



## **MANUAL DE GESTIÓN DE RIESGOS**

### **VICEPRESIDENCIA DE ESTRATEGIA**

**Versión 2.0**

**Septiembre de 2017**

©Derechos Reservados: ISA - 18/09/17

Se prohíbe la reproducción total o parcial de este documento sin autorización previa escrita.



## MANUAL DE GESTIÓN DE RIESGOS

### Contenido

1.	OBJETIVO .....	2
2.	INTRODUCCIÓN .....	2
3.	ALCANCE .....	3
4.	CONCEPTOS .....	5
4.1.	¿QUÉ ES UN RIESGO?.....	5
4.2.	¿QUÉ ES GESTIÓN INTEGRAL DE RIESGOS?.....	5
4.3.	¿QUE SON RECURSOS EMPRESARIALES?.....	5
4.4.	¿QUIÉN ES EL RESPONSABLE DE GESTIONAR LOS RIESGOS?.....	5
4.5.	¿QUÉ SE CONSIDERA UNA CAUSA DE UN EVENTO DE RIESGO? .....	6
4.6.	¿QUÉ SE CONSIDERA UNA CONSECUENCIA DE UN EVENTO DE RIESGO?..	6
4.7.	¿QUÉ SON LAS MEDIDAS DE ADMINISTRACIÓN ACTUALES?.....	6
4.8.	¿QUÉ SON LAS MEDIDAS DE ADMINISTRACIÓN POTENCIALES?.....	6
4.9.	¿QUÉ ES LA PROBABILIDAD? .....	6
4.10.	¿QUÉ ES LA SEVERIDAD?.....	6
4.11.	¿QUÉ ES EL NIVEL DE RIESGO? .....	6
4.12.	¿QUÉ ES UNA ESCALA DE PROBABILIDAD Y SEVERIDAD? .....	7
4.13.	¿CUÁLES SON LOS NIVELES DE ACEPTABILIDAD? .....	7
5.	METODOLOGÍA DE GESTIÓN INTEGRAL DE RIESGO DE ISA Y SUS EMPRESAS.....	7
5.1.	ESTABLECER EL CONTEXTO.....	8
5.2.	IDENTIFICAR LOS RIESGOS .....	9
5.3.	ANALIZAR LOS RIESGOS .....	11
5.4.	EVALUAR LOS RIESGOS .....	12
5.5.	TRATAR LOS RIESGOS.....	12

5.6.	MONITOREAR Y REVISAR .....	14
5.7.	COMUNICAR Y CONSULTAR .....	15
5.8.	EJEMPLO DE UNA BUENA DEFINICIÓN DE UN RIESGO .....	16
6.	MEJORAMIENTO CONTINUO.....	16
7.	GESTIÓN DEL CAMBIO .....	17
8.	ESCALAS Y NIVELES DE LOS RIESGOS .....	17
9.	GOBIERNO DE LA GESTIÓN INTEGRAL DE RIESGOS .....	19
9.1.	RACI DE ISA.....	20
9.2.	RACI DE LAS FILIALES.....	21
9.3.	REPORTE Y FLUJO DE INFORMACIÓN DE LOS REGISTROS DE RIESGOS...	21
10.	ANEXOS .....	24

## **1. OBJETIVO**

Presentar la metodología del modelo de gestión integral de riesgos en el Grupo ISA y dar claridad sobre los conceptos que las buenas prácticas sugieren y establecen para gestionar los riesgos en la organización, buscando garantizar un modelo de gestión eficiente para la administración de los mismos.

Este manual aplica a todas las empresas del grupo empresarial y contiene las directrices y líneas de actuación necesarias para gestionar los riesgos a los que nos encontramos expuestos.

## **2. INTRODUCCIÓN**

En ISA y sus empresas la gestión integral de riesgos soporta las decisiones estratégicas, es transversal y de gran importancia para la organización ya que tiene el fin de proteger y preservar la integridad de los recursos y el logro de los objetivos.

En el actuar de la organización guiado por el marco de referencia y durante el desarrollo normal de las operaciones, se monitorean de manera sistemática las expectativas de los grupos de interés y los riesgos del entorno, con el fin de mantener coherencia en el logro de la estrategia y asegurar la sostenibilidad empresarial.

En este sentido, ISA se compromete de manera responsable, transparente y ética a gestionar los riesgos y las oportunidades; con el fin de crear valor para sus grupos de interés, mantener su ventaja competitiva y contribuir al desarrollo de las sociedades donde tiene presencia.

Estamos expuestos permanentemente a riesgos que pueden desviarnos de lo que hemos logrado y la consecución de la estrategia, de allí la necesidad de garantizar una gestión integral de los riesgos que permita mantener la integridad de los recursos empresariales, la

continuidad y sostenibilidad de los negocios. Para el logro de esto, debemos promover el compromiso hacia una activa y oportuna identificación de los riesgos, una efectividad en la ejecución de las medidas administración, al igual que un continuo seguimiento en cada una de las actividades que desarrollamos, esto teniendo en cuenta que la gestión de los riesgos es responsabilidad de todos los colaboradores del grupo ISA.

#### **POLÍTICA DE GESTIÓN INTEGRAL DE RIESGOS:**

##### **Propósito:**

Proteger y preservar la integridad de los recursos empresariales, la continuidad y sostenibilidad de los negocios a través de la gestión permanente de los riesgos a los cuales se encuentran expuestas ISA y sus empresas.

##### **Principios:**

- Consideramos riesgo todo evento incierto, que en caso de ocurrir, puede desviarnos del logro de los objetivos o afectar los recursos empresariales.
- Soportamos nuestras decisiones estratégicas en los resultados de la gestión de riesgos; la cual consideramos transversal y de interés prioritario para nuestras empresas.
- Implementamos de manera permanente, homologada y sistemática el ciclo de la gestión integral de riesgos, de acuerdo con las mejores prácticas y metodologías.

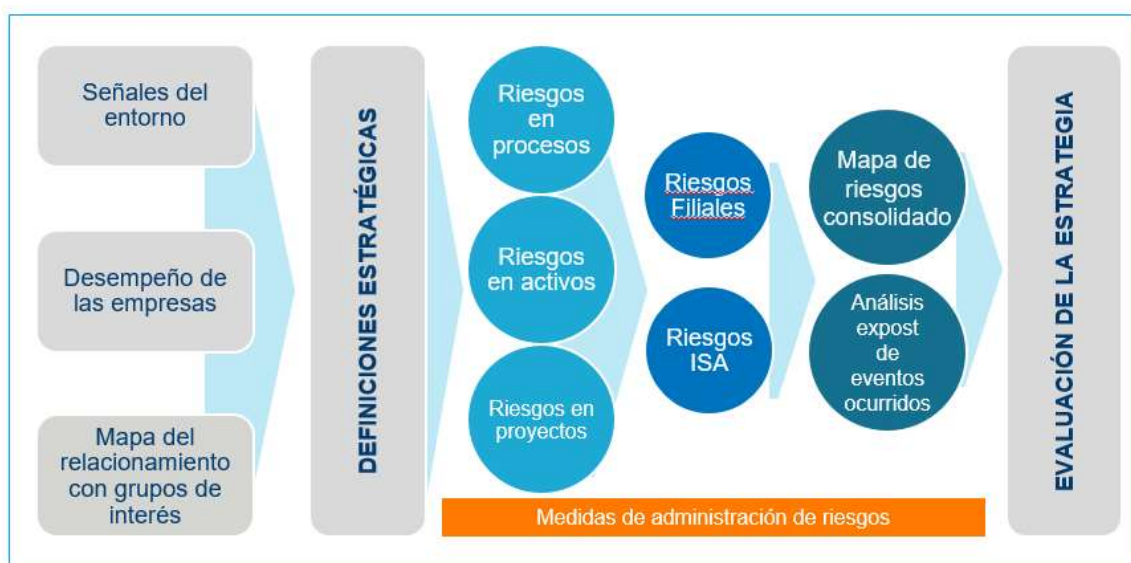
Promovemos el compromiso individual de nuestros trabajadores con una activa identificación, valoración, tratamiento, seguimiento y comunicación de los riesgos en el desarrollo de sus actividades.

### **3. ALCANCE**

Este manual aplica para la gestión integral de riesgos estratégicos de procesos, activos y proyectos de ISA y todas sus empresas. La gestión de riesgos es responsabilidad de todas las personas del Grupo ISA, en sus actividades del día a día, como en el relacionamiento con los grupos de interés y la incorporación de las señales del entorno frente a las situaciones que pueden desviar el logro de los objetivos empresariales y afectar los recursos estratégicos de la misma.

La metodología de gestión integral de riesgos planteada en este manual aplica a todas las etapas del ciclo de vida de los activos (estructuración de ofertas, ingeniería, construcción y montaje, operación, mantenimiento y disposición final), incluyendo los procesos habilitadores (por ejemplo: selección de personal, formación, gestión de la información, gestión legal, financiero, etc).

En el gráfico que aparece a continuación, se puede visualizar cómo la gestión integral de riesgos se encuentra vinculada directamente con las conversaciones estratégicas. En dichas instancias se monitorean las señales del entorno (oportunidades y amenazas), el desempeño de las empresas (fortalezas y debilidades) y las expectativas de los grupos de interés. De este análisis, surgen decisiones sobre el futuro de las empresas que permitan aprovechar oportunidades y gestionar los riesgos identificados. Dichas decisiones son documentadas en iniciativas, indicadores y planes de trabajo con el fin de asegurar su adecuada implementación y seguimiento.



Esta metodología incluye dentro de su alcance la gestión de los riesgos en el corto, mediano y largo plazo (emergentes). El análisis de los riesgos emergentes incorpora la mirada del entorno en el largo plazo y permite anticiparse a las amenazas relacionadas con las tendencias para convertirlas en oportunidades identificadas desde el análisis que se hace del entorno.

## 4. CONCEPTOS

### 4.1. ¿QUÉ ES UN RIESGO?

Riesgo es todo **evento incierto** que pueda **desviar del logro de los objetivos** estratégicos de la compañía y/o **afectar los recursos empresariales** que para el grupo ISA son financiero y reputación.

### 4.2. ¿QUÉ ES GESTIÓN INTEGRAL DE RIESGOS?

La Gestión Integral de Riesgos (GIR) es la implementación homologada y sistemática de un conjunto de acciones tendientes a identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos.

### 4.3. ¿QUE SON RECURSOS EMPRESARIALES?

Son activos fundamentales con los que cuentan las empresas para cumplir con sus objetivos, los cuales deben ser protegidos mediante la gestión integral de riesgos.

Los recursos fundamentales definidos para el grupo ISA son:

- Financiero: activos de la empresa, recursos aportados por terceros y patrimonio de los accionistas.
- Reputación: supuestos, percepciones y creencias de los públicos clave.

Para la gestión de riesgos en las filiales operativas y en activos, se podrá tener en cuenta el recurso humano, el cual hace referencia a los trabajadores, contratistas y terceros.

### 4.4. ¿QUIÉN ES EL RESPONSABLE DE GESTIONAR LOS RIESGOS?

Todos los colaboradores de la organización son responsables de la gestión integral de riesgos, sin embargo, los dueños del proceso y proyectos son responsables del registro y seguimiento de la gestión de riesgos.

#### 4.5. ¿QUÉ SE CONSIDERA UNA CAUSA DE UN EVENTO DE RIESGO?

Es la descripción de una situación que puede dar origen a un evento de riesgo.

#### 4.6. ¿QUÉ SE CONSIDERA UNA CONSECUENCIA DE UN EVENTO DE RIESGO?

Es la descripción de los impactos generados ante la materialización de un riesgo.

#### 4.7. ¿QUÉ SON LAS MEDIDAS DE ADMINISTRACIÓN ACTUALES?

Como su nombre lo dice son medidas que se están ejecutando en la actualidad y se clasifican en:

- Medidas de administración de **prevención actuales**: Acciones que se están haciendo actualmente y permiten disminuir las causas de los riesgos.
- Medidas de administración de **protección actuales**: Acciones que se ejecutan una vez el riesgo se materializó y disminuyen la severidad de los riesgos.

#### 4.8. ¿QUÉ SON LAS MEDIDAS DE ADMINISTRACIÓN POTENCIALES?

Son las que se definen cuando las medidas de administración actuales no permitan disminuir la probabilidad y/o severidad del riesgo actual y también se clasifican en medidas de prevención y de protección.

#### 4.9. ¿QUÉ ES LA PROBABILIDAD?

Es una medida de certidumbre asociada a un evento futuro y suele expresarse como un número entre 0% y 100%. Hace referencia al nivel de posibilidad de que algo suceda.

#### 4.10. ¿QUÉ ES LA SEVERIDAD?

Impacto que se puede generar con el riesgo y suele expresarse como un valor de afectación financiera o reputacional, para esta última se tiene una escala descriptiva.

#### 4.11. ¿QUÉ ES EL NIVEL DE RIESGO?

Es el resultado de multiplicar la probabilidad por la severidad.



#### 4.12. ¿QUÉ ES UNA ESCALA DE PROBABILIDAD Y SEVERIDAD?

Es una representación numérica de una variable a medir, para este caso usamos escalas para la probabilidad y para la severidad en el recurso reputación y en los proyectos para la variable tiempo.

#### 4.13. ¿CUÁLES SON LOS NIVELES DE ACEPTABILIDAD?

Criterios definidos por la Junta Directiva en función del apetito, la tolerancia y la capacidad del riesgo. Establecen una posición y responsabilidad frente al nivel de riesgo.

### 5. METODOLOGÍA DE GESTIÓN INTEGRAL DE RIESGO DE ISA Y SUS EMPRESAS

La metodología aplicada por ISA y sus empresas en la gestión integral de riesgos se basa en la Norma ISO 31000, en la cual se pueden identificar las siguientes etapas.



## 5.1. ESTABLECER EL CONTEXTO

La gestión integral de riesgos en ISA incluye los riesgos para activos, procesos, proyectos y objetivos estratégicos, y por esto es importante que en el contexto se identifique sobre qué asunto se hará gestión.

El contexto hace referencia a la información inicial que se requiere tanto interna como externa para identificar adecuadamente los riesgos que podrían materializarse a corto o largo plazo, es decir, para un análisis de riesgos es fundamental entender cuáles son los objetivos del proceso o del proyecto, el entorno que rodea el negocio y los criterios con los cuales se realizará la evaluación de los mismos.

### CONTEXTO EXTERNO

Es el ambiente externo en el cual la organización busca alcanzar sus objetivos estratégicos. Para entenderlo se hace una revisión de las características y percepciones de los grupos de interés, así como un análisis de los competidores, del entorno político, económico (características del sector, tendencias macroeconómicas, etc.), social, tecnológico, ambiental y normativo (tributario y regulatorio).

Adicionalmente, para los proyectos se incluye una revisión de las características de los documentos de selección del inversionista, bases de licitación, pliegos de la convocatoria o documentos equivalentes.

### CONTEXTO INTERNO

Es el ambiente Interno en el cual la organización busca alcanzar sus objetivos estratégicos. Este contexto incluye todo aquello dentro de la organización que pueda tener influencia en la forma en que son gestionados los riesgos, por ejemplo: gobierno, estructura, roles y responsabilidades, políticas, objetivos, sistemas de gestión y de información, capacidades, cultura, entre otros. Adicionalmente, se tiene en cuenta el desempeño de los procesos, proyectos y activos, como por ejemplo los hallazgos de las auditorías internas, los cuales podrían servir de insumo importante para la identificación y análisis de los riesgos.

## 5.2. IDENTIFICAR LOS RIESGOS

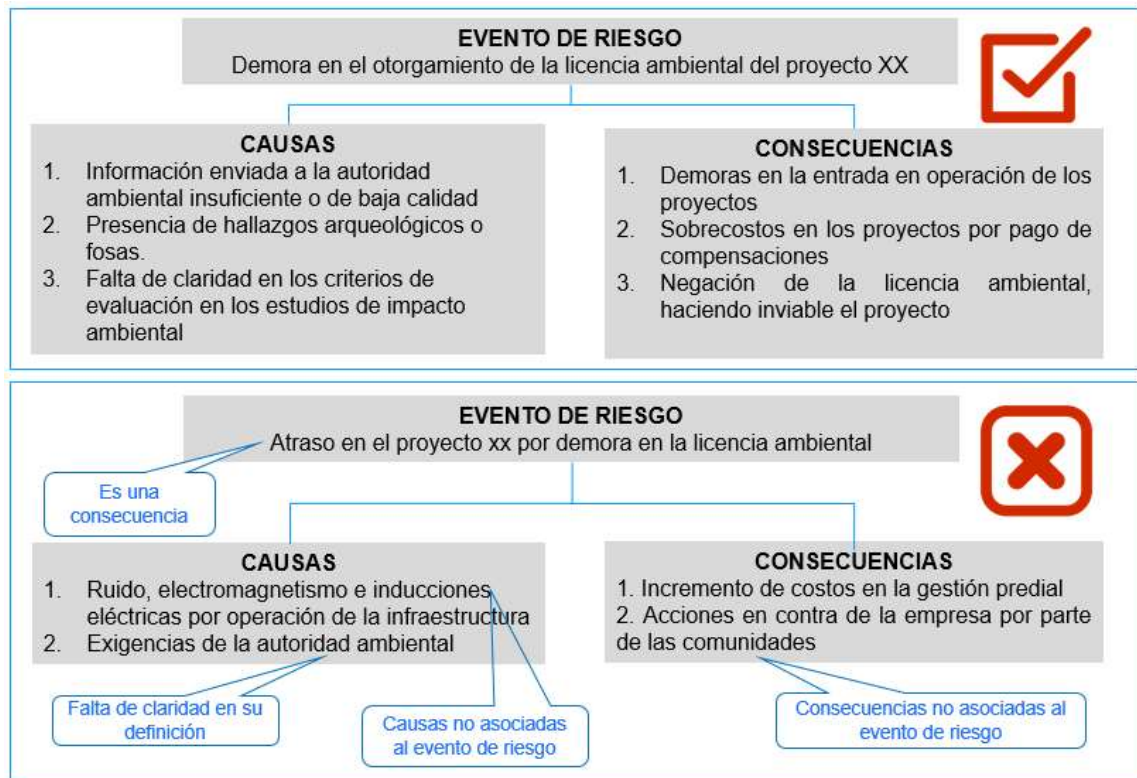
Proceso de encontrar, reconocer y describir los riesgos. Al hacer la descripción del riesgo, se deben tener en cuenta las siguientes recomendaciones:

- La redacción deberá ser en un lenguaje común y comprensible para toda la compañía.
- La descripción debe tener presente las siguientes características:
  - Que sea un evento incierto
  - Que pueda desviar del logro de los objetivos estratégicos, del proceso, de los activos o de los proyectos y que puede afectar los recursos empresariales.

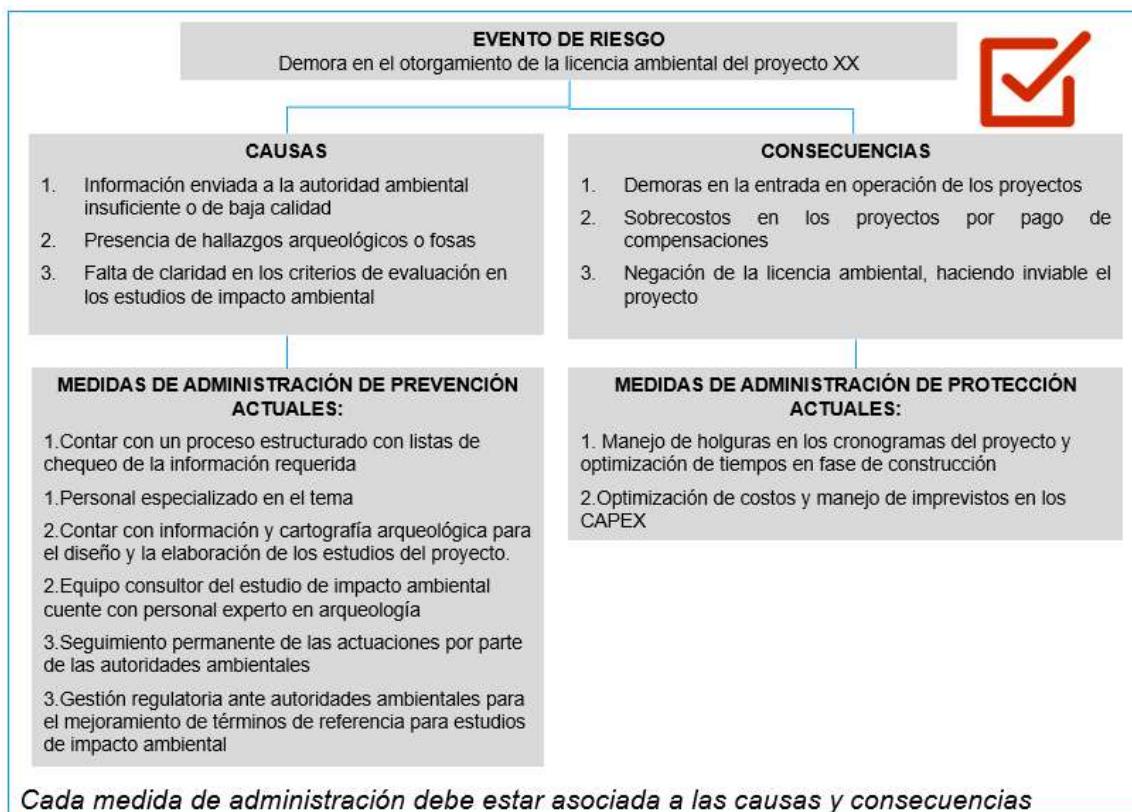
En esta etapa se diligencia en el formato de registro de riesgos la siguiente información:

- Descripción del **evento de riesgo**
- Las causas y medidas de administración de prevención actuales.
- Las consecuencias y medidas de administración de protección actuales.

A continuación, un ejemplo de la identificación de las causas y consecuencias de los riesgos:



Ejemplo de identificación de las medidas de administración de prevención y protección actuales:



### 5.3. ANALIZAR LOS RIESGOS

En esta etapa se hace la definición de la **probabilidad** del riesgo de acuerdo a las causas definidas y la definición de la **severidad** de acuerdo a las consecuencias identificadas. Posteriormente, se calcula el **nivel de riesgo**.

Para la cuantificación del riesgo es importante responder a preguntas como: ¿Cuál es la probabilidad de que el evento suceda?, ¿De cuánto es la pérdida si el riesgo se materializa?

La definición de la probabilidad y severidad se puede hacer mediante información histórica, datos reales, simulaciones, juicio de expertos y/o referenciamiento (para mayor información ver Norma ISO 31010). Es importante que una vez se haya identificado cual es la probabilidad y la severidad del riesgo, queden bien documentadas en el formato de registro de riesgos, en el campo denominado “descripción de la valoración”, explicando cuáles fueron los supuestos realizados, las hipótesis planteadas y las herramientas o técnicas utilizadas.

#### 5.4. EVALUAR LOS RIESGOS

Es el proceso de comparación de los resultados del nivel de riesgo calculado en la etapa anterior con los niveles de escalamiento en el recurso financiero y reputación definido para ISA y sus empresas. Como resultado de esta comparación, se da una clasificación de riesgos en cuatro colores: rojo, naranja, amarillo y verde.

En esta etapa se toma la decisión de qué se hará con el riesgo dependiendo de su color y de los niveles de aceptabilidad definidos por cada empresa, es decir, aquí se define cuáles riesgos requieren tratamiento y cuál es la prioridad que se les debe dar.

Para los proyectos se evalúa la severidad en costos, reputación y tiempo.

#### 5.5. TRATAR LOS RIESGOS

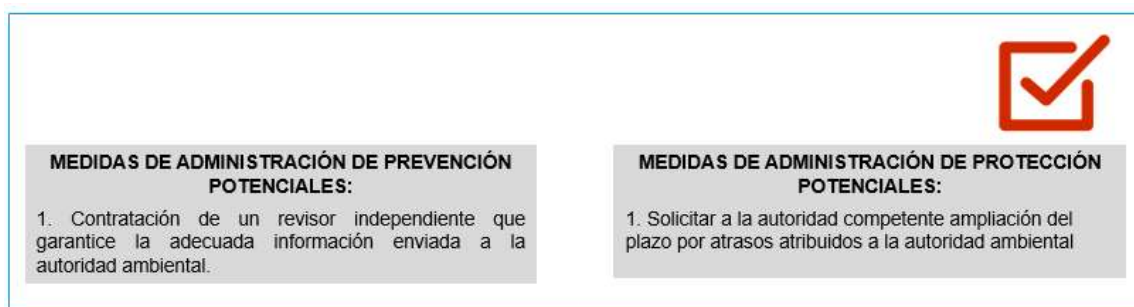
En esta etapa de tratamiento de los riesgos, quien hace la gestión de riesgos deberá definir qué hacer entre las siguientes alternativas:

- No hacer nada: significa que el riesgo es aceptado
- Evitarlo o eliminarlo: decidir no iniciar o continuar la actividad que lo originó.
- Administrarlo: definir medidas de administración de prevención y protección para disminuir la probabilidad y/o la severidad.

- Transferirlo: compartir el riesgo con una o varias partes

En caso de que las medidas de administración actuales que se han definido en la etapa de identificación no permitan disminuir la probabilidad y/o severidad del riesgo actual, deberá evaluarse la posibilidad de identificar **medidas de administración potenciales tanto de prevención como de protección** y/o evitarlo y/o transferirlo mediante seguros, cláusulas en los contratos, coberturas naturales, etc. En caso de que el riesgo sea aceptado se validará con el nivel correspondiente de acuerdo al escalamiento definido en cada una de las compañías.

A continuación, un ejemplo de medidas de administración potenciales:



MEDIDAS DE ADMINISTRACIÓN DE PREVENCIÓN POTENCIALES:	MEDIDAS DE ADMINISTRACIÓN DE PROTECCIÓN POTENCIALES:
1. Contratación de un revisor independiente que garantice la adecuada información enviada a la autoridad ambiental.	1. Solicitar a la autoridad competente ampliación del plazo por atrasos atribuidos a la autoridad ambiental

Es importante valorar el costo de ejecutar las medidas de administración, esto teniendo en cuenta que, al hacer una comparación con el impacto que se puede llegar a tener en caso de materializarse el riesgo, puede dar una idea de si se justifica hacer la implementación después de hacer un análisis costo beneficio. De allí la importancia de que las medidas que sean definidas sean efectivas.

Las medidas de administración potenciales también deberán quedar en el formato de registro de riesgos, teniendo en cuenta que es la herramienta definida para ISA y sus empresas para registrar, reportar y hacer seguimiento a los riesgos identificados y a las medidas de administración actuales y potenciales. En el formato hay unos campos adicionales que permiten hacer seguimiento a las medidas de administración potenciales, en donde aparece quién es el responsable de cada acción, cuál es el costo de implementar la medida y la fecha de implementación. Adicionalmente, hay unos campos diseñados para

que quede el registro del seguimiento que se hace en los grupos primarios, los cuales deben realizarse como máximo con una periodicidad trimestral.

En algunas ocasiones las medidas de administración que fueron definidas para mitigar los riesgos, pueden llegar a ser iniciativas que hacen parte del plan de desarrollo y/o de los instrumentos de gestión, con impacto en el sistema de compensación variable, por lo cual el seguimiento a la efectividad de las mismas se hará desde la Vicepresidencia de Estrategia.

En las filiales operativas es una buena práctica en la definición de medidas de administración establecer un plan de continuidad del negocio, de contingencia, emergencia y/o crisis para aquellos riesgos de baja probabilidad, pero de alto impacto.

#### 5.6. MONITOREAR Y REVISAR

El autocontrol es el principio fundamental para la gestión de los riesgos y está presente en cada nivel de la empresa. El seguimiento de los riesgos está asociado con los niveles de responsabilidad en la estructura de la organización, pasando por la capa de procesos para llegar a los niveles más altos de las compañías, incluyendo sus juntas directivas. Adicionalmente, la función de auditoría soporta su actuar en los análisis de los riesgos empresariales.

El monitoreo de los riesgos se hace en tres momentos y en tres instancias diferentes (Metodología de las tres líneas de defensa). La primera instancia se encuentra en los procesos quienes se encargan de la ejecución de todo el ciclo de gestión de riesgos, la segunda en el área de riesgos quien se encarga de monitorear la implementación de las prácticas efectivas en gestión de riesgos y finalmente la tercera instancia se encuentra en auditoría, quien se encarga del aseguramiento o verificación efectiva de la gestión integral de riesgos y de sus controles.



## 5.7. COMUNICAR Y CONSULTAR

La comunicación y consulta, está presente en todas las etapas del proceso para la gestión de riesgos y permite:

- Reunir diferentes áreas involucradas en el análisis de los riesgos (causas, consecuencias, medidas de administración y valoración) para lograr un proceso adecuado de toma de decisiones.
- La divulgación y capacitación sobre el modelo de gestión de riesgos.

Conocer la actualización trimestral del perfil de riesgos a los grupos de interés de acuerdo a las siguientes 17 categorías de riesgo. En algunas filiales, pueden ser menos categorías teniendo en cuenta que algunas de ellas pueden no aplicarles.



## 5.8. EJEMPLO DE UNA BUENA DEFINICIÓN DE UN RIESGO

A continuación, se muestra un ejemplo de cómo debe ser una buena definición de un riesgo, de sus causas, consecuencias y medidas de administración.

En la medida de lo posible cada una de las causas debe contar con su medida de administración de prevención y cada consecuencia debe contar con su medida de administración de protección.



## 6. MEJORAMIENTO CONTINUO

Dentro de las acciones definidas para el mejoramiento continuo del modelo de gestión integral de riesgos, se tiene:

- Revisiones periódicas del modelo y de su aplicación.

- Auditorías
- Análisis expost

## ANÁLISIS EXPOST

Ante la materialización de un riesgo, se deberá elaborar un análisis expost con el fin de canalizar las lecciones aprendidas y evitar la repetición del mismo. El responsable de dicho análisis será el área o áreas involucradas en el evento materializado y deberá ser presentado en el nivel correspondiente. Las lecciones aprendidas serán comunicadas a las áreas que las requieran para la toma de decisiones. Después de realizado el análisis expost, debe enviarse al área de riesgos de cada compañía, para verificar que la retroalimentación de este análisis sea incluida en el mapa.

Para la elaboración de este análisis se deberá establecer un contexto, en el cual es necesario definir qué hizo que el riesgo se materializara y qué acciones se llevaron a cabo para evitar que el riesgo se materializara. Se sugiere utilizar herramientas como la línea de tiempo, espina de pescado, 5 por qué, eliminación de causa riesgo. Adicionalmente, se deberá valorar cuál fue la pérdida en términos financieros y reputacionales y finalmente identificar las lecciones aprendidas o de mejoramiento.

## 7. GESTIÓN DEL CAMBIO

Cada vez que se dé un cambio significativo en los procesos y/o proyectos o que se cambie una decisión de alto impacto, se hará un análisis de los riesgos actuales e identificación de los riesgos nuevos que se presentan bajo la misma metodología establecida en este manual. Dicho análisis se deberá comunicar a las áreas interesadas para su seguimiento y ejecución de las medidas de administración definidas.

## 8. ESCALAS Y NIVELES DE LOS RIESGOS

En la imagen que aparece a continuación, se pueden observar las escalas de probabilidad y severidad y los niveles de riesgo definidos para la variable tiempo y los recursos financiero y reputación.

		Escala		Niveles de riesgo (Probabilidad x Severidad)																													
		Probabilidad	Severidad																														
Procesos y Proyectos*	Recurso financiero**	Corresponde a un <b>porcentaje</b> estimado por el dueño del proceso o las áreas encargadas para el caso de proyectos que hace el análisis de riesgos.	Corresponde a un <b>valor en USDM</b> estimado por el dueño del proceso que hace el análisis de riesgos  En proyectos, varía de acuerdo al nivel de inversión así:  <b>Muy crítico:</b> >6% <b>Crítico:</b> Entre 3% y 6% <b>Moderado:</b> Entre 1.5% y 3% <b>Leve:</b> 1.5%																														
	Recurso reputación	<b>Muy alta:</b> >76% <b>Alta:</b> Entre 51% y 75% <b>Baja:</b> Entre 26% y 50% <b>Muy baja:</b> 25%	<table><tr><th></th><th>CREDIBILIDAD</th><th>CONFIANZA</th><th>PÚBLICOS CLAVES</th><th>MEDIOS LOCALES / REGIONALES</th><th>MEDIOS NACIONAL / INTERNACIONAL / REDES SOCIALES</th></tr><tr><td>8 LEVE</td><td>NO</td><td>NO</td><td>NO CONOCEN</td><td>NO</td><td>NO</td></tr><tr><td>13 MODERADO</td><td>SI</td><td>NO</td><td>CONOCEN</td><td>SI AISLADA</td><td>NO</td></tr><tr><td>21 CRITICO</td><td>SI</td><td>SI</td><td>CUESTIONAN</td><td>SI CONTINUA</td><td>SI AISLADA</td></tr><tr><td>34 MUY CRITICO</td><td>SI</td><td>SI</td><td>ACUSAN</td><td>SI CONTINUA</td><td>SI CONTINUA</td></tr></table>		CREDIBILIDAD	CONFIANZA	PÚBLICOS CLAVES	MEDIOS LOCALES / REGIONALES	MEDIOS NACIONAL / INTERNACIONAL / REDES SOCIALES	8 LEVE	NO	NO	NO CONOCEN	NO	NO	13 MODERADO	SI	NO	CONOCEN	SI AISLADA	NO	21 CRITICO	SI	SI	CUESTIONAN	SI CONTINUA	SI AISLADA	34 MUY CRITICO	SI	SI	ACUSAN	SI CONTINUA	SI CONTINUA
	CREDIBILIDAD	CONFIANZA	PÚBLICOS CLAVES	MEDIOS LOCALES / REGIONALES	MEDIOS NACIONAL / INTERNACIONAL / REDES SOCIALES																												
8 LEVE	NO	NO	NO CONOCEN	NO	NO																												
13 MODERADO	SI	NO	CONOCEN	SI AISLADA	NO																												
21 CRITICO	SI	SI	CUESTIONAN	SI CONTINUA	SI AISLADA																												
34 MUY CRITICO	SI	SI	ACUSAN	SI CONTINUA	SI CONTINUA																												
Proyectos*	Tiempo	<b>Muy alta:</b> >76% <b>Alta:</b> Entre 51% y 75% <b>Baja:</b> Entre 26% y 50% <b>Muy baja:</b> 25%	Corresponde a los <b>días</b> de atraso en el proyecto estimados por las áreas técnicas.																														

\* Incluye la estructuración de la oferta y la ejecución de los proyectos \*\* El recurso financiero en proyectos hace referencia a la afectación en los costos.

Cada empresa tiene la responsabilidad de definir sus niveles de aceptabilidad, considerando que no superen los de ISA y sean aprobados por su Junta Directiva, por lo tanto, para el análisis de riesgos de los procesos se deberá utilizar los niveles de aceptabilidad definidos por cada filial. Dichos niveles son revisados cada año y en caso de hacer alguna modificación, deberá ser presentada para su aprobación a la Junta Directiva de cada una de las empresas.

## **9. GOBIERNO DE LA GESTIÓN INTEGRAL DE RIESGOS**

Para garantizar el buen funcionamiento del modelo de gestión integral de riesgo en ISA y sus empresas y lograr una mejor comprensión de los roles en la gestión, se han definido las siguientes responsabilidades:

## 9.1. RACI DE ISA

	<div> <span>R</span> Responsable           <span>A</span> Aprobar           <span>C</span> Consultar           <span>I</span> Informar         </div>			
	Marco de referencia	Contexto- Valoración- Tratamiento- Monitoreo- Comunicación.	Análisis expost	Aseguramiento
Junta Directiva	A	C*	C*	I
Comité Corporativo	C	A	A	I
VP Estrategia - Riesgos	R	C	C	C
Auditoría	I			R
VP (incluye DCC)	C	R	R	C
Direcciones	I	R	R	C
Equipos	I	R	R	C

C\* Conocimiento, seguimiento del riesgo y propuesta de medidas de administración adicionales

**Marco de referencia:** Política y manual de riesgos

**Contexto- Valoración- Tratamiento- Monitoreo- Comunicación:**

- Definir particularidades del entorno de los negocios y geografías
- La valoración incluye identificación, análisis y evaluación de los riesgos (para riesgos verdes, amarillos, naranjas y rojos)
- Monitoreo y revisión, comunicación y consulta

**Análisis expost:** Incluye el análisis de eventos materializados y la incorporación de lecciones aprendidas

**Aseguramiento:** Verificación efectividad de la gestión integral de riesgos y de los controles

## 9.2. RACI DE LAS FILIALES

		R Responsable	A Aprobar	C Consultar	I Informar
	Marco de referencia	Contexto- Valoración- Tratamiento- Monitoreo- Comunicación.	Análisis expost	Aseguramiento	
Junta Directiva ISA	A	I	C*	I	
Junta Filial	A	C*	C*	A	
VPE- Riesgos	R	I*	I	I	
VP (incluye DCC)	C	C	I	I	
Auditoría filial	I			R	
Riesgos filial	I	C	C	C	
Comité de gerencia filial	I	A	A	I	
Dirección filial	I	R	R	C	
Equipos filial	I	R	R	C	

C\* Conocimiento, seguimiento del riesgo y propuesta de medidas de administración adicionales

**Marco de referencia:** Política y manual de riesgos

**Contexto- Valoración- Tratamiento- Monitoreo- Comunicación:**

- Definir particularidades del entorno del negocio y del país
- Valoración incluye identificación, análisis y evaluación de los riesgos (para riesgos verdes, amarillos, naranjas y rojos)
- I\* indica que el equipo de riesgos ISA hace comentarios mediante comunicación interna con el área funcional de ISA, quien consolida y se comunica con la filial
- Monitoreo y revisión, comunicación y consulta

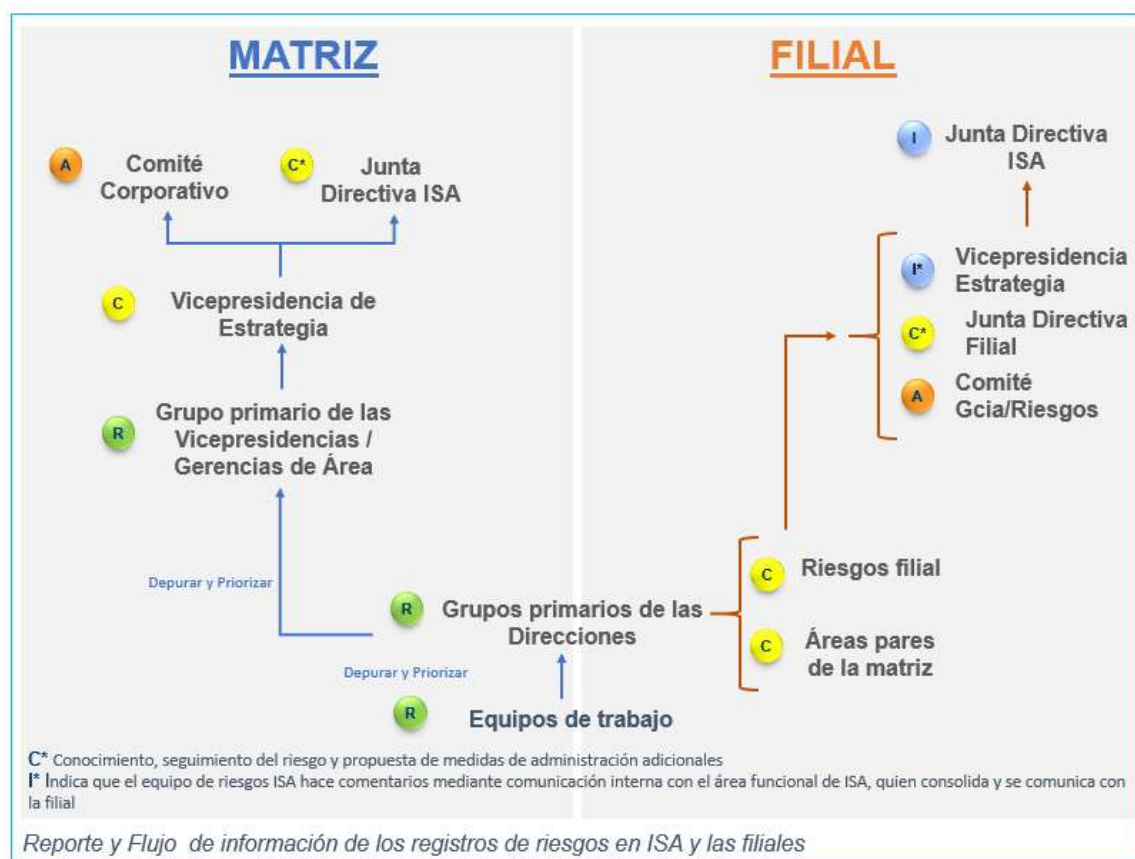
**Análisis expost:** Incluye el análisis de eventos materializados y la incorporación de lecciones aprendidas

**Aseguramiento:** Verificación efectividad de la gestión integral de riesgos y de los controles

## 9.3. REPORTE Y FLUJO DE INFORMACIÓN DE LOS REGISTROS DE RIESGOS

Para el registro de los riesgos, se ha diseñado un formato de riesgos que aplica de igual manera para ISA, sus empresas y proyectos.

A continuación, se muestra gráficamente el flujo información para el registro de los riesgos de acuerdo a lo establecido en la RACI de ISA y sus filiales, en lo referente al contexto, valoración, tratamiento, monitoreo y comunicación.



La identificación de riesgos se hace con una periodicidad trimestral.

En ISA, la Vicepresidencia de Estrategia realiza una retroalimentación a los Vicepresidentes sobre lo presentado en la Junta, estos a su vez deberán replicar la información a sus Directores y estos a sus equipos de trabajo.

Los directores corporativos en sus conversaciones con sus pares en las filiales harán seguimiento e identificación de riesgos.



La actualización del formato, así como la comunicación permanente del mismo, será responsabilidad del dueño del proceso.

Por cumplimiento de las leyes anticorrupción en los diferentes países y a los lineamientos establecidos por ISA en este tema, en los formatos de registro de riesgos de todas las filiales y de los procesos se deberán incluir los eventos relacionado con el riesgo de fraude y corrupción, incluso si su valoración da como resultado un nivel de riesgo verde.

Las filiales deberán enviar a la vicepresidencia de estrategia de ISA cada trimestre (a más tardar la segunda semana del mes siguiente al cierre del trimestre) la siguiente información, con el fin de consolidarla para la actualización del perfil de riesgos del grupo y la presentación trimestral a la Junta de ISA:

- Formato de registro de riesgos (con todos los riesgos)
- Diagramas de análisis de riesgos (en Power Point diseñada para explicar de manera resumida la información relacionada con cada uno de los riesgos) de los eventos de riesgo rojos y naranjas. Ver ejemplo de en el numeral 5.8
- Alertas que se consideren deben ser escaladas. Es importante tener claridad de que las alertas deben ser temporales, ya que hacen referencia a posibles eventos de los cuales no se tiene información suficiente para ser valorados y se espera que para el próximo informe puedan ser incluidas como riesgos o eliminados ya que después de hacer un análisis del tema no ameritan ser evaluadas como riesgos.

Para la estructuración de ofertas en todos los negocios, se hace un proceso de identificación, análisis, evaluación y tratamiento de riesgos utilizando el formato de riesgos. Una vez la oferta es adjudicada, el gestor de proyectos recibe el formato de riesgos para ser incluido en su seguimiento mensual.

## **10. ANEXOS**

### **ANEXO 1: FUNCIONES DEL COMITÉ DE JUNTA Y GOBIERNO**

Las funciones del comité de junta y gobierno frente a los temas de riesgos vienen regladas desde el código país (Colombia, donde se tiene la matriz del grupo). El siguiente es un resumen de las mismas:

- Revisión de los niveles de riesgos naranjas y rojos del grupo empresarial, validando el nivel rojo existente o recomendando medidas adicionales de administración e informar a la junta.
- Revisar y evaluar la adecuación de la gestión de riesgos y los límites de riesgos en la organización
- Proponer a la junta las políticas de riesgos.
- Valorar sistemáticamente estrategia, lineamientos, políticas y límites de gestión y priorización de riesgos
- Impulsar la adecuación de la gestión del riesgo en la sociedad a un modelo avanzado que permita la configuración de un perfil de riesgos acorde con los objetivos estratégicos y un seguimiento del grado de adecuación de los riesgos asumidos a ese perfil.

### **ANEXO 2: FORMATOS**

Como anexos a este manual deberá tenerse en cuenta los siguientes formatos:

- Formato de registro de riesgos en Excel
- Diagramas de análisis de riesgos en Power Point diseñada para explicar de manera resumida la información relacionada con cada uno de los riesgos.