TABLA DE CONTENIDO

1. OBJETIVO....4
2. ALCANCE....4
3. RESPONSABLES....4
4. DOCUMENTOS DE REFERENCIA....5
5. DEFINICIONES....6
6. CONDICIONES GENERALES....13
6.1 Responsabilidades en la Administración del Riesgo....14
6.2 Clasificación del Riesgo....20
7. POLITICA PARA LA GESTIÓN DE LOS RIESGOS EN TRANSMILENIO S.A. 22
7.1 Objetivo....22
7.1.1 Objetivos específicos....22
7.2 Alcance....22
7.3 Principios....23
7.4 Declaración de la política....23
7.5 Metodologías a aplicar para la administración del Riesgo....26
7.6 Nivel de aceptación del riesgo....26
7.7 Niveles para calificar el impacto....27
7.8 Tratamiento de Riesgos....27
7.9. Estrategias para dar cumplimiento a la política....27
7.10 Cultura de gestión de riesgos....28
7.11 Seguimiento al nivel del riesgo residual....28
8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO....28
8.1. Establecimiento del contexto estratégico....29
8.3. Análisis del riesgo....32
8.4. Evaluación del riesgo....33
8.5. Tratamiento del riesgo....35
8.6. Monitoreo y seguimiento....36
9. COMUNICACIÓN....36

10. ANEXOS.....37

MODIFICACIONES:

VERSION	FECHA	CAMBIO	SOLICITÓ
0	Diciembre de 2015	Primera versión del documento	Jefe Oficina Asesora de Planeación
1	Diciembre de 2017	Actualización General del Documento	Jefe Oficina Asesora de Planeación
2	Marzo 2019	Se realiza la actualización del documento en el marco de la Guía del DAFP para la administración del riesgo y el diseño de controles en entidades públicas. Riesgos de Gestión, Corrupción, y Seguridad Digital. Versión 4.	Jefe Oficina Asesora de Planeación
3	Julio 2019	• Ampliación de la estrategia de socialización de la política de riesgos. • Aclaración del concepto del nivel residual del riesgo. • Se incorporan políticas específicas relacionadas con el reporte de eventos de riesgo y los niveles de responsabilidad tanto de la Junta Directiva como de la Alta Dirección. • Se define la etapa de transición para la instrumentalización de la Política de Riesgos.	Jefe Oficina Asesora de Planeación
4	Agosto 2020	• Incorporación Anexo Guía para el Reporte de eventos de riesgo • Incorporación de políticas de Riesgos de Interrupción • Incorporación Anexo Guía para la aplicación BIA • Ampliación del alcance de las políticas de riesgo a los riesgos de Seguridad de la Información • Ajuste a la metodología de acuerdo con la Guía del DAFP. • Se incluye como anexo los criterios de valoración de los riesgos de seguridad de la información	Jefe Oficina Asesora de Planeación
5	Noviembre 2021	• Capítulo 2. ALCANCE. Se amplía el alcance del Manual en relación con los Riesgos de Seguridad Digital. • Capítulo 3. RESPONSABLES, se incorpora un párrafo donde se aclara que la Dirección de TIC es responsable de la definición y actualización de los criterios para los riesgos de Seguridad Digital. • Se incorporan los capítulos 6.1 donde se aclaran las Responsabilidades en la Administración del Riesgo y 6.2 Tipos de riesgo	Jefe Oficina Asesora de Planeación

VERSION	FECHA	CAMBIO	SOLICITÓ
		• Acorde con Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, que emitió el DAFP en Diciembre de 2020. Versión 5, se ajusta todo el manual. • Se describen cada una de las metodologías que se aplicaran para la administración de los riesgos de gestión, corrupción y seguridad digital acorde con los lineamientos expedidos por DAFP.	
6	Septiembre de 2022	• Se realizan ajustes al documento en cuanto a su estructura separando las tipologías de Gestión del Riesgo en Anexos para facilitar la administración de cada una. • Se ajustan tablas de probabilidad e impacto de los riesgos de gestión • Se incorporan las metodologías de gestión de riesgos de SARLAFT y de Continuidad de negocio	Jefe Oficina Asesora de Planeación
7	Junio de 2024	• Se actualiza el documento teniendo en cuenta la Guía para la Administración del Riesgo y el diseño de controles en entidades públicas V6 del DAFP, que incorpora los riesgos fiscales • Se modifica el término de seguridad digital por Seguridad de la Información	Jefe Oficina Asesora de Planeación

1. OBJETIVO

Establecer las directrices y lineamientos para llevar a cabo una adecuada administración de los riesgos de TRANSMILENIO S.A., definiendo los roles y responsabilidades, así como las metodologías que se aplicarán para la identificación, análisis, valoración, tratamiento, monitoreo, revisión y comunicación de los riesgos; estas etapas se encuentran comprendidas dentro del Sistema de Administración de Riesgos de la Entidad.

2. ALCANCE

Este manual aplica para la administración de los siguientes tipos de riesgos de los procesos definidos en el mapa de procesos institucional así:

- Riesgos de Gestión
- Riesgos de Corrupción
- Riesgos de Seguridad de la Información
- Riesgos de Lavado de Activos y Lucha contra el Terrorismo – SARLAFT
- Riesgos de Interrupción

El componente de riesgos de Seguridad de la Información tendrá aplicación sobre los procesos o áreas que estén incorporados en el alcance del Sistema de Gestión de Seguridad de la Información (SGSI) según la planeación establecida para la vinculación progresiva de dichas áreas en este alcance.

Este documento es para conocimiento y aplicación de todos los servidores públicos y contratistas de TRANSMILENIO S.A.

3. RESPONSABLES

El Profesional Universitario Grado 04 – Gestión Integral de la Oficina Asesora de Planeación, es el responsable por la actualización del manual.

El (la) Jefe de la Oficina Asesora de Planeación o quien haga sus veces será responsable por su aplicación y cumplimiento.

La Dirección de TIC es responsable de la definición y actualización de los criterios para los riesgos de Seguridad de la Información

Todos los gestores de riesgos serán responsables por el cumplimiento de este manual.

La revisión y/o actualización de este documento debe realizarse cuando se considere pertinente por parte de los responsables de su aplicación y cumplimiento.

4. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia.
- **Circular 092 de 2020**. Mediante la cual se establece la Ruta metodológica para la implementación del SARLAFT en las entidades distritales en la Implementación del Sistema de Administración de Riesgos de Lavado de Activos y Financiación del Terrorismo -SARLAFT.
- **Decreto 371 de 2010:** por el cual se establecen lineamientos para preservar y fortalecer la transparencia y para la prevención de la corrupción en las TRANSMILENIO S.A., y Organismos del Distrito Capital.
- **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 2641 de 2012:** por medio del cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011, señalando como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la contenida en el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Octubre de 2018. Versión 4.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Diciembre de 2020. Versión 5.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Noviembre de 2022. Versión 6.
- GTC-ISO-TS 22317:2017. Seguridad de la sociedad. Sistemas de gestión de la continuidad de negocio. Directrices para el análisis de impacto en el negocio (BIA).
- Manual Operativo Sistema de Gestión MIPG. Consejo para la Gestión y Desempeño Institucional. Octubre de 2018.
- Manual de Funciones de TRANSMILENIO S.A.

- NTC – ISO 22300:2021. Seguridad y resiliencia. Vocabulario.
- NTC – ISO 22301:2019. Seguridad y resiliencia. Sistema de gestión de continuidad del negocio. Requisitos.
- Norma ISO 27001 Sistema de Gestión de Seguridad de la Información
- Norma ISO 31000 Gestión de Riesgos. Directrices. Estándar normativo internacional que proporciona las directrices genéricas sobre la gestión del riesgo.
- Protocolo para la identificación y declaración del conflicto de intereses en TRANSMILENIO S.A.
- Políticas Anticorrupción de TRANSMILENIO S.A.
- Programa de Transparencia y Ética Pública de TRANSMILENIO S.A.

5. DEFINICIONES

Aceptar el riesgo: decisión informada de aceptar las consecuencias y probabilidad de un riesgo en particular.

Activo: En el contexto de seguridad de la información 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 en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

Actividades de Control: son las acciones establecidas a través de políticas y procedimientos que contribuyen a garantizar que se lleven a cabo las instrucciones de la dirección para mitigar los riesgos que inciden en el cumplimiento de los objetivos.

Administración de riesgos: conjunto de elementos de control que, al interrelacionarse, permiten a la entidad pública evaluar aquellos eventos negativos, tanto internos como externos, que puedan afectar o impedir el logro de sus objetivos institucionales o los eventos positivos que permitan identificar oportunidades para un mejor cumplimiento de su función. Se constituye en el componente de control que al interactuar sus diferentes elementos le permite a la entidad pública autocontrolar aquellos eventos que pueden afectar el cumplimiento de sus objetivos.

Análisis de riesgo: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

Apetito al 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. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar**.**

Autoevaluación del control: elemento de control que, basado en un conjunto de mecanismos de verificación y evaluación, determina la calidad y efectividad de los controles internos a nivel de los procesos y de cada área organizacional responsable, permitiendo emprender las acciones de mejoramiento del control requeridas. Se basa en una revisión periódica y sistemática de los procesos de la entidad para asegurar que los controles establecidos son aún eficaces y apropiados.

Bien público: Son todos aquellos muebles e inmuebles de propiedad pública (este concepto comprende: bienes del Estado y aquellos productos del ejercicio de una función pública a cargo de particulares). Estos se clasifican en bienes de uso público y bienes fiscales, definidos así: a) Bien de uso público: aquellos cuyo uso pertenece a todos los habitantes del territorio nacional. Ejemplos: Las calles, plazas, puentes, vías, parques etc. b) Bienes fiscales: aquellos que están destinados al cumplimiento de las funciones públicas o servicios públicos (Consejo de Estado, 2012), es decir, afectos al desarrollo de su misión y utilizados para sus actividades. Ejemplos: Los terrenos, edificios, oficinas, colegios, hospitales, otras construcciones, fincas, granjas, equipos, enseres, mobiliario etc.

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. Nota: Tratándose de riesgo fiscal, se usa el término circunstancia inmediata (Causa Inmediata, pero se asocia a la misma causa inmediata).

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

Causa Raíz (Causa Eficiente o Causa Adecuada): Es el evento (acción u omisión) que de presentarse es generador directo de un efecto dañoso sobre los bienes, recursos o intereses patrimoniales de naturaleza pública. Es la condición necesaria, de tal forma que, si ese hecho no se produce, el daño no se genera. Así las cosas, la causa raíz se asocia con aquel hecho potencial generador del daño.

Confidencialidad: Propiedad de la información que la hace no disponible o sea divulgada a individuos, entidades o procesos no autorizados

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. Nota: Tratándose de riesgo fiscal, el impacto siempre será económico y se identificará en la redacción de riesgos como efecto dañoso, sobre bienes públicos, recursos públicos o intereses patrimoniales públicos.

Control: medida que mitiga al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones).

Compartir el riesgo: se asocia con la forma de protección para disminuir las pérdidas que ocurran luego de la materialización de un riesgo, es posible realizarlo mediante contratos, seguros, cláusulas contractuales u otros medios que puedan aplicarse.

Consecuencia: son 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.

Criterios del riesgo: son los términos de referencia frente a los cuales se evalúa la importancia de un riesgo.

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

Evaluación del riesgo: proceso global de las etapas identificación del riesgo, análisis del riesgo y valoración del riesgo. Se busca confrontar los resultados del análisis de riesgo inicial frente a los controles establecidos, con el fin de determinar la zona de riesgo final (Riesgo Residual).

Evento: incidente o situación que ocurre en un lugar y durante un período determinado, este puede ser cierto o incierto y su ocurrencia puede ser única o ser parte de una serie.

Factor de riesgo: son las fuentes generadoras de riesgos

Fuente de riesgo: elemento que, por sí solo o en combinación con otros, tiene el potencial de generar un riesgo.

Frecuencia: medida del coeficiente de ocurrencia de un evento expresado como la cantidad de veces que ha ocurrido un evento en un tiempo dado.

Gestión del Riesgo: proceso efectuado por la alta dirección de la entidad y por todo el personal para proporcionar a la administración un aseguramiento razonable con respecto al logro de los objetivos.

Gestión del Riesgo Fiscal: son las actividades que debe desarrollar cada Entidad y todos los gestores públicos para identificar, valorar, prevenir y mitigar los riesgos fiscales

Gestor Fiscal: Son los servidores públicos y las personas de derecho privado que manejen o administren recursos o fondos públicos, desarrollando actividades económicas, jurídicas y tecnológicas, tendientes a la adecuada y correcta adquisición, planeación, conservación, administración, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes públicos, así como, a la recaudación, manejo e inversión de sus rentas, en orden a cumplir los fines esenciales del Estado (artículo 3 de la Ley 610 de 2000 o la norma que lo sustituya o modifique). A título de ejemplo son gestores fiscales, entre otros (sin perjuicio de las particularidades de cada entidad): representante legal, ordenador del gasto, autorizado para contratar, pagador, tesorero, almacenista.

Gestor público: Es todo aquel que participa, concurre, incide o contribuye directa o indirectamente en el manejo o administración de bienes, recursos o intereses patrimoniales de naturaleza pública, sean o no gestores fiscales, por lo tanto, son todos los gestores públicos y no sólo los que desarrollan gestión fiscal, los llamados a prevenir riesgos fiscales. A título de ejemplo, además de los gestores fiscales, son gestores públicos, entre otros (sin perjuicio de las particularidades de cada entidad): los contratistas, los interventores, los supervisores y en general todos los servidores públicos.

Identificación del riesgo: proceso para encontrar, reconocer y describir los riesgos que pueden ayudar o impedir a una organización a logar o no sus objetivos. En esta etapa se deben establecer las fuentes o factores de riesgo, los eventos o riesgos, sus causas y sus consecuencias. Para el análisis se pueden involucrar datos históricos, análisis teóricos, opiniones informadas y expertas y las necesidades de las partes involucradas.

Impacto: se entiende como las consecuencias que puede ocasionar a la organización la materialización del riesgo.

Intereses patrimoniales de naturaleza pública: Son expectativas razonables de beneficios, que en condiciones normales se espera obtener o recibir y que sean susceptible de estimación económica. A diferencia del recurso público, los intereses patrimoniales de naturaleza pública son expectativas.

Integridad: Propiedad de exactitud y completitud.

Interrupción: incidente bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización.

Mapa de Riesgos: documento con la información resultante de la gestión del riesgo.

Monitorear: comprobar, supervisar, observar, o registrar la forma en que se lleva a cabo una actividad con el fin de identificar sus posibles cambios.

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. En general la fórmula del Nivel del Riesgo poder ser Probabilidad * Impacto, sin embargo, pueden relacionarse las variables a través de otras maneras diferentes a la multiplicación, por ejemplo, mediante una matriz de Probabilidad – Impacto

Parte involucrada: persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada por una decisión o una actividad.

Patrimonio público: se entiende como el conjunto de bienes o recursos o intereses patrimoniales de naturaleza pública, susceptibles de estimación económica (artículo 6 Ley 610 de 2000 y sentencia C340-07).

Pérdida: consecuencia negativa que trae consigo un evento.

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.

Plan de Continuidad del Negocio: información documentada que orienta a una organización para responder una interrupción y reanudar, recuperar y restaurar la oferta de productos y servicios de acuerdo con sus objetivos de continuidad de negocio.

Probabilidad: se entiende como la posibilidad de ocurrencia del riesgo, ésta puede ser medida con criterios de frecuencia o factibilidad.

Proceso: Conjunto de actividades interrelacionadas o que interactúan las cuales transforman entradas en salidas.

Proceso de administración de riesgo: aplicación sistemática de políticas, procedimientos y prácticas de administración a las diferentes etapas de la administración del riesgo.

Punto de Riesgo: Actividades en las que potencialmente se genera riesgo. Tratándose de riesgo fiscal los puntos de riesgo son todas las actividades que representen gestión fiscal, por ejemplo, aquellas de administración, gestión, ordenación, ejecución, manejo, adquisición, planeación, conservación, custodia, explotación, enajenación, consumo, adjudicación, gasto, inversión y disposición de los bienes o recursos públicos o intereses de naturaleza pública. Para la identificación y priorización de los puntos de riesgo, la entidad deberá tener en cuenta aquellas actividades en las cuales se han presentado advertencias, alertas, hallazgos fiscales y/o fallos con responsabilidad fiscal, así como, aquellas actividades que la organización identifique que pueden generar riesgos fiscales.

Recurso público: Para efectos del capítulo de riesgos fiscales, entiéndase como recurso público, los dineros comprometidos y ejecutados en ejercicio de la función pública. Ejemplos: Los recursos de inversión y recursos de funcionamiento de cada entidad; los recursos generados por actividades comerciales, industriales y de prestación de servicios, por parte de entidades estatales; los recursos parafiscales; los recursos que resultan del ejercicio de funciones públicas por particulares.

Reducción del riesgo: aplicación de controles para reducir las probabilidades de ocurrencia de un evento y/o su ocurrencia.

Riesgo: efecto de la incertidumbre sobre los objetivos[1] institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

[1] Fuente ISO 31000 Gestión del Riesgo - Directrices

Nota 1 a la entrada: Un efecto es una desviación respecto a lo previsto. Puede ser positivo, negativo o ambos, y puede abordar, crear o resultar en oportunidades y amenazas.

Nota 2 a la entrada: Los objetivos pueden tener diferentes aspectos y categorías, y se pueden aplicar a diferentes niveles.

Nota 3 a la entrada: Con frecuencia, el riesgo se expresa en términos de fuentes de riesgo, eventos potenciales, sus consecuencias y sus probabilidades.

Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

Nota: los eventos potenciales hacen referencia a la posibilidad de incurrir en pérdidas por deficiencias, fallas o inadecuaciones, en el recurso humano, los procesos, la tecnología, la infraestructura o por la ocurrencia de acontecimientos externos.[2]

Riesgo de gestión: posibilidad de que suceda algún evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

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 de seguridad de la información: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar un 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 fiscal: Es el efecto dañoso sobre los recursos públicos y/o los bienes y/o intereses patrimoniales de naturaleza pública, a causa de un evento potencial

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.

Sistema de administración de riesgo: conjunto de elementos del direccionamiento estratégico de una entidad concerniente a la Administración del Riesgo.

Tratamiento del riesgo: proceso para modificar o mitigar el riesgo.

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**.**

[2] Guía para la administración del riesgo y diseño de controles en entidades públicas. Diciembre de 2020. Versión 5.

Valoración del riesgo: proceso de comparación de los resultados del análisis de riesgos con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o intolerables, determinando cuales riesgos necesitan tratamiento y su prioridad para intervención.

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

6. CONDICIONES GENERALES

TRANSMILENIO S.A., ha desarrollado un compromiso con la Gestión del Riesgo, para ello ha definido un esquema de administración del riesgo, en el cual cada uno de los tipos de gestión del riesgo, se implementará y gestionará atendiendo el marco de las **Tres Líneas de Defensa** de la siguiente manera:

Tabla 1. Tipos de gestión del riesgo por líneas de defensa

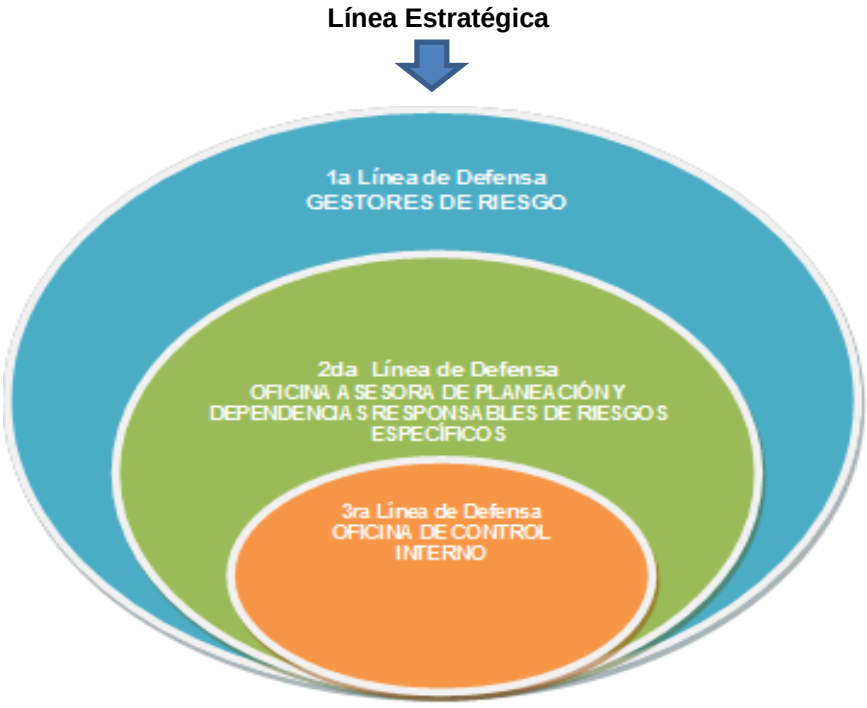
TIPOS DE GESTION DEL RIESGO	1RA LINEA DE DEFENSA	2da LINEA DE DEFENSA	3ra LINEA DE DEFENSA
Riesgos Institucionales	Líderes de Proceso	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Gestión	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Corrupción	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Seguridad de la Información	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Dirección de TIC	Oficina de Control Interno
Riesgos Técnicos	Funcionarios Contratistas Proveedores Concesionarios	Procesos Misionales	Oficina de Control Interno
Riesgos de Contratación	Proveedores y Contratistas	Dirección Corporativa Contratación Subgerencia Jurídica	Oficina de Control Interno

TIPOS DE GESTION DEL RIESGO	1RA LINEA DE DEFENSA	2da LINEA DE DEFENSA	3ra LINEA DE DEFENSA
Riesgos Laborales/ Seguridad salud y en el trabajo	Funcionarios de TRANSMILENIO S.A.	Dirección Corporativa Talento Humano	Oficina de Control Interno
Riesgos de lavado de activos y lucha contra el terrorismo	Funcionarios de TRANSMILENIO S.A.	Oficial de Cumplimiento	Oficina de Control Interno
Riesgos de Interrupción	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Oficina Asesora de Planeación – OAP	Oficina de Control Interno

Fuente: TRANSMILENIO S.A.

6.1 Responsabilidades en la Administración del Riesgo

El proceso de Gestión de riesgos se encuentra soportado en la Línea Estratégica y las Tres Líneas de Defensa como se muestra en la siguiente figura:



Gestión del Riesgo según las tres Líneas de Defensa

Línea Estratégica:

Define el marco general para la gestión del riesgo y supervisa su cumplimiento, está a cargo de los siguientes responsables

- **Junta Directiva**

La Junta Directiva cuenta con el apoyo del Comité de Coordinación de Control Interno en el cual se tomarán las decisiones pertinentes frente a los riesgos críticos de la entidad cuando sea el caso. Anualmente se deberá presentar a la Junta Directiva, el estado de la Gestión de Riesgo de TRANSMILENIO S.A.

- **Alta Dirección**

El Representante Legal de la Entidad es el principal responsable de la gestión del riesgo a través de un compromiso que se materializa en el establecimiento de los lineamientos en materia de Riesgos.

- **El Representante de la Alta Dirección**

El Representante de la Alta Dirección para el Sistema de Administración de Riesgos en TRANSMILENIO S.A., quien será el líder de riesgos, está en cabeza del Jefe de la Oficina Asesora de Planeación, quien es el responsable de formular, orientar y sugerir a las instancias que corresponda las mejoras o actualización de la presente política y de apoyar el adecuado cumplimiento de la misma al interior de la entidad.

- **Comité Institucional de Gestión y Desempeño**

En este Comité se analiza la gestión del riesgo y se aplican las mejoras que se consideren para una adecuada gestión y mitigación de los eventos que afecten el cumplimiento de los objetivos

- **Comité Institucional de Coordinación de Control Interno**

En este Comité debe realizarse el análisis de eventos y riesgos críticos cuando sea el caso.

La Alta Dirección, a través de sus Comités debe monitorear y revisar el cumplimiento de los objetivos institucionales para una adecuada gestión de riesgos.

Primera Línea de Defensa:

Tiene como objetivo el desarrollo e implementación de los procesos de gestión de riesgo y control a través de las etapas de identificación, análisis, valoración, monitoreo y acciones de mejora, basados en las directrices técnicas y metodológicas emitidas por la Oficina Asesora de Planeación y dependencias responsables de riesgos específicos como segunda línea de defensa, de quien se recibe el acompañamiento para su implementación.

En TRANSMILENIO S.A. está conformada por los siguientes responsables:

- **Gestor de Riesgo Líder (Dueño del proceso)**

Es el responsable de la gestión del riesgo desde cada uno de los procesos que lidera, es decir, del desarrollo de las actividades de identificación, análisis, valoración y definición del plan de tratamiento, así como del seguimiento y verificación a través de ejercicio del autocontrol.

Dentro de sus principales funciones se encuentran:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso
- Identificar los riesgos de sus procesos y determinar su probabilidad de ocurrencia y el impacto en caso de llegar a materializarse.
- Identificar los controles con los que cuentan los procesos y evaluarlos de acuerdo con la metodología para la gestión de riesgos definida y aprobada.
- Analizar los riesgos identificados con el fin de establecer el riesgo inherente y el riesgo residual de cada proceso a su cargo.
- Informar al Representante de la Alta Dirección para el Sistema de Administración de Riesgos acerca de los cambios ocurridos en su proceso, de nuevos procedimientos para que sean tenidos en cuenta dentro del Sistema y que podrían afectar la matriz de riesgos.
- Revisar y reportar a la Oficina Asesora de Planeación, los eventos de riesgos que se han materializado en la entidad, desde cada una de las tipologías, así como las causas que dieron origen a esos eventos de riesgos materializados, como aquellas que están ocasionando que no se logre el cumplimiento de los objetivos y metas, a través del análisis de indicadores asociados a dichos objetivos.

- Establecer e implementar el tratamiento de los riesgos evaluados, determinando los planes de acción y controles necesarios para administrarlos y garantizar que se encuentren dentro de los niveles de aceptación establecidos.
- Actualizar el Mapa de Riesgos de los procesos, cuando lo considere pertinente, teniendo en cuenta lo establecido en este manual.
- Realizar reuniones internas con el fin de tomar decisiones relacionadas con el tratamiento de los riesgos de su proceso, compartiendo los análisis y decisiones tomadas en los comités de Alto nivel, relacionados con la gestión de riesgos.

- **Equipos de trabajo de los procesos**

Son las personas que pertenecen al proceso objeto de análisis y que por su conocimiento y experiencia están en la capacidad de suministrar la información necesaria asociada a cada riesgo, para llevar a cabo las etapas de identificación, análisis, valoración y planes de tratamiento.

- **Funcionarios y Contratistas**

Todos los servidores públicos y contratistas de TRANSMILENIO S.A., son responsables de acatar y dar cumplimiento a la presente política para la administración y gestión de riesgos de la entidad mediante el cumplimiento de las siguientes funciones:

- Reportar oportunamente los eventos de riesgo de los cuales tengan conocimiento de acuerdo con los lineamientos y procedimientos establecidos para tal fin.
- Asistir a todas las capacitaciones o sensibilizaciones programadas sobre el Sistema de Administración de Riesgos.
- Cumplir con las políticas de riesgos establecidas en el presente documento.

Segunda Línea de Defensa:

Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los Riesgos desde cada una de las tipologías, que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos.

Está conformada por la Oficina Asesora de Planeación y las dependencias que tienen bajo su responsabilidad la implementación de riesgos específicos presentados en la tabla 1 de este documento.

Por otra parte, son las encargadas de definir el marco conceptual, técnico y metodológico, sobre el cual la primera línea de defensa debe realizar la implementación.

Dentro de sus funciones se encuentra:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar la actualización de las matrices de riesgos.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar.
- Definir los instrumentos, metodologías y procedimientos tendientes a que TRANSMILENIO S.A., administre efectivamente sus riesgos.
- Desarrollar e implementar el sistema de reportes sobre la administración de riesgos de TRANSMILENIO S.A.
- Realizar el seguimiento a los controles propuestos y planes de tratamientos relacionados con la gestión de riesgos y proponer las actualizaciones y modificaciones correspondientes.
- Coordinar los programas de sensibilización o socialización relacionados con el Sistema de Administración de Riesgos.
- Recopilar la información de cada una de las matrices de riesgo de los procesos y consolidarla para obtener el mapa de riesgos por procesos y el mapa de riesgos institucional así como realizar la publicación en la Intranet.
- Presentar informes a la Gerencia General y equipo directivo de acuerdo con las solicitudes de la misma.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado, así como pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos de tal manera, que se encuentren documentadas y actualizadas en los procedimientos.

Tercera Línea de Defensa:

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos de la entidad desde cada una de las tipologías, validando que la línea estratégica, la primera

y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro de los objetivos institucionales y del proceso.

Está conformada por la Oficina de Control Interno la cual debe llevar a cabo las siguientes actividades:

- Revisar los cambios en el "Direccionamiento estratégico" o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos desde todas las tipologías y que afectan el cumplimiento de los objetivos de los procesos.
- Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la primera línea de defensa y realizar las recomendaciones así como el seguimiento para el fortalecimiento de los mismos.
- Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado, de igual manera pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos verificar que se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.
- Hacer seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción. En especial deberá adelantar las siguientes actividades:

    - Verificar la publicación del Mapa de Riesgos de Corrupción en la página web de la entidad.
    - Seguimiento a la gestión del riesgo.
    - Revisión de los riesgos y su evolución.

- Verificar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma adecuada.

- Realizar la evaluación independiente al cumplimiento de las políticas, procedimientos y metodología de la gestión de riesgos, así como el aseguramiento de la efectividad de los controles, que estos estén alineados con el riesgo y estén funcionando en forma oportuna y efectiva.

  Entre las acciones que debe adelantar se encuentran:

  - Determinar la efectividad de los controles.
  - Recomendar ajustes o mejoras a la valoración de los riesgos como resultado de las auditorías.
  - Recomendar ajustes o mejoras a los controles como resultado de las auditorías.
  - Analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de corrupción.
  - Determinar si se adelantaron acciones de monitoreo.
  - Revisar las acciones del monitoreo.
  - Recopilar la evidencia de la ejecución de los controles.

De igual manera la Oficina de Control Interno, “en concordancia con la Guía de auditoria basada en riesgos para las entidades públicas del DAFP y las normas aplicables para el ejercicio de auditoría Interna” utilizará los instrumentos aprobados y adoptados por la Entidad (Código de Ética y carta de representación).

6.2 Clasificación del Riesgo

- ✓ **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la entidad y por tanto generan un impacto en la misma. De igual manera incluye la posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección, la ejecución y administración de procesos
- ✓ **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad como la prestación del servicio a la ciudadanía, daños a la flota, a la infraestructura y activos fijos en general de la entidad.

- ✓ **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- ✓ **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos o fallas tecnológicas que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- ✓ **Riesgos de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales, así como las relaciones laborales entre otros.
- ✓ **Riesgos ambientales:** Todos los relacionados con el impacto ambiental en que TRANSMILENIO S.A. puede incurrir en el desarrollo de sus actividades
- ✓ **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
- ✓ **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Incluye el fraude interno y externo
- ✓ **Riesgos de Seguridad de la Información:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar un pérdida o daño en un activo de información TRANSMILENIO S.A.
- ✓ **Riesgos de lavado de activos y financiación del terrorismo:** Son todas las pérdidas que se materializan cuando una persona quiere dar apariencia de legalidad a las actividades ilícitas o transacciones y fondos vinculados al lavado de activos y financiación del terrorismo
- ✓ **Riesgos de interrupción del negocio:** Son los incidentes bien sea esperado o no, que causa una alteración negativa y no planeada de la oferta esperada de los productos y servicios de acuerdo con los objetivos de la organización.
- ✓ **Riesgo Fiscal:** Es el efecto dañoso sobre los recursos públicos o los bienes o intereses patrimoniales de naturaleza pública, a causa de un evento potencial.

7. POLITICA PARA LA GESTIÓN DE LOS RIESGOS EN TRANSMILENIO S.A.

7.1 Objetivo

Generar confianza en los grupos de valor y de interés de TRANSMILENIO S.A. administrando los Riesgos de Gestión, de Corrupción, de Seguridad de la Información, de Interrupción y de Riesgos de Lavado de Activos y Financiación del Terrorismo que impidan el logro de los objetivos institucionales

7.1.1 Objetivos específicos

- Integrar la gestión del riesgo en todos los procesos de TRANSMILENIO S.A.
- Fortalecer la cultura y práctica continua de la administración del riesgo, haciendo participes a los funcionarios, proveedores, contratistas, clientes, órganos de control y en general a aquellas entidades y personas que tengan relación con TRANSMILENIO S.A.
- Establecer e implantar la metodología para la ejecución del proceso de gestión de riesgo, (la identificación, medición, control y monitoreo de los riesgos institucionales en el marco del contexto de TRANSMILENIO S.A. y procesos de información, comunicación y divulgación)
- Establecer los roles y responsabilidades de quienes participan en la administración de los riesgos institucionales.
- Establecer la alineación de la administración del riesgo con los objetivos estratégicos de la entidad.
- Gestionar los riesgos al nivel de aceptación definido

7.2 Alcance

Esta política aplica para la gestión de los riesgos de los procesos definidos en el mapa de procesos institucional y debe ser divulgada a todos los servidores públicos y contratistas de TRANSMILENIO S.A., para lo cual se mantendrá activa su publicación en la intranet, se socializará por parte de la Oficina Asesora de Planeación en los procesos de sensibilización a los enlaces de las dependencias, a los equipos de trabajo que se requieran y con campañas de comunicación a través de los medios y herramientas con los que cuenta la Entidad.

La actualización, modificación y mantenimiento de esta política será responsabilidad de la Alta Dirección a través del Jefe de la Oficina Asesora de Planeación – OAP como su representante.

7.3 Principios

La gestión de riesgos en TRANSMILENIO S.A., debe:

- Crear valor y salvaguardar a la entidad de la materialización de los riesgos.
- Ser parte integral de todos los procesos de TRANSMILENIO S.A., y de la toma de decisiones.
- Ser una actividad sistemática, estructurada y oportuna que tenga en cuenta la incertidumbre y esté basada en la mejor información disponible
- Estar alineada con el contexto de TRANSMILENIO S.A., de tal manera que tenga en cuenta los factores internos y externos facilitando un proceso transparente e incluyente para lograr la mejora continua de la operación y gestión de TRANSMILENIO S.A.
- Tomar como marco conceptual y metodológico para la Gestión de Riesgos, la normatividad vigente en la materia, así como las Guías y lineamientos emitidos por el Departamento Administrativo de la Función Pública (DAFP) que se encuentran vigentes y la Norma Técnica Colombiana NTC- ISO 31000.
- Implementar el proceso de Gestión de riesgos, soportado en las TRES LINEAS DE DEFENSA.

7.4 Declaración de la política

La Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A., optimiza su gestión empresarial, con el fin de generar confianza a sus grupos de valor y de interés, frente a los estados de vulnerabilidad institucional que potencialmente impidan el logro de sus objetivos institucionales, a través de la incorporación de una cultura de gestión de riesgo y de la implementación de un sistema de administración del riesgo, que permita asegurar razonablemente que los potenciales eventos de riesgo se encuentren debidamente tratados por cada uno de los procesos, realizando un seguimiento a través de la autoevaluación y autocontrol, ejercido por cada uno de los responsables de los procesos y los mecanismos de verificación fijados por la Entidad.

Por lo anterior, todos los servidores públicos y contratistas estarán comprometidos con el cumplimiento de las **Políticas de Gestión de Riesgos**, definidas en el presente documento, así como con el fortalecimiento de la cultura de gestión de riesgos y mejora continua del sistema.

- **Políticas relativas a la Administración del Riesgo:**

- La administración del riesgo está bajo la responsabilidad de la Gerencia General de TRANSMILENIO S.A., quien ha delegado la función de su Administración a la Oficina Asesora de Planeación.
- La Oficina Asesora de Planeación, será la responsable de la definición de la metodología técnica (Políticas, Procesos, metodologías, instrumentos).
- Siempre que se presente una incorporación, ajuste, modificación a los procesos de TRANSMILENIO S.A., así como la incorporación de nuevas políticas operativas o se presenten cambios en el contexto externo de la organización, se realizará el análisis para la identificación de nuevos riesgos o su ajuste.
- En caso de cambios al mapa de procesos de la entidad, que conlleve a la creación de un nuevo proceso, se realizará la identificación de riesgos relacionados con este y se generará su nueva matriz de riesgo.
- Los riesgos de corrupción se desarrollarán bajo la guía del Departamento Administrativo de la Función Pública y la metodología establecida por el documento “Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano”. La matriz se realizará de forma independiente a la de gestión.
- Los riesgos contractuales, deben ser incorporados en la Matriz de Riesgo Contractual soporte en cada proceso licitatorio, de acuerdo con los lineamientos establecidos en el manual de contratación de la entidad y en la normatividad legal vigente en la materia.
- Los riesgos de seguridad de la información y tecnológicos, estarán bajo la responsabilidad de la Dirección de TIC, la cual deberá desarrollar en la entidad, la metodología de acuerdo con la normatividad vigente en la materia y la matriz se realizará de forma independiente a la de gestión.
- Los riesgos de seguridad y salud en el trabajo estarán bajo la responsabilidad de la Dirección Corporativa, la cual deberá desarrollar en la entidad, la metodología de acuerdo con la normatividad vigente en la materia.
- Los riesgos de Interrupción, los riesgos de lavado de activos y financiación del terrorismo tendrán metodologías y matrices independientes para su adecuada gestión y monitoreo.
- Los Gestores Líderes (Dueños de proceso) de cada uno de los procesos, serán los responsables directos de la identificación, medición y control de los riesgos, que impidan el logro de los objetivos de su proceso, con la coordinación de los gestores de riesgo designados, aplicando los criterios técnicos definidos por la Oficina Asesora de Planeación.

- Los Gestores de riesgo, son responsables de coordinar el monitoreo de los riesgos y controles correspondientes a su proceso, con el fin de procurar que sean identificados todos los riesgos que impidan el logro de sus objetivos y que éstos se encuentren debidamente tratados en cumplimiento de las políticas, procedimientos y metodología del sistema de gestión de riesgo.
- La Oficina Asesora de Planeación, como responsable técnico del sistema, tendrá un rol permanente de facilitador técnico, cuyo equipo orientará y asesorará sobre el cumplimiento de las políticas, procedimientos, metodologías que deben ser acatadas por todos los procesos bajo el liderazgo del **Gestor líder** (Directivo dueño de proceso) y del **Gestor de riesgo** (Enlaces de cada proceso, designados como Gestores de Riesgo por el Gestor Líder)
- El gestor líder designará al gestor de riesgo, que asumirá la suplencia en caso de su ausencia temporal.
- Cuando existan conflictos de interés en el desarrollo de la política y la metodología para la gestión del riesgo en la entidad se deberá aplicar lo contenido en el Protocolo para la identificación de conflicto de intereses en TRANSMILENIO S.A.

- **Políticas Relativas al Reporte de Eventos de Riesgo:**

- Los funcionarios de TRANSMILENIO S.A., están obligados a reportar, los eventos de riesgo de los cuales tengan conocimiento.
- El reporte de eventos de riesgo debe cumplir con el proceso definido para tal fin, haciendo uso del formato o herramienta definido por parte de la Oficina Asesora de Planeación.
- Los eventos de riesgo, una vez identificados, deben ser reportados por el Gestor de riesgo líder a la Oficina Asesora de Planeación, en el momento que se genere la situación detectada.
- La materialización de los riesgos de seguridad de la información deberá iniciar con el proceso de gestión de incidentes de seguridad, ya sea a través del reporte interno en la entidad, como el reporte a entidades externas competentes relacionadas con delitos informáticos y ciberseguridad de acuerdo con los lineamientos definidos por la Dirección de TIC.
- Todos los eventos de riesgo relacionados con incidentes de fraude, corrupción o soborno serán reportados por los canales definidos por la entidad en el procedimiento de Atención de Peticiones Quejas, Reclamos y Sugerencias.

7.5 Metodologías a aplicar para la administración del Riesgo

TRANSMILENIO S.A. para los riesgos de gestión, corrupción, seguridad de la información, riesgos de lavado de activos y financiación del terrorismo– SARLAFT y de Interrupción aplicará las metodologías establecidas en los anexos de este manual para administrar los riesgos, donde se incluyen entro otros aspectos los relacionados con:

I. Niveles para calificar la probabilidad y el impacto.
II. Estrategias para combatir o tratar el riesgo
III. Monitoreo y Seguimiento al riesgo residual.

Vale la pena aclarar que estas metodologías estas soportadas en los lineamientos dados por el DAFP, en sus diferentes guías, así como la normatividad vigente en la materia.

7.6 Nivel de aceptación del riesgo

- Apetito del Riesgo: La Alta Dirección, define como nivel de aceptación de riesgo residual, la zona denominada con nivel BAJO lo que significa que asume los riesgos que se encuentren en este nivel

- Tolerancia del Riesgo: La Alta Dirección define como nivel de tolerancia del riesgo residual la zona denominada con nivel MODERADO dado la fortaleza de los monitoreos.

- Capacidad del Riesgo: La Alta Dirección define como capacidad del riesgo residual la zona de riesgo ALTA y EXTREMA para lo cual se deberán elaborar planes de tratamiento que permitan la mitigación de los efectos que produzcan dichos riesgos y el monitoreo de los mismos en los períodos establecidos.

Para los riesgos de gestión y de interrupción se tiene contemplado la aceptación de los riesgos con un nivel de riesgo residual MODERADO con un monitoreo permanente de los mismos en los períodos determinados para tal fin

Para los riesgos de corrupción, así como para los riesgos de lavado de activos y financiación del terrorismo, no se admite aceptación del riesgo y siempre se deberán elaborar planes de tratamiento de acuerdo con los lineamientos establecidos por el DAFP y la normatividad vigente en la materia.

Para los riesgos de seguridad de la información, se tiene contemplado la aceptación de los riesgos con una calificación BAJO. Para el nivel MODERADO se aceptan, sin embargo, se deben realizar acciones de reducción del riesgo.

7.7 Niveles para calificar el impacto

Para la calificación del impacto se tendrá en cuenta lo establecido en los numerales de Análisis de Riesgos incorporados en cada uno de los Anexos dispuestos para los tipos de gestión del riesgo que se explican en este documento.

7.8 Tratamiento de Riesgos

Para el tratamiento de los riesgos se deberá tener en cuenta lo establecido en los numerales Tratamiento del Riesgo de cada uno de los anexos dispuestos para los tipos de gestión del riesgo de la Entidad

7.9. Estrategias para dar cumplimiento a la política

Para desarrollar y dar cumplimiento a la presente política para la gestión de riesgos, se han establecido las siguientes estrategias:

- Designar al Jefe de la Oficina Asesora de Planeación, como representante de la Alta Dirección para el Sistema de Administración de Riesgos.
- Designar como Gestor de Riesgo, al líder de cada uno de los procesos
- Actualizar la política y procedimientos relacionados con la gestión de riesgos.
- Documentar las actividades para el reporte de riesgos.
- Trabajar de manera articulada los riesgos que se generen en la implementación de cada una de las políticas del modelo de gestión en el marco de MIPG
- Actualizar los mapas de riesgos existentes de los procesos definidos en el mapa de procesos institucional cuando se considere pertinente.
- Documentar los riesgos que se han identificado en la operación normal de la Entidad
- Identificar riesgos materializados al interior de la institución.

- Presentar los informes sobre la gestión de riesgos al Comité Institucional de Coordinación de Control Interno cuando se requiera y una vez al año a la Junta Directiva por parte del Representante de la Alta Dirección para el Sistema de Administración de Riesgos.
- Diseñar planes de sensibilización y socialización permanente para los servidores públicos de todos los niveles con el objetivo de generar una cultura de prevención de riesgos al interior de la Entidad.

7.10 Cultura de gestión de riesgos

La Alta Dirección y los líderes de los diferentes procesos son los responsables de la integración y divulgación de las buenas prácticas institucionales para la administración y gestión de los riesgos de TRANSMILENIO S.A.

Los programas de formación o sensibilización en temas de riesgos son obligatorios para todos los servidores públicos y contratistas de la entidad.

Todos los servidores públicos directos o indirectos de TRANSMILENIO S.A., que por acción u omisión violen, faciliten o transgredan el contenido de esta política para la administración y gestión de riesgos, así como los documentos que la desarrollan, estarán sujetos a las medidas disciplinarias pertinentes, de conformidad con las normas legales vigentes.

7.11 Seguimiento al nivel del riesgo residual

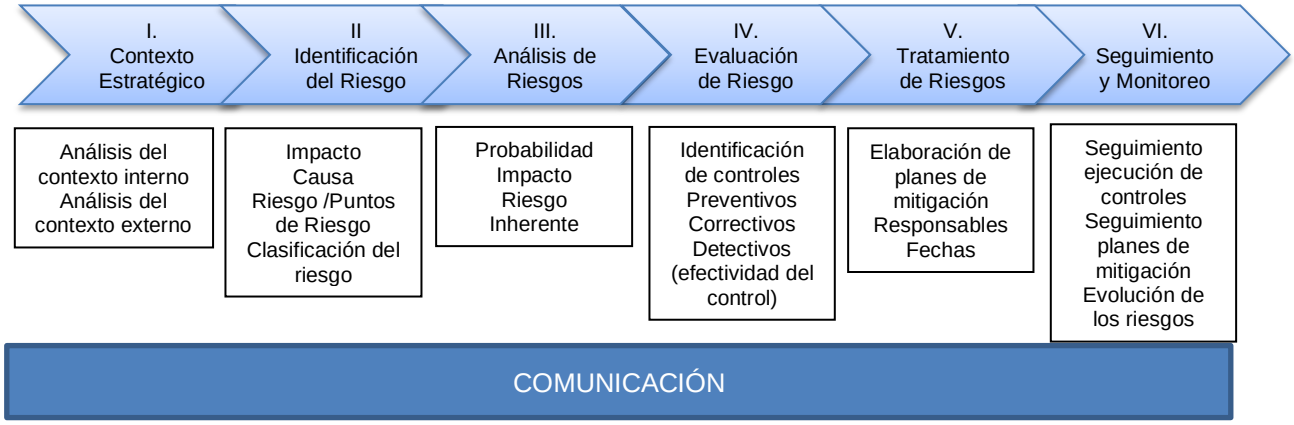
La Alta Dirección de TRANSMILENIO S.A., ha asignado roles y responsabilidades para el monitoreo y revisión de la gestión de riesgo, dando alcance al marco de las **tres líneas de defensa**, definidas como principio del sistema y que se establecen en el numeral 6.1 de este manual.

8. METODOLOGÍA PARA LA GESTIÓN DEL RIESGO

Las metodologías descritas en los anexos de este documento contemplan las etapas requeridas para una adecuada administración del riesgo de acuerdo con la naturaleza de los mismos y de acuerdo con lo establecido en la normatividad legal vigente en la materia

Dichas etapas comprenden los siguientes aspectos: contexto estratégico, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de los riesgos y monitoreo.

Etapas a seguir en la metodología de riesgos



8.1. Establecimiento del contexto estratégico

El contexto estratégico, es la base sobre la cual se establecen las causas de los riesgos a identificar, estos se clasifican en Contexto Interno, Contexto Externo y Contexto del proceso.

I. Contexto Interno

Se determinan las características o aspectos esenciales del ambiente interno en el cual la organización busca alcanzar sus objetivos

El establecimiento del contexto interno incluye:

- La plataforma estratégica, el gobierno corporativo, la estructura organizacional, la determinación de responsabilidades, los niveles de autoridad y los flujos de comunicación.
- Los objetivos, las metas, las estrategias y las políticas dispuestas por TRANSMILENIO S.A. como parte de la cadena de valor de la entidad, donde se evidencian los procesos.
- La forma y el alcance de las relaciones contractuales desarrolladas en TRANSMILENIO S.A.
- Las normas, directrices y modelos adoptados por TRANSMILENIO S.A.
- Capacidades expresadas en términos de recursos y el conocimiento (por ejemplo, capital, tiempo, personas, tecnologías, entre otros).
- Sistemas de gestión, control y administración como buen gobierno corporativo, control interno, código de integridad y las políticas institucionales entre otros.

Entre los factores claves del contexto interno se consideran:

a. Financieros: Presupuesto de funcionamiento, recursos de inversión, capacidad financiera.

b. Talento Humano: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional

c. Procesos: capacidad instalada, infraestructura, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

d. Tecnología: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.

e. Estratégicos: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

f. Comunicación Interna: canales utilizados y su efectividad, flujo de la información necesaria para el desarrollo de las operaciones

II. Contexto Externo

Se determinan las características o aspectos esenciales del entorno en el cual la organización busca alcanzar sus objetivos.

La determinación del contexto externo incluye:

- Las obligatoriedades o compromisos normativos institucionales con las regulaciones, aplicaciones y los planes ya determinados.
- Los factores clave y que tengan impacto en el logro de los objetivos, metas y planes de TRANSMILENIO S.A., o del proceso.
- Las relaciones con las partes interesadas, proveedores y usuarios.
- Las consecuencias sociales y culturales, legales, regulatorias, financieras, tecnológicas, económicas, naturales, entre otras, de la gestión de las partes interesadas.

Entre los factores claves del contexto externo se determinan los principales aspectos del entorno en el cual opera la entidad, entre los cuales

a. Económicos y financieros: Disponibilidad de capital, liquidez, mercados financieros, desempleo, competencia.

b. Políticos: Cambios de gobierno, legislación, políticas públicas, regulación.

c. Sociales y culturales: Demografía, responsabilidad social, orden público.

d. Tecnológicos: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.

e. Ambientales: Cambios normativos, lineamientos ambientales que impactan la operación.

f. Legales y Reglamentarios: Normatividad que regula a la Entidad

g. Articulación interinstitucional: Relación con otras entidades del sector, del gobierno, territoriales, ONG, entre otros.

III. Contexto de procesos

Se determinan los aspectos claves del proceso y sus interrelaciones. El insumo principal es la caracterización de cada uno de los procesos:

- Objetivo del proceso
- Alcance
- Procedimientos asociados
- Interrelación con otros procesos
- Responsables del proceso
- Activos de seguridad de la información del proceso
- Riesgos del proceso
- El ciclo PHVA el cual presenta la ejecución del proceso

8.2. Identificación del riesgo

La identificación del riesgo se lleva a cabo determinando las causas y el impacto con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos institucionales.

A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

Para la identificación de riesgos se debe tomar como base el plan estratégico de TRANSMILENIO S.A., se debe recopilar toda la información existente del proceso a evaluar teniendo en cuenta diferentes fuentes de información como son:

- Las caracterizaciones y procedimientos de cada proceso.

- Los requerimientos realizados a la mesa de ayuda.
- Los informes de la Oficina de Control Interno y otros órganos de control y vigilancia.
- Las Peticiones, Quejas, Reclamos y Sugerencias.
- Participación ciudadana.
- Resultados de encuestas de satisfacción.
- Las actividades diarias y propias del quehacer institucional.
- El resultado del monitoreo de seguridad de la información realizado a la infraestructura tecnológica
- Los incidentes de seguridad de la información gestionados por la entidad
- Los resultados de la medición del plan de cultura y sensibilización de la entidad
- Factores de riesgo que tenga que ver con procesos, talento humano, tecnología, infraestructura, eventos externos entre otros.

Con el análisis de esta información y la ayuda del líder del proceso se identifican todos los riesgos potenciales que pertenecen al proceso.

La identificación debe estar enfocada a aquellos riesgos potenciales que puedan incidir en el adecuado cumplimiento de los objetivos de los procesos, en la medida que se implementen nuevos procesos o procedimientos se da paso a la identificación de nuevos riesgos.

La etapa de identificación del riesgo debe ser realizada por los líderes de cada proceso de manera permanente y producto de lo desarrollado en la etapa del contexto estratégico.

La identificación 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

Cada una de las metodologías contiene el detalle de la identificación del riesgo de acuerdo con su naturaleza.

8.3. Análisis del riesgo

Una vez identificados los riesgos siguiendo la estructura definida en el ítem anterior, deben ser calificados en dos aspectos importantes: El primero está relacionado con la probabilidad de materialización o de

ocurrencia del riesgo y el segundo en el impacto o la consecuencia que tendría para TRANSMILENIO S.A, con el fin de estimar la zona de riesgo inicial es decir lo que se denomina Riesgo Inherente.

Este análisis deberá llevar a escalas de valoración cualitativa o cuantitativa tanto para la probabilidad como para el impacto, lo que permitirá posteriormente ubicar el riesgo inherente dentro del mapa colorimétrico y conocer la zona de riesgos inicial.

Cada una de las metodologías contiene el detalle del análisis del riesgo de acuerdo con su naturaleza.

8.4. Evaluación del riesgo

- **Nivel de riesgo inherente**

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).

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. En cada una de las metodologías se define las zonas en la matriz de calor.

- **Valoración de Controles**

Para llevar a cabo la evaluación del riesgo, después de conocer el nivel del riesgo inherente, se deben identificar los controles existentes para mitigarlo para lo cual se debe tener en cuenta lo siguiente:

- 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 si 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.
- Cada control debe ser evaluado de acuerdo con los criterios de calificación definidos, para conocer el nivel de riesgo residual y así establecer el tratamiento que se dará a cada riesgo.
- Los controles establecidos deben ser coherentes con lo definido en los planes a los que aporte la Entidad, la normatividad interna y externa aplicable, los procedimientos e instrucciones de trabajo y las políticas de operación o lineamientos determinados para la gestión.

- Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

- **Descripción del control**

Para una adecuada redacción del control se recomienda que se siga la siguiente estructura que facilitará entender su tipología y otros atributos para su valoración.

- **Responsable de ejecutar el control:** identificar el(los) cargos específicos de los servidores responsables de llevar a cabo la actividad de control. En caso de que sean controles automáticos se identificará el sistema que realiza la actividad. Evitar asignar áreas de manera general o nombres de personas.

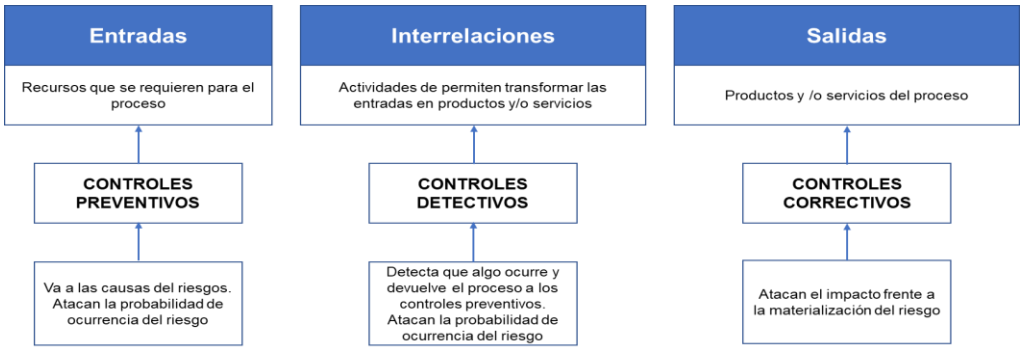
- **Acción:** se determina mediante verbos que indican la acción que deben realizar como parte del control. Debe indicar cuál es el propósito del control. El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo.

- **Complemento:** Corresponde a los detalles que permiten identificar claramente el objeto del control. Debe establecer el cómo se realiza la actividad de control. El control debe indicar el cómo se realiza, cual es la fuente de información que sirve para ejecutar el control, cual es la evidencia de la aplicación del control entre otros.

- **Tipos de control**

Existen tres tipos de controles como se resumen a continuación:

Activación de los Tipos de Controles en el ciclo de un proceso



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Diciembre de 2020. V.5

- **Evaluación del diseño del control**

Cada una de las metodologías contiene los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

- **Nivel del riesgo residual**

Es el resultado de aplicar la efectividad de los controles al riesgo inherente. Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de calor del riesgo residual (después de los controles).

Teniendo en cuenta que es a partir de los controles que se dará el desplazamiento en la matriz de calor, cada metodología presenta el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

8.5. Tratamiento del riesgo

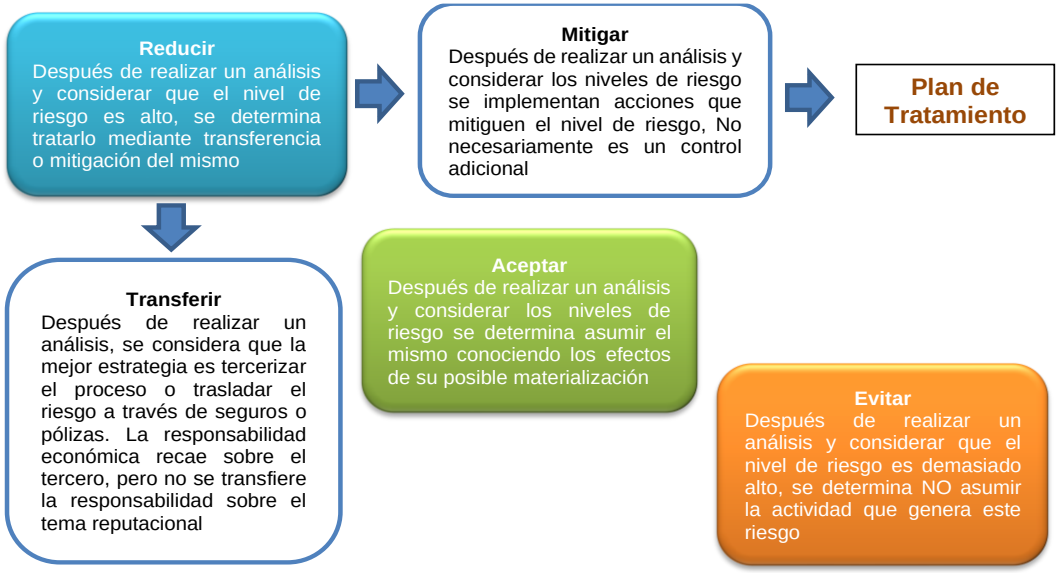
Es la decisión que toma la primera línea de defensa frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir, evitar o transferir.

Al momento de evaluar las opciones existentes en materia de estrategias para tratar el riesgo y partiendo de lo que establezca la política de administración del riesgo, los dueños de los procesos tendrán en cuenta la importancia del riesgo, lo cual incluye el efecto que puede tener sobre la entidad, la probabilidad e impacto de este y la relación costo-beneficio de las medidas de tratamiento.

En los casos en que una respuesta ante el riesgo derive en que el riesgo residual sigue superando los niveles aceptables para la Alta Dirección, se deberá volver a analizar y revisar dicha estrategia.

En la siguiente figura se observan las tres opciones mencionadas y su relación con la necesidad de definir planes de acción/tratamiento dentro del respectivo mapa de riesgos.

Estrategias para tratar el riesgo



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades pública. Diciembre de 2020, Versión 5.

De acuerdo con el nivel de riesgo residual obtenido, cada metodología define los criterios para seleccionar las opciones de manejo que se le debe dar a un riesgo de acuerdo con su naturaleza.

8.6. Monitoreo y seguimiento

Los líderes de los procesos, en conjunto con sus equipos de trabajo, deben monitorear y revisar periódicamente la gestión de riesgos y si es el caso realizar los ajustes de acuerdo con las dinámicas de la Entidad (primera línea de defensa).

En cada una de las metodologías de administración de riesgos se ha establecido como se llevará a cabo el monitoreo y seguimiento a los riesgos.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos.

9. COMUNICACIÓN

La comunicación y consulta con las partes involucradas tanto internas como externas en la gestión del riesgo se debe dar en todas las etapas del Sistema de Administración del Riesgo con la participación de los líderes de proceso y sus equipos de trabajo.

En cada una de las metodologías de administración de riesgos se ha establecido como se llevará a cabo la comunicación y divulgación de los riesgos

10. ANEXOS

Anexo 1. Metodología para la Administración de los Riesgos de Gestión.

Anexo 2. Metodología para la Administración de los Riesgos de Corrupción.

Anexo 3. Metodología para la Administración de los Riesgos de Seguridad de la Información.

Anexo 4. Metodología para la Administración de los Riesgo de Lavado de Activos y Financiación del Terrorismo.

Anexo 5. Metodología para la Administración de los Riesgos de Interrupción y continuidad del Negocio.