TERMINAL METROPOLITANA
de Transporte de Barranquilla S.A.
VOY SEGURO, USO LA TERMINAL

ALCALDÍA DE BARRANQUILLA | Soy BARRANQUILLA

POLITICA DE ADMINISTRACIÓN DEL RIESGO

TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.

2022

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO GENERAL 4
2.1 OBJETIVOS ESPECIFICOS 4
3. ALCANCE 5
4. RESPONSABILIDADES 5
5. MARCO NORMATIVO 6
6. GLOSARIO 8
7. ESTRUCTURA PARA LA IDENTIFICACIÓN DEL RIESGO 11
7.1 IDENTIFICACIÓN DEL RIESGO 11
7.2 ANALISIS Y VALORACIÓN DEL RIESGO 20
7.3 TRATAMIENTO DEL RIESGO 29
7.4 HERRAMIENTAS PARA LA GESTION DEL RIESGO 30
7.5 MONITOREO Y REVISION 31
8. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN 31
9. METODOLOGIA PARA LA GESTION DE RIESGOS EN LA TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A. 32

1. INTRODUCCIÓN

La Política de Administración del Riesgo es un compromiso frente a la identificación, tratamiento, control de los riesgos, que influencian los resultados de la gestión y permiten el cumplimiento de los objetivos de Terminal Metropolitana de Transportes de Barranquilla S.A. A través de este lineamiento se direcciona la cultura organizacional, en función del pensamiento basado en riesgos, así mismo involucra mediante un ámbito estratégico y líneas de defensa, a todos los servidores de la entidad, soportándose en los mecanismos de comunicación disponibles y cubriendo las responsabilidades institucionales de cada proceso y propias de cada servidor.

La presente política reconoce los parámetros establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas Versión 5 de 2020.

Es importante que para la implementación del riesgos cada entidad realice una análisis de sus estrategias, formulación de objetivos, análisis de datos y estadísticas para la toma de decisiones, que le permitirá una identificación adecuada del riesgo, de conformidad con sus necesidades, estableciendo un enfoque preventivo, hacia la protección de sus recursos, alcanzando mejores resultados, facilitando la toma de decisiones y mejorando así la prestación de los servicios a sus usuarios y clientes , entendiendo esto, como la generación de valor público, eje fundamental del quehacer de las instituciones públicas.

2. OBJETIVO GENERAL

Servir de guía metodológica, estableciendo los lineamientos necesarios para la administración de los riesgos de la entidad, asegurando así una gestión adecuada en cuanto al tratamiento de estos, encaminada a evitar, reducir, compartir, transferir o asumir el Riesgo residual, que contribuya al cumplimiento de los objetivos y metas institucionales, facilitando la toma de decisiones y generando valor público.

2.1 OBJETIVOS ESPECIFICOS

- Establecer una metodología clara y adecuada para las distintas etapas requeridas para la gestión del riesgo.
- Definir los niveles de aceptación de los riesgos en los casos que se requiera
- Definir los niveles para calificar la probabilidad y el impacto en los riesgos identificados.
- Proporcionar la información necesaria a los grupos de interés sobre los riesgos actuales o potenciales a los cuales se puede ver expuesta la entidad.
- Fomentar en la entidad una cultura organizacional con enfoque preventivo, encaminada a la administración adecuada de riesgos.
- Involucrar y comprometer a los servidores de la entidad hacia la búsqueda de acciones encaminadas a prevenir, identificar, controlar y mitigar los riesgos.
- Proporcionar una guía que le permita a los lideres de procesos de la entidad definir e implementar los mecanismos de verificación y evaluación periódica de los riesgos identificados.

3. *ALCANCE*

Aplica a todos los procesos, proyectos, servicios y planes de la entidad, conforme a cada tipo y clasificación de riesgo, bajo la responsabilidad de los líderes de proceso y líneas de defensa.

4. *RESPONSABILIDADES*

LINEAS DE DEFENSA	RESPONSABLES	RESPONSABILIDAD FRENTE A LA GESTIÓN DEL RIESGO
LINEA ESTRATEGICA	✓ Alta Dirección ✓ Comité Institucional de Coordinación de Control Interno	Definición y evaluación de la Política de Administración del Riesgo. La evaluación debe considerar su aplicación en la entidad, cambios en el entorno que puedan definir ajustes, dificultades para su desarrollo, riesgos emergentes
PRIMERA LINEA DE DEFENSA	Líderes de procesos/ servidores en sus diferentes niveles	✓ Realiza el mantenimiento efectivo de controles internos, por consiguiente, identifica, evalúa, controla y mitiga los riesgos ✓ 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.
SEGUNDA LINEA DE DEFENSA	Jefes de planeación, o quienes hagan sus veces; coordinadores de equipos de trabajo, coordinadores de sistemas de gestión, gerentes de riesgos (donde existan), líderes o coordinadores de contratación, financiera y de TIC, entre otros que se deberán definir acorde con la complejidad y misionalidad de cada organización.	✓ Asegura de que los controles y procesos de gestión del riesgo de la 1ª línea de defensa sean apropiados y funcionen correctamente, además, se encarga de supervisar la eficacia e implementación de las prácticas de gestión de riesgo. ✓ Asesoría a la 1ª línea de defensa en temas clave para el Sistema de Control Interno: i) riesgos y controles
TERCERA LINEA DE DEFENSA	**OFICINA DE CONTROL INTERNO**	✓ Evalúa de manera independiente y objetiva los controles de 2ª línea de defensa para asegurar su efectividad y cobertura; así mismo, evalúa los controles de 1ª línea de defensa que no se encuentren cubiertos ✓ Asesoría, orientación técnica y recomendaciones frente a la administración del riesgo en coordinación con la Oficina Asesora de Planeación o quien haga sus veces se garantiza el cumplimento efectivo de los objetivos. ✓ Monitoreo a la exposición de la organización al riesgo y realizar recomendaciones con alcance preventivo. ✓ 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. ✓ Formar a la alta dirección y a todos los niveles de la entidad sobre las responsabilidades en materia de riesgos

5. MARCO NORMATIVO

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 872 de 2003. Crea el sistema de la calidad en la rama ejecutiva del poder público y en otras entidades prestadoras de servicios.

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.

NTC ISO 31000:2018. Lineamientos Administración / Gestión de riesgos

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 Consejo para la Gestión y Desempeño Institucional Versión 4 marzo de 2021

Guía para la administración del riesgo y el diseño de controles en entidades públicas - Versión 5 diciembre 2020.

Guía “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano” de la secretaria de Transparencia de la Presidencia de la República

6. GLOSARIO

A continuación, una serie de conceptos, necesarios para la comprensión de la metodología que se desarrolla a partir de la adopción de la política de administración del riesgo, hasta la valoración del riesgo. (Definiciones dadas por la guía de riesgos y diseño de controles versión 5. Fuente: Elaborado y actualizado por la Dirección de Gestión y Desempeño Institucional de Función Pública, 2020)

- **Activo:** En el contexto de seguridad digital son elementos tales como aplicaciones de la organización, servicios web, redes, Hardware, información física o digital, recurso humano, entre otros, que utiliza la organización para funcionar en el entorno digital.

- **Apetito de riesgo:** Es el nivel de riesgo que la entidad puede aceptar, relacionado con sus Objetivos, el marco legal y las disposiciones de la Alta Dirección y del Órgano de Gobierno.

- **Capacidad de riesgo:** Es el máximo valor del nivel de riesgo que una Entidad puede soportar y a partir del cual se considera por la Alta Dirección y el Órgano de Gobierno que no sería posible el logro de los objetivos de la Entidad.

- **Causa:** todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo

- **Causa Inmediata:** Circunstancias bajo las cuales se presenta el riesgo, pero no constituyen la causa principal o base para que se presente el riesgo.

- **Causa Raíz:** Causa principal o básica, corresponde a las razones por la cuales se puede presentar el riesgo.

- **Consecuencia:** los efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

- **Control:** Medida que permite reducir o mitigar un riesgo

- **Disponibilidad:** Propiedad de ser accesible y utilizable a demanda por una entidad.

- **Factores de Riesgo:** Son las fuentes generadoras de riesgos.
- **Integridad:** Propiedad de exactitud y completitud.
- **Impacto:** las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Nivel de riesgo:** Es el valor que se determina a partir de combinar la probabilidad de ocurrencia de un evento potencialmente dañino y la magnitud del impacto que este evento traería sobre la capacidad institucional de alcanzar los objetivos**.**
- **Plan Anticorrupción y de Atención al Ciudadano:** Plan que contempla la estrategia de lucha contra la corrupción que debe ser implementada por todas las entidades del orden nacional, departamental y municipal.
- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. La probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.
- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.
- **Riesgo de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).
- **Riesgo de Corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado
- **Riesgo Inherente**: Nivel de riesgo propio de la actividad. El resultado de combinar la probabilidad con el impacto nos permite determinar el nivel del riesgo inherente, dentro de unas escalas de severidad.
- **Riesgo Residual**: El resultado de aplicar la efectividad de los controles al riesgo inherente.

- **Tolerancia del riesgo:** Es el valor de la máxima desviación admisible del nivel de riesgo con respecto al valor del Apetito de riesgo determinado por la entidad.

- **Vulnerabilidad:** Representan la debilidad de un activo o de un control que puede ser explotada por una o más amenazas

7. ESTRUCTURA PARA LA IDENTIFICACIÓN DEL RIESGO

7.1 IDENTIFICACIÓN DEL RIESGO

ANALIZAR LOS OBJETIVOS ESTRATEGICOS Y DE PROCESOS

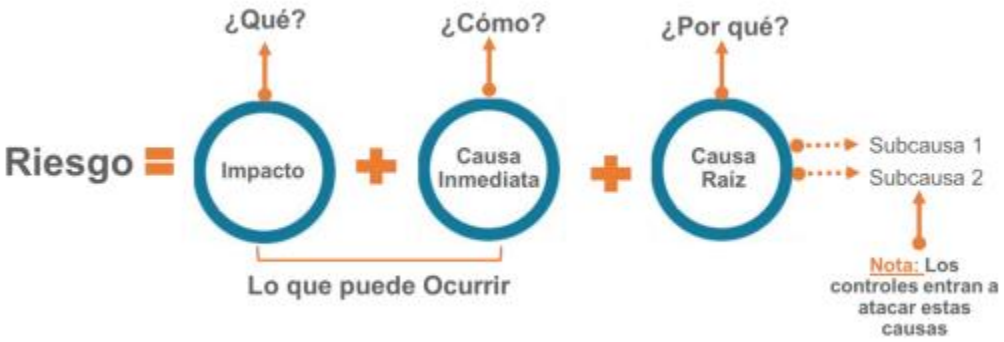
Los objetivos de los procesos se deben analizar con base en las características mínimas, deberán ser específicos, medibles, alcanzables, relevantes y temporales. Así mismo, se debe revisar si están alineados con la Misión y Visión de la entidad, asegurándose que los objetivos de proceso contribuyen a los objetivos estratégicos

La entidad debe analizar los objetivos e identificar los posibles riesgos que afectan su cumplimiento y que puedan ocasionar su éxito o fracaso. Éstos se deben actualizar, por medio de un ejercicio participativo, que por lo general se lleva a cabo entre los líderes de proceso, equipo colaborador, quienes haciendo un análisis del proceso e identifican sus posibles riesgos asociados.

De este modo, para el desarrollo de esta etapa, se deben considerar los siguientes componentes:

- ***DESCRIPCIÓN DEL RIESGO***:

La descripción del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso. Se propone una estructura que facilita su redacción y claridad que inicia con la frase **POSIBILIDAD DE** y se analizan los siguientes aspectos:



La anterior estructura evita la subjetividad en la redacción y permite entender la forma como se puede manifestar el riesgo, así como sus causas inmediatas y causas principales o raíz, esta es información esencial para la definición de controles en la etapa de valoración del riesgo.

Desglosando la estructura propuesta tenemos:

- **Impacto:** Las consecuencias que puede ocasionar a la organización la materialización del riesgo.
- **Causa inmediata:** Circunstancias o situaciones más evidentes sobre las cuales se presenta el riesgo, las mismas no constituyen la causa principal o base para que se presente el riesgo.
- **Causa raíz:** Es la causa principal o básica, corresponden a las razones por la cuales se puede presentar el riesgo, so n la base para la definición de controles en la etapa de valoración del riesgo. Se debe tener en cuenta que para un mismo riesgo puede n existir más de una causa que puede ser analizada.

- ***FACTORES DE RIESGO:***

Se establecen los factores de riesgo como insumo para determinar las causas generadoras de riesgo; por esta razón, cada una de las causas generadoras del riesgo identificado, deben estar asociadas al factor externo o interno de riesgo, según corresponda.

FACTORES INTERNOS

- Actividades y controles gerenciales
- Actividades individuales
- Aspectos técnicos y tecnológicos
- Económico (Por falta de recursos)
- Relaciones comerciales y legales
- Comportamiento Humano

FACTORES EXTERNOS

- Circunstancias políticas
- Eventos naturales

- ***CASUAS DEL RIESGO:***

Las causas son los medios o circunstancias directamente relacionados con los factores internos o externo que permiten la materialización del riesgo. Se debe garantizar la coherencia entre las causas y el riesgo identificado, teniendo en cuenta que los controles estarán orientados a la eliminación o mitigación de causas asociadas al riesgo. “Una definición inadecuada de las causas, conlleva a un tratamiento incipiente y poco efectivo de los riesgos identificados por definición errada de los controles”.

- ***CONSECUENCIAS DEL RIESGO***

Son los efectos sobre los objetivos de los procesos y de la entidad, que se generan o pueden generarse con la materialización del riesgo; generalmente se dan sobre las personas o los bienes materiales o inmateriales con incidencias importantes tales como:

- Daños físicos
- Fallecimiento
- Sanciones
- Pérdidas económicas
- Pérdidas de información
- Pérdidas de bienes
- Pérdidas de imagen, credibilidad y confianza,
- Interrupción del servicio
- Daño ambiental.

Se deben determinar las consecuencias del riesgo en escala ascendente; definiendo cual podría ser el efecto menor que puede causar la materialización del riesgo hasta llegar al efecto mayor generado, el cual deberá ser el elegido.

CLASIFICACIÓN DEL RIESGO EN ENTIDADES PUBLICAS

De acuerdo con la naturaleza de la entidad, los objetivos institucionales y el ciclo de operación, se han identificado los siguientes tipos de riesgos: de **Proceso,** de **Proyecto y** de **Corrupción.**

Riesgos de Proceso: Aquellos riesgos asociados al logro de los objetivos de los procesos institucionales, se identifican y/o validan en cada vigencia por los líderes de proceso y sus respectivos equipos de trabajo a través de la metodología propia de Función Pública y se clasifican en:

1. Estratégicos: Asociado a la administración de la Entidad y se enfoca a asuntos globales relacionados con la misión y el cumplimiento de los objetivos estratégicos, la definición de políticas, diseño y conceptualización de la entidad por parte de la alta gerencia.
2. De imagen: Relacionado con la percepción y la confianza por parte de la ciudadanía hacia la Institución.
3. Operativos: Comprenden riesgos provenientes del funcionamiento y operatividad de los sistemas de información institucional, de la definición de los procesos, la estructura de la entidad y la articulación entre dependencias.
4. Financieros: Relacionado con el manejo de recursos que incluyen la ejecución presupuestal, la elaboración de los estados financieros, los pagos, manejos de excedentes de tesorería y el manejo sobre los bienes.
5. Cumplimiento y conformidad: Se asocian con la capacidad de la entidad para cumplir con los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
6. Tecnológicos: Están relacionados con la capacidad tecnológica de la Entidad para satisfacer sus necesidades actuales y futuras y el cumplimiento de la misión.
7. De corrupción: Relacionados con acciones, omisiones, uso indebido del poder, de los recursos o de la información para la obtención de un beneficio particular o de un tercero.
8. De información: Se asocia a la calidad, seguridad, oportunidad, pertinencia y confiabilidad de la información agregada y desagregada.

Riesgos de Proyecto: Son aquellos riesgos asociados a los Proyectos de Gestión identificados en cada vigencia y pretenden tratar eventos y grupos de interés que pudieran impedir el resultado esperado; generalmente están relacionados al costo, tiempo y calidad del proyecto, a las fases y áreas de conocimiento y son analizados por los líderes de proceso una vez se definen los planes de trabajo de cada proyecto en cada vigencia y sus acciones de control formarán parte de las actividades propias del proyecto. La Entidad ha establecido los siguientes riesgos de proyecto.

1. Financieros: Relacionados con el manejo de recursos asociados al proyecto, la ejecución presupuestal, los pagos del proyecto.
2. Tecnológico: Relacionados con la capacidad tecnológica de la Entidad para atender el propósito del proyecto y la generación de resultados de este.
3. De calidad: Relacionados con las políticas de aseguramiento y control de calidad.
4. Contractual: Relacionado con los atrasos o incumplimiento de los contratos en cada vigencia.
5. Cumplimiento: Se asocian con el cumplimiento, por parte de la entidad, de los requisitos legales, contractuales, de ética pública y en general con su compromiso ante la comunidad.
6. Estratégico: Relacionado con la priorización, métricas y alcance del proyecto frente a las metas.
7. Comunicación: Relacionado con los canales y medios utilizados para informar durante las diferentes etapas del proyecto y la inoportunidad de la comunicación.
8. Recurso Humano: Se asocia a la cualificación, competencia y disponibilidad de personal requerido para realizar el proyecto**.**
9. Integración: Se refiere a la integración de sistemas, áreas, entidades, etapas y demás elementos que se requieran coordinar para el desarrollo del proyecto.
10. Grupos de Interés: Se refiere al reconocimiento pleno de los grupos de interés asociados al proyecto, sus necesidades, expectativas, aportes y motivaciones.

Riesgos de Corrupción: Son los eventos que, por acción u omisión, mediante el uso indebido del poder, de los recursos o de la información, se lesionen los intereses de una entidad y, en consecuencia, del Estado, para la obtención de un beneficio particular4, se identifican en cada vigencia junto con los proyectos de proceso, se administran mediante el Mapa de riesgos institucional y se determinan acciones preventivas permanentes para evitar su materialización.

Por otro lado, la Guía de administración de riesgos y diseño de controles emitida por la función pública, permite agrupar los riesgos identificados en las siguientes categorías:

Ejecución y administración de procesos	Pérdidas derivadas de errores en la ejecución y administración de procesos.
Fraude externo	Pérdida derivada de actos de fraude por personas ajenas a la organización (no participa personal de la entidad).
Fraude interno	Pérdida debido a actos de fraude, actuaciones irregulares, comisión de hechos delictivos abuso de confianza, apropiación indebida, incumplimiento de regulaciones legales o internas de la entidad en las cuales está involucrado por lo menos 1 participante interno de la organización, son realizadas de forma intencional y/o con ánimo de lucro para sí mismo o para terceros.
Fallas tecnológicas	Errores en *hardware*, *software*, telecomunicaciones, interrupción de servicios básicos.
Relaciones laborales	Pérdidas que surgen de acciones contrarias a las leyes o acuerdos de empleo, salud o seguridad, del pago de demandas por daños personales o de discriminación.
Usuarios, productos y prácticas	Fallas negligentes o involuntarias de las obligaciones frente a los usuarios y que impiden satisfacer una obligación profesional frente a éstos.
Daños a activos fijos/ eventos externos	Pérdida por daños o extravíos de los activos fijos por desastres naturales u otros riesgos/eventos externos como atentados, vandalismo, orden público.

RIESGOS DE CORRUPCIÓN:

Las etapas que los conforman son las siguientes:

1. Análisis del contexto estratégico
2. Identificación de los factores de riesgo/causa o actividad generadora del riesgo.
3. Identificación y definición de los riesgos: teniendo en cuenta que cumpla con 4 aspectos: acción u omisión, uso del poder, desviar la gestión de lo público, para beneficio propio o privado.

RIESGO DE CORRUPCIÓN
Definición de riesgo de corrupción: **Riesgo de corrupción:** posibilidad de que por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. *"Esto implica que las prácticas corruptas son realizadas por actores públicos y/o privados con poder e incidencia en la toma de decisiones y la administración de los bienes públicos" (Conpes N° 167 de 2013).* Es necesario que en la descripción del riesgo concurran los **componentes de su definición**, así: ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, se sugiere la utilización de la matriz de definición de riesgo de corrupción y la matriz de riesgos de gestión por separado, incorporando cada uno de los componentes de su definición.

MATRIZ: DEFINICIÓN DEL RIESGO DE CORRUPCIÓN				
Descripción del riesgo	**Acción u omisión**	**Uso del poder**	**Desviar la gestión de lo público**	**Beneficio privado**
Posibilidad de recibir o solicitar cualquier dádiva o beneficio a nombre propio o de terceros con el fin de celebrar un contrato.	X	X	X	X

Fuente: Secretaría de Transparencia de la Presidencia de la República.

7.2 ANALISIS Y VALORACIÓN DEL RIESGO

Para el análisis de la valoración del riesgo, se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias e impacto.

- ***DETERMINAR LA PROBABILIDAD***

Se entiende como la posibilidad de ocurrencia del riesgo. Para efectos de este análisis, la probabilidad de ocurrencia está asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

A continuación, se muestra una tabla de actividades típicas relacionadas con la gestión de una entidad pública, bajo las cuales se definen las escalas de probabilidad:

	Frecuencia de la Actividad	Probabilidad
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

PARA RIESGOS DE GESTION U OPERATIVOS

CRITERIOS DE PROBABILIDAD

Descriptor	Frecuencia	Calificación de la probabilidad
1. Rara vez	No se ha presentado en los últimos 5 años	1
2. Improbable/Poco probable que ocurra	Se ha presentado al menos 1 vez en los últimos 5 años	2
3. Posible que ocurra	Se ha presentado al menos 1 vez en los últimos 2 años	3
4. Probable que ocurra	Se ha presentado al menos 1 vez en el último año	4
5. es casi seguro que ocurra	Se ha presentado más de 1 vez en el año	5

- ***DETERMINAR EL IMPACTO***

Para la construcción de la tabla de criterios se definen los impactos económicos y reputacionales como las variables principales.

Cuando se presenten ambos impactos para un riesgo, tanto económico como reputacional, con diferentes niveles se debe tomar el nivel más alto.

Bajo este esquema se facilita el análisis para el líder del proceso, dado que se puede considerar información objetiva para su establecimiento, eliminando la subjetividad que usualmente puede darse en este tipo de análisis.

Nivel	Calificación	Impacto (consecuencias) Cualitativo
Leve	1	✓ No hay interrupción de las operaciones de la entidad ✓ No se generan sanciones económicas o administrativas. ✓ No se afecta la imagen institucional de forma significativa.
Menor	2	✓ Interrupción de las operaciones de la Entidad por algunas horas. ✓ Reclamaciones o quejas de los usuarios que implican investigaciones internas disciplinarias. ✓ Imagen institucional afectada localmente por retrasos en la prestación del servicio a los usuarios o ciudadanos.
Moderado	3	✓ Interrupción de las operaciones de la Entidad por un (1) día. ✓ Reclamaciones o quejas de los usuarios que podrían implicar una denuncia ante los entes reguladores o una demanda de largo alcance para la entidad. ✓ Inoportunidad en la información ocasionando retrasos en la atención a los usuarios. ✓ Reproceso de actividades y aumento de carga operativa. ✓ Imagen institucional afectada en el orden nacional o regional por retrasos en la prestación del servicio a los usuarios o ciudadanos. ✓ Investigaciones penales, fiscales o disciplinarias.
Mayor	4	✓ Interrupción de las operaciones de la Entidad por más de dos (2) días. ✓ Pérdida de información crítica que puede ser recuperada de forma parcial o incompleta. ✓ Sanción por parte del ente de control u otro ente regulador. ✓ Incumplimiento en las metas y objetivos institucionales afectando el cumplimiento en las metas de gobierno. ✓ Imagen institucional afectada en el orden nacional o regional por incumplimientos en la prestación del servicio a los usuarios o ciudadanos.
Catastrófico	5	✓ Interrupción de las operaciones de la Entidad por más de cinco (5) días. ✓ Intervención por parte de un ente de control u otro ente regulador. ✓ Pérdida de Información crítica para la entidad que no se puede recuperar. ✓ Incumplimiento en las metas y objetivos institucionales afectando de forma grave la ejecución presupuestal. ✓ Imagen institucional afectada en el orden nacional o regional por actos o hechos de corrupción comprobados.

PARA RIESGOS DE CORRUPCIÓN

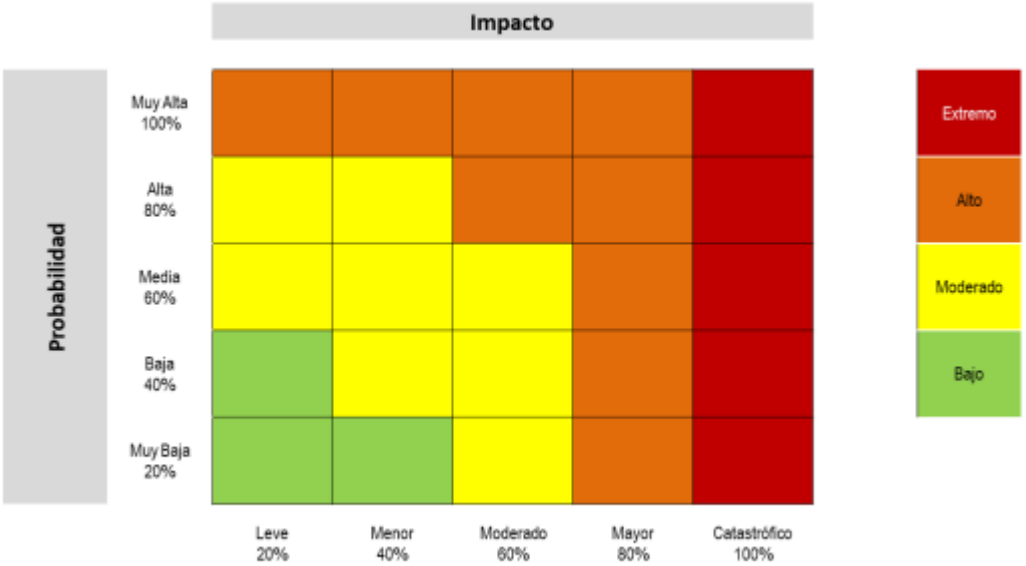
Para cada riesgo identificado se debe aplicar los siguientes criterios:

CRITERIOS PARA CALIFICAR EL IMPACTO EN RIESGOS DE CORRUPCIÓN

	RIESGO:		
N°	**PREGUNTA: ¿SI EL RIESGO DE CORRUPCION SE MATERIALIZA PODRIA…**	**RESPUESTA**	
		SI	**NO**
1	¿AFECTAR AL GRUPO DE FUNCIONARIOS DEL PROCESO?		
2	¿AFECTAR EL CUMPLIMIENTO DE METAS Y OBJETIVOS DE LA DEPENDENCIA?		
3	¿AFECTAR EL CUMPLIMIENTO DE MISION DE LA ENTIDAD?		
4	¿AFECTAR EL CUMPLIMIENTO DE LA MISION AL SECTOR AL QUE PERTENECE LA ENTIDAD?		
5	¿GENERAR PERDIDA DE CONFIANZA DE LA ENTIDAD, AFECTANDO SU REPUTACIÓN?		
6	¿GENERAR PERDIDA DE RECURSOS ECONOMICOS?		
7	¿AFECTAR LA GENERACION DE LOS PRODUCTOS O LA PRESTACIÓN DE SERVICIOS?		
8	¿DAR LUGAR AL DETRIMENTO DE CALIDAD DE VIDA DE LA COMUNIDAD POR LA PERDIDA DEL BIEN, SERVICIOS O RECURSOS PUBLICOS?		
9	¿GENERAR PERDIDA DE INFORMACION DE LA ENTIDAD?		
10	¿GENERAR INTERVENCIÓN DE LOS ORGANOS DE CONTROL, DE LA FISCALIA U OTRO ENTE?		
11	¿DAR LUGAR A PROCESOS SANCIONATORIOS?		
12	¿DAR LUGAR A PROCESOS DISCIPLINARIOS?		
13	¿DAR LUGAR A PROCESOS FISCALES?		
14	¿DAR LUGAR A PROCESOS PENALES?		
15	¿GENERAR PERDIDA DE CREDIBIIIDAD DEL SECTOR?		
16	¿OCASIONAR LESIONES FISICAS O PERDIDAS DE VIDAS HUMANAS?		
17	¿AFECTAR LA IMAGEN REGIONAL?		
18	¿AFECTAR LA IMAGEN NACIONAL?		
19	¿GENERAR DAÑO AMBIENTAL?		
	TOTAL		

EVALUACIÓN DE RIESGOS

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE). **Análisis preliminar (riesgo inherente):** trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto, sin tener en cuenta la aplicación de controles. Este grado se analiza dentro de un mapa de calor como el que se muestra a continuación.



PROBABILIDAD	IMPACTO				
	1 - Leve	2 - Menor	3 - Moderado	4 - Mayor	5 - Catastrófico
5 - Muy Alta	A	A	A	A	E
4 - Alta	M	M	A	A	E
3 - Media	M	M	M	A	E
2 - Baja	B	M	M	A	E
1 - Muy Baja	B	B	M	A	E

IDENTIFICACIÓN Y VALORACIÓN DE CONTROLES

Un control se define como la medida que permite reducir o mitigar el riesgo. Para la valoración de controles se debe tener en cuenta:

- ✓ La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- ✓ Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.

Estructura para la descripción del control: para una adecuada redacción del control se propone una estructura que facilitará más adelante entender su tipología y otros atributos para su valoración. La estructura es la siguiente:

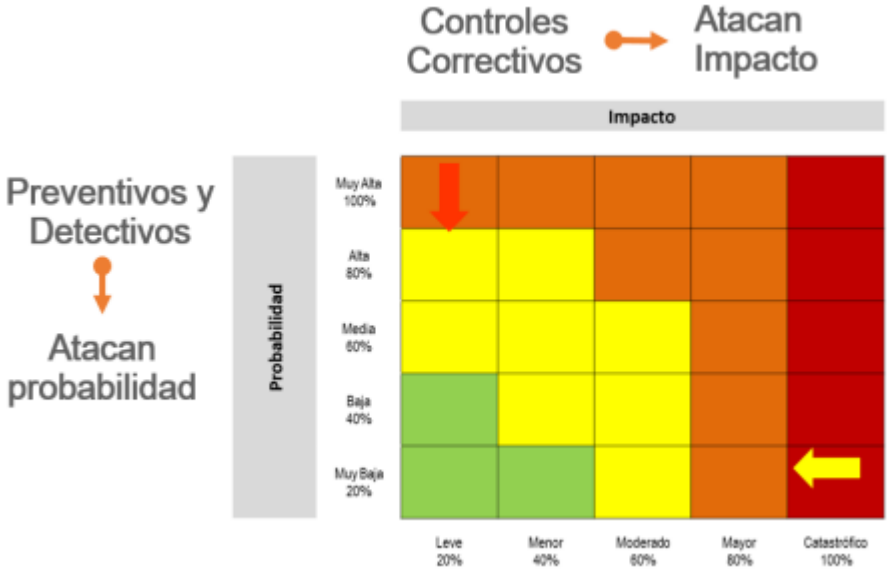
- ✓ **Responsable de ejecutar el control:** identifica el cargo del servidor que ejecuta el control, en caso de que sean controles automáticos se identificará el sistema que realiza la actividad.
- ✓ **Acción**: se determina mediante verbos que indican la acción que deben realizar como parte del control.
- ✓ **Complemento:** corresponde a los detalles que permiten identificar claramente el objeto del control.

Tipología de Controles: Dentro de los controles se encuentran los siguientes:

- ✓ **Control preventivo**: Control accionado en la entrada del proceso y antes de que se realice la actividad originadora del riesgo, se busca establecer las condiciones que aseguren el resultado final esperado.
- ✓ **Control detectivo**: Control accionado durante la ejecución del proceso. Estos controles detectan el riesgo, pero generan reprocesos.
- ✓ **Control correctivo**: Control accionado en la salida del proceso y después de que se materializa el riesgo. Estos controles tienen costos implícitos

Así mismo, de acuerdo con la forma como se ejecutan tenemos:

- ✓ **Control manual:** Controles que son ejecutados por personas.
- ✓ **Control automático:** Son ejecutados por un sistema.



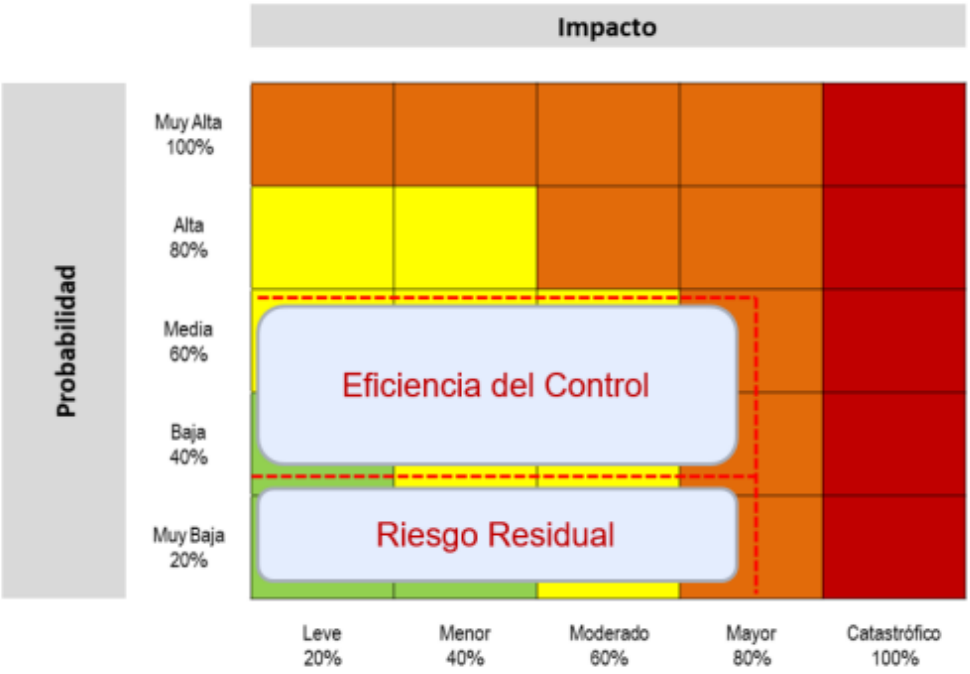
EVALUACIÓN DE CONTROLES PARA RIESGOS DE GESTION U OPERATIVOS Y DE RIESGOS DE CORRUPCION

Para evaluar los controles tanto de los riesgos de gestión, como los de corrupción, se aplica las valoraciones teniendo en cuenta la siguiente tabla:

Criterios Para Calificar la Solidez del Control	
a. El Control No Aplica	N
b. El Control es Redundante	R
c. El Control es efectivo, es clave y no se cumple	1
d. El Control es efectivo, no es clave y no se cumple	1
e. El Control es efectivo, no es clave y se cumple	4
f. El Control es efectivo, es clave y se cumple	5
g. El Control es aceptable, es clave y no se cumple	1
h. El Control es aceptable, no es clave y no se cumple	1
i. El Control es aceptable, no es clave y se cumple	3
j. El Control es aceptable, es clave y se cumple	4
k. El Control es inaceptable, es clave y no se cumple	1
l. El Control es inaceptable, no es clave y no se cumple	1
m. El Control es inaceptable, no es clave y se cumple	2
n. El Control es inaceptable, es clave y se cumple	3

NIVEL DE RIESGO (RIESGO RESIDUAL)

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Para la aplicación de los controles se debe tener en cuenta que los estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.



7.3 TRATAMIENTO DEL RIESGO

Para el tratamiento del riesgo, se busca establecer definir los siguientes aspectos:

- ✓ **Estrategias para combatir el riesgo**

Decisión que se toma frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar. Se analiza frente al riesgo residual, esto para procesos en funcionamiento, cuando se trate de procesos nuevos, se procede a partir del riesgo inherente.

Frente al plan de acción referido para la opción de reducir, es importante mencionar que, conceptualmente y de manera general, se trata de una herramienta de planificación empleada para la gestión y control de tareas o proyectos. Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo; así mismo, las entidades deben incluir las matrices relacionadas con la redacción de este tipo de riesgos, las preguntas para la definición del nivel de impacto y la matriz de calor correspondiente, donde se precisan las zonas de severidad aplicables.

7.4 HERRAMIENTAS PARA LA GESTION DEL RIESGO

Como producto de la aplicación de la metodología se contará con los mapas de riesgo. Además de esta herramienta, se encuentra la siguiente:

INDICADORES CLAVE DE RIESGO

Hace referencia a una colección de datos históricos, por periodos de tiempo, relacionados con algún evento cuyo comportamiento puede indicar una mayor o menor exposición a determinados riesgos. No indica la materialización de los riesgos, pero sugiere que algo no funciona adecuadamente y, por lo tanto, se debe investigar.

Un indicador clave de riesgo, o KRI, por su sigla en inglés (Key Risk Indicators), permite capturar la ocurrencia de un incidente que se asocia a un riesgo identificado previamente y que es considerado alto, lo cual permite llevar un registro de ocurrencias y evaluar a través de su tendencia la eficacia de los controles que se disponen para mitigarlos.

7.5 MONITOREO Y REVISION

Los gerentes públicos y los líderes de los procesos, en conjunto con sus equipos, deben monitorear y revisar periódicamente la gestión de riesgos de corrupción y si es el caso ajustarlo (primera línea de defensa).

Le corresponde, igualmente, a la oficina de planeación adelantar el monitoreo (segunda línea de defensa), para este propósito se sugiere elaborar una matriz. Dicho monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de llevar a cabo un seguimiento constante a la gestión del riesgo y a la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características, una actividad difícil de detectar. Para tal efecto deben atender a los lineamientos y las actividades descritas en la primera y segunda línea de defensa de este documento.

8. LINEAMIENTOS RIESGOS DE SEGURIDAD DE LA INFORMACIÓN

En primer lugar, se debe tener en cuenta que la política de seguridad digital se vincula al modelo de seguridad y privacidad de la información (MSPI), el cual se encuentra alineado con el marco de referencia de arquitectura TI y soporta transversalmente los otros habilitadores de la política de gobierno digital: seguridad de la información, arquitectura, servicios ciudadanos digitales.

Teniendo en cuenta lo anterior, la Terminal Metropolitana de Transportes de Barranquilla S.A. elaboró y aprobó el siguiente documento **https://www.ttbaq.com.co/wp-content/uploads/2022/PLANES/10.PLAN-DE-TRATAMIENTO-DE-RIESGOS.pdf**, el cual cumple con los parámetros y lineamientos definidos por el Gobierno nacional en esta materia.

9. *METODOLOGIA PARA LA GESTION DE RIESGOS EN LA TERMINAL METROPOLITANA DE TRANSPORTES DE BARRANQUILLA S.A.*

Atendiendo la metodología de Función Pública Guía para la administración del riesgo y los lineamientos de la secretaria de Transparencia de la Presidencia de la República con respecto a las políticas de transparencia y acceso a la información pública y lucha contra la corrupción se definen los siguientes pasos para la adecuada gestión del riesgo que deberán seguir los equipos de trabajo de cada proceso de la entidad al inicio de cada vigencia o cuando amerite:

RIESGOS DE CORRUPCIÓN: Para este tipo de riesgos, solo se colocó un factor generalizado, debido a que la mayoría de las causas generadoras son a nivel interno, es decir se producen más comúnmente al interior de la entidad. A continuación, se muestra el esquema aplicado para la TTBAQ por procesos

PLANEACIÓN ESTRATEGICA

- Concentración de autoridad o exceso de poder.
- Extralimitación de funciones.

FORTALECIMIENTO DE TECNOLOGIA E INFORMACIÓN Y COMUNICACIONES

- Ausencia de controles en los archivos tecnológicos
- Ausencia de sistemas de información que pueden facilitar el acceso a información y su posible manipulación o adulteración.
- Ocultar la información considerada pública para los usuarios.
- Ausencia o debilidad de canales de comunicación
- Uso y/o divulgación de información privilegiada por funcionarios y contratistas en beneficios de terceros.

CONTROL Y SEGUIMIENTO OPERATIVO

- Cobros asociados al trámite.
- Tráfico de influencias: (amiguismo, persona influyente).
- Influencia de tramitadores.

GESTION DEL TALENTO HUMANO

- Deficiencias en los procesos de selección de personal
- Presentación y /o radicación de documentación falsa.

GESTION FINANCIERA

- Inclusión de gastos no autorizados.
- Inversiones de dineros públicos en entidades de dudosa solidez financiera a cambio de beneficios indebidos para servidores públicos encargados de su administración.
- Inexistencia de archivos contables.
- Afectar rubros que no corresponden con el objeto del gasto en beneficio propio o a cambio de una retribución económica.
- Acuerdos entre personas externas, funcionarios y /o contratistas.

GESTION DOCUMENTAL

- No aplicación de herramientas archivísticas
- Alteración de información.

GESTION DE SERVICIOS ADMINISTRATIVOS Y LOGISTICOS

- Tráfico de influencias para la adjudicación de contratos
- Concentrar las labores de supervisión en poco personal.
- Supervisión de contratos

GESTION JURIDICA Y DE CONTRATACIÓN

- Estudios previos o de factibilidad deficientes.
- Estudios previos o de factibilidad manipulados por personal interesado en el futuro proceso de contratación. (Estableciendo necesidades inexistentes o aspectos que benefician a una firma en particular).
- Pliegos de condiciones hechos a la medida de una firma en particular.
- Disposiciones establecidas en los pliegos de condiciones que permiten a los participantes direccionar los procesos hacia un grupo en particular. (Ej.: media geométrica).
- Adendas que cambian condiciones generales del proceso para favorecer a grupos determinados.

- Urgencia manifiesta inexistente.
- Contratar con compañías de papel que no cuentan con experiencia.

PARA RIESGOS DE CORRUPCIÓN

DESCRIPCION DEL RIESGO	ACCION U OMISION	USO DEL PODER	DESVIAR LA GESTION DE LO PUBLICO	BENEFICIO PRIVADO	EL RIESGO ES DE CORUPCION ?
Posibilidad de alterar la información presentada a la direccion y a los entes de control, mediante la modificacion, omision o manipulación de los informes, seguimientos, auditorias y demas informacion que maneja la oficina , para el beneficio propio o de terceros.	X	X	X	X	SI
Posibilidad de incumplir con la aplicaciones de la normatividad y demas lineamientos establecidos por ley, debido a Interpretaciones subjetivas de la misma, con el fin de obtener un beneficio propio y/o para terceros.	x	x	x	x	SI

POSIBILIDAD + IMPACTO + CAUSA INMEDIATA - CAUSA RAIZ

Paso 2: Mediante lluvia de ideas al interior del equipo de trabajo del proceso, se analizan las causas que podrían afectar el cumplimiento del objetivo del proceso, se identifica el riesgo, sus causas y consecuencias.

IDENTIFICACIÓN DEL RIESGO					
No.	Proceso	Tipo de riesgo	Causas	Riesgo	Consecuencias
1					
2					

Paso 3: Se procede al análisis y valoración del riesgo identificado. Con la matriz de probabilidad e impacto se determina el nivel del riesgo inherente

PROBABILIDAD (de ocurrencia del riesgo)		
Probabilidad (1 - 5)	Frecuencia de la actividad	Calificación de la probabilidad
	0	

NOTA:	PARA CALIFICAR LA PROBABILIDAD DE QUE OCURRA EL RIESGO, ES DE 1 - 5, SIGUIENDO LA TABLA A CONTINUACIÓN	
1	La actividad que conlleva el riesgo se ejecuta como máximos 2 veces por año	
2	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	
3	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	
4	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	
5	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	

IMPACTO (Si el riesgo sucede)	RIESGO INHERENTE		
Niveles para calificar el impacto (1 – 5)	Calificacion de la consecuencia	Factor de riesgo (Probabilidad x Consecuencia)	Zona de riesgo
	0	0	

NOTA:	PARA CALIFICAR EL IMPACTO DEL RIESGO , ES DE 1 - 5, acompañado el numero de un guión y el NIVEL de impacto como se muestra a continuación:
	1-Leve
	2-Menor
	3-Moderado
	4-Alta
	5-Catastrofico

Paso 4: Determinar el control actual relacionada con cada riesgo identificado

CONTROLES		ATRIBUTOS DE LOS CONTROLES				
Controles	Responsable de la aplicación del control	¿El control es preventivo (25), detectivo (15) o correctivo (10)?	¿El Control es Automático (25) o Manual (15)?	¿El Control esta Documentado (20) o Sin Documentar (0)?	¿La Frecuencia del Control es Continua (15) o Aleatoria (10)?	¿Se deja evidencia con registro (15) o no (0) de la ejecución del control?

Paso 5: Se califican los controles y se determina el nuevo nivel del riesgo, se documenta el resultado final como Riesgo Residual, calificando su manejo.

PARA RIESGOS DE GESTIÓN / OPERATIVOS / CORRUPCIÓN

Criterios Para Calificar la Solidez del Control	
a. El Control No Aplica	N
b. El Control es Redundante	R
c. El Control es efectivo, es clave y no se cumple	1
d. El Control es efectivo, no es clave y no se cumple	1
e. El Control es efectivo, no es clave y se cumple	4
f. El Control es efectivo, es clave y se cumple	5
g. El Control es aceptable, es clave y no se cumple	1
h. El Control es aceptable, no es clave y no se cumple	1
i. El Control es aceptable, no es clave y se cumple	3
j. El Control es aceptable, es clave y se cumple	4
k. El Control es inaceptable, es clave y no se cumple	1
l. El Control es inaceptable, no es clave y no se cumple	1
m. El Control es inaceptable, no es clave y se cumple	2
n. El Control es inaceptable, es clave y se cumple	3

PASO 6: PARA LOS RIESGOS DE CORRUPCIÓN

Para los riesgos asociados a posibles actos de corrupción se deben definir los lineamientos para su tratamiento. Es claro que este tipo de riesgos no admiten aceptación del riesgo.

OPCIONES DE MANEJO PARA RIESGOS DE CORRUPCIÓN:

- Reducir el riesgo
- Evitar el riesgo
- Transferir el riesgo

TRATAMIENTO DEL RIESGO			
ACCIONES PARA MITIGAR EL RIESGO	FECHA A IMPLEMENTAR	RESPONSABLE DE LA ACCION	INDICADORES

Paso 7: La Oficina de Planeación se encarga de consolidar consolida el Mapa de riesgos Institucional con los riesgos de gestión y de Corrupción, lo presenta ante el Comité Institucional de gestión y Desempeño y lo publica, deberá publicarse antes del 31 de enero de cada vigencia, en la pagina web de la entidad.

Paso 8: Los líderes de los procesos en conjunto con sus equipos deben monitorear y revisar periódicamente el documento del Mapa de Riesgos de gestión y Corrupción y si es del caso ajustarlo. Según el resultado de la administración del riesgo, el líder del proceso solicitará ajuste a los riesgos o controles y elaborará acciones de mejoramiento o correctivas correspondientes.

La periodicidad de seguimiento de los riesgos de gestión por parte de los lideres y sus equipos de trabajo es permanente, a través de reuniones de autocontrol. La oficina de Control Interno realiza verificación cuatrimestralmente, de conformidad con lo establecido por la ley (Con corte a abril 30, agosto 30 y diciembre 30),

PRIMER SEGUIMIENTO Y MONITOREO			
ACCIONES IMPLEMENTADAS	% DE AVANCE	EVIDENCIAS	OBSERVACIONES

La oficina de Control interno, realiza seguimiento y monitoreo semestral a la administración de los riesgos de gestión y seguimiento cuatrimestral a los riesgos de corrupción, de conformidad con lo establecido por la ley, o cuando las circunstancias lo ameriten, a partir de Modificaciones o Cambios Sustanciales en el Contexto Estratégico, Modificaciones o Cambios relevantes en los Procesos o Procedimiento o cualquier hecho sobreviviente externo o interno que afecte la Operación de la Institución. Para realizar el seguimiento a las acciones de respuesta y su efectividad se tendrá en cuenta lo definido en el Mapa de Riesgo por Procesos, específicamente los Indicadores de cada acción establecida.

CONTROL DE CAMBIOS			
FECHA	**VERSION**	**DESCRIPCION DEL CAMBIO**	**APROBADO POR**
31/01/2019	1	Emisión del documento	Oficina de Planeación y Presupuesto
17/05/2022	2	Se ajusta el documento de conformidad con la nueva metodología establecida por la función pública “Guía para la administración del riesgo y diseño de controles en entidades públicas “versión 5 y los lineamientos de secretaria de Transparencia de la Presidencia de la República, relacionados *las políticas de transparencia y acceso a la información pública y lucha contra la corrupción*	Comité de Coordinación de Control interno/ Comité institucional de Gestión y Desempeño