N° INFORME: OCI-2021-053

PROCESO / ACTIVIDAD REALIZADA:

Desarrollo Estratégico Consultoría al Sistema de Gestión del Riesgo

EQUIPO AUDITOR:

Nohra Lucia Forero Cespedes (Contratista)

OBJETIVO(S):

Mediante informe de Consultoría, evaluar la actualización normativa interna relacionada con la Gestión de Riesgos, con base en los criterios establecidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 de diciembre 2020, identificando oportunidades de mejoramiento que permitan agregar valor a la gestión de riesgos, control y gobierno de la Entidad.

ALCANCE:

La consultoría contempla la revisión del borrador de la última actualización del Manual de Gestión del riesgo elaborado por la Oficina Asesora de Planeación, verificando que cuente con lineamientos definidos por el Departamento Administrativo de la Función Pública en la guía para la administración del riesgo y el diseño de controles en entidades Públicas versión 5, en los siguientes aspectos: Política Administración de Riesgos, Identificación de Riesgos, Valoración de Riesgos e Información, Comunicación y Consulta.

CRITERIOS:

1. Manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 5 de agosto de 2021, Incluye Política de Gestión de Riesgos, (Borrador en actualización)
2. Manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 4 de agosto de 2020, Incluye Política de Gestión de Riesgos.
3. Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre 2018.

4. Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 diciembre 2020.
5. Guía de auditoría interna basada en riesgos para entidades públicas versión 4 de julio de 2020.
6. Acuerdo No.007 de 2017 Por el cual se modifica la estructura organizacional y las funciones de unas dependencias de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A.
7. Directiva 001 de la Secretaría General y Secretaría Jurídica Distrital del 3 de marzo de 2021.

FORTALEZAS:

1. El personal de la Oficina Asesora de Planeación, designado por el representante de la Alta Dirección demostró amabilidad, diligencia y disposición frente a los requerimientos del profesional de la Oficina de Control Interno asignado, así como para la concertación de reuniones, acorde con los tiempos disponibles.
2. La actualización adelantada al Manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 5 de agosto de 2020 (Borrador en actualización), tomó como insumo las recomendaciones del Informe OCI-2020-051 Consultoría en la implementación y/o actualización del Sistema de Gestión del Riesgo, realizado por la Oficina de Control Interno.
3. El plan de trabajo establecido para la actualización del manual de riesgos se ha cumplido de acuerdo lo programado.

DESCRIPCIÓN DEL TRABAJO REALIZADO

De conformidad con el Plan Anual de Actividades de la Oficina de Control Interno de la Entidad correspondiente al año 2021, se adelantó una consultoría a los criterios internos normativos para la Gestión del Riesgos de TRANSMILENIO S.A, para lo cual se realizó lo siguiente:

Revisión del Manual M-OP-002 para la Gestión del Riesgo en TRANSMILENIO S.A. Versión 5 (Borrador en actualización):

Condiciones generales del Manual

La Oficina de Control Interno realizó la revisión del Manual M-OP-002 para la Gestión del Riesgo en TRANSMILENIO S.A. Versión 5 (Borrador en actualización), donde se comparó que en éste se relacionaran los aspectos descritos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020, así como los cambios que se presentaron en relación con el Manual M-OP-002 en su versión 4, presentando los siguientes resultados:

• **Objetivo (Manual):** Se observó que en el manual se establece el objetivo, pero se debe verificar la redacción de la última frase, "*etapas se encuentran comprendidas dentro del Sistema de Administración de Riesgos de la Entidad*."

• **Alcance (Manual):** En comparación con el manual versión 4, esta nueva versión (borrador) resalta que los riesgos de Seguridad de la Información se encuentran enmarcados dentro del alcance del Sistema de Gestión de Seguridad de la Información (SGSI).

Sin embargo, se considera necesario utilizar los mismos términos en los diferentes Sistemas de Gestión de la entidad para generar de esta forma homogeneidad, lo anterior se presenta porque se observó que el manual en su versión 5 (Borrador) se utiliza el término de Seguridad Digital, pero en el SGSI se utiliza Seguridad de la información.

• **Responsables (Manual)**: En comparación con la versión 4 del manual, en la versión 5 (borrador) se evidenció que se establecen responsabilidades para la Dirección de TIC en lo referente a la definición y actualización de los criterios para los riesgos de Seguridad de la Información.

• **Documentos de Referencia**: Se utilizó la normativa vigente aplicable en materia de riesgos para entidades públicas del Departamento Administrativo de la Función Pública, sin embargo, su nombre debe corregirse pues quedó nombrado de forma diferente. Desde la competencia de la tercera línea defensa en materia de auditorías sería importante incluir la Guía de auditoría

interna basada en riesgos para entidades públicas Versión 4 Julio de 2020, la cual contiene lineamientos en materia del ejercicio de auditorías basadas en riesgos.

• **Definiciones**: Se evidencian los mismos términos establecidos desde el manual versión 4.

• **Condiciones Generales:** Se evidenció un esquema de administración del riesgo por categoría de riesgos y su responsable por línea defensa, así como las responsabilidades de cada una de ellas.

• **Responsabilidades en la administración del riesgo**: Se establecen funciones por cada una de las líneas de defensa, a los comités y áreas que tienen responsabilidades en la administración y gestión de los riesgos de la institución, también se observó que incorporan a la Dirección de TIC, a la Dirección corporativa, a Contratación, a la subgerencia jurídica y Talento humano asociándolas de acuerdo con el tipo de riesgo que cada una tiene a cargo.

No obstante lo anterior, la descripción de cada una de las responsabilidades podría ajustarse su redacción, iniciando por la actividad que cada uno debe cumplir.

• **Clasificación del riesgo:** Se evidenció que, en este título se establecen las tipologías de los riesgos y no la clasificación del riesgo descrita en el manual de la función pública en su versión 5.

Política para la Gestión del Riesgo en TRANSMILENIO S.A:

Aunque se observó que se establecen diferentes políticas para la gestión de los riesgos, no se están plasmando políticas referentes a la Directiva 1 de la Secretaria General y Jurídica Distrital de marzo de 2021, en los temas relacionados con:

Existencia de inhabilidades, incompatibilidades o conflicto de intereses, el registro de denuncias por posibles actos de corrupción, existencia de inhabilidades, incompatibilidades o conflicto de intereses elevadas por la ciudadanía a través de los diferentes canales de atención, el seguimiento a las denuncias por posibles actos de corrupción, y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses elevadas por la ciudadanía a través del Sistema Distrital para la Gestión de Peticiones Ciudadanas y Protección de identidad del denunciante.

También se considera pertinente reforzar las políticas referentes a los riesgos de fraude.

• **Objetivo de la Política:** Se observó que el Objetivo se establece de acuerdo con lo descrito en la Guía del DAFP.

• **Alcance de la Política:** En el alcance de la política no se describe cómo se gestionan los riesgos de Seguridad de la Información, pues estos son gestionados de acuerdo con la política de seguridad de la información.

• **Principios:** En el manual se establecen principios que rigen la gestión de riesgos en TRANSMILENIO S.A.

• **Declaración de la Política:** Fue incluida en el numeral 7.4. Declaración de la Política del Manual M-OP-002 Versión 5 (Borrador en actualización), la cual se describe de igual forma que en la versión 4 del manual, siendo coherente con los lineamientos y sugerencias de la (NTC ISO31000 Numeral 2.4). “Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo La gestión o administración del riesgo establece lineamientos precisos acerca del tratamiento, manejo y seguimiento a los riesgos”.

Esta declaración se estructuró en las siguientes políticas:

> **Políticas relativas a la Administración del Riesgo:** Aunque se observa que cumple con los pasos definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP Versión 5 diciembre 2020, se considera importante fortalecer las políticas referentes al riesgo de fraude, Lo anterior, en razón a que los riesgos de corrupción en su definición difieren de los riesgos de fraude, por tanto, no es posible asimilar que corrupción es sinónimo de fraude.
>
> También se considera pertinente establecer políticas enfocadas en la Directiva 001 de la Secretaría General y Secretaría Jurídica Distrital del 3 de marzo de 2021.
>
> **Políticas Relativas al Reporte de Eventos de Riesgo:** En estas políticas se establece que “*El reporte de eventos de riesgo debe cumplir con el proceso definido para tal fin, haciendo uso de la herramienta definida, guías, instructivos y entrenamiento por parte de la Oficina Asesora de Planeación.”*, pero se observó que en los documentos del proceso que no se encuentra el “Anexo 2. Denominado Guía para el reporte de eventos de Riesgo”, que contenía el ABC para realizar el reporte de los riesgos (corrupción, gestión

y seguridad de la información) que se puedan llegar a materializar en los diferentes procesos, en el momento de la consultoría éste no se encontraba publicado, pero si se observó el “Anexo 3. Formato reporte de evento de riesgos”.

Este último contiene los siguientes ítems: “Descripción del Evento de Riesgo, Información del proceso, tipo de riesgo, Riesgo Materializado, Causa originadora, controles vulnerados, plan de acción correctivo, nombre del líder que lo reporta y nombre del receptor por la Oficina asesora de Planeación”, y el que permite efectuar el reporte, por lo tanto se considera necesario que se nombren los anexos que se han elaborado para permitir que quien va a ejecutar alguna actividad tenga claro con qué herramientas cuenta.

Políticas relativas a los Riesgos de Interrupción: En comparación con el manual Versión 4, esta versión 5 (borrador en actualización) no contiene este título, no obstante, la Entidad dio inicio al proceso de continuidad de negocio, por lo cual se debe evaluar la armonización de los tipos de riesgo.

• **Metodología para la Gestión del Riesgo:** La Oficina de Control Interno evidenció que las actividades descritas para el contexto Interno, Externo y de procesos, cumplen con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP Versión 5 diciembre 2020.

• **Nivel de aceptación del riesgo:** El numeral 7.6. Nivel de aceptación del riesgo del Manual M-OP-002 Versión 5 (Borrador en actualización) no presenta cambios en su redacción de acuerdo con lo descrito en la versión 4 del manual, sin embargo, se considera necesario que quede explicito en este punto, qué acciones tomar en el caso en que después de controles el riesgo se posiciona en Zona de Riesgo Residual alta o extremo, ya que de acuerdo a como se realice la valoración de los riesgos éstos podrían no reducir su impacto, quedando en riesgos residual alto y extremo. También se debe describir específicamente cuál es el apetito, la tolerancia y la capacidad del riesgo, de acuerdo con lo establecido en la guía del DAFP versión 5, en el numeral 1.2 Marco conceptual para el apetito de riesgo.

• **Niveles para calificar el impacto**: En el manual M-OP-002 Versión 5 (Borrador en actualización), mediante los numerales 8.3 “Análisis de los riesgos de Gestión”, en las tablas 3

Escala de valoración de la probabilidad para los riesgos de gestión y la tabla 4 Escala de valoración del impacto / consecuencia, el numeral 9.3 " Análisis de los riesgos de Corrupción", en las tablas 8, 9 y 10 y el numeral 10.3 "Valoración del Riesgos" en la tabla 17, se amplió el paso a paso registrado y más adelante se evalúa cada una de ellas.

• **Tratamiento del Riesgo**: Fueron incorporadas las actividades obligatorias definidas por el DAFP para el tratamiento de riesgos de gestión, corrupción y seguridad de la información, lo cual se puede evidenciar a través de los numerales 8.5, 9.5 Tratamiento del riesgo y 10.4 Evaluación y tratamiento del riesgo contenida en el manual M-OP-002 Versión 5 (Borrador en actualización).

• **Estrategias para dar cumplimiento a la política:** Se observó que se establecen estrategias para cumplir con la gestión de los riesgos para evitar la materialización de estos, sin embargo, sería importante incluir una, que se enfoque en capacitar a los responsables en la identificación de los riesgos y en la creación de controles para que éstos ayuden a la no materialización de los riesgos.

• **Cultura de gestión de riesgos**: Esta actividad se mantiene igual con relación al manual versión 4, cumple con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 5 (Borrador en actualización).

• Seguimiento al nivel de riesgo Residual: Fue incluida la periodicidad cuatrimestral para los riesgos de gestión y de corrupción y anual para los riesgos de seguridad de la información, dentro de la Política de Gestión del riesgo de TRANSMILENIO S.A, contenida en el manual M-OP-002 versión 5 (Borrador en actualización).

Metodología para la administración del riesgo de gestión:

En este punto se mantienen los mismos seis (6) pasos que se establecieron en la versión 4, para gestionar los riesgos en la entidad, se podría nombrar y describir en el paso 2 "identificación del riesgo" de acuerdo como se establece en la guía del DAFP.

• Establecimiento del contexto estratégico: Se mantiene la estructura de establecer el contexto estratégico teniendo en cuenta el contexto interno, externo y de los procesos, cumpliendo de esta manera con los establecido en la guía del DAFP.

• **Identificación del riesgo:** Esta actividad se encuentra desarrollada dentro del manual versión 5 (Borrador en actualización), sin embargo, podría ampliarse un poco en su descripción de acuerdo con lo establecido por el DAFP, teniendo en cuenta también la identificación de los puntos de riesgos y las fuentes generadoras de riesgos para cada uno de los procesos. Lo anterior a fin de que los líderes de procesos tengan claridad sobre las actividades a realizar en el momento de la identificación de riesgos y evitar así reprocesos.

• **Análisis del Riesgo**: Cumple con los lineamientos del DAFP, efectuando la actualización de la nueva metodología para determinar la probabilidad y el impacto para los riesgos de gestión, en este punto se especifica que con la nueva metodología los riesgos de gestión se valoran de manera cuantitativa y que los de corrupción de manera cualitativa, sin embargo, se considera oportuno establecer ejemplos para facilitar la aplicación de las metodologías establecidas para el correspondiente cálculo.

• **Cálculo de Probabilidad:** Se observó que para los riesgos de gestión se establece la nueva metodología del DAFP donde la probabilidad se calcula de acuerdo con número de veces que se ejecuta la actividad durante el año, para la cual se considera se deben establecer criterios que permitan ajustar la frecuencia de acuerdo con el número de veces que las actividades se ejecutan en la entidad.

• **Cálculo de Impacto:** Se observó que para los riesgos de gestión se establece la nueva metodología donde el impacto se calcula de acuerdo con la afectación económica que se puede llegar a presentar y o la afectación reputacional. En el tercer párrafo se debe revisar la redacción. También se debe especificar cómo vamos a reducir el impacto, teniendo en cuenta que no se tienen controles correctivos que son, según la guía del DAFP en su versión 5, los que aplicarían para disminuir el mismo.

• **Evaluación del Riesgo**: Esta actividad cumple con los lineamientos del DAFP, sin embargo, se debe aclarar el porcentaje en los mapas de calor del nivel de riesgo moderado. Toda vez que en los mismos se presenta el error que en nivel moderado se tiene 80% y de acuerdo con la metodología del Manual debería ser el 60%.

• **Valoración de los Controles**: Esta actividad cumple con los lineamientos del numeral 3.2.2.3 Análisis y evaluación de los controles – diseño de controles de la Guía para la administración

del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 diciembre 2020, para los riesgos de gestión y para los riesgos de corrupción de acuerdo con lo establecido en el Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre 2018.

> **Descripción del Control:** Se observó en la versión 5 en borrador del manual se aplica la descripción, sin embargo, se podrían incluir ejemplos para dar mayor claridad a quien deba redactar el control.
>
> **Tipos del Control:** Se evidenció que se establecen los tipos de controles que se describen en la guía del DAFP.
>
> **Evaluación del diseño del Control:** En esta se presentan la calificación que se le da a cada uno de los tipos de los controles lo que ayudará a disminuir la probabilidad y el impacto, describiendo también la fórmula a utilizar para observar esta reducción, en este punto se considera importante incluir ejemplos y ampliar la explicación en qué caso se aplica la fórmula para la probabilidad y el impacto.

• **Nivel de riesgo residual**: Se observó que se especifica cómo debe quedar la ubicación del riesgo, se considera pertinente se efectúe una revisión a los porcentajes dados en el mapa de calor, teniendo en cuenta que el nivel moderado presenta un porcentaje de 80% igual que el mayor.

• **Tratamiento del riesgo**: Se establece para los riesgos de gestión las estrategias para tratar el riesgo y se indican las acciones que se deben ejecutar para el tratamiento de los mismos, se debe revisar la redacción de este punto teniendo en cuenta que indican "*(…) Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la Alta Dirección, se deberá volver a analizar y revisar dicha estrategia. (…)*" y más adelante consideran que *"(…) Los riesgos de nivel alto 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 acción o plan de tratamiento (…)*"

• **Herramientas para la Gestión del Riesgos**: En el manual Versión 5 (borrador), no se describen las herramientas para la gestión del riesgo por lo tanto no se tiene en cuenta dentro

del manual dónde se debe extraer la información para evidenciar el número de eventos que se presenta y tampoco cómo se mediría el desempeño del control, ni se tienen en cuenta los indicadores clave de riesgo, de acuerdo con lo establece la guía del DAFP en su versión 5.

Metodología para la Administración del Riesgo de Corrupción:

Para esta parte del manual, se observó que se mantiene la estructura propuesta en la versión 4 de la Guía para la administración del riesgo y el diseño de controles en entidades públicas, de acuerdo con lo establecida en la versión 5 de la misma.

• **Establecimiento del contexto estratégico:** Se mantiene de la misma forma como se establecen los riesgos de gestión.

• **Identificación de riesgo de corrupción:** En éste, se establece cómo se deben describir los riesgos y se presenta una matriz con un ejemplo y relacionan los puntos que se deben tener presentes en la identificación de los mismos.

• **Análisis del riesgo de corrupción**: En este punto se establece cómo se debe hacer el análisis manteniendo la misma estructura que en el manual anterior donde la probabilidad y el impacto se consideran de forma cualitativa. Por otro lado, se debería tener en cuenta lo relacionado con el l lavado de activos y la financiación del terrorismo.

• **Nivel de Riesgo Inherente:** Este punto se mantiene igual que la versión 4 de la Guía del DAFP.

• **Evaluación del Riesgo:** Se mantiene de la misma forma que en la versión 4 de la Guía de DAFP, sin embargo, se debe revisar la redacción para dejar la descripción en tercera persona.

• **Diseño de Controles:** Se mantienen los 6 pasos establecidos en la versión anterior de la guía del DAFP, (se adjunta el manual con ajustes en algunas palabras).

• **Valoración de controles:** Al igual que los puntos anteriores, se mantiene su valoración de acuerdo con lo establecido en la Versión 4 de la Guía del DAFP.

• **Nivel de riesgo (riesgo residual):** Este numeral no se encuentra dentro del Índice del manual, pero si se describe dentro de la misma, sin presentar observaciones.

• **Tratamiento del riesgo:** Se mantiene de la misma forma que la establecida en el manual versión 4.

Metodología para la Administración del Riesgo de Seguridad Digital:

Sobre la metodología para la gestión de los riesgos de seguridad digital, se incorpora en el manual en su versión 5 borrador, donde ese efectúa una descripción general y remite a los instructivos, manuales que tiene diseñados la Dirección de TIC.

• **Identificación de Activos:** Se describe que se debe seguir con los lineamientos del instructivo I-DT-001 Instructivo de identificación, valoración y clasificación de activos de información.

• **Identificación de Riesgos:** este punto se describe de acuerdo con lo establecido en la guía del DAFP versión 5.

• **Valoración de los riesgos:** Para este caso para el cálculo de la probabilidad se observa que se establece de la misma forma que para los riesgos de gestión de acuerdo con lo establecido en la guía versión 5 del DAFP, para el cálculo del impacto se modifica y se tiene en cuenta por la afectación económica, reputacional.

• **Evaluación y tratamiento del riesgo**: Se establece que los controles que se utilizarán serán como mínimo los indicado es en el Anexo A de la norma ISO/IEC 27001:2013, también hace referencia que se seguirán los lineamientos de los numerales 8.4 Evaluación del riesgo y 8.5 Tratamiento del Riesgo.

• **Monitoreo y revisión de los riesgos**: Cumple con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 diciembre de 2020, en cuanto a definir el marco general para la gestión del riesgo y el control y supervisar su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno, se deben tener en cuenta en este punto las funciones establecidas en el numeral 3.5 monitoreo y revisión de la guía del DAFP versión 5.

• **Comunicación y Consulta**: Cumple con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5 diciembre de 2020, en

cuanto a La comunicación y consulta con las partes involucradas, tanto internas como externas, y durante diferentes etapas del proceso específicamente para los riesgos de corrupción.

CONCLUSIONES Y RECOMENDACIONES GENERALES

1. Definir en el numeral 5. Definiciones, los riesgos de seguridad de la información, a fin de facilitar su despliegue, monitoreo y evaluación.
2. Evaluar la incorporación de políticas relacionadas con:

    - Acciones que se deben adelantar cuando se presenta la materialización de un riesgo de acuerdo con la persona que lo detecta y a la línea de defensa a la que pertenece. Lo anterior teniendo en cuenta que, aunque se describe que, “Los funcionarios de TRANSMILENIO S.A., están obligados a reportar, los eventos de riesgo de los cuales tengan conocimiento.”, no se especifica qué debe hacer la segunda y la tercera línea de defensa en caso de detectar una materialización de un riesgo en sus seguimientos.
    - Acciones que se deben ejecutar cuando dependiendo del impacto del riesgo, uno de éstos se materialice y donde se establezca que hay riesgos que no se pueden materializar por el impacto que representan para la entidad.
    - Establecer como política para TRANSMILENIO S.A, la No tolerancia con la corrupción y el fraude, al igual que políticas enfocadas hacia la gestión, y tratamiento de riesgos de fraude, ya que no se están implementando en el desarrollo del manual.
    - Fortalecer las políticas existentes en la Entidad, enfocándolas a la aplicación de la Directiva 1 de la Secretaria General y Jurídica Distrital de marzo de 2021, por medio de la cual se definen directrices para la gestión y atención de denuncias por posibles actos de corrupción y/o existencia de inhabilidades, incompatibilidades o conflicto de intereses y protección de identidad del denunciante, si bien se cuenta con medidas adoptadas en la entidad al respecto, falta fortalecer lo relacionado con los numerales 4 *protección de identidad del denunciante* y 4.1 *medidas de protección adicionales*.
    - Incluir como política, que mínimo una vez al año se debe efectuar actualización de la matriz de riesgos.

- Dar continuidad con la implementación que se está desplegando y que ha sido liderada por la oficina Asesora de Planeación, a fin de contar con un plan de continuidad del negocio, más aún cuando se han presentado eventos que han afectado la operación y la liquidez de la entidad.

- Por otro lado, en el párrafo que describe "*El reporte de eventos de riesgo debe cumplir con el proceso definido para tal fin, haciendo uso de la herramienta definida, guías, instructivos y entrenamiento por parte de la Oficina Asesora de Planeación*", mencionar el formato por medio del cual se debe realizar el reporte de eventos de riesgos que corresponde al M-OP-002 Anexo 3. Lo anterior en razón a que el Manual de gestión (versión 5 borrador) no se menciona tal formato y resulta necesario que los usuarios conozcan cuál es y cómo aplicarlo.

3. Delimitar en el Alcance los riesgos de seguridad de la información en el numeral 7.2, toda vez que lo debe contener, de acuerdo con lo descrito en el paso 1 de la Guía para la administración del riesgo y el diseño de los controles en entidades públicas versión 5.

4. Describir en el numeral 7.6 Nivel de Aceptación del Riesgo, cuál es el apetito la tolerancia y la capacidad del riesgo, de acuerdo con lo establecido en la guía del DAFP versión 5, en el numeral 1.2 Marco conceptual para el apetito de riesgo.

   También establecer qué acciones tomar, cuando después de aplicar los controles, el riesgo residual queda en una zona superior a la aceptada por la Alta Dirección o si esto no puede suceder dejarlo específico dentro del párrafo. "*La Alta Dirección, define como nivel de aceptación de riesgo residual, la zona denominada como MODERADA para los riesgos de gestión*.".

5. Establecer en la metodología para la administración de riesgos de gestión los puntos que se presentan a continuación de acuerdo con lo descrito en la Guía del DAFP en su versión 5.

   - Incluir en la descripción de la etapa II. Identificación del riesgo, de la Gráfica 2 lo siguiente:

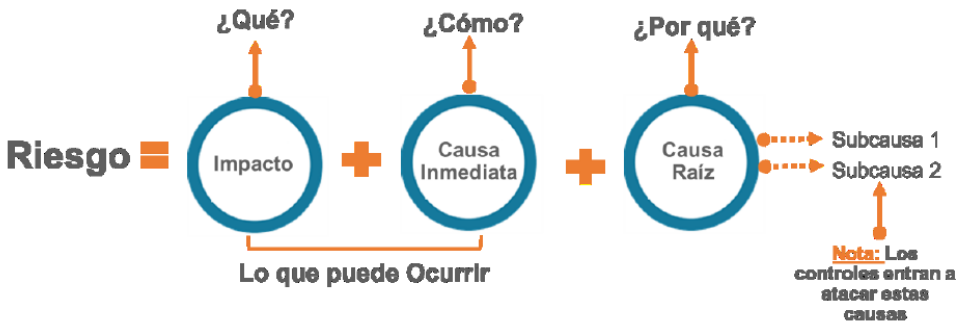
     La identificación de los puntos de riesgos

Identificación de las áreas de impacto

Identificación de áreas de factores de riesgos

- En el numeral 8.1 identificación del riesgo, tener en cuenta los factores naturales.
- Incluir dentro del numeral 8.1.2 Contexto externo en relación con partes interesadas a los concesionarios, lo anterior teniendo en cuenta la importancia que tienen para la entidad y las actividades que éstos desarrollan.
- Incluir dentro del numeral 8.2 identificación del riesgo, que la información a evaluar son las evidencias o indicios que tiene el proceso que puedan ocurrir eventos, así como las bases de datos o información documentada donde se evidencien las veces que se ejecuta la actividad, también que se deben tener los reportes de los incidentes.
- Incluir la Figura 2. Estructura propuesta para la redacción del riesgo de la Guía de DAFP versión 5, como ejemplo para una adecuada descripción del Riesgo.

Figura 2. Estructura propuesta para la redacción del riesgo



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

- Describir dentro de la metodología que se deben detectar los riesgos que se podrían presentar por actividades en cada una de las etapas del proceso, lo cual soporta también la necesidad de ampliar la identificación del riesgo de acuerdo con lo

establecido en el paso dos (2) de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 5.

- En el numeral 8.3 Análisis del Riesgo especificar que, para la evaluación de la probabilidad, ahora es cuantitativa para los riesgos de gestión y cualitativa para los riesgos de corrupción.
- Incluir en el numeral 8.3 Análisis del riesgo, una breve explicación sobre el por qué se considera más propicio para TRANSMILENIO seleccionar la afectación económica en SMMLV y con esos intervalos y evaluar los criterios que se utilizan para el análisis del riesgo tanto en su probabilidad como en el impacto, teniendo en cuenta el presupuesto o los activos que maneja la entidad y cada proceso y el número máximo de veces que se puede ejecutar una actividad y aclarar cómo cada dependencia debe realizar la calificación de sus riesgos.

A continuación, se presenta en valores la tabla de afectación económica en salarios mínimos.

Tabla 2: Afectación económica en salarios mínimos legales vigentes y en pesos

	Afectación Económica
Leve 20%	Afectación menor a 10 SMLMV. $8,778,030
Menor 40%	Entre 10 y 50 SMLMV $8,778,030 y $43,890,150
Moderado 60%	Entre 50 y 100 SMLMV $43,890,150 y $87,780,300
Mayor 80%	Entre 100 y 500 SMLMV $87,780,300 y $438,901,500
Catastrófico 100%	Mayor a 500 SMLMV $438,901,500

Fuente: propia Oficina de Control Interno

De acuerdo con la tabla anterior, se observa que las escalas son muy pequeñas si se considera el presupuesto o los activos de la entidad, por tal razón se recomienda evaluar la escala y ajustar a la realidad de la entidad y de los procesos, toda vez que se podrían ubicar la mayoría de los riesgos en las escalas más altas.

- Con relación a este punto la Oficina de Control interno, realizó una simulación donde se tomó el riesgo “Cumplimiento del Plan Anual de Actividades de la Oficina de Control Interno en un porcentaje inferior al 90%”. Se efectuaron dos sensibilizaciones calificándolos por la afectación económica y con la afectación reputacional, dando como resultado que los controles que la oficina de control interno tiene establecidos solo permiten disminuir la probabilidad, toda vez que los controles correctivos aplicarían solamente para la materialización del riesgo.
- Incluir un ejemplo para poder evidenciar cómo se calcula con los valores y como queda ubicado, a fin de facilitar la comprensión de los responsables de la aplicación, tanto para cuando se debe calcular, teniendo en cuenta la probabilidad, como cuando se debe hacer teniendo en cuenta el impacto.
- Fortalecer la implementación de controles automáticos, lo anterior, teniendo en cuenta que el peso de tener implementado controles automáticos es del 25% lo que permite disminuir la calificación de la probabilidad y el impacto para el riesgo residual.
- Aclarar en el numeral 8.5 Tratamiento del Riesgo cuando se debe implementar un plan de tratamiento para los riesgos de gestión, lo anterior teniendo en cuenta que el párrafo “Pero en caso de que una respuesta ante el riesgo derive en un riesgo residual que supere los niveles aceptables para la Alta Dirección, se deberá volver a analizar y revisar dicha estrategia”, no es claro si se realizaran o no planes de tratamiento para aquellos riesgos cuyos controles no se consigue disminuir su calificación inherente a moderado en su calificación residual, ya que en un párrafo siguiente se menciona “Para efectos del mapa de riesgos, cuando se define la opción de reducir, se requerirá la definición de un plan de acción o plan de tratamiento que especifique: i) responsable, ii) fecha de implementación, y iii) fecha de seguimiento.”.

6. Incluir un numeral donde se mencionen las herramientas que se usan para la gestión y la administración de riesgos como, tal y como se presenta en el numeral 3.4 “Herramientas para le gestión del riesgo” de la guía del DAFP (Versión 5), las herramientas que menciona la guía son, que como producto de la aplicación de la metodología se contará con mapas de riesgos, la gestión de eventos y los indicadores clave de riesgo.

También es importante tener en cuenta que para la gestión de los eventos (riesgos materializados) se deben considerar incidentes que generan o podrían generar pérdidas a la entidad, que como se ha descrito en puntos anteriores se debe contar con bases históricas que permita revisar el riesgo y lo que sucede con los controles y así medir el desempeño de los mismos.

Para los indicadores clave de riesgo, se debe contar con datos históricos que reflejen una mayor o menor disposición a determinados riesgos, que podrán servir como insumo para realizar análisis adicionales.

Lo anterior a fin de facilitar al responsable su implementación y medición en el día a días de los controles ya que esto no se encuentra establecido en el manual en su versión 5 (borrador).

7. Ampliar el análisis de los riesgos de corrupción, teniendo en cuenta lo referente al lavado de activos y financiación del terrorismo.
8. Actualizar el Anexo 1. DOFA Gestión de Riesgos TMSA, porque aunque se cumple con los requisitos mínimos para realizar el ejercicio y su estructura, la fecha de actualización es de 2018, y ameritaría una revisión y/o actualización dado que no incluye el “Acuerdo 07 de 03 de septiembre de 2019 Por el cual se actualiza el Plan Estratégico de TRANSMILENIO S.A., adoptado con Acuerdo de Junta Directiva 4 de 2015", o los cambios del actual plan de desarrollo de la Administración Distrital y otros aspectos relacionados con las metas de movilidad.
9. Incluir una nota en el numeral 11. Monitoreo y Revisión de los Riesgos de corrupción, sobre el tiempo de entrega de los soportes para el monitoreo y seguimiento que debe efectuar la Oficina de Control interno, con el fin de prevenir el riesgo de incumplir con las fechas previstas para su publicación en la página WEB de TRANSMILENIO
10. Fortalecer en el numeral 12. Comunicación y Consulta, en relación con capacitar a los responsables de los riesgos en cada uno de los procesos en lo relacionado a la identificación, monitoreo y control de los riesgos, teniendo en cuenta que son ellos los que tienen el conocimiento de las actividades que ejecutan, los controles de cada una de ellas y

son los que determinan qué riesgos pueden afectar a sus procesos en el cumplimiento de los objetivos.

- Establecer buenas prácticas que permitan hacer un seguimiento a los eventos que se presentan y las actividades que se adelantan para que no se presenten nuevamente y tener en cuenta qué hacen otros procesos que les permiten tener una ejecución adecuada en el manejo de los riesgos, que permita un desempeño mejor como entidad.

11. Evaluar los siguientes comentarios sobre el contenido del manual

- En el numeral 1. **Objetivo** del Manual, Cambiar la redacción del último párrafo de la siguiente manera: “Las etapas para la gestión de los riesgos se encuentran comprendidas dentro del Sistema de Administración de riesgos de la entidad”, lo anterior con el fin de evitar confusiones dado que el borrador en su redacción presenta lo siguiente: “*…Etapas se encuentran comprendidas dentro del sistema de administración de riesgos de la Entidad”.*

- En el numeral 2. **Alcance del Manual, u**nificar la utilización de los mismos términos relacionados con seguridad digital y seguridad de la información, que se mencionan el M-DT-001 (Política de seguridad y privacidad de la Información) y en el M-DO-002 (Manual para la gestión del riesgo versión 5 en borrador), generando así concordancia entre los dos manuales, a fin de evitar confusiones en el despliegue de su implementación y facilitar la gestión de monitoreo y evaluación.

  Es importante resaltar que, el significado Seguridad Digital se enfoca en la seguridad de la información solo en formato digital y la Seguridad de la Información en cualquier formato en que este se encuentre, por otro lado, al verificar el Manual de Políticas de Seguridad y Privacidad de la Información - M-DT-001 no se menciona el término Seguridad Digital y sí el de Seguridad de la Información, durante la revisión efectuada al manual M-OP-002 versión 5 (Borrador en actualización) se observó que se están utilizando los dos términos.

  Por otro lado, se recomienda que en el alcance sea más claro y específico, teniendo en cuenta que se contradice para los riesgos de Seguridad de la Información (Seguridad

Digital) ya que en primer párrafo se indica que aplica para todos los procesos definidos en el mapa de procesos y en el segundo es de acuerdo con el Sistema de Gestión de Seguridad de la Información (SGSI).

- En el numeral 4. **Documentos de Referencia**, registrar correctamente el nombre de la Guía del DAFP. El nombre actual es: Guía para la administración del riesgo y el diseño de controles en entidades púbicas. No Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital y el Diseño de Controles en Entidades Públicas. Diciembre de 2020. Versión 5.

  De igual forma para la versión 4, Guía para la administración del riesgo y el diseño de controles en entidades públicas (RIESGOS DE GESTIÓN, CORRUPCIÓN Y SEGURIDAD DIGITAL)

- En el numeral 5. **Responsabilidades en la Administración del riesgo**, se recomienda modificar y/o ajustar la redacción de las responsabilidades de la Junta Directiva, Alta Dirección y, representante de la Alta Dirección a fin de dar mayor claridad a cada uno de los roles y promover la mejora de la gestión, tal y como se presenta a continuación:

  Junta Directiva, M-DO-002 versión 5 (Borrador): Se presentará anualmente a la Junta Directiva, el estado de la Gestión de Riesgo de TRANSMILENIO S.A. de igual manera, con el apoyo del Comité de Coordinación de Control Interno se tomarán las decisiones pertinentes para implementar y mantener en funcionamiento en forma eficiente del Sistema de Administración de Riesgos.

  Propuesta Oficina de Control Interno: Tomar las decisiones pertinentes para implementar y mantener en funcionamiento en forma eficiente el Sistema de Administración de Riesgos con el apoyo del Comité de Coordinación de Control Interno, teniendo en cuenta el estado de la Gestión de Riesgo de TRANSMILENIO S.A. que se presenta anualmente a la Junta Directiva.

  Para la Alta Dirección, M-DO-002 versión 5 (Borrador): 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.

Propuesta Oficina de Control Interno: Establecer los lineamientos en materia de riesgo, es importante resaltar que en el caso de TRANSMILENIO S.A. es el representante Legal el primer responsable de la gestión del riesgo de la entidad

El Representante de la Alta Dirección, M-DO-002 versión 5 (Borrador): 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.

Propuesta Oficina de Control Interno: El representante de la alta dirección, será el líder de la administración de los riesgos, por lo tanto, es 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 ésta al interior de la entidad. En TRANSMILENIO A.S. el Jefe de la Oficina Asesora de Planeación es el representante de la Alta Dirección.

- En el numeral 7.7 **Niveles para calificar el impacto**, ajustar el nombre del numeral 10.3 Valoración del riesgo en el manual para la gestión del riesgo M-DO-002 versión 5 (borrador), dado que se definió así: “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”.
- En el numeral 8.3.2 **Cálculo del Impacto**, cambiar la redacción del párrafo “*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*.”, por ha decidido o decidió.
- En los **mapas de calor**, verificar el porcentaje dado a la calificación moderada debido a que presenta un porcentaje del 80%.

- En el numeral 8.4.1 **Nivel de Riesgo Inherente**, borrar el corchete “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)}”
- En el numeral 8.4.2.1 Descripción del control, verificar la redacción del párrafo “*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.*” Lo anterior teniendo en cuenta que se repite “cómo se realiza”.
- En la Tabla 5. Evaluación diseño del control, en el numeral 8.4.2.3. Evaluación del diseño del control, verificar la palabra “*caracteristicas (sic)*”, “solo *(sic)*”, “implementacion *(sic)*” y “*materializaciond el riesgos (sic)*”.
- En el numeral 9.3.2 Calculo del Impacto, verificar la palabra “*catastrofico (sic)*”.
- En el numeral 9.4 Evaluación del Riesgo, dejar en tercera persona el párrafo que dice “*Un control puede ser tan eficiente que me ayude a mitigar varias causas, en estos casos se repite el control, asociado de manera independiente a la causa específica.*”
- En el numeral 9.4.1 Diseño de los Controles, verificar la palabra “*Gestion (sic)*”, así como revisar la redacción del párrafo “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.”, teniendo en cuenta que se repite “cómo se realiza”.
- Actualizar el nombre del numeral 10. Metodología para la administración del riesgo de seguridad digital, de acuerdo con lo establecido en la política de la seguridad de la información. A fin de evitar confusiones y reprocesos toda vez, que como se mencionó anteriormente en el Manual de Gestión del Riesgo M-DIO-002 se indica: riesgos de

seguridad digital y en el Manual de Políticas de Seguridad de la Información se indica riesgos de seguridad de la información.

Durante la presente consultoría, se realizaron reuniones a fin de aclarar las dudas generadas con ocasión de la información suministrada a la Oficina de Control Interno y el 29 de septiembre de 2021 se realizó socialización de resultados del presente informe, con los responsables de la información por parte de la Oficina Asesora de Planeación.

Cualquier aclaración adicional, con gusto será suministrada.

Bogotá D.C., 30 del mes de septiembre del 2021.

LUIS ANTONIO RODRÍGUEZ OROZCO

Jefe Oficina de Control Interno

Elaboró: Nohra Lucia Forero Cespedes (Contratista)

Revisó: Luz Marina Díaz Ramírez (Contratista)