



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



Nº INFORME: OCI-2022-066

PROCESO / ACTIVIDAD REALIZADA: Seguimiento implementación proceso continuidad del negocio en la entidad.

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

OBJETIVO(S):

Verificar el estado de avance de la implementación de la continuidad del negocio en TRANSMILENIO S.A., teniendo como referencia el plan de trabajo presentado por el contratista de la Oficina Asesora de Planeación quien suscribió los contratos CTO1112-21 y CTO729-22 para ello.

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, antes mencionado, en el marco de la suscripción de los contratos CTO1112-21 y CTO729-22, las cuales fueron presentados y aprobados por el supervisor de dichos contratos para la implementación del plan de continuidad del negocio en TRANSMILENIO S.A.

CRITERIOS:

- Ley 1955 de 2018, por el cual se expide el Plan Nacional de Desarrollo 2018-2022.
- "Pacto por Colombia, Pacto por la Equidad". Artículo 147.
- Ley 1523 de 2012, «Por la cual se adopta la política nacional de gestión del riesgo de desastres y se establece el Sistema Nacional de Gestión del Riesgo de Desastres» - Artículo 2º
- Modelo Integrado de planeación y gestión, 3ª. Dimensión: Gestión con valores para resultados.



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



- Norma NTC-ISO 22301 Norma internacional para sistemas de gestión de la continuidad de negocio.
- Contratos de prestación de servicios 1112-21 y 729-22
- Planes de trabajo desarrollo de actividades implementación continuidad del negocio en TRANSMILENIO S.A.

DESCRIPCIÓN DEL TRABAJO REALIZADO

La Oficina de Control Interno, en el marco de la Ley 87 de 1993 y el desarrollo del Plan Anual de Auditorías, aprobado para la presente vigencia, efectuó una revisión del estado de implementación del plan de continuidad del negocio.

Este proceso de revisión involucró la solicitud, análisis y verificación de la información que se encuentra relacionada con la formulación, implementación, ejercicios de prueba y el mantenimiento del Plan de Continuidad del Negocio, la cual fue remitida por la Oficina Asesora de Planeación y el contratista responsable de su desarrollo.

La anterior revisión se realizó de acuerdo con las fases y o actividades propuestas por el contratista en los planes de trabajo y que detallan el conocimiento, reconocimiento y diagnóstico del estado en el que se encuentra la entidad en el tema de la continuidad del negocio, esto con el propósito de diseñar su implementación teniendo en cuenta que TRANSMILENIO S.A. es una empresa de transporte y una gran parte operacional depende de la parte tecnológica para su funcionamiento.

Es del caso señalar que, el objetivo general del plan de continuidad del negocio está relacionado con: «establecer las medidas y/o acciones a seguir en caso de un evento no planificado que afecte la normal operación de los procesos, detallar las actividades de respuesta inmediata para los incidentes y así mitigar los impactos para la continuidad a la prestación de los servicios de TRANSMILENIO S.A.», de igual manera, que los objetivos específicos corresponden a:

- Proteger la integridad de los colaboradores de TRANSMILENIO

- Preparar a la entidad en las acciones necesarias para mantener la disponibilidad del servicio de transporte ante la ocurrencia de interrupciones significativas.
- Minimizar el impacto de las interrupciones sobre el servicio de transporte.
- Asegurar una oportuna restauración de las operaciones afectadas por el evento.
- Cumplir con los requisitos contractuales y contemplados en la normativa vigente.
- Proteger a TRANSMILENIO de impactos reputacionales, legales y operativos que pondrían en riesgo la entidad.
- Minimizar la toma de decisiones durante una situación de desastre.
- Implementar proyectos de mejora hacia la continuidad del negocio.

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, documentación entregada por el contratista.



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



La metodología utilizada para el desarrollo de la continuidad del negocio está basada en la norma ISO 22301-19, es decir, la implementación de procesos y procedimientos recomendados allí, teniendo en cuenta el ciclo del planear, el hacer, el verificar y el actuar.

Bajo esta metodología se han identificado procesos críticos, como lo son: supervisión y control de la operación del SITP y Gestión de TIC (parte operativa y parte tecnológica) que pueden interrumpir la operación, sin embargo, no son menos importantes los otros procesos, tanto misionales como de apoyo, para lo cual es importante identificar un líder de continuidad del negocio que administre y coordine las respuestas y la recuperación en caso de una crisis, esto con el apoyo del equipo que se faculte para tal fin.

En otras actividades realizadas, se identificaron los riesgos del proyecto y los de la continuidad del negocio, los cuales fueron incorporados en una nueva versión del Manual de Riesgos de TRANSMILENIO S.A., que aún se encuentra en revisión. En cuanto a la definición de la política de continuidad del negocio, la misma se socializó con la Oficina Asesora de Planeación, sin embargo, aún no con el Comité de MIPG para su respectiva aprobación.

De igual forma, el contratista realizó el análisis de los impactos que se pueden llegar a producir dentro de todos los procesos de la entidad si se llegara a interrumpir uno de ellos. Así, con esta acción se identificaron los procesos más críticos para la empresa, estableciendo dónde se debe centrar el mayor esfuerzo de la continuidad del negocio para que, en caso de ser interrumpidos, el impacto sea mínimo y pueda recuperarse en el menor tiempo posible.

Ahora, el análisis de impacto señalado anteriormente fue enviado a cada uno de los responsables de los procesos y, a la fecha, el 40% de ellos no ha enviado la información solicitada la que es necesaria para concretar lo evidenciado en el primer análisis.

A continuación, se relacionan los procesos que no han aportado la información solicitada:



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



Proceso	Equipos de trabajo
Gestión de TIC	Infraestructura (Seguridad y Telecomunicaciones)
Gestión de mercadeo	Gestión de mercadeo
Planeación del SITP	Estudios de proyección, Equipos e Infraestructura, Transporte.
Supervisión y control de la operación del SITP	BRT, Buses, Seguridad, Modos.
Monitoreo Integral a la Gestión del SITP	Monitoreo Integral a la Gestión del SITP
Gestión de Talento Humano	Salud y seguridad en el trabajo, Nómina.
Gestión de Servicios Logísticos	Gestión documental, mantenimiento y seguros.
Adquisición de Bienes y Servicios	Adquisición de Bienes y Servicios.
Gestión económica de los agentes del sistema	Gestión económica de los agentes del sistema

Fuente: Información suministrada por el auditado.

Adicionalmente, otro de los inconvenientes que se ha presentado para el desarrollo de la implementación del plan de continuidad del negocio ha sido la imposibilidad de realizar una campaña de concientización, la cual fue propuesta por el contratista al área de comunicación interna de la Subgerencia de Atención al Usuario y Comunicaciones (SAUC), toda vez que no se ha llevado a cabo por diversos ajustes solicitados por dicha área, retrasando así el cronograma propuesto.

Aunado a lo anterior, los responsables y, en general todos los involucrados, dejan de lado el tema y el contratista se ve en la obligación de realizar reprocesos para la retroalimentación de todo lo avanzado, lo que genera retrasos innecesarios.

Actualmente, el proyecto esta siendo objeto de ajustes en los planes y procedimientos, escenarios y estrategias de continuidad del negocio y el programa de ejercicios y pruebas, esto con el propósito de validar su efectividad en el tiempo, de acuerdo con lo establecido en los planes de trabajo.

Vale la pena mencionar en esta parte, que a pesar de que el contratista ha realizado una serie de simulacros de tecnología, lo ha hecho sin la participación de usuarios, por lo tanto, se está planeando ejecutarlos con la asistencia de personas, esto a finales del mes de noviembre o primeras semanas de diciembre de 2022.

Con el trabajo realizado por el contratista, se ha identificado una serie de escenarios de desastres, los cuales se detallan en la siguiente tabla:

Escenario	Amenazas	Principales Consecuencias
<p>Escenario No. 1 Pérdida de información</p> <p>Categoría I y Categoría II</p>	<ul style="list-style-type: none"> • 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. 	<ul style="list-style-type: none"> • Parálisis de la operación • Atraso en el cumplimiento de pagos a operadores • Imposibilidad de uso de los servicios de TI.
<p>Escenario No. 2</p> <p>Daños severos o imposibilidad de funcionamiento del centro de datos de TRANSMILENIO</p> <p>Categoría III</p>	<ul style="list-style-type: none"> • Desastres naturales como movimientos telúricos, inundaciones, ciclones, etc. • Incendios, terrorismo, fallas prolongadas de 	<ul style="list-style-type: none"> • Parálisis de la operación • Atraso en el cumplimiento de pagos a los operadores • Imposibilidad de uso de los servicios de TI. • Afectación de la reputación • Pérdidas económicas

Escenario	Amenazas	Principales Consecuencias
	<ul style="list-style-type: none"> energía, etc. Ciberataques 	<ul style="list-style-type: none"> Fallas en la distribución de comunicados a los usuarios del servicio de transporte. Parálisis de las principales aplicaciones que apoyan la gestión.
<p>Escenario No. 3</p> <p>Daños severos o imposibilidad de uso de las instalaciones físicas TRANSMILENIO (Edificio Elemento).</p> <p>Categoría II</p>	<ul style="list-style-type: none"> Desastre natural (terremotos, avalanchas, inundaciones) Huelgas de personal, terrorismo, incendio. Daños físicos en las acometidas de telecomunicaciones Fallas prolongadas de energía 	<ul style="list-style-type: none"> Parálisis de la operación Atraso en el cumplimiento de pagos a los operadores Imposibilidad de uso de los servicios de TI. Afectación de la reputación Pérdidas económicas Fallas en la distribución de comunicados a los usuarios del servicio de transporte. Perdida de supervisión de la operación (quedan inoperativos los centros de control de Buses y de BRT)
<p>Escenario No. 4</p> <p>Perdida de los enlaces de comunicaciones</p> <p>Categoría II</p>	<ul style="list-style-type: none"> 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. 	<ul style="list-style-type: none"> Parálisis de la operación Atraso en el cumplimiento de pagos a los operadores Imposibilidad de uso de los servicios de TI. Afectación de la reputación Pérdidas económicas Fallas en la distribución de comunicados a los usuarios del servicio de transporte. Perdida de supervisión de la operación

Escenario	Amenazas	Principales Consecuencias
<p>Escenario Nro. 5</p> <p>Imposibilidad de uso de las aplicaciones y/o infraestructura aprovisionada en la nube.</p> <p>Categoría II</p>	<ul style="list-style-type: none"> • Fallas de telecomunicaciones • Ataques cibernéticos 	<ul style="list-style-type: none"> • Pérdida de información • Afectación de la reputación • Pérdidas económicas • Perdida de supervisión de la operación
<p>Escenario Nro. 6</p> <p>Fallas en los sistemas de manejo de transporte provistas por los operadores y concesionarios</p> <p>Categoría II</p>	<ul style="list-style-type: none"> • Fallas de telecomunicaciones • Vencimiento de contratos o terminación anticipada de los mismos. • Desastres naturales, movimientos telúricos. • Asonada, desórdenes públicos. • Ataques cibernéticos 	<ul style="list-style-type: none"> • Pérdida de información • Afectación de la reputación • Pérdidas económicas • Parálisis de la operación • Imprecisión en la información de base para el pago de los operadores.
<p>Escenario Nro. 7</p> <p>Daños en instalaciones de la infraestructura base para el funcionamiento del servicio de transporte: Portales, estaciones, paraderos, patios y talleres de buses</p> <p>Categoría III</p>	<ul style="list-style-type: none"> • Desórdenes públicos, actos de vandalismo • Desastres naturales 	<ul style="list-style-type: none"> • Parálisis de la operación del servicio de transporte • Afectación de la imagen publica • Pérdida de vidas de ciudadanos, funcionarios y/o contratistas de la entidad.

Fuente: Información suministrada por los auditados, plan de continuidad del negocio 2022

Por otro lado, se estableció que existe otra etapa importante que consiste en identificar, con los datos aportados por algunas dependencias, la secuencia de recuperación, la descripción de los procesos que deben activarse en caso de interrupción de los servicios, el tiempo objetivo para que el servicio sea reanudado y los recursos tecnológicos o económicos de los otros procesos que deben ser recuperados.



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



Para ello se han utilizado 5 variables, a las cuales se les asignó un peso porcentual de importancia así:

- Los diferentes impactos que genera la interrupción del proceso sobre TransMilenio 25%.
- Los objetivos de continuidad identificados por cada uno de los procesos 20%.
- Procesos que brinden información permanente al usuario del servicio 15%.
- Los procesos que ejecutan actividades críticas con mayor frecuencia 15%.
- Participación del proceso en el cumplimiento de la misionalidad de TRANSMILENIO 25%.

Con base en lo anterior, a continuación, se describen algunas de estas secuencias:

Franja de Recuperación	Proceso	Equipo de Trabajo
0-30 min	Gestión TIC	Infraestructura (Seguridad y Telecomunicaciones)
0-30 min	Gestión de grupos de interés	Servicio al Usuario y Atención en Vía
2-4 horas	Gestión TIC	ITS SIRCI
2-4 horas	Gestión de grupos de interés	Comunicación Externa Gestión Social
2-4 horas	Supervisión y Control de la Operación del SITP	BRT, Buses, Seguridad
2-4 horas	Gestión Económica de los Agentes del Sistema	Gestión Económica de los Agentes del Sistema
4-8 horas	Supervisión y Control de la Operación del SITP	Modos
2-4 horas	Gestión Jurídica	Gestión de concesiones

Fuente: Información suministrada equipo auditado- Secuencia de recuperación

Es importante mencionar que, dentro de lo identificado como «crítico» por el contratista, se encuentra la parte de tecnología y para ello se está sugiriendo mantener y migrar la

Informe OCI-2022-066 Continuidad del Negocio Página 9 de 11



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



mayor información posible a la nube, que es un modelo de servicio en el cual los datos de un sistema de cómputo se almacenan, administran y se respaldan de forma remota, típicamente, en servidores que están en la nube y que son administrados por un proveedor del servicio.

En lo referente a la parte operativa y, en especial a los centros de control, se está estudiando la posibilidad de que en caso de suceder un incidente que afecte la operación y las instalaciones de TRANSMILENIO S.A. y estas no se puedan controlar y monitorear desde la sede administrativa, se puedan llevar a cabo desde los centros de control de los operadores.

RECOMENDACIONES:

1. Adoptar la metodología relacionada con los riesgos de interrupción del negocio e iniciar el monitoreo de estos, con el fin de mitigar su materialización.
2. Gestionar las acciones necesarias para agilizar el apoyo en cuanto a la concientización o socialización del proceso de continuidad del negocio para que todos los funcionarios estén enterados y participen activamente de él, apropiándolo como parte de la cultura organizacional.
3. Identificar un líder del proceso de continuidad del negocio para la entidad, quién será el encargado de crear o mejorar planes o estrategias para mantener en funcionamiento la empresa luego de presentarse algún evento disruptivo como desastres naturales, terrorismo, errores humanos o de automatización.
4. Presentar al Comité de MIPG la «Política de Continuidad del Negocio», para poder tener una adecuada planificación, control y mejoramiento de las estrategias de la continuidad, las que serán implementadas para asegurar el servicio a los usuarios en caso de presentarse un evento de interrupción.
5. Gestionar con los responsables de los procesos el envío de la información pendiente para la elaboración de un plan de recuperación acertado.



OTROS INFORMES DE LA OFICINA DE CONTROL INTERNO



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.

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.