

HISTORIA DEL DOCUMENTO					
VERSIÓN	DESCRIPCIÓN	ELABORÓ	REVISÓ	APROBÓ	FECHA
1	Versión inicial del documento.	Subgerencia de Gestión de Riesgos y Control Interno	Comité de Riesgos	Comité de Riesgos	18/11/2020.
2	Ajustes cambios estructura organizacional	Gerencia de Gestión de Riesgos y Cumplimiento	Gerencia Corporativa de Gestión de Riesgos	Junta Directiva	22/10/2021

TABLA DE CONTENIDO

1. DEFINICIÓN DE LA GESTIÓN INTEGRAL DE RIESGOS.....	2
2. OBJETIVO.....	2
3. ALCANCE	3
4. MARCO LEGAL, NORMAS RELACIONADAS Y MARCO DE REFERENCIA	3
5. ESTRUCTURA Y GOBIERNO	3
6. GLOSARIO.....	10



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

1. DEFINICIÓN DE LA GESTIÓN INTEGRAL DE RIESGOS

La Gestión Integral de Riesgos se define como “La cultura, capacidades y prácticas, integradas con la definición de la estrategia y el desempeño, en las que las organizaciones confían para gestionar el riesgo de cara a la creación, preservación y materialización del valor”. El proceso de Gestión Integral de Riesgos requiere la implementación de un enfoque estandarizado a nivel organizacional para asegurar que los riesgos sean identificados, evaluados, controlados y reportados de forma consistente y oportuna.

Esta definición considera, los siguientes conceptos básicos de la Gestión Integral de Riesgos:

- Es un proceso continuo.
- Es realizado por todo el personal en todos los niveles de la Compañía (la Junta Directiva, la Alta Gerencia y todo el personal).
- Se aplica en el establecimiento de la estrategia de la organización.
- Se aplica en toda la Compañía, en cada nivel y unidad de negocio, e incluye la adopción de una perspectiva del riesgo a nivel conjunto.
- Está enfocada en gestionar los riesgos a fin de reducir la probabilidad de que se produzca un evento que afecte el logro de objetivos o el despliegue de la estrategia y en gestionar impactos cuando éstos se produzcan.
- Permite proporcionar un nivel de seguridad razonable a la Junta Directiva y a Presidencia en cuanto al control, monitoreo y Gestión Integral de Riesgos.
- El enfoque en resumen está orientado al logro de los objetivos.

2. OBJETIVO

2.1 Objetivo General.

Establecer los criterios y lineamientos a seguir para facilitar el cumplimiento de la misión y de los objetivos de la Organización; a través de la Gestión Integral de Riesgos (GIR). La misión es preservar el valor de Primax Colombia S.A. (en adelante “Primax Colombia” o “la Compañía”) a través de la prevención de eventos internos y externos que puedan impactar negativamente en el logro de los objetivos.

2.2 Objetivos Específicos.

- a. Facilitar el cumplimiento de los objetivos de Primax Colombia, mediante la aplicación de un enfoque basado en el Marco Integrado de Control Interno COSO – ERM¹ (en adelante “Marco COSO ERM”).

¹ COSO, por sus siglas en Inglés, se refiere el *Committee of Sponsoring Organizations of the Treadway Commission*. Esta organización emitió en 2017, el nuevo marco de Gestión Integral de Riesgos conocido como el “*Enterprise Risk Management – Aligning Risk with Strategy and Performance*”. El nuevo Marco COSO ERM integra el riesgo con la estrategia, al considerar en forma explícita el riesgo durante el proceso de planificación estratégica. A la vez, intenta mejorar el enfoque de la Gestión Integral de Riesgos como una manera de crear, preservar, mantener y generar valor en la organización.

La información contenida en este documento es propiedad de Primax. Este documento ha sido desarrollado exclusivamente por y para Primax, su uso o discusión fuera del ámbito del proceso interno de la compañía, así como la reproducción, distribución o comunicación del contenido de este por cualquier medio, queda expresamente prohibido sin consentimiento del centro de especialización



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

- b. Establecer consideraciones, estándares y criterios que permitan a la Compañía administrar adecuadamente los riesgos, con la participación de la Gerencia y la Junta Directiva.
- c. Gestionar los riesgos mediante el establecimiento de un marco de control aplicable en la Compañía, orientada al logro de sus objetivos.
- d. Definir los roles y responsabilidades en materia de Gestión Integral de Riesgos en todos los niveles de la Compañía y evaluar el desempeño de cada responsable.
- e. Fomentar una cultura de control y Gestión Integral de Riesgos en las actividades diarias y toma de decisiones de la Junta Directiva, Alta Gerencia, demás Gerencias y colaboradores, a través de normas, procedimientos, capacitación y seguimiento de su cumplimiento para minimizar las actividades que pudiesen impactar en el cumplimiento de los objetivos estratégicos de la Compañía.

3. ALCANCE

El ámbito de aplicación de la presente Política es de carácter total, es decir, aplica a todas las unidades de negocio, áreas, comités, proyectos entre otros entes existentes de Primax Colombia.

4. MARCO LEGAL, NORMAS RELACIONADAS Y MARCO DE REFERENCIA

El marco de referencia empleado para la definición de los lineamientos presentados en este documento son los siguientes:

- a. Marco Integrado COSO ERM, emitido en el año 2004 y actualizado en el año 2017.
- b. Marco Integrado COSO - Control Interno, emitido en el año 2013.
- c. Estándar Internacional ISO 31000 – Gestión de Riesgos.
- d. Estándar Internacional ISO 22301 – Sistema de Continuidad de Negocios.
- e. Estándar Internacional ISO 27001 – Sistema de Gestión de Seguridad de Información.
- f. Estándar Internacional ISO 37000 – Sistema de Gestión Antisoborno.

5. ESTRUCTURA Y GOBIERNO

La estructura organizacional debe satisfacer los requerimientos de la Gestión Integral de Riesgos del Grupo Económico Romero (GR) en términos de calidad y cantidad de recursos, estos deben tener acceso a toda la información relevante de la Compañía para desarrollar su trabajo de manera eficaz y eficiente. Adicionalmente, esta estructura debe ser independiente de las funciones operativas y de control de las mismas.



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

En Primax Colombia

a. De la Junta Directiva

La Junta Directiva supervisa el desarrollo de estrategia de negocio y mantiene la responsabilidad por el establecimiento de una Gestión Integral de Riesgos alineada al cumplimiento de los objetivos organizacionales.

Entre sus responsabilidades específicas están:

1. Evaluar y aprobar los planes de negocios de la Compañía considerando el análisis de los riesgos que estos conllevan.
2. Evaluar la idoneidad de la estrategia de la Compañía, su alineación con la misión, visión y valores, y el riesgo que implica el desarrollo de la estrategia.
3. Establecer un Sistema de Control Interno y una Gestión Integral de Riesgos (Gobierno Corporativo).
4. Aprobar las funciones y responsabilidades de los órganos de administración, control y monitoreo del riesgo.
5. Aprobar los recursos necesarios para el adecuado desarrollo de la Gestión Integral de Riesgos.
6. Establecer y supervisar periódicamente el despliegue del modelo corporativo de Gobierno de Gestión Integral de Riesgos y propiciar un ambiente interno en la Compañía que facilite su desarrollo adecuado.
7. Tomar conocimiento sobre los principales riesgos afrontados por la Compañía, unidades de negocio y proyectos.

b. Del Comité de Riesgos

Es el órgano de apoyo delegado por la Junta Directiva de la Compañía y dentro de los límites designados, es el responsable de tomar decisiones vinculadas a los riesgos significativos a los que esté expuesta la Compañía, unidad de negocio o proyecto. Los miembros del Comité de Riesgos son designados por el Presidente de la Junta Directiva.

Entre las responsabilidades específicas relacionadas con la Gestión Integral de Riesgos están:

1. Revisar periódicamente y aprobar los lineamientos, políticas y metodología propuestos por la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos de Excellia para el despliegue del modelo Corporativo de Gestión Integral de Riesgos.
2. Aprobar el apetito al riesgo de la Compañía.
3. Revisar y aprobar el Plan Anual de Gestión Integral de Riesgos.



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

4. El contenido del plan considera las actividades que el Comité y la Compañía desarrollarán durante todo el año a fin de incrementar su nivel de madurez de la Gestión Integral de riesgos.
5. Efectuar seguimiento al avance del Plan Anual de Gestión Integral de Riesgos, durante las sesiones del Comité de Riesgos.
6. Monitorear el nivel de exposición de la Compañía al riesgo mediante los reportes de riesgo e indicadores claves de desempeño (KPI) definidos.
7. Identificar y analizar nuevos riesgos a los que la Compañía pudiera estar expuesta.
8. Recomendar focos de atención para la Gestión Integral de Riesgos, en función a la evaluación del entorno externo e interno de la Compañía, así como hechos de importancia conocidos por los Directivos.
9. Aprobar las estrategias de respuesta definidas para los riesgos residuales Muy Altos y Altos.
10. Compilar y reportar los resultados ejecutivos de la Gestión Integral de Riesgos obtenidos en la sesión del Comité de Riesgos, a la Junta Directiva.
11. Promover proyectos para apoyar las mejores prácticas de buen gobierno corporativo y conducta ética.
12. Revisar y aprobar las acciones de fortalecimiento de la cultura de Gestión Integral de Riesgos, que contemplan actividades de sensibilización y capacitación en diversos niveles de la Compañía.

c. Del Presidente:

Establece la Gestión Integral de Riesgos en la Compañía en coordinación con la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos de Excellia y propicia un ambiente de control interno adecuado que contribuya al logro de objetivos de la Compañía.

Entre las responsabilidades específicas relacionadas con la Gestión Integral de Riesgos están:

1. Asegura que el sistema de control interno y la administración de riesgos sea implementado oportunamente en la Compañía.
2. Optimiza la relación riesgo-retorno a través de una adecuada supervisión y el cumplimiento de políticas, directivas, metodologías, procedimientos y estrategias de prevención, identificación, transferencia y mitigación de los riesgos.
3. Promueve el desarrollo de una cultura interna de control que fomente la prevención y gestión de los diferentes tipos de riesgos.
4. Proporciona la información necesaria para que se realice el monitoreo periódico del desempeño general de la Gestión Integral de Riesgos al Responsable de Gestión de Riesgos y Cumplimiento, así como a la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos de Excellia.
5. Es responsable de contar con los colaboradores idóneos que cumplan el perfil profesional recomendado por la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos de Excellia para desempeñar el rol de Responsable de Gestión de Riesgos y Cumplimiento, de forma tal que pueda cumplir las funciones asignadas de acuerdo con lo definido en la presente Política.



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

P-EVA-GIR-RN-002

Versión 2

22/10/2021

Página 6 de 10



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

d. De los Responsables de procesos:

Cada responsable, en su ámbito de acción, debe administrar los riesgos relacionados al logro de los objetivos de sus procesos y de verificar que los controles implementados para mitigar los riesgos identificados funcionan de manera efectiva, en caso de identificar oportunidades de mejora o ausencia de controles deben propiciar su implementación.

Entre las responsabilidades específicas relacionadas con la Gestión Integral de Riesgos están:

1. Implementar la Gestión Integral de Riesgos en los procesos bajo su responsabilidad conforme a los lineamientos, políticas, estatuto y metodología aprobados por el Comité de Riesgos.
2. Revisar la vinculación entre las operaciones y los niveles de apetito de riesgo, verificando que los controles implementados para mitigar los riesgos funcionan de manera efectiva.
3. Identificar y priorizar (efectuar valoración) de los riesgos que enfrenta el proceso bajo su cargo.
4. Monitorear y controlar los riesgos de sus procesos; a través de la verificación del funcionamiento efectivo de los controles clave a manera de autoevaluación del diseño y operatividad.
5. Ejecutar las actividades que se les asignen dentro del Plan Anual de Gestión Integral de Riesgos de la Compañía.
6. Asegurar que la documentación de sus procesos está actualizada:
 - Diagrama de flujo
 - Matriz de riesgos y controles
7. Reportar cualquier evento de materialización de riesgos al Responsable de Gestión de Riesgos y Cumplimiento de la Compañía.
8. Identificar oportunidades de mejora, en materia de control interno, en los procesos bajo su responsabilidad, gestionar su implementación y monitorear su cumplimiento.
9. Comunicar los cambios en sus procesos y en los riesgos asociados al Responsable de Riesgos y Cumplimiento de la Compañía.
10. Realizar el diseño y/o rediseño de controles bajo la asesoría del Responsable de Riesgos y Cumplimiento de la Compañía.
11. Definir indicadores clave de desempeño (KPIs) en coordinación con el Responsable de Riesgos y Cumplimiento de la Compañía y monitorear su desempeño.

e. Del Responsable de la Gestión de Riesgos y Cumplimiento de la Compañía

Dedica la totalidad de su tiempo a las labores relacionadas con la Gestión Integral de Riesgos, definidas a nivel de actividades en el Plan Anual de Gestión Integral de Riesgos con las áreas de la Compañía.

Entre las responsabilidades específicas están:



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

1. Elaborar reportes para el Comité de Riesgos y otros solicitantes de información relacionada con la Gestión Integral de Riesgos.
 2. Coordinar las actividades de Gestión Integral de Riesgos consignadas en el Plan Anual de Gestión Integral de Riesgos con las áreas de la Compañía.
 3. Desarrollar e implementar el programa de indicadores clave de desempeño (KPI). Incluye monitorear su cumplimiento en coordinación con la Vicepresidencia Corporativa de Gestión Integral de Riesgos de Excellia.
 4. Asistir a los Responsables de Procesos en la implementación del mapa de riesgos de procesos, facilitando el entendimiento y aplicación de la metodología definida.
 5. Facilitar el taller de actualización de los criterios para la valoración de riesgos.
 6. Coordinar y facilitar los talleres de identificación y evaluación (priorización) de riesgos.
 7. Validar los resultados del proceso de identificación y evaluación de riesgos.
 8. Evaluar el cumplimiento de los planes de acción y las oportunidades de mejora para la mitigación de riesgos.
 9. Evaluar el motivo de origen de los riesgos materializados y recomendar las oportunidades de mejora correspondientes.
 10. Soportar a los Responsables de Procesos en la documentación de políticas y procedimientos asociados a sus procesos y revisar su actualización periódica.
 11. Asesorar a los Responsables de Procesos en el diseño y/o rediseño de procesos en términos de control interno y de controles, y validar oportunidades de mejora orientadas a la mitigación de riesgos.
 12. Verificar, periódicamente, que los controles más relevantes sean efectivos a nivel de diseño.
 13. Establecer los canales de comunicación efectiva con el fin de que las áreas involucradas en la identificación, administración y monitoreo de riesgos, tengan pleno conocimiento de los niveles de riesgo asumidos de acuerdo a las políticas establecidas por el Comité de Riesgos y las normas legales vigentes.
 14. Establecer iniciativas orientadas al fortalecimiento de la Gestión Integral de Riesgos en coordinación con la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos de Excellia.
- f. Del personal de Primax Colombia en general

El personal de la Compañía debe cumplir con lo establecido en la Política de Gestión Integral de Riesgos, así como con los lineamientos de las metodologías, procedimientos y políticas relacionadas al tema, sin excepción alguna.

En Excellia (Corporativo del Grupo Económico Romero)

- a. De la Vicepresidencia Corporativa de Auditoría y Gestión Integral de Riesgos:



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

Facilita el cumplimiento de los objetivos de las empresas del GR, mediante la aplicación de una metodología basada en el Marco Integrado de Control Interno COSO – ERM, estableciendo un estándar que permita a la Compañía administrar adecuadamente los riesgos, en conjunto con otros actores del modelo corporativo de Gestión Integral de Riesgos: Junta Directiva, Comité de Riesgos, Gerencias, entre otros.

Asimismo, define los roles y responsabilidades en materia de Gestión Integral de Riesgos en todos los niveles de la Compañía y fomenta una cultura de control y Gestión Integral de Riesgos en las actividades diarias y toma de decisiones de la Junta Directiva, Comité de Riesgos, Gerencias y colaboradores.

Entre las responsabilidades específicas relacionadas con la Gestión Integral de Riesgos están:

1. Guiar la interacción entre la Gestión Integral de Riesgos, los planes de negocio y las actividades de gestión empresarial.
2. Formular, revisar, actualizar y difundir la Política para la Gestión Integral de Riesgos, aplicable a la Compañía.
3. Elaborar la metodología corporativa de Gestión Integral de Riesgos e identificar aspectos a ser incorporados o actualizados en los modelos, parámetros y escenarios que se utilizarán para la medición y control de los riesgos.
4. Preparar el Plan Anual de Gestión Integral de Riesgos en coordinación con el Responsable de la Gestión de Riesgos y Cumplimiento de Excellia.
5. Brindar asesoría y apoyo a las distintas las unidades de negocio de la Compañía para el diseño y la implementación de la Gestión Integral de Riesgos, así como el análisis de la consistencia, eficiencia y suficiencia de los esfuerzos de mitigación de riesgos definidos.
6. Identificar las necesidades de capacitación, difusión y otros aspectos relacionados a la Gestión Integral de Riesgos que pudieran ser requeridos al interior de la Compañía.
7. Establecer un Plan de Capacitación para todo el personal de la Vicepresidencia Corporativa Gestión Integral de Riesgos y Responsable de Riesgos de las Compañías. Para el adecuado despliegue del modelo corporativo de Gestión Integral de Riesgos es preciso con el conocimiento actualizado en materia de control interno, así como marcos y metodologías vigentes para la Gestión Integral de Riesgos (COSO, estándares, entre otros).
8. Establecer el plan para reforzar la cultura de Gestión Integral de Riesgos con las respectivas gerencias de las unidades de negocio.
9. Identificar y organizar las necesidades de contratación de personal o adquisición de consultorías y/o software para la gestión de riesgos de la Compañía a fin de optimizar recursos.
10. Participar de las sesiones del Comité de Riesgos.
11. Enviar el cronograma de convocatorias a las sesiones del Comité de Riesgos.
12. Consolidar la información a presentar durante la sesión del Comité de Riesgos.
13. Enviar la agenda y el contenido (presentación) a revisar en cada sesión del Comité de Riesgos, de forma anticipada, a los miembros y a los invitados.



POLÍTICA PARA LA GESTIÓN INTEGRAL DE RIESGOS

14. Redactar y enviar el acta posterior a la sesión del Comité.
15. Elaboración del modelo y evaluación de desempeño de los responsables de la gestión integral de riesgos.

6. GLOSARIO

- a. **Apetito de riesgo:** El apetito de riesgo es el nivel de riesgo que la Compañía decide asumir durante el proceso de consecución de sus objetivos. La determinación de este punto permite controlar y mantener los riesgos en los niveles deseados.
- b. **Capacidad de riesgos:** Es el nivel de riesgo que afecta el cumplimiento de los objetivos de la Compañía.
- c. **Control Interno:** Se refiere a la gestión para proporcionar seguridad razonable sobre el logro de las tres siguientes categorías de objetivos: Efectividad y eficiencia de las operaciones, suficiencia y confiabilidad de la información financiera y cumplimiento con las leyes y regulaciones aplicables.
- d. **Mapa de procesos:** Es un diagrama de valor; un inventario gráfico de los procesos de una empresa.
- e. **Mapa de riesgos:** Gráfico que ilustra el impacto y probabilidad de ocurrencia de los riesgos.
- f. **Proceso:** Conjunto de actividades, tareas procedimientos organizados y repetibles que producen un resultado esperado.
- g. **Gestión Integral de Riesgos:** Se refiere a la gestión y aplicación de un conjunto de políticas, procedimientos y controles para identificar riesgos, analizarlos y gestionar su impacto y/o probabilidad de ocurrencia.
- h. **Riesgo Residual:** Nivel resultante del riesgo después de aplicar los controles.
- i. **Tolerancia al riesgo:** Es la desviación del nivel de riesgo que la Compañía quiere aceptar.