N° INFORME: OCI-2018-059

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

EQUIPO AUDITOR: Germán Ortíz Martín, Auditor Líder de la Oficina de Control Interno y Gilberto Antonio Padilla Castro, Auditor acompañante de la Dirección Técnica de Buses y Greecy Andrea Rivera Barbosa como Experto técnico de la Oficina de Control Interno.

FECHAS:

Reunión de apertura: 18 de junio de 2018

Ejecución de la Auditoría: Desde el 18 al 22 de junio de 2018

Reunión de Cierre: 29 de junio de 2018.

INFORME DISTRIBUIDO A: Subgerente General – Director TIC´s

OBJETIVO:

Verificar el grado de cumplimiento y/o conformidad del Sistema Integrado de Gestión implementado en la Entidad en el Proceso de Gestión TIC´s (Subsistemas de: Gestión de Calidad, Gestión Medio Ambiental, Gestión de Salud y Seguridad en el Trabajo, Gestión Documental, Responsabilidad Social) (lo aplicable del pacto global), Gestión de Seguridad de la Información y el MECI- Modelo Estándar de Control Interno.

ALCANCE:

El ciclo de auditorías SIG 2018 aplica al Sistema Integrado de Gestión implementado en la Entidad en el proceso de Gestión TIC´s, bajo los lineamientos aplicables de la NTD - SIG 001:2011 y se integra por los Subsistemas de: Gestión de Calidad (lo aplicable de la ISO 9001:08 y 15), Gestión Medio Ambiental (lo aplicable de la ISO 9001:08 y 15), Gestión de Salud y Seguridad en el Trabajo (lo aplicable de la OHSAS 18001:07),

Gestión Documental (Aplicación TRD aprobadas por el Archivo Distrital), Responsabilidad Social (lo aplicable del pacto global), Gestión de Seguridad de la Información (lo aplicable de la ISO/IEC 27001:13), Subsistema de Control Interno (MECI).

Bajo los requisitos de la actualización de las normas ISO 9001:2015 e ISO 14001:2015, la Oficina de Control Interno realizará recomendaciones encaminadas hacia la mejora continua en virtud de aquellos requisitos exigibles en tales normas, pero no exigibles en la versión 2008.

El corte de la evaluación se realizó al 30 de abril de 2018 y contiene únicamente pruebas generales, dado que por ser un proceso de complejidad técnica y aplicación transversal a TRANSMILENIO S.A, requiere un mayor tiempo de ejecución para abarcar profundidad de muestras y pruebas técnicas especializadas en tecnología de la información. Así mismo en virtud de haber realizado recientemente en marco de auditoria SIG al proceso de *"Evaluación y Gestión del Modelo de operación SITP" pruebas de seguridad de activos de información;* para este ejercicio de auditoría no se realizó esta prueba con el proceso de Gestión TIC´s.

CRITERIOS DE LA AUDITORÍA

- NTD -SIG 001:2011
- ISO 9001:2008 (15); ISO 14001:2007 (15); OHSAS 18001:2007; IEC/ISO 27001.
- 10 principios del Pacto Global.
- Ley 594 de 2000;
- Ley 1712 de 2014
- Ley 1581 Protección de datos personales.
- Ley 1273 Protección de la información y de los datos tecnologías de la Informa.
- Ley 527 Acceso y uso de los mensajes de datos
- Decreto 1499 de 2017 (7.1 Ambiente de Control),
- Decreto 1008 del 14 de junio de 2018 Mintic´s
- Directiva 011 Promoción y uso del software libre en el Distrito Capital

- Decreto 2693 Gobierno en Lí-nea de la República de Colombia,
- Decreto 619 Estrategia de Gobierno Electrónico de los organismos y de las entidades de Bogotá
- Decreto 316 Acciones para el Desarrollo de la Estrategia Distrital de Gobierno
- Decreto 2573 Estrategia de Gobierno en línea
- Resolución 419 Control de flota e Información al usuario - SIRCI y
- Directiva Presidencial 04 Política Cero Papel en la Administración Pública
- Decreto 1078 Decreto Único IT
- Decreto 415 Definición de los lineamientos para el fortalecimiento TI
- Caracterizaciones, procedimientos, protocolos, formatos del SIG del proceso Gestión Tics vigentes en la plataforma de intranet de TRANSMILENIO S.A.

RIESGOS DE LA AUDITORÍA:

a) Demora en la ejecución de la auditoría debido a documentación del proceso desactualizada y/o no controlada.
b) Demora en la realización de la auditoría debido a que la dinámica del proceso difiera de lo descrito en la caracterización del proceso desactualizada.
c) Incumplimiento al cronograma del ciclo de auditorías SIG debido a demoras y/o entrega errada de la información por parte del auditado.

DESCRIPCIÓN DEL TRABAJO REALIZADO:

De conformidad con el Plan Anual de Auditorías de la Oficina de Control Interno de la Entidad correspondiente al 2018 fue efectuada auditoría al proceso de Gestión TIC´s (Subprocesos de Planeación, Administración y Soporte de la Tecnología) y teniendo en cuenta el objetivo y alcance descritos anteriormente, se desarrollaron las siguientes actividades:

a) Entendimiento del proceso**:** Se llevó a cabo el entendimiento del proceso basado en la revisión documental del proceso publicada en la intranet al corte de la evaluación, y en entrevistas realizadas a los colaboradores responsables de las diferentes actividades del proceso.

b) Revisión documentación interna: Se consultaron las políticas, manuales, procedimientos y demás documentos internos definidos por TRANSMILENIO S. A, con el fin de verificar el cumplimiento de los procedimientos vigentes y los requisitos del proceso. De igual manera se consultó la normativa externa aplicable, con el fin de establecer el cumplimiento de la misma.

c) Identificación de riesgos y controles: Se identificaron los riesgos clave que pudieran impactar el proceso, así como la existencia de controles efectivos que mitiguen su materialización. De igual forma se realizó seguimiento a los planes de tratamiento de riesgos registrados en el mapa de riesgos del proceso Desarrollo Estratégico encontrando debilidades en la gestión del riesgo.

d) Diseño de programas de trabajo: Basados en el entendimiento adquirido del Proceso de Gestión TIC´s, se diseñó la programación del trabajo de auditoría SIG y las Listas de verificación cuyo contenido correspondieron a las diferentes pruebas de auditoría, de modo que a través de su ejecución nos permitieran determinar la existencia, funcionalidad y aplicación de los controles y requisitos identificados para el proceso.

e) Obtención y análisis de la información objeto de auditoría: Teniendo en cuenta la metodología definida por la Oficina de Control Interno de la Entidad, fue solicitada la información objeto de auditoría para seleccionar muestras con el fin de validar los controles claves y requisitos establecidos en el proceso. Lo anterior mediante aplicación de pruebas de observación, indagación y comparación dado el alcance de la auditoría.

f) Definición de no conformidades: Como parte del proceso de comparación entre el criterio (el estado correcto del requisito) y la condición (el estado actual). Teniendo en cuenta que durante la auditoría se encontraron diferencias entre ambos, esta fue la base para elaborar el informe.

g) Definición de observaciones: Surgieron como oportunidades de mejoramiento que pueden contribuir al fortalecimiento del Sistema de Control Interno de la Entidad.

h) Análisis y socialización del informe de auditoría con los líderes del proceso: Durante la semana del 18 al 22 de junio de 2018, se efectuaron reuniones con los líderes de proceso y/o responsables, con el objetivo de analizar cada una de las no conformidades y observaciones identificadas durante nuestra auditoría y el 25 de junio se socializó el informe con el director del proceso Gestión Tics y su equipo de trabajo.

i) Planes de mejoramiento: Se reiteró durante la reunión de cierre, que, para la implementación de las acciones correctivas, preventivas y/o de mejora derivada del presente informe los responsables del proceso deben elaborar el respectivo plan de mejoramiento de acuerdo con los lineamientos definidos por la Entidad y descritos en la última parte del informe.

CONCLUSIONES:

Mediante la auditoría realizada al Proceso de Gestión TIC´s, se logró evaluar el cumplimiento de los requisitos aplicables definidos en la NTD 01:2011, NTC ISO 9001:2008, NTC ISO 14001:2004, NTC OHSAS 18001:2007 y NTC ISO IEC 27001:2013, de acuerdo con las directrices de Calidad, Gestión Ambiental, Seguridad y Salud en el Trabajo y Seguridad de la Información, concluyendo que el proceso presenta debilidad en el grado de conformidad frente a los requisitos del Sistema Integrado de Gestión, encontrando oportunidades de mejora para el logro de los objetivos estratégicos trazados para el proceso evaluado. Algunos de los aspectos relevantes corresponden a estructura

organizacional (Toma de conciencia), aplicación y lineamientos en la administración de software, controles de seguridad de información, en la administración del riesgo, entre otros.

RECOMENDACIONES, OBSERVACIONES Y/O NO CONFORMIDADES:

No conformidad No. 1:

Debilidad en la Toma de conciencia organizacional

Asegurarse que las personas que realizan el trabajo bajo el control de la organización tomen conciencia de la política de calidad, los objetivos de calidad los mapas de riesgo y los aspectos de salud y seguridad en el trabajo como contaminación visual del puesto de trabajo y el consumo de alimentos en el mismo; según lo contemplado en el numeral 10.1 párrafos 5 y 6 del Manual del Sistema Integrado de Gestión versión 1 de noviembre de 2015, para generar conciencia y gestionar el cambio por parte de los servidores públicos y partes interesadas para la implementación sostenibilidad y el mejoramiento del Sistema Integrado de Gestión en la Entidad.

Se denota debilidad de conocimiento mínimo del SIG, específicamente en: 1) Misión, 2) Política del SIG, 3) ubicación en intranet de la política y la misio, 4) valores del código de ética, 5) ubicación y utilización de los mapas de riesgos, 6) Los objetivos de calidad, mapas de riesgo, 7) Directiva Cero papel, 8) Contaminación en el puesto de trabajo y 9) consumo de alimentos en el puesto de trabajo; esta situación se identificó mediante una prueba, aplicada a una muestra representativa de 19 personas con un nivel de confianza del 96% y un error del 9%, y utilizando como criterio de calificación que del total de respuestas el promedio por encima del 71% evidenciaría fortaleza de conocimiento mínimo del sistema Integrado de gestión (SIG) y el promedio por debajo del 70% debilidad de conocimiento mínimo del SIG, teniendo en cuenta que es una entidad que debe contar con un grado de madurez del SIG; encontrando como resultado un promedio del 62%.

Lo anterior incumple con lo establecido en la norma: NTC ISO 9001:2008 numeral 5.3 Política de Calidad y NTC ISO 9001:2015 en el numeral 7.3 Toma de conciencia de la norma: NTC ISO/IEC 27001:2013, literal a) Toma de conciencia por parte de los

servidores públicos y los servidores públicos del numeral 7.1. de la NTD 001:2001numeral 7 (Responsabilidad del TIC´s).

No conformidad No. 2:

Debilidad en el Control de Documentos.

Asegurarse que la documentación utilizada en las actividades de los subprocesos de Gestión TIC´s corresponda a los documentos controlados en el Sistema Integrado de Gestión SIG.

El sistema Integrado de Gestión ha establecido para garantizar su funcionamiento desde el tema documental el procedimiento P-OP-001 V2 de fecha julio de *2016 "Control de documentos oficiales del sistema integrado de gestión SIG"* el control de documentos o información:

Se evidenció debilidad en la utilización, codificación y disposición de los registros según se encuentran documentados en el SIG, encontrando específicamente los siguientes hechos, que contravienen lo señalado en la norma:

- Solicitud de actualizaciones del SIRCI**:** Se observa que el formato código RDT-001 Solicitud de Actualizaciones SIRCI, es diligenciado por el concesionario RBSAS, señalando los cambios o actualizaciones que se hacen de los diferentes aplicativos, no obstante, no corresponde con la versión del formato registrado en el control de documentos del proceso.
- Se observó que los formatos: 1) "*Código R-DT-004 Especificación de Requerimientos de Software-ERS de fecha Dic-17 y2) Código R-DT-005 Plan y* identificamos que existe el formato código *"R-DT-006 Inventario de Software Ejecución de Pruebas de Aceptación Dic-2017"*, no presentan identificación de la versión, ni la fecha de actualización del formato registrado, lo que evidencia que no son controlados por el SIG.

- En cuanto al Inventario de Software, se observa en producción la herramienta *“Proactivanet”* utilizada para el control de inventario de software y hardware, adicionalmente*”* adoptado para el Sistema Integrado de Gestión el cual no cumple con lo establecido en el numeral 5. del Décimo primer lineamiento *"Inventario de Activos de Información" del Sistema Integrado de Gestión Distrital (mayo 2015) y los numerales 8.7.1. y 8.7.2. del Manual de Políticas de Seguridad de la Información (M-DT-001-1 Manual Seguridad de la Información), respecto de: "(...) 8.7.1. Cada uno de los activos debe estar clasificado como: Misión crítica, No-Crítica. Las auditorías periódicas al inventario de software se deben efectuar para dar cumplimiento a la ley sobre software licenciado. 8.7.2. Todos los activos de información deben ser justificados y tener asignado un propietario. TRANSMILENIO S.A. debe identificar a los propietarios para todos los activos de información y asignar la responsabilidad del mantenimiento de los controles para la adecuada protección de éstos. Se debe elaborar y mantener el inventario de activos identificando los propietarios y custodios de los activos, directivos o gestores responsables de proteger los activos, ubicación, número de serie, número de versión, estado de desarrollo / pruebas / producción (...)".*

  En virtud de lo anterior, la Oficina de Control, interno evidenció un hallazgo producto de la evaluación realizada al proceso *“Evaluación y Gestión del Modelo de operación SITP” en el marco de auditorías del SIG-2018.*

  Lo anterior incumple con lo establecido en la norma: NTC ISO 9001: 2008 numeral 4.2.4 Control de los registros ISO 9001:2015 7.5.3.1 literal a) Control a la información documentada intencionadas, 7.5.3.2 literal a, b, c y d; 7.5.3; NTC ISO 9001:2008 numeral 4.2.4 Control de documentos, NTC ISO/IEC 27001:2013 7.5.3, Anexo A (A8-A8.1., A8.1.1.), Anexo A (A8-A8.1., A8.1.2.). NTD 001:2001 4.2.4 Planificación documental del SIG. (Responsabilidad del TICS).

No conformidad No. 3:

Debilidad en la uniformidad y control del desarrollo de software

Unificar y liderar las políticas de TIC´s, dada las competencias estipuladas en el Artículo décimo tercero del Acuerdo 007 de 2017, mediante el cual se establece que la dirección de TIC´s debe dirigir, en coordinación con los ámbitos de la Alta Gerencia, Gerencia de Integración y Dirección y Control de la Operación, la planeación, desarrollo e implementación de tecnologías de la información y comunicaciones con el propósito de unificar y liderar bajo la dirección de TIC´s, los desarrollos de software que requiera TRANSMILENIO S.A.

Mediante el procedimiento compra y actualización de software Código: P-DT-005, se establecen como objetivo las actividades y responsabilidades para la compra o actualización de las herramientas informáticas (software) requeridas para el desarrollo de las tareas asignadas y reportadas como necesarias para la gestión institucional.

Se observó desarticulación para el control y desarrollo de software en relación con las políticas de TIC´s, lo anterior se evidencia en prueba de verificación adelantada en la Dirección de Buses y la Dirección e BRT, cuyos desarrollos están tratándose de manera independiente en cada dirección.

Lo anterior incumple lo establecido en los numerales de las normas: NTC ISO 9001:2015 numeral 8.3.2 “Planificación del diseño y desarrollo” literales e) y f), NTC ISO 9001:2008 numeral 7.3.1 “planificación del diseño y desarrollo”, NTC ISO 27001: 2013 numeral 6.2. literal c y d Objetivos de Seguridad de la información y planes para lograrlos, NTD 001:2001 numeral 4.2.2 Planificación de la Gestión del Riesgo. (Responsabilidad del TICS).

No conformidad No. 4:

Debilidad en el control y administración de Aplicaciones (ACCES)

Administrar desde la dirección de TIC´s el liderazgo de los procesos de desarrollo, mantenimiento y soporte de la plataforma de TIC´s de la Empresa, velando por la funcionalidad, confiabilidad, oportunidad y seguridad de la operación del software, hardware y comunicaciones.

La caracterización tiene como propósito identificar las actividades clave que permitan asegurar *"Administración de las Tecnologías de la Información y Las Comunicaciones"* de fecha diciembre de 2014 en su ciclo PHVA contiene la actividad del hacer (H) *"Administrar la infraestructura tecnológica (servidores, bases de datos,* aplicaciones, *redes de datos, equipos de comunicaciones, cámaras, planta telefónica, ups´s, etc) de la Entidad"*, entre otras.

Se evidenció debilidad de control y administración de la aplicación ACCES la cual es de uso y manejo actual por parte de la Subgerencia Económica para la liquidación previa de los agentes del sistema TRANSMILENIO S.A, de modo que esta aplicación es de total autonomía en administración, creación y asignación de usuarios de la Subgerencia Económica, por consiguiente contradice lo expuesto en el numeral 8.4.5.4 "Uso de Herramientas de administración de sistemas del *Manual de Políticas de Seguridad de la Información código M-DT-001 versión 1 de fecha julio de 2017" la cual expresa: "La Dirección TIC's de TRANSMILENIO S.A., controlará el uso de programas utilitarios que podrían tener la capacidad de anular el sistema y los controles de las aplicaciones."*

Lo anterior incumple lo establecido en los numerales de las normas: NTC ISO 9001: numeral 8.3.4 "Controles del diseño y desarrollo" literal c), NTC ISO 9001:2008 numeral 7.3.6 "Validación del diseño y desarrollo" NTC ISO 27001: 2013 numeral 6.1.3. literal a, b y c Tratamiento de Riesgos de Seguridad de la información, y Anexo A 9 4.2 "Procedimiento de ingreso seguro", NTD 001:2001 numeral 4.2.2 Planificación de la Gestión del Riesgo. (Responsabilidad del TIC´s).

No conformidad No. 5:

Debilidad en la consolidación del Informe de control de supervisión SIRCI.

Implementar los lineamientos técnicos de verificación para compilar el único informe final que deben aprobar y firmar todas las partes que integran los módulos de responsabilidad SIRCI, dada la importancia de certificar el cumplimiento mensual del objeto contractual del contrato SIRCI, el cual constituye un servicio externo estratégico para TRANSMILENIO S.A.

La Entidad propende asegurar mediante el protocolo código T-DT-001 versión 0 de 2015, la revisión de informes de interventoría al contrato de concesión del SIRCI el cual es conocimiento y aplicación del personal adscrito a la Gerencia de la Integración, al personal regularizador del contrato de concesión del SIRCI, al personal de la Dirección de TIC's, contratistas de presentación de servicios que apoyan las labores de la Dirección de TIC's unificar y que realicen seguimiento a los informes proyectados por la interventoría respecto al contrato de concesión del SIRCI y personal de la interventoría designado para proyectar y ajustar los informes mensuales que exige TRANSMILENIO S.A.

No se encontraron documentados los lineamientos para compilar internamente entre las áreas el único informe de satisfacción de cumplimiento de las obligaciones contractuales para el proceso de pago final que deben aprobar y firmar todas las partes que integran los módulos de responsabilidad SIRCI, situación que evidencia que la organización *"no asegura completamente los controles internos para verificar el cumplimiento de los externos",* ya que una vez realizada toda la traza de verificación al informe de interventoría SIRCI del mes de abril de 2018 en el proceso de TIC´s, se evidenciaron soportes de control a inconsistencias y/o aclaraciones específicas de la revisión de cada uno de los anexos que componen la estructura de entrega del respectivo informe sin embargo no está documentado el paso a paso que deben realizar todas las partes.

Lo anterior incumple lo establecido en los numerales de las normas: NTC ISO 9001: 2015 numeral 8.1 literal e) párrafo 3 *"La organización debe asegurarse de que los procesos contratados externamente estén controlados" 8.4.1 control de productos y servicios suministrados externamente literal a, b y c párrafo 2; numeral 6.1 Acciones para abordar riesgos y oportunidades literal c) "Prevenir o reducir efectos no deseados" NTC ISO 9001:2008 numeral 7.1 "Planificación de la realización del producto", 7.4.1 "Proceso de Compras", 5.4.1 "Planificación del SGC": NTC ISO IE 27001-2013 numeral 9.1 Seguimiento, medición, análisis y medición literal a)* , NTD 001:2001 numeral 4.2.2 Planificación de la Gestión del Riesgo.

En la reunión de cierre de la auditoria se precisa que esta No conformidad es responsabilidad del Comité Gerencia de la Integración.

No conformidad No. 6:

Debilidad en la aplicación de controles automáticos y manuales del directorio activo.

Tomar acciones que permitan asegurar la correcta actualización de la base de datos del personal (funcionarios y Contratista) que labora en TRANSMILENIO S.A, en las fichas de control del directorio activo, con el fin de establecer las fechas exactas de los contratos y/o novedades del caso (retiro de personal) con el fin de mantener actualizada la información que necesita el proceso para su adecuada gestión y control.

TRANSMILENIO S.A, debe asegurar mediante el procedimiento código P-DT-011, V 0 de fecha de 2015, los permisos para otorgar acceso a los medios de procesamiento de información, ya que éste documento define los pasos a seguir para otorgar, modificar o retirar accesos usuarios a los sistemas de información o aplicativos y medios de

procesamiento de información de TRANSMILENIO S.A., como base de todo sistema de seguridad informática.

Se evidenció, el 21 de junio, en las fichas de control automático de la herramienta del directorio activo *"ausencia de marcación de fecha expiración para la categoría contratista",* la cual debería estar relacionada a la vigencia del contrato suscrito por el contratista; esta situación es reincidente de acuerdo con la desviación detectada en una muestra de cuatro seleccionados aleatoriamente el 18 de abril de 2018, mediante prueba de recorrido a la gestión del riesgo del informe 2018IE5819 por la Oficina de Control Interno

Por lo anterior se presenta un incumplimiento en el cierre de las acciones correctivas acordadas en la prueba de recorrido al proceso Tics de fecha abril 18 de 2018 que debía haberse cerrado en mayo de 2018, lo que afecta el cumplimiento de las normas: NTC ISO 9001: 2015 numeral 10.2.1 literal a) subnumeral 1), literal b) subnumeral d), NTC ISO 9001:2008 numeral 8.5.2 "Acción correctiva", NTC ISO 9001: 2015 numeral 6.1 Acciones para abordar riesgos y oportunidades literal c) "Prevenir o reducir efectos no deseados" NTC ISO 9001:2008 numeral 5.4.2 NTC ISO IE 27001-2013 numeral 6.1.3 Tratamiento de riesgos de seguridad de la información literal a b y c Anexo A.9.2.6, Retiro o ajuste de los derechos de acceso, NTD 001:2001 numeral 4.2.2 Planificación de la Gestión del Riesgo. (Responsabilidad del TICS).

No conformidad No. 7:

Asegurar y fortalecer la estrategia de la satisfacción del cliente interno a través de la Mesa de Ayuda de TRANSMILENIO S.A, con el fin de realizar el seguimiento y las percepciones de los clientes internos del grado en que se cumplen sus necesidades y expectativas.

El proceso de Gestión de TIC´s tiene contemplado el procedimiento P-DT-009 Soporte Técnico a Usuarios Finales, el cual en términos generales opera según lo señalado en el

citado documento, no obstante, se observan requerimientos en los que se cierra el caso sin solución eficaz, como:

a) Caso 1: Creación de un usuario de cuenta de correo institucional de la dirección de buses, el cual fue cerrado sin haberse solucionado. Respecto a éste, el área de soporte técnico manifestó no tener licencias de correo.
b) Caso 2: Disco duro lleno en el equipo de un funcionario de la dirección de BRT, el cual Mesa de ayuda argumentó ausencia de dispositivos de almacenamiento que soporten la capacidad de información a respaldar.

En virtud de lo anterior, determinamos cumplimiento respecto del tiempo de respuesta, pero no frente a la solución que permita determinar el cierre eficaz de los casos.

Por otro lado, el procedimiento establece una evaluación que debe realizar el usuario al finalizar el cierre del caso, el cual no está siendo realizado puesto que no se ofrecen herramientas mediante las cuales se genere una encuesta de satisfacción del servicio respecto a la solución presentada por la Mesa de ayuda.

Por lo anterior se presenta un incumplimiento a las normas NTC ISO 9001: 2015 numeral 8.2.1 Comunicación con el cliente literal c, NTC ISO 9001:2008 numeral 7.2.3 Comunicación con el cliente, y en concordancia NTD 001:2001 numeral 6.5 literal b) Satisfacción de los usuarios.

No conformidad No. 8:

Gestionar las actividades necesarias para documentar y evidenciar la toma de acciones preventivas y de mejora utilizando la totalidad de las fuentes definidas en el procedimiento Acciones correctivas, preventivas y de mejora P-OP-017-1.

- No se evidenciaron acciones preventivas y de mejora documentadas por el Proceso Gestión TIC´s al corte de la evaluación. Según lo definido en el procedimiento P-OP-017-1 Acciones correctivas, preventivas y de mejora del SIG, los dueños de los procesos deben reportar a la Oficina Asesora de Planeación las acciones emprendidas las cuales deben incluir preventivas y de mejora. Durante la vigencia

2017 y al corte de la evaluación (30 de abril de 2018), la dependencia no reportó las acciones enunciadas.

- No se evidenció que en el proceso auditado se tomen como fuente para la toma y documentación de acciones preventivas y de mejora la totalidad de las fuentes definidas en el procedimiento para la mejora continua, en el proceso se utilizan solamente los informes de auditoría para efectos de documentar acciones correctivas. No se evidenciaron planes de mejoramiento derivados de otras fuentes tales como: Propuestas de mejoramiento resultado de actividades de autocontrol durante el desempeño del proceso, los resultados de encuestas de satisfacción, peticiones, quejas y/o reclamos, la gestión de riesgos, el producto no conforme, y los demás definidos en el numeral 6.1 del procedimiento P-OP-17-1 Acciones correctivas y preventivas del SIG.

Con lo anterior, es importante precisar que en virtud del Modelo Integrado de Planeación de la Gestión, como primera línea de defensa, las Gerencias Operativas (en este caso la Dirección de TIC´s) son responsables de los riesgos así como de gestionar la implementación de acciones tanto correctivas como preventivas para hacer frente a las deficiencias del proceso y control, a su vez, deben ejecutar procedimientos de control sobre los riesgos de manera constante en el día a día.

Lo anterior incumple con lo establecido en la norma: ISO 9001: 2008 8.5.1 Mejora Continua, 8.5.3 Acciones Preventivas; ISO 9001:2015 10.1 Generalidades, 10.3, Mejora continua y 6.1 Acciones para abordar riesgos y oportunidades.

OBSERVACIONES.

Observación No. 1:

Actualizar los procedimientos: P-DT-010 V0 noviembre de 2015 *“Monitoreo del uso de los medios de procesamiento de información”*, P-DT-011 V0 noviembre de 2015 *“Otorgar acceso a los medios de procesamiento de información”,* P-DT-012 V0 noviembre de 2015

"*Intercambio seguro de información electrónica"* y los protocolos: T-DT-001 V0 octubre de 2015 "Revisión de informes de interventoría al contrato de concesión del SIRCI"; toda vez que a la fecha de la auditoria se evidenció desactualización, lo cual podría generar incumplimiento en las normas NTC ISO 9001:2015 numeral 7.5.2 Creación y actualización de la documentación, NTC ISO 9001:2008 numeral 4.2.3 Control de documentos, NTC ISO IE numeral 7.5.2 Creación y actualización de la documentación.

Observación No. 2:

Verificar el cumplimiento de controles para la aplicación de las Tablas de Retención Documental en los aplicativos de la entidad, con el fin de no incurrir en incumplimiento conforme al numeral 4.2.1 (d) Requisitos de la documentación generalidades de la norma ISO 9001:2008, numeral 7.5.1. Información documentada generalidades de la norma ISO 9001:2015, artículos 7, 8 y 9 del Decreto 2609 de 2012, artículos 4 y 47 del Decreto 103 de 2015 y artículo 18. Uso de tecnologías de información del Acuerdo 04 de 2013, se verificó la tabla de retención documental del proceso, las evidencias obtenidas respecto a la no aplicabilidad de la TRD desde el momento de creación de la documentación producida en la dependencia, y radicada mediante el sistema de información CORDIS, representa un riesgo de pérdida de la información y de la memoria institucional, toda vez que aun cuando el sistema CORDIS cuenta con los campos para vincular la serie, la subserie, el expediente y la ubicación del documento, tales campos no están parametrizados de modo que pueda ser aplicada la TRD.

Los resultados de esta prueba no se documentan en el informe de esta evaluación puesto que han sido considerados en el informe de evaluación del proceso de "Gestión Logística de la Dirección Corporativa" mediante el cual se documenta y formaliza la No conformidad al dueño y directamente responsable del proceso de gestión documental.

Observación No. 3:

Asegurar las acciones correspondientes para prevenir la materialización de riesgos que impactan la continuidad de prestar un soporte especializado de desarrollo de software experto en un proyecto de gran dimensión para TRANSMILENIO S.A, como lo es “la bodega de datos”.

El procedimiento “*Soporte técnico a usuarios finales código P-DT-009, V 1 de fecha de marzo de 2018”,* define establecer las actividades y responsabilidades para asegurar la correcta prestación del servicio de soporte a los usuarios internos de TRANSMILENIO S.A., así como la administración y control sobre las incidencias generadas por dichos usuarios, que requieren un determinado nivel de soporte en herramientas de tecnologías de información y que han sido reportadas a través de los diferentes canales dispuestos para ello por la Dirección de TIC´s.

- Se denota posible materialización del riesgo *“Que no se pueda mantener la continuidad o integridad en las tecnologías de la información” lo cual incluye el soporte especializado para el software* “ para el desarrollo de software de uso de la Subgerencia Económica llamado “Tablero de indicadores y/o prebodega de datos”, el cual fue liderado y supervisado por TIC’s y al momento de la auditoría se detectó que la transferencia de conocimiento del software se canalizó y recibió en personal “contratista”, sin embargo existe documentación de los código fuentes, manuales de operación en la dirección de TIC’s

Lo cual podría generar un incumplimiento NTC ISO 9001: 2015 6.1 Acciones para abordar riesgos y oportunidades literal c) “Prevenir o reducir efectos no deseados” NTC ISO 9001:2008 numeral 5.4.2 “Planificación del SGC”, NTC ISO IE 27001-2013 numeral 6.1.3 Tratamiento de riesgos de seguridad de la información literal b, NTD 001:2001 numeral 4.2.2 Planificación de la Gestión del Riesgo. (Responsabilidad del TICS)

BALANCE DE LA AUDITORÍA:

Proceso Auditado	Total, No Conformidades	Total, Observaciones
Gestión TICS	8	3

FORTALEZAS:

- Se revisó de manera muestral, el proceso de copias de seguridad de las bases de datos de la organización denotando que existe un ejercicio de tres (3) replicas a las bases de datos 1) RMAN ORACLE, 2) Contingencia directa GOOGLE y 3) Export de base de datos ORACLE al servidor principal, que permiten evidenciar la realización del Backup diario y contar con una base de datos para atender contingencias. Es de anotar que no se incluyó en este ejercicio la verificación del proceso de Backup de cintas magnéticas.

- Disposición para atender la auditoría por parte del director y personal TICS.

SOLICITUD PLAN DE MEJORAMIENTO:

De acuerdo con lo establecido en el procedimiento “P-PO-017-1 Acciones correctivas y preventivas del SIG, se debe presentar un Plan de Mejoramiento que contenga las correcciones, acciones correctivas, preventivas y/o de mejora derivadas de las No Conformidades y observaciones contenidas en el Informe de Auditoría. Dicho Plan de Mejoramiento deberá formularse en el formato R-OP-025, el cual se encuentra en la Intranet de la Entidad en el micrositio del Sistema Integrado de Gestión, Desarrollo Estratégico.

Para lo anterior, si los líderes del proceso lo requieren, la Oficina de Control Interno dentro de su rol de asesoría y acompañamiento, los puede asesorar en la formulación metodológica del Plan de Mejoramiento, que deberá presentarse dentro de los cinco días hábiles siguientes al recibo del informe de auditoría.

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.,17 de julio de 2018.

Luis Antonio Rodríguez Orozco

Jefe Oficina de Control Interno

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

Gilberto Antonio Padilla Castro, Profesional Especializado Grado 6 Auditor acompañante

Experto técnico Ing. Greecy Andrea Rivera Barbosa de la Oficina de Control Interno.

Código: 801.01-5-5.2