

	Guía Metodológica de Gestión de Riesgos LA/FT/FP y C/ST (SARLAFT Y PTEE)	Código: G-GC-001 Fecha: 2026-07-06 Versión: 01
---	---	---

PRESENTACIÓN

La Concesión Costera Cartagena Barranquilla S.A.S. adopta una metodología de gestión de riesgos orientada a garantizar el cumplimiento de la normatividad local e internacional aplicable, así como a fortalecer la prevención, identificación, evaluación y control de los riesgos que puedan afectar el desarrollo de sus actividades.

La presente metodología aplica exclusivamente para la gestión de los riesgos asociados al Sistema de Administración del Riesgo de Lavado de Activos y Financiación del Terrorismo y de la Proliferación de Armas de Destrucción Masiva (SARLAFT) y al Programa de transparencia y ética empresarial PTEE. En este marco, permite administrar dichos riesgos mediante la implementación de acciones preventivas, detectivas y correctivas que contribuyen al control efectivo de los riesgos identificados y al fortalecimiento de los mecanismos de gestión y control de la organización.

Para efectos de cumplimiento normativo en materia de LA/FT/FPADM y C/ST, la concesión adopta la metodología descrita en el presente documento. No obstante, para la gestión integral de los demás riesgos corporativos, la organización se rige por la metodología establecida por ISA y sus empresas.

La metodología se fundamenta en las buenas prácticas establecidas en la norma internacional ISO 31000 sobre Gestión de Riesgos y se desarrolla a través de las siguientes etapas:

- Comprensión de la organización y de su contexto.
- Valoración del riesgo.
- Actividades de control o tratamiento del riesgo.
- Monitoreo y supervisión.
- Comunicación y consulta.

Para el desarrollo de estas etapas se cuenta con la participación de las áreas y responsables de los diferentes procesos de la Concesión, con el fin de asegurar que las acciones definidas para la gestión del riesgo se implementen de manera efectiva y permitan obtener resultados confiables, objetivos y alineados con los niveles de riesgo aceptados por la Concesión.

	Guía Metodológica de Gestión de Riesgos LA/FT/FP y C/ST (SARLAFT Y PTEE)	Código: G-GC-001 Fecha: 2026-07-06 Versión: 01
---	---	---

maquinaria, equipos y demás activos que puedan ser utilizados indebidamente o generar riesgos de corrupción, fraude o LA/FT/FPADM.

d. Canales

Medios utilizados para la movilización de recursos y prestación del servicio, tales como pagos, anticipos, transferencias, compensaciones, indemnizaciones y demás mecanismos de interacción financiera u operativa, susceptibles de uso indebido o falta de trazabilidad.

e. Actividades

Procesos de construcción, operación, mantenimiento vial, recaudo de peajes y demás actividades propias del contrato de concesión, incluyendo el uso de peajes, patios, bodegas, campamentos, centros de control y demás infraestructura operativa, expuestos a riesgos operacionales, de corrupción o LA/FT/FPADM.

2. VALORACIÓN DEL RIESGO

En esta segunda etapa se determinará y describirán los riesgos potenciales que podrían afectar el logro de los objetivos y generar una lista estructurada de eventos que puedan representar amenazas. Se pueden utilizar herramientas como entrevistas, talleres de trabajo, análisis FODA, listas de verificación, revisiones documentales y análisis de procesos.

2.1 Identificación de riesgos

La Concesión debe llevar a cabo de manera periódica la identificación y/o actualización de los riesgos. En este sentido, la identificación de riesgos debe considerar los factores mencionados en el numeral 1. A continuación, se detallan los aspectos que deben ser identificados y documentados en la matriz de riesgos como primer paso del proceso:

- Identificación y descripción del riesgo: definición clara del riesgo que podría afectar negativamente los objetivos de la empresa.
- Tipo de riesgo: clasificación del riesgo según naturaleza, por ejemplo, operativo, financiero, legal, reputacional, tecnológico o ambiental.
- Causas o factores generadores: identificación de causas o circunstancias en las que se podría originar el riesgo.
- Probabilidad de ocurrencia: estimación de la frecuencia o la posibilidad de que el riesgo suceda.
- Grado de impacto: Evaluación de la magnitud de afectación en caso de que el riesgo.
- Nivel del riesgo: determinar la prioridad del riesgo.

- g. Controles existentes: Medidas o mecanismos ya implementados para mitigar o gestionar el riesgo.
- h. Responsables: Personas o áreas encargadas de la gestión o monitoreo del riesgo.
- i. Plan de acción o de tratamiento: Medidas adicionales a implementar para reducir o controlar el riesgo, cuando sea necesario.

La identificación de causas o fallas corresponde a las fuentes generadoras de riesgo, las cuales pueden ser internas o externas a la Concesión. Estas causas deben analizarse considerando los factores de riesgo definidos en el numeral 1, los cuales constituyen la base para la identificación, análisis y evaluación de los riesgos LA/FT/FPADM y PTEE.

En este sentido, la Concesión deberá asegurar que los riesgos identificados estén asociados a dichos factores, permitiendo una adecuada segmentación y trazabilidad dentro de la matriz de riesgos.

2.2 Análisis y priorización del riesgo

Una vez se han identificado los riesgos, se procede a hacer un análisis, de preferencia conjunto con las áreas críticas de la Concesión, con el fin de priorizar los riesgos de acuerdo con su probabilidad e impacto. Este análisis permite entender la magnitud del riesgo y sus posibles consecuencias. La medición del perfil de riesgo se realiza a través de la estimación de la probabilidad de ocurrencia del evento, así como de sus impactos en caso de materializarse:

- **Probabilidad:** Hace referencia a la frecuencia con la que ocurre el evento durante el período evaluado. Los criterios para su clasificación se establecen de acuerdo con la siguiente tabla:

Calificación	Valor	Descripción
Recurrente	5	Se espera que el evento o eventos pueda presentarse con cierta periodicidad - frecuencia por lo menos una (1) vez cada mes.
Frecuente	4	Se espera que el evento o eventos pueda presentarse por los menos una vez cada semestre.
Ocasional	3	Se espera que el evento o eventos pueda presentarse 1 vez cada año.
Remoto	2	Se espera que el evento o eventos pueda presentarse 1 vez cada 5 años.
Improbable	1	El evento o los eventos no se han presentado en un periodo menor a 5 años.

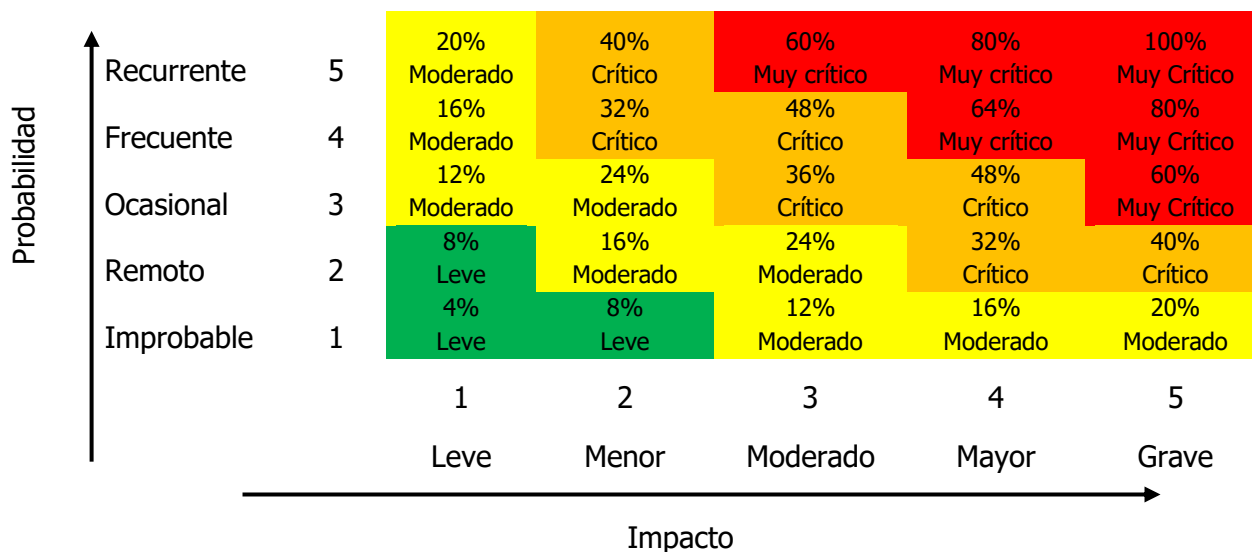
- **Impacto:** Las siguientes preguntas permiten evaluar el impacto del riesgo utilizando la metodología del panel de expertos:

1. ¿Podría la Concesión enfrentar pérdidas económicas?
2. ¿Es probable que este riesgo genere sanciones o multas financieras?
3. ¿Puede generar afectación reputacional o contagio para el Grupo ISA u otras compañías del grupo?
4. ¿Este riesgo podría causar un daño a la reputación de la Concesión en el sector?
5. ¿Existe la posibilidad de que el evento provoque una cobertura mediática negativa para la Concesión?
6. ¿Podría interrumpir la operación o mantenimiento del corredor vial y amenazar el curso normal del negocio?
7. ¿Podría generar conflictos con comunidades o autoridades locales?
8. ¿Podría generar intervención de organismos de control, de la Fiscalía u otras autoridades competentes?
9. ¿Puede dar lugar a procesos disciplinarios, sancionatorios, fiscales o penales?

De acuerdo con el número de respuestas afirmativas se mide el nivel de impacto del riesgo, teniendo en cuenta los siguientes criterios:

Medición del Impacto	Descripción
Grave	Si se responde entre ocho (8) y nueve (9) preguntas afirmativas.
Mayor	Si se responde entre cinco (5) y siete (7) preguntas afirmativas.
Moderado	Si se responde entre tres (3) y cuatro (4) preguntas afirmativas.
Menor	Si se responde al menos dos (2) preguntas afirmativas.
Leve	Si se responde solo una (1) pregunta afirmativa.

Así las cosas, una vez se asigna el valor aplicable para cada riesgo en probabilidad e impacto, el resultado se enmarca en un mapa de calor cuya dimensión corresponde a niveles de cinco (5) filas por (5) columnas que le dan una mayor flexibilidad a la determinación de los riesgos intermedios.



Como se puede observar, la combinación entre la probabilidad de ocurrencia y la magnitud del impacto permite determinar el nivel o perfil del riesgo inherente de la siguiente manera:

	Riesgo Muy Crítico	> 50%	Diseñar e implementar controles preventivos y/o detectivos que permiten reducir el nivel de exposición al riesgo.
	Riesgo Crítico	> 24% y <= 50%	
	Riesgo Moderado	> 8% y <= 24%	
	Riesgo Leve	< 8%	Monitorear el riesgo para identificar los cambios que puedan presentarse.

2.3 Evaluación de riesgo

- **Apetito al riesgo:** La Concesión tiene como objetivo llevar los riesgos inherentes hasta un nivel máximo de exposición moderado en los riesgos identificados. Lo anterior, sin limitar a que las diferentes áreas desarrollen un plan de acción para la implementación de controles en riesgos inferiores y moderados.

Nivel de Exposición Riesgo Inherente	Nivel de Riesgo Residual Objetivo
Muy crítico	Moderado
Crítico	Moderado
Moderado	Leve
Leve	Leve

Las opciones como respuesta a la evaluación de los riesgos son las siguientes:

Recurrente	5	Reducir	Reducir	Evitar/Reducir	Evitar/Reducir	Evitar/Reducir
Frecuente	4	Reducir/Aceptar	Reducir	Reducir	Evitar/Reducir	Evitar/Reducir
Ocasional	3	Reducir/Aceptar	Reducir/Aceptar	Reducir	Evitar/Reducir	Evitar/Reducir
Remoto	2	Aceptar	Reducir/Aceptar	Reducir/Aceptar	Reducir	Evitar/Reducir
Improbable	1	Aceptar	Aceptar	Reducir/Aceptar	Reducir/Aceptar	Reducir/Aceptar
		1	2	3	4	5
		Leve	Menor	Moderado	Mayor	Grave

- **Evitar el riesgo:** Se evita el riesgo si se decide no proceder con la actividad que probablemente generaría el riesgo, utilizando un activo, servicio o producto distinto o modificando el proceso, de manera que las amenazas originales ya no lo afecten
- **Reducir o mitigar el riesgo:** Actividades y medidas tendientes a reducir la probabilidad y/o minimizar la severidad de su impacto. Se consigue mediante la optimización de los procedimientos y la implementación de controles (prevención, planificación).

3. ACTIVIDADES DE CONTROL – TRATAMIENTO DEL RIESGO

Conceptualmente un control se define como una actividad/acción/herramienta que permite reducir el riesgo. Una vez identificado y evaluado el riesgo inherente, se debe diseñar y describir las actividades de control y herramientas necesarias para gestionar la probabilidad de ocurrencia e impacto de materialización de los riesgos identificados.

Con el fin de identificar los controles existentes, actualizarlos, mejorarlos o diseñarlos, se recomienda realizar mesas de trabajo con los líderes de los procesos y expertos, quienes, con el apoyo de sus equipos de trabajo, serán los encargados de posteriormente implementar y monitorear su ejecución., La **Estructura para la descripción del control** debe incluir, como mínimo, los siguientes elementos:

- Qué se hace.
- Cómo se hace.
- Resultado/registro.
- Responsable de la ejecución y seguimiento.
- Frecuencia o periodicidad (en caso de que aplique).
- Describir o referenciar qué se hace en caso de que como resultado de la aplicación del control se identifique algún error (si aplica).

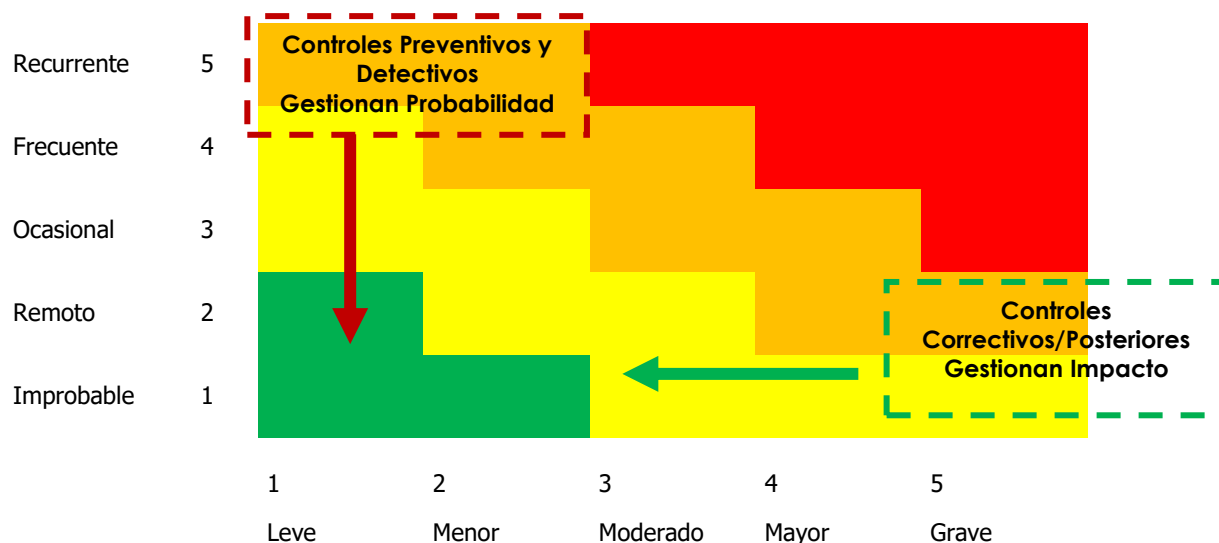
Posteriormente, se evalúa la idoneidad y eficacia de los controles que la Concesión posee con el fin de mitigar y dar respuesta los riesgos evaluados. A partir de esta evaluación, se realiza medición del riesgo residual, el cual considera, por consiguiente, la consistencia de los controles. La evaluación de los controles se realiza teniendo en cuenta los siguientes criterios:

Descripción	Opción	Valor
Asignación responsable del control	Asignado	15
	No Asignado	0
Documentación del control	Documentado	15
	No Documentado	0
Frecuencia	Continua	15
	Aleatoria	0
Propósito	Prevenir	15
	Detectar	10
	Corregir	5
Clase de control	Automático	15
	Dependiente IT	10
	Manual	5
Evidencia	Con registro	10
	Sin registro	0
Qué pasa con las observaciones y desviaciones	Se tienen instrucciones específicas sobre cómo tratarlas oportunamente	15
	No se tienen instrucciones sobre cómo investigar o resolver oportunamente	0

De acuerdo con la estructura del control la cual se evalúa mediante los puntajes mencionados en la tabla, los controles pueden clasificarse de la siguiente manera:

Solidez Diseño		
Fuerte	80 a 100	80% de gestión en probabilidad o impacto
Moderado	40 a 79	50% de gestión en probabilidad o impacto
Débil	0 a 39	20% de gestión en probabilidad o impacto

Según el tipo y objetivo del control, la gestión de los riesgos puede desarrollarse de la manera ilustrada a continuación:



3.1 Tolerancia al riesgo

Una vez se encuentran definidos los niveles de riesgo residual, de no alcanzarse el perfil de riesgo residual esperado, se deben detectar las posibles debilidades existentes definiendo un tratamiento o plan de acción al riesgo residual orientado a:

Leve	Gestión integral del riesgo por parte de los equipos de proceso dentro de la operación normal, aplicando controles rutinarios y monitoreo periódico.	Seguimiento anual
Moderado	Gestión integral del riesgo a cargo de la Gerencia, Oficial de Cumplimiento y equipos de proceso, con participación y seguimiento de medidas adicionales cuando se requiera.	Seguimiento semestral
Crítico	Conocimiento y participación de la Junta Directiva cuando aplique, seguimiento del Comité correspondiente, Gerencia General, Oficial de Cumplimiento y equipos de proceso. Se deberán implementar medidas adicionales en el corto plazo.	Seguimiento trimestral
Muy crítico	Seguimiento prioritario con participación de la Junta Directiva, Comité correspondiente, Gerencia General, Oficial de Cumplimiento y equipos de proceso. Se deberán definir e implementar medidas adicionales inmediatas.	Seguimiento continuo

	Guía Metodológica de Gestión de Riesgos LA/FT/FP y C/ST (SARLAFT Y PTEE)	Código: G-GC-001 Fecha: 2026-07-06 Versión: 01
---	---	---

4. MONITOREO Y SUPERVISIÓN

La evaluación de los riesgos debe ser revisada de forma regular (mínimo una vez al año) de modo tal que se mantengan actualizados y que su nivel de criticidad sea acorde a la realidad.

Adicionalmente, deben ser revisados en los casos extraordinarios, en los que existan cambios significativos en la estructura o procesos de la Concesión.

Asimismo, dados los procedimientos recomendados, la Concesión tiene la responsabilidad de identificar y evaluar los riesgos a través de procedimientos periódicos de Debida Diligencia y Auditoría, los cuales deben ser adelantados con recursos económicos y humanos que sean suficientes para cumplir con el objetivo de realizar una correcta evaluación

La eficacia es medida con base en el aporte de las actividades de control a la minimización del riesgo inherente, su eventual materialización y el comportamiento de los riesgos residuales.

Como resultado de la revisión de la alta dirección se determina la eficacia de las acciones establecidas y el cierre o ampliación del seguimiento sobre las oportunidades reportadas.

5. COMUNICACIÓN Y CONSULTA

La comunicación y consulta es transversal a todas las etapas del proceso para la gestión del riesgo, es por esto por lo que la Concesión cuenta con planes de comunicación y consulta que involucra tanto las partes internas como externas responsables, interesadas, de control y que en general hacen parte de la gestión del riesgo, con el objetivo de abordar aspectos relacionados con los riesgos de la Concesión, sus causas, sus consecuencias y las medidas que se establecen para su tratamiento.

Lo anterior se realiza con el objetivo de garantizar que los responsables del proceso de gestión del riesgo y las partes involucradas entiendan las bases sobre las cuales se toman las decisiones, y las razones por las cuales se requieren acciones específicas. Existen distintos mecanismos de comunicación y consulta a saber:

▪ Capacitación

- Inducción a nuevos empleados: Como parte del proceso de inducción a la Concesión, los nuevos colaboradores serán capacitados sobre la gestión de riesgos y sus obligaciones frente al mismo.
- Sensibilización: Fortalecimiento de la cultura de gestión del riesgo a través de campañas dirigidas a todo el personal con una periodicidad al menos anual.

	Guía Metodológica de Gestión de Riesgos LA/FT/FP y C/ST (SARLAFT Y PTEE)	Código: G-GC-001 Fecha: 2026-07-06 Versión: 01
---	---	---

▪ **Informes y Reportes Asociados a la Gestión de Riesgos**

Los informes permiten a la Concesión contar con un lenguaje común para administrar los resultados de la implementación y seguimiento de la gestión de riesgos y con ello entregar información que soporte la toma de decisiones en forma oportuna y efectiva.

CONTROL DE VERSIONES			
Fecha	Cambio /Modificación	Revisado por:	Aprobado por:
2026-03-04	Versión original.		