N° INFORME: OCI-2020-046

PROCESO/SUBPROCESO/ACTIVIDAD: Desarrollo Estratégico -Evaluación Sistema de Gestión del Riesgo

RESPONSABLE DEL PROCESO/SUBPROCESO/ACTIVIDAD: Jefe Oficina Asesora de Planeación.

EQUIPO AUDITOR: Germán Ortíz Martín, Auditor, Contratista.

OBJETIVO(S):

Evaluar la Administración del Riesgo de TRANSMILENIO S.A, mediante informe de Consultoría con base en los criterios de referencia normativa interna y externa que aplica a TRANSMILENIO S.A. Así mismo identificar oportunidades de mejoramiento que permitan agregar valor a la gestión de riesgos, control y gobierno de la Entidad.

ALCANCE:

La consultoría contempla la verificación del cumplimiento por parte de la Entidad de conformidad con lo establecido Guía para la administración del riesgo y el diseño de controles en entidades públicas (riesgos de gestión, corrupción y seguridad digital) 2018 y la concordancia con los lineamientos para la tercera línea defensa de acuerdo con la Guía de auditoría interna basada en riesgos para entidades públicas versión 4 de julio de 2020 emitida por el Departamento Administrativo de la Función Pública, en los siguientes aspectos: Política Administración de Riesgos, Identificación de Riesgos, Valoración de Riesgos e Información, Comunicación y Reporte.

El trabajo realizado mediante mesas de trabajo con un representante de la Oficina de Asesora de Planeación incluyo revisar conjuntamente consideraciones de ajustes a los anexos del Manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 4. (Borrador en actualización).

LIMITACIONES AL ALCANCE: Este trabajo de consultoría no incluye la verificación de riesgos y controles de las matrices de Riesgo de Gestión en virtud del proceso de actualización que se está adelantando por parte de la Oficina Asesora de Planeación para la fecha de este trabajo, por otra parte, la matriz de riesgos de corrupción incorporó ajustes de actualización con fecha agosto de 2020.

DECLARACIÓN:

Esta consultoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por el profesional de la Oficina de Control Interno a cargo de la realización del trabajo.

Una consecuencia de esto es la presencia del riesgo de muestreo, es decir, el riesgo de que la conclusión basada en la muestra analizada no coincida con la conclusión a que se habría llegado en caso de haber examinado todos los elementos que componen la población.

RIESGOS CUBIERTOS:

1. El manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 4 (Borrador en actualización), no cuente con requisitos mínimos del lineamiento externo obligatorio para las entidades públicas emitido por el Departamento Administrativo de la Función Pública, en el marco del Modelo de Planeación y Gestión MIPG.
2. Que los anexos del manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 4 (Borrador en actualización) no guarden relación con el mismo.

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 4 de agosto de 2020 (Borrador en actualización), tomó como insumo las recomendaciones del Informe OCI-2019-058 Consultoría en la implementación y/o actualización del Sistema de Gestión del Riesgo, realizado por la Oficina de Control Interno.

PERÍODO ANALIZADO: a partir 1° de enero al 31 de agosto de 2020.

CRITERIOS:

1. 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, (Borrador en actualización)
2. Manual para la Gestión del Riesgo en TRANSMILENIO S.A. código M-OP-002, Versión 3 de julio de 2019. (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 de auditoría interna basada en riesgos para entidades públicas versión 4 de julio de 2020.
5. 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.

6. La normatividad interna y externa aplicable como (ISO 31000:2018 y NTC GTC137), para ser considerada como mejores prácticas en materia de Riesgos

DESCRIPCIÓN DEL TRABAJO REALIZADO:

De conformidad con el Plan Anual de Actividades de la Oficina de Control Interno de la Entidad correspondiente al año 2020, 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 4 (Borrador en actualización)**:** La Oficina de Control Interno presentó al representante de la Alta Dirección el resultado del análisis a la Política de Gestión de Riesgos y demás componentes así:

- **Objetivo y Alcance:** Se evidenció incorporación de los riesgos de *"Seguridad de la información",* así como las actividades obligatorias del Departamento Administrativo de la Función Pública - DAFP, dentro de los objetivos específicos del capítulo de la Política de Gestión del riesgo de TMSA, contenida en el manual M-OP-002 Versión 4 (Borrador en actualización).
- **Responsables:** Se evidenció la incorporación de este nuevo ítem, el cual permite asignar puntualmente a los responsables de la actualización del manual M-OP-002 Versión 4 (Borrador en actualización), así mismo la responsabilidad de cumplimiento por parte de los gestores de riesgo, el cual es un nuevo rol que más adelante se explicará. Frente al tema de la periodicidad para su actualización esta dado cuando se considere pertinente.
- **Documentos de Referencia:** Se utilizó la normativa vigente aplicable en materia de riesgos para entidades públicas del Departamento Administrativo de la Función Pública, así como las directrices de las normas técnicas ISO 3100:2018 e ISO 27001-

2013. Desde la competencia de la tercera línea defensa en materia de auditorías se incluyó para este ejercicio la Guía de auditoría interna basada en riesgos para entidades públicas Versión 4 Julio de 2020, la cual contiene lineamientos actualizados en materia del ejercicio de auditoria basadas en riesgos.

- **Definiciones:** Se incluyó un nuevo termino denominado *"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".*
- **Generalidades:** Se evidenció un esquema de administración del riesgo por categoría de riesgos y su responsable por línea defensa. Entre los tipos de riesgos nuevos para esta actualización se incorporaron los riesgos de Seguridad de la Información y Tecnológicos, Riesgos Técnicos, Riesgos de Contratación, Riesgos laborales-Seguridad y Salud en el trabajo; los cuales son de gran importancia para la operación de la Entidad, no obstante, estas subcategorías pueden estar contenidas en las tres grandes estructuras de riesgos.
- **Política para la gestión del Riesgo de Gestión y Corrupción en TRANSMILENIO S.A**: El Objetivo, el alcance y los principios cumplen con los lineamientos de las actividades obligatorias del DAFP. Sin embargo, en consideración a lo mencionado en el ítem de documentos de referencia se hace necesario para el ítem 7.3 Principios (deberes de las tres líneas de defensa) fortalecer la redacción de la tercera línea de defensa en virtud de la Guía de auditoría interna basada en riesgos para entidades públicas versión 4 de julio de 2020. Por otra parte, no se observa, en el título de la política, la inclusión de los riesgos de Seguridad de la Información y Tecnológicos, los cuales hacen parte de los tres (3) grandes tipos de riesgos.
- **Nivel de aceptación del riesgo Niveles de aceptación del Riesgo:** En el numeral 7.4. Nivel de aceptación del riesgo del Manual M-OP-002 Versión 4 (Borrador en actualización) se incluyó la siguiente nota de salvedad en cuanto a los riesgos de

corrupción: *no se admite la aceptación del riesgo y siempre se deberán elaborar planes de tratamiento de acuerdo con los lineamientos establecidos por el DAFP*. Igualmente, fue incluida la siguiente salvedad para los riesgos de seguridad de la información: *se tiene contemplado la aceptación de los riesgos con una calificación BAJO, para el nivel MODERADO se aceptan, pero se realizan acciones de reducción del riesgo.*

- **Niveles para calificar el impacto:** En el manual M-OP-002 Versión 4 (Borrador en actualización), mediante el numeral 7,5 "Niveles para calificar la probabilidad de impacto" se amplió el paso a paso registrado en el numeral 8.3. Análisis del Riesgo las Tabla No. 1: Escalas de valoración de la probabilidad para los riesgos de gestión y corrupción, Tabla No. 2 Escalas de valoración del impacto / consecuencia, y la Tabla No.3. Criterios para calificar el Impacto - Riesgos de Corrupción.
- **Tratamiento del Riesgo:** Fueron incorporadas las actividades obligatorias definidas por el DAFP para el tratamiento de riesgos dentro de la Política de Gestión del riesgo de TMSA, contenida en el manual M-OP-002 Versión 4 (Borrador en actualización). Así mismo, se incluyó la salvedad para los riesgos de corrupción: *la respuesta será evitar, compartir o reducir el riesgo, en ningún caso el riesgo de corrupción podrá ser aceptado*.
- **Seguimiento al nivel de riesgo Residual:** Fue incluida la periodicidad anual para los riesgos de gestión y periodicidad trimestral para los riesgos de corrupción, dentro de la Política de Gestión del riesgo de TRANSMILENIO S.A, contenida en el manual M-OP-002 versión 4 (Borrador en actualización), indicando las fechas de los seguimientos y corte de la información para la realización de esta actividad según lo dispuesto en el Decreto 1081 de 2015 *"Por medio del cual se expide el Decreto Reglamentario Único del Sector Presidencia de la República"* al Plan Anticorrupción y de Atención al Ciudadano – PAAC, dada la importancia e impacto de la realización de esta actividad donde participan todos los procesos de la Entidad, se consideraría como una buena práctica analizar las tareas y tiempos utilizados en los ejercicios anteriores

para su realización, con el fin de fijar los plazos para el monitoreo y seguimiento, así como para la entrega del soporte de evidencias que verifica la tercera línea defensa.

Adicionalmente, se evidenció que las matrices de riesgos en actualización y las que están publicadas en la intranet, presentan error en la formulación, toda vez que al aplicar la formula del riesgo en residual el formato Excel no se obtiene el resultado de combinar el impacto y la probabilidad, sólo se tiene en cuenta el impacto, por lo tanto, el nivel de riesgo residual no representa la adecuada aplicación de la metodología definida por la Entidad en manual M-OP-002 versión 4 (Borrador en actualización) para los siguientes procesos:

- *"Planeación del SITP"* enviada a la oficina de control interno por correo electrónico el 27 de agosto de 2020 producto de la jornada de acompañamiento del 27 de julio y 13 de agosto por parte, de la oficina asesora de planeación (en revisión).
- *"Evaluación y Mejoramiento de la gestión"* (en revisión) enviada la Oficina Asesora de planeación el 25 de agosto y producto de la jornada del 3 de agosto,
- *"Gestión del Talento humano"* enviada por correo electrónico del 10 de septiembre por parte de la Dirección Corporativa (en revisión),
- "Desarrollo Estratégico" publicada en el micrositio de la Entidad MIPG con fecha 3 de septiembre.

- **Declaración de la Política:** Fue incluida en el numeral 7.8. Declaración de la Política del Manual M-OP-002 Versión 4 (Borrador en actualización). La cual es 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: Cumple con los pasos definidos en la Guía para la administración del riesgo y el diseño de controles en entidades públicas del DAFP Versión 4 octubre 2018.
- Políticas Relativas al Reporte de Eventos de Riesgo: Es importante mencionar que el *"Anexo 2. Denominado Guía para el reporte de eventos de Riesgo",* contiene 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, los cuales se realizan mediante el "*Anexo 3. Formato reporte de evento de riesgos"*, el cual 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",* no obstante, el primer paso es revisar las acciones a ejecutar contenidas en el plan de tratamiento para los riesgos que de acuerdo con su calificación se les implementó; de la misma forma, en el evento que éste no sea suficiente al momento de una posible materialización y/o no exista plan de tratamiento se deberá adelantar el plan de acción correctivo.
- Políticas relativas a los Riesgos de Interrupción: Estas directrices están contenidas de manera detallada en el Anexo 4. Guía para la aplicación formulario BIA (Business Impact Analysis), el cual no está conectado con el manual M-OP-002 versión 4 (Borrador en actualización) Así mismo mediante el Anexo 5. Instrumento BIA, se iniciaría el levantamiento de información para determinar el plan de continuidad de negocio, el cual, de acuerdo con el nivel de desarrollo, ameritaría políticas de confidencialidad.

- **Niveles de responsabilidad:** Se evidencia incorporación de responsabilidades desde el equipo directivo y los lineamientos precisos se encuentran en cabeza del

representante de la Alta Dirección para la Administración de Riesgos en TRANSMILENIO S.A, dentro de la Política de Gestión del riesgo de TRANSMILENIO S.A, contenida en el manual M-OP-002 Versión 4 (Borrador en actualización). Se observaron, los siguientes ajustes:

- Junta Directiva: la responsabilidad de la Junta Directiva en cuanto a su rol en materia de riesgos.
- El representante de la Alta Dirección: Una de sus funciones indica: *"Realizar el seguimiento a los controles propuestos y planes de tratamientos relacionados con la gestión de riesgos y proponer las actualizaciones y modificaciones correspondientes."* Esta función no indica la periodicidad, sin embargo, en el párrafo de las funciones del Comité Institucional de Coordinación de Control Interno se menciona la presentación semestral del informe de la gestión del riesgo en TRANSMILENIO S.A, el cual por estructura lo realiza el representante de la Alta Dirección o cuando sea necesario (Comité Extraordinario).

  Por otra parte, frente a los reportes de riesgos indicados en la guía *"Anexo 2. Guía para el reporte de eventos de Riesgo".* Otras dos (2) funciones de la Alta Dirección son: 1) *"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 y Presentar informes a la Gerencia General de acuerdo con las solicitudes de esta."* Lo anterior tampoco presenta periodicidad. Por tanto, se recomienda incluirla 2) *"Presentar el informe general de la gestión de riesgos al gerente por parte de la OAP por lo menos una vez finaliza la vigencia y éste sea utilizado como insumo para el informe de gestión de TRANSMILENIO S.A.".*

- Comité Institucional de Coordinación de Control Interno: Semestralmente este comité deberá presentar los resultados de la gestión del riesgo. Razón por la cual las funciones del representante de la alta Dirección se deben alinear con ésta.
- Gestor de Riesgo Líder (Dueños del proceso): Dado que este responsable es nuevo para el manual M-OP-002 Versión 4 (Borrador en actualización), las funciones se comunicaron mediante reunión del comité operativo de primer semestre de 2020 desde la Oficina Asesora de Planeación. De sus principales funciones se evidenció la necesidad de informar los cambios en materia de riesgos del proceso a la representante de la Alta Dirección
- Oficina de Control Interno: Se indica que una de las funciones de la OCI es analizar el diseño e idoneidad de los controles y si son adecuados para prevenir o mitigar los riesgos de Corrupción. No obstante, en la normativa aplicable, es deber de la OCI evaluar no solo el diseño e idoneidad de los controles de los riesgos de corrupción, sino de todas las categorías.
- Funcionarios y Contratistas: Se evidenció la necesidad de fortalecer la redacción de una de sus funciones con el fin de no generar sesgo o ambigüedad a la hora de reportar eventos de riesgo.

- **Estrategias para dar cumplimiento a la política:** cumplen con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización) objeto de la Consultoría para que todas los colaboradores y responsables interactúen y trabajen de manera articulada para el cumplimiento del mismo.
- **Cultura de gestión de riesgos:** Esta actividad cumple con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización), así mismo, es responsabilidad de todos los servidores públicos directos o indirectos de TRANSMILENIO S.A.

- **Metodología para la Gestión del Riesgo:** La Oficina de Control Interno evidenció que tanto 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 DAFP Versión 4 octubre 2018.
- **Identificación del riesgo:** Esta actividad cumple con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización), en cuanto a la implantación 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. Existe de manera informada la Estructura para la identificación de riesgos de gestión en TRANSMILENIO S.A. Esta sección de riesgos de gestión requiere complementar un párrafo para ayuda del lector a ubicar el anexo explicativo.
- **Análisis del Riesgo:** Cumple con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización), se alinea con el numeral Niveles para calificar el impacto y contiene las tablas de Escalas de valoración de la probabilidad para los riesgos de gestión y corrupción, Escalas de valoración del impacto / consecuencia, y Criterios para calificar el Impacto - Riesgos de Corrupción, Mapa de Calor Riesgo Inherente, y Nivel de riesgo inherente. De lo anterior se observó la utilización de los porcentajes sugeridos por el DAFP para cada rango (Insignificante, menor, moderado, mayor y catastrófico) para calificar los riesgos en cuanto a Impacto/Consecuencia, en materia cuantitativa, éstos se podrían evaluar de acuerdo con las condiciones de la Entidad.
- **Evaluación del Riesgo:** Esta actividad cumple con los lineamientos del DAFP y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización), en cuanto a realizar 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. Al igual que, la

clasificación de las actividades de control Preventivas, Detectivas y Correctivas se vinculan con la matriz de acciones Preventivas, correctivas y de mejora.

- **Diseño de Controles:** Esta actividad cumple con los lineamientos del numeral 3.2.2 Valoración de los controles – diseño de controles de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre 2018 y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización).
- **Valoración de los Controles:** Esta actividad cumple con los lineamientos del numeral 3.2.2 Valoración de los controles – diseño de controles de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre 2018 y es concordante con la declaración de la Política de Riesgos del manual M-OP-002 Versión 4 (Borrador en actualización). Incluye las tablas *de Evaluación diseño del control, Resultados de la evaluación del diseño del control, Calificación de la Ejecución del Control, Calificación solidez del control, Calificación solidez del conjunto de controles, Resultados de los posibles desplazamientos de la probabilidad y del impacto de los riesgos, Mapa de calor riesgo residual – Riesgos de Gestión.* Sin embargo, se evidencio la tabla para los riesgos de corrupción falta citar el consecutivo de tabla en manual M-OP-002 Versión 4 (Borrador en actualización).
- **Tratamiento del Riesgo:** Cumple con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre de 2018, en cuanto a las clasificaciones dadas para adoptar plan de tratamiento, sin embargo, se observó que en el manual no se indica a qué riesgos residuales se les debe o no realizar plan de tratamiento de riesgo.
- **Monitoreo y Ejecución:** Cumple con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre de 2018, en cuanto a definir el marco general para la gestión del riesgo y el control y supervisa su cumplimiento, está a cargo de la alta dirección y el comité institucional de coordinación de control interno, por ello el capítulo 8.6.1 Asignación de roles y

responsabilidades para monitoreo y revisión de la gestión de riesgos del manual M-OP-002 Versión 4 (Borrador en actualización), asigna estas actividades por línea de Defensa así:

- Primera Línea Defensa: Cumple con los pasos de la Guía del DAFP, no obstante, el manual no tiene una periodicidad clara de seguimiento por parte del líder del proceso a la administración del riesgo.

- Segunda Línea Defensa: Cumple con los pasos de la Guía del DAFP.

- Tercera Línea Defensa: Presenta en una de sus funciones una redacción general “Mejorar los controles” y en otra de sus funciones un párrafo que amerita revisarse que indica que “En especial deberá adelantar las siguientes actividades” y no indica nada más, razón por la cual se debe revisar la redacción.

- **Reporte de la Gestión del Riesgo:** Cumple con los pasos de la Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFP Versión 4 octubre de 2018, en cuanto a conservar evidencia de la comunicación de la información y reporte de la administración del riesgo en todas sus etapas. Adicionalmente, los riesgos de seguridad digital deberán ser reportados a las autoridades o instancias respectivas que el gobierno disponga. Por lo anterior el párrafo *“Para riesgos de seguridad de la información se debe reportar el incidente de seguridad correspondiente de acuerdo con los lineamientos que disponga la Dirección de TIC y se debe verificar si se tomaron las acciones y se actualizó el mapa de riesgos*” debe tener un vínculo formal de registro con la Dirección de TIC.
- **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 4 octubre de 2018, en cuanto a La comunicación y consulta con las partes involucradas, tanto internas como externas, debería tener lugar durante todas las etapas del proceso para la gestión del riesgo de acuerdo con lo que señala el Instituto Colombiano de Normas

Técnicas y Certificación - ICONTEC. Norma Técnica Colombiana NTC-ISO31000. 2011. p. 132, en cuanto a que este análisis debe garantizar que se tienen en cuenta las necesidades de los usuarios o ciudadanos, de modo tal que los riesgos identificados, permitan encontrar puntos críticos para la mejora en la prestación de los servicios. Es preciso promover la participación de los funcionarios con mayor experticia, con el fin de que aporten su conocimiento en la identificación, análisis y valoración del riesgo.

RECOMENDACIONES y CONCLUSIONES:

Como resultado de la consultoría a los criterios internos para la Gestión de Riesgos de TRANSMILENIO S.A realizada en el marco de los roles, enfoque hacia la prevención y liderazgo estratégico contemplados en el artículo 2.2.21.5.3 “Roles de las Oficinas de Control Interno” del Decreto 648 de 2017, cuyo objetivo principal es promover el mejoramiento continuo de los procesos de la entidad para ayudar a la alta dirección en la búsqueda del cumplimientos de los objetivos institucionales presentamos las siguientes recomendaciones para los diferentes acápites del manual M-OP-002, Versión 4 (Borrador en actualización):

- **Responsables:** Analizar la viabilidad de incluir la actualización del manual por lo menos una vez en cada vigencia.
- **Documentos de Referencia:** incluir en el presente manual los apartes mencionados en la Guía de auditoría interna basada en riesgos para entidades públicas Versión 4 Julio de 2020, para articular y armonizarlo con las actividades de la tercera línea de Defensa.
- **Definiciones:** En virtud a que en el manual M-OP-002, Versión 4 (Borrador en actualización) se incluyó la definición de Riesgo Digital, es pertinentes que en conjunto con la Dirección de TIC se adelanten jornadas de sensibilización a través de los

gestores de riesgos en materia de Seguridad de la Información en especial con eventos como la activación de permisos y privilegios en los sistemas de información de la Entidad, así como el retiro de usuarios que no cuenten con vinculación laboral con la Entidad.

- **Generalidades:** Para la tabla de las tres líneas defensa de este numeral es pertinente: 1) Realizar énfasis en las Tres grandes categorías de riesgos Gestión, corrupción y de seguridad de la información, 2) Realizar una referencia cruzada para indicar al lector que los riesgos, técnicos, de contratación, Laborales, Seguridad y salud en el trabajo) pueden estar contenidos en las tres grandes categorías (Gestión, Corrupción, Seguridad de la Información).
- **Política para la gestión del Riesgo de Gestión y Corrupción en TRANSMILENIO S.A**: Incluir en el título la política los riesgos de Seguridad de la Información y Tecnológicos, los cuales hacen parte de las tres (3) grandes generalidades de riesgos, así mismo asociar para la tercera línea defensa el *"Capítulo 2 metodología para la realización de la auditoría interna basada en riesgos de la Guía de auditoría interna basada en riesgos para entidades públicas versión 4 de julio de 2020*" con el fin de articular el presente documento con las disposiciones del Departamento Administrativo de la Función de la Pública en materia de auditoría.
    - En consecuencia, se hace necesario incorporar un párrafo que permita ampliar al lector la independencia y objetividad de la Oficina de Control Interno así: "*Por lo anterior y 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 se utilizaran los instrumentos aprobados y adoptados por la Entidad (Código de Ética y carta de representación."*
- **Seguimiento al nivel de riesgo Residual:** Incluir una nota de tiempo de entrega de los soportes para el monitoreo y seguimiento de la primera línea de defensa hacia la segunda y tercera línea de defensa, con el fin de evitar incumplir con las fechas de

Ley del Plan Anticorrupción y de Atención al Ciudadano – PAAC en página web de TRANSMILENIO S.A

De la misma forma, revisar y ajustar las fórmulas definidas en las matrices de riesgos (Excel) del 100% de los procesos que se encuentran en revisión a fin de evidenciar concordancia en la metodología definida por la Entidad versus los resultados de la valoración, análisis y evaluación de las matrices de riesgo de los procesos.

- **Declaración de la Política:**

A. Políticas Relativas al Reporte de Eventos de Riesgo: En cuanto al párrafo *"Los funcionarios de TRANSMILENIO S.A., están obligados a reportar, los eventos de riesgo de los cuales tengan conocimiento."* incluir a fin de contar con una correcta interpretación por parte de los usuarios del manual la definición de la frase *"Todos los eventos"*. Por otra parte, es importante que los procesos cuenten con un plan de tratamiento para aquellos riesgos que según su calificación lo amerite de una manera clara y ajustada al entorno.

B. Políticas relativas a los Riesgos de Interrupción: Incluir la referencia cruzada con el Anexo 4 Guía para la aplicación formulario BIA (Business Impact Analysis) y el Anexo 5. Instrumento BIA, para fortalecer esta actividad del manual M-OP-002 versión 4 (Borrador en actualización) y dada la magnitud e importancia para la Entidad, se hace necesario que este capítulo sea trabajado de manera sensible con todos los procesos y con acuerdos de confidencialidad, incorporando el plan de continuidad desde el punto de vista de los Concesionarios, lo anterior en virtud de los diferentes hechos ocurridos de vandalismo durante el noviembre de 2019 y hechos sucesivos, como parte de la flota de buses incinerada en el primer semestre de 2020.

- **Niveles de responsabilidad:**

- El representante de la Alta Dirección: Ajustar esta función para que se relacione con el reporte al CICI (Semestralmente), no obstante, cuando sea necesario (Comité Extraordinario) dado que el reporte de riesgos por los procesos es cada quince (15) días y puede llegar a presentarse la necesidad de comunicar, informar de un caso específico que se materialice para alguna categoría de riesgos en especial los temas Seguridad de la Información que son de gran sensibilidad para la entidad, dadas las mejoras y novedades de tecnología en ejecución (Centro de Control entre otros).

  Así mismo frente a las responsabilidades del *"Anexo 2. Guía para el reporte de eventos de Riesgo*", se pueden evaluar las dos recomendaciones citadas en el acápite de Niveles de responsabilidad del representante de la Alta Dirección.
- Gestor de Riesgo Líder (Dueños del proceso): Actualizar las disposiciones dadas a los gestores de riesgo en el marco del comité operativo con el fin articular con el manual M-OP-002 Versión 4 (Borrador en actualización), para *"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."*
- Oficina de Control Interno: Complementar la redacción de la función de la Oficina de Control Interno citada en este numeral en virtud de que sus diferentes trabajos analiza el diseño e idoneidad de los controles y si son adecuados no solo para los riesgos de corrupción, sino para los riesgos de Gestión, Tecnológicos y de Seguridad de la Información.
- Funcionarios y Contratistas: La OCI recomienda que la función de "Reportar oportunamente los eventos de riesgo de los cuales tengan conocimiento de acuerdo con los lineamientos y procedimientos establecidos para tal fin." Se incluya específicamente los riesgos de gestión, corrupción y de tecnología.

- **Cultura de gestión de riesgos:** La OCI recomienda incluir en el plan institucional de capacitación de la entidad para la vigencia 2021, las capacitaciones en materia de riesgos dirigida a los funcionarios y definir actividades de sensibilización e interiorización para los contratistas y colaboradores de la Entidad.
- **Identificación del riesgo:** Vincular en el párrafo “Las metodologías para la identificación de causas pueden ser consultadas en el procedimiento de acciones correctivas, preventivas y de mejora de la Entidad.” el código del procedimiento de acciones correctivas, preventivas y de mejora de la Entidad. Así mismo en el aparte concerniente a los riesgos de Seguridad de la Información se considera importante conectar al lector con el Anexo 6. Lineamientos Riesgos de Seguridad de la Información.
- **Análisis del Riesgo:** Revisar el nivel de tolerancia (apetito al riesgo) descrito en el actual manual M-OP-002 Versión 4 (Borrador en actualización), en virtud de la realidad operacional de la Entidad, dado que el DAFP, utilizó unos porcentajes estándares de nivel general para todas las entidades públicas y en consecuencia se puede evaluar si éstos están acordes al total del presupuesto asignado para TRANSMILENIO S.A. para los criterios en cuanto a que:
    - Impacte o afecte la ejecución del presupuesto
    - Pérdida de cobertura en la prestación de los servicios de la Entidad
    - Pago de indemnizaciones a terceros por acciones legales que pueden afectar el presupuesto total de la entidad
    - Pago de sanciones económicas por incumplimiento en la normatividad aplicable ante un ente regulador las cuales afecten en determinado porcentaje.
- **Diseño de Controles:** Como buena práctica para los ejercicios de acompañamiento a los procesos que adelanta la Oficina asesora de Planeación, se utilice como ejemplo de lo pasos del diseño uno o más de los controles que tengan debidamente adecuados en el mismo proceso, y de esta forma realizar de manera práctica el ejercicio de verificación de los seis (6) pasos que exige la normatividad.

Complementando lo anterior se puede incluir para el numeral *"8.4.1. Diseño de los controles"* manual M-OP-002 Versión 4 (Borrador en actualización) una periodicidad para la revisión que debe adelantar el dueño del proceso y adicionar un párrafo para que el dueño del proceso deje como evidencia un correo informando a la OAP, la realización de esta actividad; lo anterior contribuiría a la trazabilidad de la gestión del riesgos de la entidad en especial al monitoreo y "*Seguimiento del Plan Anticorrupción y de Atención al Ciudadano – PAAC"* que debe adelantar la Oficina asesora de Planeación y Control Interno.

- **Valoración de los Controles:** Incluir el consecutivo para la tabla que menciona qué, en los casos de riesgos de corrupción, solo se podrá hacer desplazamiento en probabilidad y no existen impactos insignificantes ni menores.
- **Tratamiento del Riesgo:** Definir específicamente a cuáles riesgos residuales se les debería diseñar plan de tratamiento de riesgos, toda vez que el manual no hace claridad del tema, lo que indica que se podrían tener riesgos residuales en estado bajo con plan de tratamiento sin que lo amerite y riesgos residuales altos o extremos sin plan de tratamiento de riesgos.
    - **Monitoreo y Ejecución:**
        - Primera Línea Defensa: Definir una periodicidad de seguimiento a fin de fortalecer la administración del riesgo y facilitar las actividades de monitoreo y seguimiento.
        - Tercera Línea Defensa: Fortalecer la redacción de la página 47 título actividades de evaluación y seguimiento frente a "Mejorar los controles" ya que no indica a qué corresponde dicha actividad, razón por la se sugiere el siguiente párrafo: *"Mejorar los controles mediante recomendaciones a las pruebas realizadas en sus diferentes trabajos para cada vigencia"* y revisar en esta sección el párrafo que conduce a unas actividades que no están descritas.

- **Reporte de la Gestión del Riesgo:** Desde este aparte del manual conducir al responsable (Dirección de TIC) al registro de estos eventos en una bitácora.

- **Anexo 1. DOFA Gestión de Riesgos TMSA:** Cumple con los requisitos mínimos para realizar el ejercicio y su estructura, no obstante, la fecha de actualización es de 2018, y ameritaría una 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**.**

- **Anexo 2. Guía para el reporte de eventos de Riesgo:** Este es nuevo Anexo para el Manual M-OP-002 Versión 4 (Borrador en actualización) y se encontraron las siguientes oportunidades de mejora:
  - 3.1.4 Oficina Asesora de Planeación - OAP: Corregir en la sección de responsabilidades "Informe al Comité Institucional de Control Interno"
  - 3.1.7 Oficina de Control Interno – OCI: Corregir la redacción de las responsabilidades de la Oficina de Control Interno conforme a su respectivo rol:
    a) Ejecuta el programa de auditoria a la gestión de eventos de riesgo. (Esta tarea no la adelanta la Oficina de Control Interno) La Oficina de Control Interno realiza un plan de auditoría con enfoque de riesgos aprobado por el Comité de Coordinación de Control Interno.
    b) Genera las recomendaciones proactivas relacionadas
    c) Reporta resultados al Comité Institucional de Coordinación de Control Interno.
  - 3.2 Políticas de Reporte de Eventos de Riesgo: Complementar que "Todos los eventos de riesgo" se reporten mediante correo electrónico, con la celeridad del caso ante lo sucedido para actuar con oportunidad.

- **Anexo 3. Formato Reporte de eventos de riesgo:** Este es nuevo Anexo para el Manual M-OP-002 Versión 4 (Borrador en actualización), y se encuentra coherentemente estructurado para los análisis de datos y seguimiento, si se llegase a convertir en plataforma digital
- **Anexo 4. Guía para la aplicación formulario BIA y Anexo 5. Instrumento BIA:** Son nuevos Anexos para el Manual M-OP-002 Versión 4 y se encuentran coherentemente estructurados, no obstante, dado que es la primera vez que la entidad adopta este modelo se recomienda que para su diligenciamiento se asignen desde los procesos el máximo capital humano de experiencia y conocimiento e importancia de los procesos Core (Misionales) de negocio.
- **Anexo 6. Lineamientos Riesgos de Seguridad de la Información:** El soporte allegado correspondió al borrador de denominado *"Matriz de riesgo de seguridad de la información junio de 2020"* (En construcción), por lo anterior es indispensable validar con la Dirección de TIC el respectivo anexo y su versión final.

Conclusión:

Se evidencia un avance importante para la Gestión del Riesgo desde el Manual M-OP-002 Versión 4 (Borrador en actualización), el cual aborda aspectos significativos en materia de Riesgos de Seguridad de la Información y Continuidad de negocio, no obstante, es importante que se evalué para la realización de todo este ejercicio el impacto de los contratos con los concesionarios frente al tema de continuidad de negocio, para que sea alineado con el principio de este manual *"Crear valor y salvaguardar a la entidad de la materialización de los riesgos."*

Otro aspecto que evidenció la Oficina de Control Interno, corresponde a la matriz de riesgos del proceso Desarrollo Estratégico publicada en el micrositio de la entidad MIPG

con corte a 31 de agosto de 2020, la cual contiene al inicio de cada riesgo la alineación con los objetivos estratégicos de la Entidad, no obstante la verificación de la concordancia entre el objetivo de cada proceso versus la cobertura de los riesgos, se evaluará a través de la auditoria de aseguramiento que realiza la Oficina de Control Interno.

De acuerdo con los anteriores resultados y con el fin de fortalecer la madurez del Modelo Integrado de Planeación y Gestión para TRANSMILENIO S.A, se debe fortalecer el proceso de articulación de las tres líneas de defensa, elevando su importancia para ajustes, modificaciones y aprobaciones en materia de riesgos a las sesiones del Comité Institucional de Coordinación de Control Interno (CICI), cuando fuere el caso.

Este trabajo fue socializado mediante las mesas de trabajo con el representante de la Oficina Asesora de Planeación.

Cualquier información adicional con gusto será suministrada.

Bogotá D.C., 24 de septiembre de 2020,

LUIS ANTONIO RODRÍGUEZ OROZCO

Jefe Oficina de Control Interno

Elaboró: Germán Ortíz Martín

Revisó: Luz Marina Díaz Ramírez

Código: 801.01-5-5.2