N° INFORME: OCI-2018-076

PROCESO / ACTIVIDAD REALIZADA: Auditoría al Proceso Gestión de TIC´s.

EQUIPO AUDITOR: Germán Ortíz Martín (auditor líder), Contratista Jorge Iván Flórez Franco (auditor acompañante).

OBJETIVOS:

1. Evaluar el diseño y la eficacia operacional de los controles internos para una muestra de las actividades registradas en la caracterización del proceso auditado.

2. Identificar oportunidades de mejoramiento que permitan agregar valor a los procesos de gestión de riesgos, control y gobierno de la Entidad**.**

ALCANCE:

El alcance previsto para este trabajo de auditoría comprende la evaluación de los controles internos, la identificación de oportunidades de mejora y la evaluación del grado de conformidad con el Sistema Integrado de Gestión aplicable al proceso Gestión TIC´s, con las actividades derivadas de la caracterización que cubren la definición estratégica, direccionamiento, planeación y administración de las Tecnologías de la Información y las Comunicaciones (TIC) incluidos los ITS, así como de la seguridad de la información y mapas de riesgos de gestión de TRANSMILENIO S.A.

Por lo anterior se abordó para este ejercicio los siguientes temas puntuales: **a)** Revisión a los elementos que componen el Plan Estratégico de Tecnología de la Información y las Comunicaciones de acuerdo a lo señalado en el Decreto 415 de 2016 para los productos y/o entregables del mapa de ruta de proyectos con culminación trimestres II, IV de 2017 y III, IV de 2018 , **b)** La Políticas de Backup y Restore, **c)** Los Planes de Continuidad y Contingencias de Tecnología de la Información TI, **d)** Las Políticas de Logs a los sistemas de Información de la muestra y **e)** las Políticas de Gestión de Cambio. Como criterio de verificación para cada uno de los temas anteriores se utilizó la documentación vigente, adoptada y aprobada por el Proceso Gestión de TIC´s en el Sistema Integrado de Gestión

de TRANSMILENIO S.A, y se utilizaron las técnicas de muestreo aleatorio simple para poblaciones finitas en los diferentes temas a analizar.

La presente auditoría no contempla los aspectos auditados en el marco de la auditoría del Sistema Integrado de Gestión SIG del mes de julio de 2018.

LIMITACIONES AL ALCANCE: Este trabajo de aseguramiento no incluye la verificación de riesgos y controles incluidos en el Plan Anticorrupción y de Atención al Ciudadano, debido a que la Oficina de Control Interno realizó un trabajo particular de seguimiento a éstos con fecha de corte 31 de agosto de 2018, mediante el informe 071 de 2018.

PERÍODO AUDITADO: 01 de septiembre de 2017 al 31 de agosto de 2018.

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 DE LA AUDITORÍA

- *Decreto 415 marzo 7 de 2016: "Definición de los lineamientos para el fortalecimiento Institucional en materia de tecnologías de la información y las comunicaciones".*
- *Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.*
- *Norma NTC-ISO-IE 27001-2013.*

- *Procedimiento P-DT-007 versión 2 de fecha junio de 2017".*
- *Protocolo a seguir para la administración de Bases de Datos T-DT-004 V2, abril 2018.*
- *Protocolo a seguir para gestionar el uso de los Medios Removibles T-DT-003 V0, Dic 2017.*
- *Procedimiento administración de usuarios P-DT-007 V2, junio 2017.*
- *Procedimiento código P-DT-010 versión 0 de noviembre de 2015 "Procedimiento para el monitoreo del uso de los medios de procesamiento de información".*

- Normativa interna y/o externa incluida en el Normograma del proceso y aplicable al alcance definido para el presente trabajo de aseguramiento

- Caracterizaciones, procedimientos, protocolos, formatos del SIG del proceso Gestión Tics vigentes en la plataforma de intranet de TRANSMILENIO S.A.

RIESGOS CUBIERTOS:

RIESGOS DEL PROCESO VIGENTES

1. Que la planeación tecnológica no sea acorde con las funciones, actividades, responsabilidades o desarrollo de la Empresa.

2. Que el plan estratégico de tecnologías de la información y las comunicaciones no se desarrolle.

3. Falta en la Planificación o en el Seguimiento a la Gestión institucional

4. Que no se pueda mantener la continuidad o integridad en las tecnologías de la información

5. Que se altere el estado de los activos de información de la Empresa

6. Que los servicios o la infraestructura tecnológica no sean apropiada al desarrollo de las funciones de la Empresa.

7. Que no se puedan atender las necesidades o requerimientos de los usuarios de las tecnologías de la información y las comunicaciones.

RIESGOS IDENTIFICADOS POR LA OFICINA DE CONTROL INTERNO

1. Debilidad de interacción con otros procesos para la ejecución de las actividades del proceso de Gestión TIC´s.

2. Debilidad en la confidencialidad y disponibilidad de la información.

DESCRIPCIÓN DEL TRABAJO REALIZADO:

De conformidad con el Plan Anual de Actividades de la Oficina de Control Interno del año 2018, se adelantó auditoría interna al Proceso *"Gestión de TIC´s"*, para el periodo comprendido entre 01 de septiembre de 2017 al 31 de agosto de 2018.

El trabajo de auditoría fue realizado bajo los estándares previstos en los procedimientos adoptados para la Oficina de Control Interno y en las actividades determinadas en el alcance de la auditoría, el cual fue expuesto en la reunión de apertura al Director de Tecnologías de la Información y las Comunicaciones junto con su equipo de trabajo.

Así mismo, se ejecutaron pruebas de recorrido con el fin de evaluar el diseño e implementación de los controles claves establecidos el proceso Gestión de TIC´s objeto de esta auditoría, basadas en la documentación soporte enviada por los responsables de las actividades del proceso.

En virtud de la mejora continua, la Oficina de Control Interno durante la auditoría desarrolló las pruebas descritas a continuación:

Planeación Estratégica de las Tecnologías de la Información y las Comunicaciones de TMSA

Se realizó prueba para revisar la Planeación Estratégica de las Tecnologías de la Información y las Comunicaciones de TMSA, de acuerdo con lo señalado en el Decreto 415 de 2016 de MINTIC.

Se verificó con soportes publicados en la Intranet y pagina web de la Entidad, el cumplimiento para la elaboración del PETIC de TRANSMILENIO S.A, con los lineamientos del Decreto 415 de 2016 – MINTIC.

Avance de los proyectos del PETIC de trimestres de culminación II/2017 y IV/2018.

Se realizó prueba para verificar que los alcances y entregables dentro de la muestra seleccionada para los trimestres II, IV de 2017 y III, IV de 2018 en etapa de culminación para los proyectos PETIC-TMSA.

Políticas Copias de Respaldo

Se revisó la existencia y cumplimiento de las políticas de copia de respaldo Backup de TRANSMILENIO S.A, acuerdo al numeral 9,6 del Manual de Seguridad de la Información M-DT-001 v2.

Políticas de Gestión y Continuidad en TI.

Se verificó la existencia de los procedimientos formales correspondientes para la Gestión de Continuidad de TI

Logs de Auditoria para verificar Accesos a los Sistemas de Información

Se verificó actividades de los usuarios, excepciones, fallas y eventos de seguridad de la muestra seleccionada los registros de logs de acuerdo con los lineamientos

Gestión de Cambios TI

Se verificó la existencia de los procedimientos formales correspondientes para la Gestión de Cambios y como resultado de la verificación al proceso Gestión de TIC´s, no fue posible evaluar la aplicabilidad, formalidad, efectividad, oportunidad y eficacia de lo establecido e indicado en el Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018, toda vez que el proceso Gestión de TIC´s no cuenta con un procedimiento formal para la Gestión de Cambios.

FORTALEZAS:

- Disposición para atender la auditoría por parte del director y personal TIC´s.

- Apoyo desde la Gerencia General a la Dirección de TIC´s para adelantar el plan estratégico de Seguridad de la Información

HALLAZGOS

HALLAZGO N° 1: Falta de Comité y procedimientos formales para Gestión de Cambios de Tecnología de la Información.

Descripción del hallazgo o situación encontrada para "Gestión de Cambios": La Oficina de Control Interno solicitó al proceso de Gestión de TIC´s los procedimientos para la Gestión de Cambios, mencionados en el Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018, para verificar el cumplimiento de:

1. *Numeral 8.9.4 Trabajo en áreas seguras Literal d) "Cualquier cambio, modificación, actualización, ajuste o soporte que se realice sobre los procesos, áreas seguras y sistemas de procesamiento de información, que puedan afectar alguno o todos los pilares de seguridad de la información (integridad, confidencialidad y disponibilidad) deben pasar por la aprobación del Comité de cambios antes de su ejecución."*
2. *Numeral 9.4.3 Migración a ambiente de producción Literal d) "Documento de control de cambios o documentación de implementación".*
3. *Numeral 9.5 Política de Seguridad en las Operaciones Literal d) "TRANSMILENIO S.A., debe implementar un proceso documentado para la gestión de cambios, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información".*
4. *Numeral 9.7 Política de Seguridad de la Información para las relaciones con los proveedores Literal h) "Toda gestión del proveedor que represente una modificación, mantenimiento, revisión al servicio de tecnología de la información, comunicaciones o equipos de suministros, debe pasar por el*

Procedimiento Gestión de Cambios y seguir las directrices del Líder u oficial de seguridad de la información, antes de su ejecución".

5. *Así mismo lo establecido en el numeral 12.1.2 Gestión de Cambios de Cambios "Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la seguridad de la información" de la NTC-ISO-IE 27001-2013.*

Como resultado de la verificación al proceso Gestión de TIC´s, no fue posible evaluar la aplicabilidad, formalidad, efectividad, oportunidad y eficacia de lo establecido en el Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018 y a lo establecido en el numeral 12.1.2 de la NTC-ISO-IE 27001-2013, toda vez que no se ha conformado el Comité de Cambios y no existe procedimiento formal para la Gestión de Cambios.

Criterios aplicados: *Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018 y Norma NTC-ISO-IE 27001-2013. (Anexo A 12.1.2) "Gestión de Cambios"*

Posible causa identificada por la Oficina de Control Interno: Debilidad en la aplicación de la normatividad de la seguridad de la Información al Interior de TRANSMILENIO S.A.

Descripción del riesgo:

1) Fallas en la confiabilidad de los sistemas de información y
2) Fallas de Seguridad en la Tecnología de información TI.

Descripción del impacto:

1) Posible materialización de riesgo en la integridad de la Información, toda vez que un cambio en un sistema de información sin el debido procedimiento, análisis de impacto

en el sistema o autorización podría acarrear cambios no deseados. Así mismo cuando se transfiere un sistema de información de una etapa de desarrollo a la de producción sin el debido proceso se pueden afectar la información de forma incorrecta.

2) Vulnerabilidad en la Seguridad de la Información TI, en casos como: Actualizaciones de Sistemas Operativos y Motores de Bases de Datos entre otros, los cuales pueden contener problemas de seguridad no detectados por el proveedor, en el momento de entregarlos para su instalación.

Recomendaciones:

1. Elaborar un procedimiento de "Gestión de Cambios", que incluya responsabilidades para asegurar el control satisfactorio de todos los cambios realizados en TI. Es importante considerar que dicho procedimientos contenga:
    a. Cambios de emergencia
    b. Parches de los Sistemas operativos y motores de bases de datos
    c. Documentación de todos los cambios realizados
    d. Autorizar los cambios por las personas interesadas y el oficial de Seguridad.
    e. Seguimiento a los cambios y cambios de estatus

2. Implementar el Comité de cambios, donde se adelanten reuniones periódicas y el cual incluya la participación coordinada e interdisciplinaria de un equipo de la Dirección de Tecnologías de la Información y las Comunicaciones, el oficial de la Seguridad de la Información y las partes interesadas. Así mismo elaborar las actas respectivas que plasmen las decisiones tomadas en dicho comité.

HALLAZGO N° 2: Falta de procedimientos formales para Gestión de Continuidad de Tecnología de la Información.

Descripción del hallazgo o situación encontrada: La Oficina de Control Interno solicitó al proceso de Gestión de TIC´s, mediante correo de fecha martes 18/09/2018 5:03 p. m, los procedimientos para la Gestión de Continuidad de TI, mencionados en el Manual de

Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018, para verificar el cumplimiento del numeral 9.9 "Política de Gestión de Continuidad del Negocio TI" de los siguientes literales:

c.) La Dirección de Tics, debe elaborar el plan de recuperación ante desastres y retorno a la normalidad, para cada uno de los servicios y sistemas de información que tengan un impacto alto en los procesos de la entidad.
d.) Debe asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización y la documentación de dichas pruebas.
e.) Debe verificar a intervalos regulares los controles de Continuidad de la Seguridad de la Información, implementados con el fin de asegurar que son válidos y eficaces durante situaciones adversas.
f.) Se debe establecer, documentar y mantener procesos, procedimientos para asegurar el nivel de Continuidad requerido para la Seguridad de la Información durante una situación adversa.

Como resultado de la verificación al proceso Gestión de TIC´s, no fue posible evaluar la aplicabilidad, formalidad, efectividad, oportunidad y eficacia de lo establecido e indicado en el Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018, toda vez que el proceso Gestión de TIC´s no cuenta con un procedimiento formal para la Política de Gestión de Continuidad del Negocio.

Criterios aplicados: Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.

Posible causa identificada por la Oficina de Control Interno: Falta de direccionamiento en los mecanismos de formulación, comprobación, actualización y seguimiento por parte de los procesos Gestión de TIC´s asociados a la Continuidad de TI en TRANSMILENIO S.A.

Descripción del riesgo: Falta de unificación de criterios para mantener la continuidad de tecnología de la Información.

Descripción del impacto:

1. Que no se pueda minimizar el número de procesos críticos de TRANSMILENIO S.A que dependen de Tecnología de la Información, por no estar cubiertos por un plan de continuidad TI.

Recomendaciones:

De acuerdo al numeral 9.9 “Políticas de Gestión de Continuidad de Negocio” del Manual de Políticas de Seguridad y Privacidad de la Información código M-DT-001 versión 2 de Julio de 2018, aplicar lo referente a:

1) Elaborar los Planes de recuperación ante desastres y retorno a la normalidad para todos los servicios y sistemas de información que tengan alto impacto en los procesos de TRANSMILENIO S.A. teniendo en cuenta
   a. Acciones a realizar mientras TI este recuperando los servicios.
   b. Asegurarse que los dueños de la información entienden los tiempos de recuperación de TI.
   c. Lograda la exitosa reanudación de TI, valorar y actualizar lo adecuado del Plan.

2) Programar y realizar pruebas de los planes establecidos para la recuperación de desastres en TI.

3) Verificar que los planes establecidos para la recuperación de desastres en TI continúen siendo vigentes a través del tiempo (Actualización permanente). Así mismo que los cambios en los procedimientos y las responsabilidades sean comunicados de forma clara y oportuna.

4) Verificar periódicamente que los planes establecidos para la recuperación de desastres en TI correspondan a las necesidades de los procesos de TRANSMILENIO S.A

Al elaborar los planes de continuidad de TI, considerar el procesamiento alternativo y la capacidad de recuperación de todos los servicios críticos de TI, también cubrir los roles y responsabilidades, los procedimientos, los procesos de comunicación y el enfoque de pruebas.

HALLAZGO N° 3: Incumplimiento al literal (f) del numeral 9.6 del Manual de Seguridad de la Información M-DT-001 versión 2 de Julio de 2018 en cuanto a Backup´s y pruebas de Restore.

Descripción del hallazgo o situación encontrada: La Oficina de Control Interno verificó al proceso de Gestión de TIC´s, el día martes 24/09/2018, el cumplimiento de las políticas de Backup y Restore, mencionadas en el literales a, b, c, e y f del numeral 9.6 del *Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018,* encontrando como resultado que no existe evidencia documentada en relación al literal (f) el cual indica que: "Es responsabilidad de quien (es) ejecute (n) el rol de Administrador de Backup realizar pruebas de restauración de copias de seguridad de manera trimestral siguiendo los lineamientos del Procedimiento Backup y Recuperación de la Información".

El incumplimiento del literal (f) obedece a que una vez verificada la información oficial en intranet y realizada una reunión de entendimiento con el auditado se evidenció que:

1. No se encontró documentado el proceso de restauración de copias de seguridad de manera trimestral como lo define el literal f del numeral 9.6 del Manual de Seguridad de la Información M-DT-001 v2.

2. No se encontró a la fecha de la auditoría que se realicen pruebas formales de restauración de los Backup de la información de los usuarios, almacenada en la unidad (\\server-file\Dependencia)(P:), ni de las bases de datos corporativas de TMSA, donde se utilicé el Backup tipo: FULL y los respectivos Backup tipo: INCREMENTALES, para restaurar una instancia de las bases de datos corporativas. como lo indica el numeral "7,4

Procedimiento de toma de Backup de archivos de los usuarios del procedimiento P-DT-007 versión 2 de fecha junio de 2017".

4. No se encontró a la fecha de la auditoría que se realicen pruebas formales de la efectividad del Backup de las bases de datos corporativas llevadas a la nube (Google).

Criterios aplicados:

1. Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.
2. Protocolo a seguir para la administración de Bases de Datos T-DT-004 V2, abril 2018.
3. Protocolo a seguir para gestionar el uso de los Medios Removibles T-DT-003 V0, Dic 2017.
4. Procedimiento administración de usuarios P-DT-007 V2, junio 2017.

Posible causa identificada por la Oficina de Control Interno: Falta de aplicación estricta para dar cumplimiento al *Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.* concerniente a realizar pruebas de restauración, comprobación, actualización y seguimiento por parte del proceso Gestión de TIC´s a las Políticas de Backup´s y "Restore" en TRANSMILENIO S.A.
Descripción del riesgo: Que no pueda recuperar la información de las copias de seguridad, lo cual podría impactar en la continuidad e integridad de los servicios ofrecidos por TI.

Descripción del impacto:
1. No poder garantizar la continuidad de servicio que satisfaga el requerimiento del Negocio para asegurar el mínimo impacto en caso de una interrupción de servicios de Tecnología de la Información.

Recomendaciones:

Las siguientes recomendaciones son basadas en los criterios del *Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018*.

1. Elaborar los procedimientos de restauración de la información y/o pruebas de efectividad de los Backup, tanto para los archivos de usuarios como para las bases de datos corporativas. (Literal a) Numeral 9.6)

2. Realizar pruebas de restauración, comprobación, actualización y seguimiento por parte del proceso Gestión de TIC´s a las Políticas de Backup´s y "Restore" en TRANSMILENIO S.A, dejando evidencia escrita para tal fin. (Literal f) Numeral 9.6)

3. Socializar con los dueños de la información el tiempo máximo de posible pérdida de información, que se deriva de las actividades técnicas del Backup de la Información. (Literal d) Numeral 9.6)

4. Realizar visitas periódicas al custodio externo para verificar las condiciones físicas y medioambientales en que se encuentran los respaldos de la información. (Literales b, c y h) Numeral 9.6)

5. Considerar incrementar el porcentaje de cintas que se destinan para el custodio externo, toda vez que en la actualidad se encuentra en las instalaciones de TRANSMILENIO S.A EL 90% de las cintas magnéticas de Backup. (Literales b, c y h) Numeral 9.6) y Experto Técnico Equipo Auditor.

6. Concientizar al administrador de cada sistema de información de validar periódicamente que su sistema de información se encuentre debidamente respaldado, de acuerdo con lo indicado en el *literal (d) del numeral 9,6 "Políticas Copias de Respaldo - del Manual de Seguridad de la Información M-DT-001 versión 2 de Julio de 2018 la y en concordancia a la NTC-ISO IE 27001-2013 y GTC-ISO/IE 27002-2015.*

HALLAZGO N° 4: Incumplimiento a las Políticas de Operación del numeral 6 del *“Procedimiento para el monitoreo del uso de los medios de procesamiento de*

información" código P-DT-010 versión 0 de noviembre de 2015 ", concernientes al tema de "Logs" de TRANSMILENIO S.A.

Descripción del hallazgo o situación encontrada: La Oficina de Control Interno verificó al proceso de Gestión de TIC´s, entre los días 2 al 8 de octubre de 2018, el cumplimiento de las políticas de Logs, mencionadas en los numeral 6, 6.1, 6,2, y 6.3 del "*Procedimiento para el monitoreo del uso de los medios de procesamiento de información*", Código P-DT-010 versión 0 de noviembre de 2015 lo concordante a las políticas de operación de Logs, sin encontrar evidencia documentada de las siguientes actividades:

- *Parametrización de los eventos que se guardarán para monitoreo y/o auditorías.*
- *Análisis de monitoreo periódico por cada parte interesada para detectar incidentes.*
- *Comité de logs con sus respectivos lineamientos.*
- *Seguridad de los registros de logs.*
- *Acuerdos de los líderes de los procesos con la Dirección de TIC´s para determinar los periodos de retención.*

Las cuales se deben realizar con los administradores de las aplicaciones, bajo la orientación de la Dirección de TIC´s.

Por lo anterior se configura un incumplimiento a los numerales anteriormente citados del *“Procedimiento para el monitoreo del uso de los medios de procesamiento de información"* vigente a la fecha de la auditoría “*Código P-DT-010 versión 0 de noviembre de 2015.*

Nota: En virtud de lo manifestado por el auditado en cuanto a encontrarse esté procedimiento en etapa de ajuste; la auditoría expresa la importancia de contar con estas actividades para los procedimientos de TRANSMILENIO S.A, toda vez que no se pueden eliminar, dado su grado de relevancia en materia de constituirse en lineamientos claves para el Sistema de Control Interno de TRANSMILENIO S.A.

Criterios aplicados:

1. Procedimiento código P-DT-010 versión 0 de noviembre de 2015 "Procedimiento para el monitoreo del uso de los medios de procesamiento de información".

2. Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.

Posible causa identificada por la Oficina de Control Interno: Debilidad en la aplicación estricta de las políticas de Logs por parte del proceso Gestión de TIC´s a los procesos en TRANSMILENIO S.A.

Descripción del riesgo: Que no se pueda contar con el registro adecuado para el monitoreo de las actividades de los usuarios en los diferentes sistemas de Información de TRANSMILENIO S.A.

Descripción del impacto:

1. No poder administrar los problemas y/o posibles eventos en los sistemas de información, al no mantener unas adecuadas pistas de monitoreo y/o auditoria que permitan rastrear, analizar y determinar la causa raíz de los incidentes.

Recomendaciones:

Realizar y hacer seguimiento estricto documentado a la totalidad de las actividades descritas en los numerales 6, 6.1, 6,2, y 6.3 del "*Procedimiento para el monitoreo del uso de los medios de procesamiento de información"*. Código P-DT-010 versión 0 de noviembre de 2015, que se describen a continuación:

- *Determinar y parametrizar los eventos que generarán registros de auditoría en los medios de procesamiento de información y los sistemas de información de TRANSMILENIO S.A.*
- *Definir la periodicidad del monitoreo de los registros de auditoria sobre los aplicativos donde operan los procesos administrativos de TRANSMILENIO S.A.*
- *Determinar los periodos de retención de los registros (logs) de auditoria de los medios de procesamiento de información administrados y los sistemas de información de la entidad.*
- *Habilitar los registros de auditoría y sistemas de monitoreo de los medios de procesamiento de información administrados, acorde a los lineamientos establecidos por el comité de revisión de logs.*
- *Revisar periódicamente los archivos de logs de las aplicaciones a su cargo, con el fin de establecer posibles eventos, incidentes, amenazas a la seguridad de la información o problemas de capacidad entre otros.*
- *Registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros, de acuerdo con las directrices establecidas por la Dirección de Tecnologías de la Información y la Comunicación.*
- *Analizar los resultados de cada monitoreo efectuado y generar un plan de acción para a los incidentes reportados según la clasificación de los mismos establecidos en la Política Gestión de Incidentes de Seguridad de la Información.*
- *Velar por el cumplimiento de la integridad, disponibilidad y confidencialidad de los registros de auditoria generados en la plataforma tecnológica y los sistemas de información del TRANSMILENIO S.A. Estos registros deben ser almacenados y su acceso debe ser restringido.*
- *Actualizar el procedimiento al menos una (1) vez al año.*
- *Almacenar en librerías de Backup y autorizar el acceso a los administradores de los medios de procesamiento de información.*
- *Registrar las actividades del administrador, que muestren los tiempos de inicio y terminación de los procesos, tiempos de inicio del sistema, cambios en la configuración del sistema, errores y acciones correctivas.*
- *Cuando se trate de desarrollos a la medida se recomienda contemplar como obligación contractual, la implementación y/o actualización, de un log o bitácora de auditoria para la aplicación en construcción.*

HALLAZGO N° 5: Accesos no autorizados al sistema de información ERP-JSP7 de TRANSMILENIO S.A.

Descripción del hallazgo o situación encontrada: La Oficina de Control Interno realizó al proceso de Gestión de TIC´s, entre los días 10, 11 y 12 de octubre de 2018 pruebas a los logs del aplicativo ERP-JSP7 de los módulos contabilidad, tesorería y presupuestos del periodo 01 de septiembre de 2017 al 31 de agosto de 2018, para verificar el cumplimiento de las políticas de control de acceso a este sistema de información, evidenciando, contra la lista de personal retirado y novedades, accesos no autorizados al sistema de información ERP-JSP7 para cinco (5) personas retiradas y un (1) en incapacidad.

Por lo anterior se configura un incumplimiento en materia de seguridad de la información que infringe los controles establecidos en los literales j, e y h del numeral 8.4.1 "Requisitos del negocio para control de acceso" y literal s) 8.4.4 Control de acceso a sistemas y aplicaciones del numeral del *Manual de Políticas de Seguridad y Privacidad de la Información código M-DT-001 versión 2 de julio de 2018 adoptado y vigente para TRANSMILENIO S.A.*

8.4.1 Requisitos del negocio para control de acceso
Literal j) Los derechos de acceso a la información de todos los funcionarios de planta, contratistas y usuarios externos a la Entidad se deben cancelar al terminar su vinculación como empleado, contrato o acuerdo, o se deben ajustar cuando se requieran cambios, previamente solicitados por el área o profesional responsable.

Literal e) Quien (es) ejecute (n) el rol de Administrador de recursos informáticos debe (n) velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red. Quien (es) ejecute (n) El rol de Administrador de control de acceso lógico podrá (n) realizar una verificación de los

controles de acceso de los funcionarios públicos, oficiales, proveedores, contratistas y terceras partes en la periodicidad que se establezca para ello, a fin de cerciorarse que dichos usuarios acceden solamente a los recursos autorizados para la realización de sus tareas, funciones u obligaciones; así mismo debe realizar la deshabilitación o suspensión de aquellos usuarios que contando con acceso activo, presenten cualquier tipo de novedad que así lo amerite.

Literal h) Los perfiles y derechos de acceso serán revisados periódicamente (anualmente) por el área de soporte de la dirección de TIC´s y los propietarios de la información. Adicionalmente, es responsabilidad del usuario, informar cualquier privilegio que no corresponda con su perfil para que sea ajustado.

8.4.4 Control de acceso a sistemas y aplicaciones
Literal s) No está permitido facilitar el usuario o la contraseña a otra persona para adelantar cualquier labor en los sistemas de información

Criterios aplicados:

1. Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018.

Posible causa identificada por la Oficina de Control Interno: Debilidad en la desactivación de los usuarios por parte del proceso Gestión de TIC´s en los sistemas de información de TRANSMILENIO S.A.

Descripción del riesgo: Suplantación de Identidad de los empleados y/o terceros con los usuarios retirados de TRANSMILENIO S.A, en los sistemas de información.

Descripción del impacto:

Afectación de las operaciones, transacciones y demás actividades asociadas a los sistemas de información, por no realizar una efectiva administración de cuentas que garantice que se gestionan las desactivaciones, suspensiones, modificaciones y cierre de cuentas de usuario por motivo de retiro y/o desvinculación en TRANSMILENIO S.A.

Acceso a consulta de información considerada como critica de TRANSMILENIO S.A.

Recomendaciones:

1. Aplicar con rigurosidad los controles establecidos en los numerales 8.4.1, 8.4.2, y 8.4.4 del Manual de Políticas de Seguridad y Privacidad de la Información Código M-DT-001 Versión 2 de fecha Julio de 2018, en especial lo relacionado con:

a. Revisiones periódicas por el área de soporte de la dirección de TIC´s y partes interesadas.

b. Velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red.

HALLAZGO N° 6: Subproyecto PETIC Vigencias Futuras no desarrollado en la fecha programada III trimestre de 2017.

Descripción del hallazgo o situación encontrada: La Oficina de Control Interno realizó, entre los días 23, 24 y 25 de octubre de 2018, el seguimiento al cumplimiento de los alcances y/o entregables dentro de la muestra seleccionada para el los trimestres II, IV de 2017 y III, IV de 2018 en etapa de culminación a los proyectos PETIC de TMSA, y como resultado evidenció que para la "RUTA ADMINISTRATIVA el subproyecto "Vigencias Futuras" no se desarrolló, ni se actualizó su respectivo cambio en el anexo del PETIC publicado en la página web de TRANSMILENIO S.A

Por lo anterior se configura un incumplimiento a lo citado en el numeral 5.9.1.5 "Ruta Administrativa" al no desarrollar el subproyecto en la fecha proyectada (III trimestre de 2017) del "Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETIC) código T-DT-005 versión 0 de fecha de actualización julio de 2018". Así mismo incumplimiento a los controles del mapa de riesgos de gestión del proceso Gestión TIC´s aplicables a los siguientes riesgos:

Riesgo #2 *"Que el plan estratégico de tecnologías de la información y las comunicaciones no se desarrolle"*
Controles:
Que la formulación, consolidación o presentación del PETIC no se haya desarrollado satisfactoriamente.
Negligencia, desconocimiento o indecisión para el desarrollo de las actividades plateadas en el PETIC
Que las condiciones para el cumplimiento del PETIC hayan cambiado de su formulación al momento de su implementación.
Riesgo #3 *"Falta en la Planificación o en el Seguimiento a la Gestión institucional."*
Controles:
Bajo nivel de planeación en la determinación de las TIC's

Criterios aplicados:

1. Plan Estratégico de Tecnologías de la Información y las Comunicaciones (PETI) código T-DT-005 versión 0 de fecha de actualización julio de 2018.

2. Mapa de Riesgos de Gestión del Proceso Gestión de TIC´s. versión 2 de fecha de actualización 22 de marzo de 2018.

Posible causa identificada por la Oficina de Control Interno: Falta de Monitoreo al desarrollo y avance de los subproyectos que hacen parte integral de las proyectos del PETIC de TRANSMILENIO S.A.

Descripción del riesgo: Que el plan estratégico de tecnologías de la información y las comunicaciones no se desarrolle y Falta en la Planificación o en el Seguimiento a la Gestión institucional.

Descripción del impacto:

1. Inadecuada asociación y seguimiento a los subproyectos del PETIC de TRANSMILENIO S.A. con los planes estratégicos de acción, de adquisiciones, ascenso tecnológico y avance de resultados.

2. Materialización de los riesgos de gestión que el proceso Gestión de TIC´s ha identificado.

Recomendaciones:

1. Priorizar la ejecución de actividades por fecha de culminación para los proyectos del PETIC de TRANSMILENIO S.A, así mismo monitorear de manera estricta los avances de metas de la Planeación Estratégica de Tecnología de la Información, realizando los ajustes respectivos y priorizando la ejecución de actividades por fecha de culminación para los proyectos del PETIC de TRANSMILENIO S.A.

2. Adelantar un plan de contingencia como opción de tratamiento de los riesgos del proceso de acuerdo a las disposiciones actuales del “Manual para la Gestión de Riesgo código M-OP-002 versión 1 de fecha diciembre de 2017", numerales 5.8 Opciones de Tratamiento de Riesgos y 6.5 Tratamiento de los Riesgos.

RESUMEN DE HALLAZGOS:

N°	Título de Hallazgo	Repetitivo
1	Falta de Comité y procedimientos formales para Gestión de Cambios de Tecnología de la Información	No
2	Falta de procedimientos formales para Gestión de Continuidad de Tecnología de la Información.	No
3	Incumplimiento al literal f del numeral 9.6 del Manual de Seguridad de la Información M-DT-001 versión 2 de Julio de 2018 en cuanto a Backup´s y pruebas de Restore.	No
4	Incumplimiento a las Políticas de Operación del numeral 6 del "Procedimiento para el monitoreo del uso de los medios de procesamiento de información" código P-DT-010 versión 0 de noviembre de 2015 ", concernientes al tema de "Logs" de TRANSMILENIO S.A.	No
5	Accesos no autorizados al sistema de información ERP-JSP7 de TRANSMILENIO S.A.	No
6	Subproyecto PETIC Vigencias Futuras no desarrollado en la fecha programada III trimestre de 2017.	No

El presente informe fue comentado y socializado con el director de la Dirección de TIC´s.

OBSERVACIONES.

Observación No. 1: *"**Desactualización de la referencia cruzada documentación"*** Se evidencia que el numeral *7.5 "Procedimiento de cambio de contraseña (password)" del Procedimiento código P-DT-007 versión 2 de fecha junio de 2017 contiene una referencia*

que esta desactualizada (remite a la versión 1 del procedimiento M-DT-001, la cual no está vigente)

Recomendación: Actualizar la referencia cruzada del Procedimiento código P-DT-007 versión 2 de fecha junio de 2017, con la versión 2 del actual y vigente manual *"Políticas de Seguridad y Privacidad de la Información código M-DT-001 de fecha julio de 2018".*

Observación No. 2: ***"Control en la Segregación de funciones de terceros ERP-JSP7"*** Una vez verificada la no aplicación de las políticas de control de cambios evidenciadas en el hallazgo número No. 1 de este informe, se constató que los registros de solicitud de soporte de usuarios oficialmente establecidos por la mesa de ayuda disminuyeron y se canalizaron directamente con la persona asignada por la empresa de atender el soporte al ERP-JSP7, que es la misma persona que recibe, atiende, aprueba, y entrega la solución, lo cual puede afectar las validaciones previas que se deben surtir por parte del área de Tecnología de la Información y los usuarios finales.

Recomendación: Establecer entre la Dirección corporativa y el proceso Gestión de TIC´s los lineamientos y criterios para adelantar el desarrollo del soporte técnico ERP-JSP7, guardando los principios de segregación de funciones e interacción administrativa de trazabilidad.

Observación No. 3: "Debilidad de conocer el Backup más antiguo, tanto de las Bases de Datos corporativas, como de los archivos de usuarios". Derivado del proceso de verificación al cumplimiento de las políticas de Backup y Restore del hallazgo No. 3 de este informe, el equipo auditor solicitó evidencia que permitiera conocer el Backup más antiguo, tanto de los archivos de usuarios como de las bases de datos de los Sistemas de Información de la Entidad; por lo cual se conoció con prontitud solo lo referente a los respaldos de los archivos de usuarios, mientras que lo referente a las bases de datos corporativas, no se pudo conocer dado que no se contaba con el Inventario de la información mínima relevante de recuperación de todos los Backup de TRANSMILENIO S.A.

Recomendación: Realizar un inventario y depuración de los registros Backup, con la implementación de un procedimiento de registro y control de éstos donde quede registrada la información referente al Backup (tipo, contenido, fecha de realización, tiempo de retención entre otros), de tal modo que se pueda consultar fácilmente información relevante de cada Backup.

Observación No. 4: "Usuarios Genéricos en los Sistemas de Información Corporativos."

En el ejercicio de la Auditoría, se evidenció el uso frecuente de los usuarios genéricos en los Sistemas de Información de la Entidad, lo cual es una práctica corporativa generalizada, sin embargo, se deben implementar algunos controles que permitan asegurar el acceso exclusivo a personal activo y autorizado.

Recomendación: Evaluar este tipo de accesos para que solo se permitan, cuando sean estrictamente necesarios por razones operativas o de negocio, así como establecer el cambio periódico de sus contraseñas, para evitar que personas que ya se hayan retirado de la empresa, las puedan seguir utilizando.

OPORTUNIDADES DE MEJORA

Oportunidad de mejora No. 1 Riesgos de Gestión:

Evaluar y aplicar la identificación, valoración y diseño de riesgos de gestión bajo la metodología Riesgos de la vigencia 2018 emitida por Departamento Administrativo de la Función Pública 2018, en el marco de los lineamientos MIPG que aplican para las entidades del Distrito. Así mismo considerar las observaciones y recomendaciones del informe 050 de 2018 de la Oficina de Control Interno descritas para los siguientes riesgos:

- *Que la planeación tecnológica no sea acorde con las funciones, actividades, responsabilidades o desarrollo de la Empresa.*
- *Falta en la Planificación o en el Seguimiento a la Gestión institucional*.
- *Que no se pueda mantener la continuidad o integridad en las tecnologías de la información*.
- *Que no se altere el estado de los activos de información de la empresa*
- *Que los servicios de la infraestructura tecnológica no sean apropiados al desarrollo de las funciones de la empresa*.
- *Que no se puedan atender las necesidades o requerimientos de los usuarios de las tecnologías de información y las comunicaciones.*

Lo anterior con el propósito de fortalecer los riesgos actuales e incorporar los correspondientes que se están desarrollando en virtud de: "*El Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información -SGS, código T DT-007 versión 0 de fecha agosto de 2018 y del Plan Estratégico de Seguridad de la Información (PESI) código T-DT-006 versión 0 de fecha julio de 2018.*

Oportunidad de mejora No. 2.

Adelantar las acciones necesarias para garantizar el mantenimiento y actualización que se deriva de las nueve (9) soluciones de proyectos para el "Control de Flota de TransMilenio" oficializado en el plan tecnología de la información propuesto para culminar en la vigencia 2019 y 2020.

- De acuerdo con lo evidenciado en el control de seguimiento, el PETIC no contempla el mantenimiento y actualización para las nuevas soluciones, que se requieren para las vigencias 2019 y 2020.

La Dirección de Tics remitió el plan de mejoramiento resultante de los seis (6) hallazgos, no obstante, consideramos que, por su impacto en la Entidad, se podrían implementar acciones sobre las oportunidades de mejora y las observaciones.

Los hallazgos y observaciones relacionados en el presente informe corresponden a la evaluación realizada conforme a la Planeación del trabajo de Auditoría dentro del alcance establecido, por lo tanto, es responsabilidad del área auditada, efectuar una revisión de carácter general sobre los aspectos evaluados.

Cualquier información adicional con gusto será suministrada.

Bogotá D.C., 1 de noviembre de 2018.

Luis Antonio Rodríguez Orozco

Jefe Oficina de Control Interno

Elaboró: Germán Ortíz Martín, Auditor de la Oficina de Control Interno.

Experto técnico Ing. Jorge Iván Florez Franco Auditor Oficina de Control Interno.

Código: 801.01-5-5.2