TABLA DE CONTENIDO

1. OBJETIVO

Brindar los lineamientos para la aplicación del ciclo de gestión de riesgos a nivel de procesos, con el fin de asegurar la adecuada gestión de estos riesgos y producir información confiable para la toma de decisiones en Ecopetrol S.A. y las compañías del Grupo Ecopetrol que consolidan estados financieros.

2. CONDICIONES GENERALES

Los lineamientos para la Gestión de Riesgos de Procesos son establecidos por la Gerencia Corporativa de Aseguramiento de Control Interno para el cumplimiento de Ecopetrol S.A. y las compañías del Grupo[1]. Estos lineamientos son detallados en este documento y deben ser ejecutados a través del cumplimiento del ciclo para la gestión de riesgos a nivel de procesos[2].

El procedimiento para la gestión de riesgos de proceso está basado en el Ciclo de Gestión de riesgos que resulta común en todas las metodologías y marcos de referencia de la gestión de riesgos y que comprende las etapas de planeación, identificación, valoración, tratamiento, monitoreo y comunicación, como se muestra a continuación:

Figura 1. Ciclo de gestión de riesgos

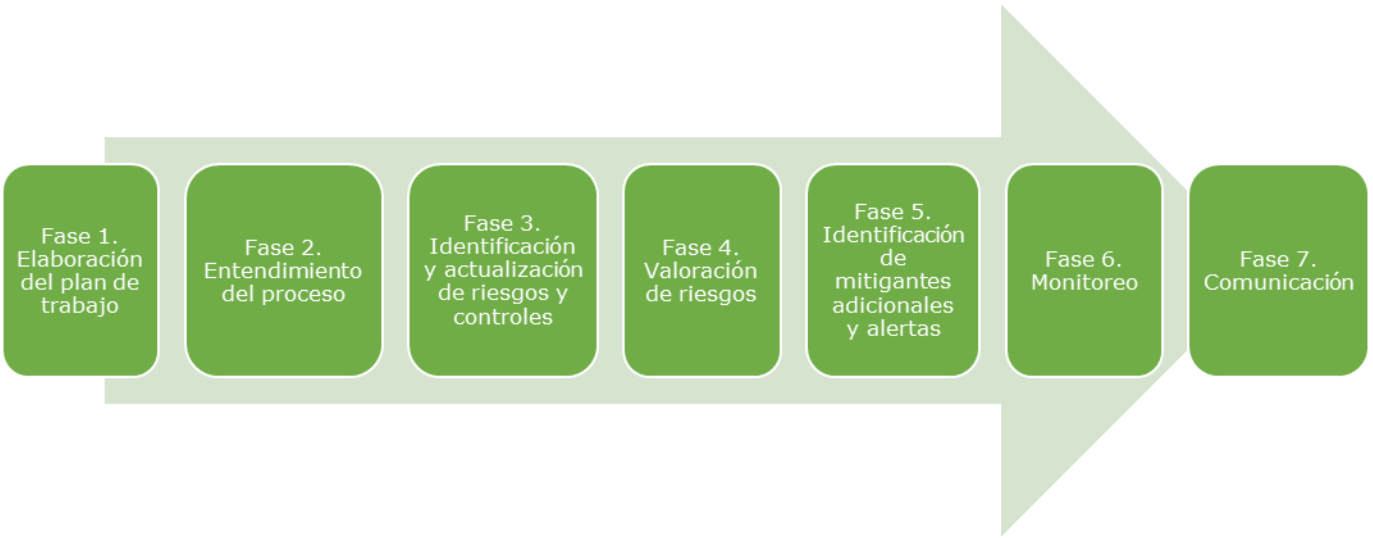
[1] Para las compañías del Grupo se debe considerar su tamaño y realidad operativa.
[2] En el desarrollo de este documento se entenderá por Proceso, todo aquel contenido en el Mapa de procesos oficial de la Compañía, incluyendo los Sistemas de Gestión.

Para efectos de la aplicación del Ciclo de Gestión de Riesgos en Ecopetrol S.A. y su Grupo Empresarial, *Riesgo* es todo evento de ocurrencia incierta que de materializarse genera un impacto negativo[3] en el logro o cumplimiento de los objetivos de la compañía y procesos, y se puede medir en términos de la probabilidad de ocurrencia de las causas y del impacto de las consecuencias.

El éxito de la gestión de riesgos depende de la aplicación de este procedimiento, cuyas actividades deberán realizarse como mínimo con una periodicidad anual.

3. DESARROLLO

El ciclo de gestión de riesgos de proceso se surte mínimo una vez al año y cada vez que se requiera de acuerdo con la naturaleza del proceso, y se cumple a través de las siguientes fases:



3.1 FASE 1 - ELABORACIÓN DEL PLAN DE TRABAJO

Se requiere elaborar un plan de trabajo anual con actividades anuales y recurrentes que aseguren la adecuada gestión de riesgos de proceso, con el fin de definir el alcance, los recursos, tiempo, lineamientos y herramientas requeridos para desarrollar las actividades propias de la gestión de riesgos de proceso.

[3] El ámbito positivo del riesgo, es desarrollado a través de los procesos de definición de la estrategia, en el análisis de aprovechamiento de oportunidades para el logro de las metas de negocio o procesos.

3.1.a **Entradas**

- *Información del Proceso*: Mapa de procesos, objetivo y alcance del proceso bajo análisis, flujos de actividades de los subprocesos, interacciones y atributos (entradas, salidas, documentos, indicadores, entre otros).

- *Lecciones Aprendidas*: Experiencias, evaluaciones y oportunidades de mejora detectadas en la aplicación previa del Ciclo de Gestión de Riesgos.

- *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, entre otros.

3.1.b **Proceso**

Con base en el cronograma diseñado por la Gerencia Corporativa de Aseguramiento de Control Interno de Ecopetrol S.A., cada área/compañía debe definir un plan de trabajo enmarcado dentro de las fechas dadas.

Las actividades de este plan deben estar alineadas con las actividades descritas en este procedimiento, y deben contar con el(los) responsable(s), fecha de inicio y fecha de finalización, entregables, recursos requeridos, herramientas para definir cómo se registra y analiza la información en cada una de las etapas, definición de cómo se realizará la divulgación de los resultados a las partes interesadas, internas y externas, entre otros.

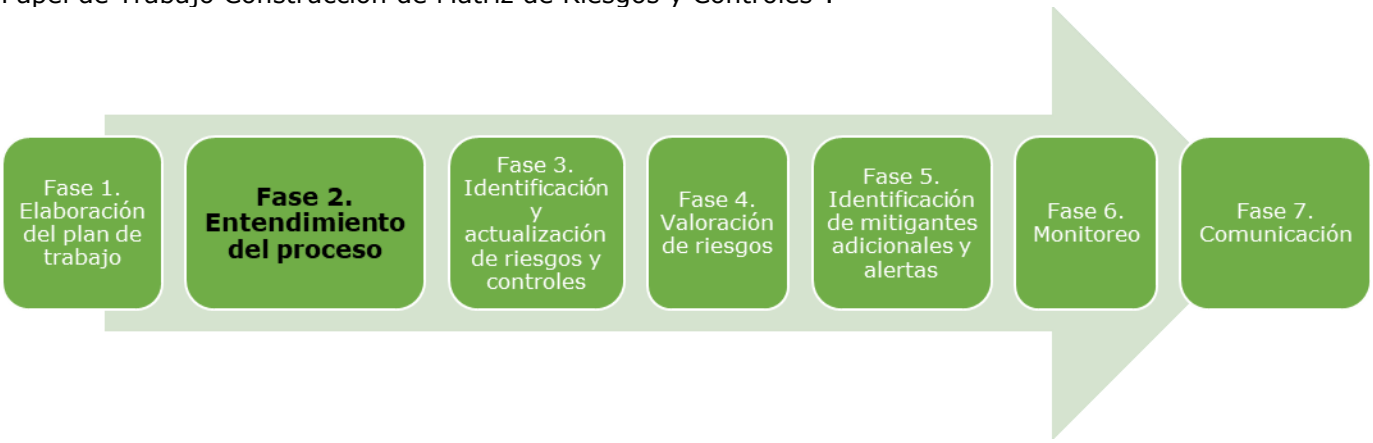
Dentro de la definición de los integrantes del equipo de trabajo se debe contar con personal experto en las diferentes temáticas para asegurar la identificación de los riesgos, medidas de mitigación y alarmas de riesgo con el suficiente detalle. El equipo de trabajo necesariamente debe incluir a los dueños de proceso, expertos técnicos y un profesional en Riesgos y Control Interno o quien haga sus veces en las compañías.

3.1.c **Salidas**

Al terminar esta fase, se debe contar con un plan de trabajo anual de gestión de riesgos para cada proceso de Ecopetrol y para cada compañía, en los formatos definidos para tal fin, el cual debe ser divulgado con antelación y cada vez que se requiera, a los participantes del ciclo de gestión de riesgos en el (las) área(s) involucradas.

3.2 FASE 2 - ENTENDIMIENTO DEL PROCESO

Cada vez que se requiera identificar, documentar y gestionar los riesgos y sus medidas de mitigación y alarmas, es necesario que se realice previamente un análisis del proceso que será sujeto de revisión, a fin de comprender en detalle las actividades, interacciones, resultados y demás información relevante para el ejercicio. Para documentar este ejercicio, se debe diligenciar el formato GEE-F-043 "Formato Papel de Trabajo Construcción de Matriz de Riesgos y Controles".



3.2.a **Entradas**

- *Información del Proceso*: Descripción del proceso y objetivos, forma de operar del proceso, alcance y limitaciones del alcance del proceso frente al objetivo del mismo, cambios reales o potenciales en el diseño del proceso (transición), actividades, interacciones internas o externas, roles y responsabilidades, entregables, transacciones, información y sistemas de información del proceso, eventos o situaciones que pueden causar fallas en el proceso, fallas presentadas dentro de la operación y alcance del proceso, terceros relevantes del proceso, relación de cuentas significativas a procesos, entre otros.

- *Información de los objetivos*: Objetivos de proceso y objetivos estratégicos asociados al proceso (tomados de los Tableros Balanceados de Gestión –TBG- de las áreas relacionadas con el proceso), partes involucradas para el cumplimiento del objetivo, forma de medición del cumplimiento del objetivo, factores críticos de éxito para lograr el objetivo, insumos críticos para el desempeño del proceso, entre otros.

3.2.b **Proceso**

Realizar el entendimiento de la secuencia lógica del proceso, la información relacionada con el funcionamiento del mismo: ¿Qué hace el proceso? ¿Para qué? ¿Con qué procesos interactúa? ¿Cuáles son los principales entregables? Entre otros.

Revise la forma de operar el proceso, realice el entendimiento de sus objetivos y alcance, sus entradas, actividades de transformación y sus salidas. Así mismo, se deben identificar sus interacciones con otros procesos y demás datos de entrada del numeral 3.2.a, y frente a este entendimiento, analizar como mínimo:

- Si el proceso ha tenido cambios significativos con impacto en el sistema de control interno (por ejemplo: Alcance, roles y responsabilidades, actividades críticas, transacciones financieras, sistemas de información, entre otros).
- Si presenta limitaciones en su alcance con respecto a los objetivos de los mismos. En caso de presentar limitaciones de alcance, estas deben ser claramente documentadas en el ejercicio de entendimiento del proceso.
- Qué eventos o situaciones internas o del entorno, potenciales o reales se presentan causando posibles fallas en el proceso.
- Qué situaciones del proceso conllevaron a tener asuntos identificados en autoevaluaciones, monitoreos preventivos, pruebas de la gerencia y otras auditorías, considerando particularmente las situaciones recurrentes y al menos los asuntos detectados en el semestre anterior al análisis efectuado.
- La identificación[4] de los terceros relevantes que interactúan en el mismo (contratistas que presten servicios relevantes que formen parte de los procesos, cuya ejecución pudiera afectar el Sistema de Control Interno).
- La asociación al proceso de transacciones y cuentas significativas de los estados financieros con base en las definiciones de cuentas y procesos significativos que realiza la Gerencia Corporativa de Aseguramiento de Control Interno de forma anual.
- La identificación de los sistemas de información críticos y relevantes para la ejecución y desempeño del proceso.
- La alineación de los objetivos del proceso y su alcance con los objetivos estratégicos del (los) TBG(s) de las áreas que se relacionan con el proceso sujeto de análisis.
- La forma de medición del cumplimiento de los objetivos y los factores críticos de éxito para lograr el objetivo.
- La segregación de funciones de las actividades, roles y responsabilidades y sistemas de información relacionadas con el proceso.

3.2.c **Salidas**

Al finalizar esta fase, se debe tener un entendimiento suficiente del proceso para realizar el análisis de riesgos y controles. De igual forma se debe conocer el panorama completo de objetivos (estratégicos y del proceso) relacionados con el alcance de la matriz de riesgos y controles.

[4] Para la identificación de terceros relevantes (Organizaciones Prestadoras de Servicios OPS) diligencie el GEE-F-043 "Formato Papel de Trabajo Construcción de Matriz de Riesgos y Controles"

3.3 FASE 3 - IDENTIFICACIÓN Y ACTUALIZACIÓN DE RIESGOS Y CONTROLES

La identificación de riesgos permite, en una forma sistemática y estructurada, determinar los eventos que pueden afectar negativamente los objetivos (estratégicos, operacionales, de reporte, de cumplimiento) del proceso. Estos eventos deben ser considerados, bien sea que se encuentren o no bajo el control de la organización. Así mismo, la asociación y actualización de controles permite realizar un ejercicio de valoración y tratamiento más aproximado a la realidad operativa del proceso.

3.3.a **Entradas**

- *Información del proceso*: Mapa de Procesos vigente; resultados del entendimiento del proceso efectuado.

- *Información de los objetivos*: Alineación de objetivos del proceso y objetivos estratégicos de los TBG de las áreas asociadas al proceso y sus indicadores, resultados de indicadores de objetivos estratégicos y de proceso del periodo anterior, factores de entorno que puedan afectar el logro de los objetivos.

- *Información de los riesgos y medidas de mitigación*: Matriz de riesgos y controles de los procesos[5], matriz de despliegue de Riesgos Empresariales en procesos vigente, reporte de eventos materializados actualizado, resultados recientes de autoevaluaciones, hallazgos de pruebas de la gerencia, resultados de asuntos detectados en el último semestre de monitoreos preventivos y auditorías internas y externas con afectación a la matriz de riesgos y controles, y los lineamientos para la identificación y documentación de riesgos y controles de proceso vigentes.

- *Otros:* Resultados organizacionales, cambios regulatorios, cambios tecnológicos, iniciativas o proyectos en curso, entre otros que pueden influir en la gestión de riesgos del

[5] Si se cuenta con Matriz de Riesgos y Controles Transversales y de Múltiples Ejecutores, se debe considerar en el ejercicio.

proceso/compañía, normativas que impacten el diseño de riesgos y medidas de mitigación (p.e. ISO 37001 – Sistema de Gestión Antisoborno).

3.3.b **Proceso**

a. IDENTIFICACIÓN/ACTUALIZACIÓN DE RIESGOS

Para procesos nuevos o procesos que presenten cambios significativos de tal forma que se deba realizar un nuevo ejercicio de gestión de riesgos, se deben identificar los riesgos que puedan impactar el logro de los objetivos previamente analizados.

Por el contrario, si se trata de un ejercicio de actualización, se debe partir de los riesgos previamente identificados y verificar su vigencia y suficiencia frente al cubrimiento de los objetivos del proceso.

En ambos casos el uso del formato GEE-F-043 "Formato Papel de Trabajo Construcción de Matriz de Riesgos y Controles" es requerido para garantizar la trazabilidad del ejercicio[6].

b. DEFINICIÓN DE RIESGOS

Los riesgos deben definirse mediante tres elementos: Evento, causas y consecuencias[7].

*Definir el Evento***:** El evento se debe redactar como aquella situación que de materializarse, genera un impacto negativo en el logro o cumplimiento de los objetivos de los procesos. Para identificarlos tome el objetivo analizado y pregúntese qué situación podría ocurrir que haga que su cumplimiento se desvíe. Éste no se debe redactar como la negación del objetivo, ni como la no gestión de las actividades del proceso. Por eso, evite utilizar términos como "Inadecuado, Insuficiente, No asegurar".

*Establecer las Causas***:** Hace referencia a ¿por qué podría ocurrir dicho evento? Se debe realizar el análisis de las causas directas, sean internas y del entorno que dan origen al evento, incluyendo las que son gestionadas directamente dentro del alcance del proceso y las que no, teniendo en cuenta que es sobre estas causas que se establecerán las medidas de mitigación del riesgo (Controles o acciones de tratamiento), por lo tanto estas deben ser concretas y coherentes.

*Establecer las Consecuencias***:** Hace referencia a ¿cuál sería el impacto de la materialización del evento de riesgo sobre los recursos (personas, ambiente, económico, reputación, entre otros)?
Se deben determinar las consecuencias directas.

La definición de riesgos se puede realizar utilizando las siguientes técnicas:

- Lluvia de ideas: Consiste en reunir al equipo de trabajo definido, para que cada participante exponga lo que considera puedan ser los riesgos que afectan los objetivos del proceso, seguido de un análisis y consolidación.

[6] Para Ecopetrol se debe documentar la hoja de identificación de este formato. Para las compañías aplica el formato desarrollado por cada compañía para este fin.
[7] Para la definición de los riesgos de cumplimiento, consulte el Anexo 3 de este documento.

- Encuestas: Consiste en aplicar cuestionarios de preguntas abiertas o una lista de chequeo de riesgos previamente identificados. Es práctico cuando el equipo de trabajo es numeroso o disperso y se dificulte aplicar otras técnicas.

- Entrevistas: Consiste en un diálogo estructurado a través de preguntas y respuestas. Tiene la ventaja de que se accede a la opinión de un experto con disponibilidad restringida u obtener mayor calidad al no estar sesgado por una sesión grupal. En la entrevista se busca conocer las opiniones con respecto a los riegos del proceso. Es útil para obtener información de primera mano de los expertos.

- Otras herramientas: Alternativas como listado de riesgos tipo por negocio, técnicas de diagramación (causa-efecto, espina de pescado, diagramas de influencia), análisis DOFA, técnica Delphi, entre otras.

Aunque las técnicas de identificación no garantizan por sí mismas una identificación absoluta, se debe hacer un análisis de suficiencia de los riesgos identificados en función de los objetivos y alcance del proceso.

Para ello, la identificación o actualización de los riesgos deberá considerar que:

- Los riesgos sean significativos en su posible afectación al logro del objetivo.
- Un riesgo puede estar asociado a varios objetivos.
- Los riesgos deben ser suficientes para cubrir el alcance del objetivo del proceso.
- Se tengan definidas únicamente las causas directas del evento del riesgo (no la causa de la causa).
- Siempre se incluyan las causas internas y externas aplicables al proceso.
- Se contemplen y subsanen las observaciones en relación a los riesgos de proceso derivadas de autoevaluaciones, monitoreos, pruebas de la gerencia y otras auditorías internas y externas.
- Se cubran todos los objetivos (estratégicos, operacionales, de reporte, cumplimiento) de los procesos y cubren la operación del proceso para aquellos casos en los que se identificaron limitaciones del alcance del proceso frente a los objetivos.
- Se incluyan los riesgos empresariales según la matriz de riesgos empresariales versus procesos[8]
- Se incluyan los factores de riesgo de soborno, de acuerdo con la norma ISO 37000.
- Si el riesgo es del alcance de otro proceso, éste debe ser incluido en la matriz del proceso que corresponda.
- Se deben determinar los puntos del proceso en donde hay riesgos no identificados que pueden impactar la operación normal y el cumplimiento de los objetivos del mismo y que no hayan sido evidenciados en los pasos anteriores.
- Se consideran los eventos de los riesgos empresariales que puedan impactar los objetivos del proceso analizado.
- En caso de que el proceso sujeto de análisis presente limitaciones en su diseño o alcance (existen diferencias entre lo que está escrito y lo que se hace en el proceso, no tenga suficiencia de actividades diseñadas o documentadas, no tenga suficiencia entre sus interacciones con otros procesos, se encuentre en proceso de documentación o cambio/transición, entre otros) asegúrese de identificar los riesgos que tengan alcance

[8] Si la compañía ha desarrollado la relación entre los riesgos empresariales y los riesgos de proceso.

suficiente de manera que se dé cobertura a todo el hacer del proceso, independientemente del estatus de diseño en el que éste se encuentre.

c. CATEGORIZACIÓN DE RIESGOS

Los riesgos identificados deberán ser clasificados de acuerdo con la categoría del evento del mismo, según los siguientes criterios:

- **Estratégico**: Riesgo asociado a los objetivos estratégicos del área o de la compañía, o aquellos riesgos identificados según la matriz de riesgos empresariales versus procesos.
- **Financiero:** Riesgo cuya materialización impacta directamente la confiablidad y razonabilidad de las cifras de los estados financieros.
- **Cumplimiento**: Riesgo asociado al incumplimiento de las leyes y normas aplicables a la compañía, con énfasis en fraude, apropiación indebida de activos, corrupción, soborno, reportes fraudulentos, lavado de activos, financiación del terrorismo, FCPA.
- **Operacional:** Riesgos relacionados directamente con el hacer del proceso, por causas internas o externas.

Las categorías no son excluyentes entre sí, de manera que un riesgo puede ser categorizado en una o más categorías.

d. IDENTIFICACIÓN / ACTUALIZACIÓN DE CONTROLES Y OTROS MITIGANTES

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

Para un proceso cuyos riesgos están recientemente establecidos se debe realizar un ejercicio nuevo de identificación de controles, partiendo de las causas de los riesgos identificados.

Para un ejercicio de actualización, se debe partir de los controles previamente establecidos y verificar su vigencia y suficiencia frente al cubrimiento de los riesgos del proceso. Esto se realiza alineando primero las causas directas del riesgo con los controles existentes.

En ambos casos el uso del formato GEE-F-043 "Formato Papel de Trabajo Construcción de Matriz de Riesgos y Controles" es requerido para garantizar la trazabilidad del ejercicio.

e. DEFINICIÓN DE CONTROLES Y OTROS MITIGANTES

La definición de controles y acciones de tratamiento deberá efectuarse conforme con lo establecido en el "Procedimiento de gestión de controles y medidas de mitigación", GEE-P-006.

Un mitigante existente debe ser modificado, entre otros, cuando:

- No está alineado con las causas directas del riesgo asociado.
- Existen cambios en la operatividad del mitigante o del proceso asociado.
- No mitiga la causa asociada.
- Existen recomendaciones derivadas autoevaluaciones, monitoreos, pruebas de la gerencia y otras auditorías internas y externas sobre su diseño/operatividad.
- La acción de mitigación no se ejecutó o no es efectiva.
- Hayan cambios en el alcance, responsables, fechas de inicio o finalización, de la acción de mitigación.

Se debe tener en cuenta que para los mitigantes existentes que sean actualizados, también deben ser actualizados sus atributos para garantizar su coherencia. Esto es, analizar si la modificación de la acción de mitigación ocasiona cambios en el ejecutor, frecuencia, tipo, clasificación, entre otros aplicables.

3.3.c **Salidas**

Al finalizar esta etapa se debe tener el Formato del formato GEE-F-043 "Formato Papel de Trabajo Construcción de Matriz de Riesgos y Controles" con los riesgos asociados a los objetivos del proceso, y los controles y otros mitigantes correspondientes a los riesgos tratados, previamente validado por los dueños de proceso.

3.4 FASE 4 - VALORACIÓN DE RIESGOS

La valoración de riesgos obedece a un análisis semi-cuantitativo que busca priorizar los riesgos asignándole a éstos valores dentro de escalas o rangos predefinidos de probabilidad e impacto.

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 estimación de la probabilidad de ocurrencia del evento y el impacto de sus consecuencias sobre los recursos (personas, ambiente, económico, reputación, clientes, entre otros[9]).

[9] Según se defina para cada una de las compañías.

El ejercicio de valoración se realiza a partir de los riesgos identificados, documentándolo en el Formato de Valoración de Riesgos definido para tal fin[10] en el cual se debe registrar el resultado de la valoración y considerando dos instancias principales: La valoración inherente y la valoración residual, como se ilustra en la siguiente figura:

Figura 2. Valoración Inherente y Residual

3.4.a **Entradas**

- *Información de riesgos y medidas de mitigación*: Definición de apetito al riesgo (plasmado en la Matriz de valoración de riesgos - RAM de la compañía), formato de valoración de riesgos, matriz de riesgos y controles de los procesos, matriz de riesgos y controles transversales y de múltiples ejecutores[11], resultados de las acciones de tratamiento y resultados de indicadores claves de riesgo (KRI's) del último año, relación de cuentas significativas a procesos.

- *Información resultado de la gestión de riesgos y controles*: Análisis de autoevaluaciones, resultados de las pruebas de controles efectuadas a través de los monitoreos preventivos, hallazgos de Pruebas de la Gerencia y auditorías internas y externas, realizadas a los procesos.

- *Otros*: Información de contexto y entorno relacionada con los riesgos del proceso, tal como proyección de cambios regulatorios, cambios tecnológicos, iniciativas o proyectos en curso, entre otros, información histórica de incidentes o riesgos 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 compañía, así no se encuentren registrados en bases de datos formales).

3.4.b **Proceso**[12]

La valoración de riesgos se realiza durante la ejecución del ciclo y deberá al menos, revisarse y de ser necesario volver a ejecutarse cada vez que ocurra un evento materializado de riesgo, cuando se

[10] El formato SCI-F-005 aplica para la valoración de riesgos de procesos en Ecopetrol S.A. Las compañías que tengan más o menos recursos o descriptores, deberán hacer la correspondiente adaptación de dicho formato.
[11] Si se cuenta con Matriz de riesgos y controles Transversales y de Múltiples Ejecutores, se debe considerar en el ejercicio.
[12] Para Ecopetrol S.A. se debe implementar el formato Matriz de Valoración de riesgos, SCI-F-005.

presenten fallas de control, cuando las acciones de tratamiento asociadas resulten inefectivas o sean canceladas, y cuando los mitigantes no sean suficientes.

a. VALORACIÓN INHERENTE

La valoración inherente es la valoración del riesgo a partir de la medición de la probabilidad e impacto sin tener en cuenta el efecto de los mitigantes.

Para realizar la estimación de la probabilidad, a partir de los descriptores de probabilidad definidos en la matriz RAM de la compañía, se debe identificar el nivel de probabilidad de que el riesgo se materialice.

Para esto, se debe analizar la información histórica de eventos materializados o estadísticas del riesgo a valorar que se hayan presentado en el sector, la compañía o el proceso, 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 impactos de su materialización sobre el logro de los objetivos asociados.

La situación definida debe ser delimitada por datos numéricos, para facilitar y precisar el valor del escenario. A partir de lo anterior, se documenta el escenario o situación con base en la cual se realizará la valoración inherente del riesgo, 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 conjuntamente con los dueños de proceso, gerentes, o jefes del área relacionada con el riesgo en estudio, para garantizar que el escenario corresponda a situaciones críticas según criterio de experto del proceso.

Si se cuenta con información para la construcción de escenarios tanto hipotéticos como reales, se debe dar prelación al escenario real, siempre y cuando este provea información suficiente para efectuar el ejercicio de valoración.

Partiendo del escenario de valoración definido, se debe seleccionar 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 de la matriz RAM (Personas, Ambiente, Recursos Económicos, Reputación, Clientes, de acuerdo con lo definido en la Matriz de Valoración de la Compañía) según el impacto que éstos generen, teniendo en cuenta los efectos directos sobre los recursos de esta matriz. Para ello identifique de los descriptores, el que mejor refleje el impacto del escenario, calificando cada una de las variables aplicables según el escenario.

La valoración inherente del riesgo está dada por la combinación de la probabilidad y el impacto más alto.

b. VALORACIÓN RESIDUAL

La valoración residual se entiende como el nivel de riesgo resultante una vez se aplican los mitigantes sobre la probabilidad de ocurrencia e impactos sobre los recursos valorados. 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 de los mismos.

Una vez obtenida la valoración inherente del riesgo, se procede a estimar la valoración residual, en función de la suficiencia y efectividad del conjunto de mitigantes asociados al riesgo (controles y acciones de tratamiento finalizadas con comprobación de efectividad).

La calificación de los controles está dada por los factores de a) suficiencia de los mitigantes, b) clasificación del control, c) tipo de control y d) efectividad del control.

a) *Suficiencia de los mitigantes*: Asocie todos los mitigantes del riesgo y evalúe si los mismos son suficientes para gestionar las causas, según lo establecido en el Procedimiento para la gestión de controles y acciones de tratamiento en el Grupo Ecopetrol, GEE-P-006. Si los controles asociados no son suficientes, se entiende que los mismos no tienen incidencia en la reducción de impacto y probabilidad.

b) *Clasificación de control:* Está basado en la clasificación de los controles preventivos, detectivos o correctivos, según la siguiente asociación:

Control preventivo	Mitiga las causas del riesgo
Control detectivo	Mitiga las causas y/o reduce los impactos del riesgo
Control correctivo	Mitiga o reduce los impactos del riesgo

c) *Tipo de control*: Se debe indicar si el control es automático, manual, o manual dependiente de TI, de conformidad a lo que se haya definido en la matriz de riesgos y controles.

d) *Efectividad del control*: Para establecer la efectividad para cada uno de los controles con base en los resultados obtenidos en Revisoría Fiscal, pruebas de la gerencia, autoevaluaciones de control interno y monitoreos preventivos de control interno y auditorías, indicando si la inefectividad corresponde a operatividad o diseño.

A partir de la combinación de los factores anteriores, se asigna un puntaje de máximo 100 puntos posibles para cada control asociado de acuerdo con la siguiente estructura:

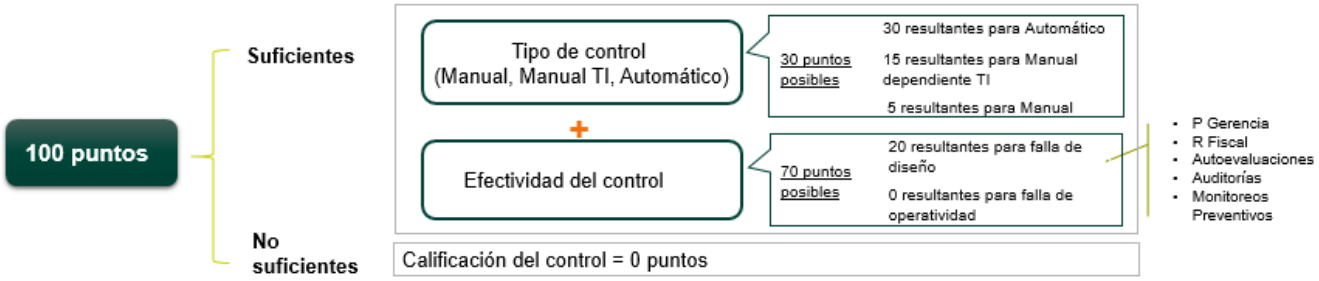


Figura 3. Esquema de puntuación de controles

La calificación resultante determinará si el control es débil, moderado o fuerte:

- Control fuerte: Control con asignación de 90 puntos en adelante.
- Control moderado: Control con asignación entre 75 y 89 puntos.
- Control débil: Control con 74 puntos o menos.

Para evaluar el control partiendo de la calificación o puntaje obtenido, se debe analizar en qué medida éste gestiona la probabilidad o el impacto del riesgo, teniendo en cuenta que:

- Un control disminuye la probabilidad directamente si la actividad de control gestiona directamente la causa asociada al riesgo.
- Un control no disminuye la probabilidad si la actividad de control no mitiga la causa del riesgo.
- Un control disminuye el impacto directamente si la actividad de control está encaminada a disminuir directamente uno o más de los impactos del riesgo.
- Un control disminuye el impacto indirectamente si la actividad de control puede disminuir en cierta medida uno de los impactos del riesgo en caso de materialización.
- Un control no disminuye el impacto si la actividad de control no reduce el impacto del riesgo.

Finalmente, según la evaluación realizada para cada control, se debe identificar nivel de desplazamiento del riesgo inherente en función del número de columnas y filas de acuerdo con la siguiente tabla:

Calificación del control	Ayuda a disminuir la probabilidad	Ayuda a disminuir el impacto	# Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	# Columnas en la matriz de riesgo que se desplaza en el eje del impacto
Fuerte	directamente	directamente	2	2
Fuerte	directamente	indirectamente	2	1
Fuerte	directamente	no disminuye	2	0
Fuerte	no disminuye	directamente	0	2
Moderado	directamente	directamente	1	1
Moderado	directamente	indirectamente	1	0
Moderado	directamente	no disminuye	1	0
Moderado	no disminuye	directamente	0	1

En resumen, el desplazamiento del riesgo inherente en el mapa de calor o en la matriz RAM dependerá del promedio de los niveles de probabilidad y e impacto resultantes de la aplicación del análisis anterior a cada control, obteniendo así el riesgo residual.

NOTA: Se debe tener en cuenta que si el control que se está calificando es nuevo, obedeciendo al reemplazo de un control racionalizado sobre el cual se hayan identificado fallas en los ejercicios de monitoreo (auditorías internas o externas, pruebas de la Gerencia, autoevaluaciones de control interno, entre otros), el mismo debe tener la calificación de inefectividad del control anterior hasta que éste opere y se evalúe su efectividad, momento en el cual se deberá revisar la valoración de los riesgos asociados.

3.4.c **Salidas**

Al finalizar esta etapa se debe tener la valoración inherente y residual de los riesgos identificados en los formatos definidos para tal fin, en los niveles VH (Very High – Muy alto); H (High – Alto); M (Medium – Medio); L (Low – Bajo) y N (Null – Muy bajo) de acuerdo con la matriz RAM de la compañía, y aprobados por el dueño de proceso correspondiente.

3.5 FASE 5 - DEFINICIÓN DE MITIGANTES ADICIONALES Y ALERTAS DE RIESGO

En esta etapa se definen las actividades adicionales de mitigación (controles o acciones de tratamiento) con las que se busca prevenir las causas o protegerse de las consecuencias para aquellos riesgos cuya valoración residual sea "Very High", "High" y "Medium[13]", a través del análisis de las causas identificadas y la efectividad de todos los mitigantes asociados, con el fin de seleccionar la opción adecuada entre actividades de control y acciones de tratamiento, económicamente viables para llevar el riesgo residual a una valoración de riesgo aceptable ("Low" o "Null").

Si la valoración del riesgo residual es "Medium" los mitigantes adicionales son opcionales a decisión y juicio del dueño de proceso, excepto para los siguientes casos:

- Cuando los controles asociados al riesgo han tenido hallazgos de diseño y operatividad detectados mediante autoevaluaciones, pruebas de la gerencia, Revisoría Fiscal o monitoreos preventivos en el último año.
- El riesgo es de categoría estratégica.

También se definen las alertas de riesgo o KRI (Indicador Clave de Riesgo – Key Risk Indicator) como herramientas de medición que permite monitorear, de manera preventiva, el comportamiento de las variables asociadas a las causas de los riesgos, para indicar cambios en el nivel de exposición a los riesgos, generando alertas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización. Los KRIs deben identificarse para aquellos riesgos con valoración residual "Very High" y "High" y con alineación directa con los objetivos estratégicos asociados al proceso.

[13] De acuerdo con los niveles de las matrices RAM de cada compañía.

3.5.a **Entradas**

- *Información de riesgos y medidas de mitigación*: Resultados del ejercicio de valoración de riesgos, matriz de riesgos y controles de los procesos, matriz de riesgos y controles transversales y de múltiples ejecutores[14], informes de auditorías internas o externas realizadas al proceso analizado, los cuales pueden ser un insumo para determinar las nuevas medidas de mitigación, reporte de eventos materializados actualizado, entre otros.

3.5.b **Proceso[15]**

a. IDENTIFICACIÓN DE NUEVAS MEDIDAS DE MITIGACIÓN

Se debe establecer la medida de mitigación más adecuada entre actividades de control y acciones de tratamiento (ATs) económicamente viables de acuerdo con las siguientes opciones:

- Actividades de Control: Se formulan o redefinen controles para mitigar las causas a través de una actividad sistemática y recurrente dentro del proceso analizado.

- Acciones de Tratamiento: Si la causa del riesgo no se puede gestionar con una actividad de control recurrente, en este caso se debe crear una acción de tratamiento.

- Controles Transversales: Si la causa se puede mitigar a través de una actividad sistemática y recurrente a ser ejecutada por todas las áreas de la empresa, se debe generar junto con el proceso Gobierno, el mitigante transversal.

[14] Si se cuenta con Matriz de Riesgos y Controles Transversales y de Múltiples Ejecutores, se debe considerar en el ejercicio.
[15] Los lineamientos para la construcción de controles y acciones de tratamiento deben ser consultados en el "Procedimiento de gestión de controles y medidas de mitigación", GEE-P-006.

- Controles de Múltiples Ejecutores: Si la causa se puede mitigar a través de una actividad sistemática y recurrente a ser ejecutada por algunas áreas de la empresa, se debe generar junto con el proceso Gobierno el mitigante de múltiples ejecutores.

b. DEFINICIÓN DE KRI[16]

Para la definición de alertas o KRIs, se debe seleccionar:

- Las causas documentadas del riesgo que tengan la mayor probabilidad de ocurrencia[17].
- Las causas que han generado la materialización del riesgo (cuando aplique).

De las anteriores causas seleccionadas, tome al menos una e identifique cuáles son las variables que pueden ser sujetas de medición y se debe determinar qué información es necesaria para el diseño del indicador (cómo, cuándo y dónde se obtiene la información de la variable). Una vez validada la disponibilidad de la información asociada, formule un KRI que cumpla con los criterios definidos en este documento.

Tenga en cuenta que un KRI:

- Debe ser específico y claro, 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.

- 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, indicando un buen comportamiento cuando el resultado del KRI es menor al límite de alerta) o un valor mínimo (si su tendencia es positiva, indicando un buen comportamiento cuando el resultado del KRI es mayor al límite de alerta).

- Debe tener una frecuencia de medición específica: semanal, mensual, trimestral. Para la definición de esta frecuencia se debe tener en cuenta el ciclo de la información o datos de entrada así como la oportunidad en la generación de la alerta.

- Debe ser diferente a los indicadores de resultado de los objetivos del mapa estratégico de la Compañía y de los indicadores del proceso, pero puede ser un indicador de medio, siempre y cuando esté asociado a las causas seleccionadas.

[16] Puede consultar un ejemplo de KRI en los anexos de este documento.
[17] Para determinar cuál causa tiene la mayor probabilidad de ocurrencia, recurra a juicio de expertos.

3.5.c **Salidas**

Al finalizar esta fase se debe tener:

- Medidas de mitigación nuevas o actualizadas (Acciones de tratamiento, actividades de control, Controles Transversales, Controles de Múltiples Ejecutores y Otros Mitigantes) y documentadas.
- KRIs diseñados.

3.6 FASE 6 - MONITOREO DE RIESGOS

El objetivo del monitoreo es verificar que los riesgos identificados, valorados y tratados, se encuentran permanentemente dentro de los límites tolerables de la compañía, con el fin de retroalimentar el ciclo de riesgos y tomar acciones que aseguren una adecuada gestión de los mismos.

El alcance del monitoreo de los riesgos de proceso incluye el seguimiento a las acciones de tratamiento, las alertas generadas por medio de los KRIs, las materializaciones de eventos, y la medición de la efectividad de los controles y acciones de tratamiento a través de las autoevaluaciones, monitoreos preventivos de Control Interno, Pruebas de la Gerencia y auditoría internas y externas, entre otros.

3.6.a **Entradas**

- Matrices de riesgos y controles
- Resultados de la valoración.
- Alarmas de riesgo – KRIs diseñadas
- Eventos materializados del riesgo
- Información de la ejecución de los controles y acciones de tratamiento
- Información de cambios externos que puedan incrementar la exposición al riesgo
- Resultados de las Autoevaluaciones de Control Interno, Pruebas de la Gerencia, Auditorías Internas y Externas.

3.6.b **Proceso**

a. MONITOREO A LAS ACCIONES DE TRATAMIENTO

Este seguimiento[18] asegura una retroalimentación sistemática del avance de las acciones de tratamiento, brindando las alertas frente a lo planeado para gestionar el riesgo y la medición de la efectividad al finalizar su ejecución.

Para hacer el seguimiento de las acciones de tratamiento, el(los) ejecutor(es) de la(s) acción(es) de tratamiento debe reportar: i) el avance real de las acciones de tratamiento, que será un valor porcentual de acuerdo con el cumplimento de las actividades del plan de trabajo y los hitos y fechas definidos, ii) comentarios o justificaciones que soporten el estado de ejecución de la acción, y iii) medición de la efectividad de la acción al cierre de la misma.

El estado de las acciones de tratamiento se debe actualizar periódicamente[19] y se definirá según el avance real, el avance planeado, la fecha de inicio y finalización de la siguiente manera:

- *No iniciada*: La fecha de inicio no ha ocurrido y la acción no tiene avance asociado.
- *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.
- *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*: 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.

La efectividad de la ejecución de las acciones de tratamiento deberá gestionarse de acuerdo con lo establecido en el "Procedimiento de gestión de controles y medidas de mitigación", GEE-P-006. En caso de no ser efectiva, deberá entenderse que el riesgo no ha sido gestionado y por tanto, deberá analizarse el riesgo nuevamente dentro del ciclo y contemplar su incidencia sobre la valoración del riesgo y la definición de mitigantes y alertas del riesgo, según corresponda.

b. MONITOREO DE EVENTOS MATERIALIZADOS DE RIESGO

Los eventos materializados se entienden como la ocurrencia de situaciones cuyas consecuencias afectaron el logro de los objetivos definidos para la estrategia, procesos o proyectos. Para el análisis de los eventos materializados documente como mínimo los siguientes elementos:

- Describa detalladamente el evento materializado
- Fecha de ocurrencia del evento
- Asocie el evento a un riesgo de la matriz
- Determine si la causa del evento estaba identificada en la matriz de riesgos y controles
- Establezca si el evento se originó por personas, procesos o ambiente.

[18] En Ecopetrol, el seguimiento de las acciones de tratamiento se realiza por parte del profesional de la Gerencia de Aseguramiento de Control Interno mensualmente con base en lo reportado por los procesos.
[19] En Ecopetrol, el seguimiento o revisión se realiza en forma mensual, reportando cuando aplique según el plan de trabajo/hitos definidos. En las compañías se realiza según calendario o periodicidad definida por la Gerencia Corporativa de Aseguramiento de Control Interno de Ecopetrol.

- Determine cuál fue el impacto del evento sobre cada uno de los recursos de la compañía (Ej.: personas, ambiente, económico, etc.)
- Identifique el mitigante establecido para la causa que originó el evento
- Analice la operatividad y diseño del mitigante
- Si la causa o el riesgo no estaban identificados previamente, defínalos
- Establezca si el riesgo tiene definido un KRI asociado a la causa que lo materializó
- Identifique si el KRI alertó sobre la posible materialización del evento
- Establezca si el evento ocurrido modifica la valoración actual del riesgo
- Establezca si el evento ocurrido implica modificaciones en los mitigantes
- Documente la acción a ejecutar.

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, y se valida y ajusta la valoración del riesgo. Estos eventos y su análisis deben registrarse en el "Formato para la gestión de materialización de Riesgos", GEE-F-044. Los planes de acción que surjan producto del análisis del evento materializado deberán ser reportados por los responsables de su ejecución y monitoreados por la Gerencia Corporativa de Aseguramiento de Control Interno[20].

c. MONITOREO A LAS ALERTAS GENERADAS POR MEDIO DE LOS KRI

Los KRI pueden alertar sobre cambios en el nivel de exposición y genera alertas tempranas que conducen a reforzar o enfocar la gestión para evitar su materialización.

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

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

El monitoreo se gestiona de la siguiente forma:

- Cuando el resultado de un KRI se encuentre por fuera de su límite de alerta, la Gerencia Corporativa de Aseguramiento de Control Interno deberá efectuar la revisión de la efectividad de los controles y de las acciones de tratamiento asociadas a los riesgos; así como evaluar la necesidad de activar medidas de prevención adicionales, implementar planes de acción alternativos o focalizar el monitoreo a ciertos factores de riesgo, entre otros, a fin de minimizar las posibilidades de tener eventos materializados del riesgo.

- Realizar gráficas del comportamiento de los resultados históricos que permitan visualizar si el KRI se aleja o se acerca a su límite de alarma, para identificar tendencias o estacionalidades en los resultados del KRI (ver anexos). Las gráficas aplican una vez se cuente con dos o más reportes de KRI, de manera que pueda establecerse una tendencia.

[20] En Ecopetrol, el seguimiento o revisión se realiza en forma mensual, reportando cuando aplique según el plan de trabajo/hitos definidos. En las compañías se realiza según calendario o periodicidad definida por la Gerencia Corporativa de Aseguramiento de Control Interno de Ecopetrol.

- Calcular el promedio y el número de veces fuera del límite durante el último año de mediciones, con el fin de analizar los resultados del KRI en el tiempo.

- Cuando se presente un evento materializado, se deberá analizar si se cuenta con un KRI asociado a la causa que generó el evento, y si éste presentó las respectivas alertas tempranas. Documente este análisis en el Formato de Materialización de Riesgos. Si no se emitió ninguna alerta se deberá revisar y ajustar el diseño del KRI para que refleje mejor las variables del riesgo.

d. MONITOREO A LA EFECTIVIDAD DE LOS CONTROLES

El seguimiento de las actividades de control se realiza a través del monitoreo de su diseño y efectividad, que se efectúa como mínimo a través de:

- Autoevaluaciones de Control Interno
- Monitoreos Preventivos de Control Interno
- Pruebas de la Gerencia
- Auditorías Internas y Externas.

La efectividad del diseño y la operatividad de los controles deberán gestionarse de acuerdo con lo establecido en el "Procedimiento de gestión de controles y medidas de mitigación", GEE-P-006.

3.6.c **Salidas**

El resultado de la etapa de monitoreo deberá retroalimentar las etapas de identificación, valoración y tratamiento de los riesgos, dependiendo de los asuntos identificados a través de:

- Reporte del estado de ejecución de las Acciones de Tratamiento
- Resultado de KRIs
- Formato con el análisis de riesgos materializados
- Resultados de autoevaluaciones de Control Interno
- Informes de Monitoreos Preventivos de Control Interno
- Observaciones de Pruebas de la Gerencia
- Observaciones de auditorías internas y externas.

3.7 FASE 7 - COMUNICACIÓN

La comunicación se define como un proceso interactivo de intercambio de información que permite socializar los resultados, compartir datos, opiniones y perspectivas, facilitando el adecuado flujo de información y diálogo entre los interesados o partes involucradas. La comunicación permite que se construya cada etapa del ciclo de gestión de riesgos de manera conjunta con las áreas y procesos de la Compañía.

La comunicación es implementada en cada una de las fases de este procedimiento y debe asegurar:

- Generación de un lenguaje común y cultura en materia de gestión de riesgos.
- Realimentación de la gestión de riesgos a través de la incorporación de los resultados obtenidos de cada una de las fases y la interacción entre las áreas ejecutoras de procesos y el gobierno del Sistema de Control Interno.
- Divulgación de los roles y responsabilidades de los participantes e involucrados.
- Divulgación de la información relevante de la gestión de riesgos de proceso.
- Identificación de sinergias entre las diferentes áreas para robustecer la gestión de los riesgos.
- Incorporación de la gestión de riesgos como variable estratégica para la toma de decisiones.

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

Fase/ Elemento	Entregable	Periodicidad	Canal de Comunicación/ Emisor	Receptor
Elaboración del plan de trabajo	Cronograma	Ecopetrol: Como mínimo anual Subordinadas: Según la guía GEE-G-002	Correo electrónico del dueño del proceso/ Gerente de Cumplimiento de la subordinada	Gerencia Corporativa de Aseguramiento de Control Interno
Identificación y actualización de Riesgos y Controles	Matriz de riesgos y controles	Ecopetrol: Mensual Subordinadas: Según la guía GEE-G-002	Ecopetrol: BWise Subordinadas: Reporte de gestión de riesgos	Gerencia Corporativa de Aseguramiento de Control Interno
Valoración de Riesgos	Formato de valoración de riesgos.	Ecopetrol: Mínimo anual o cuando se requiera Subordinadas: Según la guía GEE-G-002	Correo electrónico del dueño del proceso/ Gerente de Cumplimiento de la subordinada	Gerencia Corporativa de Aseguramiento de Control Interno

Identificación de mitigantes adicionales y alertas de riesgo	Matriz de riesgos y controles	Ecopetrol: Mensual Subordinadas: Según la guía GEE-G-002	Ecopetrol: BWise Subordinadas: Reporte de gestión de riesgos	Gerencia Corporativa de Aseguramiento de Control Interno
Eventos materializados de riesgo	Formato de materialización de riesgos GEE-F-044	Ecopetrol: Cada vez que suceda un evento Subordinadas: Según la guía GEE-G-002	Correo electrónico del dueño del proceso donde se detectó el evento/ Gerente de Cumplimiento de la subordinada	Gerencia Corporativa de Aseguramiento de Control Interno
Acciones de Tratamiento	Reporte de seguimiento/ efectividad en Bwise para Ecopetrol Matriz de riesgos y controles para subordinadas	Ecopetrol: Mensual Y cada vez que se cierre una acción de tratamiento Subordinadas: Según la guía GEE-G-002	Ecopetrol: Bwise / Ejecutor de la acción de tratamiento Subordinadas: Reporte de gestión de riesgos	Gerencia Corporativa de Aseguramiento de Control Interno
Controles	Reporte de: autoevaluaciones, pruebas de la gerencia, monitoreos preventivos, auditoría internas y externas	Autoevaluaciones Trimestral Pruebas de la gerencia, monitoreos preventivos, auditorías internas y externas, cuando se realicen las evaluaciones de controles	Autoevaluaciones: Ecopetrol: Bwise Subordinadas: autoevaluaciones Otros monitoreos: Ecopetrol: Informes de monitoreos Subordinadas: Formato de hallazgos de acuerdo con periodicidad definida	Gerencia Corporativa de Aseguramiento de Control Interno
KRIs	Ecopetrol: Reporte de BWise Subordinadas: Matriz riesgos y controles	Ecopetrol: Mensual Subordinadas: Según la guía GEE-G-002	Ecopetrol: BWise Subordinadas: Formato Gestión de Riesgos	Gerencia Corporativa de Aseguramiento de Control Interno.

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	31/01/2018	Deroga: PDO-P-025 Procedimiento Ciclo Riesgos Procesos PDO-I-027 Instructivo para el diseño y seguimiento a Acciones de Tratamiento PDO-G-039 Guía para el diseño, prueba e implementación de KRIs PDO-I-017 Instructivo de construcción y actualización de matrices integrales de control interno PDO-I-030 Instructivo de valoración de riesgos.
2	05/02/2019	Se incluye el análisis de transacciones y cuentas significativas Se incluye la categorización de riesgos. Deroga el formato GEE-F-045. Se actualiza el capítulo relacionado con valoración de riesgos. Nota: Se publica con esta fecha dado que esta es la fecha de divulgación del documento, que fue utilizado para efectos de la ejecución del ciclo de gestión de riesgos de la vigencia.

Para mayor información dirigirse a:
Autor(es): Edna Carolina Vargas **Teléfono**: 50559 **Buzón:** geraseconint@ecopetrol.com.co **Dependencia:** Gerencia Corporativa de Aseguramiento de Control Interno

Revisado electrónicamente por:	Aprobado electrónicamente por:
ANGÉLICA MARÍA ALAIX M **Profesional** **Cédula de Ciudadanía No. 52.516.825** **Gerencia Corporativa de Aseguramiento de Control Interno** **MÓNICA JIMÉNEZ G.** **Secretaria General** **Cédula de Ciudadanía No. 52.411.766** **Secretaría General & Soporte a Presidencia**	**HELBER ALONSO MELO HERNÉNDEZ** **Gerente Corporativo de Aseguramiento de Control Interno** **Cédula de Ciudadanía No. 79.862.626** **Gerencia Corporativa de Aseguramiento de Control Interno**

*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.*
*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.*

5. ANEXO 1

Ejemplo de un KRI

Objetivo	Riesgo	Causa	KRI
Asegurar el inicio, ejecución, cierre y balance de los contratos	Incumplimiento de las obligaciones pactadas en el contrato	No tomar acciones oportunas frente a las alertas de seguimiento del contrato, solicitudes, pagos, reclamaciones realizadas por el contratista.	Porcentaje de contratos con reclamaciones por presuntos incumplimientos de Ecopetrol

Descripción: Porcentaje de contratos con reclamaciones por presuntos incumplimientos de Ecopetrol. Este KRI monitorea la causa: No tomar acciones oportunas frente a las alertas de seguimiento del contrato, solicitudes, pagos, reclamaciones realizadas por el contratista.

Fórmula: Número de contratos con reclamaciones por presuntos incumplimientos de Ecopetrol en el mes / Número de contratos en ejecución y en cierre y balance.

Frecuencia de medición: Mensual

Unidad de Medida: Porcentaje

Fuente: - Informe nacional consolidado pestaña reclamaciones del mes.
- Reporte de contratación SAP oficial TODAS LAS SOCIEDADES

Límite de alerta: 0,15% (valor máximo)

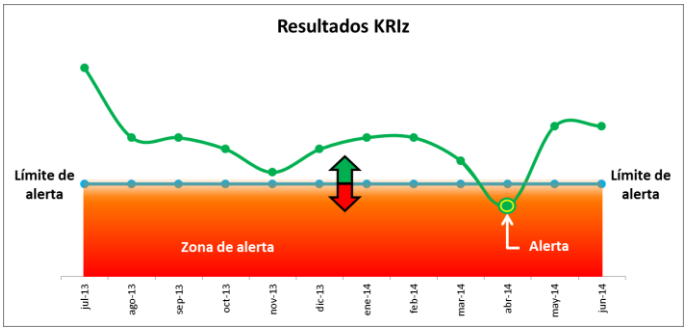
Tendencia: Negativa (valores menores al límite de control indican mejor comportamiento)

Ubicación Evidencia: Archivo de medición UAE ubicado en el SharePoint gerencia de Abastecimiento.

6. ANEXO 2

Ejemplo de tendencia de KRIS

Ejemplo resultados de KRI con límite de alerta máximo (tendencia negativa).



Ejemplo resultados de KRI con límite de alerta mínimo (tendencia positiva).

7. ANEXO 3

Para realizar la incorporación explicita del evento de riesgo de cumplimiento que contemple asuntos de fraude, corrupción, soborno, lavado de activos y financiación de terrorismo, y violaciones a la ley FCPA en las matrices de riesgos y controles de sus procesos, a continuación se provee el evento genérico, que debe ser incorporado para cada proceso con las respectivas causas y consecuencias, según su contexto y particularidades acorde con el nivel de despliegue de la matriz de riesgos y controles.

EVENTO DE RIESGO DE CUMPLIMIENTO GENÉRICO: *Eventos de fraude, corrupción, soborno, lavado de activos, financiación del terrorismo y violaciones a la ley FCPA en el proceso de "Nombre del proceso/subproceso"*

La identificación de estos eventos debe realizarse durante la fase 3 de *Identificación y actualización de riesgos y controles* del ciclo de gestión de riesgos de procesos, y sobre los eventos identificados se deberá surtir el resto de fases del ciclo, con lo que aseguraremos el diseño particular de cada uno de estos riesgos, de acuerdo con la naturaleza de los procesos.

A continuación se ilustra un riesgo, a manera de ejemplo:

Proceso nivel 1	Descripción del objetivo del proceso	Nombre del riesgo	Descripción del riesgo
Gestión de Contratos	Asegurar el inicio, ejecución, cierre y balance de los contratos, realizando una adecuada gestión de eventualidades y haciendo la evaluación del desempeño del contratista.	Eventos de fraude, corrupción, soborno, lavado de activos, financiación del terrorismo y violaciones a la ley FCPA en el proceso de Gestión de Contratos	Eventos de fraude, corrupción, soborno, lavado de activos, financiación del terrorismo y violaciones a la ley FCPA en el proceso de Gestión de Contratos Debido a: - Recibir o Autorizar pagos, de bienes y/o servicios que no cumplan con las condiciones pactadas, o que no se hubieren recibido. - Modificación de la información de los contratos en los sistemas por interlocutores no autorizados. - Uso indebido de los recursos en la ejecución contractual. - Pagos dobles. - Fuga de la información crítica del proceso. Lo cual puede ocasionar vinculación en procesos legales y pérdidas económicas.