TABLA DE CONTENIDO

1. OBJETIVO 6
2. ALCANCE 6
3. RESPONSABLES 6
4. DOCUMENTOS DE REFERENCIA 7
5. DEFINICIONES 7
6. CONDICIONES GENERALES 12
6.1 Responsabilidades en la Administración del Riesgo 13
6.2 Clasificación del Riesgo 20
7. POLITICA PARA LA GESTIÓN DE LOS RIESGOS EN TRANSMILENIO S.A. 21
7.1 Objetivo 21
7.1.1 Objetivos específicos 21
7.2 Alcance 21
7.3 Principios 22
7.4 Declaración de la política 22
7.5 Metodologías a aplicar para la administración del Riesgo 25
7.6 Nivel de aceptación del riesgo 25
7.7 Niveles para calificar el impacto 26
7.8 Tratamiento de Riesgos 26
7.9 Estrategias para dar cumplimiento a la política 26
7.10 Cultura de gestión de riesgos 27
7.11 Seguimiento al nivel del riesgo residual 27

8. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN 27
8.1 Establecimiento del contexto estratégico 28
8.1.1 Contexto Interno.....28
8.1.2 Contexto Externo 29
8.1.3 Contexto de procesos.....30
8.2 Identificación del riesgo 30
8.3 Análisis del Riesgo 32
8.3.1 Cálculo de la probabilidad.....32
8.3.2 Cálculo del impacto 33
8.4 Evaluación del Riesgo 34
8.4.1 Nivel de riesgo inherente..... 34
8.4.2 Valoración de los controles 35
8.4.2.1 Descripción del control 35
8.4.2.2. Tipos de control.....36
8.4.2.3. Evaluación del diseño del control 37
8.4.3 Nivel del riesgo residual.....38
8.5 Tratamiento del Riesgo..... 39
9. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE CORRUPCION 40
9.1 Establecimiento del contexto estratégico 40
9.2 Identificación de riesgo de corrupción..... 41
9.3 Análisis del riesgo de corrupción 42
9.3.1 Calculo de probabilidad.....42
9.3.2 Cálculo del impacto 43
9.3.3 Nivel de riesgo inherente.....45
9.4 Evaluación del Riesgo 46
9.4.1 Diseño de los controles.....46
9.4.2 Valoración de los controles 48
9.4.2.1 Evaluación del diseño del control 48
9.4.2.2 Análisis de la ejecución del control 50
9.4.2.3 Análisis de la solidez individual del control.....50
9.4.3 Nivel de riesgo (riesgo residual).....52
9.5 Tratamiento del riesgo..... 53
10. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DIGITAL.....55
10.1 Identificación de activos..... 55
10.2 Identificación de riesgos 55
10.3 Valoración de riesgos..... 56

10.4 Evaluación y tratamiento del riesgo 57
11. MONITOREO Y REVISIÓN DE LOS RIESGOS 57
12. COMUNICACIÓN Y CONSULTA 58
13. TABLA DE FORMATOS 59

LISTA DE TABLAS

Tabla 1. Gestión de los tipos de riesgos según líneas de defensa 12
Tabla 2. Estructura para la identificación de riesgos de gestión en TRANSMILENIO S.A. 31
Tabla 3. Escalas de valoración de la probabilidad para los riesgos de gestión 32
Tabla 4. Escalas de valoración del impacto / consecuencia. 33
Tabla 5. Evaluación diseño del control. 37
Tabla 6. Estructura para la descripción de riesgos de corrupción en TRANSMILENIO S.A. 41
Tabla 7. Estructura para la descripción de riesgos de corrupción en TRANSMILENIO S.A. 42
Tabla 8. Escalas de valoración de la probabilidad para los riesgos de corrupción. 43
Tabla 9. Criterios para calificar el Impacto - Riesgos de Corrupción. 44
Tabla 10. Escalas de valoración del impacto para los riesgos de corrupción. 45
Tabla 11. Evaluación diseño del control. 48
Tabla 12. Resultados de la evaluación del diseño del control. 49
Tabla 13. Calificación de la Ejecución del Control 50
Tabla 14. Calificación solidez del control. 51
Tabla 15. Calificación solidez del conjunto de controles. 51
Tabla 16. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos 52
Tabla 17. Escalas de valoración del Impacto / consecuencia para Riesgos de Seguridad Digital 56

LISTA DE GRAFICAS

Gráfica 1. Gestión del Riesgo según las tres Líneas de Defensa 13
Gráfica 2. Etapas a seguir en la metodología de riesgos 28
Gráfica 3. Mapa de Calor Riesgo Inherente 34
Gráfica 4. Activación de los Tipos de Controles en el ciclo de un proceso 36
Gráfica 5. Desplazamiento zona de riesgo acorde con tipo de control 39
Gráfica 6. Estrategias para tratar el riesgo 40
Gráfica 7. Mapa de Calor Riesgo Inherente – Riesgos de Corrupción 45
Gráfica 8. Mapa de calor riesgo residual – Riesgos de Corrupción 53
Gráfica 9. Opciones de Tratamiento del Riesgo de Corrupción 54

MODIFICACIONES:

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

VERSION	FECHA	CAMBIO	SOLICITÓ
		en Diciembre de 2020. Versión 5, se ajusta todo el manual. • Se describen cada una de las metodologías que se aplicaran para la administración de los riesgos de gestión, corrupción y seguridad digital acorde con los lineamientos expedidos por DAFP.	

1. OBJETIVO

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

2. ALCANCE

Este manual aplica para la administración de los riesgos de gestión, corrupción y de seguridad digital, de los procesos definidos en el mapa de procesos institucional.

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

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

3. RESPONSABLES

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

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

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

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

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

4. DOCUMENTOS DE REFERENCIA

- Constitución Política de Colombia.
- **Decreto 371 de 2010:** por el cual se establecen lineamientos para preservar y fortalecer la transparencia y para la prevención de la corrupción en las TRANSMILENIO S.A., y Organismos del Distrito Capital.
- **Ley 1474 de 2011:** por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública.
- **Decreto 2641 de 2012:** por medio del cual se reglamentan los artículos 73 y 76 de la Ley 1474 de 2011, señalando como metodología para diseñar y hacer seguimiento a la estrategia de lucha contra la corrupción y de atención al ciudadano, la contenida en el documento "Estrategias para la Construcción del Plan Anticorrupción y de Atención al Ciudadano".
- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas. Octubre de 2018. Versión 4.
- Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas. Diciembre de 2020. Versión 5.
- Manual Operativo Sistema de Gestión MIPG. Consejo para la Gestión y Desempeño Institucional. Octubre de 2018.
- Manual de Funciones de TRANSMILENIO S.A.
- Norma ISO 31000 Gestión de Riesgos. Directrices. Estándar normativo internacional que proporciona las directrices genéricas sobre la gestión del riesgo.
- Norma ISO 27001 Sistema de Gestión de Seguridad de la Información
- Protocolo para la identificación de conflicto de intereses en TRANSMILENIO S.A.

5. DEFINICIONES

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

Apetito de riesgo: es el nivel de riesgo que la entidad puede aceptar en relación con sus objetivos, el marco legal y las disposiciones de la alta dirección. El apetito de riesgo puede ser diferente para los distintos tipos de riesgos que la entidad debe o desea gestionar.

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

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

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

Apetito al riesgo: 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.

Capacidad de riesgo: es el máximo valor del nivel de riesgo que una entidad puede soportar y a partir del cual la alta dirección considera que no sería posible el logro de los objetivos de la entidad.

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

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 mitiga al riesgo (Procesos, políticas, dispositivos, prácticas u otras acciones).

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

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

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

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

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

Factor de riesgo: 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[1] 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.

[1] Fuente ISO 31000 Gestión del Riesgo - Directrices

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

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

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

Riesgo de corrupción: posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado.

Riesgo de seguridad digital: combinación de amenazas y vulnerabilidades en el entorno digital. Puede debilitar el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Incluye aspectos relacionados con el ambiente físico, digital y las personas.

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 correspondientes medidas de tratamiento.

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

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

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

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.

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

6. CONDICIONES GENERALES

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

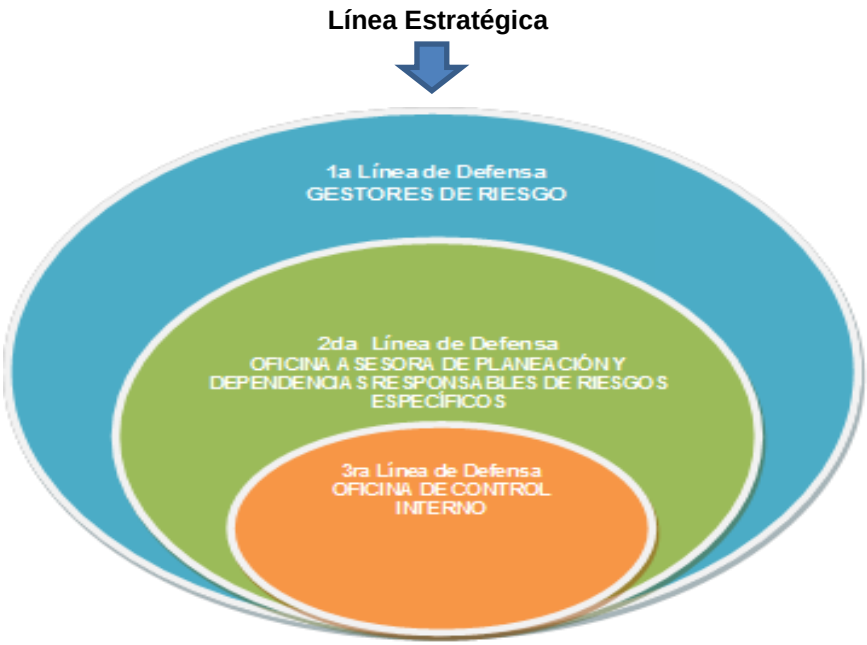
Tabla 1. Tipos de gestión del riesgo por líneas de defensa

TIPOS DE GESTION DEL RIESGO	1RA LINEA DE DEFENSA	2da LINEA DE DEFENSA	3ra LINEA DE DEFENSA
Riesgos Institucionales	Líderes de Proceso	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Gestión	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Corrupción	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Oficina Asesora de Planeación – OAP	Oficina de Control Interno
Riesgos de Seguridad Digital y Tecnológicos	Gestor Líder de Riesgo de cada proceso Gestor equipo operativo Servidores Públicos	Dirección de TIC	Oficina de Control Interno
Riesgos Técnicos	Funcionarios Contratistas Proveedores Concesionarios	Procesos Misionales	Oficina de Control Interno
Riesgos de Contratación	Proveedores y Contratistas	Dirección Corporativa Contratación Subgerencia Jurídica	Oficina de Control Interno
Riesgos Laborales/ Seguridad salud y en el trabajo	Funcionarios de TRANSMILENIO S.A.	Dirección Corporativa Talento Humano	Oficina de Control Interno

Fuente: TRANSMILENIO S.A.

6.1 Responsabilidades en la Administración del Riesgo

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



Gráfica 1. Gestión del Riesgo según las tres Líneas de Defensa

Línea Estratégica:

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

- **Junta Directiva**

La Junta Directiva cuenta con el apoyo del Comité de Coordinación de Control Interno mediante el cual se tomarán las decisiones pertinentes para implementar y mantener en funcionamiento en forma eficiente el Sistema de Administración de Riesgos de la Entidad. Anualmente se deberá presentar a la Junta Directiva, el estado de la Gestión de Riesgo de TRANSMILENIO S.A.

- **Alta Dirección**

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

- **El Representante de la Alta Dirección**

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

- **Comité Institucional de Gestión y Desempeño**

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

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

Es la máxima instancia de toma de decisiones frente a los riesgos críticos y su adecuado tratamiento de tal manera que permita minimizar la probabilidad de ocurrencia y el impacto en caso de que se materialicen.

Por lo menos una vez al año se deberá presentar a este Comité, el informe del estado de la gestión de riesgo de TRANSMILENIO S.A.

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 de Coordinación 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, 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 sobre el perfil de riesgo inherente y residual de la entidad, en las fechas establecidas en el numeral 10.1 de este manual, y de acuerdo con las políticas de tolerancia establecidas y aprobadas.
- Revisar los informes presentados de los eventos de riesgos que se han materializado en la entidad, incluyendo los riesgos de corrupción, así como las causas que dieron su origen, 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 las acciones establecidas 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.

Primera Línea de Defensa:

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

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

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

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

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos pueden generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de sus procesos, para la actualización de la matriz de riesgos de su proceso
- Identificar los riesgos de sus procesos y determinar su probabilidad de ocurrencia y el impacto en caso de llegar a materializarse.
- Identificar los controles con los que cuentan los procesos y evaluarlos de acuerdo con la metodología para la gestión de riesgos definida y aprobada.
- Analizar los riesgos identificados con el fin de establecer el riesgo inherente y el riesgo residual de cada 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.
- 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.
- Establecer e implementar el tratamiento de los riesgos evaluados, determinando los planes de acción y controles necesarios para administrarlos y garantizar que se encuentren dentro de los niveles de aceptación establecidos.
- Actualizar el Mapa de Riesgos de los procesos, cuando lo considere pertinente, teniendo en cuenta lo establecido en este manual.
- Realizar reuniones internas con el fin de tomar decisiones relacionadas con el tratamiento de los riesgos de su proceso, compartiendo los análisis y decisiones tomadas en los comités de Alto nivel, relacionados con la gestión de riesgos.

- **Equipos de trabajo de los procesos**

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

- **Funcionarios y Contratistas**

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

Segunda Línea 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.

Está conformada por la Oficina Asesora de Planeación y a las dependencias que tienen bajo su responsabilidad la implementación de riesgos específicos presentados en la tabla 1 de este documento, por otra parte, son las encargadas de definir el marco conceptual, técnico y metodológico, sobre el cual la primera línea de defensa debe realizar la implementación.

Dentro de sus funciones se encuentra:

- Revisar los cambios en el Direccionamiento Estratégico o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de solicitar y apoyar 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.
- Definir los instrumentos, metodologías y procedimientos tendientes a que TRANSMILENIO S.A., administre efectivamente sus riesgos.
- Desarrollar e implementar el sistema de reportes sobre la administración de riesgos de TRANSMILENIO S.A.
- Realizar el seguimiento a los controles propuestos y planes de tratamientos relacionados con la gestión de riesgos y proponer las actualizaciones y modificaciones correspondientes.
- Coordinar los programas de sensibilización o socialización relacionados con el Sistema de Administración de Riesgos.
- Recopilar la información de cada una de las matrices de riesgo de los procesos y consolidarla para obtener el mapa de riesgos por procesos y el mapa de riesgos institucional y realizar la publicación en la Intranet.
- Presentar informes a la Gerencia General de acuerdo con las solicitudes de la misma.

- 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.

Tercera Línea 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 la cual debe llevar a cabo las siguientes actividades:

- Revisar los cambios en el “Direccionamiento estratégico” o en el entorno y como estos puedan generar nuevos riesgos o modificar los que ya se tienen identificados en cada uno de los procesos, con el fin de que se identifiquen y actualicen las matrices de riesgos por parte de los responsables.
- Revisión de la adecuada definición y desdoblamiento de los objetivos institucionales a los objetivos de los procesos, que han servido de base para llevar a cabo la identificación de los riesgos, y realizar las recomendaciones a que haya lugar.
- Revisar que se hayan identificado los riesgos significativos 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, de igual manera pronunciarse sobre cualquier riesgo que este por fuera del perfil de riesgo de la entidad o que su calificación del impacto o probabilidad del riesgo no es coherente con los resultados de las auditorías realizadas.
- Hacer seguimiento a las actividades de control establecidas para la mitigación de los riesgos de los procesos se encuentren documentadas y actualizadas en los procedimientos y los planes de acción establecidos como resultados de las auditorías realizadas, se realicen de manera oportuna, cerrando las causas raíz del problema, evitando en lo posible la repetición de hallazgos o materialización de riesgos.

- Hacer seguimiento a la gestión de riesgos de corrupción. En este sentido es necesario que en sus procesos de auditoría interna analice las causas, los riesgos de corrupción y la efectividad de los controles incorporados en el mapa de riesgos de corrupción. En especial deberá adelantar las siguientes actividades:

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

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

    Entre las acciones que debe adelantar se encuentran:

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

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

6.2 Clasificación del Riesgo

- ✓ **Riesgos estratégicos:** posibilidad de ocurrencia de eventos que afecten los objetivos estratégicos de la 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, la ejecución y administración de procesos
- ✓ **Riesgos operativos:** posibilidad de ocurrencia de eventos que afecten los procesos misionales de la entidad como la prestación del servicio a la ciudadanía, daños a la flota, a la infraestructura y activos fijos en general de la entidad.
- ✓ **Riesgos financieros:** posibilidad de ocurrencia de eventos que afecten los estados financieros y todas aquellas áreas involucradas con el proceso financiero como presupuesto, tesorería, contabilidad, cartera, central de cuentas, costos, etc.
- ✓ **Riesgos tecnológicos:** posibilidad de ocurrencia de eventos o fallas tecnológicas que afecten la totalidad o parte de la infraestructura tecnológica (hardware, software, redes, etc.) de una entidad.
- ✓ **Riesgos de cumplimiento:** posibilidad de ocurrencia de eventos que afecten la situación jurídica o contractual de la organización debido a su incumplimiento o desacato a la normatividad legal y las obligaciones contractuales, así como las relaciones laborales entre otros.
- ✓ **Riesgos ambientales:** Todos los relacionados con el impacto ambiental en que TRANSMILENIO S.A. puede incurrir en el desarrollo de sus actividades
- ✓ **Riesgo de imagen o reputacional:** posibilidad de ocurrencia de un evento que afecte la imagen, buen nombre o reputación de una organización, ante sus clientes y partes interesadas.
- ✓ **Riesgos de corrupción:** Posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado. Incluye el fraude interno y externo
- ✓ **Riesgos de Seguridad Digital:** posibilidad de ocurrencia de un evento adverso que afecte la confidencialidad, integridad o disponibilidad de la información de TRANSMILENIO S.A.

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

7.1 Objetivo

Generar confianza en los grupos de valor y de interés de TRANSMILENIO S.A. administrando los Riesgos de Gestión, de Corrupción y de Seguridad Digital, que impidan el logro de los objetivos institucionales

7.1.1 Objetivos específicos

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

7.2 Alcance

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

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

7.3 Principios

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

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

7.4 Declaración de la política

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

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

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

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

impidan el logro de sus objetivos y que éstos se encuentren debidamente tratados en cumplimiento de las políticas, procedimientos y metodología del sistema de gestión de riesgo.

- La Oficina Asesora de Planeación, como responsable técnico del sistema, tendrá un rol permanente de facilitador técnico, cuyo equipo orientará y asesorará sobre el cumplimiento de las políticas, procedimientos, metodologías que deben ser acatadas por todos los procesos bajo el liderazgo del **Gestor líder** (Directivo dueño de proceso) y del **Gestor de riesgo** (Enlaces de cada proceso, designados como Gestores de Riesgo por el Gestor Líder)
- El gestor líder designará al gestor de riesgo, que asumirá la suplencia en caso de su ausencia temporal.
- Cuando existan conflictos de interés en el desarrollo de la política y la metodología para la gestión del riesgo en la entidad se deberá aplicar lo contenido en el documento T-DA-002 Protocolo para la identificación de conflicto de intereses en TRANSMILENIO S.A.

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

- Los funcionarios de TRANSMILENIO S.A., están obligados a reportar, los eventos de riesgo de los cuales tengan conocimiento.
- El reporte de eventos de riesgo debe cumplir con el proceso definido para tal fin, haciendo uso del formato definido por parte de la Oficina Asesora de Planeación.
- Los eventos de riesgo, una vez identificados, deben ser reportados por el Gestor de riesgo líder a la Oficina Asesora de Planeación, en el momento que se genere la situación detectada.
- La materialización de los riesgos de seguridad digital deberá iniciar con el proceso de gestión de incidentes de seguridad, ya sea a través del reporte interno en la entidad como el reporte a entidades externas competentes relacionadas con delitos informáticos y ciberseguridad de acuerdo con los lineamientos definidos por la Dirección de TIC.
- Todos los eventos de riesgo relacionados con incidentes de fraude, corrupción o soborno serán reportados por los canales definidos por la entidad en el procedimiento P-SC-001 Atención de Peticiones quejas, reclamos y sugerencias.

7.5 Metodologías a aplicar para la administración del Riesgo

TRANSMILENIO S.A. para los riesgos de gestión, corrupción o seguridad digital, aplicará las metodologías establecidas en este manual para administrar los riesgos, las cuales se describen en los capítulos 8, 9 o 10 según corresponda, donde se incluyen entro otros aspectos los relacionados con:

1. Niveles para calificar la probabilidad y el impacto.
2. Estrategias para combatir o tratar el riesgo
3. Monitoreo y Seguimiento al riesgo residual

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

7.6 Nivel de aceptación del riesgo

- Apetito del Riesgo: La Alta Dirección, define como nivel de aceptación de riesgo residual, la zona denominada con nivel BAJO

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

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

Para los riesgos de corrupción no se admite aceptación del riesgo y siempre se deberán elaborar planes de tratamiento de acuerdo con los lineamientos establecidos por el DAFP.

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

7.7 Niveles para calificar el impacto

Para la calificación del impacto se tendrá en cuenta lo establecido en los numerales 8.3 Análisis de los riesgos de gestión, 9.3 Análisis de los riesgos de corrupción y 10.3 análisis de los riesgos de seguridad digital de este documento.

7.8 Tratamiento de Riesgos

Para el tratamiento de los riesgos se deberá tener en cuenta lo establecido en el numeral 8.5 de este documento

7.9 Estrategias para dar cumplimiento a la política

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

- Designar al Jefe de la Oficina Asesora de Planeación, como representante de la Alta Dirección para el Sistema de Administración de Riesgos.
- Designar como Gestor de Riesgo, al líder de cada uno de los procesos
- Actualizar la política y procedimientos relacionados con la gestión de riesgos.
- Documentar las actividades para el reporte de riesgos.
- Trabajar de manera articulada los riesgos que se generen en la implementación de cada una de las políticas del modelo de gestión en el marco de MIPG
- Actualizar los mapas de riesgos existentes de los procesos definidos en el mapa de procesos institucional cuando se considere pertinente.
- Documentar los riesgos que se han identificado en la operación normal de la Entidad
- Identificar riesgos materializados al interior de la institución.
- Presentar los informes sobre la gestión de riesgos al Comité Institucional de Coordinación de Control Interno y una vez al año a la Junta Directiva por parte del Representante de la Alta Dirección para el Sistema de Administración de Riesgos.
- Diseñar planes de sensibilización y socialización permanente para los servidores públicos de todos los niveles con el objetivo de generar una cultura de prevención de riesgos al interior de la Entidad.

7.10 Cultura de gestión de riesgos

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

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

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

7.11 Seguimiento al nivel del riesgo residual

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

Se realizarán actividades de monitoreo y revisión, de los riesgos de gestión y corrupción cada cuatro meses, de seguridad digital mínimo una vez al año en el marco de la normatividad vigente, por parte de los responsables de cada una de las líneas de defensa.

8. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE GESTIÓN

La metodología descrita a continuación contempla las siguientes etapas requeridas para la administración del riesgo: contexto estratégico, identificación de riesgos, análisis de riesgos, evaluación de riesgos, tratamiento de los riesgos y monitoreo.



Gráfica 2. Etapas a seguir en la metodología de riesgos

8.1 Establecimiento del contexto estratégico

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

8.1.1 Contexto Interno

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

El establecimiento del contexto interno incluye:

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

Entre los factores claves del contexto interno se consideran:

i. Financieros: Presupuesto de funcionamiento, recursos de inversión, infraestructura, capacidad instalada.

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

iii. Procesos: capacidad, diseño, ejecución, proveedores, entradas, salidas, gestión del conocimiento.

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

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

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

8.1.2 Contexto Externo

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

La determinación del contexto externo incluye:

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

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

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

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

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

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

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

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

vii. Articulación interinstitucional: Relación con otras entidades del sector, del gobierno, territoriales, ONGs.

8.1.3 Contexto de procesos

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

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

8.2 Identificación del riesgo

La identificación del riesgo se lleva a cabo determinando las causas con base en el contexto interno, externo y del proceso que pueden afectar el logro de los objetivos institucionales. A partir de este contexto se identifica el riesgo, el cual estará asociado a aquellos eventos o situaciones que pueden entorpecer el normal desarrollo de los objetivos del proceso o los estratégicos.

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

- Las caracterizaciones y procedimientos de cada proceso.
- Los requerimientos realizados a la mesa de ayuda.

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

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

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

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

La identificación del riesgo debe contener todos los detalles que sean necesarios y que sea fácil de entender tanto para el líder del proceso como para personas ajenas al proceso, debe cumplir con la siguiente estructura:

Tabla 2. Estructura para la identificación de riesgos de gestión en TRANSMILENIO S.A.

CONSECUENCIA QUE AFECTA LA ENTIDAD Y SU ENTORNO Impacto	CAUSAS Y FUENTES DE RIESGO	DESCRIPCIÓN DEL RIESGO
Lo que podría generar **(Consecuencia que afecta la entidad y su entorno)**	Por **Causa Inmediata** Debido a… **(Causa raíz)** Ausencia de… Falta de… Insuficiente… Debilidades en…	**Evento que puede ocurrir** y entorpecer el normal desarrollo de las actividades institucionales. Se debe evitar el uso de palabras negativas como “Que no…”, “No tener…” Iniciar con “Posibilidad de…”

Fuente: TRANSMILENIO S.A.

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.

Las metodologías para la identificación de causas pueden ser consultadas en el procedimiento de acciones correctivas, preventivas y de mejora de la Entidad.

8.3 Análisis del Riesgo

Una vez identificados los riesgos siguiendo la estructura definida en el ítem anterior, deben ser calificados en dos aspectos importantes: El primero está relacionado con la probabilidad de materialización o de ocurrencia del riesgo y el segundo en el impacto o la consecuencia que tendría para TRANSMILENIO S.A, con el fin de estimar la zona de riesgo inicial es decir lo que se denomina Riesgo Inherente.

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

8.3.1 Cálculo de la probabilidad

Se entiende como la posibilidad de ocurrencia del riesgo y estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando. De este modo, la probabilidad inherente será el número de veces que se pasa por el punto de riesgo en el periodo de 1 año.

Dependiendo de la frecuencia de una actividad se le aplicará un porcentaje de probabilidad

Teniendo en cuenta lo anterior a continuación se establecen los criterios que se tendrán en cuenta para definir el nivel de probabilidad

Tabla 3. Escalas de valoración de la probabilidad para los riesgos de gestión

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Muy Baja	La actividad que conlleva el riesgo se ejecuta como máximo 2 veces por año	20%
Baja	La actividad que conlleva el riesgo se ejecuta de 3 a 24 veces por año	40%
Media	La actividad que conlleva el riesgo se ejecuta de 24 a 500 veces por año	60%

	FRECUENCIA DE LA ACTIVIDAD	PROBABILIDAD
Alta	La actividad que conlleva el riesgo se ejecuta mínimo 500 veces al año y máximo 5000 veces por año	80%
Muy Alta	La actividad que conlleva el riesgo se ejecuta más de 5000 veces por año	100%

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

8.3.2 Cálculo del impacto

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.

Para la construcción de la tabla de criterios de impacto se definen los impactos económicos y reputacionales como las variables principales. Por lo anterior, TRANSMILENIO ha decidió tomar la siguiente tabla de valoración teniendo en cuenta diferentes escenarios que facilitan la calificación al equipo encargado de valorar el riesgo.

Tabla 4. Escalas de valoración del impacto / consecuencia.

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

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

NOTA: Frente al análisis de probabilidad e impacto se debe utilizar el criterio del líder del proceso y su equipo de trabajo como conocedores del quehacer tanto de su proceso como de la Entidad, los cuales deberán definir cuántas veces se desarrolla la actividad, esto para el nivel de probabilidad. Para determinar el impacto o afectación se deberá definir mediante la tabla establecida que contiene la afectación desde el punto económico y reputacional.

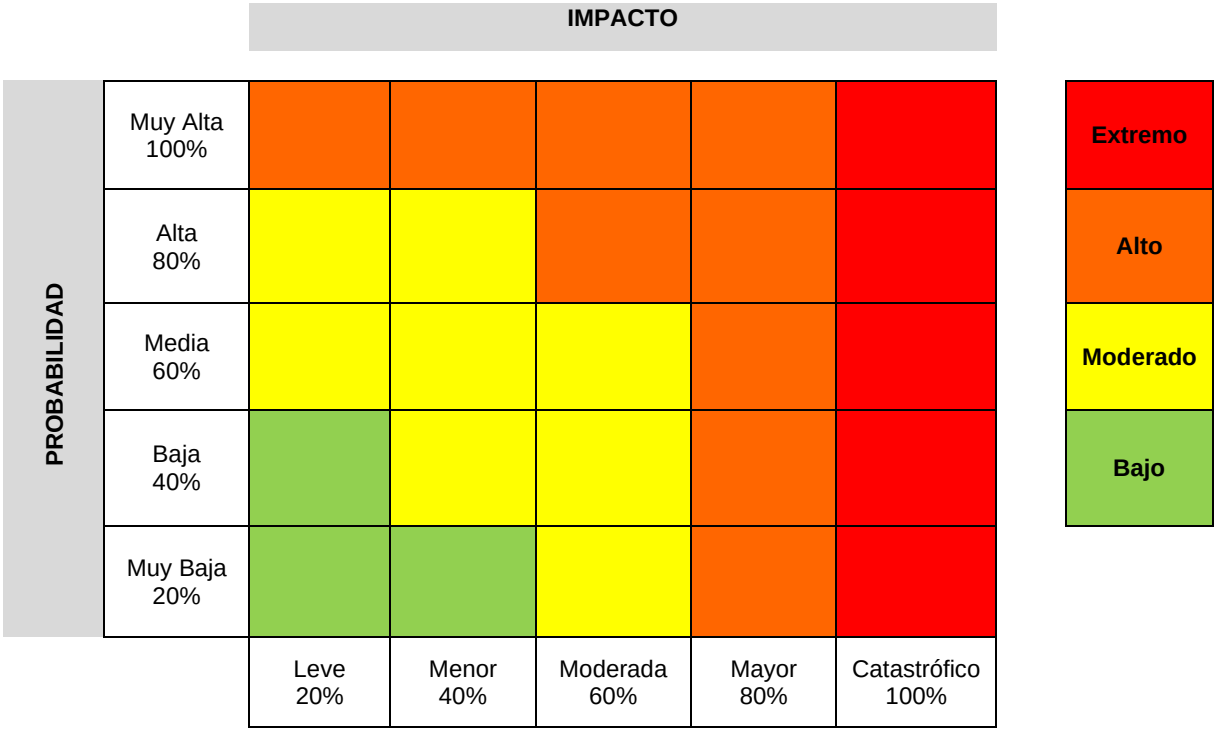
8.4 Evaluación del Riesgo

8.4.1 Nivel de riesgo inherente

A partir del análisis de la probabilidad de ocurrencia del riesgo y sus consecuencias o impactos, se busca determinar la zona de riesgo inicial (RIESGO INHERENTE).

Se trata de determinar los niveles de severidad a través de la combinación entre la probabilidad y el impacto. Se definen 4 zonas de severidad en la matriz de calor.

Gráfica 3. Mapa de Calor Riesgo Inherente



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

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”.

En esta etapa, se busca confrontar los resultados del análisis del riesgo inicial frente a los controles establecidos con el fin de conocer la zona de riesgo final (Riesgo Residual)}

8.4.2 Valoración de los controles

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

- La identificación de controles se debe realizar a cada riesgo a través de las entrevistas con los líderes de procesos o servidores expertos en su quehacer. En este caso sí aplica el criterio experto.
- Los responsables de implementar y monitorear los controles son los líderes de proceso con el apoyo de su equipo de trabajo.
- Cada control debe ser evaluado de acuerdo con los criterios de calificación definidos, para conocer el nivel de riesgo residual y así establecer el tratamiento que se dará a cada riesgo.
- Los controles establecidos deben ser coherentes con lo definido en los planes a los que aporte la Entidad, la normatividad interna y externa aplicable, los procedimientos e instrucciones de trabajo y las políticas de operación o lineamientos determinados para la gestión.
- Al momento de definir las actividades de control por parte de la primera línea de defensa, es importante considerar que los controles estén bien diseñados, es decir, que efectivamente estos mitigan las causas que hacen que el riesgo se materialice.

8.4.2.1 Descripción del control

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

Responsable de ejecutar el control: identificar el cargo específico del servidor responsable de llevar a cabo la actividad de control. En caso de que sean controles automáticos se identificará el sistema que realiza la actividad. Evitar asignar áreas de manera general o nombres de personas.

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

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

8.4.2.2. Tipos de control

Existen tres tipos de controles como se resumen a continuación:

Gráfica 4. Activación de los Tipos de Controles en el ciclo de un proceso



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

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

- ✓ Control manual: controles que son ejecutados por personas.
- ✓ Control automático: son ejecutados por un sistema.

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.

8.4.2.3. Evaluación del diseño del control

A continuación, se analizan los atributos para el diseño del control, teniendo en cuenta características relacionadas con la eficiencia y la formalización.

En la tabla 5 se puede observar la descripción y peso asociados a cada uno:

Tabla 5. Evaluación diseño del control.

Caracteristica			Descripción	Peso
Atributos de eficiencia	Tipo	Preventivo	Va hacia las causas del riesgo, aseguran el resultado final esperado	25%
		Detectivo	Detecta que algo ocurre y devuelve el proceso a los controles preventivos. Se puede generar reprocesos	15%
		Correctivo	Dado que permiten reducir el impacto en la materializaciond el riesgos, tienen un costo en su implemnetacion	10%
	Implementación	Automático	Son actividades de procesamiento o validación de información que se ejecutan por un sistema y/o aplicativo de manera automática sin la intervención de personas para su realización	25%
		Manual	Controles que son ejecutados por una persona, tiene implícito el error humano.	15%
Atributos Informativos (*)	Documentación	Documentado	Controles que están documentados en el proceso, ya sea en manuales, procedimientos, flujogramas o cualquier otro documento propio del proceso.	-
		Sin documentar	Identifica a los controles que pese a que se ejecutan en el proceso no se encuentran documentados en ningún documento propio del proceso.	-
	Frecuencia	Continua	El control se aplica siempre que se realiza la actividad que conlleva el riesgo.	-
		Aleatoria	El control se aplica aleatoriamente a la actividad que conlleva el riesgo	-
	Evidencia	Con registro	El control deja un registro permite evidencia la ejecución del control.	-
		Sin registro	El control no deja registro de la ejecución del control.	-

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

(*) Los atributos informativos solo permiten darle formalidad al control y su fin es el de conocer el entorno del control y complementar el análisis con elementos cualitativos; sin embargo, estos no tienen una incidencia directa en su efectividad.

Una vez se tenga valorado el control con la siguiente formula se establece el riesgo residual

- Cuando hay un solo control para mitigar el riesgo:

Probabilidad Inherente % **X** Valoración Control% = Resultado%
Probabilidad Inherente% **–** Resultado% = Probabilidad Residual %

- Cuando hay dos controles o más para mitigar el riesgo

Probabilidad Inherente % **X** Valoración Control 1% = Resultado 1% Probabilidad Inherente % **–** Resultado 1% = Probabilidad Residual 1%
Probabilidad Residual 1% **X** Valoración Control 2 = Resultado 2% Probabilidad Residual 1% **–** Resultado 2 %= Probabilidad Residual Final %

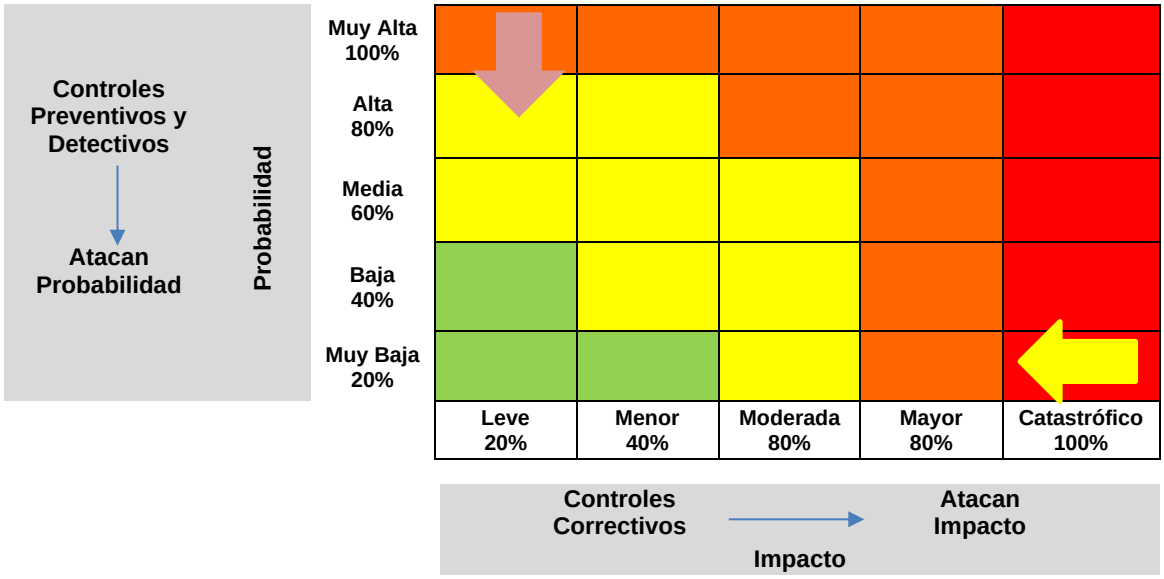
Nota. Cuando hay más de un control se debe tener en cuenta que estos mitigan el riesgo de forma acumulativa, esto quiere decir que una vez se aplica el valor de uno de los controles, el siguiente control se aplicará con el valor resultante luego de la aplicación del primer control.

8.4.3 Nivel del riesgo residual

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

Teniendo en cuenta que es a partir de los controles que se dará el desplazamiento en la matriz de calor que corresponde a la siguiente figura, se muestra cuál es el movimiento en el eje de probabilidad y en el eje de impacto de acuerdo con los tipos de controles.

Gráfica 5. Desplazamiento zona de riesgo acorde con tipo de control



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

El resultado, permite ubicar en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto después de valorar los controles para establecer el plan de tratamiento que se requiera.

8.5 Tratamiento del Riesgo

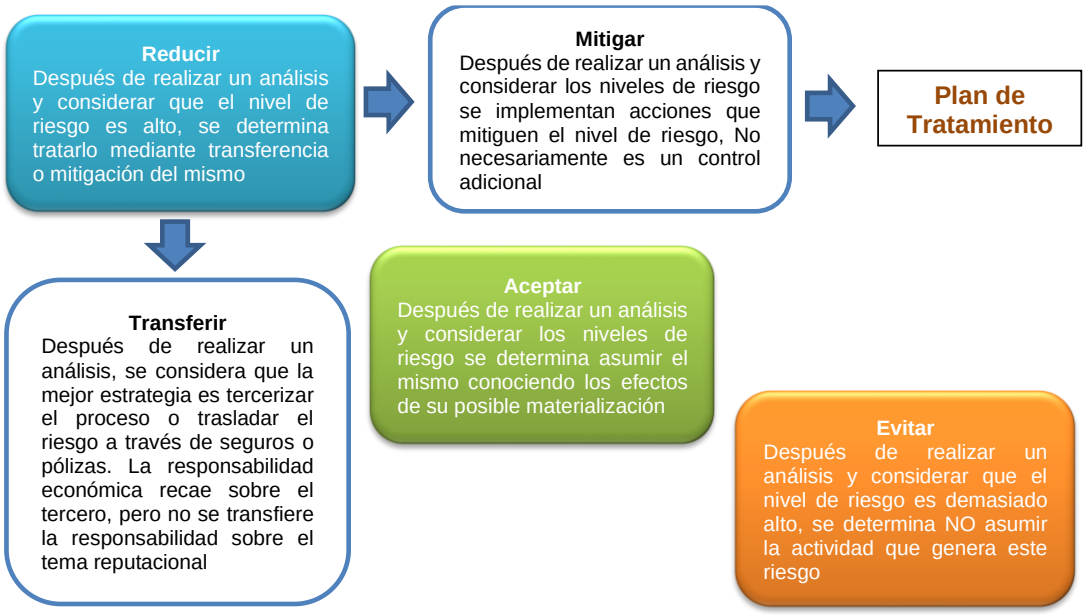
Es la decisión que toma la primera línea de defensa frente a un determinado nivel de riesgo, dicha decisión puede ser aceptar, reducir o evitar.

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

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

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

Gráfica 6. Estrategias para tratar el riesgo



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

De acuerdo con el nivel de riesgo residual obtenido, 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 o moderado se debe adoptar la opción de tratamiento “Aceptar” el riesgo.
- Los riesgos de nivel alto y extremo deben optar por la opción de tratamiento de “Reducir” el riesgo.

Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de tratamiento que especifique: acción, responsable y fecha de implementación.

Nota: el plan de acción acá referido es diferente a un plan de contingencia, el cual se enmarca en el Plan de Continuidad de Negocio y se consideraría un control correctivo.

9. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE CORRUPCION

9.1 Establecimiento del contexto estratégico

Al igual que los riesgos de gestión, para los riesgos de corrupción hay que determinar los parámetros internos y externos que se han de tener en cuenta para la administración de estos riesgos, para esto se tendrán en cuenta los lineamientos dados en el capítulo 8.1 de este manual.

9.2 Identificación de riesgo de corrupción

Para la identificación de los riesgos de corrupción al igual que los de gestión, se determinan las causas fuentes del riesgo y los eventos con base en el análisis de contexto para la entidad y del proceso, que pueden afectar el logro de los objetivos.

Los riesgos de corrupción se establecen sobre procesos.

Ahora bien, teniendo en cuenta que un riesgo de corrupción es la posibilidad de que, por acción u omisión, se use el poder para desviar la gestión de lo público hacia un beneficio privado, es necesario que en su descripción concurran TODOS los componentes de su definición, así:

ACCIÓN U OMISIÓN + USO DEL PODER + DESVIACIÓN DE LA GESTIÓN DE LO PÚBLICO + EL BENEFICIO PRIVADO.

El riesgo debe estar descrito de manera clara y precisa. Su redacción no debe dar lugar a ambigüedades o confusiones con la causa generadora de los mismos.

Con el fin de facilitar la identificación de riesgos de corrupción y evitar que se presenten confusiones entre un riesgo de gestión y uno de corrupción, su identificación debe cumplir con la siguiente estructura:

Tabla 6. Estructura para la descripción de riesgos de corrupción en TRANSMILENIO S.A.

MATRIZ, DEFINICIÓN RIESGO DE CORRUPCIÓN				
Descripción del riesgo	Acción u omisión	Uso del poder	Desviar la gestión de lo público	Beneficio privado
Ejemplo; Direccionamiento indebido de los pronunciamientos de carácter ambiental, por parte de los funcionarios responsables del proceso, para asegurar toma de decisiones que favorezcan un interés personal o de terceros, en detrimento de la entidad.	X	X	X	X

Fuente. Secretaria de Transparencia de la Presidencia de la República

- De acuerdo con la matriz anterior, si se marca con una X cada componente de su definición quiere decir que se trata de un riesgo de corrupción

- Definido el riesgo de corrupción acorde con la estructura anterior, es importante identificar el factor de riesgo (Externo, Interno, Proceso o Información) y las causas o todos aquellos factores internos y externos que solos o en combinación con otros, pueden producir la materialización de un riesgo, así como identificar sus consecuencias.

  A continuación, se ilustra en un ejemplo la forma en que se deben estructura los riesgos de corrupción de TRANSMILENIO S.A.

Tabla 7. Estructura para la descripción de riesgos de corrupción en TRANSMILENIO S.A.

FACTOR DE RIESGO	CAUSAS Y FUENTES DEL RIESGO	NOMBRE DEL RIESGO	DESCRIPCION DEL RIESGO	CONSECUENCIAS
EXTERNO	Intereses particulares o beneficio propio impidiendo que se muestre la gestión real de la Entidad	Manipulación de información de planes, programas y proyectos	Manipulación de la información relacionada con los Proyectos de Inversión, planes, y programas de la Entidad, por parte de funcionarios del proceso con acceso a dicha información, con el fin de favorecer indebidamente a terceros o para beneficio propio, en detrimento de la entidad.	Planes, programas y proyectos inconclusos Pérdida de la imagen institucional Pérdida de confianza en lo público procesos disciplinarios Detrimento patrimonial Perdida de recursos

Fuente: Estructura de Riesgos TRANSMILENIO S.A

9.3 Análisis del riesgo de corrupción

Al igual que los riesgos de gestión, una vez identificados los riesgos de corrupción, en este punto se busca establecer la probabilidad de ocurrencia del riesgo y sus consecuencias o impacto, con el fin de estimar la zona de riesgo inicial (RIESGO INHERENTE).

9.3.1 Calculo de probabilidad

Se analiza qué tan posible es que ocurra el riesgo, se expresa en términos de frecuencia o factibilidad, 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; **factibilidad** implica analizar la presencia de factores internos y externos que pueden propiciar el riesgo, se trata en este caso de un hecho que no se ha presentado, pero es posible que suceda.

Los criterios para la calificación de la probabilidad son:

Tabla 8. Escalas de valoración de la probabilidad para los riesgos de corrupción.

NIVEL	RANGO	DESCRIPCIÓN	FRECUENCIA
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

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

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.

9.3.2 Cálculo del impacto

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.

El impacto se debe analizar y calificar a partir de las consecuencias identificadas en la fase de descripción del riesgo de corrupción

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

Tabla 9. Criterios para calificar el Impacto - Riesgos de Corrupción.

No	Pregunta	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 misión de la entidad?		
4	¿Afectar el cumplimiento de misión de la entidad?		
5	¿Generar pérdida de confianza de la entidad, afectando su reputación?		
6	¿Generar pérdida de recursos económicos?		
7	¿Afectar la generación de los productos o la prestación de servicios?		
8	¿Dar lugar al detrimento de calidad de vida de la comunidad por la pérdida del bien, servicios o 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?		

Fuente: Secretaría de Transparencia de la Presidencia de la República

Responder afirmativamente de una (1) a (5) cinco pregunta(s) genera un impacto moderado.

Responder afirmativamente de seis (6) a once (11) preguntas genera un impacto mayor.

Responder afirmativamente de doce (12) a diecinueve (19) preguntas genera un impacto catastrófico.

IMPORTANTE

Para cada riesgo de corrupción se deben responder las 19 preguntas

Si la respuesta a la pregunta 16 es afirmativa el riesgo se considera catastrofico

De acuerdo con las preguntas anterior los criterios para calificar el impacto en riesgos de corrupción son:

Tabla 10. Escalas de valoración del impacto para los riesgos de corrupción.

NIVEL	RANGO	DESCRIPCIÓN
3	MODERADO	Genera medianas consecuencias sobre la Entidad
4	MAYOR	Genera altas consecuencias sobre la Entidad
5	CATASTROFICO	Genera altas consecuencias sobre la Entidad

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4

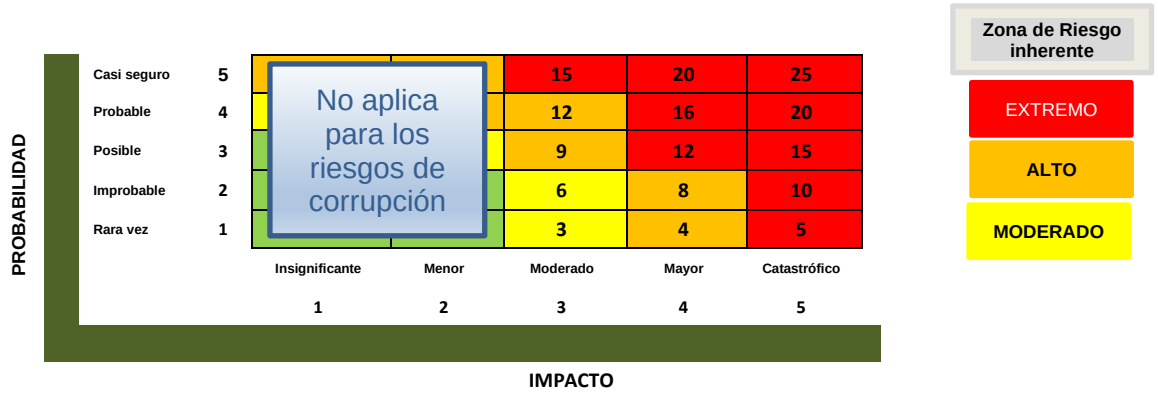
9.3.3 Nivel de riesgo inherente

El nivel de riesgo inherente se obtiene de multiplicar la probabilidad de ocurrencia (tabla 8) por el impacto del riesgo (tabla 10), 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. El producto de los dos proporciona la zona de riesgo inherente, siendo el valor máximo 25 y el mínimo 9 para este tipo de riesgos

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:

Gráfica 7. Mapa de Calor Riesgo Inherente – Riesgos de Corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4

Según los diferentes valores que se pueden obtener, el “nivel de riesgo inherente” para los riesgos de corrupción puede ser: “Extremo”, “Alto” o “Moderado”.

9.4 Evaluación del Riesgo

Para llevar a cabo la evaluación del riesgo, después 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.

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

Para cada causa debe existir un control.

Las causas se deben trabajar de manera separada (no se deben combinar en una misma columna o renglón).

Un control puede ser tan eficiente que contribuya a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.

9.4.1 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 nombre del cargo del servidor responsable de llevar a cabo la actividad de control. El control debe iniciar con un cargo responsable o un sistema o aplicación. Evitar asignar áreas de manera general o nombres de personas. (Ejemplo: Profesional Universitario Grado 04 - Gestión Integral. Profesional Especializado Grado 06- Gestion Ambiental, estos nombres deben estar acordes con el manual de funciones vigente de la Entidad)

- **Paso 2:** Debe tener una periodicidad definida para su ejecución. Todos los controles deben tener una periodicidad específica. Si queda a criterio la periodicidad de la realización del control, tendríamos un problema en el diseño del control. (Ejemplo, una vez al mes, cada seis meses)

- **Paso 3:** Debe indicar cuál es el propósito del control. El control debe tener un propósito (verificar, validar, cotejar, comparar, revisar, etc.) para mitigar la causa de la materialización del riesgo.

- **Paso 4:** Debe establecer el cómo se realiza la actividad de control. El control debe indicar el cómo se realiza, de tal forma que se pueda evaluar si la fuente u origen de la información que sirve para ejecutar el control es confiable para la mitigación del riesgo. Cuando estemos evaluando el control debemos preguntarnos si la fuente de información utilizada es confiable.
- **Paso 5:** Debe indicar qué pasa con las observaciones o desviaciones resultantes de ejecutar el control. Si el responsable de ejecutar el control no realiza ninguna actividad de seguimiento a las observaciones o desviaciones, o la actividad continúa a pesar de indicar esas observaciones o desviaciones, el control tendría problemas en su diseño.

- **Paso 6:** Debe dejar evidencia de la ejecución del control.

    - Para cada causa debe existir un control
    - Las causas se deben trabajar de manera separada
    - Un control puede ser tan eficiente que puede ayudar a mitigar varias causas, en esos casos se debe repetir el control asociándolo a la causa que mitiga

La descripción del control debe incluir que actividad de control se lleva a cabo (Revisar, verificar, supervisar, cotejar, entre otros).

Ejemplo:
Cada vez que se emite una autorización para el uso de un espacio de publicidad o un contrato de espacios en el Sistema, el Profesional Especializado Grado 06 Negocios Colaterales o el Profesional Universitario Grado 03 Gestión de Negocios actualizan una base de datos que contiene la información relacionada con los espacios arrendados por publicidad del sistema o los datos del contrato , dicha información se da a conocer al personal contratista que se encuentre en vía para que verifique los sitios, las cantidades de avisos, maquinas o equipos según el objeto del contrato dejando evidencia registro fotográfico de dicha verificación. En caso de novedades se reportan de inmediato al Profesional Especializado Grado 06 o Profesional Universitario Grado 3 Gestión de Negocios para que el contratista

tome las acciones pertinentes y se cobren los valores adicionales o los incumplimientos a que haya lugar según el caso.

9.4.2 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.

9.4.2.1 Evaluación del diseño del control

Se han considerado las siguientes preguntas para el análisis y evaluación del diseño del control de acuerdo con seis (6) variables establecidas

En la herramienta dispuesta para la gestión del riesgo se debe marcar con una X los aspectos que se cumplen en el diseño del control:

Tabla 11. Evaluación diseño del control.

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA Y PESO EN LA EVALUACIÓN	
1. Responsable	¿Existe un responsable asignado a la ejecución del control? Es el cargo que ejecuta directamente el control	Asignado 15	No asignado 0
	¿El responsable tiene la autoridad y adecuada segregación de funciones en la ejecución del control? Será el dueño del proceso el responsable de su ejecución	Adecuado 15	Inadecuado 0
2. Periodicidad	¿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? Periodicidad con la que se aplica el control (ejemplo: diario, semanal, mensual, cuando se requiera, etc.)	Oportuna 15	Inoportuna 0

CRITERIO DE EVALUACIÓN	ASPECTO A EVALUAR EN EL DISEÑO DEL CONTROL	OPCIONES DE RESPUESTA Y PESO EN LA EVALUACIÓN	
3. Propósito	¿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.?	Prevenir 15 Detectar 10	No es un control 0
4. Cómo se realiza la actividad de control	¿La fuente de información que se utiliza en el desarrollo del control es información confiable que permita mitigar el riesgo?	Confiable 15	No confiable 0
5. Qué pasa con las observaciones o desviaciones	¿Las observaciones, desviaciones o diferencias identificadas como resultados de la ejecución del control son investigadas y resueltas de manera oportuna?	Se investigan y resuelven Oportunamente 15	No se investigan y resuelven oportunamente. 0
6. Evidencia de la ejecución del control	¿Se deja evidencia o rastro de la ejecución del control que permita a cualquier tercero con la evidencia llegar a la misma conclusión?	Completa 10	Incompleta 5 No existe 0

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4.

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 evalúe como bien diseñado.

Tabla 12. Resultados de la evaluación del diseño del control.

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

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.

9.4.2.2 Análisis de la ejecución del control

Aunque un control esté 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 asegurarse por parte de la primera línea de defensa que el control se ejecute.

Para determinar la ejecución del control el responsable del proceso debe confirmar como se lleva a cabo este control de la siguiente manera:

Tabla 13. Calificación de la Ejecución del Control

RANGO DE CALIFICACIÓN DE LA EJECUCIÓN	RESULTADO PESO DE EJECUCIÓN DEL CONTROL
Fuerte	El control **SIEMPRE** 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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4.

9.4.2.3 Análisis de la solidez individual del control

La calificación de probabilidad e impacto se realiza al riesgo, este riesgo puede tener varias causas y a su vez varios controles. Por lo tanto, es importante primero evaluar la solidez de cada uno de los controles y después el conjunto de controles asociados al riesgo.

En la evaluación del diseño y ejecución de los controles las dos variables (Diseño y Ejecución) son importantes y significativas en el tratamiento de los riesgos y sus causas.

La calificación de la solidez de cada control se obtiene dependiendo de los resultados obtenidos en el **diseño** de cada control y el peso de la **ejecución** de cada control. Se escoge la calificación entre fuerte, moderado y débil, tal como se detalla en la siguiente tabla:

Tabla 14. Calificación solidez del control.

PESO DEL DISEÑO DE CADA CONTROL ** Tabla No 12	PESO DE LA EJECUCIÓN DE CADA CONTROL ** Tabla No 13	SOLIDEZ INDIVIDUAL DE CADA CONTROL FUERTE: 100 MODERADO: 50 DÉBIL: 0	SE DEBEN ESTABLECER ACCIONES PARA FORTALECER EL CONTROL SÍ /NO
Fuerte: Calificación entre 96 y 100	Fuerte (siempre se ejecuta)	Fuerte + Fuerte = Fuerte	No
	Moderado (algunas veces)	Fuerte + Moderado = Moderado	Sí
	Débil (no se ejecuta)	Fuerte + Débil = Débil	Sí
Moderado: Calificación entre 86 y 95	Fuerte (siempre se ejecuta)	Moderado + Fuerte = Moderado	Sí
	Moderado (algunas veces)	Moderado + Moderado = Moderado	Sí
	Débil (no se ejecuta)	Moderado + Débil = Débil	Sí
Débil: Calificación entre 0 y 85	Fuerte (siempre se ejecuta)	Débil + Fuerte = Débil	Sí
	Moderado (algunas veces)	Débil + Moderado = Débil	Sí
	Débil (no se ejecuta)	Débil + Débil = Débil	Sí

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4.

La solidez del conjunto de controles se obtiene calculando el promedio de la solidez individual de los controles por cada riesgo

Tabla 15. Calificación solidez del conjunto de controles.

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.

Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas. Octubre de 2018, Versión 4.

9.4.3 Nivel de riesgo (riesgo residual)

Es el resultado que se obtiene después de hacer el desplazamiento de la calificación de probabilidad e impacto del riesgo inherente como producto de la calificación de los controles. El cálculo del riesgo residual se realizará de acuerdo con la siguiente tabla. Tratándose de riesgos de corrupción únicamente hay disminución de probabilidad. Es decir, para el impacto no opera el desplazamiento.

Tabla 16. Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos

Solidez del conjunto de los controles	Controles que 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	No aplica para riesgos de corrupción
Fuerte	Directamente	Indirectamente	2	
Fuerte	Directamente	No disminuye	2	
Fuerte	No disminuye	Directamente	0	
Moderado	Directamente	Directamente	1	
Moderado	Directamente	Indirectamente	1	
Moderado	Directamente	No disminuye	1	
Moderado	No disminuye	Directamente	0	

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 probabilidad

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

El resultado, permite ubicar en el mapa de calor el punto de intersección resultante de la probabilidad y el impacto después de controles para establecer el plan de tratamiento que se requiera. En los riesgos de corrupción solo se podrá hacer desplazamiento en probabilidad y no existen impactos insignificantes ni menores.

Gráfica 8. Mapa de calor riesgo residual – Riesgos de Corrupción

PROBABILIDAD	IMPACTO				
	Insignificante	Menor	Moderado	Mayor	Catastrófico
	1	2	3	4	5
Casi seguro 5			Reducir el riesgo Evitar el riesgo Compartir o Transferir	20 Reducir el riesgo Evitar el riesgo Compartir o Transferir	25 Reducir el riesgo Evitar el riesgo Compartir o Transferir
Probable 4			12 Reducir el riesgo Evitar el riesgo Compartir o Transferir	16 Reducir el riesgo Evitar el riesgo Compartir o Transferir	20 Reducir el riesgo Evitar el riesgo Compartir o Transferir
Posible 3			9 Reducir el riesgo Evitar el riesgo Compartir o Transferir	Reducir el riesgo Evitar el riesgo Compartir o Transferir	15 Reducir el riesgo Evitar el riesgo Compartir o Transferir
Improbable 2			6 Asumir el riesgo Reducir el riesgo	8 Reducir el riesgo Evitar el riesgo Compartir o Transferir	10 Reducir el riesgo Evitar el riesgo Compartir o Transferir
Rara vez 1			3 Asumir el riesgo Reducir el riesgo	4 Reducir el riesgo Evitar el riesgo Compartir o Transferir	5 Reducir el riesgo Evitar el riesgo Compartir o Transferir

No aplica para los riesgos de corrupción

9.5 Tratamiento del riesgo

El tratamiento del riesgo es la respuesta establecida por la primera línea de defensa para la mitigación de los riesgos.

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, por lo anterior todos los riesgos de corrupción sin excepción deben tener plan de tratamiento.

9. Opciones de Tratamiento del Riesgo de Corrupción



Fuente: Guía para la administración del riesgo y el diseño de controles en entidades públicas, Octubre de 2018, Versión 4.

a. Aceptar el riesgo: el nivel de riesgo cumple con los criterios de aceptación de riesgo no es necesario poner controles y este puede ser aceptado. La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo. ESTA OPCION DE TRATAMIENTO NO APLICA PARA LOS RIESGOS DE CORRUPCIÓN

b. Reducir el Riesgo: El nivel de riesgo debería ser administrado mediante el establecimiento de controles, de modo que el riesgo residual se pueda reevaluar como algo aceptable para la entidad. Estos controles disminuyen normalmente la probabilidad y/o el impacto del riesgo. Se deben seleccionar controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

c. Compartir o transferir el riesgo**:** Cuando es muy difícil para la entidad reducir el riesgo a un nivel aceptable o se carece de conocimientos necesarios para gestionarlo, este puede ser compartido con otra parte interesada que pueda gestionarlo con más eficacia. Cabe señalar que normalmente no es posible transferir la responsabilidad del riesgo. Los dos principales métodos

de compartir o transferir parte del riesgo son: seguros y tercerización. Estos mecanismos de transferencia de riesgos deberían estar formalizados a través de un acuerdo contractual.

d. Evitar el Riesgo: Cuando los escenarios de riesgo identificado se consideran demasiado extremos se puede tomar una decisión para evitar el riesgo, mediante la cancelación de una actividad o un conjunto de actividades. Puede ser una decisión simple, la menos arriesgada y costosa, pero es un obstáculo para el desarrollo de las actividades de la entidad y, por lo tanto, hay situaciones donde no es una opción.

Si se requiere plan de tratamiento se debe describir la acción que se implementará, asignando un responsable, la fecha inicio, y la fecha vencimiento, debe señalar la evidencia que soporta la acción y el indicador que medirá la eficacia o efectividad de las acciones de tratamiento propuestas.

10. METODOLOGÍA PARA LA ADMINISTRACIÓN DEL RIESGO DE SEGURIDAD DIGITAL

10.1 Identificación de activos

La identificación de los activos se tendrá en cuenta para realizar el proceso de identificación y valoración de riesgos de seguridad digital. Esto dado que los riesgos se identificarán teniendo en cuenta los activos críticos. Por lo anterior, el proceso de identificación, valoración y clasificación de activos de información se llevará a cabo siguiendo los lineamientos del instructivo I-DT-001 Instructivo de identificación, valoración y clasificación de activos de información.

10.2 Identificación de riesgos

La identificación de riesgos se realiza teniendo en cuenta la afectación de los tres (3) atributos o propiedades de la información: Confidencialidad, Integridad y Disponibilidad. Por lo anterior, los siguientes riesgos serán definidos como mínimos:

- Pérdida de confidencialidad
- Pérdida de integridad
- Pérdida de disponibilidad

Los riesgos se identificarán sobre cada uno de los procesos y teniendo en cuenta los respectivos activos críticos de cada proceso con el fin de detectar las situaciones de riesgos, amenazas y/o vulnerabilidades que pueden ser explotadas para comprometer la información. Por lo anterior, para identificar los riesgos sobre los activos se tendrán en cuenta los variables como:

- Activos críticos (o grupos de activos) donde se identificará el riesgo
- Amenazas
- Causas / Vulnerabilidades
- Consecuencias

Es importante esclarecer que los riesgos mencionados no necesariamente son los únicos identificables, también podrán identificarse riesgos relacionados con incumplimiento normativo o conocimiento, entre otros, que se relacionan indirectamente con la afectación de las propiedades de la información.

10.3 Valoración de riesgos

Para realizar la valoración de riesgos de seguridad digital, se manejarán los criterios de probabilidad y riesgo que son usados en la valoración de los riesgos de gestión. Estos criterios: probabilidad y riesgo se especifican en el numeral 8.3 Análisis de riesgo de este documento. Sin embargo, los criterios de impacto que se manejan específicamente para los riesgos de seguridad digital son los siguientes:

Tabla 17. Escalas de valoración del Impacto / consecuencia para Riesgos de Seguridad Digital

	Afectación Económica	Afectación Reputacional	Afectación Poblacional
Leve 20%	Afectación menor a 10 SMLMV Afectación ≥1% del presupuesto anual de la entidad.	El riesgo afecta la imagen de algún área de la organización.	Afectación ≥5%
Menor 40%	Entre 10 y 50 SMLMV Afectación ≥5% del presupuesto anual de la entidad.	El riesgo afecta la imagen de la entidad internamente, de conocimiento general nivel interno, de junta directiva y accionistas y/o proveedores	Afectación ≥10%
Moderada 60%	Entre 50 y 100 SMLMV Afectación ≥20% del presupuesto anual de la entidad	El riesgo afecta la imagen de la entidad con algunos usuarios, de relevancia frente al logro de los objetivos	Afectación ≥40%
Mayor 80%	Entre 100 y 500 SMLMV Afectación 35% del presupuesto anual de la entidad.	El riesgo afecta la imagen de la entidad con efecto publicitario sostenido a nivel del sector administrativo, nivel departamental o municipal	Afectación ≥70%
Catastrófica 100%	Mayor a 500 SMLMV Afectación ≥50% del presupuesto anual de la entidad.	El riesgo afecta la imagen de la entidad a nivel nacional con efecto publicitario sostenido a nivel país	Afectación ≥90%

10.4 Evaluación y tratamiento del riesgo

Posterior a la valoración del riesgo inherente se deberán evaluar los controles que se han implementado actualmente para mitigar dichos riesgos. Para el caso de los riesgos de Seguridad Digital los controles que se utilizarán como mínimo para su mitigación, serán aquellos indicados en el Anexo A de la norma ISO/IEC 27001:2013.

Por otro lado, sean cualquiera los controles utilizados o definidos para mitigar los riesgos, estos deberán documentarse y evaluarse en su diseño, según lo definido para los riesgos de gestión. Así mismo, para el tratamiento de riesgos se deberán seguir los lineamientos especificados para los riesgos de gestión.

Estos lineamientos y criterios están especificados en el numeral 8.4 Evaluación del riesgo y 8.5 Tratamiento del Riesgo

11. MONITOREO Y REVISIÓN DE LOS RIESGOS

Teniendo en cuenta que ningún riesgo se mantiene estático, puesto que el negocio es dinámico, se debe realizar un monitoreo y revisión constante tanto a los riesgos identificados, así como su valoración y planes de tratamiento.

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

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

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). 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, es responsabilidad del líder proceso actualizar su matriz de riesgos y remitir la información a la Oficina Asesora de Planeación.

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.

Se realizarán actividades de monitoreo y revisión de los riesgos de gestión y de corrupción cada cuatro meses, de seguridad digital mínimo una vez al año por parte de los responsables de cada una de las líneas de defensa.

Para los riesgos de corrupción el seguimiento por parte de la segunda y tercera línea de defensa se realizará de acuerdo con la normatividad así:

- ***Primer seguimiento:*** Con corte al 30 de abril. En esa medida, la publicación por parte de la OCI deberá surtirse dentro de los diez (10) primeros días del mes de mayo.
- ***Segundo seguimiento:*** Con corte al 31 de Agosto. La publicación por parte de la OCI deberá surtirse dentro de los diez (10) primeros días del mes de septiembre.
- ***Tercer seguimiento:*** Con corte al 31 de diciembre. La publicación por parte de la OCI deberá surtirse dentro de los diez (10) primeros días del mes de enero.

El Jefe de la Oficina de Control Interno o quien haga sus veces, debe adelantar seguimiento a los mapas de riesgo, verificando la efectividad de los controles.

El informe de seguimiento a los riesgos de corrupción, adelantado por la Oficina de Control Interno se debe publicar en la página web de la Entidad en el link de transparencia.

12. COMUNICACIÓN Y CONSULTA

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

Para los riesgos de corrupción, y como parte de los ejercicios de participación ciudadana en la formulación de planes de la Entidad, la Oficina Asesora de planeación gestionara con al Subgerencia de Atención al Usuario y Comunicaciones la publicación en la página web de la Entidad, en el link de Transparencia, el proyecto de Plan Anticorrupción y Atención al Ciudadano que se defina para cada vigencia, por lo menos 10 días antes de finalizar el mes de enero de cada año, lo anterior con el fin de recibir observaciones de la ciudadanía y grupos de valor y realizar los ajustes que se consideren pertinentes para poder publicar formalmente el PAAC el 31 de enero, en cumplimiento de la normatividad legal vigente.

El Representante de la Alta Dirección para el Sistema de Administración de Riesgos debe identificar las necesidades de capacitación relacionadas con la gestión de riesgos y presentarlo a la Dirección Corporativa, para su respectiva aprobación. De igual manera, como parte de la gestión interna en temas relacionados con el sistema de Administración de riesgos de la Entidad, la Oficina Asesora de Planeación llevara a cabo las siguientes actividades:

- Capacitaciones y/o sensibilizaciones periódicas.
- Publicaciones periódicas en materia de riesgos a través de la Intranet de la Entidad y/o página web de TRANSMILENIO S.A.
- Publicación de los mapas de riesgo por proceso en la herramienta dispuesta por la Entidad para consulta de todos los servidores públicos.

13. TABLA DE FORMATOS

CODIGO	NOMBRE	UBICACION	RESPONSABLE
R-OP-031	Reporte de eventos	Intranet	Profesional Universitario Grado 4 Gestión Integral
N.A	Matriz de Riesgos	Herramienta dispuesta por la Entidad	Profesional Universitario Grado 4 Gestión Integral