N° INFORME: OCI-2023-059

PROCESO / ACTIVIDAD REALIZADA: Seguimiento a la implementación del sistema de continuidad del negocio en la entidad.

EQUIPO AUDITOR: Oscar Pulgarin Lara - Profesional Universitario Grado 4 Oficina de Control Interno

OBJETIVO(S):

Evaluar por parte de la Oficina de Control Interno, el estado actual del grado de implementación del Sistema de Gestión de Continuidad de Negocio (SGCN) en TRANSMILENIO S.A.

ALCANCE:

El alcance corresponde a la verificación del cumplimiento y el estado de las actividades descritas en los planes de trabajo presentados por el contratista, en el marco de la suscripción de los contratos CTO1112-21, CTO729-22 y CTO1774-23, las cuales fueron presentados y aprobadas para la implementación del plan de continuidad del negocio en TRANSMILENIO S.A., teniendo como referencia la ISO 22301-2019 norma internacional para sistemas de gestión de la continuidad de negocio.

CRITERIOS:

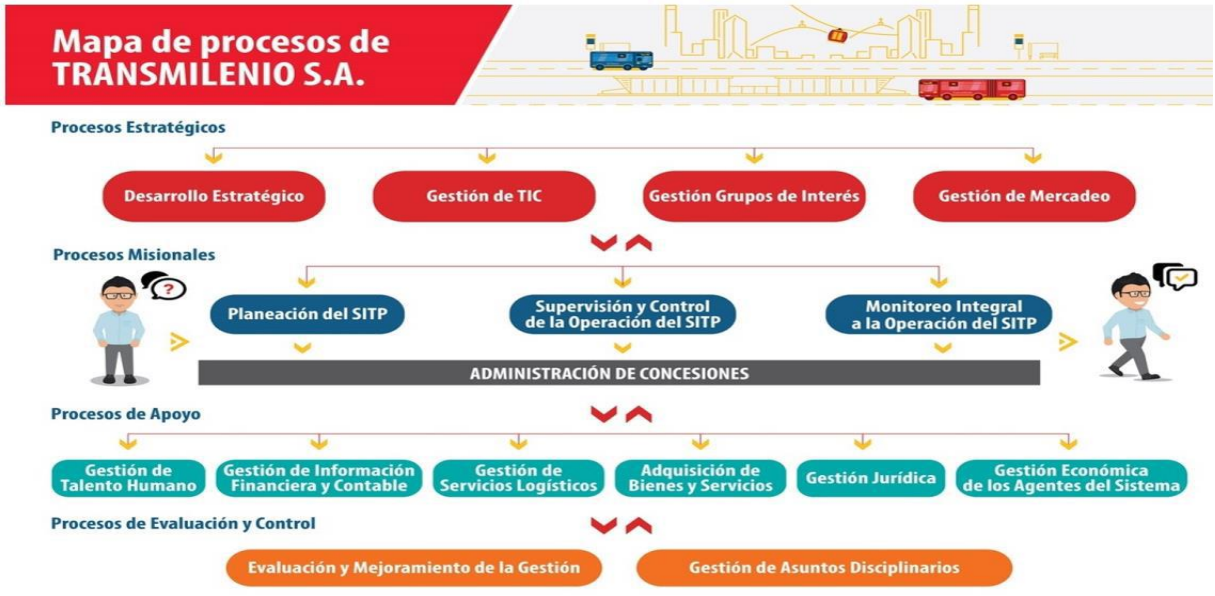
- Norma ISO 22301-2019
- Modelo integrado de planeación y gestión, 3ª. Dimensión: Gestión con valores para resultados.
- Manual de supervisión e interventoría V3 de 2019.
- Planes de trabajo y desarrollo de actividades de la implementación de la continuidad del negocio en TRANSMILENIO S.A.

DESCRIPCIÓN DEL TRABAJO REALIZADO

La Oficina de Control Interno consciente de la importancia que representa la implementación de un sistema de continuidad del negocio en la entidad, lo cual corresponde a una planificación y preparación anticipada de una serie de actividades para garantizar el funcionamiento durante y después de eventos de emergencia o disruptivos, incorporó en el plan anual de auditorías de la presente vigencia, la verificación del avance de implementación, que con ocasión de la suscripción de los contratos CTO1112-21, CTO729-22 y CTO1774-23 se ha venido adelantando desde la Oficina Asesora de Planeación.

Teniendo en cuenta lo anterior, se realizó el análisis y verificación de información relacionada con la formulación, implementación, los ejercicios de prueba y el mantenimiento del plan de continuidad del negocio, teniendo como parámetros los informes presentados por el contratista y los requisitos mínimos que determina la norma ISO 22301-19.

El alcance del plan de continuidad del negocio está definido y cubre los procesos de la cadena de valor de TRANSMILENIO S.A., así:



Fuente: Mapa de proceso de la entidad aplicativo SIGEST

Teniendo en cuenta el objeto de los contratos, la metodología utilizada para el desarrollo de la continuidad del negocio que se viene adelantando para la entidad, basada en la norma ISO 22301-19, es decir, la implementación de procesos y procedimientos recomendados en esta norma. A continuación, se describen los correspondientes avances y dificultades presentadas:

Análisis de Impacto del Negocio (BIA)

Durante el año 2021 se logró construir el informe de análisis de impacto al negocio (BIA) de TRANSMILENIO S.A. en el cual se analizaron la totalidad de los grupos de trabajo que participan en toda la cadena de valor de la entidad.

Sin embargo, una vez presentado el proyecto por parte de la OAP y el contratista a la Subgerencia General, esta recomendó estructurar el modelo de gobierno de continuidad de negocio, focalizándolo en los equipos de trabajo que tienen un tiempo de recuperación objetivo (RTO) de un (1) día y bajo el escenario de interrupción prolongado de los servicios de TIC. Con base en lo anterior, el contratista realizó una nueva distribución del escenario de impacto del negocio el cual quedó de la siguiente manera:

Franja de Recuperación	Proceso	Equipo de Trabajo
a) 0 - 30 Min	B - Gestión TIC	Infraestructura (Seguridad, Telecomunicaciones, Infraestructura y Sistemas de información)
	C - Gestión de grupos de interés	Servicio al Usuario y Atención en Vía
d) 2 - 4 Horas	F - Supervisión y Control de la Operación del SITP	BRT
		Buses
	C - Gestión de grupos de interés	Comunicación Externa
		Gestión Social
	B - Gestión TIC	ITS SIRCI
	F - Supervisión y Control de la Operación del SITP	Dirección Técnica de Infraestructura - DTI
		Seguridad
e) 4 - 8 Horas	L - Gestión Jurídica	Supervisión de los contratos de concesión
f) 1 día	M – Gestión Económica de loa Agentes del Sistema	Gestión Económica de los Agentes del Sistema (Pagos)

Fuente: Información suministrada por el auditado.

Alcance del Sistema de Continuidad del Negocio (SGCN).

Desde diferentes áreas de la entidad, como la Dirección Técnica de Seguridad y la Subgerencia de Atención al Usuario y Comunicaciones se han generado documentos tales como:

Protocolos T-DS-012 a T-DS-030 de plan de prevención preparación y respuesta a emergencias (portales, estaciones, troncales).

E Protocolo T-SC-006 de comunicación externa en caso de crisis.

En los protocolos mencionados se define un alcance correspondiente a partes operativas, por tanto, es necesario definir y aprobar un alcance general para la entidad en el cual se incluya la parte administrativa, en términos de continuidad del negocio, igualmente, determinar el gobierno de este, articulado con los documentos anteriormente mencionados.

Lista de requisitos legales, normativos y de otra índole

La entidad cuenta con un normograma, el cual es definido por cada uno de los procesos de acuerdo con su dinámica de funcionamiento. Se encuentra publicado en la Web para las consultas pertinentes y la Oficina de Control Interno realiza el correspondiente seguimiento de su actualización.

Política de la continuidad del negocio.

La Oficina Asesora de Planeación, junto con el contratista encargado del desarrollo e implementación del Sistema de gestión para la continuidad del negocio (SGCN), definieron una propuesta de política para el sistema, pero, está aún no ha sido llevada para su aprobación al Comité Institucional de Gestión y Desempeño.

Evidencia de competencias y capacitaciones del personal

La Oficina Asesora de Planeación ha trabajado en la concientización de la continuidad del negocio para los grupos críticos, sin embargo, no se ha definido ni realizado una

capacitación estructurada en el tema para todos los funcionarios de la entidad, para que en caso de presentarse una interrupción de las actividades por la circunstancia que sea, se tenga el conocimiento del qué hacer para volver a la normalidad.

Registros de comunicación del proyecto continuidad del negocio

Durante los años 2021 y 2022 el contratista desarrolló diferentes campañas para ser socializadas al interior de la entidad, a través de los diferentes canales que se poseen para que todos los funcionarios conozcan del proyecto y su importancia. En la actualidad, la información ha sido difundida a los funcionarios delegados conocedores de cada uno de los procesos.

Estructura de respuesta a incidentes

En la actualidad la entidad cuenta con procedimientos en la Dirección de TIC, sin embargo, no se han realizados simulacros de gestión de incidentes informáticos y ciberseguridad.

De igual manera, en la Dirección Técnica de Seguridad se detallan procedimientos correspondientes al plan de prevención, preparación y respuesta a emergencias, diseñados para portales, estaciones y troncales, pero no para el resto de la empresa, por ejemplo, los centros de control.

En la entidad se deben establecer, implantar y mantener procedimientos de continuidad de negocio para gestionar todos los incidentes y poder lograr la continuidad de las actividades con base en los objetivos de recuperación que se hayan definido e identificado en el análisis de impacto de negocio.

Planes de continuidad del negocio

Los planes de continuidad del negocio son una recolección de procedimientos e información que es desarrollada, compilada y mantenida a disposición para su uso en caso de una emergencia o desastre.

Es necesario tener definido un gobierno de continuidad del negocio que se encargue de articular y dirigir las diferentes estrategias institucionales que den respuesta a dichos

eventos, generando el menor trauma posible, con el menor tiempo de retrasos en la operación y el funcionamiento del sistema TransMilenio, esto con el propósito de que los usuarios no se vean afectados.

En la actualidad, no se ha definido el gobierno de continuidad en la entidad.

Revisión por la dirección

La alta dirección debe revisar el sistema de gestión de la continuidad del negocio en la organización a intervalos planificados para garantizar su idoneidad, adecuación y eficacia continuas.

No obstante lo anterior, en la entidad este requisito aún no se ha llevado a cabo, dado que no existe formalmente el SGCN, lo mismo que el tema de acciones correctivas y preventivas y las auditorías.

La Oficina de Control Interno ha venido realizando seguimiento al estado de implementación y generado las recomendaciones correspondientes.

Procedimiento para el control de la información documentada

La entidad cuenta con el procedimiento P-OP-001 «Control de los documentos oficiales del sistema de gestión de TRANSMILENIO S.A.», en el cual se describen todos los lineamientos para la generación de los documentos que soportan su quehacer.

Por su parte, no se han incorporado al aplicativo correspondiente los documentos que se han generado, como por ejemplo el procedimiento de continuidad del negocio pues aún no se ha oficializado el sistema de gestión de continuidad del negocio.

Escenarios de incidentes

Existen diferentes escenarios que pueden afectar la continuidad del negocio de una empresa, es por lo que, en TRANSMILENIO S.A., el contratista, junto con los diferentes equipos asignados al desarrollo e implementación del sistema de gestión de continuidad

del negocio, han visualizado los diferentes escenarios que se pueden presentar y lo han descrito de la siguiente manera:

Escenario	Amenazas
Escenario No. 1 Pérdida de información **Categoría I y Categoría II**	• Daños en repositorios de datos principales • Imposibilidad de recuperar datos desde las copias de respaldo. • Pérdida de copias de respaldo por deterioro o daño de los medios (Cintas o Discos) derivados de la incorrecta manipulación o almacenamiento. • Inundaciones, incendios, acceso físico no autorizado. • Errores en la administración de la plataforma de gestión de copias de respaldo.
Escenario No. 2 Daños severos o imposibilidad de funcionamiento del centro de datos de TRANSMILENIO **Categoría III**	• Desastres naturales como movimientos telúricos, inundaciones, ciclones, etc. • Incendios, terrorismo, fallas prolongadas de energía, etc. • Ciberataques
Escenario No. 3 Daños severos o imposibilidad de uso de las instalaciones físicas TRANSMILENIO (Edificio Elemento). **Categoría II**	• Desastre natural (terremotos, avalanchas, inundaciones) • Huelgas de personal, terrorismo, incendio. • Daños físicos en las acometidas de telecomunicaciones • Fallas prolongadas de energía
Escenario No. 4 Perdida de los enlaces de comunicaciones **Categoría II**	• Fallas en hardware de comunicaciones (Core Switch, Router, Gateway) • Falla prolongada de Energía Eléctrica. • Inundaciones, incendios, etc. • Errores en la administración de la plataforma • Falla general de los proveedores • Ausencia de mecanismos de redundancia de proveedores de comunicaciones
Escenario Nro. 5 Imposibilidad de uso de las aplicaciones y/o infraestructura aprovisionada en la nube. **Categoría II**	• Fallas de telecomunicaciones • Ataques cibernéticos
Escenario Nro. 6 Fallas en los sistemas de manejo de transporte provistas por los operadores y concesionarios **Categoría II**	• Fallas de telecomunicaciones • Vencimiento de contratos o terminación anticipada de los mismos. • Desastres naturales, movimientos telúricos. • Asonada, desórdenes públicos. • Ataques cibernéticos
Escenario Nro. 7 Daños en instalaciones de la infraestructura base para el funcionamiento del servicio de transporte: Portales, estaciones, paraderos, patios y talleres de buses **Categoría III**	• Desórdenes públicos, actos de vandalismo • Desastres naturales

Fuente: Información suministrada por el auditado.

Mitigación del riesgo

La entidad cuenta con documentación relacionada con la mitigación de los riesgos, tales como el Manual para la Gestión del Riesgo en TRANSMILENIO S. A. V.5 M-OP-002, el Anexo 5. Riesgos de interrupcion_V1, y las Matrices de riesgos de los procesos de TRANSMILENIO S.A., cuyo objeto es reducir la posibilidad de que se materialicen los riesgos identificados por la entidad.

Plan de mantenimiento Sistema de Gestión de Continuidad del Negocio

Se han suscrito los contratos CTO1112-21, CTO729-22 y CTO1774-23 cuyo objeto corresponde a apoyar la implementación del plan de continuidad del negocio de TRANSMILENIO S.A., así como en la ejecución de los ejercicios de prueba y el

mantenimiento de dicho plan, teniendo en cuenta los lineamientos legales, los requisitos de la norma ISO 22301 que se encuentre vigente o aquella que la sustituya o reemplace, sin embargo, y teniendo en cuenta la importancia de la implementación de éste sistema, la entidad no cuenta con un recurso dedicado 100% a la operación y mantenimiento del mismo.

RECOMENDACIONES:

- Definir un alcance al sistema de continuidad del negocio, en el cual se indique el inicio, la identificación y socialización de los elementos críticos que puedan definirse como incidente o desastre que impidan continuar con la operación.

  Así mismo, se debe realizar una conclusión con los análisis y las acciones de mejora que fueron identificadas producto de la reacción de las áreas ante la situación de interrupción presentada, ya sea durante simulacros o eventos reales.
- Aprobar la política y la estructura de gobierno del plan de continuidad del negocio de TRANSMILENIO S.A., que permita una adecuada planificación, control, liderazgo y mejoramiento de las estrategias para la continuidad, las que deberán ser implementadas para asegurar el servicio a los usuarios en caso de presentarse un evento de interrupción.
- Capacitar a todos los funcionarios y colaboradores de la entidad en los conceptos y trámite del plan de continuidad de negocio y del gobierno de continuidad definido, toda vez que, la interacción entre los procesos de apoyo y los procesos misionales exige que el plan contemple la recuperación ordenada de todos los equipos de trabajo.
- Desarrollar simulacros de interrupción que exijan la participación de directivos, colaboradores, terceros, proveedores críticos de servicios y usuarios finales de TRANSMILENIO S.A.
- Determinar para la continuidad de negocio la creación de un centro de control alterno que puedan suplir la operación en caso de presentarse fallas en el edificio en donde funciona la parte administrativa de la entidad.

- Definir los recursos humanos y económicos, que garanticen la continuidad de la implementación de este proyecto en la entidad, ya que por su importancia es necesario que esto se establezca como una necesidad duradera.

CONCLUSIONES:

El análisis de la información aportada por el contratista permite concluir que el trabajo viene desarrollándose de acuerdo con lo establecido en los planes de trabajo y cronogramas presentados a la Oficina Asesora de Planeación, quien ha sido la encargada de la supervisión de los contratos suscritos para el desarrollo e implementación del «Proceso de Continuidad del Negocio» para TRANSMILENIO S.A., el cual es susceptible de mejoramiento, de acuerdo con las recomendaciones que se presentan en este informe.

Este documento se expide el día 20 de noviembre de 2023, por parte de TRANSMILENIO S.A. y es firmado por Sandra Jeannette Camargo Acosta, jefe de la Oficina de Control Interno.

SANDRA JEANNETTE CAMARGO ACOSTA

Firmado digitalmente por SANDRA JEANNETTE CAMARGO ACOSTA
Fecha: 2023.11.23 10:15:37 -05'00'

Sandra Jeannette Camargo Acosta

Jefe Oficina de Control Interno

Elaboró: Oscar Pulgarin Lara, Profesional Universitario Grado 4 – Oficina de Control Interno.

Revisó: Luz Nelly Castañeda Contreras - Contratista Oficina de Control Interno.