TABLA DE CONTENIDO

1. OBJETIVO 4
2. ALCANCE 4
3. DOCUMENTOS DE REFERENCIA 4
4. DEFINICIONES 5
5. ESTABLECIMIENTO DEL CONTEXTO DE RIESGO 9
5.1 Contexto Externo 9
5.2 Contexto Interno. 9
5.3 Contexto de procesos. 10
6. POLITICA PARA LA GESTION DE RIESGOS EN TRANSMILENIO S.A. 10
6.1 Objetivo 10
6.1.1 Objetivos específicos 10
6.2 Alcance 11
6.3 Principios 11
6.4 Nivel de aceptación del riesgo 13
6.5 Niveles para calificar la probabilidad y el impacto. 13
6.6 Tratamiento del riesgo 14
6.7 Seguimiento al nivel del riesgo residual 14
6.8 Declaración de la política 15
6.9 Responsabilidades 17
6.10 Estrategias para dar cumplimiento a la política 20
6.11 Cultura de gestión de riesgos 20
7. METODOLOGIA PARA LA GESTION DEL RIESGO 21
7.1 Contexto estratégico 21
7.1.1 Contexto externo 21
7.1.2 Contexto interno 22
7.2 Criterios para la evaluación de los riesgos 22
7.3 Evaluación del riesgo 22
7.3.1 Identificación del riesgo 23
7.3.1.1 Identificación de la causa raíz 24

COPIA NO CONTROLADA

7.3.2 Análisis de Riesgos 25
7.3.2.1 Cálculo de la probabilidad de los riesgos de gestión y de corrupción 26
7.3.2.2 Cálculo del impacto de los riesgos de gestión 27
7.3.2.3 Cálculo del impacto de los riesgos de corrupción 29
7.3.2.4 Análisis del impacto en riesgos de corrupción 30
7.3.2.5 Nivel de riesgo inherente 31
7.3.3 Valoración de los riesgos 32
7.3.3.1 Diseño de los controles 33
7.3.3.2 Valoración de los controles 35
7.3.3.3 Resultados de la evaluación del diseño del control 37
7.3.3.4 Resultados de la evaluación de la ejecución del control 37
7.3.3.5 Solidez del conjunto de controles para la adecuada mitigación del riesgo 38
7.3.3.6 Nivel de riesgo (riesgo residual) 38
7.3.4 Tratamiento del riesgo 39
7.3.4.1 Tratamiento del riesgo – rol de la primera línea de defensa 41
7.4 Monitoreo y revisión 42
7.4.1 Monitorear y revisar la gestión de riesgos 42
7.4.2 Asignación de roles y responsabilidades para monitoreo y revisión de la gestión de riesgos 43
7.4.2.1 Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control 44
7.4.2.2 Rol de las líneas de defensa en el monitoreo y revisión de los riesgos y actividades de control 45
7.4.3 Monitoreo riesgos de corrupción 48
7.4.4 Reporte Plan de Tratamiento de Riesgos 48
7.4.5 Reporte de la gestión del riesgo 49
7.4.6 Reporte de la gestión del riesgo de corrupción 49
7.5 Seguimiento riesgos de corrupción 49
7.5.1 Acciones a seguir en caso de materialización de riesgos de corrupción 50
8. COMUNICACIÓN Y CONSULTA 51
8.1 Plan de capacitación 51
8.2 Planes para la comunicación y consulta 51
9. INFORMACIÓN, COMUNICACIÓN Y REPORTE 52
10. TABLA DE FORMATOS 53
11. ANEXOS 53

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 DAFT 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

1. OBJETIVO

Brindar a los funcionarios de TRANSMILENIO S.A., las directrices y metodología que le permita gestionar el riesgo de gestión y de corrupción, definiendo los roles y responsabilidades de la gestión de riesgo, así como las metodología que permita la identificación de los riesgos, su análisis, valoración, la selección de tratamiento para los riesgos, así como el monitoreo, revisión, comunicación y consulta de dichos riesgos; estas etapas se encuentran comprendidas dentro del Sistema de Administración de Riesgos de TRANSMILENIO S.A.

2. ALCANCE

Este manual aplica para la administración de los riesgos de gestión y corrupción, de los procesos definidos en el mapa de procesos institucional, el cual incorpora la política que define las directrices para su gestión, así como la metodología que permitirá su implementación.

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

3. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia.
- Norma ISO 31000:2018. Gestión de Riesgos. Directrices. Estándar normativo internacional que proporciona las directrices genéricas sobre la gestión del riesgo.
- Manual Operativo Sistema de Gestión MIPG. Consejo para la Gestión y Desempeño Institucional Octubre de 2018.
- 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”.

- Manual de Funciones de TRANSMILENIO S.A.
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas Octubre de 2018.

4. DEFINICIONES[1]

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

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: magnitud y tipo de riesgo que una organización está dispuesta a buscar o retener.

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.

[1] Definiciones basadas en la Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, Octubre de 2018, versión 1.

Causa: todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un 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 modifica al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones).

Controles Preventivos: controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos.

Controles Detectivos: controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes.

Controles Correctivos: permiten el restablecimiento de una actividad, después de ser detectado un evento no deseable, posibilitando la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan, y permiten mejorar las deficiencias.

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: es el resultado de un evento expresado cualitativa o cuantitativamente, sea este una pérdida, perjuicio, desventaja o ganancia, frente a la consecución de los objetivos de la entidad o el proceso.

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

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).

COPIA NO CONTROLADA

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: elemento que contempla una capacidad potencial de producir impactos/daños materiales al producto o servicio.

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.

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.

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.

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

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.

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

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

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[2] institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

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.

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 inherente: es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto.

Riesgo residual: nivel de riesgo que permanece luego de tomar medidas de tratamiento de riesgo.

[2] Fuente ISO 31000:2018 Gestión del Riesgo - Directrices

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 al riesgo: son los niveles aceptables de desviación relativa a la consecución de objetivos. Pueden medirse y a menudo resulta mejor, con las mismas unidades que los objetivos correspondientes. Para el riesgo de corrupción la tolerancia es inaceptable.

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.

5. ESTABLECIMIENTO DEL CONTEXTO DE RIESGO

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

5.1 Contexto Externo

Se determinan los principales aspectos del entorno en el cual opera la entidad, entre los cuales se consideran:

1. ECONÓMICOS: Recurso financiero, liquidez, mercados financieros, desempleo, competencia.
2. POLÍTICOS: Cambios de gobierno, legislación, políticas públicas, regulación.
3. SOCIALES: Demografía, responsabilidad social, orden público.
4. TECNOLÓGICOS: Avances en tecnología, acceso a sistemas de información externos, gobierno en línea.
5. ARTICULACIÓN INTERINSTITUCIONAL: Relación con otras entidades del sector, del gobierno, territoriales, ONGs.

5.2 Contexto Interno.

Se determinan los aspectos claves del ambiente en la cual la entidad busca alcanzar sus objetivos, entre los cuales se consideran:

1. FINANCIEROS: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.
2. TALENTO HUMANO: Competencia del personal, disponibilidad del personal, seguridad y salud ocupacional.
3. TECNOLOGÍA: Integridad de datos, disponibilidad de datos y sistemas, desarrollo, producción, mantenimiento de sistemas de información.
4. ESTRATÉGICOS: Direccionamiento estratégico, planeación institucional, liderazgo, trabajo en equipo.

5.3 Contexto de procesos.

Se determinan los aspectos claves de la interacción entre procesos y sus procedimientos asociados, transversalidad u su ejecución, entre los cuales se consideran:

1. INTERACCIÓN CON OTROS PROCESOS Y PROCEDIMIENTOS ASOCIADOS:
2. TRANSVERSALIDAD
3. EJECUCIÓN

Ver anexo 1. DOFA Gestión de Riesgos TMSA 2019.

6. POLITICA PARA LA GESTION DE RIESGOS EN TRANSMILENIO S.A.

6.1 Objetivo

Generar confianza en los grupos de interés de TRANSMILENIO S.A. a través del proceso de Administración de los riesgos de gestión y corrupción, que impidan el logro de los objetivos institucionales

6.1.1 Objetivos específicos

- Integrar el proceso de gestión de 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 el marco, la arquitectura (las políticas, los procedimientos y la estructura organizacional aplicables) para el desarrollo, implementación y seguimiento de los riegos.
- Establecer e implantar la metodología para la ejecución del proceso de gestión de riesgo, (la identificación, medición, control y monitoreo de los riesgos operativos 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 operativos.
- Establecer la alineación de la administración del riesgo con los objetivos estratégicos de la entidad.
- Gestionar los riesgos al nivel de aceptación definido.

6.2 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 presentará por parte de la OAP en los procesos de inducción de nuevos funcionarios y se ejecutará anualmente el programa de sensibilización en Gestión de Riesgos, a la cual serán convocados todos los funcionarios de TRANSMILENIO S.A.

La actualización, modificación y mantenimiento de esta política será responsabilidad de la Oficina Asesora de Planeación – OAP, con la aprobación de la Alta Dirección.

6.3 Principios

La administración 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.

- TRANSMILENIO S.A., toma como marco conceptual y metodológico para la Gestión de Riesgos, la Guía para la administración del riesgo y el diseño de controles en entidades públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP) en octubre de 2018 y la Norma Técnica Colombiana ISO 31000 emitida por ICONTEC. Implementa el proceso de Gestión de riesgos, tomando como referente las TRES LINEAS DE DEFENSA



La primera línea de Defensa esta conformada por los Líderes de cada uno de los procesos de la entidad, quienes han sido denominados como GESTORES DE RIESGO y su equipo de trabajo.

Tiene como objetivo el desarrollo e implementación de los procesos de gestión de riesgo y control a través de su identificación, análisis, valoración, monitoreo y acciones de mejora, basados en las directrices técnicas y metodológica emitidas por la segunda línea de defensa la OAP, de quien recibe la facilitación para su implementación.

La segunda línea de defensa le corresponde a la Oficina Asesora de Planeacion - OAP, cuyo objetivo es asegurar que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen de acuerdo al objetivo para el cual fueron diseñados. La OAP, es el encargado de definir el marco conceptual, técnico y metodológico, como el marco, sobre el cual la primera línea de defensa debe realizar la implementación, bajo la facilitación ofrecida por la OAP.

COPIA NO CONTROLADA

La tercera línea de defensa, le corresponde a la Oficina de Control Interno – OCI, cuyo objetivo es el de proporcionar información sobre la efectividad del Sistema de Control Interno, a través de un enfoque basado en riesgo, incluida la operación de la primer y segunda línea de defensa. La OCI, representa para la entidad el órgano de evaluación independiente, el cual dando alcance al marco normativo y de orientación profesional brinda aseguramiento interno en relación con la efectividad del sistema de control interno y la gestión de riesgo, sin realizar actividades de co-administración o determinador de acciones de gestión de la primera y segunda línea de defensa, ya que esto generaría un conflicto en el nivel de independencia y objetividad que lo caracteriza. Ver numeral 7.4.2.

6.4 Nivel de aceptación del riesgo

Teniendo en cuenta que el nivel de aceptación del riesgo corresponde a la zona del mapa térmico, en la cual la Alta Dirección ha establecido, deben ser desplazados todos los riesgos residuales, es decir aquellos que han recibido el respectivo tratamiento de control.

La Alta Dirección, define como nivel de aceptación de riesgo residual, la zona denominada como MODERADA, tanto para los riesgos de gestión como para los riesgos de corrupción.

Es importante aclarar, en relación con los riesgos de corrupción, que el DAFP establece que los riesgos inherentes de corrupción son inaceptables, es decir estarán ubicados en la zona INACEPTABLE, del mapa térmico de corrupción, sin embargo es responsabilidad de TRANSMILENIO S.A., aplicar todos los tratamientos de control necesarios para su mitigación, los cuales por mayor esfuerzo realizado, se ubicarán en la zona moderada, atendiendo que el impacto siempre debe mantenerse en un estado de inaceptable. Ver numeral 7.3.2.5. Tabla de Nivel de Riesgo.

6.5 Niveles para calificar la probabilidad y el impacto.

TRANSMILENIO S.A., ha definido criterios para la calificación de la probabilidad, basados en la guía para la administración del riesgo y el diseño de controles de entidades públicas de octubre de 2018, versión 4.

Ver numeral 7.3.2.1 Tabla No.1 ; Escalas de valoración de la probabilidad para los riesgos de gestión y Tabla No. 2: Escalas de valoración para la valoración de los riesgos de corrupción.

TRANSMILENIO S.A., ha definido criterios para la calificación tanto del impacto, basados en la guía para la administración del riesgo y el diseño de controles de entidades públicas de octubre de 2018, versión 4.

Ver numeral 7.3.2.2 Tabla No.3; Escalas de valoración del impacto/consecuencia para los riesgos de gestión y 7.3.2.3 la Tabla No. 4 : Criterios para calificar el impacto de los riesgos de corrupción.

6.6 Tratamiento del riesgo

TRANSMILENIO S.A. ha definido como tratamiento de riesgo, que todos los riesgos deben ser MITIGADOS, definiendo acciones de control frente a las causas, así como a los impactos. Ver numeral 7.3.4. figura No. 10

6.7 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 LINEAS DE DEFENSA, definidas como principio del sistema. Ver numeral 6.3 Principios y numerales 7.4.1 y 7.4.2 Correspondiente a la Metodología.

Se realizarán actividades de monitoreo y revisión, de los riesgos de gestión, por parte de los responsables de cada una de las líneas de defensa, con una periodicidad ANUAL, y cada vez que se identifique algún nuevo riesgo, cambios en el análisis de un riesgo ya identificado o cambios en los controles para mitigar el riesgo, debe actualizarse la matriz de riesgos y debe ser remitida a la Oficina Asesora de Planeación.

El líder de proceso, junto con su equipo de trabajo, deben revisar periódicamente que los controles definidos estén documentados, que se apliquen y que sean efectivos. De igual manera, deben informar al líder de riesgos sobre dicha revisión. Ver numeral 7.4.1

Se realizarán actividades de monitoreo y seguimiento, de los riesgos de corrupción, por parte de los responsables de cada una de las líneas de defensa, con una periodicidad TRIMESTRAL

Monitoreo riesgos de corrupción. 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 Asesora de Planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se sugiere elaborar una matriz para el monitoreo periódico. Este monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y 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, se deben atender las actividades descritas en la primera y segunda línea de defensa de este documento[3].

Seguimiento de riesgos de corrupción

- **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
- ***Primer seguimiento:*** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- ***Segundo seguimiento:*** Con corte al 31 de Octubre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- ***Tercer seguimiento:*** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se podrá registrar en el formato modelo *"Anexo 6 Matriz Seguimiento Mapa de Riesgos de Corrupción",* que propone la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, y se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano. Ver numeral 7.4.3

6.8 Declaración de la política

La Empresa de Transporte del Tercer Milenio "TRANSMILENIO S.A., optimiza su gestión empresarial, con el fin de asegurar niveles de confianza de sus grupos de interés, frente a los estados de vulnerabilidad institucional que potencialmente impidan el logro de sus objetivos institucionales, a

[3] Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, Octubre de 2018

través de la incorporación de la cultura de gestión de riesgo que permita asegurar razonablemente que los potenciales eventos de riesgo que puedan generar incertidumbre en el logro de los objetivos, 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 GESTION 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 Proceso de Gestión de Riesgo, esta bajo la responsabilidad de la Gerencia de TRANSMILENIO S.A., quien ha delegado la función de su Administración a la OFICINA ASESORA DE PLANEACION – OAP
- La OAP, será la responsable de la definición de la arquitectura técnica del proceso (Políticas, Procesos, metodologías, instrumentos).
- Siempre que se presenten 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.
- Se realizará la identificación de riesgos relacionados con nuevos procesos, licitaciones o servicios, previo a su salida en vivo.
- Los Gestores de Riesgo de cada uno de los procesos, serán los responsables de la Identificación de los riesgos, que impidan el logro de sus objetivos, así como de su medición y control aplicando los criterios definidos por la OAP.
- Los Gestores de riesgo, son responsables del continuo monitoreo de los riesgos y controles correspondientes a su proceso, con el fin de asegurar 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 OAP, como responsable técnico de la arquitectura 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 LIDER y la gestión del GESTOR DE RIESGO.

- Los funcionarios designados como Gestores Líder, deben asegurar al interior de su proceso, que sean reportados TODOS los eventos de riesgo a la OAP.
- El gestor líder designará al gestor de riesgo, que asumirá la suplencia en caso de su ausencia temporal.

Políticas Relativas al Reporte de Eventos de Riesgo de Gestión:

- Los funcionarios de TRANSMILENIO S.A., están obligados a reportar TODOS, 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 de la herramienta definida, guías, instructivos y entrenamiento por parte de la OAP.
- Los eventos de riesgo deben ser reportados por el Gestor de riesgo líder a la OAP, el día 15 de cada mes o siguiente día hábil. Los eventos de riesgo identificados de manera extemporánea al reporte realizado en el periodo deben reportarse en formado de REPORTE EXTEMPORANEO.
- Todos los eventos de riesgo relacionado con incidentes de Fraude o Corrupción o soborno, serán reportados por el canal exclusivo definido para tal fin una vez suplido el proceso de capacitación a los funcionarios de TRANSMILENIO S.A.
- La política entrará en vigencia a partir de su aprobación y adopción. Contará con un periodo de transición de 5 meses, en los cuales se definirán los procedimientos e instrumentos para asegurar su cumplimiento por parte de los responsables.
- El inicio formal del proceso de reporte de eventos de riesgo de gestión (Materialización de riesgos) de TRANSMILENIO S.A., iniciará a partir del 1ro de Enero de 2020.

6.9 Responsabilidades

- **Junta Directiva**

Hacer seguimiento al perfil de riesgo de TRANSMILENIO S.A., y garantizar que se destinen los recursos necesarios para implementar los controles que permitan mantener el riesgo residual dentro de los niveles de aceptación definidos, así como para implementar y mantener en funcionamiento en forma eficiente el Sistema de Administración de Riesgos.

- **Alta Dirección**

Establece los lineamientos para la Gestión del Riesgo. 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., será el líder de riesgos, esta designación está en cabeza del Jefe de la Oficina Asesora de Planeación, quien es el responsable de formular, orientar y sugerir al Comité del Sistema Integrado de Gestión las mejoras o actualización de la presente política y de apoyar el adecuado cumplimiento de la misma al interior de la entidad.

- 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, tanto internos como externos de TRANSMILENIO S.A.
- Coordinar la recolección de la información para la incorporación de los riesgos de acuerdo a la metodología planteada.
- Realizar el seguimiento permanente de los procedimientos y planes de acción relacionados con la gestión de riesgos y proponer las actualizaciones y modificaciones correspondientes.
- Coordinar los programas de capacitación de TRANSMILENIO S.A., relacionados con el Sistema de Administración de Riesgos.

- **Comité de Gestión y Desempeño Institucional**

Es la máxima instancia de toma de decisiones frente a la gestión de riesgos en la Entidad, se deben revisar los resultados de la gestión del riesgo con el fin de tomar las decisiones que permitan minimizar la probabilidad de ocurrencia y el impacto en caso de que se materialicen.

- **Responsables de los procesos**

Es el responsable de la gestión del riesgo desde cada uno de los procesos, 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.

COPIA NO CONTROLADA

Dentro de sus principales funciones se encuentran:

- 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 subproceso 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.
- 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, asegurando la coherencia y aplicabilidad de la información allí registrada.

- **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 del mismo.

- **Oficina de Control Interno**

Realiza la evaluación y seguimiento a la política, procedimientos, controles y la efectividad de los 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 funciones siguientes:

- 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 programadas sobre el Sistema de Administración de Riesgos.

- Cumplir con las políticas de riesgos establecidas en el presente documento.

6.10 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 a la OFICINA ASESORA DE PLANEACION – OAP, 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
- Actualización de la política y procedimientos relacionados con la gestión de riesgos.
- Documentación de las actividades para el reporte de riesgos.
- Trabajar de manera articulada los riesgos que se generen en la implementación de cada uno de los Subsistemas del Sistema Integrado de Gestión.
- Actualización anual de todos los mapas de riesgos existentes de los procesos definidos en el mapa de procesos institucional cuando se considere pertinente.
- Documentación de los riesgos que se han identificado en la operación normal de la Entidad Identificación de riesgos materializados al interior de la institución.
- Presentación de los informes semestrales sobre la gestión de riesgos al Comité del Sistema Integrado de Gestión y una vez al año a la Junta Directiva por parte del Representante de la Alta Dirección para el Sistema de Administración de Riesgos.
- Diseño de planes de sensibilización y capacitación permanente para los servidores públicos de todos los niveles con el objetivo de generar una cultura de prevención de riesgos al interior de la institución.

6.11 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 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. METODOLOGIA PARA LA GESTION DEL RIESGO

La metodología descrita a continuación está soportada en el formato denominado "*Matriz del Riesgo de Gestión",* en la cual los líderes de los procesos son los responsables de registrar la información y de soportar los resultados de acuerdo con el desarrollo de cada una de las fases que se describen a continuación.

La Oficina Asesora de Planeación, es responsable de 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. Actualizar las matrices y mapas de riesgo por proceso y consolidado y publicar su actualización en la Intranet de la en forma y realizar seguimiento a la implementación de los controles propuestos así como presentar informes a la Gerencia General de acuerdo a las solicitudes de la misma.

TRANSMILENIO S.A., para dar cumplimiento a la Política de Administración de Riesgos, en la cual se resalta la importancia que ésta da a la gestión de la entidad y a la consecución de los objetivos institucionales establecidos en el Plan Estratégico, presenta las siguientes actividades:

7.1 Contexto estratégico

El contexto estratégico consiste en la definición de los factores internos y externos que puedan generar riesgo impactando positiva o negativamente en la consecución de los objetivos de la entidad.

7.1.1 Contexto externo

Ambiente externo en el cual la organización busca alcanzar sus objetivos. Puede incluir el ambiente cultural, social, político, legal, reglamentario, financiero, tecnológico, económico, natural, competitivo, bien sea internacional, nacional, regional o local. Impulsadores clave y tendencias, relaciones con las partes involucradas.

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.

7.1.2 Contexto interno

Ambiente interno en el cual la organización busca alcanzar sus objetivos. Puede incluir gobierno, estructura organizacional, políticas, objetivos y estrategias implementadas para lograrlo, las capacidades entendidas en términos de recursos y conocimiento, sistemas de información y procesos para la toma de decisiones, relación con las partes involucradas internas, cultura organizacional.

El establecimiento del contexto interno incluye:

- 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).

7.2 Criterios para la evaluación de los riesgos

Establecer los criterios que se van a utilizar para la evaluación de los riesgos, tener en cuenta requisitos legales, reglamentarios, o de otra índole que puedan afectar el contexto y el proceso de la entidad.

7.3 Evaluación del riesgo

La evaluación del riesgo está estructurada en 4 partes que incluyen:

1. Identificación del riesgo.
2. Análisis del riesgo.

3. Valoración del Riesgo
4. Tratamiento del riesgo.
5. Monitoreo y revisión.

7.3.1 Identificación del riesgo

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.
- Las no conformidades encontradas en las auditorias de calidad.
- 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.

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 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. Para determinar los riesgos, es necesario realizar el siguiente ejercicio:

“Debido a (Causa concreta), puede ocurrir (Evento/riesgo), lo que podría generar (consecuencia que afecta la entidad y su entorno).

Esta etapa permite establecer los agentes generadores del riesgo (Causas) y los efectos de su ocurrencia (Consecuencias).

7.3.1.1 Identificación de la causa raíz

Es importante tener en cuenta que un riesgo puede tener muchas causas, pero debe llegar a identificarse la causa raíz que permite que el riesgo se materialice.

Para llegar a identificarla, se debe emplear la metodología denominada los "5 por qué", "la espina de pescado", "lluvia de ideas", entre otras. Las metodologías para la identificación de causas pueden ser consultadas en el procedimiento de acciones correctivas, preventivas y de mejora de la Entidad.

La identificación de riesgos debe cumplir con la siguiente estructura:

IDENTIFICACION DE RIESGOS				
DESCRIPCION DEL RIESGO	TIPO DE AFECTACION DEL RIESGO	FACTOR DE RIESGO	CAUSAS Y FUENTES DE RIESGO	DESCRIPCION DE LA CONSECUENCIA /IMPACTO

Figura No. 1: Estructura para la identificación de riesgos de gestión en TRANSMILENIO S.A.

- Descripción del riesgo que afecta los objetivos del proceso.
- Identificar el tipo de afectación del riesgo:
  - ✓ **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la organización pública y por tanto impactan toda la entidad.
  - ✓ **Riesgos gerenciales:** posibilidad de ocurrencia de eventos que afecten los procesos gerenciales y/o la alta dirección.
  - ✓ **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales 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 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.

COPIA NO CONTROLADA

- ✓ **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.

- Identificar el factor de riesgo (Talento humano, tecnología, proceso, eventos externos o infraestructura) que contempla la capacidad potencial de producir impacto/daño material al proceso.
- Identificar las causas o todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.
- Identificar las consecuencias, efectos o situaciones resultantes de la materialización del riesgo que impactan en el proceso, la entidad, sus grupos de valor y demás partes interesadas.

IDENTIFICACION DE RIESGOS							
DESCRIPCION DEL RIESGO					TIPO DE AFECTACION DEL RIESGO	FACTOR RIESGO	CAUSAS Y FUENTES DE RIESGO
DESCRIPCION DEL RIESGO	Acción u omisión	Uso del poder	Desviación de la gestión de lo público	El beneficio privado			

Figura No. 2: Estructura para la identificación de riesgos de corrupción en TRANSMILENIO S.A.

- En la descripción de los riesgos de corrupción deben concurrir TODOS los componentes de su definición, así: Acción u omisión + uso del poder + desviación de la gestión de lo público + el beneficio privado.
- El tipo de afectación del riesgo siempre será “CORRUPCION”.
- Identificar el factor de riesgo (Externo, Interno, o Proceso) que contempla la capacidad potencial de producir impacto/daño material a la entidad.
- Identificar las causas o todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo.

7.3.2 Análisis de Riesgos

El análisis de los riesgos se refiere a que, una vez identificados siguiendo la estructura definida, los riesgos deben ser calificados en dos aspectos importantes. El primero está relacionado con la probabilidad de materialización del riesgo y el segundo en el impacto que tendría para TRANSMILENIO S.A.

Se debe realizar un análisis y calificación de los riesgos con base en la experiencia y conocimiento de los líderes de los procesos, quienes tendrán la responsabilidad de evaluar cada riesgo con base en riesgos que ya hayan sido materializados y se tenga la medición de su impacto.

La evaluación de los riesgos, se deberá llevar a escalas de valoración cualitativas o cuantitativas tanto para la probabilidad como para el impacto, lo que permitirá posteriormente ubicar el riesgo dentro del mapa colorimétrico y conocer su nivel de severidad inherente.

7.3.2.1 Cálculo de la probabilidad de los riesgos de gestión y de corrupción

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia, donde frecuencia implica analizar el número de eventos en un periodo determinado. Se trata de hechos que se han materializado o se cuenta con un historial de situaciones o eventos asociados al riesgo; Total de Operaciones al Año / TOA implica.

El análisis de frecuencia deberá ajustarse dependiendo del proceso y de la disponibilidad de datos históricos sobre el evento o riesgo identificado. En caso de no contar con datos históricos, se trabajará de acuerdo con la experiencia de los responsables que desarrollan el proceso y de sus factores internos y externos.

Para los ***riesgos de gestión***, se ha establecido los siguientes criterios para calificar la probabilidad, la cual se puede calificar de manera cualitativa o cuantitativa:

NIVEL	RANGO	CRITERIOS CALIFICAR PROBABILIDAD	
1	RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	Menos del 10% del TOA
2	IMPROBABLE	El evento puede ocurrir en algún momento	Entre el 11% y el 20% de TOA
3	POSIBLE	El evento podrá ocurrir en algún momento	Entre el 21% y el 30% de TOA
4	PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias	Entre el 31% y el 50% de TOA

NIVEL	RANGO	CRITERIOS CALIFICAR PROBABILIDAD	
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Superior al 50% TOA

Tabla No. 1: Escalas de valoración de la probabilidad para los riesgos de gestión. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

Para los ***riesgos de corrupción***, se ha establecido los siguientes criterios para calificar la probabilidad, la cual se puede calificar de manera cualitativa o cuantitativa:

NIVEL	RANGO	CRITERIOS CALIFICAR PROBAILIDAD RIESGO CORRUPCION	
1	RARA VEZ	El evento puede ocurrir solo en circunstancias excepcionales (poco comunes o anormales)	No se ha presentado en los últimos 5 años
2	IMPROBABLE	El evento puede ocurrir en algún momento	Al menos 1 vez en los últimos 5 años
3	POSIBLE	El evento podrá ocurrir en algún momento	Al menos 1 vez en los últimos 2 años
4	PROBABLE	Es viable que el evento ocurra en la mayoría de las circunstancias	Al menos 1 vez en el último año
5	CASI SEGURO	Se espera que el evento ocurra en la mayoría de las circunstancias	Más de 1 vez al año

Tabla No. 2: Escalas de valoración de la probabilidad para los riesgos de corrupción. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

7.3.2.2 Cálculo del impacto de los riesgos de gestión

La valoración del impacto busca definir, en diferentes escenarios, cuáles serían las consecuencias para TRANSMILENIO S.A. si el riesgo llegara a materializarse. El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo.

El nivel de impacto deberá ser determinado con la presencia de cualquiera de los criterios establecidos, tomando el criterio con mayor nivel de afectación, ya sea cualitativo o cuantitativo.

Se ha definido la siguiente tabla de valoración teniendo en cuenta diferentes escenarios que facilitan la calificación al equipo encargado de valorar el riesgo.

NIVEL	RANGO	RISGOS ASOCIADOS		
		LEGAL/JURIDICA	IMAGEN INSTITUCIONAL	INTERRUPCIONES
1	BAJO	Llamado de atención u observaciones por parte de los entes Externos de Vigilancia y/o Control	Al interior del proceso	No hay afectación en las operaciones de TRANSMILENIO S.A., ni interrupción en la prestación del servicio. Se genera Intermitencias en la prestación del servicio.
2	MENOR	Genera Hallazgos por parte de entes de aseguramiento interno (Oficina de Control interno) y/o Hallazgos de no conformidad o incumplimiento legal como efecto de las Auditorias a los sistemas de gestión	A nivel de la entidad y conocimiento y Junta Directiva	Genera interrupciones parciales inferiores a 1 hora en la prestación del servicio y/o reprocesos de actividades con aumento de la carga operativa de hasta de 2 horas
3	MODERADO	Genera requerimientos u observaciones por parte de entes de control (Contraloría, Procuraduría) y/o ente de inspección y vigilancia. Otras entidades, que emitan Normatividad que deba ser aplicada por parte de TRANSMILENIO S.A.	A nivel de la entidad y conocimiento y Junta Directiva Posible afectación a un grupo reducido de usuarios o a sus proveedores. Comentarios en Redes Sociales Sin impacto en Medios de Comunicación reconocidos y Redes sociales de Influenciadores	Genera interrupciones parciales inferiores a 4 horas en la prestación del servicio y/o reprocesos de actividades con aumento de la carga operativa de hasta de 4 horas
4	MAYOR	Genera demandas	Posible afectación a un grupo significativos de usuarios (entre 40% y el 65%) y sus partes interesadas Comentarios en redes sociales reiterados (entre 2 y 4 días) Con impacto en Medios de Comunicación reconocidos y Redes sociales de Influenciadores	Genera interrupciones parciales inferiores a 8 horas en la prestación del servicio y/o reprocesos de actividades con aumento de la carga operativa de hasta de 8 horas
5	CATASTROFICO	Genera sanciones y/o multas por incumplimiento de la normatividad y/o derivadas de fallos judiciales	Posible afectación de a un grupo mayoritarios de usuarios (mayor al 65%) y sus partes interesadas Afectación de la movilidad de la Ciudad. Comentarios en Redes Sociales superior a 5 días Con impacto en Medios de Comunicación reconocidos y Redes sociales de Influenciadores	Genera interrupciones parciales superiores a 8 horas en la prestación del servicio y/o reprocesos de actividades con aumento de la carga operativa de hasta de 12 horas

Tabla No. 3: Escalas de valoración del impacto / consecuencia. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

El análisis de riesgos de gestión debe cumplir con la siguiente estructura:

ANALISIS DE RIESGOS								
PROBABILIDAD		IMPACTO POR RIESGO ASOCIADO					ZONA DE RIESGO INHERENTE	OPCIONES DE MANEJO DEL RIESGO
PROB	NIVEL	IMAGEN INSTITUCIONAL	JURIDICAS	INTERRUPCION	INCUMPLIMIENTO OBJETIVOS	NIVEL DE IMPACTO		

Figura No. 3: Estructura para el análisis de riesgos de gestión en TRANSMILENIO S.A.

- Analizar y determinar el nivel de probabilidad para cada causa del riesgo, considerando los criterios para calificar la probabilidad determinados por TRANSMILENIO S.A. *(Ver Tabla No. 1: Escalas de valoración de la probabilidad)*
- Analizar y determinar el nivel de impacto, desde la imagen institucional, jurídica, interrupción del proceso o de la operación, o del incumplimiento de los objetivos del proceso o de la entidad, considerando los criterios para calificar impactos determinados por TRANSMILENIO S.A. *(Ver Tabla No. 2: Escalas de valoración de consecuencia)*
- La zona de riesgo inherente se obtiene automáticamente del resultado del nivel de probabilidad por el nivel de impacto.
- Opciones de manejo del riesgo: Por política de la entidad la opción siempre será reducir el riesgo.

7.3.2.3 Cálculo del impacto de los riesgos de corrupción

El impacto de la materialización de un riesgo de corrupción es único, por cuanto lesiona la imagen, la credibilidad, la transparencia y la propiedad de las entidades y del Estado, afectando los recursos públicos, la confianza y el cumplimiento de las funciones de la administración, siendo por tanto inaceptable la materialización de un riesgo de corrupción.

Para calificar el impacto en los riesgos de corrupción, se tendrán en cuenta los siguientes criterios:

TABLA ILUSTRATIVA. CRITERIOS PARA CALIFICAR EL IMPACTO EN LOS RIESGOS DE CORRUPCIÓN

No.	Pregunta: Si el riesgo de corrupción se materializa podría…	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 la misión de la Entidad?		
4	¿Afectar el cumplimiento del sector al que pertenence la Entidad?		
5	¿Generará pérdida de confianza de la Entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien o servicios o los recursos públicos?		
9	¿Generar pérdida de información de la Entidad?		
10	¿Generar intervención de los órganos de control, de la Fiscalía, 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 pérdida de credibilidad del sector?		
16	¿Ocasionar lesiones físicas o pérdida de vidas humanas?		
17	¿Afectar la imagen regional?		
18	¿Afectar la imagen nacional?		
19	¿Generar daño ambiental?		

Responder afirmativo de uno (1) a cinco (5) preguntas genera un impacto **moderado**.
Responder afirmativo de seis (6) a once (11) preguntas genera un impacto **mayor**.
Responder afirmativamente de doce (12) a diecinueve (19) preguntas genera un impacto **catastrófico.**

MODERADO	**Genera medianas consecuencias sobre la entidad**
MAYOR	**Genera altas consecuencias sobre la entidad**
CATASTROFICO	**Genera consecuencias desastrosas para la entidad**

*Tabla No.4. Criterios para calificar el Impacto - **Riesgos de Corrupción.** Fuente: Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.*

7.3.2.4 Análisis del impacto en riesgos de corrupción

Para los riesgos de corrupción, el análisis de impacto se realizará teniendo en cuenta solamente los niveles moderado, mayor y catastrófico, dado que estos riesgos siempre serán significativos; en este orden de ideas, no aplican los niveles de impacto insignificante y menor, que si aplican para los demás riesgos.

COPIA NO CONTROLADA

7.3.2.5 Nivel de riesgo inherente

El nivel de riesgo inherente hace referencia al valor obtenido de multiplicar la probabilidad de ocurrencia por el impacto del riesgo, sin tener en cuenta el efecto de los controles.

Para la evaluación del "factor de riesgo" se han seleccionado los criterios de probabilidad e impacto, en una escala de valoración del 1 al 5, según la importancia, repetitividad u ocurrencia. Esta escala de valores aparece en los desplegables de las respectivas celdas de las columnas de impacto y probabilidad. El producto de los dos proporciona el cálculo del "factor de riesgo", siendo el valor máximo 25 y el mínimo 1.

PROBABILIDAD		IMPACTO				
		Bajo	Menor	Moderado	Mayor	Catastrófico
		1	2	3	4	5
Casi seguro	5	5	10	15	20	25
Probable	4	4	8	12	16	20
Posible	3	3	6	9	12	15
Improbable	2	2	4	6	8	10
Rara vez	1	1	2	3	4	5

Tabla No. 5: Factor de riesgo

Según los diferentes valores que se pueden obtener, se puede asignar un "nivel de riesgo" que se ha categorizado en los siguientes: "Extremo", "Alto", "Moderado", y "Bajo".

NIVEL DE RIESGO	
1 -2	BAJO
3 -6	MODERADO
7 -12	ALTO
13 - 25	EXTREMO

Tabla No. 5: Nivel de riesgo inherente .

El resultado, permite ubicar en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto para establecer el nivel del riesgo inherente, de la siguiente manera:

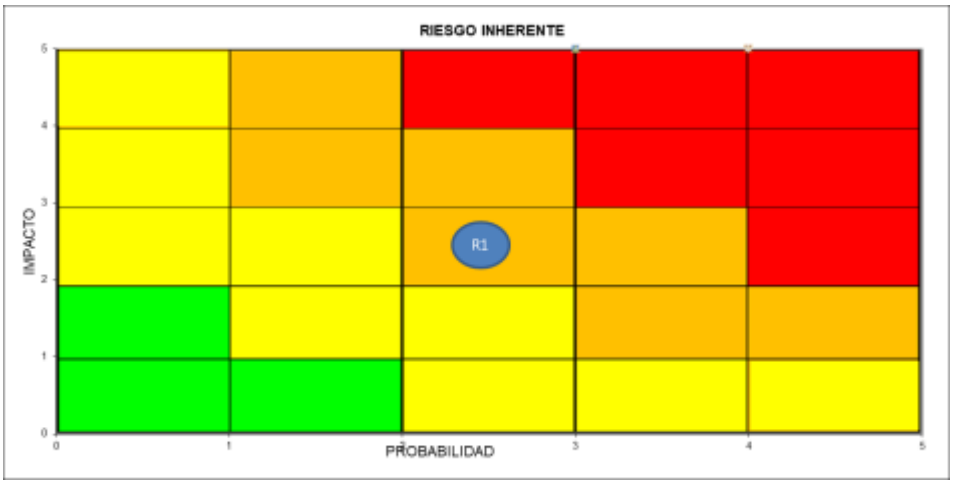


Figura No. 4: Mapa térmico riesgo inherente

Aunque se utilice el mismo mapa de calor, para los riesgos de gestión y de corrupción, a estos últimos solo les aplican las columnas de impacto Moderado, Mayor y Catastrófico.

7.3.3 Valoración de los riesgos

Luego de conocer el nivel del riesgo inherente, se deben identificar los controles existentes para mitigarlo y deben ser evaluados 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 uno.

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.

¿Qué son 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.

Las actividades de control, independientemente de la tipología de riesgo a tratar, deben tener una adecuada combinación para prevenir que la situación de riesgo se origine. Ahora, en caso de que la situación de riesgos se presente, esta debe ser detectada de manera oportuna.

Clasificación de las actividades de control

- Controles Preventivos: Controles que están diseñados para evitar un evento no deseado en el momento en que se produce. Este tipo de controles intentan evitar la ocurrencia de los riesgos que puedan afectar el cumplimiento de los objetivos. Ejemplo: Revisión al cumplimiento de los requisitos contractuales, en el proceso de selección del contratista o proveedor.
- Controles Detectivos: Controles que están diseñados para identificar un evento o resultado no previsto después de que se haya producido. Buscan detectar la situación no deseada para que se corrija y se tomen las acciones correspondientes. Ejemplo: Realizar una conciliación bancaria, para verificar que los saldos en libros corresponden con los saldos en Bancos.
- Controles Correctivos. Permiten el restablecimiento de una actividad, después de ser detectado un evento no deseable, posibilitando la modificación de las acciones que propiciaron su ocurrencia. Estos controles se establecen cuando los anteriores no operan, y permiten mejorar las deficiencias. Son de tipo administrativo y requieren políticas o procedimientos para su ejecución.

7.3.3.1 Diseño de los controles

Al momento de definir si un control o los controles mitigan de manera adecuada el riesgo se deben considerar, desde la redacción del mismo, las siguientes variables:

- Paso 1: Debe tener definido el responsable de llevar a cabo la actividad de control.
- Paso 2: Debe tener una periodicidad definida para su ejecución.
- Paso 3: Debe indicar cuál es el propósito del control.
- Paso 4: Debe establecer el cómo se realiza la actividad de control.
- Paso 5: Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control.
- Paso 6: Debe dejar evidencia de la ejecución del control.

Se ha considerado la siguiente estructura para el diseño de los controles:

COPIA NO CONTROLADA

DISEÑO DE CONTROLES						
FICHA TECNICA						
DESCRIPCION DEL CONTROL						
DESCRIPCION	TIPO	NATURALEZA	PERIODICIDAD	EJECUTOR DEL CONTROL	RESPONSABLE	INDICADOR ASOCIADO AL CONTROL

Figura No. 5: Estructura para el diseño de controles

- La descripción del control debe cumplir con los siguientes seis pasos:
  1. Tipo de actividad de control (Revisar, verificar, supervisar, cotejar, etc.)
  2. ¿Cómo se hace?
  3. Que hacer frente al resultado de la ejecución del control (Corregir, Ajustar; No aprobar, devolver, etc.)
  4. ¿Quién lo hace?
  5. ¿Con qué periodicidad lo hace?
  6. ¿Cómo deja evidencia de su ejecución?
- Definir el tipo de control de acuerdo a los siguientes criterios:
  1. Controles Preventivos
  2. Controles Detectivos
  3. Controles Correctivos
- La naturaleza del control puede ser:
  1. Control manual: Es la acción que realizan los colaboradores responsables de un proceso o actividad.
  2. Control automático: Es la acción o procedimiento aplicado desde un computador en una aplicación tecnológica (software), para prevenir, detectar o corregir errores o deficiencias.
  3. Control asistido por TI: Es la acción que es realizada por los colaboradores responsables de un proceso o actividad, y a la vez aplicado desde un computador en una aplicación tecnológica.
- Periodicidad con la que se aplica el control (ejemplo: diario, semanal, mensual, cuando se requiera, etc.)
- Ejecutor del Control: Es el cargo que ejecuta directamente el control.
- Responsable: Responsable del control será el dueño del proceso (Directivo) responsable de que se cumpla con su ejecución.
- Indicador Asociado al Control: Corresponde al indicador que permitirá en la etapa de monitoreo, evaluar la efectividad de la aplicación del control sobre el riesgo inherente,

7.3.3.2 Valoración de los controles

Una vez que se han identificado los controles, éstos deben ser evaluados con el objetivo de analizar el efecto que tienen sobre el riesgo, aclarando que hay controles que mitigan la probabilidad de ocurrencia del riesgo y otros que están diseñados para minimizar el impacto en caso de que el riesgo se materialice.

Para la adecuada mitigación de los riesgos, no basta con que un control esté bien diseñado, el control debe ejecutarse por parte de los responsables tal como se diseñó. Porque un control que no se ejecute, o un control que se ejecute y esté mal diseñado, no va a contribuir a la mitigación del riesgo.

Se ha considerado la siguiente estructura para el análisis y evaluación del diseño del control de acuerdo con las seis (6) variables establecidas:



Figura No.6: Diseño de controles de acuerdo con las seis (6) variables establecidas

- Marque una X a los aspectos que se cumplen en el diseño del control:

  1.1 ¿Existe un responsable asignado a la ejecución del control?

  1.2¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control?

  2. ¿La oportunidad en que se ejecuta el control ayuda a prevenir la mitigación del riesgo o a detectar la materialización del riesgo de manera oportuna?

  3. ¿Las actividades que se desarrollan en el control realmente buscan por si sola prevenir o detectar las causas que pueden dar origen al riesgo, Ej.: verificar, validar, cotejar, comparar, revisar, etc.?

  4. ¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?

5. ¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?

6. ¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?

- El total del diseño del control se obtiene de la sumatoria de las (6) variables establecidas, que apliquen.



Figura No.7: Esquema de análisis y evaluación de los controles

- En la ejecución del control solo es aplicable una opción, por marque una X a la que corresponda:
  1. Marque X, si el control nunca se ejecuta.
  2. Marque X, si la ejecución de control se ejecuta de acuerdo con la consideración del responsable, por fuera de la periodicidad definida. (cada vez que el funcionario se acuerda o desee realizarlo).
  3. Marque X, si el funcionario SIEMPRE ejecuta el control, de acuerdo a la que ha sido definida.
- En la solidez individual del control solo es aplicable una opción, por marque una X a la que corresponda:
  1. Evidencia o percepción negativa. Marque X, si el funcionario que ejecuta el control puede evidenciar con documentos o indicadores, que la aplicación del control NO permite prevenir o el riesgo o mitigar el impacto de su ocurrencia.
  2. Percepción positiva. Marque X, si el funcionario que ejecuta el control NO puede evidenciar con documentos o indicadores, que la aplicación del control SI permite prevenir o el riesgo o mitigar el impacto de su ocurrencia.
  3. Evidencia de su efectividad. Marque X, si el funcionario que ejecuta el control puede evidenciar con documentos o indicadores, que la aplicación del control SI permite prevenir o el riesgo o mitigar el impacto de su ocurrencia.
- El total de la calificación del control se obtiene de la sumatoria de las opciones que apliquen para la ejecución del control y la solidez individual del control.

7.3.3.3 Resultados de la evaluación del diseño del control

El resultado de cada variable de diseño, a excepción de la evidencia, va a afectar la calificación del diseño del control, ya que deben cumplirse todas las variables, para que un control se evalué como bien diseñado.

Rango de calificación del diseño	Resultado - Peso en la evaluación del diseño del control
Fuerte	Calificación entre 96 y 100
Moderado	Calificación entre 86 y 95
Débil	Calificación entre 0 y 85

Tabla No. 7: Resultados de la evaluación del diseño del control. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

Si el resultado de las calificaciones del control, o el promedio en el diseño de los controles, está por debajo de 96%, se debe establecer un plan de acción que permita tener un control o controles bien diseñados.

7.3.3.4 Resultados de la evaluación de la ejecución del control

Aunque un control este bien diseñado, este debe ejecutarse de manera consistente, de tal forma que se pueda mitigar el riesgo. No basta solo con tener controles bien diseñados, debe asegurare por parte de la primera línea de defensa que el control se ejecute. Al momento de determinar si el control se ejecuta, inicialmente, el responsable del proceso debe llevar a cabo una confirmación, posteriormente se confirma con las actividades de evaluación realizadas por auditoría interna o control interno.

Rango de calificación de la ejecución	Resultado - Peso de la ejecución del control
Fuerte	El control se ejecuta de manera consistente por parte del responsable.
Moderado	El control se ejecuta algunas veces por parte del responsable.
Débil	El control no se ejecuta por parte del responsable.

Tabla No. 8 Resultados de la evaluación de la ejecución del control. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

7.3.3.5 Solidez del conjunto de controles para la adecuada mitigación del riesgo

Dado que un riesgo puede tener varias causas, a su vez varios controles y la calificación se realiza al riesgo, es importante evaluar el conjunto de controles asociados al riesgo.

Calificación de la solidez del conjunto de controles	
Fuerte	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es igual a 100.
Moderado	El promedio de la solidez individual de cada control al sumarlos y ponderarlos está entre 50 y 99.
Débil	El promedio de la solidez individual de cada control al sumarlos y ponderarlos es menor a 50.

Tabla No. 9 Calificación de la solidez del conjunto de controles. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

7.3.3.6 Nivel de riesgo (riesgo residual)

Desplazamiento del riesgo inherente para calcular el riesgo residual

Dado que ningún riesgo con una medida de tratamiento se evita o elimina, el desplazamiento de un riesgo inherente en su probabilidad o impacto para el cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla:

Solidez del conjunto de los controles	Controles ayudan a disminuir la probabilidad	Controles ayudan a disminuir el impacto	*Columnas en la matriz de riesgo que se desplaza en el eje de la probabilidad	*Columnas en la matriz de riesgo que se desplaza en el eje del impacto
Fuerte	Directamente	Directamente	2	2
Fuerte	Directamente	Indirectamente	2	1
Fuerte	Directamente	No disminuye	2	0
Fuerte	No disminuye	Directamente	0	2
Moderado	Directamente	Directamente	1	1
Moderado	Directamente	Indirectamente	1	0
Moderado	Directamente	No disminuye	1	0
Moderado	No disminuye	Directamente	0	1

Tabla No. 10 Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos. Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

Si la solidez del conjunto de los controles es débil, este no disminuirá ningún cuadrante de impacto o probabilidad asociada al riesgo.

COPIA NO CONTROLADA

Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Se ha considerado la siguiente estructura para el riesgo residual:

RIESGO RESIDUAL			
SOLIDEZ DEL CONJUNTO DE CONTROLES PREVENTIVOS Y DE DETECCION	SOLIDEZ DEL CONJUNTO DE CONTROLES CORRECTIVOS	EFECTO RESIDUAL	ZONA DE RIESGO RESIDUAL

Figura No.8: Estructura evaluación del riesgo residual

Una vez realizado el análisis y evaluación de los controles para la mitigación de los riesgos, procedemos a la elaboración del mapa de riesgo residual (después de los controles).

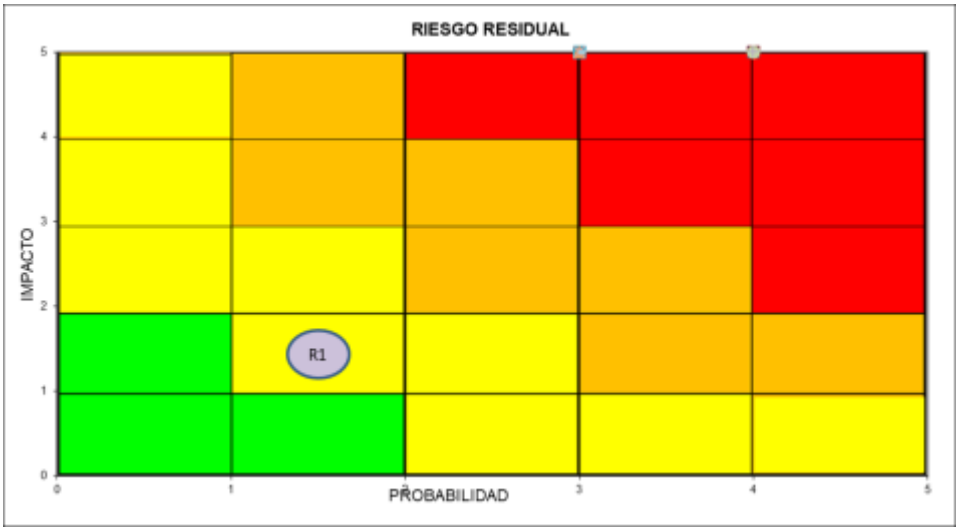


Figura No. 9: Mapa térmico riesgo residual

7.3.4 Tratamiento del riesgo

El tratamiento del riesgo es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. A la hora de evaluar las opciones existentes en materia de tratamiento del 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. Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la dirección se deberá volver a analizar y revisar dicho tratamiento.

En todos los casos para los **riesgos de corrupción la respuesta será evitar, compartir o reducir el riesgo,** en ningún caso el riesgo de corrupción podrá ser aceptado.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:



Figura No. 10: Categorías de tratamiento del riesgo

De acuerdo al nivel de riesgo residual obtenido, se definen los siguientes criterios para seleccionar las opciones de manejo que se le debe dar a un riesgo:

- Para los riesgos de nivel bajo se deben adoptar la opción de tratamiento “Aceptar” el riesgo.
- Los riesgos de nivel medio, deben optar por la opción de tratamiento “Aceptar” el riesgo o la opción “Reducir” el riesgo.
- Los riesgos de nivel alto y extremo se deben “Reducir”, “Evitar”, o “Compartir”

7.3.4.1 Tratamiento del riesgo – rol de la primera línea de defensa

Como medio para propiciar el logro de los objetivos, las actividades de control se orientan a prevenir y detectar la materialización de los riesgos. Por consiguiente, su efectividad depende, de qué tanto se están logrando los objetivos estratégicos y de proceso de la entidad. Le corresponde a la primera línea de defensa el establecimiento de las actividades de control.

Se ha considerado la siguiente estructura para el plan de tratamiento:

PLAN DE TRATAMIENTO							
PLAN REQUERIDO	OPCIONES DE MANEJO	ACCIONES BASE	DESCRIPCION	RESPONSABLE	FECHA INICIO	FECHA VENCIMIENTO	INDICADOR ASOCIADO AL PLAN DE TRATAMIENTO

Figura No.11: Formato plan de tratamiento de riesgos de gestión y de corrupción

- El plan de acción se determina según la calificación toral del control, si el control es débil requiere plan de acción, pero si el control es fuerte no requerirá plan de acción.
- A la hora de evaluar las opciones existentes en materia de tratamiento del riesgo (aceptar el riesgo, reducir el riesgo, evitar el riesgo, o compartir 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.
- Si requiere plan de acción, definir la acción base que implementara (ejemplo: mejorar el diseño del control, ajustar el control, reemplazar el control, llamado de atención al responsable, o diseñar nuevo control)
- Describir el plan de acción que implementará, asignando un responsable, la fecha Inicio, y la fecha vencimiento.
- Diseñar un indicador de eficacia, que indique el cumplimiento de las actividades para la gestión del riesgo del proceso.

7.4 Monitoreo y revisión

Teniendo en cuenta que ningún riesgo se mantiene estático, puesto que el negocio es dinámico, se debe realizar un monitoreo y revisión constante de los riesgos identificados, la calificación de probabilidad e impacto; los controles diseñados y su evaluación y así revisar las prioridades en los tratamientos de los riesgos.

Cada vez que se identifique algún nuevo riesgo, cambios en el análisis de un riesgo ya identificado o cambios en los controles para mitigar el riesgo, debe actualizarse la matriz de riesgos y debe ser remitida a la Oficina Asesora de Planeación.

El líder de proceso junto con su equipo de trabajo, deben revisar periódicamente que los controles definidos estén documentados, se aplican y son efectivos y deben informar al líder de riesgos sobre dicha revisión.

Se ha definido el cálculo de un indicador de cumplimiento de acuerdo al seguimiento realizado a la implementación de los planes de la siguiente manera:

% CUMPLIMIENTO = Número de acciones de tratamiento implementadas/Número de acciones de tratamiento programadas

Este indicador aplica de acuerdo a la fecha definida para la implementación de la acción de tratamiento cuando aplique.

7.4.1 Monitorear y revisar la gestión de riesgos

La entidad debe asegurar el logro de sus objetivos, anticipándose a los eventos negativos relacionados con la gestión de la entidad. El Modelo Integrado de Plantación y Gestión- (MIPG) en la dimensión 7 “Control Interno” desarrolla a través de las Líneas de Defensa la responsabilidad de la gestión del riesgo y control.

El modelo de las líneas de defensa es un modelo de control que establece los roles y responsabilidades de todos los actores del riesgo y control en una entidad, este proporciona aseguramiento de la gestión y previene la materialización de los riesgos en todos sus ámbitos.

7.4.2 Asignación de roles y responsabilidades para monitoreo y revisión de la gestión de riesgos

El monitoreo y revisión de la gestión de riesgos se desarrolla a través de un esquema de asignación de responsabilidades y roles, el cual se distribuye en diversos servidores de la entidad como sigue:

LINEA ESTRATEGICA		
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.		
1era Línea de Defensa	**2da Línea de Defensa**	**3ra Línea de Defensa**
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora.	Asegura que los controles y los procesos de gestión de riesgos implementados por la primera línea de defensa, estén diseñados apropiadamente y funcionen como se pretende	Proporciona información sobre la efectividad del S.C.I., a través de un enfoque basado en riesgos, incluida la operación de la primera y segunda línea de defensa
A cargo de los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad. **Rol principal:** diseñar, implementar y monitorear los controles y gestionar de manera directa en el día a día los riesgos de la entidad. Así mismo, orientar el desarrollo e implementación de políticas y procedimientos internos y asegurar que sean compatibles con las metas y objetivos de la entidad y emprender las acciones de mejoramiento para su logro.	A cargo de los servidores que tienen responsabilidades directas en el monitoreo y evaluación de los controles y la gestión del riesgo: Jefes de planeación, supervisores e interventores de contratos o proyectos, coordinadores de otros sistemas de gestión de la entidad, comités de riesgos (donde existan), comités de contratación, entre otros. **Rol principal:** monitorear la gestión de riesgo y control ejecutada por la primera línea de defensa, complementando su trabajo.	A cargo de la oficina de control interno, auditoría interna o quien haga sus veces. **El rol principal:** proporcionar un aseguramiento basado en el más alto nivel de independencia y objetividad sobre la efectividad del S.C.I. El alcance de este aseguramiento, a través de la auditoría interna cubre todos los componentes del S.C.I.

7.4.2.1 Rol de la línea estratégica en el monitoreo y revisión de los riesgos y actividades de control

LINEA ESTRATEGICA
Define el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la Alta Dirección y el Comité Institucional de Coordinación de Control Interno.
Actividades de Monitoreo y Revisión Para Realizar
La alta dirección y el equipo directivo, a través de sus comités deben monitorear y revisar el cumplimiento a los objetivos a través de una adecuada gestión de riesgos con relación a lo siguiente: ✓ Revisar los cambios en el "Direccionamiento estratégico" y cómo estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados. ✓ Revisión del adecuado desdoblamiento de los objetivos institucionales a los objetivos de procesos, que han servido de base para llevar a cabo la identificación de los riesgos. ✓ Hacer seguimiento en el Comité Institucional y de Control Interno a la implementación de cada una de las etapas de la gestión del riesgo y los resultados de las evaluaciones realizadas por Control Interno o Auditoría Interna. ✓ Revisar el cumplimiento a los objetivos institucionales y de procesos y sus indicadores e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ✓ Hacer seguimiento y pronunciarse por lo menos cada trimestre sobre el perfil de riesgo inherente y residual de la entidad, incluyendo los riesgos de corrupción y de acuerdo a las políticas de tolerancia establecidas y aprobadas. ✓ Revisar los informes presentados por lo menos cada trimestre de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, 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. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento.

7.4.2.2 Rol de las líneas de defensa en el monitoreo y revisión de los riesgos y actividades de control

1era LINEA DE DEFENSA
Desarrolla e implementa procesos de control y gestión de riesgos a través de su identificación, análisis, valoración, monitoreo y acciones de mejora. Está conformada por los gerentes públicos y líderes de los procesos, programas y proyectos de la entidad.
Actividades de Monitoreo y Revisión a Realizar
Los gerentes públicos y los líderes de proceso deben monitorear y revisar el cumplimiento de los objetivos institucionales y de sus procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente: ✓ 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 sus procesos, para la actualización de la matriz de riesgos de su proceso. ✓ Revisión como parte de sus procedimientos de supervisión, la revisión del adecuado diseño y ejecución de los controles establecidos para la mitigación de los riesgos. ✓ Revisar que las actividades de control de sus procesos se encuentren documentadas y actualizadas en los procedimientos. ✓ Revisar el cumplimiento de los objetivos de sus procesos y sus indicadores de desempeño, e identificar en caso de que no se estén cumpliendo, los posibles riesgos que se están materializando en el cumplimiento de los objetivos. ✓ Establecer la respuesta para la mitigación de los diferentes riesgos, incluyendo aquellos relacionados con la corrupción. ✓ Revisar y reportar a planeación, los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, 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. ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible la repetición del evento y lograr el cumplimiento a los objetivos. ✓ Revisar y hacer seguimiento al cumplimiento de las actividades y planes de acción acordados con la línea estratégica, segunda y tercera línea de defensa con relación a la gestión de riesgos.

2da LINEA DE DEFENSA

Asiste y guía la línea estrategia y la primera línea de defensa en la gestión adecuada de los Riesgos que pueden afectar el cumplimiento de los objetivos institucionales y de sus procesos, incluyendo los riesgos de corrupción, a través del establecimiento de directrices y apoyo en el proceso de identificar, analizar, evaluar y tratar los riesgos, y realiza un monitoreo independiente al cumplimiento de las etapas de la gestión de riesgos. Está conformada por los responsables de monitoreo y evaluación de controles y gestión del riesgo (jefes de planeación, supervisores e interventores de contratos o proyectos, responsables de sistemas de gestión, etc.

Actividades de Monitoreo y Revisión Para Realizar

Los jefes de planeación, supervisores e interventores de contratos o proyectos o responsables de sistemas de gestión deben monitorear y revisar el cumplimiento de los objetivos institucionales y de procesos a través de una adecuada gestión de riesgos, incluyendo los riesgos de corrupción, con relación a lo siguiente:

- ✓ 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 en 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.
- ✓ Revisar el adecuado diseño 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 y seguimiento para el fortalecimiento de los mismos.
- ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad.
- ✓ Hacer seguimiento a que las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos.
- ✓ Revisar los planes de acción establecidos para cada uno de los riesgos materializados, con el fin de que se tomen medidas oportunas y eficaces para evitar en lo posible que se vuelva a materializar el riesgo y lograr el cumplimiento a los objetivos.

3ra LINEA DE DEFENSA

Provee aseguramiento (evaluación) independiente y objetivo sobre la efectividad del sistema de gestión de riesgos, validando que la línea estratégica, la primer línea y segunda línea de defensa cumplan con sus responsabilidades en la gestión de riesgos para el logro en el cumplimiento de los objetivos institucionales y de proceso, así como los riesgos de corrupción. Está conformada por la Oficina de Control Interno o Auditoría Interna.

Actividades de Monitoreo y Revisión Para Realizar

La oficina de control interno o auditoría interna monitorea y revisa de manera independiente y objetiva el cumplimiento de los objetivos institucionales y de procesos, a través de la adecuada gestión de riesgos, incluyendo los riesgos de corrupción con relación a lo siguiente:

- ✓ 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 que afectan en el cumplimiento de los objetivos de los procesos, incluyendo los riesgos de corrupción.
- ✓ Revisar el adecuado diseño y ejecución de los controles para la mitigación de los riesgos que se han establecido por parte de la Primer Línea de Defensa y realizar las recomendaciones y seguimiento para el fortalecimiento de los mismos.
- ✓ Revisar el perfil de riesgo inherente y residual por cada proceso y consolidado y 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 que las actividades de control establecidas para la mitigación de los riesgos de los procesos 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.

7.4.3 Monitoreo riesgos de corrupción

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 Asesora de Planeación adelantar el monitoreo, (segunda línea de defensa) para este propósito se sugiere elaborar una matriz para el monitoreo periódico. Este monitoreo será en los tiempos que determine la entidad.

Su importancia radica en la necesidad de monitorear permanentemente la gestión del riesgo y la efectividad de los controles establecidos. Teniendo en cuenta que la corrupción es, por sus propias características una actividad difícil de detectar.

Para el efecto deben atender las actividades descritas en la primera y segunda línea de defensa de este documento[4].

7.4.4 Reporte Plan de Tratamiento de Riesgos

Consolidar información para la gestión del riesgo

1) Una vez analizado el nivel de riesgo residual y definido el tratamiento a implementar con el establecimiento de controles preventivos y detectivos, es necesario generar un reporte que consolide la información clave del proceso de gestión del riesgo.

2) En el formato de Mapa y Plan de Tratamiento de Riesgos, se inicia con el registro del riesgo identificado, luego se especifica la clase de riesgo, se transcriben las causas raíz o causas priorizadas, así como la probabilidad e impacto que quedaron después de valorar los controles para determinar el riesgo residual.

3) A partir de allí se deben analizar las estrategias DOFA o estrategias de supervivencia formuladas en la etapa de establecimiento del contexto, que contrarresten las causas raíz, para colocarlas en las actividades de control del formato y con base en su contenido se establezca la opción de tratamiento a la que corresponden.

[4] Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, Octubre de 2018

4) Luego se relaciona el soporte con el que se evidenciará el cumplimiento de cada actividad, el responsable de adelantarla (relacionando el cargo y no el nombre), el tiempo específico para cumplir con la actividad o la periodicidad de ejecución.

5) Al final de todas las actividades de control establecidas para atacar las causas del riesgo, se debe relacionar la acción de contingencia a implementar una vez el riesgo se materialice, para ello se deben analizar las estrategias DA o estrategias de fuga provenientes de la Matriz DOFA, seleccionando la(s) más apropiada(s) para el riesgo identificado.

6) No olvidar colocar el soporte, responsable y tiempo de ejecución, teniendo en cuenta que este tipo de acciones son de aplicación inmediata y a corto plazo para restablecer cuanto antes, la normalidad de las actividades para el logro de los objetivos del proceso o la estrategia.

7) Por último, se formulan los indicadores clave de riesgo (KRI por sus siglas en ingles) que permitan monitorear el cumplimiento (eficacia) e impacto (efectividad) de las actividades de control, siempre y cuando conduzcan a la toma de decisiones (Por riesgo identificado en los procesos).

7.4.5 Reporte de la gestión del riesgo

La primera línea de defensa reporta a la segunda línea de defensa, el estado de avance del tratamiento del riesgo en la operación, y la consolidación de los riesgos en todos los niveles será reportada por la segunda línea de defensa (encargado de la gestión del riesgo) hacia la alta dirección.

7.4.6 Reporte de la gestión del riesgo de corrupción

De igual forma se debe reportar en el mapa y plan de tratamiento de riesgos, los riesgos de corrupción, de tal forma que se comunique toda la información necesaria para su comprensión y tratamiento adecuado.

7.5 Seguimiento riesgos de corrupción

- **Seguimiento:** El Jefe de Control Interno o quien haga sus veces, debe adelantar seguimiento al Mapa de Riesgos de Corrupción. En este sentido es necesario que adelante seguimiento a la gestión del riesgo, verificando la efectividad de los controles.
- ***Primer seguimiento:*** Con corte al 30 de abril. En esa medida, la publicación deberá surtirse dentro de los diez (10) primeros días del mes de mayo.

- ***Segundo seguimiento:*** Con corte al 31 de Octubre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- ***Tercer seguimiento:*** Con corte al 31 de diciembre. La publicación deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El seguimiento adelantado por la Oficina de Control Interno se podrá registrar en el formato modelo *"Anexo 6 Matriz Seguimiento Mapa de Riesgos de Corrupción",* que propone la Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, y se deberá publicar en la página web de la Entidad o en lugar de fácil acceso al ciudadano,

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

7.5.1 Acciones a seguir en caso de materialización de riesgos de corrupción

En el evento de materializarse un riesgo de corrupción, es necesario realizar los ajustes necesarios con acciones, tales como:

1. Informar a las autoridades de la ocurrencia del hecho de corrupción.
2. Revisar el Mapa de Riesgos de Corrupción, en particular las causas, riesgos y controles.
3. Verificar si se tomaron las acciones y se actualizó el Mapa de Riesgos de Corrupción.
4. Realizar un monitoreo permanente.

La Oficina de Control Interno debe asegurar que los controles sean efectivos, le apunten al riesgo y estén funcionando en forma oportuna y efectiva.

Las acciones adelantadas se refieren a:

- Determinar la efectividad de los controles.
- Mejorar la valoración de los riesgos.
- Mejorar los controles.
- 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.

8. COMUNICACIÓN Y CONSULTA

La comunicación y consulta con las partes involucradas tanto internas como externas debería tener lugar durante todas las etapas del proceso para la gestión del riesgo. Este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo[5].

8.1 Plan de capacitación

Para llevar a cabo esta etapa, el Representante de la Alta Dirección para el Sistema de Administración de Riesgos debe diseñar capacitaciones y /o sensibilizaciones periódicas que cubra todos los niveles de la Entidad.

8.2 Planes para la comunicación y consulta

Teniendo en cuenta la importancia de mantener informados a todos los servidores públicos sobre las diferentes etapas del Sistema de Administración de Riesgos y sobre la evolución de cada una de ellas, se recogen, entonces, los siguientes planes para la comunicación y consulta:

- Capacitaciones y/o sensibilizaciones periódicas.
- Publicaciones en materia de riesgos a través de la Intranet de la Entidad.
- Publicación de los mapas de riesgo por proceso en la intranet de la Entidad para consulta de todos los servidores públicos.

[5] Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas, Octubre de 2018, versión 1

9. INFORMACIÓN, COMUNICACIÓN Y REPORTE

La comunicación de la información y el reporte debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

Por tanto, se debe hacer especial énfasis en la difusión, socialización, capacitación y/o entrenamiento de todos y cada uno de los pasos que componen la metodología de la administración del riesgo, asegurando que permee a la totalidad de la organización pública.

Se debe conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas.

Responsabilidades por línea de defensa para la Información, comunicación y reporte:

Línea Estratégica	• Corresponde al Comité de Auditoría de las Empresas Industriales y Comerciales del Estado y/o a los Comités Institucionales de Coordinación de Control Interno, establecer la Política de Gestión de Riesgos y asegurarse de su permeabilización en todos los niveles de la organización pública, de tal forma que se conozcan claramente los niveles de responsabilidad y autoridad que posee cada una de las tres líneas de defensa frente a la gestión del riesgo.
Primera Línea de Defensa	• Corresponde a los jefes de área y/o grupo (primera línea de defensa) asegurarse de implementar esta metodología para mitigar los riesgos en la operación, reportando a la segunda línea sus avances y dificultades
Segunda Línea de Defensa	• Corresponde al área encargada de la gestión del riesgo (segunda línea de defensa) la difusión y asesoría de la presente metodología, así como de los planes de tratamiento de riesgo identificados en todos los niveles de la entidad, de tal forma que se asegure su implementación.
Tercera Línea de Defensa	• Le corresponde a las Unidades de Control Interno, realizar evaluación (aseguramiento) independiente sobre la gestión del riesgo en la entidad, catalogándola como una unidad auditable más dentro de su universo de auditoría, y por tanto debe dar a conocer a toda la entidad el Plan Anual de Auditorias basado en riesgos, y los resultados de la evaluación de la gestión del riesgo.

10. TABLA DE FORMATOS

CODIGO	NOMBRE	UBICACION	RESPONSABLE
R-OP-028	Matriz de Riesgos	Intranet	Profesional Universitario Grado 4 Gestión Integral

11. ANEXOS

Anexo 1. DOFA Gestión de Riesgos TMSA 2019

Anexo 2. Plantilla Matriz de Riesgo de Gestión

Anexo 3. Plantilla Matriz de Riesgo de Corrupción

Anexo 4. Matriz de Riesgos Institucionales

Anexo 5. Matriz de Riesgos de Corrupción

Anexo 6. Matrices de Riesgos de Gestión por Proceso

Anexo 7. Matriz de Riesgos Desarrollo Estratégico

Anexo 8. Matriz de Riesgos Gestión de TIC

Anexo 9. Matriz de Riesgos Gestión Grupos de Interés

Anexo 10. Matriz de Riesgos Gestión de Mercadeo

Anexo 11. Matriz de Riesgos Planeación del SITP

Anexo 12. Matriz de Riesgos Supervisión y Control de la Operación del SITP

Anexo 13. Matriz de Riesgos Monitoreo Integral de la Operación SITP

Anexo 14. Matriz de Riesgos P Gestión de Talento Humano

Anexo 15. Matriz de Riesgos Gestión Información Financiera y Contable

Anexo 16. Matriz de Riesgos Gestión Jurídica

Anexo 17. Matriz de Riesgos Adquisición de Bienes y Servicios

Anexo 18. Matriz de Riesgos Gestión de Servicios Logísticos

Anexo 19. Matriz de Riesgos Gestión Económica de los Agentes del Sistema

Anexo 20. Matriz de Riesgos Evaluación y Mejoramiento de la Gestión

Anexo 21. Matriz de Riesgos Gestión de Asuntos Disciplinarios

COPIA NO CONTROLADA