# POLITICA DE ADMINISTRACIÓN DE RIESGOS

**LANCASTER BANGUERA HOLGUIN**
Gerente

Documento elaborado y aprobado los
**Comités Coordinador de Control Interno e Institucional de Gestión y Desempeño**

**Apartadó, 2024**

Tel: 828 25 25 / Cras 102 y 104 con calle 92
B. Los Industriales / Apartadó, Antioquia
E-mail: terminalapartado@tta.gov.co

## PRESENTACIÓN

En el marco del Modelo Integrado de Planeación y Gestión MIPG se estable la gestión de riesgos como un elemento imprescindible para el ejercicio de la planeación institucional, así como en el Modelo Estándar de Control Interno MECI definido con la política de Control Interno, donde se establece la formulación de la Política de Administración de Riesgos como la declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo, en la cual se determinan lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos.

Atendiendo estas exigencias normativas, los lineamientos de la guía de administración de Riesgos emitida por Función Pública, la Terminal de Transportes de Apartado formula la presente política de Administración de Riesgos constituyéndose en una herramienta de gran utilidad para anticiparse y contribuir a la prevención de eventos que afecten el cumplimiento de los objetivos estratégicos y el pilar fundamental para direccionar e influenciar la cultura organizacional, en función del pensamiento basado en riesgos; igualmente representa el compromiso del Equipo Directivo y todo el personal frente a la identificación, tratamiento y control de los riesgos que influencian los resultados de la gestión y permiten el cumplimiento de las metas establecidas en los instrumentos de Planificación.

Los lineamientos definidos en esta política establecen los niveles de aceptación de riesgo, los ciclos de establecimiento y seguimiento, los niveles de calificación, la identificación de riesgos de gestión, de corrupción, de seguridad de la información y fiscales e involucra a todos los servidores públicos de la Entidad en su gestión a través de las líneas de defensa, donde la alta dirección es responsable de la administración del riesgo así mismo todos los servidores públicos de la entidad son responsables de la reducción de los riesgos y de velar por la eficacia de los controles integrados en los procesos, actividades y tareas a su cargo. La Oficina de Control Interno, es responsable de evaluar en forma independiente el componente Administración de Riesgos, como parte integral del Sistema de Control Interno y el cumplimiento y efectividad de las políticas de riesgos

## MARCO LEGAL

- Ley 87 de 1993. Por la cual se establecen normas para el ejercicio del control interno en las entidades y organismos del Estado y se dictan otras disposiciones.
- Ley 489 de 1998. Estatuto básico de organización y funcionamiento de la administración pública. Por la cual se dictan normas sobre la organización y funcionamiento de las entidades del orden nacional, se expiden las disposiciones, principios y reglas generales para el ejercicio de las atribuciones previstas en los numerales 15 y 16 del artículo 189 de la Constitución Política y se dictan otras disposiciones.
- Directiva presidencial 09 de 1999. Lineamientos para la implementación de la política de lucha contra la corrupción.
- Ley 1474 de 2011. Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- Decreto 4170 de 2011 por el cual se crea la Agencia Nacional de Contratación Pública –Colombia Compra Eficiente–, se establece la necesidad de "crear políticas unificadas que sirvan de guía a los administradores de compras y que permitan monitorear y evaluar el desempeño del sistema y generar mayor trasparencia en las compras".
- Decreto 1083 de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del sector de función pública". (Incluye el contenido de los decretos 2145 de 1999, 1537 de 2001, 4110 de 2004, 4485 de 2009, 2482 de 2012, y 943 de 2014).
- Decreto 648 de 2017 Por el cual se modifica y adiciona el Decreto 1083 de 2015, Reglamentario Único del Sector de la Función Pública.
- Decreto 1499 DE 2017: Por medio del cual se modifica el Decreto 1083 de 2015,
  Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
  Norma ISO/IEC 27001. Lineamientos para la gestión de seguridad y privacidad de la información.
- Decreto 1008 de 2018. Establece lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital.
- Decreto 2106 de 2019. Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública"

- Manual operativo del Modelo Integrado de Planeación y Gestión versión 5.
- Guía para la Administración del Riesgo en la Gestión, Corrupción y Seguridad Digital. Diseño de Controles en Entidades Públicas versión 5 de noviembre de 2022
- Modelo nacional de gestión del riesgo de seguridad de la Información en entidades públicas

# 1. DECLARACIÓN DE LA POLITICA DE ADMINISTRACIÓN DE RIESGOS

El Gerente y su Equipo de Gobierno, en cumplimiento de las funciones como Comité Institucional de Gestión y Desempeño y Comité Coordinador de Control Interno, establecen las intenciones generales de la EICE Terminal de Transportes con respecto a la gestión del riesgo, así:

**“En la EICE Terminal de Transportes de Apartadó tenemos el compromiso de administrar los riesgos de una manera integral, fundamentados en la cultura del pensamiento basado en riesgos.”**

## 1.1. OBJETIVOS

### 1.1.1. OBJETIVO GENERAL

Determinar lineamientos para la identificación de acciones de riesgo y de control, así como la generación de respuestas oportunas y estrategias institucionales, que permitan disminuir las causas potenciales, las amenazas, las vulnerabilidades y minimizar los impactos ante una eventual materialización de eventos que puedan afectar los objetivos Institucionales; fortaleciendo la cultura del pensamiento basado en riesgos.

.

### 1.1.2. OBJETIVOS ESPECIFICOS

- ✓ identificar los riesgos que estén o no bajo el control de la organización, teniendo en cuenta el contexto estratégico en el que opera la entidad, la caracterización de cada proceso y el análisis frente a los factores internos y externos que pueden generar riesgos que afecten el cumplimiento de los objetivos.
- ✓ Establecer la probabilidad de ocurrencia, el nivel de las consecuencias o impactos, y estimar las zonas de riesgo, fortaleciendo los controles de los procesos y definiendo las acciones para el tratamiento de los riesgos.
- ✓ Realizar monitoreo, seguimiento y evaluación a las acciones para tratar los riesgos definidos en cada uno de los procesos, aplicando los lineamientos establecidos para la gestión integral del riesgo, contribuyendo al fortalecimiento del desempeño institucional.

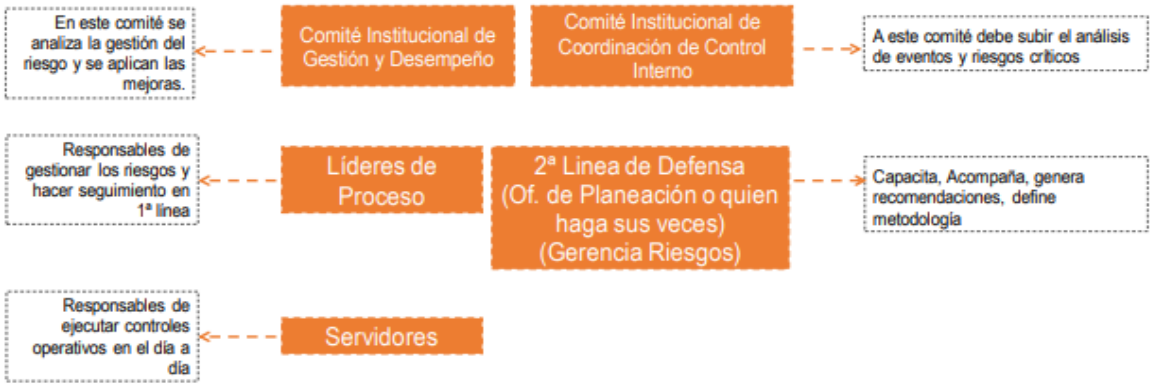
## 1.2. ALCANCE

**1.3.** La administración Integral de riesgos en la Terminal de Transportes de Apartadó es aplicable a todos los procesos del modelo de operación por procesos; igualmente a todas las acciones ejecutadas por los servidores y/o contratistas durante el ejercicio de sus funciones y obligaciones.

Incluye los principios básicos y metodológicos para la administración y gestión de riesgos y oportunidades de tipo estratégico, operacional, de cumplimiento, de corrupción, de gestión de la información y fiscales. Para los riesgos de corrupción, de gestión de la información y fiscales se deberán tener en cuenta los criterios diferenciales que establece la guía y en el caso de los riesgos de gestión de la información los que establece el modelo de seguridad y privacidad de la información de Mintic.

1.4. **INSTITUCIONALIDAD**: El Modelo Integrado de Planeación y Gestión - MIPG define para su operación articulada la creación en todas las entidades del Comité Institucional de Gestión y Desempeño, regulado por el Decreto 1499 de 2017, Decreto 0035 de marzo de 2019 y el Comité Institucional de Coordinación de Control Interno, reglamentado a través del artículo 13 de la Ley 87 de 1993 y el Decreto 648 de 2017, en este marco general, para una adecuada gestión del riesgo, dicha institucionalidad entra a funcionar de la siguiente forma.

*Figura 3 Operatividad Institucionalidad para la Administración del Riesgo*




*Fuente: Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

## 1.5. ROLES Y RESPONSABILIDADES EN LA GESTIÓN DE RIESGOS

Los roles y responsabilidades para la Administración de Riesgos están asignados en el modelo de las líneas de defensa que proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos, acorde al Modelo Integrado de Planeación y Gestión MIPG y al Modelo Estándar del Control Interno MECI, definido en la Dimensión 7 del modelo MIPG. Las líneas de defensa son el eje articulador donde se definen las responsabilidades frente al control, el cual proporciona una manera simple y efectiva para mejorar las comunicaciones en la gestión de riesgos y control mediante la declaración de las funciones y deberes esenciales relacionados.

| Línea de defensa | Responsabilidades frente a los Riesgos |
|---|---|
| **Línea Estratégica**<br><br>**ALTA DIRECCIÓN**<br>Comité institucional de coordinación de control interno y/o Comité Institucional de Gestión y Desempeño<br><br>Su rol principal es analizar los riesgos y amenazas institucionales, que puedan afectar el cumplimiento de los planes estratégicos, así como definir el marco general para la gestión del riesgo (política de administración del riesgo) y el cumplimiento de los planes de la entidad. | • Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento.<br>• Definición de la Política de Administración del Riesgo.<br>• Evaluación de la Política de riesgos. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes.<br>• Monitoreo permanentemente los riesgos.<br>• Monitoreo al estado de los riesgos aceptados (apetito por el riesgo), con el fin de identificar cambios sustantivos que afecten el funcionamiento de la entidad.<br>• Monitoreo de Riesgos relacionados con el manejo de información clasificada o reservada.<br>• Asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo. |
| **Primera Línea de Defensa**:<br>Líderes de programas, procesos y proyectos y de sus equipos de | • Desarrollo e implementación de procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.<br>• Conocimiento y apropiación de las políticas, procedimientos, manuales, protocolos y otras herramientas |

| | |
|---|---|
| trabajo (en general servidores públicos en todos los niveles de la organización)<br><br>Su rol principal es el mantenimiento efectivo de controles internos, la ejecución de gestión de riesgos y controles en el día a día. Para ello, identifica, evalúa, controla y mitiga los riesgos a través del "Autocontrol". | que permitan tomar acciones para el autocontrol en sus puestos de trabajo.<br>• Identificación de riesgos y el establecimiento de controles, así como su seguimiento, acorde con el diseño de dichos controles, evitando la materialización de los riesgos.<br>• Generación de reportes periódicamente al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.<br>• Monitoreo permanentemente de los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI.<br>• Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico).<br>• Verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción.<br>• Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad.<br>• Verificación de que los responsables estén ejecutando los controles tal como han sido diseñados.<br>• Asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades. |
| **Segunda Línea de Defensa**<br><br>Jefes de planeación o quienes hagan sus veces, Coordinadores de equipos de trabajo, comités de riesgos (donde existan), comité de contratación, áreas financieras, áreas de TIC, entre otros que respondan de manera directa por el aseguramiento de la operación. | • Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende<br>• Consolidación y análisis de información sobre temas claves para la entidad, base para la toma de decisiones y de las acciones preventivas necesarias para evitar materializaciones de riesgos.<br>• Trabajo coordinado con las oficinas de control interno o quien haga sus veces, en el fortalecimiento del Sistema de Control Interno.<br>• Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles; ii) planes de mejoramiento; iii) indicadores de gestión; iv) procesos y procedimientos. |

| | |
|---|---|
| Su rol principal es asegurar que los controles y procesos de gestión del riesgo de la 1ª Línea de Defensa sean apropiados y funcionen correctamente, supervisan la implementación de prácticas de gestión de riesgo eficaces; así mismo, consolidan y analizan información sobre temas clave para la entidad, enmarcado en la "autogestión". | • Establecimiento de los mecanismos para la autoevaluación requerida (auditoría interna a sistemas de gestión, seguimientos a través de herramientas objetivas, informes con información de contraste que genere acciones para la mejora).<br>• Generación de reportes periódicamente al Comité Institucional de Coordinación de Control Interno acerca del cumplimiento de las metas y los objetivos en relación a la gestión integral del riesgo.<br>• Monitoreo permanentemente de los cambios en el entorno (interno y externo) que puedan afectar la efectividad del SCI.<br>• Revisión de las exposiciones al riesgo con los grupos de valor, proveedores, sectores económicos u otros (monitoreo del contexto estratégico).<br>• Verificación, en el marco de la política de riesgos institucional, que la identificación y valoración del riesgo de la primera línea sea adecuada frente al logro de objetivos y metas<br>• Verificación de la adecuada identificación de los riesgos relacionados con fraude y corrupción.<br>• Verificación de que el diseño del control establecido por la primera línea de defensa sea pertinente frente a los riesgos identificados, analizando: los responsables y su adecuada segregación de funciones, propósito, periodicidad, tratamiento en caso de desviaciones, forma de ejecutar el control y evidencias de su ejecución, y efectuar las recomendaciones a que haya lugar ante las instancias correspondientes (primera, segunda, y línea estratégica).<br>• Acorde con la estructura de la entidad, el funcionario de Seguridad de la Información en Ticas verifica el desarrollo y mantenimiento de controles de TI.<br>• Monitoreo a los riesgos acorde con la política de administración de riesgo establecida para la entidad.<br>• Verificación de que los responsables estén ejecutando los controles tal como han sido diseñados.<br>• Evaluación de la gestión del riesgo de la entidad de forma integral, con énfasis en:<br>▫ La exposición al riesgo, acorde con los lineamientos y la política institucional.<br>▫ El cumplimiento legal y regulatorio.<br>▫ Logro de los objetivos estratégicos o institucionales. |

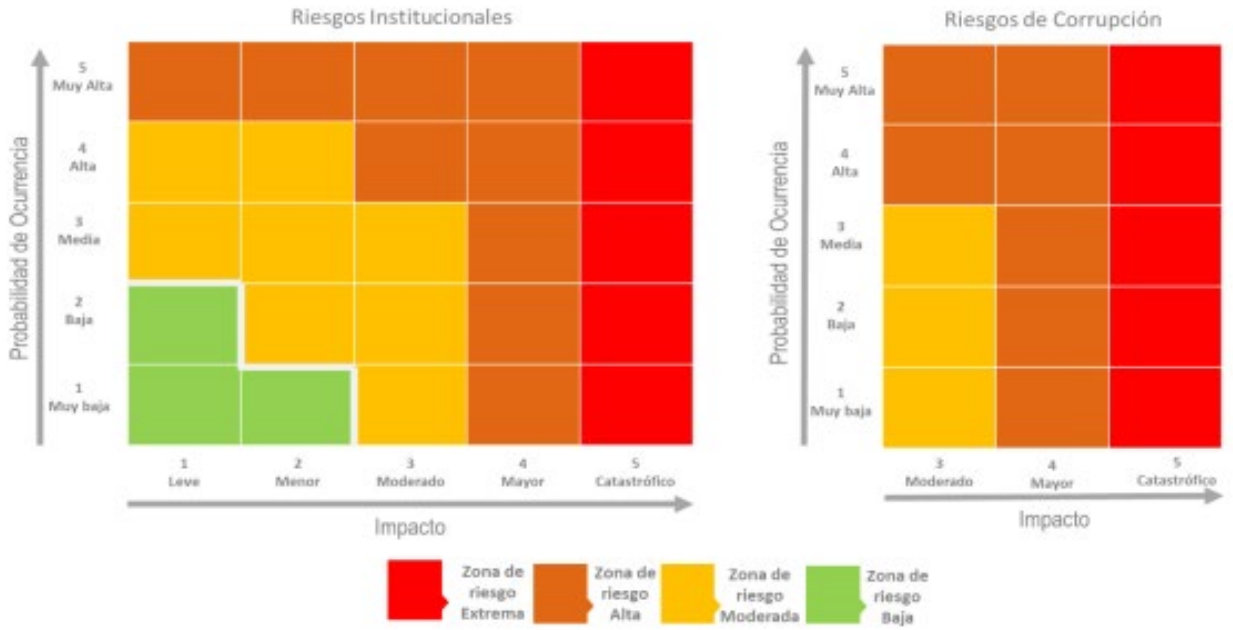
| | |
|---|---|
| | ▫ Confiabilidad de la información financiera y no financiera.<br>• Como resultado de la evaluación de la gestión del Riesgo comunicar las deficiencias a la alta dirección o a las partes responsables para tomar las medidas correctivas, según corresponda.<br>• Verificación del avance y cumplimiento de las acciones incluidas en los planes de mejoramiento producto de las autoevaluaciones.<br>• Difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación. |
| **Tercera Línea de Defensa:**<br><br>Jefes de control interno o quienes hagan sus veces<br><br>Sus roles son: liderazgo estratégico, enfoque hacia la prevención, evaluación de la gestión del riesgo, relación con entes externos de control y el de evaluación y seguimiento. | • Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa<br>• A través de su rol de asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces.<br>• Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo.<br>• Asesoría proactiva y estratégica a la Alta Dirección y los líderes de proceso, en materia de control interno y sobre las responsabilidades en materia de riesgos.<br>• Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos.<br>• Informar los hallazgos y proporcionar recomendaciones de forma independiente.<br>• Evaluación de la gestión del riesgo de la entidad de forma integral, con énfasis en:<br>▫ La exposición al riesgo, acorde con los lineamientos y la política institucional.<br>▫ El cumplimiento legal y regulatorio.<br>▫ Logro de los objetivos estratégicos o institucionales.<br><br>• Evaluación de la efectividad de las acciones desarrolladas por la segunda línea de defensa en aspectos como: cobertura de riesgos, cumplimientos de la planificación, |

| | |
|---|---|
| | mecanismos y herramientas aplicadas, entre otros, y generar observaciones y recomendaciones para la mejora.<br>• Como resultado de la evaluación de la gestión del Riesgo comunica las deficiencias a la alta dirección o a las partes responsables para tomar las medidas correctivas, según corresponda.<br>• Evaluación de la efectividad de las acciones incluidas en los Planes de mejoramiento producto de las auditorías internas y de entes externos.<br>• Realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría y, por lo tanto, debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos y los resultados de la evaluación de la gestión del riesgo. |

## 1.6. NIVELES DE ACEPTACIÓN DEL RIESGO (APETITO AL RIESGO):

En la evaluación de los riesgos se determinan los niveles de severidad a través de la combinación entre la probabilidad y el impacto y se definen las zonas de severidad en la matriz de calor, así:

**Gráfica 1.** *Matriz de calificación de nivel de severidad del riesgo*




Fuente: Política de Administración de Riesgos DAFP

El mapa de calor permite visualizar los riesgos en las zonas definidas (bajo, moderado, alto y extremo) permitiendo identificar y priorizar los riesgos asociados a su gestión que requieren mayor atención, así como los que está dispuesta a aceptar (apetito del riesgo) en función del impacto de estos en la entidad.

Frente a las zonas de riesgo se define el siguiente tratamiento:

| ZONA DE RIESGO | TRATAMIENTOS |
|---|---|
| BAJA | ACEPTAR EL RIESGO |
| MODERADA | REDUCIR (MITIGAR O TRANSFERIR EL RIESGO) |
| ALTA | REDUCIR (MITIGAR O TRANSFERIR EL RIESGO), O EVITAR |
| EXTREMA | REDUCIR (MITIGAR O TRANSFERIR EL RIESGO), O EVITAR |

Los riesgos que se encuentren en zona baja se aceptan y se continúa el monitoreo. Los riesgos de corrupción no admiten la aceptación del riesgo, siempre deben conducir a un tratamiento.

La Alta Dirección de la Terminal de Transportes de Apartadó determina que, para los riesgos residuales de gestión, de corrupción, de seguridad de la información y fiscales se tendrán los siguientes niveles de aceptación:

| Tipo de Riesgo | Zona de Riesgo | Nivel de Aceptación |
|---|---|---|
| Riesgos de Gestión, fiscales y de seguridad de la Información o fiscal | Baja | Se ACEPTARÁ el riesgo y se administra por medio de las actividades propias del proceso asociado y se realiza en el reporte trimestral de su desempeño.<br><br>Los riesgos que soporten documentación de sus controles en sus procedimientos y evidencien implementación de sus controles existentes y no presenten materialización durante la vigencia, pueden ser considerados para su ELIMINACIÓN |
| | Moderada | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo, se hace seguimiento trimestral y se registra sus avances en el seguimiento de riesgos |
| | Alta | Se debe incluir el riesgo tanto en el Mapa de riesgo del Proceso como en el Mapa de Riesgo Institucional y se establecen acciones de Control Preventivas que permitan REDUCIR (MITIGAR O TRANSFERIR) O EVITAR la materialización del riesgo. Se monitorea trimestral y se registra en el seguimiento a Riesgos. |
| | Extrema | |

| | | |
|---|---|---|
| Riesgos de Corrupción | Baja | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de ocurrencia del riesgo. La Periodicidad de seguimiento será trimestral, para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el seguimiento a Riesgos |
| | Moderada | Se establecen acciones de control preventivas que permitan REDUCIR la probabilidad de |

| | | |
|---|---|---|
| | | ocurrencia del riesgo. La Periodicidad de seguimiento será trimestral, para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el seguimiento a Riesgos |
| | Alta | Se adoptan medidas para: REDUCIR la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. TRANSFERIR O COMPARTIR una parte del riesgo para reducir la probabilidad o el impacto del mismo. Periodicidad MENSUAL de seguimiento para evitar a toda costa su materialización por parte de los procesos a cargo de los mismos y se registra en el seguimiento a Riesgos<br>EVITAR Se abandonan las actividades que dan lugar al riesgo, decidiendo no iniciar o no continuar con la actividad que causa el riesgo. |
| | Extrema | |

## 1.7. NIVELES PARA CALIFICAR EL IMPACTO:

1.7.1. Niveles para calificar el impacto de los Riesgos de Gestión y de Seguridad de la Información:

Los impactos económicos y reputacionales son las variables principales para calificar y determinar el impacto de los riesgos de gestión y de seguridad de la información, definidos en la siguiente tabla:

*Tabla 5 Criterios para definir el nivel de impacto*

| | Afectación Económica | Reputacional |
|---|---|---|
| Leve 20% | Afectación menor a 10 SMLMV . | El riesgo afecta la imagen de algún área de la organización. |
| Menor-40% | Entre 10 y 50 SMLMV | El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. |
| Moderado 60% | Entre 50 y 100 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. |
| Mayor 80% | Entre 100 y 500 SMLMV | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. |
| Catastrófico 100% | Mayor a 500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país |

*Fuente: Adaptado del Curso Riesgo Operativo Universidad del Rosario por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020.*

1.7.2. Niveles para calificar el impacto de los Riesgos Fiscales:

Considerando la naturaleza y alcance del riesgo fiscal, éste siempre tendrá un impacto económico, toda vez que el efecto dañoso siempre ha de recaer sobre un bien, recurso o interés patrimonial de naturaleza pública. Los criterios son los descritos en la siguiente tabla:

| | Afectación Económica | Reputacional |
|---|---|---|
| Leve 20% | Afectación menor a 10 SMLMV . | El riesgo afecta la imagen de algún área de la organización. |
| Menor-40% | Entre 10 y 50 SMLMV | El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o de proveedores. |
| Moderado 60% | Entre 50 y 100 SMLMV | El riesgo afecta la imagen de la entidad con algunos usuarios de relevancia frente al logro de los objetivos. |
| Mayor 80% | Entre 100 y 500 SMLMV | El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel de sector administrativo, nivel departamental o municipal. |
| Catastrófico 100% | Mayor a 500 SMLMV | El riesgo afecta la imagen de la entidad a nivel nacional, con efecto publicitario sostenido a nivel país |

### 1.7.3. Niveles para calificar el Impacto de los Riesgos de Corrupción

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo, de acuerdo a los Criterios para calificar el impacto en riesgos de corrupción:

Vigilado SuperTransporte

| N.° | PREGUNTA: SI EL RIESGO DE CORRUPCIÓN SE MATERIALIZA PODRÍA... | RESPUESTA | |
|---|---|---|---|
| | | SÍ | NO |
| 1 | ¿Afectar al grupo de funcionarios del proceso? | X | |
| 2 | ¿Afectar el cumplimiento de metas y objetivos de la dependencia? | X | |
| 3 | ¿Afectar el cumplimiento de misión de la entidad? | X | |
| 4 | ¿Afectar el cumplimiento de la misión del sector al que pertenece la entidad? | | X |
| 5 | ¿Generar pérdida de confianza de la entidad, afectando su reputación? | X | |
| 6 | ¿Generar pérdida de recursos económicos? | X | |
| 7 | ¿Afectar la generación de los productos o la prestación de servicios? | X | |
| 8 | ¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o recursos públicos? | | X |
| 9 | ¿Generar pérdida de información de la entidad? | | X |
| 10 | ¿Generar intervención de los órganos de control, de la Fiscalía u otro ente? | X | |
| 11 | ¿Dar lugar a procesos sancionatorios? | X | |
| 12 | ¿Dar lugar a procesos disciplinarios? | X | |
| 13 | ¿Dar lugar a procesos fiscales? | X | |
| 14 | ¿Dar lugar a procesos penales? | | X |
| 15 | ¿Generar pérdida de credibilidad del sector? | | X |
| 16 | ¿Ocasionar lesiones físicas o pérdida de vidas humanas? | | X |
| 17 | ¿Afectar la imagen regional? | | X |
| 18 | ¿Afectar la imagen nacional? | | X |
| 19 | ¿Generar daño ambiental? | | X |
| Responder afirmativamente de UNA a CINCO pregunta(s) genera un impacto moderado.<br>Responder afirmativamente de SEIS a ONCE preguntas genera un impacto mayor.<br>Responder afirmativamente de DOCE a DIECINUEVE preguntas genera un impacto catastrófico. | | 10 | |
| MODERADO | Genera medianas consecuencias sobre la entidad | | |
| MAYOR | Genera altas consecuencias sobre la entidad. | | |

Nivel de impacto MAYOR

## 1.8. TRATAMIENTO DE LOS RIESGOS

En el evento de materializarse un riesgo de gestión, de corrupción, de seguridad de la información o Fiscal, se deben ejecutar las siguientes acciones:

| Riesgo | Responsable | Acción |
|---|---|---|
| Riesgo de gestión, de corrupción, de seguridad de la información o Fiscal | Líder de Proceso | 1. Informar a la Secretaría de Planeación o quien haga sus veces como segunda línea de defensa en el tema de riesgos sobre el posible hecho encontrado, quien a su vez socializará al comité coordinador de Control Interno.<br><br>2. Realizar análisis de causas, efectos y controles y determinar las acciones de mejoramiento, en el Plan de mejoramiento<br><br>3. Actualizar el mapa de riesgos<br><br>4. Realizar monitoreo permanente a las acciones establecidas.<br><br>En el caso de los riesgos de corrupción Una vez se informe a la segunda línea de defensa y dependiendo del hecho de corrupción materializado, realizar de inmediato la denuncia ante la instancia de control correspondiente.<br><br>En el caso de riesgos de gestión, de seguridad de la información o fiscal, calificado en zona baja se debe verificar la calificación y ubicación del riesgo para su inclusión en el mapa de riesgos.<br><br>En el caso de riesgos de seguridad de la Información proceder de manera inmediata a aplicar el plan de contingencia o de tratamiento de incidentes de seguridad de la información que permita la continuidad del servicio o el restablecimiento de este (si es el caso) y documentar en el plan de mejoramiento. |
| | Oficina de Control Interno | 1. Informar al Líder del proceso del posible hecho de corrupción. |

| | | |
|---|---|---|
| | | 2. Informar a la segunda línea de defensa con el fin facilitar el inicio de las acciones correspondientes con el líder del proceso y ajustar el mapa de riesgos<br><br>3. Acompañar al líder del proceso en la revisión, análisis y toma de decisiones correspondiente para resolver la situación.<br><br>4. Informar al Comité Coordinador de control interno sobre las acciones tomadas.<br><br>5. Verificar que se tomaron las acciones y se actualizó el mapa de riesgos correspondiente |

## 1.8. REPORTE Y CONSOLIDACIÓN DEL PLAN DE TRATAMIENTO DE RIESGOS

**Reporte:** Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles para prevenir y detectar, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

En el formato de mapa de riesgos se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual. A partir de allí se establece el plan de tratamiento de riesgos, definiendo las actividades de control según la opción de tratamiento a la que corresponden dentro del mismo mapa de riesgos.

Las actividades de tratamiento enunciadas en el mapa de riesgos definidas como plan de Acción, donde se establecerá, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad (fecha de implementación), así como el establecimiento de fecha de seguimiento, resultados del seguimiento y estado de la Acción.

El reporte de la gestión de los diferentes tipos de Riesgo, se realiza de la siguiente manera:

| QUIEN A REPORTA | A QUIEN SE REPORTA | QUE SE REPORTA | DONDE REPORTA |
|---|---|---|---|
| La primera línea de defensa | a la segunda línea de defensa | el estado de avance del tratamiento del riesgo en la operación | En el plan de acción del mapa de riesgos |
| La segunda línea de defensa | A la línea estratégica | la consolidación de los riesgos en todos los niveles | |

En el caso de los riesgos de seguridad de la información los funcionarios de las TICS apoyarán y acompañarán a las diferentes líneas de defensa tanto para el reporte como para la gestión y el tratamiento de estos riesgos.

**Ajustes y modificaciones:** se podrán llevar a cabo los ajustes y modificaciones necesarias orientadas a mejorar el mapa de riesgos después de su publicación y durante el respectivo año de vigencia. En este caso deberán dejarse por escrito los ajustes, modificaciones o inclusiones realizadas.

## 1.9. MONITOREO, REVISIÓN Y SEGUIMIENTO

El monitoreo, revisión y seguimiento de la gestión de riesgos está alineado con la dimensión del MIPG de “Control interno”, que se desarrolla con el MECI a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad a través del modelo de líneas de defensa, ya descritas en el capítulo 1. Numeral 1.4. Roles y Responsabilidades de esta Política.

**MONITOREO Y REVISIÓN A RIESGOS DE GESTIÓN, DE CORRUPCIÓN, DE SEGURIDAD DE LA INFORMACIÓN Y FISCALES**

| ZONAS DE RIESGO | PERIODICIDAD | RESPONSABLE |
|---|---|---|
| ZONA BAJA | CUATRIMESTRAL | Comité coordinador de control Interno (Línea estratégica)<br>Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos (Primera Línea de defensa)<br>Oficina de Planeación (segunda línea de defensa) |
| ZONA MODERADA | | |
| ZONA ALTA | MENSUAL | |
| EXTREMA | | |

| | | |
|---|---|---|
| POLITICA DE ADMINISTRACIÓN DE RIESGOS | ANUAL | Comité coordinador de control Interno (Línea estratégica) |

- Su importancia radica en la necesidad de llevar a cabo un monitoreo, revisión y seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que los riesgos siempre están presentes y en especial los de corrupción son, por sus propias características, una actividad difícil de detectar.

## SEGUIMIENTO A RIESGOS DE CORRUPCIÓN

Le corresponde al jefe de Control Interno o quien haga sus veces (tercera línea de defensa) realizar el seguimiento a la gestión de los riesgos de corrupción, así:

La periodicidad de los seguimientos será la siguiente:

| PERIODICIDAD (CUATRIMESTRAL) | PUBLICACIÓN |
|---|---|
| **Primer seguimiento:** Con corte al 30 de abril | Diez (10) primeros días del mes de mayo. |
| **Segundo seguimiento:** Con corte al 31 de agosto | Diez (10) primeros días del mes de septiembre. |
| **Tercer seguimiento:** Con corte al 31 de diciembre | Diez (10) primeros días del mes de enero del año siguiente |

El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles. En especial deberá adelantar las siguientes actividades:

- ✓ Verificar la publicación del Mapa de Riesgos en la página web de la entidad.
- ✓ Seguimiento a la gestión del riesgo.
- ✓ Revisión de los riesgos y su evolución.
- ✓ Asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada

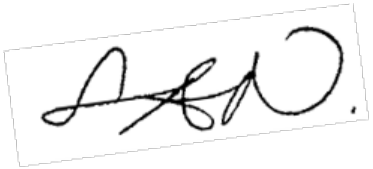
El seguimiento adelantado por la Oficina de Control Interno se deberá publicar en la página web de la entidad o en un lugar de fácil acceso para el ciudadano.

## 1.10. COMUNICACIÓN Y CONSULTA

La comunicación es un elemento imprescindible para la efectiva administración de riesgos de la Terminal de Transportes de Apartadó, lo cual se ha realizado con participación de servidores de todos los niveles, por lo tanto, para la comunicación y consulta se debe tener en cuenta los siguientes lineamientos:

- La comunicación y consulta con las partes involucradas, tanto internas como externas, debe realizarse durante todas las etapas del proceso para la gestión del riesgo.
- La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.
- Se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la organización pública.
- Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.
- Los servidores públicos y contratistas de la entidad deben conocer el mapa de riesgos antes de su publicación. Para lograr este propósito la oficina de planeación o quien haga sus veces, o la de gestión del riesgo deberá diseñar y poner en marcha las actividades o mecanismos necesarios para que los funcionarios y contratistas conozcan, debatan y formulen sus apreciaciones y propuestas sobre el proyecto del mapa de riesgos.
- Así mismo, dicha oficina adelantará las acciones para que la ciudadanía y los interesados externos conozcan y manifiesten sus consideraciones y sugerencias sobre el proyecto del mapa de riesgos.
- El mapa de riesgos se debe publicar en la página web de la entidad, en la sección de transparencia y acceso a la información pública que establece el artículo 2.1.1.2.1.4 del Decreto 1081 de 2015 o en un medio de fácil acceso al ciudadano, a más tardar el 31 de enero de cada año.

Dado en Apartadó, a los dieciséis (16) días del mes de diciembre de 2024.



**LANCASTER BANGUERA HOLGUIN**
Gerente