Manual de Gestión de Riesgos

PRIMAX

HISTORIA DEL DOCUMENTO					
VERSIÓN	**DESCRIPCIÓN**	**ELABORÓ**	**REVISÓ**	**APROBÓ**	**FECHA**
0	Versión inicial	Coordinador de Riesgos y Continuidad de Negocio	Gerente de Riesgos y Cumplimiento	Gerente de Riesgos y Cumplimiento	19/12/2025

Política de Riesgos

En **Primax Colombia** estamos convencidos de que una gestión sólida de los riesgos es fundamental para proteger nuestro patrimonio, fortalecer la confianza de los grupos de interés y alcanzar los objetivos estratégicos. Por ello, la **Gestión Integral de Riesgos (GIR)** es un componente esencial de nuestra cultura y de nuestro modelo de gestión, orientado a la creación, preservación y generación de valor sostenible.

Conscientes de que la Compañía está expuesta a riesgos, asumimos un rol activo en su gestión, implementando mecanismos efectivos de prevención, mitigación, transferencia y control, según la naturaleza de cada riesgo. Esto incluye desde la toma de seguros hasta la eliminación de riesgos críticos cuando sea necesario. En este sentido, cada proceso es responsable de la gestión de sus riesgos de acuerdo con los lineamientos de la Gerencia de Riesgos y Cumplimiento.

La Compañía se compromete a:

- Implementar un enfoque estandarizado en toda la organización para identificar, evaluar, controlar y reportar riesgos de manera oportuna y consistente.
- Alinear la gestión de riesgos con la estrategia corporativa, definiendo límites claros de valoración de riesgos y niveles de tolerancia aceptables.
- Proporcionando lo recursos necesarios (humanos, tecnológicos y financieros) para garantizar una gestión de riesgos efectiva.
- Establecer una responsabilidad diferenciada entre las áreas y unidades de negocio basada en el modelo de las tres líneas[1].
- Gestionar activamente los riesgos dentro de los umbrales definidos, asegurando la resiliencia organizacional frente a eventos que puedan comprometer la consecución de objetivos.
- Definir una estrategia de gestión de riesgos según el tipo y nivel de exposición, en la aceptación del riesgo, la interrupción de la actividad que genera la exposición, la mitigación del riesgo mediante medidas preventivas o contingentes aplicables según su naturaleza, o la transferencia de exposición a terceros.
- Desarrollar y actualizar el mapa de riesgos estratégicos y de procesos, revisándolo de manera periódica o cuando las condiciones del entorno lo exijan.

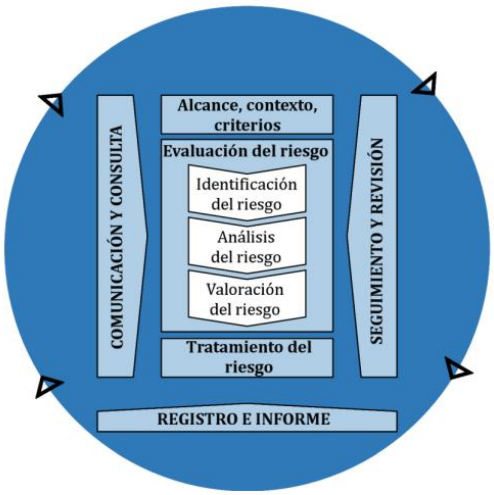
Esta política es de obligatorio cumplimiento para todos los colaboradores y constituye un marco de referencia para el ejercicio de sus funciones. Con esta política la Compañía reafirma su compromiso de liderar la gestión integral de riesgos como práctica estratégica y pilar de confianza para sus colaboradores, clientes, socios y demás grupos de interés.

[1] Modelo de las Tres Líneas del IIA (Institute of Internal Auditors), 2020

1. Alcance

Establecer los criterios y lineamientos a seguir para facilitar el cumplimiento de la misión y objetivos estratégicos de la Compañía a través de la Gestión Integral de Riesgos - GIR. La cual permite preservar el valor a través de la prevención de eventos internos y externos que puedan impactar negativamente en el logro de los objetivos.

El desarrollo operativo de la gestión de riesgos contempla la identificación, análisis, evaluación y tratamiento de los riesgos estratégicos, así como de los riesgos que se presentan en los procesos que integran la cadena de valor y proyectos que desarrolla la compañía.



2. Objetivos

- Definir lineamientos que permitan a la Compañía administrar adecuadamente los riesgos.
- Gestionar los riesgos mediante el establecimiento de un marco de control aplicable en la Compañía, orientada al logro de sus objetivos.
- 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.
- 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. Gobierno

Para que la Gestión Integral del Riesgo – GIR sea parte de la cultura de la Compañía es crucial el compromiso de todos los colaboradores y especialmente desde la Alta Gerencia. Es por ello que se define la siguiente estructura de gobierno y se detalla las responsabilidades en todos los niveles de la compañía lo cual permite que todos los elementos del GIR se armonicen.

3.1 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 estratégicos. Entre sus responsabilidades específicas están:

1. 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.
2. Establecer, promover y fomentar una cultura basada en la Gestión Integral de Riesgos.
3. Aprobar las funciones y responsabilidades de los órganos de administración, control y monitoreo del riesgo.
4. Evaluar y aprobar los planes de negocios de la Compañía considerando el análisis de los riesgos que estos conllevan.
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.

3.2 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 y políticas propuestos por la Gerencia de Riesgos y Cumplimiento para el despliegue del modelo 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, el cual debe considerar 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.
4. Efectuar seguimiento al avance del Plan Anual de Gestión Integral de Riesgos, durante las sesiones del Comité de Riesgos.
5. Monitorear el nivel de exposición de la Compañía al riesgo mediante los reportes de riesgo e indicadores claves de desempeño (KPI) definidos.
6. Identificar y analizar nuevos riesgos a los que la Compañía pudiera estar expuesta.
7. 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.
8. Aprobar las estrategias de respuesta definidas para los riesgos residuales Muy Altos y Altos.
9. 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.

3.3 Presidente

Establece la Gestión Integral de Riesgos en la Compañía 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 a la Gerencia de Riesgos y Cumplimiento
5. Velar por la ejecución de los planes de acción definidos para los riesgos estratégicos.

3.4 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 y metodología establecidos.
2. Identificar y efectuar valoración de los riesgos que enfrenta el proceso bajo su cargo.
3. Monitorear y controlar los riesgos de sus procesos; a través de las diferentes estrategias de tratamiento de los riesgos.
4. Verificar el 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, procedimientos y matriz de riesgos y controles, entre otros)
7. Reportar cualquier evento de materialización de riesgos a la Gerencia 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 Gerente de Riesgos y Cumplimiento de la Compañía.
10. Realizar el diseño y/o rediseño de controles bajo la asesoría de la Gerencia de Riesgos y Cumplimiento de la Compañía.
11. Definir indicadores clave de desempeño (KPIs) en coordinación con la Gerencia de Riesgos y Cumplimiento de la Compañía y monitorear su desempeño.

3.5 Gerencia de Riesgos y Cumplimiento

Propone y brinda los lineamientos necesarios para asegurar razonablemente una adecuada gestión de riesgos. Entre las responsabilidades específicas están:

1. Proponer la metodología 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.
2. Preparar el Plan Anual de Gestión Integral de Riesgos con las áreas de la Compañía y coordinar las actividades de Gestión Integral de Riesgos consignadas en él.

3. Elaborar reportes para el Comité de Riesgos y otros solicitantes de información relacionada con la Gestión Integral de Riesgos.
4. Asesorar y promover el desarrollo de indicadores clave de desempeño (KPI).
5. Asistir a los Responsables de Procesos en la implementación del mapa de riesgos de procesos, facilitando el entendimiento y aplicación de la metodología definida.
6. Facilitar el taller de actualización de los criterios para la valoración de riesgos.
7. Coordinar y facilitar los talleres de identificación y evaluación (priorización) de riesgos.
8. Validar los resultados del proceso de identificación y evaluación de riesgos.
9. Evaluar el cumplimiento de los planes de acción y las oportunidades de mejora para la mitigación de riesgos.
10. Evaluar el motivo de origen de los riesgos materializados y recomendar las oportunidades de mejora correspondientes.
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. Así como el análisis de la consistencia, eficiencia y suficiencia de los esfuerzos de mitigación de riesgos definidos
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.

3.6 Colaboradores de Primax

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

3.7 Auditoria Interna

Asegura y fomenta la mejora continua en la gestión de riesgos de la Compañía a través de las siguientes responsabilidades:

1. Participar de las sesiones del Comité de Riesgos.
2. Evaluar la efectividad y nivel de madurez de la Gestión de Riesgos de la Compañía
3. Promover la mejora continua del GIR a través de la identificación de oportunidades de mejora

4. Redactar y enviar el acta posterior a la sesión del Comité.

4. Metodología de Gestión de Riesgos

La metodología utilizada para el Manual de Gestión de Riesgos, está apoyada en:

- Marco Integrado COSO - Control Interno, emitido en el año 2013.
- Estándar Internacional ISO 31000 – Gestión de Riesgos.

Categorías de Riesgos

Riesgo Disponibilidad- CN

Asegura sus **operaciones críticas y servicios esenciales** durante y después de eventos disruptivos, minimizando el impacto en el negocio, protegiendo sus activos y manteniendo la confianza de sus clientes y stakeholders.

Riesgo Estratégico

Fortalecer la toma de decisiones consciente e informada, **la optimización de oportunidades y la protección de la reputación de la empresa.**

Riesgo Físico

Se enfoca en prevenir accidentes, **proteger a los colaboradores y los activos de la compañía.**

Riesgo Operativo

Proteger los activos de la organización, reducir pérdidas, **mejorar la eficiencia y la calidad en los procesos**, aumentar la resiliencia y tomar decisiones informadas

Riesgo Compliance

Asegurar el cumplimiento de leyes y políticas, evitar sanciones, proteger la reputación y **fomentar negocios éticos, honestos y transparentes.**

Esta cuenta con un enfoque de procesos, por lo cual desarrolla una serie de etapas con el fin de alcanzar la eficacia del sistema y el cumplimiento de los objetivos trazados:

1 Identificación de Riesgos

En esta etapa se busca determinar los riesgos potenciales a los que se encuentra expuesta la compañía en el desarrollo de sus actividades por parte de cada uno de los líderes o dueños de los procesos o proyectos que se gestionan, con el objetivo de dar cumplimiento con sus objetivos.

El propósito de esta etapa es generar una lista exhaustiva de riesgos con base en aquellos eventos que podrían crear, aumentar, prevenir, degradar, acelerar o retrasar el logro de los objetivos. Es esencial realizar una identificación sistemática, debido a que un riesgo potencial no identificado durante esta etapa será excluido del análisis posterior.

La identificación debe incluir todos los riesgos, sea que estén o no bajo el control de la compañía, y debe ser permanente basado en la planeación y los objetivos estratégicos.

Esta identificación se realiza a través de talleres, entrevistas, inventario de eventos de riesgo, análisis de flujo del proceso y manejo de indicadores. Considerando la normatividad aplicable a la Compañía para los sistemas de gestión riesgos cuyo diseño sea regulado.

En la identificación de riesgos se considera lo siguiente:

Factores de riesgo

Son factores de riesgo las fuentes generadoras de eventos de riesgos. Los factores de riesgo se clasifican en internos y externos. Ejemplos: Recurso Humano, Procesos, TI, Infraestructura, Externos, País, Contrapartes entre otros. Se establecen de conformidad a lo requerido en la regulación.

Causa de riesgo

Son eventos que ocasionan la materialización del riesgo

2 Valoración de Riesgos

Las **variables de medición del riesgo** son:

Probabilidad: Posibilidad de ocurrencia de cada uno de los riesgos, peligros o amenazas, conforme a la siguiente escala de medición. Ver tabla 1 a continuación

Impacto: Es el resultado de un riesgo expresado cualitativa o cuantitativamente. Los criterios de impacto son definidos por la Alta Dirección, e incluyen los siguientes aspectos: financiero, reputacional, legal, seguridad y salud, medio ambiente, calidad, terceros y contagio. Conforme a la escala de medición a continuación tabla 1.

El resultado de la combinación de la probabilidad y el impacto determina la severidad del riesgo denominada Riesgo inherente.

Niveles de riesgo

El nivel de riesgo o severidad se obtiene al multiplicar la probabilidad por el impacto y se ubica en el eje de la matriz de riesgos, como se indica a continuación:

Probabilidad \ Impacto	1	2	3	4	5
5	5	10	15	20	25
4	4	8	12	16	20
3	3	6	9	12	15
2	2	4	6	8	10
1	1	2	3	4	5

Nivel de riesgos	Probabilidad x Impacto
Muy alto	20 - 25
Alto	15 - 19
Medio alto	10 - 12
Medio	5 - 9
Bajo	3 - 4
Muy bajo	1 - 2

Tabla 1

Criterios de Impacto

Variables	Criterios	Muy Bajo 1	Bajo 2	Medio 3	Alto 4	Muy Alto 5
Impacto	Reputacional	Cobertura negativa en redes sociales que no tienen impacto en la imagen en la empresa.	Cobertura negativa en medios de comunicación regional y/o redes sociales que pueden afectar de manera indirecta a la empresa.	Cobertura negativa en medios de comunicación regionales y/o nacionales, redes sociales y/o comunicaciones emitidas por entes de control que afecta directamente a la empresa	Desprestigio de la imagen de la empresa por cobertura negativa en medios de comunicación nacionales de alta cobertura, redes sociales y/o comunicaciones emitidas por entes de control que pueda conllevar a la finalización de la relación con contrapartes.	Desprestigio de la imagen de la empresa por cobertura negativa en medios de comunicación nacionales de alta cobertura y/o internacionales, redes sociales, y/o comunicaciones emitidas por entes de control que pueda conllevar a la finalización de relación con contrapartes, disminución de ingresos para la empresa.
	Seguridad y salud	Eventos de Primeros Auxilios / Lesiones Menores que no incapacitan.	Trabajo Restringido o Tratamiento Médico (con tiempo perdido por atención).	Lesiones Graves o con pérdida de tiempo (incapacidad temporal) /Enfermedad Profesional.	Lesiones Graves o con pérdida de tiempo (incapacidad permanente) /Enfermedad Profesional.	Fatalidad o lesión grave externos (Clientes y/o comunidad)
	Medio Ambiente	Efectos sin consecuencias o limitado al sitio o proximidad cercana.	Efectos adversos menores potenciales a corto plazo, respuesta de emergencia local, limpieza de días / semanas.	Efectos adversos significativos, a mediano plazo (de 1 a 3 años), potenciales localizados, respuesta de emergencia intermedia, limpieza de semanas/meses.	Efectos adversos significativos, a largo plazo (más de 3 años), de posible diseminación, respuesta de emergencia mayor, limpieza a largo plazo.	Daños o efectos ambientales con afectación de suelo y/o agua permanentes / irreversibles.
	Calidad	El producto no cumple todos los requisitos regulados pero es detectado internamente	El producto final entregado no cumple con los requisitos legales normativos vigentes que derivan en reclamos esporadicos (Entre 1 y 5 reclamaciones al año) formales de clientes .	El producto final entregado no cumple con los requisitos legales normativos vigentes que derivan en reclamos / quejas reiterativas (entre 6 y 10 reclamaciones al año) formales de clientes.	El producto final entregado no cumple con los requisitos legales normativos vigentes que derivan en reclamos / quejas reiterativas (mas de 10 reclamaciones al año) formales de clientes.	El producto final entregado no cumple con los requisitos legales normativos vigentes en todas las terminales que derivan en pérdida de clientes con alto costo y afectan la capacidad de la empresa para captar nuevos clientes.
	Terceros (Cliente, proveedor, socio)	No se generan incumplimientos a los términos de acuerdos establecidos con terceros.	Se generan incumplimientos a los términos de acuerdos establecidos con terceros que derivan en reclamos / quejas esporádicas.	Se generan incumplimientos a los términos de acuerdos establecidos con clientes que derivan en reclamos / quejas reiterativas formales de terceros.	Se generan incumplimientos a los términos acordados que podrían derivar en la pérdida de terceros con alto costo / esfuerzo de ser reemplazados (no renovación de contratos).	Se generan incumplimientos a los términos acordados que derivan en pérdida de terceros con alto costo / esfuerzo de ser reemplazados(no renovación de contratos) y afectan la capacidad de la empresa para captar nuevos terceros.
	Aspectos legales y cumplimiento	- Investigación y/o proceso penal contra cliente, operador conjunto/ joint venture, consorcios, uniones temporales, socio. - Denuncia interpuesta ante entidad administrativa o reguladora contra el cliente, operador conjunto/ joint venture, consorcios, uniones temporales, socio.	Hallazgos a la compañía por parte del organo de control y vigilancia, incluyendo llamados de atención u observaciones por parte de organos de control internos (revisoría fiscal - auditoría interna o externa). Amonestación a un empleado de la compañía por incumplir normas, regulaciones o políticas internas	Investigaciones de cualquier tipo contra algún empleado de la compañía. La empresa es objeto de una visita completa por parte del organo de control y vigilancia	Procesos de tipo penal, fiscal o administrativo contra miembros de la alta dirección, miembros de la junta directiva y sus comités, accionistas con participación = o mayor al 5% Sanciones en primera instancia para la empresa, representante legal u oficial de cumplimiento por incumplimiento a normas o regulaciones. Vigilancia especial a la empresa por parte del órgano de control.	Medidas cautelares a la compañía por parte de las autoridades competentes y/o entes de control, o imposición de sanciones, que puedan llevar incluso a una intervención o cierre de la compañía, o la inhabilitación para desarrollar actividades sociales y/o contratar con el Estado. Condenas o fallos en firme de tipo penal, fiscal o administrativo en contra de miembros de la alta dirección, junta directiva y sus comités, accionistas con participación = o mayor al 5%
	Contagio	Factores externos de la industria con relación a temas relacionados con LA/FT/C/S y otros delitos. Cuyo impacto no incide en los objetivos y operaciones de la compañía.	Colaborador diferente a la Gerencia que esté o se involucre en temas relacionados con LA/FT/C/S y otros delitos.	Proveedor o cliente de la compañía que está involucrado en una acción o experiencia asociada a temas LA/FT/C/S	Colaborador a nivel gerencial que esté involucrado en una acción o experiencia asociada a temas LA/FT/C/S	La alta dirección, representantes legales, miembros de junta directiva y sus comités, y/o accionistas con participación = o > al 5%, que estén involucrados en una acción o experiencia asociada a temas LA/FT/C/S
	Disponibilidad de información / Confiabilidad del sistema informático	No existe indisponibilidad de la información.	No disponibilidad oportuna de información, que no afecta la toma de decisiones.	Indisponibilidad / Pérdida de información pero que no afecta la toma de decisiones.	Indisponibilidad / Pérdida parcial de la información crítica indispensable para el cliente y estratégica para el negocio.	Indisponibilidad / Pérdida parcial o total de información crítica indispensable para el cliente, estratégica para el negocio y requerida por entes regulatorios.
	EBITDA	Pérdidas menores a 0.5% del EBITDA proyectado para el año (1.075 M COP o 264 K USD).	Pérdidas entre el 0.5% al 1.0% del EBITDA proyectado para el año (de 1.075 M COP a 2.150 M COP) o (de 264 K USD a 528 K USD).	Pérdidas entre el 1.0% al 1.5 % del EBITDA proyectado para el año (de 2.150 M COP a 3.226 M COP) o (de 528 K USD a 792 K USD).	Pérdidas entre el 1.5% al 2.5%) del EBITDA proyectado para el año (de 3.226 M COP a 5.376 M COP) o (de 792 K USD a 1,319 M USD).	Pérdidas mayores al 2.5% del EBITDA proyectado para el año (mayor a 5.376 M COP o 1,319 M USD).

*Los criterios son revisados anualmente para validar su vigencia respecto al contexto del negocio.

Criterios de Probabilidad

	Criterios	Raro	Poco Probable	Posible	Probable	Casi Seguro
Probabilidad	Futuro	Prácticamente imposible que ocurra el próximo año	El evento podría presentarse una vez dentro de los próximos tres años.	El evento podría presentarse durante el segundo año.	El evento podría presentarse dentro del año en curso.	El evento puede ocurrir en cualquier momento dentro de los próximos tres meses.
	Pasado	Ha ocurrido en la industria	Ha ocurrido en los últimos 5 años en la Compañía	Ha ocurrido en los últimos 3 años	Ha ocurido en el último año	Ha ocurrido más de una vez en el último año

Nivel de Riesgo Inherente

Es el resultado del análisis de la probabilidad y el impacto de los riesgos identificados. Es aquel al que la Compañía se ve expuesta en la ejecución propia de los procesos al dar cumplimiento a los objetivos sin considerar los controles o actividades de gestión y control.

Será calculado a partir de los valores resultantes de la probabilidad por el impacto con los respectivos pesos que los mismos tengan dentro del modelo. Los valores serán ubicados en una matriz de 5 x 5 y cada uno de los cuadrantes tendrá asignado un nivel de riesgo inherente de acuerdo con el resultado obtenido.

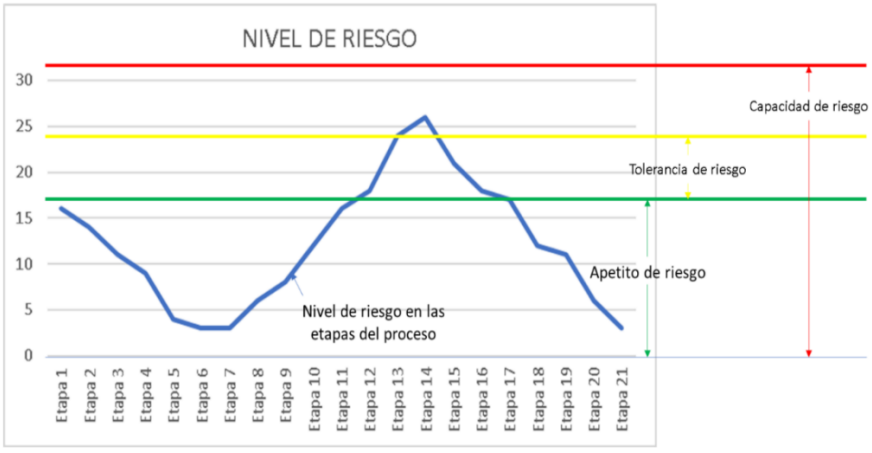
Apetito de Riesgo

El Apetito de Riesgo es el máximo nivel de riesgo que la Compañía está dispuesta a aceptar para alcanzar sus objetivos. Permite evaluar qué eventos y riesgos son asumibles por la Compañía de acuerdo a su estrategia y cuáles no.

A continuación, se desarrolla conceptualmente este tema, a fin de contar con mayores elementos de juicio para su análisis, iniciando con las siguientes definiciones:

- Tolerancia del riesgo: es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del apetito de riesgo determinado por la entidad.
- Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

Gráficamente los anteriores conceptos se relacionan así:



Fuente: Tomado de la Guía de buenas prácticas de gestión de riesgos del Instituto de Auditores Internos (IIA GLOBAL), junio de 2013.

Apetito de riesgo	
Bajo	La empresa determina los riesgos que no son tolerables.
Moderado	La empresa acepta la probabilidad de que se materialicen determinados riesgos.
Alto	La empresa está dispuesta a asumir riesgos que podrían tener un impacto significativo en el negocio.

Declaración de Apetito de Riesgo

La compañía está expuesta a diversos riesgos, por ello se cuenta con una matriz de riesgos donde se prioriza y trata aquellos que de materializarse pueden tener impacto significativo en el rendimiento anual de la empresa. Así mismo, **existen riesgos originados por variables externas, las cuales no son controlables por la empresa.**
La reputación y los colaboradores son nuestros principales pilares, razón por la cual nuestro **apetito de riesgo es bajo ante cualquier evento o situación que pueda afectarlos.**
Mantenemos un **bajo apetito al riesgo** respecto a aquellos riesgos relacionados a **gestión de operaciones, gestión de cumplimiento y gestión de ciberseguridad.** Dentro de la gestión de cumplimiento se encuentran la regulación y normas aplicables al negocio, así como la salud, seguridad y medio ambiente. Evaluamos los costos y beneficios para definir distintas estrategias de respuesta al riesgo, seleccionando aquella cuyo riesgo residual sea menor.
Tomamos decisiones alineadas a nuestros valores, siempre priorizando la calidad de los productos y los servicios que ofrecemos. Estas decisiones consideran la sostenibilidad y el crecimiento de las operaciones. Aceptamos un **apetito de riesgo moderado para el contexto de negocio, la gestión comercial y para el desarrollo de productos y servicios innovadores enfocados en generar mayor**

Nivel de Riesgo Residual

Para llegar a establecer una calificación del impacto y la probabilidad del riesgo con control, es importante considerar en cuanto disminuye la probabilidad o el impacto de acuerdo con la efectividad del control asignado. A partir de esta evaluación el responsable o dueño del proceso debe establecer la calificación del control en la matriz, que le permite determinar el nuevo grado de exposición al riesgo denominado riesgo residual.

El cálculo del valor del riesgo residual se realiza de la siguiente manera:

$$Promedio\ ponderado\ de\ probabilidad = (Peso\ C1 \times Ponderación\ C1\ \times Valoración\ C1) + (Peso\ C2 \times Ponderación\ C2\ \times Valoración\ C2) + \cdots$$

$$Promedio\ ponderado\ de\ impacto = (Peso\ C1 \times Ponderación\ C1\ \times Valoración\ C1) + (Peso\ C2 \times Ponderación\ C2\ \times Valoración\ C2) + \cdots$$

Donde:

Peso Cn = Valor de mitigación de probabilidad / impacto del control.
Ponderación Cn = % de gestión del riesgo del control con respecto al conjunto de controles
Valoración Cn = Resultado de la efectividad del control determinada por los siguientes valores numéricos:

Valoración del control	Equivalente
Efectivo	**1**
Inefectivo	**0**

$Riesgo\ residual\ probabilidad =$ Probabilidad inherente – Promedio ponderado de probabilidad

$Riesgo\ residual\ impacto =$ Impacto inherente – Promedio ponderado de impacto

3 Tratamiento de Riesgos

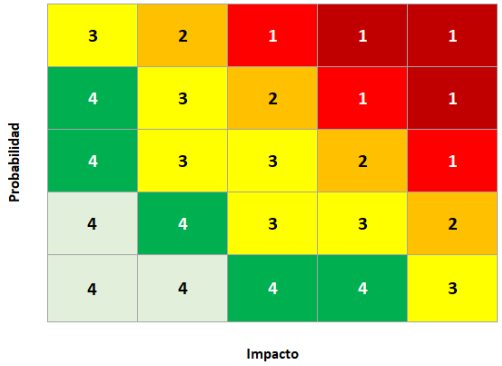
De acuerdo con los resultados obtenidos en los mapas de riesgos estratégicos y de proceso, el responsable o dueño de proceso debe aplicar medidas de tratamiento, para controlar los riesgos según el nivel deseado en línea con el apetito de riesgo. Estas son:

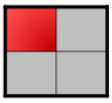
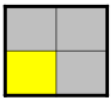
- **Evitar:** No realizar la actividad que tiene la probabilidad de generar el riesgo. Por lo general, implica rediseñar el plan operativo o de negocios.
- **Aceptar:** Es asumir totalmente el riesgo, para ello se debe establecer plan para financiar el tratamiento, aceptar la pérdida residual y elaborar los planes de contingencia para su manejo. Así mismo, efectuar un monitoreo del mismo.
- **Reducir:** Reducir o controlar la probabilidad de ocurrencia mediante la aplicación de medidas con el fin de disminuir tanto la probabilidad como el impacto, tales como:

  - Establecer controles para disminuir la probabilidad de ocurrencia del riesgo y/o el impacto financiero del riesgo.
  - Realizar auditorías o programas de verificación de cumplimiento
  - Implementar cambios en las condiciones contractuales
  - Ajustar especificaciones de productos o servicio
  - Aseguramiento de Calidad, gestión y normalización
  - Investigación y desarrollo tecnológico

- **Transferir:** Reducir su efecto a través del traspaso de las pérdidas a un tercero, cuya capacidad financiera o nivel de especialización en cierta materia le permita administrar razonablemente el riesgo o enfrentar las pérdidas originadas ante la ocurrencia del riesgo. Ejemplos, como en el caso de los contratos de seguros o a través de otros medios que permiten distribuir una porción del riesgo con otra Organización o Contratos de riesgo compartido.

Se deberá evaluar los costos y beneficios de las distintas estrategias de respuesta, y seleccionará aquella que esté alineada con el Apetito de Riesgo de la Compañía. Así mismo, de acuerdo con la siguiente ubicación del riesgo residual en la matriz se determinan las siguientes estrategias de tratamiento:



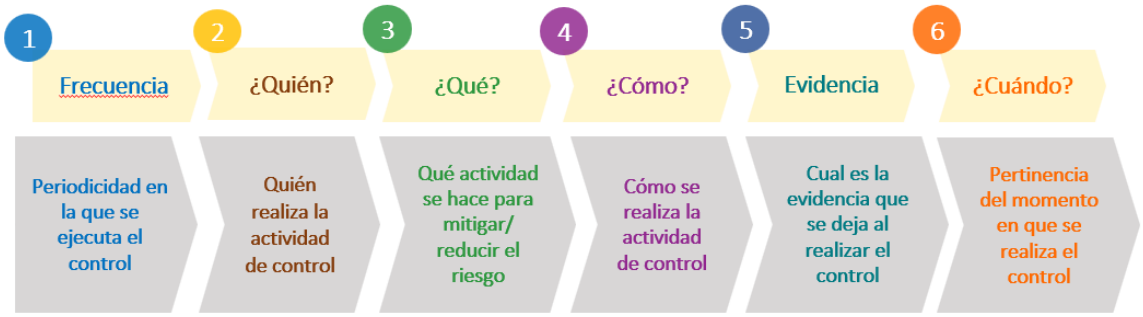
Estrategia de tratamiento	Descripción	Gestión Gerencial
1. Mejora 	Alta exposición inherente con bajos niveles de control conforman las prioridades para las actividades de mejora.	Dar prioridad para identificar e implementar planes de mejora inmediatos o de corto plazo.
2. Monitoreo de Controles 	Áreas de alto riesgo inherente donde los controles son afirmados como adecuados por la gestión.	Enfocarse en el monitoreo continuo de las actividades del control asegurando que estén funcionando conforme a su diseño.
3. Monitoreo de Riesgos 	Riesgos con una exposición inherente baja que también cuentan con un bajo nivel de control.	Pueden ser aceptados conscientemente por la alta gerencia pero el nivel de riesgo debe seguir siendo monitoreado para responder a incrementos en la exposición al riesgo.
4. Aceptar 	Áreas de baja exposición inherente con alto nivel de control.	Son conscientemente aceptados por la compañía y en algunas ocasiones pueden generar oportunidades para aumentar la efectividad de los procesos y controles.

4 Evaluación de controles

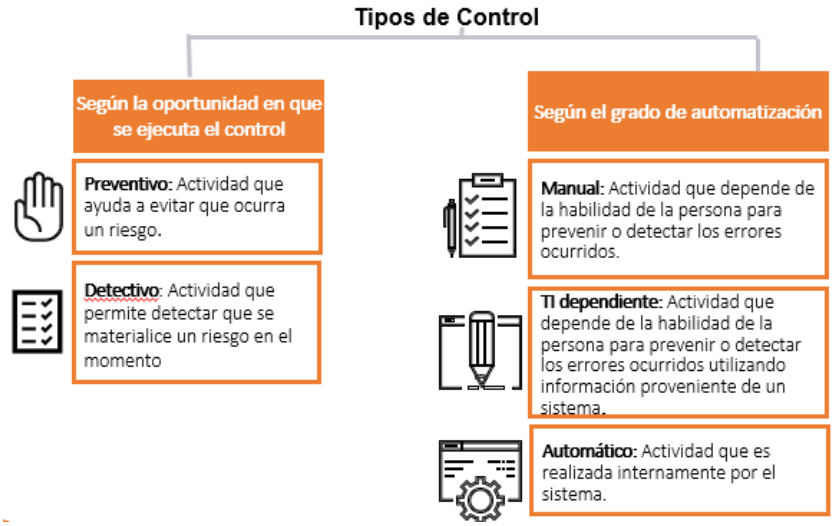
Los controles son actividades diseñadas para mitigar o reducir el impacto o probabilidad de ocurrencia de los riesgos. Se orientan a proveer un nivel razonable de aseguramiento del cumplimiento de los objetivos. Es importante considerar que:

- El despliegue de políticas permite definir lo que se espera de un adecuado funcionamiento del proceso ya que establecen los estándares del control interno
- Los procedimientos permiten llevar las políticas a la práctica
- La sola existencia de una política no es un control

El diseño de los controles debe cumplir con los siguientes **atributos**:



Para la identificación de controles es importante tener en cuenta la siguiente **tipología del control:**



La evaluación de controles se realizará mediante la ejecución de recorridos y pruebas de controles. Según la naturaleza del control, existen los siguientes métodos no excluyentes de prueba a aplicar durante la ejecución del recorrido de controles.

- **Observación**: Consiste en la verificación presencial de la ejecución del control.
- **Trazabilidad**: Consiste en la revisión de documentación de sustento o registros del sistema que permitan concluir sobre la ejecución del control en el caso de la operación seleccionada.
- **Re-cálculo**: Consiste en verificar la correcta ejecución del control mediante el recalculo de ciertos resultados o registros generados como output del mismo control.
- **Re-ejecución:** Consiste en repetir la ejecución de los procedimientos de control para validar que el resultado obtenido evidencia que éste fue ejecutado adecuadamente.

En caso sea necesario revisar la documentación generada como parte de la actividad de control, esta información se solicitará al Dueño del Proceso.

Evaluación del diseño

La evaluación de la efectividad del diseño de un control se realizará verificando la idoneidad de su definición y la presencia de los atributos establecidos, así como su capacidad para mitigar el riesgo para el cual fue diseñado. Un control podrá considerarse efectivo en diseño aun cuando presente oportunidades de mejora en algún atributo, siempre que cumpla su propósito de mitigación.

Las variables de peso y ponderación del control serán definidas por el asesor de riesgos en coordinación con el dueño del proceso/área.

Evaluación de la efectividad operativa

La evaluación de efectividad de operación de un control se realizará durante las pruebas de controles y permitirá concluir sobre su efectividad operativa.

A diferencia de la evaluación de efectividad de diseño, la evaluación de efectividad de operación busca determinar si el control mitiga el riesgo para el cual fue diseñado y si se ejecutó correctamente en los casos de prueba.

Selección de la Muestra

El tamaño de la muestra de controles a probar se seleccionará tomando en consideración los siguientes criterios:

- **Naturaleza:** Determina si el control es ejecutado manualmente o de manera automática por un sistema de soporte.
- **Frecuencia del control:** Determina la periodicidad con la que se ejecuta el control.

Naturaleza del control	Frecuencia del Control	Tamaño de la muestra
Manual	Varias veces por día	4
Manual	Diario	3
Manual	Diario o más que diario	3 o 4
Manual	Semanal	2
Manual	Mensual	1
Manual	Trimestral	1

Naturaleza del control	Frecuencia del Control	Tamaño de la muestra
Manual	Anual	1
Automático	-	1

* Esta tabla constituye el mínimo requerido para evaluar la eficacia operativa del control; no obstante, el asesor de riesgos podrá ampliarla según su criterio técnico.

La prueba de eficacia operativa debe ser documentada de forma tal que permita a un tercero, ajeno al proceso llegue a los mismos resultados que el evaluador. Para lo cual el evaluador podrá utilizar el anexo 1. Formato Prueba de Control.

La combinación de la evaluación del diseño y la eficacia operativa permite establecer la medida de solidez del control. Así:

Diseño	Operación	Solidez del control
Efectivo	Efectivo	Efectivo
Efectivo	Inefectivo	Inefectivo
Inefectivo	N/A	Inefectivo

5 Desarrollo de Planes de Acción

Los planes de acción se establecen como resultado de la identificación de oportunidades de mejora relacionadas con las deficiencias existentes en los procesos o controles. Su propósito es fortalecer los controles/ procesos existentes o en algunos casos crear nuevos controles. Los planes deben incluir:

- Descripción de la oportunidad de mejora identificada.
- Actividades a realizarse para la implementación del plan.
- Responsables para la implementación del plan.
- Requerimiento para la implementación del plan.
- Fecha de inicio y fecha límite de implementación.
- Frecuencia para realizar seguimiento del avance.

Los planes de acción deben ser validados con el responsable de la Gerencia de Riesgos y Cumplimiento.

Los planes de acción se clasifican en las siguientes categorías:

- **Implementación de control**: Se refiere al diseño o rediseño e implementación de actividades de control.

- **Diseño del proceso**: Relacionadas al diseño e implementación de procesos.
- **Automatización**: Se refiere a la implementación de actividades que serán ejecutadas por los sistemas de información o por otros sistemas tecnológicos.
- **Segregación de funciones**: Son aquellas que se encuentran relacionadas a la asignación de responsabilidades.

6 Reportes y Comunicación de resultados

Reporte de Eventos de Riesgo

Permite conocer los eventos de riesgo ocurridos en la compañía a partir de la información recibida por parte de los colaboradores, quienes están en la obligación de reportar los eventos de riesgo de los que tengan conocimiento.

Sus objetivos principales son:

- Establecer una base de datos histórica de los eventos de riesgos de la Compañía.
- Validar y controlar la gestión del riesgo en cada uno de los procesos.
- Identificar todos los posibles eventos que amenazan el logro de los objetivos en cada proceso
- Evaluar su probabilidad e impacto, a través de una base de datos histórica.
- Analizar de forma cualitativa y cuantitativa los eventos de riesgo materializados.

Los siguientes lineamientos son considerados en el proceso de reporte de eventos de riesgos:

- La base de información que contiene los registros de eventos estará sujeta a la aplicación integral de las políticas relacionadas con seguridad de la información aprobada por la Compañía.
- Coordinar la capacitación requerida para efectuar el registro de eventos de riesgo y manejo de los mismos.
- Los colaboradores dispondrán del registro de los eventos de riesgo en la herramienta definida por la Compañía.
- La Gerencia de Riesgos y Cumplimiento promueve la cultura de reporte y dará seguimiento a los eventos informados.

Para realizar el registro de eventos se deberán tener en cuenta. Lo establecido en el Anexo 2 Guía de Reporte de Eventos de Riesgo.

Comunicación de Resultados

Los reportes permiten informar a todos los interesados sobre los riesgos más relevantes del proceso y las estrategias de respuesta al riesgo que la Compañía ha adoptado. En dichos reportes informa al:

- **Dueño del proceso**: El detalle de los riesgos identificados, nivel de riesgo, efectividad de la gestión de riesgos, oportunidades de mejora, rediseño de procesos y controles y planes de acción establecidos de sus procesos a cargo. Esto incluye la entrega de la matriz de riesgos y controles.
- **Presidente**: El resumen de los niveles de riesgos importantes, oportunidades de mejora y planes de acción establecidos de los procesos evaluados. Así mismo, se presentan los planes de acción que por su alcance requiere la aprobación de su implementación.
- **Comité de riesgos.** Se reportará los riesgos residuales altos y muy altos, el estado de la de evaluación de los procesos, nivel de aseguramiento resultante y valor agregado generado.

7 Monitoreo

La Gerencia de Riesgos y Cumplimiento examinará el desempeño de la compañía, determina cómo funcionan los componentes de gestión del riesgo empresarial con el paso del tiempo en un entorno de cambios sustanciales, y como resultado identifica qué aspectos son susceptibles de revisar y modificar.

Así mismo, anualmente evaluará la eficacia de los controles críticos de los procesos y cada 3 años actualizará la matriz de riesgos de los procesos críticos. Así mismo, realizará monitoreo de los indicadores de desempeño relevantes.

El dueño del proceso efectuara el monitoreo de la gestión de riesgos a través de la autoevaluación de controles e indicadores de desempeño.

Key Risk Indicator (KRI)

Los indicadores son las medidas que permitirán a cada uno de los negocios y los entes de control monitorear el comportamiento de los riesgos para definir planes de acción, por lo anterior el dueño de proceso debe gestionar indicadores. Los indicadores deben tener establecido una meta deseada, que permita la generación de alertas e identificar cuando se requiere diseñar un plan de acción para revisar las actividades del proceso o la ejecución de los controles.

Cada dueño del proceso será responsable de registrar y conservar la información documentada de sus indicadores y en caso de ser solicitado por la Gerencia de Riesgos y Cumplimiento deberán reportar los registros correspondientes.

Los KRIs formulados deben considerar las siguientes características:

- **Relevantes:** Se enfocan en los riesgos significativos y deben ser relevantes para lo que está monitoreando.

- **No redundantes:** Evitar tener indicadores repetidos o correlacionados
- **Medibles:** Deben ser objetivos, cuantificables y verificables
- **Predictivo / Preventivo:** Pueden ser utilizados para obtener una perspectiva de los riesgos emergentes. La capacidad del indicador para predecir y proporcionar una indicación temprana sobre la tendencia y pérdidas potenciales es clave.
- **De fácil monitoreo:** Los datos utilizados deben ser simples y sencillos de recolectar. Deben permitir una fácil interpretación, comprensión, supervisión y control**.**
- **Auditables:** Los datos utilizados para la medición deben ser sólidos y el proceso debe ser repetible para las auditorías internas o externas a fin de evaluar la exactitud y consistencia.

ANEXOS

Anexo 1. Formato de prueba de control

Anexo 2. Guía Reporte de Eventos de Riesgos