

Nº INFORME: OCI-2022-050

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

EQUIPO AUDITOR Nohra Lucía Forero Céspedes - Contratista de la Oficina de Control Interno
John Edward Burgos Piñeros - Contratista de la Oficina de Control Interno

OBJETIVO

Mediante las funciones definidas para la Oficina de Control Interno, se estableció la asesoría en función de validar que se dé cumplimiento a la política para la administración del riesgo establecida para TRANSMILENIO S. A. En este sentido, se evaluó que las matrices de riesgos de gestión y corrupción se realicen de acuerdo con lo estipulado en el manual, código M-OP-002 en su versión 5 de diciembre de 2021.

ALCANCE

La asesoría contempla la revisión de 5 matrices de riesgos de gestión, las cuales fueron seleccionadas teniendo en cuenta que se encontraran distribuidas en cada una de las líneas de los procesos establecidos (estratégicos, misionales, apoyo y evaluación). En cuanto a la matriz de riesgos de corrupción, se evaluaron, de manera general, los siguientes temas seleccionados: calificaciones a los riesgos en impacto y probabilidad inherente y residual; descripción de los controles y ubicaciones en los mapas de calor, de acuerdo con las calificaciones dadas para cada riesgo.

DECLARACIÓN

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas por los auditores 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.

CRITERIOS

- Guía para la administración del riesgo y el diseño de controles en entidades públicas DAFF Versión 5 diciembre 2020.

- Manual para la Gestión del Riesgo en TRANSMILENIO S. A. código M-OP-002, Versión 5 de diciembre de 2021.

FORTALEZAS

- El personal de la Oficina Asesora de Planeación, designado por el líder del proceso, demostró amabilidad, diligencia y disposición frente a los requerimientos de los profesionales de la Oficina de Control Interno asignados, así como para la concertación de reuniones, acorde con los tiempos disponibles.

DESCRIPCIÓN DEL TRABAJO REALIZADO

De conformidad con el Plan Anual de Auditorias 2022 de la Oficina de Control Interno, se adelantó la asesoría correspondiente en el marco de los criterios normativos para la Gestión del Riesgos de TRANSMILENIO S.A. En ese orden, se realizó revisión de las recomendaciones del informe presentado en el año 2021, las matrices de los riesgos de gestión que en la actualidad se encuentran en revisión por parte de la Oficina Asesora de Planeación y, la matriz de los riesgos de corrupción.

Seguimiento a las recomendaciones del informe OCI-2021-053

Se verificó la implementación de las recomendaciones remitidas a través del informe OCI-2021-053 y, se observó que varias de estas no fueron atendidas, entre las cuales se resaltan:

- «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.»
- Con relación a «En los mapas de calor, verificar el porcentaje dado a la calificación moderada debido a que presenta un porcentaje del 80%», solo se ajustó en uno de los dos que presentaban el error.
- En el numeral 2. Alcance del Manual, unificar 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 el 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).

Nota: Es necesario que se revisen en su totalidad las recomendaciones realizadas por la Oficina de Control Interno en la vigencia 2021.

Revisiones matrices de riesgos de gestión

Se efectuó la revisión de las matrices de los riesgos de gestión que se encuentran publicadas y en revisión de la Oficina Asesora de Planeación. En total se observaron 15 matrices dentro del micrositio del MIPG en la intranet de la entidad (en mapas de riesgos, mapa de riesgo del 2022 - en revisión) y se tomó una muestra de 5 para revisión.

- Proceso de Desarrollo Estratégico
- Gestión de Grupos de Interés.
- Supervisión y Control de la Operación del SITP.
- Gestión del Talento Humano.
- Evaluación y Mejoramiento de la Gestión.

La revisión de las matrices se realizó verificando que se cumplieran con los aspectos descritos en el manual de riesgos de la entidad, tales como:

- La calificación del impacto y la probabilidad, tanto del riesgo en su estado inherente, como en su estado residual.

- Que los controles cumplieran con lo establecido para su descripción.
- Que se establecieran los planes de tratamiento cuando el riesgo residual en el mapa de calor se establece como alto y extremo.

A continuación, se presentan las observaciones encontradas en cada uno de los riesgos descritos en las matrices revisadas:

- **Desarrollo Estratégico**

Se recomienda revisar el riesgo R1 «El plan de acción que incluye las actividades institucionales que soportan el cumplimiento de la plataforma estratégica no guardan relación y consistencia», para que quede con un solo responsable a cargo. Así mismo, se debe revisar la calificación residual, toda vez que, su probabilidad da 36% y se le califica como «muy baja» cuando debería ser «baja» y, se califica en zona residual con «baja» cuando, de acuerdo con los resultados, quedaría como «moderado».

- **Gestión de Grupos de Interés**

En cuanto a la matriz de riesgos del proceso de Gestión de Grupos de Interés, se deben revisar los controles para que estos queden con un solo responsable, teniendo en cuenta que la descripción menciona más de un colaborador (equipo de comunicaciones externas).

Para las calificaciones residuales de los riesgos R1 «La información dirigida a los grupos de valor y grupos de interés, no sea manejada y entregada de manera confiable y completa», se presenta un porcentaje de 36% y se califican como «muy bajos», cuando deberían ser «bajos».

Para la zona residual que queda después de controles para los riesgos R1 y R2 «La información dirigida a los usuarios por el equipo de Atención al Usuario en Vía, sea de forma inadecuada o deficiente» no se califica de manera correcta, toda vez que, se deja como «moderado» cuando debería ser «alto». Adicionalmente, como dicha calificación cambiaría a «alto», se debe realizar plan de tratamiento.

- **Supervisión y Control de la Operación SITP**

En la matriz de este proceso de supervisión y control de la operación del SITP, es necesario que se revise el responsable del control C2 del riesgo R6 «Las actividades necesarias de aseo y mantenimiento en la infraestructura del Sistema no se ejecuten o lleven a cabo y en los plazos establecidos», toda vez, que se evidenció más de un responsable para su ejecución.

Así mismo, verificar la zona resultante de las calificaciones aplicadas a los controles, dado que se observó en la matriz que, para el riesgo R3 «Vincular un vehículo sin el cumplimiento de las condiciones para operar, de acuerdo con los procedimientos vigentes» se califica con 36% como zona «media» cuando en realidad es «baja». De igual forma, el riesgo R4 «Tomar decisiones erradas e inoportunas en las actividades de control y supervisión del Sistema», se califica como «muy baja» cuando debería ser «baja», y con el porcentaje de 21,6% se le da una calificación de «medio» o «muy bajo», cuando debería ser «bajo».

Para los riesgos R5 «errores en la aplicación de las fórmulas y procedimientos especificados para cada indicador, en la descarga de información y en el análisis de ésta» y R7 «Accidentes de tránsito donde se ven involucrados vehículos del sistema», se está aplicando de manera equivocada la reducción de la probabilidad y el impacto, por lo tanto, su calificación residual no es la adecuada.

En cuanto a los planes de tratamiento y, de acuerdo con las calificaciones dadas a los riesgos residuales, no se evidenció que se establezca este tipo planes para los riesgos R7, R8 «percepción negativa de la seguridad» y R9 «afectación a la operación por actos vandálicos o situaciones de orden público generadas por terceros». Así, teniendo en cuenta que la calificación residual es de alta y extrema se recomienda evaluarlas y, de ser necesario, establecer las acciones a las que haya lugar.

- **Gestión del Talento Humano**

En cuanto a la calificación de probabilidad e impacto en el riesgo residual, se recomienda verificar la valoración dada para el riesgo R4 «actividades de formación y desarrollo realizadas no son consistentes con las necesidades de TRANSMILENIO S. A.», toda vez que, su impacto es calificado en 20% «leve» y, es importante considerar que si la entidad no cuenta con el personal formado y capacitado de acuerdo a las necesidades y misionalidad la materialización del riesgo puede afectar la imagen de la entidad «el impacto» frente algunos usuarios de relevancia para el logro de los objetivos, por lo que esto requiere una calificación del 60% «moderado».

En cuanto a la tasación de los porcentajes para la reducción de la probabilidad e impacto, se observó que las calificaciones que se están aplicando no están acordes con la escala de colores establecidas en el manual, debido a que para el riesgo R1 «se cargue de forma errada o

imprecisa las novedades reportadas por los diferentes agentes para la liquidación de la nómina del mes», la probabilidad queda con una calificación del 28,8% «baja» y en la matriz se calificó «muy baja».

En el riesgo R3 «Vincular personas que no tenga (Sic) las competencias requeridas o no cumplan con los requisitos establecidos para el cargo en el Manual de Funciones» se presenta una situación similar, toda vez que, la probabilidad final después de controles es de 14,4% y la calificaron como «moderada» cuando debería ser «muy baja».

Para el riesgo R6 «inadecuada medición de cumplimiento de objetivos de los servidores de la Entidad», la calificación es 21,6% la dejaron como «muy baja», y debería ser «baja», en este caso la calificación final del riesgo residual se ve afectada ya que se calificó como «baja» y en realidad es «moderada».

Finalmente, se calificó el riesgo R7 «Trabajadores y o miembros del grupo familiar sin cumplir los requisitos de parametrización del Proyecto de Bienestar e Incentivos, disfruten y o se beneficien de las actividades» en 24% como «muy baja» y, debería ser «baja».

En cuanto a la aplicación de las reducciones que se deben dar por cada uno de los riesgos, de acuerdo con los controles aplicados, se evidenció una inconsistencia en la calificación del riesgo R5 «Incumplimiento normativo por parte del Sistema de Seguridad y Salud en el Trabajo», toda vez que el control que se establece es correctivo como se indica el Manual de Riesgos y en la Guía del DAFP.

Por último, se recomienda evaluar si el riesgo R1 y R2 «Errores en la liquidación de nómina» podrían tener controles correctivos en caso de evidenciarse su materialización.

• **Evaluación y Mejoramiento de la Gestión**

Se recomienda revisar la calificación de la probabilidad y el impacto de los riesgos R1 «Cumplimiento del Plan Anual de Actividades de la Oficina de Control Interno en un porcentaje inferior al 90%» y R2 «Desacertado aseguramiento y o erróneos resultados de los trabajos ejecutados por la Oficina de Control Interno», porque se observó que la probabilidad se califica en 20% «muy baja». Para dicha calificación es necesario tener en cuenta que el Plan Anual de Auditorías está conformado por varias actividades que son ejecutadas durante el año, lo que puede subir su calificación hasta en un 60% «media».

En el caso del riesgo R2 «Desacertado aseguramiento y o erróneos resultados de los trabajos ejecutados por la Oficina de Control Interno», es necesario tener en cuenta que durante el año se realizan 24 trabajos, por lo tanto, se considera pertinente ajustar la probabilidad a 60% «media».

Para la redacción de los controles se recomienda verificar los responsables asociados al cumplimiento del control, toda vez que para los riesgos R2 y R4 «Pérdida Interna de la información generada en desarrollo del proceso de Evaluación y Mejoramiento de la Gestión», se establece más de un responsable y, en el riesgo R1 no es claro quién debe ejecutarlo.

En lo referente a las calificaciones para la zona de riesgo residual, se debe revisar el riesgo R1 y R3 «Entrega Inoportuna y o con errores de la información solicitada por los entes de control y o vigilancia», pues de acuerdo con los valores que resultan de la aplicación de los controles la zona de riesgo debe ser «bajo» y no «moderado».

Revisión matrices de riesgos de corrupción

Se evidenció que es necesario analizar los criterios que aplican para la calificación del impacto teniendo en cuenta que en el riesgo R2 «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» se mencionan entre sus consecuencias las investigaciones penales, pero no se selecciona como criterio para la evaluación del impacto del riesgo.

Adicionalmente, se requiere establecer un solo responsable de la ejecución de los controles de los riesgos:

- R1 «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»
- R5 «Las bases de datos generadas a través de plataformas y o aplicativos donde se registran las PQRS, sean manipuladas indebidamente por parte del servidor público que recibe una PQRS, para favorecimiento personal»

- R6 «Direccionamiento indebido de los espacios susceptibles de explotación en la Infraestructura por parte de los funcionarios de la Subgerencia de Desarrollo de Negocios, para el beneficio de un tercero relacionado, a cambio de dádivas o favores personales»
- R8 «Gestionar bajo presión cambios no justificados, tomados por el nivel de gerencia general, gerencia de integración o alcaldía en el incremento de flota de vehículos, en beneficio de terceros o a cambio de favores para estos»
- R9 «Manipulación de los parámetros de la programación (zonal) por parte de los funcionarios de la Dirección Técnica de Buses con el fin de favorecer a terceros, en detrimento de la entidad, a cambio de dádivas o pago de favores»
- R10 «Manipulación u omisión intencional por parte de los funcionarios de la Dirección Técnica de Buses de la información al realizar el seguimiento a las obligaciones operacionales de los contratos de concesión (zonal), con el fin de favorecer a un tercero y u obtener un beneficio»
- R22 «Liquidar indebidamente los agentes del sistema por parte de los funcionarios de la Subgerencia Económica encargados de la remuneración de agentes, con el fin de favorecerlos económicamente a cambio de recibir comisiones, dádivas o favores»

También se considera pertinente revisar los controles aplicados a los riesgos relacionados anteriormente, debido a que se presenta falta de coherencia entre las causas y las actividades a desarrollar para evitar su materialización. Respecto de los controles que requieren de una evaluación, se resaltan los asociados al riesgo R31 «Ocultamiento o modificación de los resultados de auditoría interna por parte de auditores y o jefe de la OCI, para beneficio propio o de terceros».

Por otro lado, es necesario revisar las calificaciones del impacto de los riesgos que se señalan a continuación, debido a que presentan una calificación «catastrófica», lo cual no sería correcto teniendo en cuenta el número de criterios que se aplican para la valoración del impacto, así:

- R16 «Alterar datos relacionados con indicadores de desempeño de las empresas operadoras troncales por parte del equipo de trabajo encargado del cálculo y seguimiento de los indicadores, con el fin de ocultar incumplimiento de los concesionarios a cambio de sobornos»

- R17 «Alterar información respecto del estado de operatividad de la tarjeta de conducción por parte del equipo de funcionarios de la Dirección de Seguridad, con el fin de no registrar el estado actual del conductor en el sistema GestSAE a cambio de recibir beneficios a nombre propio o de terceros»

CONCLUSIONES

De acuerdo con el ejercicio de asesoramiento adelantado por la Oficina de Control Interno, se evidenció que la Oficina Asesora de Planeación ha realizado actividades para la actualización de las matrices de riesgos de gestión y de corrupción, sin embargo, no fue posible revisar el cronograma para la ejecución de dichas actividades y monitorear su avance, lo anterior, porque no fue presentado por los responsables del proceso.

Los resultados de esta asesoría fueron presentados por correo electrónico el 8 de agosto de 2022, a los responsables de la actualización de las matrices de riesgos.

RECOMENDACIONES GENERALES

1. Revisar y ajustar la redacción de los controles en lo referente al responsable de ejecutar las acciones. Lo anterior, teniendo en cuenta lo establecido en el Manual para la Gestión del Riesgo en TRANSMILENIO S.A.:

«numeral 8.4.2.1 (Descripción del control), «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.» y en el numeral 9.4.1 (Diseño de los controles), «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» (subrayado fuera de texto).
2. Verificar las calificaciones de la probabilidad y el impacto residual, toda vez que, se evidenciaron diferencias y errores en la aplicación de las fórmulas cuando se presentan controles correctivos, lo anterior, teniendo en cuenta lo establecido en la Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 5 de diciembre de 2020: «numeral 3.2.3 Nivel de riesgo (riesgo residual) que menciona, « En

caso de no contar con controles correctivos, el impacto residual es el mismo calculado inicialmente, es importante señalar que no será posible su movimiento en la matriz para el impacto.»

3. Revisar la zona residual de los riesgos después de controles, en razón a que se evidenciaron diferencias en las matrices revisadas.
4. Atender las recomendaciones realizadas por la Oficina de Control Interno, con el propósito de evitar reprocesos tales como «efectuar una nueva versión del manual por ajustes en las tablas diseñadas para medir la probabilidad y el impacto de los riesgos», que ya se había recomendado en el informe OCI-2021-053.
5. Establecer un cronograma como mecanismo de autocontrol para el monitoreo y actualización de las matrices de riesgos.
6. Tener en cuenta el componente de riesgos emitido por el Departamento Administrativo de la Función Pública - DAFP, en lo relacionado con la evaluación del sistema de control interno.

Cordialmente,

Sandra Jeannette Camargo Acosta.

Jefe Oficina de Control Interno

Elaboró: Nohra Lucia Forero Céspedes, Contratista de la Oficina de Control Interno.

John Edward Burgos Piñeros, Contratista de la Oficina de Control Interno.

Revisó: Luz Nelly Castañeda Contreras, Contratista de la Oficina de Control Interno