

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

TABLA DE CONTENIDO

1	OBJETIVO	2
2	CONDICIONES GENERALES	2
2.1	Marco normativo	2
2.2	Roles y responsabilidades	2
2.2.1	Accountable o Responsable de Riesgo Empresarial	3
2.2.2	Líder de Riesgo Empresarial	3
2.2.3	Ejecutores de Acciones de tratamiento	3
2.2.4	Ejecutores de KRIs	4
2.2.5	Gerencia Corporativa de Gestión Integrada de Riesgos (GIR)	4
3	DESARROLLO	4
3.1	PLANEAR	5
3.1.1	Entradas	5
3.1.2	Proceso.....	5
3.1.3	Salidas.....	8
3.2	IDENTIFICAR	8
3.2.1	Entradas	8
3.2.2	Proceso.....	8
3.2.3	Salidas.....	10
3.3	EVALUAR	11
3.3.1	Entradas	11
3.3.2	Proceso.....	12
3.3.3	Salidas.....	13
3.4	TRATAR.....	14
3.4.1	Entradas	14
3.4.2	Proceso.....	14
3.4.3	Salidas.....	18
3.5	COMUNICACIÓN Y CONSULTA	19
3.5.1	Entradas	19
3.5.2	Proceso.....	19
3.5.3	Salidas.....	21
3.6	SEGUIMIENTO Y REVISIÓN	21
3.6.1	Entradas	21
3.6.2	Proceso.....	21
3.6.3	Salidas.....	25

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.7	REGISTRO E INFORME.....	25
4	CONTINGENCIAS	25

1 OBJETIVO

Brindar los lineamientos para la aplicación del ciclo de gestión de riesgos empresariales en las compañías del Grupo Ecopetrol¹ ("Grupo" o "GE"), que permitan asegurar la gestión de los riesgos que puedan generar desviaciones frente al cumplimiento de la estrategia y objetivos estratégicos de cada compañía y obtener información confiable soporte para la toma de decisiones.

2 CONDICIONES GENERALES

2.1 Marco normativo

Los riesgos empresariales, corresponden a la posibilidad de ocurrencia de eventos que afecten la consecución de la estrategia y los objetivos estratégicos de la compañía. En este sentido, estos riesgos son aquellos que reflejan las principales amenazas de cada una de las compañías a las que les aplica este procedimiento, de conformidad con el alcance que se detalla en el pie de página No.1 del presente documento y que se enlistan el Anexo No. 1.

En este documento se detallan los lineamientos de la gestión de riesgos empresariales de acuerdo con los principios, marco y proceso (o ciclo de gestión de riesgos) del Sistema de Gestión Integrado de Riesgos – SRI², según lo establecido en la Guía para la Gestión Integrada de Riesgos en el Grupo Ecopetrol GEE-G-029 y basado en ISO 31000 y COSO ERM 2017, aplicables a Ecopetrol S.A. ("Ecopetrol") y a las compañías del Grupo incluidas en el alcance.

2.2 Roles y responsabilidades

Cada compañía del Grupo Ecopetrol a la que aplique el presente documento debe definir los roles y responsabilidades para la gestión de sus riesgos empresariales, de conformidad con su estructura funcional y de procesos, tomando como referencia lo establecido para Ecopetrol.

La gestión de riesgos empresariales abarca responsabilidades aplicables a diferentes instancias y roles de la compañía, que incluyen a la Junta Directiva, niveles directivos y a los trabajadores en general, de conformidad con lo establecido en la Guía para la Gestión Integrada de Riesgos en el Grupo Ecopetrol GEE-G-029. A continuación, se presentan las responsabilidades complementarias en lo relacionado con la gestión de riesgos empresariales en Ecopetrol.

¹ El Grupo Ecopetrol está conformado por todas las compañías subordinadas y aquellas sociedades en las que Ecopetrol tiene alguna participación accionaria, así como los vehículos financieros y de inversión que tiene Ecopetrol tanto en Colombia como en el exterior. De conformidad con lo establecido en el Modelo de Gobierno Corporativo aplicable al Grupo Ecopetrol, este procedimiento es aplicable a las subordinadas que de tiempo en tiempo defina la Vicepresidencia Corporativa de Cumplimiento de Ecopetrol (VCU), considerando alguno de los siguientes criterios: i) tipología de las compañías según naturaleza operativa y jurisdicción (clasificación prevista en la Guía de Gobierno Corporativo GEE-G-041); ii) la relación de control desde Ecopetrol S.A. como matriz y iii) que cuente con oficial de cumplimiento.

² En alineación con el SRI, Riesgo estratégico o empresarial, es el efecto de la incertidumbre en los objetivos estratégicos y estrategia de la compañía, bien sea positivo o negativo.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

2.2.1 Accountable o Responsable de Riesgo Empresarial

Tiene como responsabilidad:

- Designar al líder del riesgo empresarial.
- Conocer las acciones de tratamiento (ATs) para gestionar los riesgos empresariales a cargo.
- Conocer los KRIs (indicadores clave de riesgo) para el monitoreo de las alertas de los riesgos empresariales a cargo.
- Conocer los cambios que se requieran sobre las ATs y KRIs.
- Conocer la valoración inherente y residual del riesgo.
- Conocer el estado de ejecución de las ATs, los eventos materializados y su gestión, y las alertas generadas por medio de los KRIs y por otras fuentes.
- Informar a la GIR³ temas que puedan implicar cambios en los riesgos empresariales.
- Reportar las materializaciones de riesgos empresariales y los potenciales nuevos riesgos identificados, a través de las preguntas de las autoevaluaciones de control interno.
- Reportar potenciales riesgos nuevos, a través de las preguntas de las autoevaluaciones de control interno.

De acuerdo con las temáticas contenidas en un riesgo empresarial, es posible que éste tenga más de un accountable, según las áreas que tengan conocimiento técnico y liderazgo sobre estos.

2.2.2 Líder de Riesgo Empresarial

Tiene como responsabilidad:

- Definir las acciones de tratamiento (ATs) y KRIs para gestionar los riesgos empresariales a cargo.
- Aprobar la valoración inherente y residual cada vez que se requiera su actualización.
- Mantener una comunicación permanente con los ejecutores de las acciones de tratamiento, KRIs y demás participantes de la gestión de riesgos, así como con el profesional de la GIR asignado para dar apoyo metodológico.
- Asegurar la calidad y oportunidad de la información reportada en las fechas programadas en la herramienta establecida para gestión de riesgos⁴ y demás medios establecidos por la GIR, con respecto a la ejecución y efectividad de las acciones de tratamiento, materializaciones, KRIs y otras alertas.
- Identificar los eventos materializados, realizar el análisis del evento ocurrido, sus impactos, y definir las acciones para mitigar el impacto de la materialización (cuando aplique) y para reducir la probabilidad de ocurrencia de nuevos eventos. Registrar el resultado del análisis en los formatos o la herramienta¹⁰ según lo requerido por la GIR.
- Realizar seguimiento a las acciones definidas para la gestión de los eventos materializados.
- Informar al accountable del riesgo los ajustes requeridos sobre las ATs o KRIs.
- Comunicar el estado de la gestión del riesgo empresarial al accountable.
- Conocer el estado integral del riesgo, teniendo en cuenta la gestión realizada por las áreas participantes.

2.2.3 Ejecutores de Acciones de tratamiento

Tiene como responsabilidad:

- Reportar el avance de la ejecución y la efectividad de la AT en la herramienta¹⁰ como máximo el quinto día hábil del mes, según las pautas para el seguimiento y medición.

³Gerencia Corporativa de Gestión Integrada de Riesgos de Ecopetrol.

⁴ Bwise para el caso de Ecopetrol o cualquier otra que se implemente. En el caso de las compañías a las que aplique el presente documento, se utiliza la herramienta definida en cada caso.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

- Comunicar al líder del riesgo el estado de ejecución de la AT y la efectividad o beneficio obtenido para aquellas ATs finalizadas.
- Asegurar la custodia de los soportes de los hitos ejecutados.
- Reportar al líder del riesgo los cambios requeridos sobre la AT.
- Registrar el cambio aprobado en la herramienta¹⁰.
- Atender las consultas que surjan desde la GIR.

2.2.4 Ejecutores de KRIs

Tiene como responsabilidad:

- Realizar el cálculo de la medición del KRI según lo establecido (aplicación correcta de la fórmula de cálculo y fuentes de información, entre otras).
- Asegurar la custodia de los soportes de los cálculos realizados para el KRI.
- Asegurar el reporte del resultado y análisis del KRI en la herramienta¹⁰, como máximo el quinto día hábil del mes, según las pautas para el seguimiento y medición.
- Comunicar al líder del riesgo el resultado del KRI y el análisis de la alerta cuando se presente.
- Atender las consultas que surjan desde la GIR.

2.2.5 Gerencia Corporativa de Gestión Integrada de Riesgos (GIR)⁵

Tiene la responsabilidad de:

- Definir los lineamientos para la gestión de riesgos empresariales y asegurar la gestión de los mismos por parte de sus dueños en Ecopetrol y en el Grupo a través de las áreas de Cumplimiento de las compañías a las que les aplique el presente documento (o quien haga sus veces).
- Definir y actualizar los riesgos empresariales de Ecopetrol.
- Realizar seguimiento a la gestión de riesgos empresariales, mediante los KRIs, materializaciones y otras alertas o tendencias.
- Apoyar metodológicamente a los accountables, líderes de riesgo y demás participantes de la gestión del riesgo empresarial.
- Proporcionar soporte metodológico a las compañías a las que les aplique el presente documento, en relación con la aplicación del ciclo de gestión de riesgos empresariales.
- Definir el esquema de comunicaciones del ciclo de gestión de riesgos empresariales al interior de la compañía, para asegurar las revisiones del líder del riesgo y del accountable.
- Realizar seguimiento a la gestión de riesgos empresariales en lo relacionado con acciones de tratamiento y materializaciones.

3 DESARROLLO

La gestión de riesgos empresariales se enfoca en la reducción de la probabilidad de ocurrencia de éstos y en la gestión de los impactos. Los lineamientos para tal fin son establecidos por la Gerencia Corporativa de Gestión Integrada de Riesgos, para su cumplimiento en las compañías a las que les aplique el presente documento. En su ejecución intervienen todas las áreas de cada compañía.

El Ciclo de Gestión de Riesgos Empresariales comprende las etapas que se muestran a continuación:

⁵ Las áreas de cumplimiento de las compañías en alcance cumplen el rol equivalente que desempeña la GIR en Ecopetrol.
Plantilla 010 -23/08/2017 v-6

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2



Figura 1. Ciclo de Gestión de Riesgos Empresariales.

3.1 PLANEAR

En esta etapa se define el alcance de las actividades a ejecutar en el Ciclo de Gestión de Riesgos Empresariales y debe incluir la definición de un plan de trabajo para tal fin.

Las actividades del ciclo de gestión de riesgos empresariales deben planearse cada vez que se realice la definición y/o revisión a la estrategia, o de los objetivos estratégicos de cada compañía, y en la medida en que se identifiquen tendencias emergentes que generen cambios de los riesgos empresariales.

3.1.1 Entradas

- Definición estratégica (estrategia y objetivos estratégicos) de la compañía.
- Estructura organizacional.
- Mapa de procesos de la compañía.
- Otros insumos: Lineamientos y procedimientos organizacionales que pueden influir en la planeación de la gestión de riesgos. Pueden incluir niveles de autoridad y toma de decisión, roles y responsabilidades de los órganos de gobierno de la empresa, entre otros.

3.1.2 Proceso

a. Definición del alcance

Por lo menos una vez al año y cada vez que se actualice la estrategia o los objetivos estratégicos de la compañía, se debe realizar un análisis comparativo a fin de determinar los cambios presentados, así como su potencial impacto en los riesgos empresariales de la compañía.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Para las compañías a las que les aplique el presente documento, el ejercicio anterior deberá ser remitido a la GIR de acuerdo con las fechas establecidas para tal fin, según calendario general que se les comunique.

Una vez se haya identificado la necesidad de actualización de los riesgos empresariales como conclusión del análisis comparativo, se debe planear la ejecución del ciclo considerando las actividades requeridas para tal fin.

b. Análisis del contexto interno y externo

Para asegurar una adecuada identificación de riesgos, pueden adelantarse, entre otras, las siguientes actividades con el fin de contar con la mejor información disponible para evaluar el contexto externo e interno, y así considerar todo aquello que puede afectar el logro de los objetivos de la compañía.

Contexto externo	Revisión de información producida por firmas de consultoría especializadas en riesgos y en el sector Oil & Gas y energético, así como la revisión de informes de compañías aseguradoras y firmas calificadoras de riesgos:
	a. Revisión de informes publicados con análisis y comportamientos de empresas del sector (por ejemplo, anualmente las firmas de consultoría publican informes relacionados con la gestión de riesgos en el sector de Oil & Gas en el mundo). Dichos informes son uno de los insumos principales para el análisis del contexto externo, toda vez que presentan y analizan riesgos del sector. b. Entrevistas con consultores de firmas, para obtener detalle de las tendencias del entorno externo. c. Revisión de otros artículos que contienen análisis de la industria y los principales asuntos políticos y económicos a nivel nacional e internacional, tales como el informe de riesgos mundiales del World Economic Forum, entre otros.
	Benchmark de otras empresas de sectores Oil & Gas, energético y relacionados para realizar revisión de compañías locales o internacionales con el fin de enriquecer y analizar la lista de riesgos típicos de estas industrias. Para este ejercicio se puede consultar el reporte 20F generado para la SEC (Securities and Exchange Commission de Estados Unidos).
	Índices y radares de sostenibilidad tales como DJSI ⁶ , CDP ⁷ , MSCI, Sustainalytics, TCFD ⁸ , entre otros.

⁶ Dow Jones Sustainability Index.

⁷ Disclosure Inside Action.

⁸ Task Force on Climate-related Financial Disclosures.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

	Revisión y análisis de riesgos estratégicos de sus subordinadas⁹: Se realiza para determinar la incidencia o impacto que puedan tener los riesgos de otras compañías sobre los objetivos estratégicos analizados, a partir de lo siguiente: • Identificación de los riesgos estratégicos de las compañías que estén relacionados directamente con objetivos estratégicos de la compañía analizada. • Análisis de los riesgos identificados, con respecto a su relación con los riesgos contenidos en el Mapa de Riesgos Empresariales de la compañía o sus causas. Las descripciones y cifras asociadas a estos riesgos servirán como insumo para la documentación de cifras, datos, análisis y para la elaboración de la ficha técnica de los riesgos empresariales. • Análisis del impacto de la materialización de riesgos. A partir de lo anterior, las compañías a las que les aplique el presente documento, deberán realizar un análisis de alineación de su Mapa de Riesgos Empresariales con el de Ecopetrol.
Contexto interno	Entrevistas o encuestas con miembros de la Alta Dirección de la compañía, con el fin de conocer de primera mano su percepción sobre los asuntos que puedan afectar el logro de la estrategia o sus objetivos. Igualmente, se pueden incluir otros líderes de la compañía, cuya percepción y conocimiento experto, se considere importante para el análisis. Se puede tomar como referencia el listado de riesgos vigentes y plantear a los entrevistados las nuevas temáticas que surgieron como producto de la revisión de los informes de las firmas consultoras, del análisis de la situación global, nacional y regional del sector y de las condiciones particulares por las cuales se encuentre pasando la empresa y que podrían integrar el nuevo mapa de riesgos. Análisis de riesgos en procesos: Las matrices de riesgos y controles de los procesos de la compañía cuentan con información útil para la identificación, análisis y gestión de riesgos empresariales. Los riesgos de procesos que pueden ser considerados o evaluados como posibles riesgos empresariales o causas de estos, serán aquellos que estén asociados a objetivos estratégicos de la compañía, o por cuya criticidad tengan que ser considerados a nivel estratégico, entre otros¹⁰. Resultados o asuntos reportados en las autoevaluaciones de control interno, relacionados con riesgos empresariales y con potenciales nuevos riesgos.

⁹ Para las compañías que Ecopetrol controla de manera indirecta, este análisis deberá contemplar los riesgos identificados por las compañías filiales a través de las cuales ejerce dicho control indirecto.

¹⁰ Un insumo importante para la construcción de las matrices de riesgos y controles de los procesos lo constituyen los resultados, hallazgos y recomendaciones de las auditorías internas y externas; por ende, al realizar el análisis de los riesgos en los procesos como insumo para la construcción del Mapa de Riesgos Empresariales, se consideran involucrados dichos resultados.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.1.3 Salidas

Al terminar esta etapa, se debe contar con:

- Documentación del análisis del contexto interno y externo realizado.
- El análisis comparativo de cambios en estrategia y objetivos estratégicos.
- El plan de trabajo con actividades, fecha de inicio, fecha fin, responsables para la actualización del Mapa de Riesgos Empresariales, cuando aplique.

Si como resultado de lo anterior se identifica que no es necesaria la actualización del Mapa de Riesgos Empresariales, se deberá contar con el análisis de suficiencia de los riesgos empresariales vigentes documentado.

3.2 IDENTIFICAR

La identificación de riesgos permite, en una forma sistemática y estructurada, determinar los riesgos que pueden afectar negativamente los objetivos estratégicos y el logro de la estrategia de la compañía. Estos eventos deben ser considerados, bien sea que se encuentren o no bajo el control de la organización, abarcando riesgos nuevos, cambiantes, existentes y tendencias emergentes.

3.2.1 Entradas

- Herramientas definidas en la planeación.
- Documentación del análisis del entorno interno y externo realizado.
- Normativa y otros insumos existentes en la organización: lineamientos, procedimientos o resultados organizacionales que pueden influir en la gestión de riesgos.
- Mapa de Riesgos Empresariales de cada compañía vigente (listado y ficha descriptiva de los riesgos).
- Información de eventos materializados.

3.2.2 Proceso

Para llevar a cabo esta etapa, se puede partir de los riesgos vigentes verificando su permanencia y suficiencia frente al cubrimiento de los objetivos empresariales. Adicional a este análisis, se deben llevar a cabo las siguientes actividades:

- Formulación de riesgos nuevos en el mapa cuando se presenten las siguientes situaciones:
 - Cambios en los objetivos estratégicos.
 - Cambios en el contexto interno o externo.
 - Temáticas emergentes que tienen impacto en el logro de los objetivos y deben ser incluidas como riesgos empresariales, o riesgos emergentes ya identificados cuyo tratamiento corresponda a la incorporación dentro del Mapa de Riesgos Empresariales.

No todas las temáticas identificadas deben verse reflejadas como riesgos empresariales, pues algunas de éstas pueden ser incluidas también como causas o focos de riesgos, o podrían no considerarse ya que están contempladas y debidamente gestionadas en otros niveles de riesgo. Para este análisis, se debe tener en cuenta:

- El aumento significativo (en su frecuencia o impacto) de eventos materializados relacionados con el riesgo analizado.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

- La inminencia de su materialización de no llevarse a cabo medidas en el corto, mediano y largo plazo.
- El peso o relevancia otorgada por el nivel directivo, en el ejercicio de actualización y validación del Mapa de Riesgos Empresariales.

ii. Eliminación de riesgos empresariales:

Para proponer la eliminación de un riesgo del Mapa de Riesgos Empresariales vigente, se debe tener en cuenta lo siguiente:

- Que el riesgo no tenga alineación directa con los objetivos estratégicos de la compañía.
- Que las principales causas del riesgo están debidamente identificadas y gestionadas en alguno de los procesos de la compañía y su impacto no está directamente ligado con la ejecución de la estrategia.
- Que la problemática se consideró temporalmente como riesgo empresarial con el fin de darle mayor visibilidad debido a una situación coyuntural, o el contexto en el que operaba al momento de su identificación y ya no representa un impacto significativo para el logro de la estrategia.
- Que producto del análisis y revisión, se concluya que la problemática o sus causas asociadas se originan principalmente en fallas en la gestión de la compañía o sus procesos.
- Que como resultado del monitoreo del riesgo se identifica un bajo nivel de exposición, por lo que su gestión se puede dar en otros niveles de riesgo (táctico u operativo).

iii. Ratificación o modificación de riesgos existentes

Varios de los riesgos se mantienen año tras año en el Mapa de Riesgos Empresariales y su permanencia puede explicarse, entre otras, por una o varias de las siguientes razones:

- Se han identificado previamente y deben ajustarse por cambios en el contexto interno o externo.
- Se trata de riesgos inherentes a la industria.
- Las temáticas del riesgo siguen vigentes y guardan relación directa con la estrategia y objetivos estratégicos de la empresa.

a. Documentación del Mapa de Riesgos Empresariales

Se debe documentar la propuesta definitiva de Mapa de Riesgos Empresariales, lo cual incluye la ficha técnica de cada riesgo y la representación gráfica.

i. Ficha técnica

La ficha técnica del riesgo debe contener los siguientes elementos:

- **Nombre:** Es un reflejo de lo que se quiere representar con el riesgo. Debe ser un nombre corto, pero que evite ambigüedades.
- **Objetivo estratégico (o su equivalente):** Indicar el(los) objetivo(s) estratégico(s) que podría(n) verse afectado(s) en caso de materializarse el riesgo.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

- *Descripción:* Caracterización del riesgo de manera explícita. Aquí se puede incluir la justificación de la relevancia del riesgo para la compañía.
- *Evento tipo de materialización:* Establecer los eventos con los cuales se considera que este riesgo se materializa.
- *Causas:* Hace referencia a por qué podría ocurrir dicho riesgo. Se debe realizar el análisis de las causas directas, internas y del entorno que dan origen al evento. Estas deben ser concretas y coherentes.
- *Consecuencias:* Hace referencia al impacto de la materialización del riesgo sobre los recursos empresariales (personas, ambiente, económico, reputación, entre otros). Se deben determinar las consecuencias directas.
- *Procesos apalancadores:* Son los procesos que en su operar o en sus actividades de control contribuyen con la gestión del riesgo.
- *Área responsable / accountable:* Define qué áreas participan en dicha gestión, según su afinidad o conocimiento en las temáticas que componen el riesgo.

b. Validación del Mapa de Riesgos Empresariales

Los riesgos empresariales identificados surten un conjunto de validaciones previo a su aprobación, como se presenta a continuación:

- Sesiones de validación y construcción con las áreas responsables de los riesgos, con el fin de realizar ajustes a la información contenida en las fichas, así como la valoración inherente de éstos, considerando las temáticas relevantes identificadas.
- Validación con miembros del nivel directivo para socializar los riesgos propuestos y obtener las observaciones al respecto.
- Sesión con miembros de la Junta Directiva y/o su Comité de Auditoría y Riesgos (o quien haga sus veces), para presentar los riesgos identificados/actualizados como resultado de los análisis realizados, haciendo evidentes modificaciones a que haya lugar en la estructura del mapa y en el contenido o alcance de los riesgos que lo constituyen. Para esta sesión cada uno de los riesgos debe estar debidamente soportado, es decir, debe contar con suficiente información que sustente su inclusión / exclusión / modificación en el mapa.

Una vez implementados los ajustes recomendados en las instancias anteriores, se presenta el Mapa de Riesgos Empresariales a la Junta Directiva para su aprobación, según corresponda.

3.2.3 Salidas

Al terminar esta fase, se debe contar con:

- Aprobación del Mapa de Riesgos Empresariales.
- Fichas técnicas de los Riesgos Empresariales.
- Valoración de los riesgos empresariales (inherente y nivel residual preliminar)¹¹.

¹¹ La valoración inherente y residual se obtiene a partir de la aplicación metodológica de la etapa *Evaluar* del presente documento.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.3 EVALUAR

En la etapa de evaluación se realiza el análisis de la probabilidad de ocurrencia del riesgo y el nivel de los impactos del riesgo.

Esta valoración de riesgos empresariales obedece a un análisis semi-cuantitativo mediante el cual se busca priorizar los riesgos asignándole a estos, valores dentro de escalas o rangos definidos de probabilidad e impacto, según la matriz de valoración de riesgos – RAM de la compañía.

Los riesgos deben ser priorizados con el fin de lograr una efectiva distribución de los recursos disponibles para tratar aquellos riesgos críticos. Esto se logra a partir de la medición de la probabilidad de ocurrencia del evento de riesgo y el impacto sobre los recursos (personas, ambiente, económico, reputación, clientes, y otros, según se defina para cada una de las compañías a las que les aplique el presente documento).

El ejercicio de valoración se realiza a partir de los riesgos empresariales identificados, documentándolo en la herramienta o formato de valoración de riesgos definida para tal fin¹², en el cual se debe registrar el resultado de la valoración considerando dos instancias principales: la valoración inherente y la valoración residual, como se ilustra en la siguiente figura:



Figura 2. Valoración de Riesgos

3.3.1 Entradas

- Riesgos empresariales identificados y medidas de mitigación existentes (acciones de tratamiento finalizadas, controles y otros mitigantes).
- RAM – Matriz de Valoración de Riesgos.
- Matriz de riesgos y controles de los procesos.
- Resultados de autoevaluaciones, pruebas de la gerencia y revisoría fiscal sobre pruebas realizadas al diseño y operatividad de los controles.

¹² El formato SRI-F-001 es aplicado para la valoración de riesgos empresariales en Ecopetrol. Las compañías que apliquen diferentes categorías, niveles o descriptores de impacto para la valoración de riesgos, deberán hacer la correspondiente adaptación de dicho formato.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

- v. Información histórica de incidentes o riesgos empresariales materializados que permita la estimación de frecuencias de ocurrencia e impactos. Dentro de esta información se encuentran bases de datos de siniestralidad, costos y tiempos, incidentes ocurridos en la industria o en la empresa así no se encuentren registrados en bases de datos formales.
- vi. Otra información relevante que pudiese permitir la estimación de la probabilidad o impacto de los riesgos empresariales.

3.3.2 Proceso

• Valoración Inherente

La valoración del riesgo se realiza a partir de la medición de la probabilidad e impacto sin tener en cuenta el efecto de los mitigantes existentes y considerando el ambiente de control de la compañía.

A partir de los descriptores definidos en la matriz RAM de la compañía, se debe identificar la probabilidad de ocurrencia del riesgo basándose en los eventos de materialización establecidos en su ficha técnica. Para esto, se debe analizar la información histórica de eventos materializados o estadísticas del riesgo a valorar que se hayan presentado en el sector o en la compañía, e identificar cuáles han sido las situaciones reales más críticas o representativas. Si no se cuenta con suficiente información que permita establecer una situación real, se debe estructurar una situación hipotética que resulte creíble, partiendo del evento del riesgo y los posibles impactos de su materialización sobre el logro de los objetivos asociados.

La situación identificada se documentará como escenario de valoración y deberá ser delimitada por datos económicos, en la medida de lo posible, para facilitar y precisar el valor del escenario con base en el cual se realizará la valoración inherente del riesgo. Este análisis se documentará en el formato utilizado para la valoración de riesgos.

Tenga en cuenta que el escenario preferiblemente debe estar basado en la peor situación histórica ocurrida conocida. Para una construcción del escenario hipotético, se recomienda revisar con los pares en la industria, y crearlo en conjunto con los responsables o accountables del riesgo.

Partiendo del escenario de valoración definido, se selecciona el valor de la probabilidad que mejor se ajusta al evento del riesgo, considerando la información disponible sobre frecuencia o probabilidad. Posteriormente, se califican los impactos del riesgo, según la RAM, teniendo en cuenta los efectos directos sobre los recursos; para ello, identifique de los descriptores el que mejor refleje el impacto del escenario, calificando cada una de las variables aplicables.

La valoración inherente del riesgo está dada por el nivel más alto resultante de la combinación de la probabilidad e impacto(s) evaluado(s). Los niveles de dichas combinaciones son: VH (Very High – Muy Alto); H (High – Alto); M (Medium – Medio); L (Low – Bajo) y N (Null – Muy Bajo) de acuerdo con la RAM.

En caso de contar con información para la construcción de escenarios tanto hipotéticos como reales, se debe seleccionar el escenario que represente impactos más críticos.

• Valoración Residual

Una vez obtenida la valoración inherente del riesgo, se procede a estimar la valoración residual, partiendo de la suficiencia y evaluación de la efectividad de los mitigantes existentes.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

La valoración residual se entiende como el nivel de riesgo resultante una vez se aplican los mitigantes sobre la probabilidad de ocurrencia del riesgo y el impacto de las consecuencias sobre los recursos. Se realiza con el fin de establecer el nivel de exposición a los riesgos identificados, considerando la existencia de los mitigantes que operan y su efectividad en la mitigación del riesgo.

El conjunto de mitigantes a considerar puede estar compuesto por:

- Controles de riesgos de proceso asociados a las causas o consecuencias del riesgo empresarial.
- Acciones de tratamiento finalizadas cuyo análisis concluya que el beneficio propuesto para las mismas fue logrado.
- Otras actividades que contribuyen con la gestión del riesgo (por ejemplo, proyectos, iniciativas).

La valoración residual de los riesgos empresariales se obtiene a partir de la evaluación de los mitigantes, según sus características y su cubrimiento de la causa o consecuencia del riesgo empresarial. Dicho análisis se realiza con base en los últimos resultados disponibles de Revisoría Fiscal y/o Pruebas de la Gerencia, así como los resultados trimestrales de las autoevaluaciones de control interno.

Para ampliar el detalle de los criterios para la evaluación del conjunto de mitigantes, consulte el Anexo 2 de este documento.

• **Análisis de manejabilidad de riesgos empresariales**

La manejabilidad del riesgo empresarial consiste en la facilidad con que la ocurrencia o el impacto del riesgo puedan ser gestionados, de manera tal que mayor manejabilidad implica un mayor control/gestión sobre el riesgo.

Este análisis se realiza con el fin de determinar el nivel del riesgo esperado, para ello se diligencia el formato SRI-F-001 que permite ver de manera gráfica el panorama del riesgo según la posibilidad de su mitigación.

Para determinar el nivel de manejabilidad, se clasifican cada una de las causas del riesgo en internas o externas y se determina el porcentaje de éstas frente al número total de causas. A partir de estas proporciones, se puede aplicar la siguiente calificación:

Manejabilidad	% de causas internas	Valores a utilizar en el gráfico
Alta	Mayor a 67%	7 - 8 - 9
Media	Entre 50% y 67%	4- 5 - 6
Baja	Menor a 50%	1 - 2 - 3

Tabla 7. Análisis de manejabilidad.

Este análisis servirá de insumo en la etapa Tratar, y permitirá orientar las medidas de tratamiento para llevarlo al nivel residual esperado.

3.3.3 Salidas

Al finalizar esta etapa se obtiene la valoración inherente, la valoración residual y el análisis de manejabilidad de los riesgos empresariales identificados, en los formatos definidos para tal fin.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.4 TRATAR

En esta etapa se definen las actividades con las que se pretende prevenir las causas o protegerse de las consecuencias, y generar alertas sobre posibles materializaciones del riesgo empresarial. Si la valoración residual del riesgo empresarial es "Very High", "High", o "Medium" deben definirse acciones de tratamiento para gestionar las causas no cubiertas en su totalidad por los mitigantes existentes.

3.4.1 Entradas

- Mapa de Riesgos Empresariales.
- Formato matriz de valoración de riesgos empresariales.

3.4.2 Proceso

En esta etapa se analizan las causas a gestionar para cada uno de los riesgos empresariales y a partir de allí se identifican las nuevas medidas de mitigación que permitan reducir la probabilidad. De igual manera se analizan las consecuencias del riesgo y sobre éstas se identifican las medidas adicionales que puedan reducir el impacto.

Partiendo de la definición de opciones de tratamiento (evitar, aceptar, transferir, mitigar) establecidas en la Guía para la Gestión Integrada de Riesgos en el Grupo Ecopetrol GEE-G-029, en este documento desarrollaremos los pasos a seguir para la opción "Mitigar".

a. Definición de Acciones de Tratamiento

Las Acciones de Tratamiento de riesgos empresariales se establecen para eliminar o reducir la probabilidad de ocurrencia de las causas de los riesgos o disminuir el impacto de una eventual materialización de éstos. En este sentido, una Acción de Tratamiento adecuadamente diseñada deben ser medibles, cuantificables y verificables, cumpliendo con: a) Contar con una estructura claramente definida, b) Contar con un beneficio verificable frente a la efectividad de su implementación y b) Cumplir con unos requisitos mínimos, de acuerdo con el tipo de acción a realizar. Las acciones de tratamiento definidas no podrán ser las actividades normales de proceso.

La estructura de una acción de tratamiento se compone de: Nombre, Descripción, Beneficios, Plan de Trabajo, Avance del Plan, Fecha de Inicio, Fecha Final y Ejecutor.

Elementos de la AT	Definición	Ejemplo
Nombre	Nombre corto de la acción que describe brevemente la actividad a realizar.	"Diseño e implementación de estructura de seguimiento al proceso"
Descripción	Debe indicar qué se va a hacer y para qué se va a hacer. Incluye los beneficios asociados a la reducción de la probabilidad de ocurrencia de las causas o la reducción de los impactos en caso de materializarse el riesgo.	Diseño de una Estructura de Control de Gestión al interior del área W, con el propósito de reforzar el seguimiento al proceso X. Una adecuada estructura de control de gestión permitirá monitorear alarmas sobre el desempeño de indicadores, reduciendo la probabilidad de no

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Elementos de la AT	Definición	Ejemplo																														
		identificación oportuna de las desviaciones en los resultados esperados del proceso y sus posibles causas. Consecuentemente, permitirá reducir los impactos en aquellos casos en los que se apliquen oportunidades, acciones correctivas o de remediación. Esto se podrá evidenciar en el mayor número de alarmas gestionadas o en la reducción de los impactos generados por la gestión oportuna de las causas.																														
Plan de trabajo	Es la descripción detallada de las actividades que soportan la acción de tratamiento. Estará compuesto por los siguientes elementos: • Hitos que lo componen. • Porcentaje de cumplimiento planeado acumulado de las actividades durante su ejecución. • Listado de entregables que soporten las actividades finalizadas (deben ser concretos y evidenciables). • Fecha de finalización de la actividad. • Responsable de cada hito.	<table><tr><th>Hitos/ Actividad</th><th>Avance Acumulado</th><th>Entregables</th><th>Fecha</th><th>Responsable</th></tr><tr><td>Actividad 1</td><td>30%</td><td>Entregable 1</td><td>Marzo</td><td>Responsable 1</td></tr><tr><td>Actividad 2</td><td>50%</td><td>Entregable 2</td><td>Junio</td><td>Responsable 2</td></tr><tr><td>Actividad 3</td><td>60%</td><td>Entregable 3</td><td>Septiembre</td><td>Responsable 3</td></tr><tr><td>...</td><td>..</td><td>...</td><td>...</td><td></td></tr><tr><td>Actividad n</td><td>100%</td><td>Entregable n</td><td>Noviembre</td><td>Responsable n</td></tr></table>	Hitos/ Actividad	Avance Acumulado	Entregables	Fecha	Responsable	Actividad 1	30%	Entregable 1	Marzo	Responsable 1	Actividad 2	50%	Entregable 2	Junio	Responsable 2	Actividad 3	60%	Entregable 3	Septiembre	Responsable 3	...	..	...	...		Actividad n	100%	Entregable n	Noviembre	Responsable n
Hitos/ Actividad	Avance Acumulado	Entregables	Fecha	Responsable																												
Actividad 1	30%	Entregable 1	Marzo	Responsable 1																												
Actividad 2	50%	Entregable 2	Junio	Responsable 2																												
Actividad 3	60%	Entregable 3	Septiembre	Responsable 3																												
...	..	...	...																													
Actividad n	100%	Entregable n	Noviembre	Responsable n																												
Fecha de inicio de la acción	Fecha en la cual comienza la acción de tratamiento; debe contener día mes y año.	01/01/2020																														
Fecha de terminación	Fecha en la cual se da por finalizado la acción de tratamiento; debe contener día mes y año.	31/12/2023																														
Ejecutor	Es la persona responsable del liderazgo o realización de la acción de tratamiento																															

Tabla 8. Elementos de la AT.

Las acciones de tratamiento pueden estar relacionadas con el desarrollo de iniciativas o proyectos, el análisis, diseño o modificación de procesos, la creación de comités, la emisión de directrices o el cumplimiento de actividades de formación o entrenamiento, entre otros. Dependiendo del tipo de acción de tratamiento, se deberán cumplir con los siguientes requisitos mínimos:

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Tipo de acción	Requisitos mínimos
Desarrollo de nuevas tecnologías, proyectos o planes estratégicos relacionados con tecnología, generación de estrategias, modelos y/o casos de negocio.	- Los hitos deben contemplar el paso a producción y estabilización de la tecnología. - Deben existir más de un hito en el año. - Debe contemplar un hito correspondiente a la aprobación de la nueva tecnología, caso de negocio o estrategia. - El beneficio de la acción debe corresponder con el definido para el desarrollo de la nueva tecnología, proyecto, plan o caso de negocio.
Análisis, estudios o diagnósticos.	Podrán ser considerados como acciones de tratamiento, si se incluye dentro de la AT la implementación de las recomendaciones resultantes de dichos análisis.
Cambio de un proceso, modelos, estructura organizacional, roles y responsabilidades.	Su alcance debe contemplar la oficialización e implementación de dicho cambio y que se tenga evidencia de su uso.
Modificaciones a activos de la operación (Implementación nuevas unidades, automatizaciones, adaptaciones, etc.)	- Los hitos deben contemplar el paso a producción y estabilización de la modificación. - Deben existir más de un hito en el año. - Debe contemplar un hito correspondiente a la aprobación de la modificación. - El beneficio de la acción debe corresponder definido en la iniciativa/proyecto.
Emisión o actualización de documentos estratégicos y de despliegue.	Debe contemplar las actividades de construcción y aprobación del documento.
Implementación de estándares, referentes y mejores prácticas.	- Debe contemplar una actividad que evidencie la implementación del estándar /práctica. - Si el estándar es certificable y la compañía así lo determina, una actividad debe estar relacionada con la obtención de dicha certificación.
Creación de comités, grupos de trabajo o similares, o modificación de las funciones existentes en éstos.	- La acción debe contemplar la oficialización de la constitución del comité / grupo o similar y la formalización de las responsabilidades o funciones asignadas. - Se debe contar con la evidencia del funcionamiento de dichos comités (reglamento del comité / acta).
Entrenamientos, capacitaciones y formaciones y demás orientados a fortalecer competencias.	La acción debe contemplar los mecanismos que permitan verificar la apropiación del conocimiento (Ej.: evaluaciones de entrada y salida, certificaciones, informe de resultados de la formación, entre otros).
Implementación de reportes o herramientas para el registro y comunicación de información de la gestión de determinada actividad, dirigido a instancias de revisión y/o aprobación.	- Debe contemplar un hito relacionado con la formalización del reporte y de la periodicidad de presentación. - Debe contemplar un hito asociado con la presentación de al menos dos reportes generados.
Otras actividades del proceso relacionadas con los planes estratégicos del área.	- No deben ser actividades propias del quehacer del proceso. - Deben contemplar hasta la implementación del plan / iniciativa.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Tipo de acción	Requisitos mínimos
	▪ Debe tener beneficios cuantificables.
Otras actividades relacionadas con el diseño de nuevos controles.	▪ Debe contemplar una actividad asociada a la aprobación y formalización del control. ▪ Debe contemplar una actividad asociada a la ejecución del control por lo menos una vez.
Otros mitigantes con efecto demostrable en la probabilidad de ocurrencia o en el impacto del riesgo.	▪ Debe ser algo nuevo, no existente. ▪ No debe ser una actividad de proceso. ▪ Debe reducir la probabilidad o el impacto del riesgo. ▪ No deben ser actividades sistemáticas de revisión, seguimiento o monitoreo.

Tabla 9. Requisitos mínimos de los diferentes tipos de acciones.

Consideraciones generales sobre las acciones de tratamiento:

- La acción de tratamiento puede tener una duración mayor a un año; sin embargo, se debe asegurar que en los años en los cuales se ejecute, tenga hitos intermedios que evidencien su ejecución.
- En los casos que la acción de tratamiento propuesta requiera de la participación de otras áreas diferentes al área responsable del riesgo, su definición deberá ser acordada y aprobada por las partes involucradas.
- Los hitos de las acciones deben ser secuenciales y correlacionados entre sí.

b. Otros mitigantes

Se pueden asociar otros tipos de mitigantes para reducir la probabilidad o el impacto del riesgo, como pólizas de seguro, coberturas, garantías, entre otras, en cuyo caso debe:

- Analizarse el alcance de la cobertura frente al riesgo.
- Validar la vigencia del instrumento, asegurando que al menos cubra por un año.

c. Definición de indicadores clave de riesgo - KRI

Los KRI son herramientas de medición que permiten monitorear, de manera preventiva, el comportamiento de las variables asociadas a los riesgos empresariales, para generar alertas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización.

Para la definición de KRIs, se deben tener en cuenta:

- Las causas documentadas del riesgo empresarial.
- Situaciones que han generado la materialización del riesgo empresarial.
- Factores externos del riesgo empresarial.
- Focos del riesgo.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

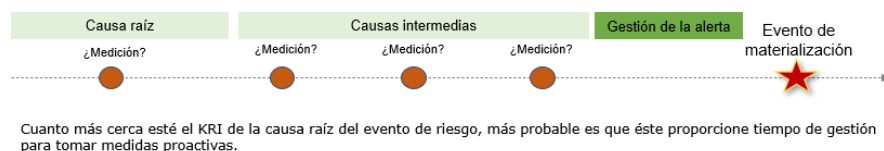


Gráfico 1. Cómo definir un KRI

A partir de los anteriores elementos, se deben identificar las variables o aspectos que pueden ser sujetas de medición y la información necesaria para el diseño del indicador: cómo, cuándo y dónde se obtiene la información de las variables. Una vez validada la disponibilidad de la información que alimenta el indicador, se debe formular un KRI que cumpla con los siguientes criterios:

- El KRI debe ser específico, claro y medible (cuantificable), basado en información disponible, reciente y confiable.
- Debe tener una descripción clara o intención de lo que se va a medir, considerando exclusiones o limitaciones aplicables.
- La fórmula de cálculo del KRI debe contener la ecuación o expresión matemática donde se relacionen las variables y constantes utilizadas para obtener el resultado. Así mismo, deben explicarse las variables que conforman la fórmula.
- Debe tener una tendencia: positiva (cuando el resultado del indicador por encima del límite de alerta indica un mejor comportamiento – no genera alerta) o negativa (cuando el resultado del indicador por debajo del límite de alerta indica un mejor comportamiento – no genera alerta).
- Debe tener un límite, el cual debe ser un valor numérico tolerable para la generación de la alerta que indique el valor máximo (si su tendencia es negativa), o mínimo (si su tendencia es positiva), a partir del cual se considera que la medición estaría en alerta.
- Debe tener una frecuencia de medición específica: semanal, quincenal, mensual, trimestral¹³.
- Debe ser diferente de los indicadores de resultado/desempeño de los objetivos estratégicos de la Compañía. Es decir, no debe ser un KPI del objetivo del proceso directamente relacionado con la temática del riesgo.
- No debe estar relacionado con la verificación de los controles asociados al riesgo en la valoración, ni a la ejecución de las acciones de tratamiento y otros mitigantes planteados para gestionar el riesgo

Todos los riesgos empresariales deben contar con al menos un KRI que permita identificar alertas preventivas sobre el comportamiento del riesgo y su posible materialización.

En todos los casos, las causas de los riesgos empresariales deberán tener acciones de tratamiento, o el mapeo de mitigantes existentes. Las causas externas, no gestionables con controles o acciones de tratamiento, deberán contar con KRIs que monitoreen su comportamiento.

3.4.3 Salidas

- Acciones de tratamiento y otros mitigantes definidos y documentados.
- KRIs definidos para los riesgos empresariales.

¹³ Periodicidades semestrales o anuales no se consideran adecuadas para generar alertas oportunas.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.5 COMUNICACIÓN Y CONSULTA

La comunicación y consulta es ejecutada transversalmente en desarrollo del ciclo de gestión de riesgos empresariales y permite la socialización a todos los involucrados sobre la información generada de los análisis y de los resultados de la gestión de riesgos; y así soportar la toma de decisiones para su adecuada gestión.

La Gerencia Corporativa de Gestión Integrada de Riesgos (o quien haga sus veces) define el esquema de comunicaciones del ciclo de gestión de riesgos empresariales al interior de la compañía, para socializar los resultados de cada etapa del ciclo y asegurar las revisiones por parte de las personas involucradas en la gestión de cada uno de los riesgos empresariales.

3.5.1 Entradas

- Salidas de cada una de las etapas del ciclo de gestión de riesgos empresariales.

3.5.2 Proceso

La comunicación se desarrolla a través de la divulgación de los resultados de la gestión de riesgos empresariales, mediante un esquema de comunicación que debe contener lo siguiente:

- Información a reportar / comunicar.
- Periodicidad.
- Canal de comunicación.
- Emisor y receptor de la información.

Para la comunicación de la gestión de riesgos empresariales, se cuenta con el siguiente esquema:

Información	Periodicidad	Canal de Comunicación	Emisor	Receptor
Propuesta de riesgo empresarial (mapa, fichas, valoración inherente, según aplique)	Cada vez que se requiera la actualización de riesgos empresariales	Sesiones de trabajo / validación con accountables, responsables y participantes del riesgo empresarial. Sesiones de Comité Directivo y/o Exco	GIR (o quien haga sus veces en la compañía)	Nivel directivo y ejecutivo
Validación propuesta de Riesgos Empresariales (mapa, fichas, valoración inherente, según aplique)	Anual o cada vez que se requiera la actualización de riesgos empresariales	Sesión de Comité de Auditoría y Riesgos de Junta Directiva	GIR (o quien haga sus veces en la compañía)	Comité de Auditoría y Riesgos de Junta Directiva

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Información	Periodicidad	Canal de Comunicación	Emisor	Receptor
Aprobación de Riesgos Empresariales (mapa, fichas, valoración inherente, según aplique)	Anual o cada vez que se requiera la actualización de riesgos empresariales	Sesión de Junta Directiva	GIR (o quien haga sus veces en la compañía)	Junta Directiva
Socialización de los riesgos empresariales aprobados	Anual o cada vez que se requiera la actualización de riesgos empresariales	Correo electrónico, o comunicado, o publicación en página web	GIR (o quien haga sus veces en la compañía)	Áreas de la compañía Externos (partes interesadas)
Planeación para definición de medidas de tratamiento y de alerta	Anual o cada vez que se requiera la actualización de riesgos empresariales	Memorando, o comunicado, o correo electrónico	GIR (o quien haga sus veces en la compañía)	Vicepresidencias Accountables / responsables de riesgos empresariales y líderes de riesgos empresariales
Acciones de tratamiento, otros mitigantes y KRIs definidos para la gestión del riesgo. Valoración residual del riesgo empresarial	Anual o cada vez que se requiera la actualización de riesgos empresariales	Correo electrónico, o memorando, o comunicado	GIR (o quien haga sus veces en la compañía)	Áreas responsables del riesgo
Resultados de la gestión del riesgo: ▪ Ejecución de Acciones de tratamiento. ▪ Resultados de KRIs. ▪ Acciones a ejecutar para gestionar alertas presentadas. ▪ Análisis de materializaciones de riesgos. ▪ Acciones a ejecutar frente a las materializaciones.	Mensual	▪ Formato GEE-F-044. ▪ BWISE. ▪ Demás herramientas definidas para el reporte de información.	Líder del riesgo empresarial. Ejecutor de Acción de tratamiento. Responsable del KRI.	GIR (o quien haga sus veces en la compañía)
Información relevante de la gestión de riesgos empresariales (estado de acciones de tratamiento, alertas y materializaciones)	Eventual o de acuerdo con solicitudes de la compañía	Sesión ExCo Sesión Comité de Auditoría y riesgos de Junta Directiva (presentación o documento)	GIR (o quien haga sus veces en la compañía)	Nivel directivo y ejecutivo Comité de Auditoría y Riesgos de Junta Directiva

Tabla 10. Esquema de comunicación.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

3.5.3 Salidas

Salidas de información de cada una de las etapas del ciclo de gestión de riesgos empresariales a sus respectivos receptores.

3.6 SEGUIMIENTO Y REVISIÓN

El objetivo de esta etapa es verificar que los riesgos empresariales identificados, valorados y tratados, se encuentran dentro de los niveles tolerables de la compañía según la RAM, con el fin de retroalimentar el ciclo de riesgos empresariales y tomar acciones que aseguren su adecuada gestión.

El alcance de esta etapa incluye el seguimiento a las acciones de tratamiento, las alertas generadas por medio de los KRIs, las materializaciones de eventos y posibles cambios en el contexto de los riesgos.

3.6.1 Entradas

- Resultado de la valoración de los riesgos empresariales.
- Resultados de las mediciones de los KRIs.
- Eventos materializados.
- Información de la ejecución de las Acciones de Tratamiento.
- Información de cambios externos que puedan incrementar la exposición al riesgo.

3.6.2 Proceso

A continuación, se detallan las actividades a ejecutar para la etapa de seguimiento y revisión:

a. Seguimiento a las Acciones de Tratamiento

Este seguimiento asegura una retroalimentación sistemática del avance de las Acciones de Tratamiento brindando las alertas frente a lo planeado para gestionar el riesgo empresarial.

Para hacer seguimiento de las Acciones de Tratamiento se debe reportar¹⁴: i) el avance real de las acciones de tratamiento, que será un valor porcentual de acuerdo con el cumplimiento de las actividades del Plan de Trabajo; y ii) comentarios o justificaciones que soporten el estado de ejecución de la acción.

El estado de las acciones de tratamiento se definirá según el avance real, el avance planeado, la fecha de inicio y finalización de la siguiente manera:

- **No iniciada/Abierta:** La fecha de inicio no ha ocurrido y la acción no tiene avance asociado.
- **En Ejecución:** La fecha de inicio ya ocurrió, la acción presenta avance igual o superior de acuerdo con el plan de trabajo establecido y la fecha de finalización no ha ocurrido.
- **En Retraso:** La fecha de inicio ya ocurrió y el avance de la acción no alcanzó el nivel planeado para el periodo o la acción no presenta ningún avance registrado, o la fecha de finalización ya ocurrió y la acción no se ha completado.
- **Cerrada / Finalizada:** La fecha de finalización ya ocurrió y el avance de la acción es igual al 100%.
- **Cancelada:** La acción fue suspendida o cancelada antes de lograr el 100% de su avance.

¹⁴ En B Wise para Ecopetrol y en el formato establecido para tal fin en las demás compañías a las que les aplique el presente documento.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

La efectividad de las Acciones de Tratamiento estará determinada por la reducción de la probabilidad de la materialización del riesgo o del impacto de las consecuencias resultantes de su posible materialización.

La efectividad de las acciones de tratamiento deberá establecerse una vez finalice su ejecución mediante la verificación del logro del beneficio planteado para la misma. En caso de no ser efectiva, deberá entenderse que la causa y/o impacto no ha sido gestionado suficientemente y, por tanto, deberá analizarse el riesgo nuevamente dentro del ciclo y contemplar la definición de un nuevo mitigante.

b. Seguimiento a las alertas generadas por medio de los KRIs

Los KRIs deben generar alertas tempranas que conduzcan a reforzar o enfocar la gestión para evitar la materialización del riesgo.

El reporte del KRI debe realizarse en la frecuencia establecida y cumpliendo con los lineamientos de reporte definidos por cada compañía. La información reportada corresponderá a:

- El resultado del cálculo del KRI.
- El estado de alerta o no, de acuerdo con el resultado y los parámetros de diseño definidos (p.ej. unidad de medida, tendencia y límite de alerta).
- El análisis del porqué se generó la alerta y la gestión que se realizará.

La alerta se gestiona de la siguiente forma:

- Cuando el resultado de un KRI se encuentre por fuera de su límite de alerta, se deberá efectuar la revisión de la efectividad de los mitigantes asociados a los riesgos empresariales (cuando aplique); así como evaluar la necesidad de implementar planes de acción alternativos o focalizar el monitoreo a ciertos factores de riesgo, entre otras, a fin de minimizar las posibilidades de tener eventos materializados del riesgo.
- Opcionalmente, analizar el comportamiento de los resultados históricos que permitan: i) visualizar si el KRI se aleja o se acerca a su límite de alerta; ii) identificar tendencias o estacionalidades en sus resultados.
- Sustener sesiones de trabajo (cuando aplique) para analizar los resultados de la medición y su gestión.

c. Eventos materializados de riesgo

Los eventos materializados se entienden como la ocurrencia de los riesgos empresariales cuyas consecuencias pudiesen afectar el logro de los objetivos definidos para la estrategia. Para el análisis de los eventos materializados, se debe documentar la información necesaria en el Formato para la Gestión de Materialización de Riesgos GEE-F-044, o en la herramienta de información¹⁵.

Con esta información se valida la suficiencia en la identificación de riesgos, causas y consecuencias; de igual manera, se verifica la necesidad de ajustar los mitigantes existentes o definir nuevas medidas

¹⁵ El formato GEE-F-044 debe ser aplicado por las compañías a las que les aplique el presente documento, mientras que en Ecopetrol, el registro debe realizarse en la herramienta B Wise o la que se implemente para tal fin.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

de mitigación. Así mismo, la valoración del riesgo empresarial debe ser validada y ajustada según aplique.

Cuando las causas de la materialización son de gestión interna de la compañía, se deben definir acciones para reducir la probabilidad de ocurrencia de un nuevo evento de materialización del riesgo asociado. Cuando las causas de la materialización son de fuentes externas, se deben definir acciones con el fin de reducir el impacto de la materialización del evento.

Igualmente, se debe analizar si se cuenta con un KRI asociado a la causa que generó el evento y si éste presentó las respectivas alertas tempranas. Este análisis queda documentado en el Formato para la Gestión de Materialización de Riesgos, GEE-F-044 o en la herramienta de información²⁵. Si no se emitió ninguna alerta, se deberá revisar y ajustar el diseño del KRI para que refleje mejor las variables que monitorean el riesgo.

A continuación, se describe por cada uno de los elementos asociados a la gestión de los riesgos empresariales el seguimiento a realizar:

Elemento	Alcance del Seguimiento	Análisis	Periodicidad	Entregable	Ejecutor
Eventos materializados de riesgo empresarial	Identificar cualquier evento del riesgo empresarial que haya ocurrido	- Análisis de causas del evento. Tener en cuenta los eventos tipo de materialización contenidos en la descripción del riesgo. - Análisis de las consecuencias de la materialización. - Identificar los cambios aplicables a la valoración del riesgo empresarial. - Realizar seguimiento a las acciones definidas para los eventos materializados. - Establecer si es conveniente adicionar un nuevo foco al riesgo empresarial. - Analizar si el evento materializado tiene efecto sobre otros riesgos empresariales o de proceso (correlación horizontal y vertical). - Analizar si se requiere la definición de mitigantes adicionales o controles en la capa de proceso, que	Seguimiento: Mensual Análisis: Cada vez que ocurra un evento.	Formato para la Gestión de Materialización de Riesgos en el Grupo Ecopetrol - GEE-F-044 y la herramienta de información ²⁵ .	GIR (o quien haga sus veces en la compañía)

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Elemento	Alcance del Seguimiento	Análisis	Periodicidad	Entregable	Ejecutor
		puedan tener impacto en la gestión de los riesgos empresariales.			
Acciones de Tratamiento	Seguimiento al avance de las acciones de tratamiento.	- Comparar el avance real con respecto al avance planeado e identificar posibles desviaciones. - Reportar las desviaciones para su gestión. - Indagar el avance con el ejecutor de la acción de tratamiento (cuando aplique).	Mensual	- Reporte en Bwise o herramienta establecida en la compañía. - Soportes de reuniones o instancias de seguimiento con el líder del riesgo empresarial.	GIR (o quien haga sus veces en la compañía)
	Verificación de efectividad de acciones de tratamiento cerradas.	Medir la efectividad de la acción de tratamiento de acuerdo con lo establecido en este procedimiento.	Cada vez que se cierre una acción de tratamiento.	- Reporte en Bwise o herramienta establecida en la compañía. - Soportes de reuniones o instancias de seguimiento con el líder del riesgo empresarial.	GIR (o quien haga sus veces en la compañía)
KRIs	Monitoreo de los resultados del indicador	- Realizar el análisis del comportamiento del KRI de acuerdo con lo establecido en este procedimiento - Verificar el cumplimiento de las acciones establecidas según los resultados de los KRI en alerta.	Mensual	- Reporte en Bwise o herramienta establecida en la compañía. - Soportes de reuniones o instancias de seguimiento con el líder del riesgo empresarial.	GIR (o quien haga sus veces en la compañía)

Tabla 11. Seguimiento a los elementos del riesgo empresarial.

Producto del seguimiento y revisión de la gestión de riesgos empresariales se debe asegurar:

- El ajuste los riesgos en caso de que haya cambios en sus componentes (nombre, descripción, causas, consecuencias, focos, accountables, mitigantes).

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

- La identificación de nuevas causas de los riesgos, derivadas de cambios en el entorno, en los objetivos estratégicos o de la coyuntura empresarial.
- Las modificaciones a las acciones de tratamiento para incluir mejoras identificadas o para complementarlas en caso de que sean insuficientes o inadecuadas.
- La identificación de eventos de materialización de los riesgos y su documentación para futuras referencias y análisis.

Como parte del seguimiento a la gestión de riesgos empresariales, el Exco (Comité Ejecutivo o quien haga sus veces) conoce los asuntos estratégicos y los riesgos empresariales para monitorear, identificar alertas, solicitar acciones, entre otras y según sea el caso, así como para emitir recomendaciones respecto de las decisiones clave que así lo prevean las matrices de decisiones y atribuciones¹⁶.

3.6.3 Salidas

Considere como salidas de esta etapa los reportes del cuadro anterior.

3.7 REGISTRO E INFORME

Esta etapa se cubre con los resultados de las etapas de *Comunicación y Consulta* y *Seguimiento y Revisión* de acuerdo con la información especificada en cada una de ellas, así como la frecuencia y mecanismos definidos.

4 CONTINGENCIAS

No aplica.

RELACIÓN DE VERSIONES

Documento Anterior			
Versión	Fecha dd/mm/aaaa	Código y Título del Documento	Cambios
Documento Nuevo			
Versión	Fecha dd/mm/aaaa	Cambios	
1	22/05/2019	Creación del documento. Deroga el documento PDO-P-022	
2	11/09/2023	Actualización del documento en alineación con la guía GEE-G-029. Inclusión de roles, responsabilidades y precisión frente a las fases del ciclo de gestión de riesgos. Documento revisado por la Vicepresidencia de Asuntos Corporativos y Secretaría General con el fin de verificar el uso correcto de la terminología y definición del alcance de este documento para las compañías del Grupo Ecopetrol según los criterios previstos en el Modelo de Gobierno Corporativo.	

¹⁶ Reglamento para el Comité Ejecutivo (ExCo) de Alta Dirección GOC-R-001, artículo 9 Funciones.

	Procedimiento para la Gestión de Riesgos Empresariales en el Grupo Ecopetrol		
	Sistema de Gestión Integrado de Riesgos Gerencia Corporativa de Gestión Integrada de Riesgos		
	CODIGO GEE-P-007	Elaborado 11/09/2023	Versión: 2

Para mayor información dirigirse a:

Autor(es): Edna Carolina Vargas.

Buzón: edna.vargas@ecopetrol.com.co

Dependencia: Gerencia Corporativa de Gestión Integrada de Riesgos

Revisado electrónicamente por:	Aprobado electrónicamente por:
ELIO RAMIRO SILVA Profesional de Riesgos y Control Interno C.C 73.196.630 Gerencia Corporativa de Gestión Integrada de Riesgos GERMÁN GONZÁLEZ REYES Vicepresidente de Asuntos Corporativos y Secretaría General C.C. 80.408.313 Vicepresidencia de Asuntos Corporativos y Secretaría General	JOHN ALEXANDER CALDAS MELO Gerente Corporativo de Gestión Integrada de Riesgos Cédula de Ciudadanía No. 79.600.634 Gerencia Corporativa de Gestión Integrada de Riesgos
<i>Documento firmado electrónicamente, de acuerdo con lo establecido en el Decreto 2364 de 2012, por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.</i> <i>Para verificar el cumplimiento de este mecanismo, el sistema genera un reporte electrónico que evidencia la trazabilidad de las acciones de revisión y aprobación por los responsables. Si requiere verificar esta información, solicite dicho reporte a Service Desk.</i>	