿El control ha sido informado formalmente en el último año al responsable de su ejecución?	SI No	1 2

Tabla 17. Criterios de Calificación de la Ejecución del Control

Calificación de la Ejecución del Control:

Con base en la evaluación de cada uno de los criterios de ejecución del control, mencionados anteriormente, se obtiene una calificación de 1 a 3, la cual se ubica en una de las siguientes escalas:

Calificación de la Ejecución del Control		
Escala	Rango	
	igual a	menor a
Fuerte	1	1,67
Moderado	1,67	2,33
Débil	2,33	Igual a 3

No. Criterios Ejecución Control	6

Tabla 18. Calificación de la Ejecución del Control

Este criterio se califica de acuerdo con las definiciones dadas por los responsables de los procesos, y periódicamente a partir de los resultados de los informes de los entes de control al proceso, eventos de riesgos registrados, resultados de los indicadores; y evalúa en qué medida el control es ejecutado de acuerdo con las criterios y variables definidas en el diseño del control.

- *Fuerte*: El control siempre se ejecuta de acuerdo a las variables del diseño del control y no existen observaciones de la Oficina de Control Interno y/o otros entes de control, ni eventos de riesgo asociados o desviaciones en los indicadores, con relación a la ejecución del control.

- *Moderado:* El control no se ejecuta permanentemente como fue diseñado y/o existen observaciones de la Oficina de Control Interno u otros entes de control, eventos de riesgo asociados o desviaciones en los indicadores, con relación a que a veces si se ejecuta el control y otras veces no.

- *Débil*: El control no se ejecuta como está diseñado y/o existen informes de la Oficina de Control Interno u otros entes de control, eventos de riesgo asociados o desviaciones en los indicadores, que así lo establecen.

Solidez Individual del Control:

La combinación entre el diseño y la ejecución del control determina la solidez individual del control, lo cual corresponde a un cálculo automático, con un rango de calificación entre 1 y 3, el cual se ubica en alguna de las siguientes escalas:

Solidez Individual del Control		
Escala	Rango	
	igual a	menor a
Fuerte	1	1,67
Moderado	1,67	2,33
Débil	2,33	Igual a 3

Tabla 19. Solidez Individual del Control

De lo anterior, se obtienen los siguientes resultados posibles:

- *Fuerte*: El control está bien diseñado y se ejecuta adecuadamente.
- *Moderado*: El control puede tener oportunidades de mejora en el diseño y/o en la ejecución del control.
- *Débil*: El control no está bien diseñado o no se ejecuta.

Solidez del Conjunto de Controles:

Esta variable se determina promediando la calificación individual de la solidez de los controles establecidos para mitigar las fallas y causas asociadas a cada riesgo. Corresponde a un cálculo automático, con un rango de calificación entre 1 y 3, el cual se ubica en alguna de las siguientes escalas:

Solidez del Conjunto de Controles		
Escala	Rango	
	igual a	menor a
Fuerte	1	1,67
Moderado	1,67	2,33
Débil	2,33	Igual a 3

Tabla 20. Solidez del Conjunto de Controles

- *Fuerte* – Corresponde controles fuertes que están bien diseñados y operando adecuadamente.
- *Moderado* – Esta calificación genera oportunidades de mejora en el diseño y/o en la ejecución del control.
- *Débil:* Esta calificación indica que los controles no están bien diseñados o no se ejecutan adecuadamente por los responsables de los procesos.

Mitigación de probabilidad e impacto:

Una vez calificados el conjunto de controles frente a cada riesgo, se determina si los controles definidos mitigan la probabilidad y/o el impacto del riesgo con los siguientes resultados:

Probabilidad:

- *Fuerte*: Existen controles diseñados específicamente a mitigar la probabilidad de que el riesgo se materialice (controles que van directamente a disminuir la probabilidad).
- *Moderado:* Existen controles que están mitigando la probabilidad de que el riesgo se materialice, pero de una manera indirecta.
- *Débil:* Los controles asociados para mitigar el riesgo no están mitigando la probabilidad que pueda conllevar a la disminución del riesgo o son muy débiles para su mitigación.

Impacto:

- *Fuerte:* Existen controles diseñados específicamente a mitigar el impacto en caso de que el riesgo se materialice de una manera directa.
- *Moderado*: Existen controles que están mitigando el impacto en caso de que el riesgo se materialice, pero de una manera indirecta.
- *Débil:* Los controles asociados para mitigar el riesgo no están mitigando el impacto en caso de que el riesgo se materialice.

10.2.2.3. Análisis de Riesgo Residual

El riesgo residual es el resultado del desplazamiento del riesgo inherente por la aplicación de los controles, es decir, considerando el nivel de mitigación de la probabilidad y el impacto descrito anteriormente.

Teniendo en cuenta que en la metodología de administración integral de riesgos de Colpensiones, los controles juegan un papel importante en el desplazamiento en el mapa de riesgos, a continuación se presenta en detalle los resultados de los posibles desplazamientos de la probabilidad y el impacto del riesgo, el cual se es establece a partir de un cálculo automático, tomando como base la calificación individual de los controles que componen cada uno de los riesgos, acorde con las variables asociadas a si el control está diseñado para mitigar la probabilidad o el impacto, o los dos.

En este entendido, el nivel de desplazamiento será máximo hasta la calificación de la solidez del conjunto de controles (Fuerte, Moderado o Débil) y seguido de este, la calificación máxima será la

de los controles diseñados para mitigar la probabilidad o el impacto.

De acuerdo con lo anterior, a continuación, se presenta la tabla de desplazamiento:

Rangos de Mitigación de la Probabilidad:

Solidez Conjunta de Controles	Solidez Individual Control (Mitiga Probabilidad)	Rango Mitigación Probabilidad	
		Mínimo	Máximo
Fuerte	Fuerte	1,33	2,00
	Moderado	0,67	1,33
	Débil	0,00	0,67
Moderado	Fuerte - Moderado	0,67	1,33
	Débil	0,00	0,67
Débil	Fuerte - Moderado - Débil	0,00	0,67

Tabla 21. Rangos de Mitigación de la Probabilidad

Rangos de Mitigación del Impacto:

Solidez Conjunta de Controles	Solidez Individual Control (Mitiga Impacto)	Rango Mitigación Impacto	
		Mínimo	Máximo
Fuerte	Fuerte	1,33	2,00
	Moderado	0,67	1,33
	Débil	0,00	0,67
Moderado	Fuerte - Moderado	0,67	1,33
	Débil	0,00	0,67
Débil	Fuerte - Moderado - Débil	0,00	0,67

Tabla 22. Rangos de Mitigación del Impacto

Resultado Mapa de Riesgos Residual:

Una vez evaluada la solidez de los controles establecidos para cada riesgo y el efecto de la mitigación, se ubicará el riesgo en el mapa de calor acorde con cada una de las escalas de calificación definidas, estableciendo así, el nivel de riesgo residual:

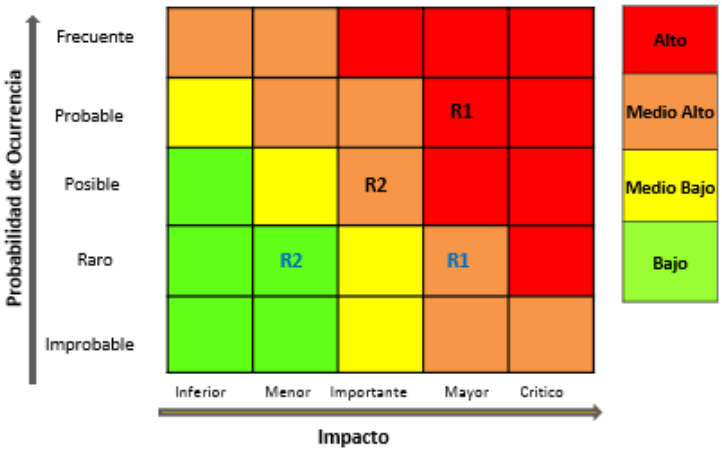


Ilustración 12. Mapa de Riesgos Residual

10.2.3. Valoración de Riesgos

El propósito de la valoración de riesgos es facilitar la toma de decisiones basada en los resultados de los análisis del riesgo y comparándolos con los criterios de valoración del riesgo.

De forma general, el apetito de riesgo en función a los criterios de valoración se muestra en el siguiente gráfico:

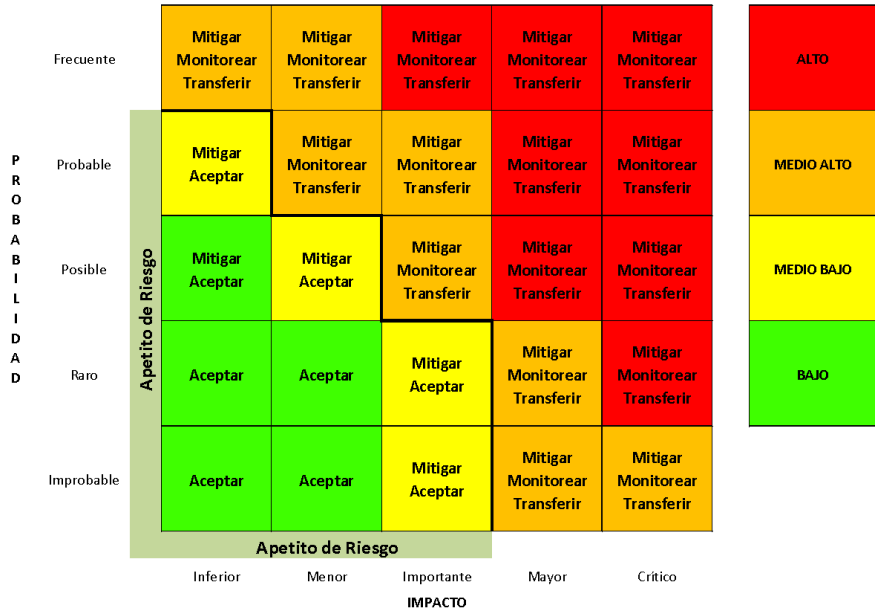


Ilustración 13. Mapa de Tratamiento de Riesgos

Así las cosas, y de acuerdo con el análisis de riesgo residual de los riesgos, se deberán tomar las siguientes acciones de acuerdo con el nivel del riesgo, con miras a definir el tratamiento a emplear y escalarlo en el marco de gobierno de la gestión integral de riesgos:

Nivel de Riesgo	Acción
Alto	Requiere acción inmediata, presentación de los riesgos y plan de acción al Comité de Auditoría y a la Junta Directiva.
Medio Alto	Necesita atención del Representantes legales, presentación de los riesgos y plan de acción a los Comités de Riesgos establecidos, según corresponda a la tipología de riesgos y al Comité de Auditoría.
Medio Bajo	Gestión del tratamiento por medio de Vicepresidencias y/o Gerencias.
Bajo	Administrar mediante procedimientos de rutina

Tabla 23. Gobierno del Tratamiento de Riesgos

MANEJO DE CONTROVERSIAS

El líder del proceso como responsable de los riesgos, si dentro de su debida diligencia decide no identificar o reconocer un riesgo, debe asumir las consecuencias de esta decisión.

En el evento en que el responsable de la Vicepresidencia de Seguridad y Riesgos Empresariales identifique un riesgo y el responsable correspondiente, no esté de acuerdo y su decisión sea no aceptarlo, se procederá generar acta en la que se reflejé esta situación.

Posteriormente, se informará esta diferencia de criterio en el Comité Integral de Riesgos, en donde cada parte expondrá sus argumentos y se debe tomar una decisión para dirimir la diferencia.

10.3. TRATAMIENTO DE RIESGOS

El tratamiento de riesgos involucra la selección de una o más actividades que permitan disminuir su impacto o la probabilidad y así mantener el nivel de riesgo residual, en los niveles de aceptación y apetito de riesgo establecidos por Colpensiones.

En general, las opciones para tratar los riesgos pueden incluir: evitar riesgos, asumir riesgos para perseguir una oportunidad, eliminar la fuente de riesgo, cambiar la probabilidad o las consecuencias, compartir el riesgo o mantener riesgos mediante decisiones informadas

Las opciones como respuesta a la evaluación de los riesgos son las siguientes:

Tratamiento	Descripción
Evitar el riesgo	Se decide no proceder con la actividad que tiene la posibilidad de generar riesgo, esta circunstancia puede incrementar la importancia de otros riesgos.
Mitigar el riesgo	Actividades y medidas tendientes a reducir la probabilidad y/o minimizar la severidad de su impacto. Se consigue mediante la optimización de los procedimientos y la implementación de controles (prevención, planificación). Es el primer tratamiento para considerar ante la presencia de un riesgo.
Transferir el riesgo	Actividades y medidas tendientes a transferir o compartir la responsabilidad por el manejo del riesgo (seguro, subcontratación controlada). Al transferir el riesgo vía contrato de seguros, no se entiende que el riesgo se reduzca, sino que las pérdidas asociadas son asumidas por la compañía aseguradora.
Aceptar el riesgo	Luego de que el riesgo ha sido reducido o transferido puede quedar un riesgo residual que se mantiene. En este caso se acepta la pérdida residual probable y se elaboran planes de contingencia para su manejo. Esta opción contempla de igual forma, la aceptación de un riesgo buscado aprovechar una oportunidad.
Monitorear el riesgo	Existen riesgos que, a pesar de haber implementado medidas de control y mitigación, no es posible reducir su perfil de riesgo a los niveles tolerados por la Junta Directiva. Estos riesgos deben tener un plan de monitoreo más exigente y con mayor frecuencia, con el fin de mantenerlo en su nivel mínimo posible.

Tabla 24. Criterios de Tratamiento de Riesgos

Plan de Tratamiento de Riesgos

Los planes de tratamiento de riesgos deben ser incorporados en los planes de mejoramiento de la dependencia y proceso responsables de su gestión, haciendo referencia a la definición y justificación de la medida(s) de tratamiento a adoptar y con la cual se espera que el riesgo identificado sufra una modificación en su nivel de riesgo. Al seleccionar las actividades de tratamiento para los riesgos, se debe tener en cuenta lo siguiente:

1. El efecto potencial que pueda tener sobre el riesgo y su alineación con la tolerancia al riesgo de Colpensiones.
2. La segregación de funciones que permita que la respuesta adoptada logre la reducción del riesgo.
3. La selección de las opciones más adecuadas para el tratamiento de los riesgos implica equilibrar los costos y los esfuerzos de la implementación frente a los beneficios obtenidos.
4. Establecer los resultados esperados para medir su eficacia y el grado en que el riesgo se modifica con su implementación.

En el siguiente gráfico se combinan los resultados de la valoración de los riesgos y los niveles junto con algunos tratamientos recomendados.

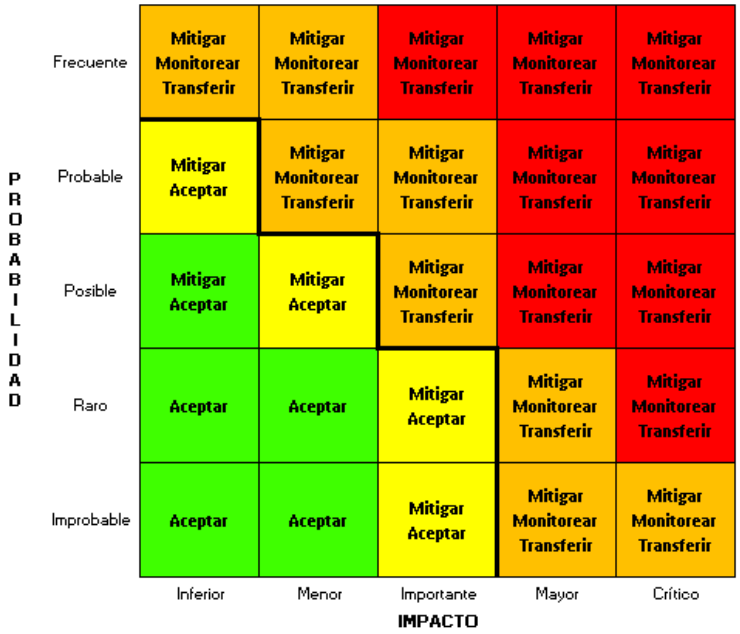


Ilustración 14. Mapa de Tratamiento de Riesgos

El plan de mejoramiento debe formularse y documentarse acorde con lo contemplado en el Instructivo de Formulación de Planes de Mejoramiento establecido por el proceso Administración de Sistemas de Gestión contemplando, entre otros, los siguientes elementos:

- **Proceso:** Proceso en el que se identificó el riesgo asociado al plan definido.
- **Riesgo asociado:** Descripción del riesgo que se encuentra en un nivel no aceptable por la entidad y para el cual se definieron planes.
- **Justificación:** razón por la cual se seleccionó el tratamiento, incorporando el análisis de costo beneficio.
- **Descripción del plan de acción:** Descripción general del plan de acción a implementar.
- **Responsable:** responsable de la aprobación e implementación del plan.
- **Fecha de inicio del plan:** Es la fecha en la cual se estima iniciar la implementación del plan.
- **Fecha fin del plan:** Es la fecha en la cual se estima estarán diseñadas e implementadas las medidas para mitigar los riesgos.
- **Actividades:** Son las actividades que sumadas dan el plan de acción.
- **Estado del plan:** Estado que se le da al plan de acción de acuerdo a su nivel de avance.

Es importante destacar que el resultado de un plan de tratamiento de riesgos debe generar un nuevo control o fortalecer alguno existente, que podrá disminuir la probabilidad de ocurrencia o el impacto en caso de materializarse el riesgo, y su objetivo es modificar la valoración del riesgo residual. Por lo anterior, una vez se termine de ejecutar el plan de tratamiento se deberá evaluar la eficacia del nuevo control aplicando la evaluación de controles y calculando nuevamente el riesgo residual. En caso de que el nivel de eficacia del nuevo control de como resultado "*Débil*" y la calificación del nivel de riesgo residual se mantenga igual, el líder del proceso debe proceder a formular un nuevo plan de tratamiento.

Igualmente, cuando se aplique la autoevaluación de riesgos y controles, contemplado en el siguiente numeral, y se identifiquen controles con resultados en la solidez individual del control "*Débil*", el líder del proceso debe formular un plan de mejoramiento, donde las actividades que se establezcan estén encaminadas a fortalecer los criterios que presentaron calificaciones bajas en la autoevaluación, obteniendo como resultados controles fuertes, a la culminación del plan de acción.

10.4. SEGUIMIENTO Y REVISIÓN

En esta etapa se desarrolla un proceso que permite la oportuna detección y corrección de las deficiencias presentadas; validando que los riesgos residuales se encuentren en los niveles establecidos por Colpensiones.

En el nivel de riesgos estratégicos, el seguimiento y revisión se realiza con base en la evolución del plan estratégico y en el seguimiento al comportamiento de las variables externas que pueden afectar a la entidad.

En el nivel de riesgo táctico, el monitoreo a la evolución del plan o proyecto en sus diferentes etapas conlleva a actualizar el mapa de riesgos del proyecto y toma de decisiones por parte de los responsables que gobiernan cada proyecto, estableciendo acciones oportunas para mitigar el impacto generado sobre el mismo.

En el nivel de riesgo por procesos, el monitoreo permanente de los procedimientos y planes de acción relacionados con el sistema integral de administración de riesgos conlleva a realizar las correspondientes actualizaciones y modificaciones en la matriz de Evaluación de Riesgos y por ende del perfil de riesgos de la entidad.

En esta etapa cada tipología de riesgo (Operacional, Continuidad del Negocio, Lavado de Activos y Financiación del Terrorismo, Fraude y Corrupción, Seguridad de la Información y Ciberseguridad y Financieros), realiza de manera independiente el monitoreo de los riesgos que afectan el cumplimiento de los objetivos de la entidad, lo cual se contempla en los documentos que hacen parte integral del presente manual.

Para cumplir con esta función, se han definido como mínimo los siguientes mecanismos:

10.4.1. Eventos de Riesgo

En el marco del objetivo de garantizar que la revisión y actualización del sistema de administración de riesgos, permita establecer medidas correctivas y preventivas en cada uno de los procesos, así como identificar oportunidades de mejora, Colpensiones cuenta con una herramienta a través de la cual se realiza el registro de eventos, dando origen a la base de datos de eventos de riesgo.

Los eventos de riesgo corresponden a la materialización de los riesgos identificados, son situaciones que, en el desarrollo de las actividades de la entidad, afectan el normal desarrollo de sus operaciones y que generan o pueden generar algún tipo de consecuencias o impacto.

La base de datos de eventos de riesgo es construida a partir de la información revelada por parte de los servidores públicos y colaboradores de la Entidad, mediante los mecanismos definidos por la Gerencia de Riesgos y Seguridad de la Información. Se construye para identificar, clasificar y almacenar información de posibles pérdidas por riesgos con el fin de adelantar la gestión necesaria para disminuir la probabilidad de ocurrencia y/o impacto en caso de materializarse, acorde con cada tipología (Operacional, Continuidad del Negocio, Lavado de Activos y Financiación del Terrorismo, Fraude y Corrupción, Seguridad de la Información y Ciberseguridad y Financieros).

La gestión de eventos de riesgo en Colpensiones involucra las etapas de gestión integral de riesgos así:



Ilustración 15. Etapas de Eventos de Riesgo

- **Identificación, Reporte y Registro**

  - En la identificación de eventos de riesgos, deben considerarse al menos las siguientes fuentes y situaciones:
    - Quejas y reclamos de los ciudadanos
    - Incumplimientos contractuales de los terceros contratados
    - Procesos jurídicos en contra de la entidad
    - Hallazgos de los órganos de control
    - Resultado de los indicadores de gestión
    - Indisponibilidad de la plataforma tecnológica, el recurso humano, la infraestructura para operar.
    - El incumplimiento en la ejecución de controles.

- Errores de los sistemas de información
- Incumplimiento del marco normativo
- Reporte a las pólizas de seguro
- Incumplimiento a las políticas organizacionales

- Es responsabilidad de todos los colaboradores de Colpensiones, reportar las situaciones que conozcan en el desarrollo de sus funciones y que puedan afectar de manera adversa los objetivos de la entidad o de los procesos que la componen, a través de la herramienta definida para este fin o informarla a través de los diferentes mecanismos establecidos.

- Los eventos de riesgos deben ser reportados en el momento de su identificación.

- En caso de presentarse un evento de riesgo cuya materialización afecte de manera crítica el desarrollo normal del proceso, se deberá informar de manera inmediata a la Gerencia de Riesgos y Seguridad de la información, mediante comunicación los canales establecidos en la gestión de riesgos, donde el Gerente o cualquiera de los profesionales del área evaluarán la situación, realizarán las recomendaciones del caso y monitorearán las actividades de contención del mismo.

- El reporte de eventos de riesgo puede realizarse de manera anónima o identificando el colaborador que lo registra.

- La claridad en la descripción de eventos de riesgo es fundamental para asegurar su adecuada clasificación, análisis y tratamiento. Por lo anterior, en el momento del reporte se deberán considerar al menos los siguientes elementos:

  - Descripción clara de la situación presentada
  - Fecha o periodo de ocurrencia de los hechos
  - Fecha de identificación del evento
  - Descripción de la forma de cómo fue identificado el evento
  - Producto o servicio afectado
  - Ciudad, sede o punto de atención donde sucedió el evento
  - Consecuencias originadas por el evento.

- La Gerencia de Riesgos y Seguridad de la Información debe mantener una base de datos confiable sobre los hechos reportados, la cual permita realizar el análisis sobre el comportamiento de los riesgos asociados a los eventos de riesgo, y sirva de base de conocimiento para atender situaciones similares que se presenten en el futuro.

- En cuanto a las acciones realizadas y/o implementadas, para subsanar los eventos de riesgo, es responsabilidad de los líderes de procesos contar con el análisis e información de la gestión realizada en la herramienta establecida por la entidad para este fin, por su

parte la Gerencia de Riesgos y Seguridad de la Información, realizará el monitoreo de las acciones sobre los eventos de mayor impacto para la Entidad (Alto y Medio Alto).

- La Gerencia de Riesgos y Seguridad de la Información debe implementar controles para que el registro de eventos de riesgo operativo cumpla con los criterios de integridad, confiabilidad, disponibilidad, cumplimiento, efectividad, eficiencia y confidencialidad de la información allí contenida.

- El registro de los eventos de riesgo incorpora las actividades asociadas a la contabilización de los eventos de riesgo que generan pérdida económica para la entidad.

- Las actividades de contabilización de eventos de riesgo son coordinadas desde la Gerencia de Riesgos y Seguridad de la Información.

- **Análisis y Valoración**

- La Gerencia de Riesgos y Seguridad de la Información, debe realizar un análisis de las situaciones reportadas por las áreas, y de acuerdo con el mismo confirmar si corresponde a un evento de riesgo.
- Confirmado el evento de riesgo, se debe clasificar el mismo con el fin de determinar el tratamiento a aplicar de acuerdo con:

Valoración del Evento	Tratamiento	Escalamiento
Alto	Corrección y Plan de Mejoramiento Coordinador por le Gerencia de Riesgos y Seguridad de la Información	Comité de Riesgos y Junta Directiva
Medio Alto	Corrección y Plan de Mejoramiento Coordinador por el líder del principal proceso afectado	Gerencia de Riesgos y Seguridad de la Información
Medio Bajo	Corrección bajo la supervisión del líder del proceso.	Líder del Proceso
Bajo	Corrección bajo la supervisión del líder del proceso	Líder del Proceso

Tabla 24. Criterios de Valoración y Tratamiento de Eventos

- En la asignación del evento de riesgo, deberá identificarse con claridad los siguientes roles:

  - Proceso afectado.
  - Proceso(s) responsable(s) del tratamiento del evento

- La Gerencia de Riesgos y Seguridad de la Información, deberá dar traslado del evento al líder del proceso y/ proyecto afectado y a los líderes de los procesos responsables del tratamiento, indicando sus recomendaciones en caso de que así se requiera.

- Para los eventos de riesgos que requieran plan de mejoramiento, es responsable del líder del proceso realizar un adecuado análisis de causas, utilizando las metodologías definidas por la Gerencia de Sistemas Integrados de Gestión, y buscando la eliminación de la causa raíz.

- En todo caso, la Gerencia de Riesgos y Seguridad de la información deberá implementar los controles necesarios para asegurar que los eventos de riesgo valorados en Alto y Medio Alto, cuenten con un adecuado análisis de causas que prevengan la materialización de eventos en el futuro.

- **Tratamiento**

- Los líderes de los procesos responsables del tratamiento de los eventos de riesgo valorados en Alto y Medio Alto, deben establecer con claridad las actividades, responsables y tiempos de implementación requeridos.

- Los eventos de riesgo valorados como alto deben tener planes de mejoramiento que no superen los tres meses para su mitigación. En caso de planes de mejoramiento que requieran un plazo mayor, el plan de mejoramiento definido debe incorporar el diseño de actividades de mitigación compensatorias de corto plazo, que permitan mitigar de manera temporal el riesgo asociado al evento.

- Los planes de mejoramiento deberán ser documentados en la herramienta establecida por el proceso de Administración de Sistemas de Gestión.

- Los planes de mejoramiento establecidos deben considerar actividades asociadas a la actualización de los documentos del proceso, así como la actualización de la matriz de evaluación de riesgos del proceso, en caso de que así se requiera.

- El cierre de los eventos de riesgo valorados en alto y medio alto, deben ser reportados a la Gerencia de Riesgos y Seguridad de la Información para su validación.

- El cierre de los eventos de riesgo valorados en medio bajo y bajo deberá realizarse bajo la supervisión del líder del proceso responsable.

- **Revisión y Seguimiento de eventos**

- Los líderes de los procesos responsables del tratamiento de los eventos de riesgos deben realizar seguimiento mensual al cumplimiento de los planes de mejoramiento o las

actividades de corrección definidas, así como registrar los avances en la herramienta establecida por la Entidad para este fin

- Los planes de mejoramiento establecidos por los líderes de los procesos responsables de los eventos tienen un seguimiento al menos mensual (Eventos valorados en alto) o trimestral (eventos valorados en medio alto), por parte de la Gerencia de Riesgos y Seguridad de la Información.

- Al menos trimestralmente, la Gerencia de Riesgos y Seguridad de la Información, realizará un análisis consolidado de la base de datos de los eventos de riesgo con el fin de evidenciar las tendencias de los eventos de riesgo, los factores de riesgo involucrados, la reiteración de los mismos, la concentración por proceso y la coincidencias o similitudes. Lo anterior, con el fin de establecer si se requieren planes de mejoramiento adicionales a los ya definidos para el tratamiento individual de los eventos de riesgo.

- **Comunicación y Reporte**

- La Gerencia de Riesgos y Seguridad de la Información, debe definir informes y reportes dirigidos a sus grupos de interés, con el fin de mantener informados a los mismos sobre la evolución de los eventos de riesgo en la entidad.

10.4.2. Autoevaluación de Riesgos y Controles

La evaluación de los riesgos y controles a nivel de los procesos y/o proyectos es responsabilidad de los líderes de los procesos, proyectos y sus colaboradores, como Primera Línea de Defensa.

A través de la metodología descrita en este manual, se realiza la evaluación de los riesgos y controles implementados en los diferentes procesos, permitiendo garantizar el análisis y la gestión de la Primera Línea de Defensa. A su vez, los resultados de la evaluación deben generar las acciones necesarias para la mitigación de riesgos y el logro de los objetivos institucionales.

Bajo este marco, la Gerencia de Riesgos y Seguridad de la Información, anualmente, define un plan de monitoreo para verificar que dicha actividad a cargo de la primera línea de defensa se cumpla de forma eficaz. Bajo este plan evalúa que los controles se encuentren adecuadamente diseñados frente al riesgo que se pretende mitigar y que los mismos sean ejecutados, de acuerdo con su diseño.

Para el establecimiento de este plan anual, se deberán considerar al menos los siguientes aspectos:

- Controles asociados a los riesgos cuyo perfil de riesgos inherente se encuentre en el máximo nivel de exposición.

- Controles asociados a los riesgos cuyo perfil de riesgos residual se encuentre por fuera del apetito de riesgo definido por la Junta Directiva.
- Comportamiento de los eventos de riesgo
- Comportamiento de los indicadores de riesgo
- Hallazgos de los órganos de control y supervisión.

10.4.3. Monitoreo a riesgos a través de indicadores

El indicador es una expresión utilizada para mostrar los resultados obtenidos, en la ejecución de un proyecto, programa o proceso, como resultado cuantitativo de comparar variables, en relación con el logro de los objetivos y metas previstos.

El monitoreo de riesgos a través de indicadores se realizar a través de tres tipos de indicadores así:

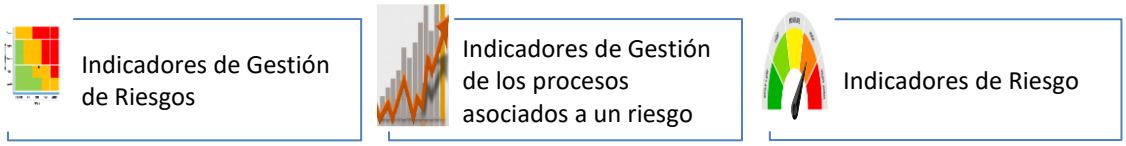


Ilustración 16. Tipos de Indicadores

- **Indicadores de Gestión de Riesgos:** Corresponden a los indicadores definidos para el proceso de gestión de riesgos, enfocados a determinar el cumplimiento consolidado de los objetivos de la gestión de riesgos definidos por la entidad. Se concentra en medir aspectos tales como:

  - El perfil de riesgo de la entidad
  - La adecuada identificación y valoración de riesgos
  - La eficacia de las medidas de control implementadas
  - El cumplimiento de los planes de mejoramiento establecidos para mitigar los riesgos.
  - El fortalecimiento de la cultura de gestión de riesgo
  - El nivel de madurez de la gestión de riesgo

- **Indicadores de gestión asociados a un riesgo**: Los indicadores definidos en las categorías: estratégicos, tácticos y operativos, permiten medir el grado de cumplimiento frente a los objetivos trazados. Dado lo anterior y partiendo de que la identificación de riesgos toma como base el objetivo de la organización, de las estrategias y/o ejecución de proyectos y/o planes de trabajo, y de los procesos, se contempla que algunos de estos indicadores permiten monitorear los riesgos asociados a estos, en los tres niveles, así:

  Riesgos Estratégicos - Indicadores Estratégicos: Basados en los objetivos estratégicos definidos en el plan estratégico institucional y se establecen para medir el grado de

cumplimiento de los objetivos establecidos, de acuerdo a los limites o metas determinadas por la Alta Dirección.

Riesgos Tácticos - Indicadores Tácticos: Basados en los objetivos definidos en los proyectos, que se establecen para monitorear y medir el cumplimiento de las estrategias, ejecución de proyectos y planes de trabajo.

Riesgos por Procesos - Indicadores Operativos: Están relacionados con las actividades de mayor impacto en los procesos y permiten medir el cumplimiento de los objetivos de éstos, en esta medida a los riesgos identificados en la ejecución de estas actividades.

Los indicadores de riesgo por procesos corresponden a los indicadores de gestión definidos en la Entidad, de tal forma que se entiende al indicador de riesgo, como el incumplimiento o tendencia negativa en el resultado del indicador del proceso, conllevando a realizar el análisis y adopción de acciones tanto correctivas, como preventivas, para minimizar la exposición o impacto del riesgo.

Los indicadores de riesgo se contemplan bajo metodología para la formulación y análisis de indicadores, –establecidos en el proceso Administración de Sistemas de Gestión.

La responsabilidad de medición y reporte de estos indicadores recae en la primera línea de defensa. El seguimiento a los mismos lo realizan de forma conjunta la primera y la segunda línea de defensa

- **Indicadores clave de Riesgo - KRIs**: Un indicador clave de riesgo es una métrica fundamental que se emplea para monitorear y mitigar los impactos de posibles amenazas. A diferencia de los KPI, que permiten medir el desempeño de un proceso en el pasado, los KRI, o indicadores de riesgo, son una métrica esencial para medir la posibilidad de un impacto futuro. El diseño de un KRI parte de identificar un riesgo que se haya evidenciado en el pasado o que se esté evidenciando actualmente. Luego, observar en retrospectiva para encontrar cuáles fueron las causas que lo desataron y en qué momento ocurrieron.

  Estos indicadores corresponden a métricas independientes formuladas, medidas y monitoreadas por la segunda línea de defensa, obteniendo directamente de las fuentes la información para su cálculo.

El monitoreo de estos indicadores busca realizar el seguimiento a los principales riesgos identificados (estratégicos, tácticos y por procesos), identificando eventos de riesgo y alertando sobre las desviaciones que evidencien sus resultados.

10.4.4. Evaluación de Riesgos en Terceras Partes

Este mecanismo de monitoreo permite evaluar el ambiente de control de los terceros considerados como críticos, detectando vulnerabilidades que puedan materializar riesgos al interior de Colpensiones. Para el efecto, la Gerencia de Riesgos y Seguridad de la Información debe realizar visitas de reconocimiento o verificación documental, según corresponda, a aquellos proveedores que de acuerdo con la metodología establecida sean considerados como críticos.

En este sentido, se desarrollan las siguientes fases las cuales permitirán llevar a cabo la evaluación del ambiente de control de las terceras partes consideradas como críticas para la operación.

Análisis y Evaluación:

La metodología de riesgo de terceras partes considera nueve dimensiones de impacto, cada una de estas considera criterios específicos frente al nivel de afectación que se puede generar a partir de las relaciones activas con las terceras partes y aliados estratégicos.



Ilustración 17. Dimensiones de Impacto en Terceros

- *Riesgo de Cumplimiento:* Mide el riesgo de incumplimiento de la tercera parte frente a la regulación requerida, haciendo que la entidad también pueda estar fuera del cumplimiento.

- *Riesgo Operacional:* Mide el riesgo en las fallas que proporcione la operación del servicio prestado por la tercera parte, o la concentración de servicios en una tercera parte.

- *Riesgo de Fraude y Corrupción:* Mide el riesgo de fraude y corrupción en el cual se puede ver involucrada una tercera parte.

- *Riesgo de Seguridad de la Información y Ciberseguridad:* Mide el riesgo de compromiso de la información de la Entidad a partir de las acciones de la tercera parte.

- *Riesgo Financiero:* Mide el riesgo de inviabilidad financiera de la tercera parte o de la relación contraída.

- *Riesgo de Continuidad del Negocio*: Mide el riesgo de interrupción de las operaciones del negocio a partir de eventos generados por la tercera parte.

- *Riesgo Reputacional:* Mide el riesgo de afectación de la imagen y reputación de la entidad ante un evento generado por una tercera parte.

- *Riesgo País:* Mide el riesgo de inviabilidad de la relación con la tercera parte por pertenecer a un país con señalamientos legales / reguladores, geopolíticos, sociales o económicos.

- *Riesgo de Lavado de Activos y Financiación del Terrorismo:* Nivel de exposición de la Entidad a impacto derivados de riesgos asociados a LAFT, los cuales pueden ser de índole económico o reputacional, derivados de la intención de dar apariencia de legalidad a los recursos obtenidos de manera ilícita o de la realización de transacciones y fondos vinculados al LAFT.

Criterios de Evaluación de Impacto:

Para cada una de estas dimensiones se consideran criterios de evaluación de impacto, clasificados en crítico, mayor, importante, menor e inferior, contemplados en el Instructivo de Evaluación de Riesgos en Terceras Partes.

Cada tercero quedará clasificado en los siguientes cuadrantes. Como se observa el eje (Y) mide el nivel de impacto que es un resultado obtenido de la evaluación ejecutada y el eje (X) representa el volumen de facturación anual en pesos (Valor del contrato).

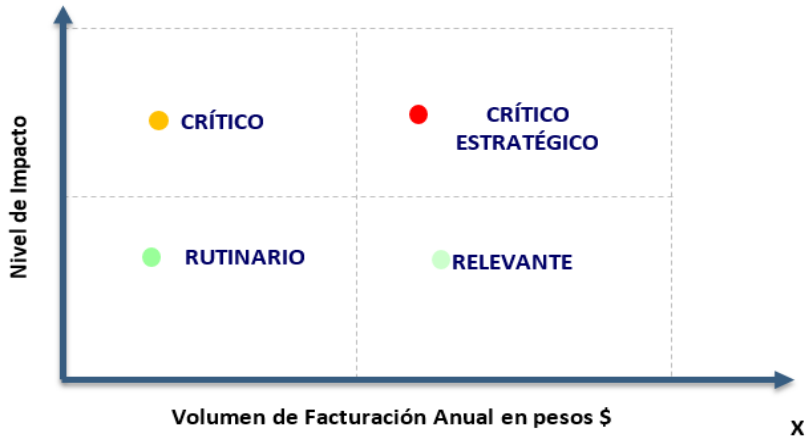


Ilustración 18. Evaluación de Impacto en Terceros

- *Crítico estratégico:* Indica que la relación entre la Tercera Parte y la entidad es de alta exposición al riesgo sobre procesos misionales de negocio y en caso de materialización de un evento es crítico o mayor su nivel de impacto generado.
- *Crítico:* Indica que la relación entre la Tercera Parte y la entidad es de alta exposición al riesgo sobre procesos estratégicos o de soporte y en caso de materialización de un evento es crítico o mayor su nivel de impacto generado.
- *Relevante:* Indica que la relación entre la Tercera Parte y la entidad no es significativa y por lo tanto se aceptan los riesgos existentes en la relación entre la Tercera Parte y la entidad.
- *Rutinario*: en la relación entre la Tercera Parte y la entidad, dado que no generan una materialización de estos de acuerdo con la evaluación realizada, sin embargo, se debe monitorear anualmente cualquier cambio sobre el estado de la relación con el tercero.

Tratamiento de Riesgo:

Considera la estructuración de controles eficientes y efectivos con los supervisores de los contratos con terceras partes, a partir de los cuales se determina el nivel de riesgo. De acuerdo con su nivel de criticidad, se establecen los siguientes lineamientos en cuanto a la definición del ambiente de control a aplicar:

	CRÍTICO ESTRATÉGICO	CRÍTICO	RELEVANTE	RUTINARIO
Crítico	• Definir planes de tratamiento y requisitos de control específicos de acuerdo con el servicio prestado y las dimensiones de impacto en las cuales la relación genera un nivel de impacto crítico.	• Definir planes de tratamiento y requisitos de control específicos de acuerdo con el servicio prestado y las dimensiones de impacto en las cuales la relación genera un	No Aplica	No Aplica

	• Requiere ejecutar evaluación de control en sitio anualmente. • Seguimiento mensual al cierre de los planes de tratamiento.	nivel de impacto crítico. • Requiere ejecutar evaluación de control en sitio cada dos años. • Seguimiento trimestral al cierre de los planes de tratamiento.		
Mayor	• Incluir en los acuerdos contractuales los requisitos de control de acuerdo con el servicio prestado y las dimensiones de impacto en las cuales la relación genera un nivel de impacto mayor. • Requiere ejecutar evaluación de control documental semestralmente. • Seguimiento trimestral al cierre de los planes de tratamiento.	• Incluir en los acuerdos contractuales los requisitos de control de acuerdo con el servicio prestado y las dimensiones de impacto en las cuales la relación genera un nivel de impacto mayor. • Requiere ejecutar evaluación de control documental anual. • Seguimiento semestral al cierre de los planes de tratamiento.	No Aplica	No Aplica
Importante	No Aplica	No Aplica	Incluir en los acuerdos contractuales los requisitos de control generales de acuerdo con el servicio prestado y las dimensiones de impacto en las cuales la relación genera un nivel de impacto importante.	Aceptación del riesgo
Menor	No Aplica	No Aplica	Aceptación del riesgo	Aceptación del riesgo
Inferior	No Aplica	No Aplica	Aceptación del riesgo	Aceptación del riesgo

Tabla 25. Criterios de Tratamiento de Riesgos en Terceros

Evaluación del Ambiente de Control:

A través de un enfoque claro y estructurado de evaluación al ambiente de control dispuesto con las terceras partes, se logra realizar un seguimiento al comportamiento de los riesgos que generan las relaciones activas con las terceras partes.

Crítico	Revisión en sitio	Prueba de recorrido en sitio para corroborar la aplicación de los requisitos de control, sobre el cuestionario y la información entregada por la tercera parte.
Mayor	Revisión de contrato	Revisión del contrato para validación de la inclusión de los requisitos de control aplicables por dimensión de impacto.
Importante	Ninguna	No requiere acción.
Menor	Ninguna	No requiere acción.
Inferior	Ninguna	No requiere acción.

Tabla 26. Criterios de Evaluación del Ambiente de Control en Terceros

La evaluación se realiza a partir del análisis de los parámetros de diseño y de operación del control, lo cual permite realizar una evaluación de manera objetiva, sobre parámetros claramente establecidos y calificables, evitando la subjetividad en la asignación de la medición. Como resultado de la calificación de los atributos de evaluación de los controles, se obtiene su nivel de madurez, el cual se clasifica en seis (6) niveles:

- **5. Optimizado:** Los procesos se han refinado hasta un nivel de práctica líder y se basan en los resultados de mejoras continuas. El proceso se soporta en la tecnología para mejorar la calidad y la efectividad.

- **4. Administrado y medible:** Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora.

- **3. Proceso definido:** Los procedimientos se han estandarizado y documentado, y se difunden a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos, y es poco probable que se detecten desviaciones.

- **2. Repetible pero intuitivo:** Se siguen procedimientos similares en diferentes áreas que realizan la tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo y su conocimiento, por lo tanto, los errores son muy probables.

- **1. Inicial / Ad Hoc:** Se reconoce que los problemas existen y requieren ser resueltos. Sin embargo; no existen procesos estándar, en su lugar existen enfoques ad hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general es desorganizado.

- **0. No existe:** No se ha reconocido la problemática existente y no se ha implementado ningún tipo de acción de control.

Identificación de riesgos y presentación de resultados:

En función de la calificación de madurez de los controles, se determina los riesgos a los que se encuentra expuesta Colpensiones, dada las condiciones de la relación con la tercera parte. Con los riesgos identificados y las observaciones se generará el informe de evaluación, el cual será socializado con el Supervisor del contrato, y presentado a la tercera parte en reunión formal de cierre de la evaluación.

El informe de evaluación con las observaciones en la materia son puestas en conocimiento de los supervisores de los respectivos contratos y responsables líderes de los procesos con el fin de que se definan acciones que fortalezcan el ambiente de control del tercero y la mitigación de los riesgos en Colpensiones.

10.4.5. Seguimiento a los planes de mejoramiento

Los planes de mejoramiento establecidos para mitigar los riesgos identificados en un nivel de exposición no tolerado, o sobre controles con calificación son definidos y liderados por los responsables de los procesos, siendo estos objetos de seguimiento por las áreas de control y la Gerencia de Riesgos y Seguridad de la Información.

Se establecen planes de acción con el objetivo de reducir el nivel de riesgo residual obtenido de los riesgos identificados. Los planes de acción consideran el nivel de riesgo, la complejidad del plan, recursos y otros factores determinados por el responsable. Así mismo, se podrán definir oportunidades de mejora destinados a mitigar riesgos con nivel residual Medio Bajo.

El seguimiento de la implementación de los planes de mejoramiento será realizado por la Gerencia de Riesgos y Seguridad de la Información y el responsable del proceso; y su documentación se realizará en las herramientas y bajo el marco establecido en el proceso de Administración del Sistema Integrado de Gestión.

10.5. METODOLOGÍA PARA LA GESTIÓN DE LAS OPORTUNIDADES

La gestión de las oportunidades en Colpensiones se realiza en el marco de la formulación y actualización de la planeación estratégica institucional, iniciando desde el máximo nivel de la gestión del riesgo, es decir, desde el nivel estratégico.

- **Identificación de Oportunidades**

Con base en los componentes de la evaluación del contexto estratégico, y siguiendo la metodología Delphi – Juicio de expertos, descrita para la identificación de riesgos estratégicos, se realiza un listado de las oportunidades que presenta, tanto el contexto interno, como el externo en el que se desenvuelve Colpensiones.

Dichas oportunidades son contrastadas con el ejercicio de Planeación Estratégica de la entidad con el fin de llegar a un consenso de las oportunidades a gestionar.

- **Priorización de Oportunidades**

La priorización de dichas oportunidades se realiza de acuerdo con la siguiente metodología:

  - Se listan las oportunidades identificadas.
  - Cada uno de los miembros de la alta dirección (Presidente, Vicepresidentes, Jefes de Oficina, Gerentes y Directores) valoran de 1 a 5, siendo 1 menos importante y 5 altamente importante, cada una de las oportunidades identificadas, en cada una de las perspectivas estratégicas definidas (Financiera, Usuario, Procesos y Gestión del Conocimiento).
  - Para cada una de las oportunidades que presenten una calificación superior a 3 se deberá establecer las vicepresidencias y gerencia responsables de su tratamiento.

- **Identificación de Estrategias**

Alineado con los lineamientos metodológicos para la formulación y actualización de la planeación estratégica institucional, las Vicepresidencias, Jefes de Oficina y Gerencias responsables, establecen las estrategias que serán el elemento conductor entre el nivel estratégico y el nivel táctico.

Dichas estrategias tienen como objetivo afrontar un riesgo identificado o aumentar los efectos positivos de una oportunidad priorizada.

- **Seguimiento al cumplimiento de estrategias**

El seguimiento al comportamiento de la gestión de oportunidades se realiza a través de indicadores estratégicos que miden el grado de cumplimiento de los mismos.

10.6. COMUNICACIÓN Y CONSULTA

Consiste en asistir a las partes interesadas, internas o externas, a comprender el riesgo, las bases con las que se toman decisiones y las razones por las que son necesarias acciones específicas. La comunicación busca promover la toma de conciencia y la comprensión del riesgo, la consulta implica obtener retroalimentación e información para apoyar la toma de decisiones.
Esta etapa se debe desarrollar en todas y cada una de las etapas del proceso.

10.7. REGISTRO E INFORME

La Vicepresidencia de Seguridad y Riesgos Empresariales, a través de la Gerencia de Riesgos y Seguridad de la Información, adelanta las actividades necesarias para garantizar que la información correspondiente al sistema integral de administración de riesgos se encuentre disponible y sea divulgada periódica y adecuadamente asegurando el funcionamiento de sus propios procedimientos y el cumplimiento de los requerimientos normativos.

Para el efecto, anualmente evalúa la estrategia de comunicación y consulta considerando las necesidades de sus grupos de interés, así:

- Ciudadanos y Empleadores
- Junta Directiva y Representante Legal
- Equipo Directivo (Vicepresidentes, Jefes de Oficina, Gerentes, Asesores y Directores)
- Colaboradores de Colpensiones (Trabajadores Oficiales, en misión, prácticas, aprendices SENA y contratistas)
- Terceros Críticos.
- Órganos de Supervisión y Control.

Bajo este marco, establece un plan de Comunicación y Consulta en cual debe contener al menos los siguientes reportes internos y externos:

Reportes Internos

La Vicepresidencia de Seguridad y Riesgos Empresariales y el Oficial de Cumplimiento presentan a la Presidencia y Junta Directiva, los siguientes informes según sea el caso.

- Informe de Riesgo de Mercado con periodicidad mensual.
- Informe de gestión, con periodicidad como mínimo semestralmente, sobre la evolución del perfil de riesgos de la entidad, detallando el comportamiento particular de cada sistema.

- Informe trimestral de la gestión del Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo.

Reportes Externos

A través del informe de Gestión Anual, se incluye una sección relacionada con la gestión adelantada en materia de administración integral de Riesgos, la cual es publicada a través de la página web de Colpensiones.

De igual manera, a través de las notas a los Estados Financieros se contemplan los temas relacionados con el sistema integral de administración de riesgos.

En el establecimiento anual de la estrategia de comunicación y consulta, se deberá tener en cuenta el marco normativo de cada sistema de gestión de riesgos, en el cual se señalan aspectos particulares del contenido mínimo de dichos informes.

11. DOCUMENTACIÓN Y REGISTRO DE LA GESTIÓN INTEGRAL DE RIESGOS

Colpensiones cuenta con la documentación correspondiente a la definición, implementación y monitoreo de los elementos y etapas del sistema de administración de riesgos, contemplados en el presente Manual y cada una de sus partes, así como, con los registros que se originen de la gestión del sistema integral de administración de riesgos.

12. PLATAFORMA TECNOLÓGICA

La gestión de riesgos, sus procedimientos y metodologías se desarrollan a través de diferentes herramientas tecnológicas, que los soportan y permiten su administración, acorde con las necesidades de cada uno de los sistemas.

El aplicativo definido por Colpensiones para la administración integral de los riesgos, está diseñado para una gestión de riesgos por procesos y permite la construcción de los mapas de riesgo, la documentación de controles, la valoración del riesgo inherente y residual, y sus respectivos reportes, el registro de los eventos sobre los que se definen planes de acción que son gestionados y documentados en el aplicativo.

La herramienta tecnológica es una solución integral para la administración de riesgos que incorpora una estructura jerárquica y de perfiles parametrizable, permitiendo una razonable seguridad sobre la información allí registrada.

13. CAPACITACIÓN Y SENSIBILIZACIÓN

La Vicepresidencia de Seguridad y Riesgos Empresariales y el Oficial de Cumplimiento, en coordinación con la Vicepresidencia de Gestión Corporativa y la Oficina de Relacionamiento y Comunicaciones son responsables del diseño e implementación del programa anual de capacitación y sensibilización del sistema integral de administración de riesgos; así como, de su revisión y actualización, y de la evaluación de los resultados, la cual está dirigida a todos los servidores públicos y colaboradores de la Entidad, con el fin de generar conciencia sobre la importancia de dar cumplimiento a las políticas y procedimientos establecidos en materia de gestión integral de riesgos de acuerdo con sus diferentes tipologías (Riesgos Operacionales, Riesgos de Seguridad de la información y Ciberseguridad, Riesgos de Continuidad del Negocio, Riesgos de Fraude y Corrupción, Riesgos de Lavado de Activos y Financiación del terrorismo y Riesgos Financieros)

El programa de capacitación y sensibilización se desarrolla en 4 fases así:

1. Diseño	Comprende el levantamiento de necesidades, la definición de los objetivos, el alcance, los grupos de interés a los cuales va dirigido y la programación de las actividades a desarrollar.
2. Desarrollo	Comprende la definición de las herramientas a utilizar y el diseño o actualización del material requerido para la implementación del programa
3. Implementación	Comprende la ejecución del programa en los plazos establecidos y sobre los grupos de interés definidos.
4. Mejoramiento	Comprende la evaluación de los resultados obtenidos con el programa y las oportunidades de mejora a considerar para los siguientes.

Tabla 27. Fases del Programa de Capacitación

El programa tiene dos objetivos fundamentales así:

- Sensibilización: Es un proceso que tiene como objetivo principal cambiar o fortalecer el comportamiento de los colaboradores de Colpensiones sobre un aspecto en particular.

- Capacitación: Busca asegurar que los Colaboradores de Colpensiones tengan el conocimiento y las habilidades necesarias para ejecutar funciones específicas.

13.1 DISEÑO

Establecimiento de Necesidades y Objetivos

El adecuado diseño de un programa de capacitación y sensibilización, parte del establecimiento de las necesidades de la organización. Para ello se considera al menos la siguiente información:

- Plan estratégico e institucional de la entidad.
- Planeación estratégica particular de la Gestión de Riesgos.
- Evolución del perfil de riesgos en sus niveles estratégicos, tácticos y por proceso.
- Comportamiento de eventos de riesgo, incidentes de seguridad y tipologías de fraude
- Hallazgos de órganos de control.
- Cambios normativos.

De igual forma y considerando los grupos de interés y los marcos de referencia y normativo, el programa de capacitación y sensibilización contempla:

- La inducción a los nuevos servidores públicos y colaboradores de la entidad, como complemento al programa institucional de ingreso.
- Capacitación dirigida a todos los servidores públicos y colaboradores de Colpensiones.
- Capacitación presencial o virtual específica a grupos focalizados.
- Formación y sensibilización dirigida a la Junta Directiva y la Alta Dirección, como líderes de la cultura de riesgos en Colpensiones.
- Los terceros siempre que exista una relación contractual y desempeñen funciones críticas de la Entidad.
- Sensibilización dirigida a los ciudadanos.

Los programas podrán ser contratados con terceros bajo la supervisión de la Vicepresidencia de Seguridad y Riesgos Empresariales y/o el Oficial de Cumplimiento.

Para llevar a cabo el programa de capacitación y sensibilización se utilizan como medios de difusión masiva, el correo corporativo, la intranet, las capacitaciones presenciales y virtuales, tanto en las áreas, como en las oficinas.

Alcance de los Programas de Capacitación y Sensibilización

Los programas de capacitación y sensibilización son elaborados por la Vicepresidencia de Seguridad y Riesgos Empresariales, a través de la Gerencia de Riesgos y Seguridad de la Información, en coordinación con la Dirección de Desarrollo de Talento Humano; constan por escrito bajo el objetivo de generar cultura en gestión integral de riesgos, desarrollando como mínimo los siguientes temas:

- El modelo de las tres líneas de defensa, responsabilidades y roles.
- Herramientas, mecanismos e instrumentos para la administración integral de riesgos.
- Lineamientos y políticas en el marco de la gestión integral de riesgos.
- Lineamientos y políticas en el marco de la gestión integral de riesgos aplicables a terceros contratistas.
- El principio de Control Interno de autocontrol.
- El régimen de responsabilidades por el incumplimiento de los deberes que obligan a una adecuada aplicación y gestión de riesgos.

Programación de Actividades y documentación

El programa de capacitación y sensibilización se establece de forma anual, en alineación con los ejercicios de planeación estratégica y establecimiento del presupuesto de la entidad.

Lo anterior, con el objetivo de que el mismo sea considerado dentro del plan anual de capacitación y sensibilización de la entidad.

El programa debe constar en un documento que contenga al menos la siguiente información:

- Objetivos y alcance del programa.
- Roles y responsabilidades.
- Audiencias objetivo para cada aspecto, quienes deben ser sensibilizados, quienes capacitados o entrenados.
- Temas y herramientas a utilizar.
- Meses en que se desarrollaran las actividades.
- Presupuesto estimado.

13.2 DESARROLLO

El programa de Capacitación y Sensibilización puede utilizar alguna de las siguientes herramientas:

- Capacitaciones Virtuales o Presenciales, internas o a través de instituciones educativas o de formación.
- Desarrollo o difusión de documentos de investigación sobre temáticas de gestión integral de riesgos.
- Talleres, pruebas de controles o pruebas de ingeniería social.
- Mailing boletines o participación en espacios de comunicación de la entidad.
- Posters con mensajes o infografías sobre que debe y que no debe hacerse.
- Videos institucionales.
- Fondos de pantalla con mensajes de sensibilización.

- Cuadernos, relojes o elementos de oficina con mensajes alusivos.
- Participación en congresos, talleres o charlas presenciales o virtuales.

Para cada una de estas herramientas, la Gerencia de Riesgos y Seguridad de la Información, la Gerencia de Prevención de Fraude y el Oficial de Cumplimiento es la responsable de revisar y mantener actualizados los contenidos de las mismas.

Las herramientas de sensibilización se desarrollan en conjunto con la Oficina de Relacionamiento y Comunicaciones con el fin de asegurar una adecuada forma de transmisión de mensajes.

13.3 IMPLEMENTACIÓN

Se debe procurar que todas las actividades definidas en el programa tengan alguna forma de medición de su eficacia.

Para el caso de las actividades de sensibilización, se debe procurar medir el número de colaboradores que consultaron el mensaje y el grado de entendimiento del mismo, en los casos en que resulte aplicable. Para el caso de las capacitaciones, se debe procurar que las mismas se evalúen mediante una prueba escrita, o mecanismos virtuales disponibles, lo que permite determinar:

- El entendimiento de los temas.
- El rendimiento y conocimiento del facilitador.
- La efectividad de los programas.
- El alcance de los objetivos propuestos.

Todo funcionario debe obtener la mitad más uno de las respuestas correctas en la evaluación. En el evento que la calificación obtenida es inferior, se presenta una nueva evaluación y si no aprueba la segunda evaluación, el caso es estudiado por la Gerencia de Riesgos y Seguridad de la Información junto con la Gerencia de Talento Humano y Relaciones Laborales.

El responsable de verificar el cumplimiento en la realización de las evaluaciones, así como la eficacia de los programas de capacitación es la Gerencia de Talento Humano y Relaciones Laborales.

- La capacitación se cita por medio electrónico y va dirigida al grupo a capacitar, dejando constancia de recibo del correo.

- Se llevan registros de asistencia por cada capacitación realizada, mediante una planilla que diligencian todos los asistentes.

Para los funcionarios que no asisten a la capacitación, se solicita a Gerencia de Talento Humano y Relaciones Laborales la inclusión de los funcionarios en la programación de la siguiente sesión.

13.4 EVALUACIÓN Y MEJORAMIENTO CONTINUO DEL PLAN

El programa de capacitación y sensibilización cuenta con métricas que permiten medir su eficacia y justificar cuantitativa o cualitativamente su desempeño. Dependiendo del programa establecido, se podrán utilizar alguna de las siguientes métricas:

- Cobertura del Programa
- Cumplimiento de Actividades
- % de aprobación de las evaluaciones
- % de conductas aprendidas.
- Nivel de Satisfacción.

Del análisis de las métricas establecidas para medir el programa, y de acuerdo con los resultados obtenidos de las mismas, se dejará un informe de cierre, con lecciones aprendidas y oportunidades de mejoramiento a considerar en el plan del siguiente año.

14. ANEXOS

PARTE I	Sistema de Gestión de la Continuidad del Negocio - SGCN
PARTE II	Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT
PARTE III	Sistema de Administración de Riesgo de Fraude y Corrupción - SARFC
PARTE IV	Sistema de Administración de Riesgos Financieros - SARF
PARTE V	Sistema de Gestión de Riesgos de Seguridad de la Información y Ciberseguridad

Documentos adicionales que soportan la Gestión Integral de Riesgos y el desarrollo del presente Manual:

- Caracterización y Flujo Proceso Gestión Integral de Riesgos
- Instructivo de Metodología de Evaluación de Riesgos por Procesos
- Instructivo de Gestión de Riesgos en Proyectos
- Instructivo de Gestión de Riesgos Estratégicos y Emergentes
- Instructivo de Gestión de Eventos de Riesgo
- Instructivo de Gestión de Riesgos de Terceras Partes

15. CONTROL DE CAMBIOS DEL DOCUMENTO

FECHA	VERSIÓN	MODIFICACIÓN	ELABORÓ	REVISÓ.	APROBÓ.
30/03/2012	1	Acuerdo No. 021 de 2012. Por el cual se aprueba el Manual de Administración de Riesgo Operativo de la Administradora Colombiana de Pensiones Colpensiones.	Nombre: Diana P. Valderrama A. Cargo: Gerente Nacional de Gestión de Riesgos	Nombre: Jorge A. Silva A. Cargo: Vicepresidente de Planeación y Riesgos	Nombre: Junta Directiva
17/05/2017	2	Acuerdo No. 114 de 2017. Aprueba el Manual del Sistema Integral de Administración de Riesgos. El cual integra los diferentes manuales de administración de riesgos aplicables a Colpensiones, así: PARTE I - Sistema de Gestión de la Continuidad del Negocio - SGCN PARTE II - Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo - SARLAFT PARTE III - Gestión de Riesgo de Fraude y Corrupción PARTE IV - Sistema de Administración de Riesgo de Mercado - SARM	Nombre: Diana P. Valderrama A. Cargo: Gerente de Riesgos Y Seguridad de la Información (A)	Nombre: Diego José Ortega R. Cargo: Vicepresidente de Seguridad y Riesgos Empresariales	Nombre: Junta Directiva
30/11/2017	3	Acuerdo Nº 126 de 2017. Aprueba la modificación de la Parte II Sistema de Administración de Riesgo de Lavado de Activos y Financiación del Terrorismo – SARLAFT del Manual del Sistema Integral de Administración de Riesgos.	Nombre: Eliana Rodríguez Cargo: Profesional Máster 320-05	Diego José Ortega R. Cargo: Vicepresidente de Seguridad y Riesgos Empresariales	Nombre: Junta Directiva

21/01/2019	4	Acuerdo No. 001 de 2019. Por el cual actualiza el Manual del Sistema Integral de Administración de Riesgos y sus Partes: Parte I – Sistema de Gestión de la continuidad del Negocio. Parte III – Sistema de Administración del Riesgo de Fraude y Corrupción. Parte IV – Sistema de Administración de Riesgo de Mercado y Contraparte. Se crea la Parte V – Sistema de Administración de Riesgo de Seguridad de la Información y Ciberseguridad.	Nombre: Antonio José Coral Triana Cargo: Gerente de Riesgos y Seguridad de la Información	Nombre: Luis Fernando Ucros V. Cargo: Vicepresidente de Seguridad y Riesgos Empresariales (A)	Nombre: Junta Directiva
25/08/2020	5	Acuerdo Nº 006 de 2020 Por el cual se modifica y actualiza el Manual del Sistema Integral de Administración de Riesgos de la Administradora Colombiana de Pensiones (Colpensiones).	Nombre: Antonio José Coral Triana Cargo: Gerente de Riesgos y Seguridad de la Información	Nombre: Fabián Mauricio Arias Jiménez Cargo: Vicepresidente de Seguridad y Riesgos Empresariales	Nombre: Junta Directiva
17/12/2021	6	Acuerdo No.15 de 2021 Actualización del Manual en los siguientes numerales: 5. Definiciones 6.2. Políticas generales 6.3. Políticas específicas 6.4. Principio y políticas gestión de riesgo en terceras partes 7.1.2. Representante Legal 7.1.7. Oficial de Cumplim. 7.1.9 Líderes de Procesos	Nombre: Antonio José Coral Triana Cargo: Gerente de Riesgos y Seguridad de la Información	Nombre: Fabián Mauricio Arias Jiménez Cargo: Vicepresidente de Seguridad y Riesgos Empresariales	Nombre: Junta Directiva

		9.1.1 Declaración Cualitativa del Apetito de Riesgo 10. Metodología para la Gestión Integral de Riesgos 10.1.1. Análisis de Riesgos 10.2.2.1. Análisis de Riesgo Inherente 10.2.1.3 Identificación de riesgos por proceso 10.2.3 Valoración del riesgo 10.4.1. Eventos de riesgo 10.4.4. Evaluación de riesgos en terceras partes Principales cambios en el marco de la actualización por la CE 025 de 2020 SARO, gestión de riesgo de terceras partes y riesgo de cumplimiento. Actualización de las Partes I, II, III, IV Y V del Manual SIAR.			
31/08/2022	7	Acuerdo Nº 10 de 2022 Por el cual se modifica y actualiza el Manual del Sistema Integral de Administración de Riesgos de la Administradora Colombiana de Pensiones (Colpensiones), en el siguiente numeral. MARCO INTEGRAL DE APETITO DE RIESGO Y AGREGACIÓN DE RIESGOS 9.1. MARCO INTEGRAL DE APETITO DE RIESGO 9.1.2. Declaración Cuantitativa del Apetito	Nombre: Antonio José Coral Triana Cargo: Gerente de Riesgos y Seguridad de la Información	Nombre: Antonio José Coral Triana Cargo: Vicepresidente de Seguridad y Riesgos Empresariales (A)	Nombre: Junta Directiva

		de Riesgo: Se actualiza la metodología de cálculo del apetito, capacidad y tolerancia de riesgo. 9.2. AGREGACIÓN DE RIESGOS 10.2.2.1. Análisis de Riesgo Inherente. Se ajustan los criterios económicos, en el marco del valor del apetito de riesgo, para la valoración del impacto del riesgo.			