N° INFORME: OCI-2019-074

PROCESO/SUBPROCESO/ACTIVIDAD: Dirección de TIC

RESPONSABLE DEL PROCESO/SUBPROCESO/ACTIVIDAD: Director de TIC.

EQUIPO AUDITOR: German Ortiz Martin – Contratista, Auditor.

Jorge Iván Flórez Franco – Contratista, Auditor.

Luz Marina Díaz Ramírez, - Contratista, Coordinadora.

OBJETIVOS:

1. Evaluar la Administración del riesgo del Proceso de Dirección de TIC.
2. Evaluar el diseño y efectividad operativa en la aplicación de controles necesarios para mitigar los riesgos asociados al proceso.
3. Evaluar el cumplimiento de la normativa externa e interna, considerando las políticas y procedimientos aplicables al proceso.

ALCANCE:

El alcance previsto para este trabajo de auditoría corresponde al proceso de Gestión TIC, dentro de la cadena de valor de la Entidad que hace parte de los procesos Estratégicos. Una vez analizada la caracterización y documentación del proceso se tomó como referente de auditoría el mapa de riesgos versión 3, el cual fue publicado en el micrositio del Modelo Integrado de Planeación y Gestión (MIPG) el 31 de mayo de 2019 y teniendo en cuenta que para el inició de la auditoría han trascurrido tres (3) meses de aplicación de controles al proceso, se adelantaron pruebas para evaluar el diseño y efectividad de los controles específicos establecidos para las actividades identificadas en la caracterización, los procedimientos, los instructivos, los manuales y los protocolos, utilizando como criterio la metodología de riesgos establecida por la Entidad, que incluye lineamientos del DAFP, ISO 3100-2018 entre otros. El detalle de la evaluación realizada se presenta en la descripción del trabajo realizado.

De las seis (6) actividades claves del proceso registradas en la caracterización, fueron objeto de evaluación en el presente informe cuatro (4), las cuales se describen en el contenido del mismo. Las restantes dos (2) que no se auditaron corresponden a formulación del Plan de acción de TIC y toma de acciones correctivas, preventivas y de mejora, en razón a que tales actividades fueron

evaluadas en otros trabajos adelantados por la Oficina de Control Interno durante la vigencia 2019.

El alcance de la auditoría consideró las siguientes actividades del proceso Evaluado:

- Evaluación del diseño y aplicación de los controles definidos en la Matriz de Riegos para mitigar los riesgos asociados.
- Gestión asociada a Sistemas de Información (Desarrollo, construcción, adquisición, seguimiento, aprobación y puesta en marcha, instalación y desinstalación de software)
- Mantenimiento y soporte (gestión de medios removibles, bitácora de ingreso Dara Center y soporte técnico a usuarios finales).
- Activos de información (Lineamientos, matriz de inventarios de activos y software, control y actualización de activos de la información en la Entidad).
- Servicios de TI (administración de usuarios, intercambio seguro de información, componente tecnológico teletrabajo, gestión de medios removibles, realización de respaldos y restauración de la información, plan y cultura sensibilización del SGSI, implementación del SGI, riesgos en seguridad digital y tecnologías emergentes).
- Planeación Estratégica de la Seguridad de la Información (PESI)
- Planeación estratégica de las tecnologías de la información y comunicaciones (Manual de las Políticas de la seguridad y privacidad de la información, proyectos asociados al PETI, cumplimiento hoja de ruta.

Para la realización de las pruebas los criterios de selección de la muestra se encuentran documentados y soportados en los papeles de trabajo de la Oficina de Control Interno.

PERÍODO AUDITADO: 1 de agosto de 2018 al 30 de septiembre de 2019.

DECLARACIÓN:

Esta auditoría fue realizada con base en el análisis de diferentes muestras aleatorias seleccionadas y los criterios utilizados para la selección de la muestra se encuentran consignados como soporte de las pruebas de trabajo y documentadas en los formatos establecidos por la Oficina de Control Interno para los propósitos mencionados.

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.

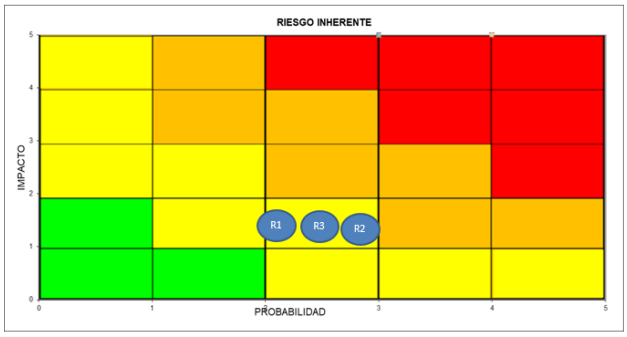
CRITERIOS:

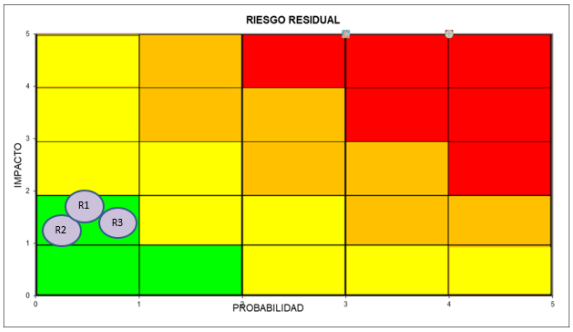
- Caracterización del Proceso, indicadores, mapas de riesgos, Procedimientos, Protocolos, Instructivos, Manuales y demás documentos del Sistema de Gestión de TRANSMILENIO S. A. vigentes y publicados en la intranet de la Entidad al corte de la presente evaluación.
- La demás normatividad interna y/o externa asociada con el proceso auditado y a la estructura de auditoría del marco Internacional (NIA) que aplica a Colombia.

RIESGOS CUBIERTOS:

La Oficina de Control Interno tomó como insumo el mapa de riesgos del Proceso de Gestión de TIC del micrositio de MIPG el 28 de noviembre de 2019 y que reposa en la carpeta electrónica de los documentos asociados a la auditoría.

El mapa de riesgos del proceso cuenta con tres (3) riesgos, en estado de Riesgo Inherente moderado, de los cuales, posterior a controles (riesgo residual) se encuentran ubicados en el perfil bajo. A continuación, se muestra el mapa térmico del proceso:





PERFIL DE RIESGO	
1 -2	BAJO
3 -6	MODERADO
7 -12	ALTO
13 - 25	EXTREMO

RIESGO	INHERENTE		RESIDUAL	
	PROB	IMP	PROB	IMP
R1	3	2	1	2
R2	3	2	1	2
R3	3	2	1	2

Los Riesgos del Proceso descritos en la Matriz que se encuentran vigentes son:

- Los proyectos asociados al plan estratégico PETI no puedan ser ejecutados de acuerdo con la meta establecida

- El plan estratégico de Seguridad de la Información no se pueda implementar de acuerdo a la hoja de ruta establecida
- Imposibilidad de apoyar técnicamente todas las necesidades de la entidad relacionadas con TIC´S

Producto del entendimiento del proceso, la Oficina de Control Interno, identificaron los riesgos relacionados a continuación:

#	Actividad clave del proceso	Riesgo Identificado por la Oficina de Control Interno
1	Desarrollo de Software (R-DT-004 Especificación de Requerimientos de Software ERS y P-DT-013 Construcción de Sistemas de Información P-DT-004 Gestión Ambientes de prueba de software).	Construcción de Sistemas de Información que no atienden las necesidades de información de los procesos misionales y de apoyo de la Entidad
2	Desarrollo de Softwrare (R-DT-005 Plan y Ejecución de Pruebas de Aceptación y T-DT-002 Protocolo Estándares para el Desarrollo de Software en TRANSMILENIO S. A).	Incumplimiento en los requerimientos funcionales para el desarrollo de Software, Impacto: Perdida de Recursos
3	PETI, PESI	Riesgos sobre continuidad del Negocio asociados a TIC, que puedan afectar la operación: Interrupciones no planificadas de TI Ciberataques Brechas de datos Interrupción suministro de red Actos de terrorismo y/o vandalismo
4	P-DT-005 Compra y Actualización de Software	Compra de Software no necesario para la entidad, duplicidad de herramientas para una misma solución de necesidades de Software.
5	T-DT-004-2 Protocolo Admón. Bases de Datos	Perdida de la Oportunidad de la Información, al no estar documentado el procedimiento de realización de los Backups. No garantizar la preservación, mantenimiento y verificación de copias de respaldo de la información.
6	R-DT-001 Solicitud de Actualizaciones a la Plataforma Tecnológica del SIRCI	Ausencia de procedimiento formal de gestión de cambios. Impacto: Perdida de la integridad de datos, Daños Operacionales y Daños en

#	Actividad clave del proceso	Riesgo Identificado por la Oficina de Control Interno
		los Datos
7	T-DT-001 Protocolo Revisión Informe Interventoría SIRCI	Inadecuada Supervisión del contrato de Interventoría del SIRCI, en el componente Tecnológico.
8	P-DT-008 Mantenimiento Equipos de Computo	Falta de mantenimiento de los equipos de cómputo. Efectuar pagos al proveedor, de mantenimiento a equipos, que no se estén realizando.
9	P-DT-016 Procedimiento Instalación y desinstalación de Software y T-DT-003 Gestión Medios Removibles	Vulnerabilidad técnica y legal en los equipos de uso corporativos de la Entidad. Pérdida y/o fuga de información.
10	R-DT-009 Bitácora de ingreso Data Center	Pérdida y/o fuga de la información y los equipos de uso corporativo. Accidentes laborales por acceso a sitios prohibidos (Alto Voltaje eléctrico). Demandas contra la entidad.
11	P-DT-009: Soporte Técnico a Usuarios Finales	Incorrecta prestación del servicio de soporte a los usuarios. Incorrecta administración sobre los requerimientos de los usuarios.
11	I-DT-001 Instructivo Identificación Valoración y Clasificación Activos de Información	Inadecuada identificación, registro, valoración y clasificación de los Activos de Información, Inadecuado manejo de la información de la Entidad.
12	R-DT-010 Matriz de Inventario de Activos de Información Transmilenio. R-DT-006 Inventario de Software	Inadecuada o nula gestión y actualización de los Activos de la Información de la Entidad.
13	P-DT-007 Procedimiento Administración Usuarios	Suplantación de Identidad de los empleados y/o terceros con los usuarios retirados de TRANSMILENIO S.A, en los sistemas de información. Usuarios activos de colaboradores en los sistemas de información que no tienen vinculó laboral con la Entidad.
14	P-DT-012 Intercambio Seguro Información	Uso indebido de información por personal no autorizado, pérdida de la Confidencialidad, integridad y disponibilidad de la información.
15	R-DT-007 Visita Componentes tecnológicos Teletrabajo	Ubicación de la "Data" de la entidad en software y/o herramientas no licenciadas, no seguras. Software del Teletrabajador no Licenciado,

#	Actividad clave del proceso	Riesgo Identificado por la Oficina de Control Interno
		tipo Malware y Tipo Scanner o Sniffer.
16	T-DT-007 Plan Cultura y Sensibilización del SGSI	Pérdida de la Integridad, confidencialidad y oportunidad de la Información. Riesgos sobre la continuidad del negocio, seguridad digital y tecnologías emergentes no identificados, analizados ni valorados.
17	Manual de Supervisión	El incumplimiento de los objetivos contractuales que afecten la operación y/o las actividades estratégicas que ha determinado TRANSMILENIO S.A para su funcionalidad.
18	Normativa vigente de SG-SST de Colombia	Incumplimiento a la normatividad legal vigente debido a falta supervisión en el pago y/o aportes al SG-SST, quedando al descubierto la cobertura en la atención de accidentes de trabajo y enfermedades laborales.

FORTALEZAS.

Disposición para atender la auditoría por parte del director y personal del proceso de Gestión de TIC.

DESCRIPCIÓN DEL TRABAJO REALIZADO:

Durante la auditoría efectuada al Proceso de Gestión de TIC, y teniendo en cuenta el objetivo y alcance descritos anteriormente, los cuales fueron expuestos en la reunión de apertura con el Director de TIC junto con su equipo de trabajo, se desarrollaron las siguientes actividades:

a) **Entendimiento del proceso**: Se llevó a cabo el entendimiento del proceso basado en entrevista realizadas a los colaboradores de las actividades claves del proceso.

b) **Revisión de la Documentación**: Se consultó y analizó el mapa de riesgos del proceso, caracterización, manuales, procedimientos, instructivos, formatos, políticas y en general documentos definidos para el proceso y publicados en la intranet de la Entidad al corte de la evaluación, de acuerdo con el Sistema de Gestión, con el fin de verificar los requisitos del Proceso.

c) **Identificación de riesgos y controles:** Se identificaron los riesgos claves que pudieran afectar o impactar las actividades y objetivos del proceso auditado y se verificó la existencia y efectividad de controles que mitiguen su materialización. De igual manera, los riesgos

identificados por la Oficina de Control Interno fueron cotejados contra los registrados en el Mapa de Riesgos de Gestión.

d) **Diseño del programa de trabajo:** Basados en el entendimiento adquirido del Proceso, la Oficina de Control Interno, se diseñó el plan de pruebas, que a través de su ejecución permitiera determinar el adecuado diseño, la existencia, funcionalidad y aplicación de los controles y requisitos identificados para el proceso.

e) **Reunión de Apertura:** Se efectuó la reunión de apertura el 4 de septiembre de 2019, con El Director de TIC y su equipo de trabajo.

f) **Obtención y análisis de la información objeto de la auditoría:** Teniendo en cuenta la metodología definida por la Oficina de Control Interno de la Entidad, fue solicitada la información objeto de la auditoría para seleccionar muestras, con el fin de validar el diseño y aplicación de los controles claves y requisitos establecidos en el proceso.

g) **Ejecución de Pruebas:** El trabajo de auditoría fue realizado bajo los estándares previstos en los procedimientos adoptados para la Oficina de Control Interno y la participación de los profesionales designados por el Director de TIC a través de los cuales se realizaron pruebas de indagación, comparación, inspección, observación y análisis efectuado sobre la documentación soporte remitida por la dependencia.

h) **Definición de hallazgos y recomendaciones:** Surgieron de un 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 evidenciaron diferencias entre ambos, tales fueron tomadas como hallazgos, los cuales fueron registrados en el presente documento y pre-validados con los responsables de las actividades del proceso.

i) **Definición de observaciones y recomendaciones:** Surgieron como sugerencias de mejores prácticas y pueden contribuir al mejoramiento del proceso y fortalecimiento del Sistema de Control Interno de la Entidad.

j) **Análisis y Socialización del Informe con los responsables y líderes del proceso:** Teniendo en cuenta la disponibilidad de tiempo por parte del Director de TIC, los profesionales que atendieron la auditoría y de los auditores de la Oficina de Control Interno, se realizó la socialización del informe para el día 24 de noviembre de 2019, no obstante, se efectuaron reuniones previas con los Profesionales que lideran las diferentes actividades del proceso,

con el objetivo de analizar y pre validar cada uno de los hallazgos y oportunidades de mejora identificadas durante la auditoría.

Como parte de la ejecución del trabajo y en virtud de la mejora continua, la Oficina de Control Interno desarrolló las siguientes actividades a saber:

A. Matriz de Riegos.

Fueron analizados los riesgos de gestión mapeados, encontrando que en la matriz de riesgos versión 3 del proceso Gestión TIC se cuenta con tres (3) riesgos, los cuales son muy generales y están calificados desde su etapa inherente en una zona moderada, lo cual no se relaciona con el nivel de importancia e impacto que genera el proceso de Gestión de TIC a la Entidad. Una vez aplicados los controles a los tres (3) riesgos, pasan a una zona de importancia baja, denotando la necesidad de reevaluar un análisis específico al proceso.

Con relación a la matriz de riesgos versión 2 (versión anterior), el proceso Gestión TIC, presentaba veinte (20) controles y se cubría el tema de “La continuidad o integridad en las tecnologías de la información”, actualmente la versión 3 presenta ocho (8) controles y no cubre específicamente el tema mencionado. Como resultado de este ejercicio de auditoría dos (2) de los tres (3) riesgos de gestión del proceso equivalentes al 67% se materializaron, lo cual denota la debilidad en el diseño y la aplicación de los controles establecidos. Por otra parte, se evidenció debilidad por parte de la Dirección TIC, como proceso técnico para la implementación y divulgación y publicación en el Micrositio de la Entidad MIPG para todos los procesos de la Entidad en materia de Seguridad Digital, de conformidad con los lineamientos del Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), del Ministerio de Tecnologías de la Información y las Comunicaciones. (Numeral 4.1.3 Alineación o creación de la política de gestión de riesgo de seguridad digital.) Lo anterior se documentó en la recomendación No. 3.

B. Sistemas de información

Se validó que los sistemas de información desarrollados durante el periodo de la auditoría contaran con las evidencias de la trazabilidad definida por la entidad, así como con las evidencias que soportan la adecuada realización de cada una de las etapas, para lo cual se validó: especificación de requerimientos de software, ejecución de pruebas de aceptación, protocolo estándares para desarrollo de Software en TRANSMILENIO S.A., construcción de sistemas de información, ambientes de prueba de software y gestión ambientes de prueba de

software. Con lo anterior se evidenciaron debilidades ya que no se cuenta con los soportes definidos por la entidad para evidenciar cada una de las etapas en referencia, lo cual deja expuesto el riesgo de desarrollo de sistemas de información fuera de los lineamientos establecidos por TI de TRANSMILENIO S. A. Lo anterior generó el hallazgo No. 6

Sobre la compra y actualización de software se tomaron muestras de las compras efectuadas en el periodo auditado para lo cual se verificó que existieran los soportes definidos por la entidad para: el reporte de necesidades de Software por parte de Directores, Subgerentes o jefes de oficina, los soportes de las respuestas a dichas necesidades por parte de la Dirección de TIC, la gestión efectuada por la Dirección de TIC a la solicitud de las dependencias, así como solicitudes que se encontraran pendientes y/o sin resolver por parte de TIC.. Con lo Anterior, no se documentó hallazgo.

Sobre software no autorizados instalados en los equipos de la red de la Entidad, se evidenció la existencia de software tipo juegos, malware y sniffer instalados en equipos de cómputo de diferentes dependencias, registrando esta desviación en el hallazgo No. 1

Sobre administración de base de datos, se verificó que se cumpliera con los lineamientos dispuestos por la Entidad en el Manual de Políticas y Seguridad de la Información M-DT-001-3, evidenciando que si bien se realiza restore de la información, no existe un procedimiento documentado para la realización de Backup de la Información en la Entidad. Lo anterior se registró en el hallazgo No. 5.

Sobre la formalización de requerimientos a las modificaciones para el control de cambios a la plataforma tecnológica del SIRCI, la Oficina de Control Interno revisó los informes de Interventoría del SIRCI, de los meses de agosto y noviembre del 2018 y los meses de marzo y mayo del 2019. En el informe de Interventoría del mes de Agosto de 2018, se evidenció, que el concesionario realizó cambios a la plataforma del SIRCI, que no fueron enviados con el tiempo suficiente para su revisión y respectiva toma de acciones, dificultando que la interventoría pueda realizar su labor para emitir concepto al Ente Gestor para garantizar la gestión de cambios conforme a lo indicado en el contrato. Lo anterior, en razón a que no está formalizado. un procedimiento para que el Concesionario realice la gestión de Cambios apropiada. Producto de lo anterior se generó la recomendación No. 2.

Adicionalmente se verificó si existen inconsistencias entre el reporte mensual del concesionario y del supervisor del contrato del SIRCI en cuanto al indicador de control de la flota, de la muestra

tomada y con los resultados obtenidos, no se documentó hallazgo.

C. Mantenimiento y Soporte

- Se verificó que se esté realizando el mantenimiento a los equipos de cómputo de la entidad (tanto en calidad de arrendamiento como en propiedad), constatando que se cumpliese lo definido en el procedimiento formalizado para lo pertinente, encontrando debilidad en la gestión, lo cual se registró en el hallazgo No. 7.
- Sobre los responsables y lineamientos definidos en materia de control instalación y desinstalación de software en la Entidad, se verificó el debido licenciamiento de software, que se evidenciaran los registros que demuestran control adecuado sobre el inventario de activos de información, se comparó el inventario de software formalizado versus el instalado aplicando la herramienta proactivanet, encontrando debilidad en la gestión, con lo cual fue documentado el hallazgo No. 9, indicando que esta situación es reiterativa y que no se evidenciaron acciones tomadas por la Dirección de TIC para eliminar las causas de las observaciones y hallazgos encontrados.
- Sobre la gestión de medios removibles, se tomó una muestra del total de equipos de cómputo que se encuentran en la red de la entidad de la sede administrativa, validando cuáles tienen el puerto USB abierto, de tales equipos se tomó una muestra encontrando un número importante de equipos de cómputo con puerto USB abierto sin la respectiva autorización del directivo y/o jefe de Oficina, lo que evidenció debilidad en la gestión, documentando el hallazgo No. 3.
- Sobre el cumplimiento a lineamientos para el control de acceso de áreas seguras y del control a la bitácora de ingreso a Data Center, se verificó el adecuado cumplimiento al formato: R-DT-009 "Bitácora Ingreso al Data Center" del periodo auditado, encontrando debilidad en su aplicación, pues de la muestra tomada se evidenciaron formatos con campos sin diligenciar sobre fechas, horas de ingreso, de salida, referencia de equipo, persona a nombre de quien se registra el equipo, entre otros. De igual manera se verificó si en el centro de la UPS, centro de cableado y planta eléctrica, se aplicara con un control efectivo y con criterios claramente definidos mediante los cuales se otorgan accesos restringidos y/o seguros, evidenciando debilidad en dicha situación. Lo anterior se registró en el hallazgo 4.
- Sobre la gestión asociada a soporté técnico a usuarios finales, se validaron los registros de todos los soportes realizados a través de la Mesa de Ayuda, verificando a la luz del procedimiento aplicable la correcta clasificación por tipos de servicio, la priorización dada por

la Dirección de TIC para los requerimientos efectuados por los usuarios, se constató si la Dirección de TIC realiza seguimiento a las acciones de la mesa de ayuda y si son tomadas acciones de mejora, producto de lo anterior se evidenció debilidad en la gestión realizada e incumplimiento al procedimiento definido, razón por la cual se documentó el hallazgo No. 8.

d. Activos de información

- Para constatar la adecuada gestión de los activos de la información a cargo de la Dirección de TIC, se verificó la actualización de la base de datos, para lo cual se tomó una muestra en las áreas misionales, validando que tales activos estuviesen, figuraran en la matriz de Activos de Información emitida por la Dirección de TIC, encontrando diferencias y debilidad en la gestión, lo cual fue registrado en el hallazgo No. 9

e. Servicios de TI

- Sobre la administración de usuarios, se solicitó a la Dirección de TIC el archivo de log a los siguientes sistemas de información: Correo electrónico, Sistema Operativo, Sistema de Información JSP7, de igual manera se solicitó el listado de funcionarios y contratistas desvinculados durante el periodo de la auditoría a la Dirección Corporativa, evidenciando actividad en los sistemas de información por parte de funcionarios y contratistas, posterior a su desvinculación con la Entidad. Lo anterior se registró en el hallazgo No. 2.

- En relación con el intercambio seguro de la información, fueron verificados los accesos que realiza la Entidad a la red de Recaudo Bogotá, y se validó si Recaudo Bogotá tiene acceso a las bases de datos de TRANSMILENIO S. A., con lo anterior se verificó si existen acuerdos de confidencialidad entre la Entidad y Recaudo Bogotá, evidencias de movimiento y tráfico seguro entre las redes de las dos entidades, con lo anterior se evidenció debilidad al respecto, lo cual fue registrado en la recomendación No 1.

f. Planeación Estratégica de Seguridad de la Información

- Se verificó la hoja de ruta de implementación del Sistema de Gestión de Seguridad de la Información – SGSI, y de los componentes que se encontraban en un porcentaje de avance menor al 50%, de acuerdo con el análisis GAP que hizo la Oficina de Control Interno mediante el informe de consultoría con fecha de junio de 2019, se realizó la verificación del grado de implementación de los mismos, evidenciando entre otros, que no se cuenta con plan de

continuidad del negocio, con riesgos asociados al tema, no se cuenta con riesgos identificados, analizados, ni valorados en materia de seguridad digital, tecnologías emergentes y la hoja de ruta de implementación del SGSI está desactualizada. Lo anterior se registró en el hallazgo No. 10.

G Supervisión de contratos de Prestación de Servicios Personales de profesionales adscritos a la Dirección de TIC

- Se tomó una muestra de los contratos de PSP de la Dirección de TIC y se verificó que los documentos contractuales se encuentren publicados en el SECOP II, así como los aportes al sistema de seguridad social, evidenciando debilidades en la supervisión de contratos. Lo anterior se registró en los hallazgos 11 y 12.

HALLAZGOS

Hallazgo N° 1 – Software no autorizado instalado en equipos de TRANSMILENIO S.A

Descripción del hallazgo o situación encontrada:

Se evidenció mediante la utilización de la herramienta Proactivanet usada por la Entidad para el control, registro y monitoreo de software y hardware de la Entidad, que persiste la instalación y uso de software no autorizado en seis (6) de once (11) equipos de TRANSMILENIO S.A, equivalentes al 54% de la muestra tomada, en la categoría de software "Juegos", "Malicioso" y "Desconocido", dejando descubierto el riesgo que identificó la Oficina de Control Interno "Vulnerabilidad técnica y legal en los equipos de uso corporativos de la Entidad".

La Oficina de Control Interno validó lo enunciado, mediante los reportes de consulta emitidos por el sistema de información Proactivanet con fecha del 07 de octubre de 2019, el cual permite identificar los equipos que tienen instalado el mencionado software sin la autorización del formato R-DT-008 así:

a) Software "The Elder Scrolls: Skyrim SE" en el computador del usuario sergio.supelan categoría juegos, presentando actividad de ejecución según reporte de login.

b) Software "Wireshark" computador en el usuario David.monroy y adicional a fecha de esta consulta aparece otra instalación en el usuario (gabriel.gonza) en categoría "software malicioso" este software registra ejecución y se encuentra instalado en las Direcciones de TIC y BRT respectivamente por personal de Contratistas.

c) Software "Secured Yahoo Powered" en el computador usuario Contraloría categoría "software malicioso", instalado en equipo asignado a la Contraloría.

d) Software "Baidu PC Faster" en el computador usuario Carlos.Viancha en categoría "software malicioso", instalado en equipo de Contratista de la Subgerencia de Atención al Usuario y Comunicaciones.

e) Software "ByteFence Anti-Malware" en el computador usuario Alejandro. Medra en categoría "software malicioso", instalado en equipo de la Subgerencia técnica y de servicios

f) Software "Free Online TV" en el computador usuario David.cadena en categoría "software desconocido", instalado en equipo de Subgerencia de Comunicaciones y Atención al Usuario

Lo anterior evidencia incumplimiento por parte de la Dirección de TIC a las etapas 130 y 140 del numeral 7.1 Procedimiento Instalación y desinstalación de Software Protocolo de Gestión de Medios Removibles P-DT-016 y al Numeral 9.5: “Política de Seguridad en las Operaciones” del Manual de Políticas De Seguridad y Privacidad de la Información M-DT-001 versión 3 de Abril de 2019:

1. P-DT-016 Procedimiento Instalación y desinstalación de Software -7.1. Procedimiento para instalación y desinstalación de software en equipo de los usuarios.

Etapa 130: Desinstalar el software de acuerdo con el manual de la aplicación identificada como no autorizada y los lineamientos descritos en este documento.

Etapa 140: Registrar en help desk y reportar al responsable del área de sistemas para realizar llamado de atención al usuario.

2. Manual de Políticas De Seguridad y Privacidad de la Información M-DT-001 versión 3 de Abril de 2019.

Numeral 9.5: “Política de Seguridad en las Operaciones”, el cual establece lineamientos de operaciones correctas y seguras para las operaciones, literal: “r” que establece: “Está totalmente prohibida la instalación de software no autorizado en los equipos de TRANSMILENIO S.A.” y literal: “q”: “TRANSMILENIO S.A., debe implementar procedimientos para controlar la instalación de software en sistemas en producción

Es importante recordar que la presencia de Software "Wireshark" de categoría "malicioso" es de observancia para las políticas de seguridad de la información de TRANSMILENIO S.A, toda vez que un Sniffer es un software que en el mundo de la tecnología es utilizado para

inspeccionar fallas en la red y también es usado para fines maliciosos (Hacker) como: robar contraseñas, interceptar correos electrónicos, espiar conversaciones de chat, entre otros.

La Oficina de Control Interno puso en conocimiento a la Dirección TIC, mediante el informe de Derechos de Autor OCI-021-2019 de abril 01 de 2019, las novedades de software no autorizado en equipos de la Entidad, sin evidenciar acciones al respecto, por lo tanto, en el presente informe se reitera la solicitud de un plan de mejoramiento que elimine de raíz las causas de las situaciones presentadas.

Posibles causas identificadas por la Oficina de Control Interno:

1) Incumplimiento a la “Política de Seguridad en las Operaciones”, del Manual de Políticas de Seguridad y Privacidad de la Información M-DT-001 versión 3 de Abril de 2019, por parte de la Dirección TIC desde su rol de seguimiento que debe realizar a las novedades detectadas por la herramienta "Proactivanet".

2) Debilidad en la ejecución de los controles por parte de la Dirección TIC al Procedimiento P-DT-016 versión 0 de Enero de 2019 por no desinstalar en equipos de uso corporativo software no autorizado.

Descripción del riesgo:

1) Vulnerabilidad técnica y legal en los equipos de uso corporativos de la Entidad.

2) Pérdida y/o fuga de información.

3) Intervención de acciones legales en materia de derechos de autor por los organismos competentes.

Descripción del impacto:

1) Pérdida de información digital de uso corporativo de TRANSMILENIO S.A

2) Sanciones y Multas por utilizar software no licenciado de acuerdo con la Legislación Colombiana.

3) Interrupción o saboteo de las operaciones de TRANSMILENIO S.A.

Recomendaciones:

1) Realizar una revisión al 100% de los equipos de cómputo propios y/o en alquiler, con que cuenta la Entidad para el desarrollo de las actividades, constatando en cuales se encuentran

software de este tipo.

2) Desinstalar de los equipos de uso corporativo de TRANSMILENIO S.A, el software no autorizado de categoría "Juegos", "Malicioso" y "Desconocido" para la totalidad de equipos en los cuales se encuentren dichos software.

3) Implementar mecanismos que garanticen la desinstalación en el ambiente de red interno de software no autorizado en los equipos de uso corporativo de TRANSMILENIO S.A.

4) Implementar campañas de sensibilización dirigidas a la totalidad de los colaboradores de la Entidad, sobre la importancia de cumplir con la normativa en materia de seguridad y privacidad de la información externa e interna aplicable, así como las consecuencias tanto para la entidad como para los colaboradores.

5) Ejercer mayor control en la aplicación de los controles por parte de la Dirección TIC al Procedimiento para instalación y desinstalación de software en equipo de los usuarios P-DT-016 versión 0 de Enero de 2019

Hallazgo N° 2 – "Acceso no autorizado al sistema directorio activo y actividad en correo corporativo después de desvinculación con TRANSMILENIO S.A."

Descripción del hallazgo o situación encontrada:

Se evidenció que un (1) usuario de ocho (8) verificados equivalente al 13%, correspondientes a funcionario, y relacionado con el usuario john.alonso quien perteneció a la Dirección TIC, presentó actividad de ingreso el día 5/09/2019 6:55:03 p.m. al directorio activo de TRANSMILENIO S.A posterior a su retiro, dado que se desvinculó de la Entidad el día 9/07/2019, y previamente el proceso de Talento Humano notificó la novedad a la Dirección TIC mediante correo electrónico de fecha lunes, 08 de julio de 2019 3:40 p. m. en cumplimiento a la etapa 120 "Solicitar la eliminación de usuarios mediante herramienta de soporte helpdesk", del Procedimiento Administración Usuarios P-DT-007 .

La anterior situación incide en la materialización del riesgo identificado por la OCI "Usuarios activos que no tienen vínculo laboral con la Entidad" con el posible Impacto de configurarse una posible Suplantación de Usuarios.

Así mismo se evidenció que dos (2) contratistas de veintitrés (23) verificados, equivalentes al 9%, presentaron actividad en el servicio de correo electrónico corporativo los días 16/09/2019, 23/09/2019 y su desvinculación fue el 02/09/2019 y 20/09/2019 respectivamente, de los cuales

se encontró que el supervisor, notificó su desvinculación mediante correo de fecha 4 de septiembre de 2019 10:42 a. m, al área de Soporte Técnico el respectivo retiro.

Por lo anterior se configura incumplimiento por parte de la Dirección TIC a las etapas 140, 150, 170 y 180 del numeral 7.2 Procedimiento para creación y eliminación de usuarios del documento P-DT-007 Administración Usuarios y a los literales j, c, h del numeral 8.4.1 Requisitos del negocio para control de acceso, literal s numeral 8.4.4 Control de acceso a sistemas y aplicaciones del Manual Seguridad y Privacidad de la Información M-DT-001 Version.3, en virtud a que se evidenció "Accesos no autorizados al Directorio activo", por parte de funcionarios y/o terceros con los usuarios del personal que laboró en TRANSMILENIO S.A.

Posibles causas identificadas por la Oficina de Control Interno:

1) Debilidad en la desactivación de los usuarios por parte del proceso Gestión de TIC en los sistemas de información de TRANSMILENIO S.A.

2) Falta de un monitoreo para verificar usuarios autorizados

Descripción del riesgo:

1) Suplantación de Identidad de los empleados y/o terceros con los usuarios retirados de TRANSMILENIO S.A, en los sistemas de información.

2) Utilización de usuarios desvinculados de los funcionarios y/o contratistas que puedan afectar las operaciones de los sistemas de información de la Entidad.

3) Usuarios activos de colaboradores en los sistemas de información que no tienen vinculó laboral con la Entidad.

Descripción del impacto:

1) Suplantación de un funcionario en los sistemas de información de TRANSMILENIO S.A.

2) Acceso y/o a consulta de información considerada como privilegiada de TRANSMILENIO S.A.

3) Emitir correos con el dominio corporativo a nombre de TRANSMILENIO S.A, afectando la imagen corporativa y/o reputaciones

Recomendaciones:

1. Reevaluar las acciones del plan de mejoramiento anterior, dado que está situación evidenciada es recurrente, registrando acciones que eliminen de raíz las causas que generaron en problema.

2. 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 3 de fecha Abril de 2019.
3. Revisiones estrictas periódicas por la dirección de TIC y partes interesadas, tomando las acciones necesarias para evidenciar el debido control y mitigar el riesgo asociado.
4. Velar por el cumplimiento del procedimiento de autorización y controles para proteger el acceso a las redes de datos y los recursos de red P-DT-007.

Hallazgo N° 3 – Incumplimiento a los lineamientos para el control de Medios Removibles (copiado de información por medio de puertos USB).

Descripción del hallazgo o situación encontrada:

Se evidenció que de 662 equipos de cómputo localizados en red de la Entidad, mediante la herramienta Proactivanet, 192 (29%) no tienen instalada la herramienta TRAPS (Sistema de información, utilizado por la Entidad para el bloqueo de puertos USB) dejando descubierto el riesgo de fuga y/o perdida de la información.

Adicionalmente, se evidenció que 174 (90%) de los 192 equipos de cómputo (Salvo las excepciones a los directivos de la Entidad,) no tienen bloqueado el puerto USB no se evidenció el permiso para acceso y/o posibilidad de copiado de información el cual se debe formalizar a través del formato “R-DT-008 "Autorización, uso y acceso a medios externos”, no obstante solamente tres (3) de cuatrocientos ochenta y ocho (488) contaban con permisos (R-DT-008) específicos para la utilización de los puertos USB.

La Oficina de Control Interno validó lo enunciado, mediante el reporte emitido por el sistema de información Proactivanet con fecha del 30 de septiembre de 2019 a las 15:37, el cual permite identificar los equipos que tienen activa la herramienta adquirida por la entidad "TRAPS" para el bloqueo del copiado de información por los puertos USB.

Lo anterior evidencia incumplimiento por parte de la Dirección de TIC al Protocolo de Gestión de Medios Removibles: T-DT-003, por no aplicar a la totalidad de equipos de la Entidad la herramienta TRAPS, toda vez que la herramienta cuenta con una capacidad para 600 licencias para equipos de acuerdo con el (Contrato 579 de 2017 TMSA-SAMC-16-2017) y por no tener soporte de la totalidad de las autorizaciones de los usuarios con puertos USB abiertos, a los siguientes numerales: 6 "Condiciones Generales"

Párrafo 7: La utilización de un medio removible requiere previamente una solicitud por parte de

Directivo del área correspondiente a través del diligenciamiento del formato R-DT-008 (Autorización de uso y acceso a redes, aplicaciones y herramientas), que deberá ser firmado y envido por correo a la mesa de ayuda de soporte técnico. (soportetecnico@transmilenio.gov.co). Con base en la solicitud recibida, el Técnico Administrativo de la Dirección de TIC's con apoyo del equipo de Mesa de Ayuda, actualizará la Base de datos de usuarios registrados con privilegio de uso de medios removibles.

Párrafo 10: Que dice: Ningún invitado y/o visitante ocasional a la entidad, puede conectar sus PC ó Portátiles a la red LAN de TRANSMILENIO S.A., ni USB en equipos de la Entidad, sin la autorización formal del Jefe del Área y con revisión del dispositivo y/o equipo por parte de la mesa de soporte de TRANSMILENIO S.A

7. "Protocolo a seguir para gestionar el uso de medios removibles: Por regla general, ningún equipo tendrá habilitados los medios removibles, tales como (Unidades CD, DVD formatos (R/W), unidades multi-lectoras, puertos USB, etc.), salvo en aquellos equipos expresamente autorizados.

7.1 Información compartida y/o traslado de información literal C. Condiciones de excepción: El uso de un medio removible (memorias USB, SD, discos duros externos, unidades de CD/DVD en formato R/W, Discos ópticos, etc.), debe ser definido y asignado formalmente por la jefatura, dirección o subgerencia a no más de dos (2) usuarios del área solicitante.

En el formato del hallazgo en mención, se detallan los siete (7) casos reportados por la Dirección de TIC, que contaron con el formato: R-DT-008: “Autorización, Uso y Acceso a Medios Externos”.

Posibles causas identificadas por la Oficina de Control Interno:

1. Incumplimiento a los lineamientos del Protocolo a seguir para gestionar el uso de los medios removibles T-DT-003 en cuanto al control de permisos de medios removibles (copiado de información por medio de puertos USB).

2. Debilidad en la instalación de las licencias disponibles de la herramienta adquirida por TRANSMILENIO S.A, para el bloqueo de puerto USB del 100% de los equipos de cómputo conectados a la Red de TRANSMILENIO S.A.

3) Debilidad en el diligenciamiento de los controles documentales del Protocolo a seguir para gestionar el permiso y uso de los medios removibles T-DT-003, formato R-DT-008.

Descripción del riesgo:

1) Fuga y/o Pérdida de información de uso corporativo.

Descripción del impacto:

1) Vulnerabilidad de los activos de información.

2) Pérdida de la confidencialidad de la información.

3) Interrupción de algunas y/o todas las operaciones de red por ingreso a través de puerto USB de virus no identificado por el antivirus.

Recomendaciones:

1) Dar cumplimiento estricto al Protocolo de Gestión de Medios Removibles: T-DT-003 y la revisión de los permisos que ameritan el R-DT-008 Autorización uso y acceso a Medios externos.

2) Utilizar la herramienta "TRAPS" y/o cualquier otro mecanismo para restringir el 100% de equipos que actualmente están descubiertos (192).

3) Ejercer mayor control sobre los permisos con que cuentan los equipos conectados a la red de la Entidad.

Hallazgo N° 4 – Incumplimiento a los lineamientos del control de acceso de áreas seguras.

Descripción del hallazgo o situación encontrada:

Se evidenció incumplimiento al Manual de seguridad y privacidad de la información M-DT-001 V3 de abril de 2019 al numeral 8.9.1 "Perímetros de seguridad física - controles físicos de entrada" establecidos en los párrafos 11 al 16 en cuanto a:

Los privilegios de acceso a las áreas seguras de TRANSMILENIO S.A deben ser definidos y otorgados por el profesional u oficina encargada del área segura, para ello debe tener en cuenta los siguientes tipos de usuario: Visitantes (servidores públicos, contratistas, proveedores o terceras partes) que requieren acceder muy rara vez.

Teniendo en cuenta lo anterior, los únicos que deben tener privilegios de acceso permanente a las áreas seguras son los profesionales que trabajan regularmente en ellas. Los demás usuarios deben solicitar autorización para el acceso y portar un documento que demuestre su identidad. En este tipo de casos, se debe asignar por parte del área responsable del área segura un profesional que acompañe y supervise la labor de dicho visitante, hasta su salida.

Para el ingreso de los visitantes, en las áreas seguras se debe llevar un registro de ingreso verificando previamente que esté autorizado por el funcionario correspondiente. (Negrilla

subrayada)

La Oficina de Control Interno validó los formatos R-DT-009 Bitácora de Ingreso al Data Center y otras áreas seguras, utilizados como control de accesos, identificando las áreas seguras de las instalaciones (pisos 2, 4, 5, 6 y 7) del edificio sede de TRANSMILENIO S.A, que son cinco (5), de los cuales seleccionaron las áreas seguras de mayor nivel de criticidad e impacto para la Entidad tales como Centro de Datos, UPS, Cableado y cuartos eléctricos, tomando como muestra tres (3) equivalentes al 60% de la muestra del 100% evidenciando lo siguiente:

1. La bitácora actual que está siendo utilizada únicamente para el control y registro del Data Center presenta campos sin diligenciar.

2. En recorrido por los demás pisos se evidenciaron otras áreas seguras como planta eléctrica (piso 6) y centro de cableado (piso 5), las cuales no están aplicando el diligenciamiento de control de acceso en la bitácora R-DT-009, sin embargo estas áreas presentan cerraduras físicas y eléctricas en sus puertas de acceso así como la siguiente señalización:

Piso 2: "Prohibido el ingreso a personal no autorizado" y "Peligro Alto Voltaje"

Piso 4 "Cuarto eléctrico y de datos", "Prohibido el ingreso a personal no autorizado", "Peligro Riesgo Eléctrico"

Piso 5: "Cuarto eléctrico y de datos", "Prohibido el ingreso a personal no autorizado", "Peligro Riesgo Eléctrico"

Piso 6: "Peligro Riesgo Eléctrico" "Precaución no entre en la habitación cuando suene la alarma, el sistema de extinción del fuego está siendo descargado"

Piso 7: "Cuarto eléctrico y de datos", "Prohibido el ingreso a personal no autorizado", "Peligro Riesgo Eléctrico"

3. Se evidenció el acceso permanente (todos los días) de un tercero al centro de cableado del piso 5, mediante autorización y el uso de una tarjeta de acceso.

El profesional entrevistado de la Dirección de TIC confirmó al equipo auditor que, fue otorgado la tarjeta de acceso al tercero, aclarando que el centro de datos estaba completo, sin observaciones y que adelantaría el correctivo inmediato.

Posibles causas identificadas por la Oficina de Control Interno:

1. Desconocimiento de la correcta aplicación del manual Seguridad y Privacidad de la

Información del acceso a áreas seguras.

2. Falta de supervisión en la correcta aplicación del control documental (Bitácora R-DT-009) de acceso a áreas seguras.

3. Falta de revisión periódica a los accesos de las zonas restringidas.

4. Falta de apropiación a la cultura de Seguridad y Privacidad de la Información.

Descripción del riesgo:

1) Pérdida y/o fuga de la información y los equipos de uso corporativo.

2) Accidentes por acceso a sitios prohibidos (Alto Voltaje eléctrico).

3) Demandas contra la entidad.

Descripción del impacto:

1) Afectación directa a la prestación de los servicios eléctricos y de infraestructura tecnológica.

2) Interrupción Operacional del Negocio por saboteo en equipos, redes y sistemas eléctricos.

3) Pérdidas económicas.

Recomendaciones:

1) Incorporar en el registro de control acceso formato R-DT-009 Bitácora de Ingreso al Data Center, las otras áreas seguras que no están controlando documentalmente como Centro de Datos ubicado en el piso 5, UPS piso 6, Cableado piso 2 y cuartos eléctricos piso 6 de la actual sede administrativa de TRANSMILENIO S.A.

2) Diligenciar completamente el formato R-DT-009.

3) Dar cumplimiento al numeral 8.9.1 "Perímetros de seguridad física - controles físicos de entrada" establecidos en los párrafos 11 al 16 del Manual de seguridad y privacidad de la información M-DT-001 V3 de abril de 2019, toda vez que se deben incluir para este control todas las áreas definidas como seguras dentro de la Entidad.

Hallazgo N° 5 – Incumplimiento a los lineamientos definidos en el Manual M-DT-001: "Políticas de la Seguridad y Privacidad de la Información", Numeral 9.6: "Políticas de Copias de Respaldos.

Descripción del hallazgo o situación encontrada:

No se evidenció procedimiento documentado para la realización de Backup, de acuerdo con lo

manifestado por la Dirección de TIC, dicho procedimiento se encuentra elaboración.

No obstante lo anterior, la Dirección de TIC evidenció bitácora con la realización de respaldos y restauraciones de la información de TRANSMILENIO S.A.

Se considera importante precisar que la Dirección de TIC está teniendo en cuenta las Bases de Datos del Motor de ORACLE (Sistema ERP JSP7 y lo que se tiene de CORDIS), las Bases de Datos SQL Server (Sistema T-DOC). Tanto las Bases de Datos ORACLE como SQL Server se están llevando a la Nube de TRANSMILENIO S.A. Por otra parte el procedimiento existía pero fue retirado del Micrositio del proceso de Gestión de TIC

Por lo anterior se evidenció: Incumplimiento al Manual: M-DT-001 "Manual de las Políticas de la Seguridad y Privacidad de la Información", Numeral 9.6: "Política de Copias de Respaldo" y literal "a", que dice textualmente: "TRANSMILENIO S.A. debe seguir un procedimiento definido para las actividades de backup, teniendo en cuenta la criticidad y las necesidades de disponibilidad de los datos. Este procedimiento debe estar debidamente documentado para seguimiento y control".

Posibles causas identificadas por la Oficina de Control Interno:

1. Falta documentar el procedimiento para la realización de Backup

2. Desconocimiento del procedimiento de Control de los Documentos Oficiales del Sistema Integrado de Gestión SIG, código: P-OP-001

Descripción del riesgo.

1) Perdida de la Oportunidad de la Información, al no estar documentado el procedimiento.

2) No garantizar la preservación, mantenimiento y verificación de copias de respaldo de la información.

Descripción del impacto:

1) No recuperar oportunamente y en forma uniforme la información, en caso de un siniestro

2) Pérdida de la capacidad operativa

3) Pérdida de los Activos de Información.

4) Reprocesos en los Sistemas de Información.

Recomendaciones:

1) Dar cumplimiento estricto al Manual de las Políticas de la Seguridad y Privacidad de la Información M-DT-001, en el numeral 9.6: "Políticas de Copias de Respaldo".

2) Documentar e implementar un procedimiento de Backup que dé cumplimiento a lo requerido por el manual de políticas de seguridad y privacidad de la información.

3) Socializar el procedimiento de Backup en toda la entidad

Hallazgo N° 6 – Incumplimiento al procedimiento: P-DT-013: "Construcción de Sistemas de Información.

Descripción del hallazgo o situación encontrada:

1. Se evidenció incumplimiento al procedimiento P-DT-013: Construcción de Sistemas de información, ya que para 1 de 5 (20%) casos evaluados, no se realizó el diligenciamiento de los formatos que garantizan la trazabilidad de los cambios, modificaciones, requerimientos, entrega y recibo a satisfacción del software por parte del usuario final, dejando descubierto el riesgo de Software, que no corresponda a las especificaciones requeridas por el usuario final, los casos son los siguientes:

a) El 30 de Septiembre de 2019 se adelantó reunión con el Ingeniero encargado de la Ruta: Inteligencia de Negocios y se evidenció que para el desarrollo de los Sistemas de Información referentes a dicha ruta de negocios, no se elaboraron los formatos R-DT-004: "Especificación de Requerimientos de Usuario ERS".

2. Por otra parte, se evidenció que para 3 de 5 casos evaluados (60%), los formatos fueron diligenciados de forma incompleta y/o no fueron registradas las modificaciones efectuadas a los requerimientos del usuario final, dejando descubierto los riesgos de entrega de software cuyas especificaciones no quedaron acordadas en la fase inicial y/o que el usuario final aduzca que el software no corresponda al solicitado, los casos son los siguientes:

a) El día 30 de Septiembre de 2019 se adelantó reunión con la ingeniera encargada de la Ruta Transaccional: “Sistema de Apoyo a la Interventoría y Desincentivos”. Para dicho Sistema de Información, se evidenció que se elaboró el correspondiente formato ERS, sin embargo el Usuario Final en el “Modulo de Hallazgos”, realizó modificaciones a las funcionalidades requeridas y éstas no fueron registradas en el formato R-DT-004 en la definición de los “Casos de Uso” respectivos, quedando desactualizados los requerimientos del usuario en el formato ERS.

Según el procedimiento P-DT-013: “Construcción de Sistemas de Información”, Etapa No. 45, cuando surgen cambios en los requerimientos establecidos en el documento línea base ERS, se debe aclarar y/o negociar los requerimientos funcionales, en reunión con el equipo de proyecto y luego actualizar la versión del documento “R-DT-004 Especificación de Requerimientos de Software – ERS” y realizar los cambios a los requerimientos concertados, diligenciar los requerimientos modificados, en la sección control de cambios de éste documento.

b) Los formatos R-DT-04 para las rutas: Transaccional: "Sistema de apoyo a la interventoría y desincentivos" y la ruta Espacial y Control de la Información, no presentan en los campos Usuario Líder y Profesional Dirección de TIC nombre, firma y cargo de quién solicita el desarrollo y tampoco la firma y cargo del profesional de la Dirección de TIC encargado de gestionarlo.

Por lo anterior se evidencia incumplimiento al procedimiento: P-DT-013: "Construcción de Sistemas Información", donde se establece los requerimientos de los usuarios y los lineamientos definidos para la construcción de Sistemas de Información, para la Entidad.

Se considera importante aclarar que según el procedimiento: P-DT-013: “Construcción de Sistemas de Información”, el objetivo del debido diligenciamiento de estos formatos es dejar la trazabilidad de las actividades para la construcción de los Sistemas de Información, a partir de los requerimientos definidos por los usuarios finales, para la obtención de producto de Software y que sean: correctos, fiables, y sostenibles en el tiempo.

El formalismo del documento ERS: R-DT-004, es el primer eslabón del ciclo de vida de desarrollo de sistemas en la Entidad y es el documento formal, con el cual tanto el usuario final, como la Dirección de TIC, formalizan todas las funcionalidades del Sistema de Información a desarrollar, el cual se convierte en el documento base para las debidas entregas a satisfacción al usuario final, por esto debe ser debidamente diligenciado, modificado si hay cambios en los requerimientos y firmado por las partes que intervienen.

Posibles causas identificadas por la Oficina de Control Interno:

1) Debilidad en la aplicación, verificación y gestión de controles en el desarrollo de los Sistemas de Información de la Entidad definidos en el procedimiento P-DT-013.

2. Falta de registro de las modificaciones, cuando los usuarios plantean cambios en las funcionalidades.

3. Desconocimiento del procedimiento P-DT-013 por parte del personal de la Dirección de TIC

Descripción del riesgo.

1) Generar Software, que no corresponda a las especificaciones requeridas por el usuario final.

Descripción del impacto:

1) El Usuario no recibe el Software a entera satisfacción.

2) Pérdida de recursos por reprocesos.

Recomendaciones:

1) Dar cumplimiento estricto al procedimiento P-DT-013: "Construcción de Sistemas de Información".

2) Socializar a los profesionales adscritos a la Dirección de TIC del procedimiento y los formatos relacionados exigiendo su estricto cumplimiento.

3) Realizar adecuada supervisión al cumplimiento del procedimiento P-DT-013

4) Dejar la respectiva evidencia en los formatos definidos por la Dirección de TIC (R-DT-004) en lo concerniente a construcción de sistemas de información, a fin de evidenciar el cumplimiento del debido proceso y mitigar los riesgos asociados.

5) En caso de modificaciones a las funcionalidades iniciales, registrar dichas modificaciones en el documento: ERS.

6) Diligenciar todos los formatos requeridos para el desarrollo de Software en la Entidad, según el procedimiento: P-DT-013

Hallazgo N° 7 – Debilidad en la aplicación de controles al mantenimiento de equipos de cómputo e Incumplimiento al procedimiento: P-DT-008: "Mantenimiento Equipos de Computo

Descripción del hallazgo o situación encontrada:

La Oficina de Control Interno se reunió con el proceso de Gestión de TIC, el pasado viernes 4 de Octubre y solicitó el Plan de Mantenimiento de los Equipos de Cómputo de la vigencia 2019, propiedad de TRANSMILENIO S.A., junto con los soportes de la realización de dichos mantenimientos, la Dirección de TIC remitió vía correo electrónico los informes que presenta el Proveedor del Contrato de Mantenimiento de Equipos de Cómputo y Mesa de Ayuda, contrato 292 - 18 de 2018, de los meses de Junio, Julio y Septiembre de 2019, para el pago de las cuentas, sin embargo no adjuntaron el informe de cada mantenimiento preventivo detallado, que se encuentra establecido en el procedimiento P-DT-008 (numeral 6,1).

Con lo anterior, no se evidenciaron los soportes de la realización de cada mantenimiento preventivo realizados parte del contratista, de acuerdo con lo establecido en numeral "6.1",

"Mantenimiento Preventivo", del Procedimiento: P-DT-008: "*Mantenimiento de Equipos de Cómputo*", ya que se debe entregar un informe por cada mantenimiento preventivo realizado, el cual debe incluir en detalle las actividades realizadas y actualización de la hoja de vida de cada uno de los equipos (Usuario, ubicación, seriales, modelo, dirección IP, entre otros), formato previamente acordado con el usuario final, por lo que se constituye un incumplimiento al procedimiento enunciado. Es importante indicar que lo descrito en los informes de Gestión del Proveedor y los Informes de Supervisión del contrato 292-18 de 2018, de los meses desde Septiembre de 2018 hasta Agosto de 2019, no registran el detalle de lo definido en el procedimiento, por lo tanto se incumple también lo definido en el Manual de Supervisión e Interventoría: "M-DA-015", respecto de los informes de supervisión lo siguiente: Numeral 9.3: "Seguimiento Técnico", literal "g", que dice textualmente: *"Suministrar al contratista todos los detalles, especificaciones técnicas, etc., necesarios, que deba utilizar en la ejecución del contrato, llevando el respectivo registro de documentos vigentes"*.

Se considera importante mencionar que en el documento: "Estudios Previos Arriendo de Computadores" (el cual forma parte integral del contrato 292 -18 de 2018), dice textualmente: "*Entregar, máximo diez (10) días hábiles después de finalizada la actividad, un informe detallado sobre la ejecución de cada jornada de mantenimiento preventivo junto con las planillas debidamente diligenciadas y firmadas por los usuarios, en donde conste la aceptación del mantenimiento*". Con lo anterior no se evidenció que para el período de la auditoría se haya dado cumplimiento a lo enunciado, pues no existen soportes de la entrega por parte del contratista de los informes detallados sobre la ejecución de cada jornada de mantenimiento preventivo y en los informes de supervisión desde septiembre del 2018 hasta agosto de 2019, no se registró nada al respecto.

Posibles causas identificadas por la Oficina de Control Interno:

1. Debilidad en la aplicación, verificación y gestión de controles en el Mantenimiento de equipos de cómputo de la Entidad: P-DT-008.

2. Desconocimiento del procedimiento P-DT-008 por parte del personal de la Dirección de TIC.

3. Debilidad en la Supervisión del contrato del mantenimiento preventivo de Equipos de cómputo de la Entidad

Descripción del riesgo:

1) No se controle el mantenimiento de los equipos de cómputo.

2) Pagar mantenimientos al proveedor, que no se estén realizando.

Descripción del impacto:

1) Fallas en los equipos por falta de mantenimiento preventivo

2) Deterioro de los equipos de cómputo

3) Investigaciones, sanciones debido a debilidad en la supervisión de los contratos

Recomendaciones:

1) Dar cumplimiento estricto al procedimiento P-DT-008: "Mantenimiento Equipos de Cómputo", en cuanto a documentar los soportes de mantenimiento realizados a los equipos.

2) Solicitar al proveedor de mantenimiento preventivo un informe detallado sobre la ejecución de cada jornada de mantenimiento preventivo junto con las planillas debidamente diligenciadas y firmadas por los usuarios, en donde conste la aceptación del mantenimiento. Además la actualización en la hoja de vida de cada uno de los equipos de estas actividades realizadas del mantenimiento preventivo.

3) Dar efectivo y oportuno cumplimiento a lo definido en el contrato suscrito con el proveedor y dejar evidencia en los informes de supervisión.

4) Cumplir las disposiciones del Manual de Supervisión e Interventoría y dejar evidencia en los informes de supervisión, de lo definido en el procedimiento y en las obligaciones contractuales

Hallazgo N° 8 – Incumplimiento al procedimiento: P-DT-009: "Soporte Técnico a Usuarios Finales

Descripción del hallazgo o situación encontrada:

Se evidenció incumplimiento al procedimiento P-DT-009: "Soporte Técnico a Usuarios Finales", versión 2 de abril de 2019, ya que no se está realizando en debida forma la priorización de los requerimientos de soporte técnico recibidos por parte de los usuarios internos de la Entidad, toda vez que a todos los requerimientos se les da la misma prioridad (alta), tampoco se evidenciaron registros sobre el análisis, seguimiento y toma de acciones por parte de la Dirección de TIC a dichos requerimientos. De igual manera la mesa de ayuda no está siendo centralizada y gestionada por la Dirección de TIC. Los casos se presentan a continuación:

1. En cuanto a la priorización, de acuerdo con lo definido en el procedimiento enunciado, para cada servicio requerido por los usuarios se debe asignar prioridad, de igual forma, en el numeral: "5": "Definiciones", se establece qué prioridad es el orden en el tiempo de atención y solución

con el cual será trabajado el incidente por parte del personal de TIC y en la etapa No. 30, define lo siguiente: "Recibir el caso en la mesa de ayuda, realizar el diagnostico, categorizarlo y priorizarlo", por parte del coordinador de la Mesa de Ayuda. Lo anterior en razón a que el 100% de los requerimientos que recibe la mesa de ayuda son categorizados como prioridad "Alta" y la Oficina de Control Interno, ha evidenciado que no todos los casos deben ser priorizados en esa categoría, según el procedimiento P-DT-009: "Soporte Técnico a Usuarios Finales".

Se considera importante mencionar que el procedimiento de soporte técnico a usuarios finales con código P-DT-009, define los niveles de prioridad de la siguiente manera:

- Baja: procedimiento menor que requiere un nivel de intervención básico por parte del personal de tecnologías de información. Tiempo de Respuesta: 0 - 30 minutos.

- Alta: cuando se presenta una caída importante de las herramientas de tecnologías de información afectando a uno o varios usuarios. Tiempo de respuesta: 0 - 20 minutos.

- Crítica: cuando se presenta una falla general de las herramientas de tecnologías de información afectando a la mayoría de los usuarios. Tiempo de respuesta: inmediato.

De la muestra seleccionada, correspondiente a seis (6) de doce (12) meses reportados por la dirección de TIC, (Octubre y Diciembre de 2018 y Febrero, Abril, Junio y Agosto de 2019), se evidenció que para el 100% de los registros mensuales reportados, los requerimientos de los usuarios se categorizan como de prioridad: "Alta". Lo anterior evidencia que no está siendo aplicado lo descrito en el procedimiento enunciado. Como ejemplo de esto, se evidenció que en los meses de febrero y abril de 2019, 44 registros y 20 registros respectivamente, su categorización debió haber sido: "Baja", según el ejemplo dado en el procedimiento P-DT-009, donde dice textualmente: "Nivel de Prioridad Baja: procedimiento menor que requiere un nivel de intervención básico por parte del personal de tecnologías de información. Ejemplo: preguntas de configuración. Tiempo de Respuesta: 0 - 30 minutos".

2. Se evidenció además incumplimiento a este mismo procedimiento, ya que los requerimientos de los usuarios a los módulos del ERP Corporativo JSP7, no están siendo gestionados en su totalidad por la Mesa de Ayuda de la Entidad, sino que están llegando directamente al correo de la funcionaria adscrita a la empresa que suministra el sistema de información JSP7 y cuya ubicación física de su puesto de trabajo se encuentra en el área de Contabilidad de la Dirección Corporativa, adicionalmente, los casos que le llegan a dicha funcionaria son solucionados y

respondidos por ella, sin el cumplimiento de los parámetros definidos por la entidad en el procedimiento P-DT-009 y sin el control o gestión por parte de la Dirección de TIC.

Verificada la información suministrada por la Dirección de TIC (Bitácora de la Mesa de Ayuda) vs los informes de supervisión del contrato 429 -19, se evidenció que los setenta y ocho (78) requerimientos asociados al Sistema JSP7 reportados en los informes de supervisión de ASP Solutions no fueron cubiertos por la mesa de ayuda gestionada por la Dirección de TIC, contraviniendo con lo indicado en el numeral 6: "Condiciones Generales (Políticas de Operación", y subnumeral 6.1, literal "a", tabla "1": "Servicios Cubiertos por la Mesa de Ayuda": "Software: ERP (Seus) JSP7", de conformidad con el Procedimiento Soporte Técnico a Usuarios Finales con código P-DT-009.

Posibles causas identificadas por la Oficina de Control Interno:

1. Desconocimiento y falta de aplicación procedimiento P-DT-09 por parte del personal de la Dirección de TIC encargado de supervisar la labor de Mesa de Ayuda.

2. Desconocimiento del procedimiento P-DT-009 por parte del tercero contratado por la Entidad para gestionar la Mesa de Ayuda.

3. Obligaciones contractuales de Mesa de Ayuda diferentes en los tiempos de las actividades descritas en el procedimiento.

4. Debilidad en la aplicación y supervisión de los parámetros y controles definidos en el procedimiento P-DT-009

Descripción del riesgo:

1) Incorrecta prestación del servicio de soporte a los usuarios.

2) Incorrecta administración y control sobre los requerimientos de los usuarios.

3) Dejar de atender requerimientos críticos, por no tener una adecuada clasificación.

Descripción del impacto:

1) Falencia en algunas actividades de Supervisión del contrato de la Mesa de Ayuda de la Entidad.

2) Inadecuada prestación de servicios a los usuarios.

3) Desconocimiento de los reales tiempos promedios de atención a los usuarios

4) Registro incompleto de las soluciones realizadas en las Bases de Datos de Conocimiento.

5) Falta de control, análisis y seguimiento de los casos requeridos, atendidos y solucionados por la mesa de ayuda de la Dirección de TIC.

Recomendaciones:

1) Dar cumplimiento estricto al procedimiento P-DT-009: "Soporte Técnico a Usuarios Finales".

2) Socializar el procedimiento a quienes son responsables de aplicar y dar cumplimiento al procedimiento, así como a quienes ejercen supervisión del contrato de mesa de ayuda.

3) Realizar seguimiento a la aplicación de los controles definidos en el procedimiento P-DT-009.

4) Ajustar las actividades definidas en el Anexo Técnico: R-DA-103, para que sean concordantes con el procedimiento P-DT-009.

5) Incorporar en el registro de la Mesa de Ayuda de la Entidad, la totalidad de requerimientos de usuarios incluyendo los requerimientos al ERP Corporativo: JSP7.

Hallazgo N° 9 – Incumplimiento al manual: M-DT-001: "Manual de las Políticas de la Seguridad y la Privacidad de la Información", numeral: 9.2.1.1: "Inventario de Activos".

Descripción del hallazgo o situación encontrada:

No se asegura en la entidad, que los inventarios de activos de información de TRANSMILENIO S.A., se encuentren actualizados, por lo que se evidenció incumplimiento a lo definido en el numeral 9.2.1.1 “Inventarios de Activos” del Manual de las políticas de Seguridad de la Información debido a que cinco (5) de los veintiocho (28) contratos que la entidad tiene suscritos para la legalización de Software y que equivalen al 17,8%, no están relacionados en el inventario de activos (Formato: R-DT-010: "Matriz de Inventario de Activos de Información de TRANSMILENIO S.A, versión abril 2019), de información suministrado por la Dirección de TIC a la Oficina de Control Interno, mediante correo electrónico del 23 de septiembre de 2019 . Los contratos son:

- Contrato: CCE31909, Software de Microsoft

- Contrato: CTO640-18, Software de AUTOCAD

- Contrato: CTO570-17, Software de CISCO

- Contrato: CTO664-018, Software de ADOBE CLOUD

- Contrato: CTO389-05, Software ARANDA

Por lo tanto, se constituye un Incumplimiento al Manual de las Políticas de la Seguridad y la Privacidad de la Información: M-DT-001 ", numeral: 9.2.1.1: "Inventario de Activos", literal: "d", que define lo siguiente: "Mantener actualizado el inventario de los activos de información tecnológicos incluyendo redes, servidores, aplicaciones, dispositivos de red, estaciones de trabajo, portátiles y licencias de software, así como aires acondicionados, generadores de energía, unidades de potencia (UPS). "

También incumple el literal "c", que define lo siguiente: "La matriz de identificación y clasificación de activos de información se debe actualizar por lo menos una vez al año y/o cuando se presenten retiros, adquisiciones o reemplazos en los activos identificados".

Posibles causas identificadas por la Oficina de Control Interno:

1. Incumplimiento a los lineamientos sobre el manejo de los Activos de la Información.

2. No realización de actividades de actualización, sobre el inventario de Activos de Información.

3. Inadecuado entendimiento sobre la identificación de los Activos de la Información (los activos de información deben estar claramente identificados).

4. Falta de detalle completo sobre los Activos de la información

Descripción del riesgo.

1) No identificación de los Activos de la Información de la Entidad.

2) Al no tener el inventario de activos de información actualizado no se puede determinar los activos críticos, ni su nivel de clasificación, para asociarlos a los respectivos procesos.

Descripción del impacto:

1) No asignación de los custodios, sobre los Activos de Información, no registrados en la Matriz de Inventario de los Activos de la Información.

2) Pérdida de los Activos de la Información de la Entidad (confidencialidad, integridad y disponibilidad).

Recomendaciones:

1) Actualizar de forma inmediata el Inventario de Activos de la Información, del proceso TIC.

2) Velar por el cumplimiento de las Directrices sobre la realización del inventario de los Activos de la Información por parte de TIC.

3) Realizar actividades permanentes para monitorear los Activos de información de la Entidad.

4) Identificar a nivel de detalle los Activos de la Información de la Entidad.

5) Cumplir con los lineamientos sobre el manejo de los Activos de la información.

Hallazgo N° 10 – Incumplimiento en la ejecución de la Planeación Estratégica de la Seguridad de la Información: PESI, según el "Mapa de Ruta del SGSI - Gel 2019 - 2020"

Descripción del hallazgo o situación encontrada:

No se evidenciaron soportes de la oportuna implementación del Mapa de Rutas del SGSI, ya que actividades identificadas para el desarrollo del mismo y allí registradas, no se están cumpliendo en los plazos definidos.

Se tomaron 42 Objetivos de Control de los 121 registrados en el Análisis GAP, los cuales presentaron menos del 50% de avance en su implementación (ver informe de consultoría de la Oficina de Control Interno mediante radicado 2019-80101-CI-06268). De estos 42 Objetivos de Control, se tomaron los que tenían actividades planeadas para los trimestres I, II y III de 2019, según el "Mapa de Ruta SGSI - GEL - 2019 - 2020". En total fueron 19 objetivos de Control equivalentes al 45% de la muestra, que cumplían con esta característica, encontrando que 5 de 19 Objetivos de Control, es decir el 26% de la muestra, que tenían actividades programadas para desarrollar en los trimestres enunciados, no se realizaron en las fechas programadas. Los cinco (5) Objetivos de Control son:

A.17.1.2: Implementación de la continuidad de la seguridad de la información, Avance GAP (0% de avance)

A.6.1.5: Seguridad de la información en gestión de proyectos, Avance GAP (0% de avance)

A.17.1.3: Verificación, revisión y evaluación de la continuidad de la seguridad de la información, Avance GAP (0% de avance)

A.12.1.3: Gestión de la capacidad, Avance GAP (20% de avance)

A.12.1.4: Separación de las instalaciones de desarrollo, pruebas y operación, Avance GAP (20% de avance).

Por lo anterior se configura en materialización del Riesgo de Gestión # 2 denominado "El plan estratégico de Seguridad de la Información no se pueda implementar de acuerdo a la hoja de ruta establecida" e incumplimiento a la implementación de la Planeación Estratégica de la Seguridad de la información de TRANSMILENIO S.A., PESI, enmarcada en el Mapa de Ruta de Proyectos del PETIC, Numeral 5.9.1: "Mapa de Ruta de Proyectos", donde dice textualmente: "las estrategias se implementan por medio de proyectos, que tienen un alcance, un tiempo de ejecución, y un costo definidos. Para tener control sobre el trabajo en el largo plazo los proyectos se encadenan de forma que se puedan tener hitos verificables y fases controlables en la implementación de cada estrategia. Para lo anterior se crea el documento: Mapa de Ruta de Proyectos, en donde se especifican cada una de las rutas de los proyectos que están siendo ejecutados en la Entidad desde de la Dirección de TIC, con la respectiva definición de cada uno, así como los productos, metas y fechas de culminación.". Este documento se encuentra anexo al PETI.

Posibles causas identificadas por la Oficina de Control Interno:

1) Falta de seguimiento en la ejecución del PESI, actividades del 2019.

2) Falta de asignación de recursos para la implementación de componentes de la estrategia de seguridad de la Información en Transmilenio S.A.

3) Mayores tiempos en los procesos contractuales.

4) Falta de seguimiento a los controles establecidos en la Matriz de Riesgos del Proceso: Gestión de TIC.

Descripción del riesgo.

1) El Plan Estratégico de Seguridad de la Información no se pueda implementar de acuerdo a la hoja de ruta establecida.

2) Incumplimiento de la Ejecución de la Planeación Estratégica de la Seguridad de la Información PESI.

Descripción del impacto:

1) Pérdida de la confidencialidad, integridad y oportunidad de la información.

2) Los procedimientos definidos por la Dirección de TIC, no se actualicen en su integridad

3) Investigaciones entes de control.

4) Incumplimiento en los lineamientos de la política de Sistema de Gestión de la Seguridad de la Información: SGSI.

Recomendaciones:

1) Planificar y cumplir adecuadamente, las actividades del Mapa de Rutas del SGSI.

2) Implementar un plan de Contingencia, para cumplir con la planeación del PESI.

3) Realizar seguimientos periódicos a la ejecución de la Planeación Estratégica de la Seguridad de la Información, implementando acciones correctivas.

Hallazgo N° 11 – Debilidad en la publicación de los documentos del proceso contractual del Megaproyecto: Centro de Gestión, en el SECOP II

Descripción del hallazgo o situación encontrada:

Con el fin de verificar el cumplimiento de la normatividad vigente relacionada con el cumplimiento del artículo 2.2.1.1.1.7.1 del Decreto 1082 de 2015, se realizó el análisis de la documentación registrada en el SECOP II de los procesos que tienen que ver con el desarrollo de Software contratado por la Entidad. Se revisaron en total 5 contratos seleccionados por la Oficina de Control Interno para verificar lo enunciado, evidenciando que para un proceso (1), equivalente al 20%, se evidenciaron debilidades, en cuanto a la publicación de información incompleta, en el SECOP II, en el siguiente proceso de contratación:

Contrato: CTO753-18
Monto: 5.361.950.000

SECOP II							
FACTURA					Certificado Cumplimiento	Informe Supervisor	Estado SECOP II
Factura	Fecha	Valor Bruto	IVA	Valor Pagar			
U-1	11-ene	450.584.034	85.616.966	536.195.000	Si	Si	Aceptada
U-2	11-feb	450.584.034	85.610.966	536.195.000	No	No	Pagada

INFORMACION SOBRE PAGOS					
Fuente	OP	Fecha	Valor Bruto	Iva	Valor Pagado
U-2	1397	28-feb	450.584.034	85.610.966	536.195.000

Se evidenció que la factura No. U-1, se encuentra en estado: "aceptada", sin embargo, la dependencia no va a proceder con su pago, ya que tiene mal liquidado el valor del IVA. Tampoco se evidencian acciones pertinentes para cambiar al estado "Rechazada", esta factura.

La factura Numero: U-2, no tiene Certificado de Cumplimiento ni informe del Supervisor publicados en el SECOP II, sin embargo, esta fue pagada al proveedor y se encuentra en estado: "Pagada".

Teniendo en cuenta lo anterior, se pudo observar el incumplimiento del artículo 2.2.1.1.1.7.1 del Decreto 1082 de 2015, toda vez que no se encuentra publicada la totalidad de información al

corte de la verificación realizada por la Oficina de Control Interno y que se genera en desarrollo del proceso contractual.

Lo anterior, evidencia la materialización del riesgo de incumplimiento a la normatividad legal vigente.

Posibles causas identificadas por la Oficina de Control Interno:

1) Falta de seguimiento en la publicación de documentos que se generen en desarrollo del proceso contractual.

2) Falta de correcta aplicación de controles definidos por la legislación aplicable y de los requisitos contractuales a los procesos objeto de la muestra.

Descripción del riesgo:

1) Incumplimiento al principio de transparencia, al no publicar la totalidad de información relacionada con los procesos contractuales.

2) Incumplimiento a las directrices normativas

Descripción del impacto:

1) Sanciones e investigaciones

Recomendaciones:

1. Dar efectivo cumplimiento a los puntos de control definidos, de modo que sé que permita llevar el seguimiento de la información que se genere en desarrollo del proceso de contratación, para efectos de realizar su publicación de conformidad a los términos señalados en la norma.

2. Cumplir las disposiciones del Decreto 1082 de 2015 en lo referente a publicación de documentos de los procesos contractuales en el SECOP II.

Hallazgo N° 12 – Debilidad en la supervisión de los contratos relacionada con los aportes al sistema de Seguridad Social para contratos de prestación de servicios personales adscritos a la Dirección de TIC.

Descripción del hallazgo o situación encontrada:

Se evidenció debilidad en el cumplimiento al "Manual de Supervisión e Interventoría" M-DA-015 adoptado por la Entidad, ya que de nueve (9) contratos objeto de la muestra, uno (1) equivalente al 11%, presentó las siguientes debilidades:

1. En el contrato de prestación de servicios profesionales y de apoyo a la gestión CTO347-19, verificadas las planillas de pago al sistema de seguridad social, correspondientes a los meses de: abril, mayo, junio y julio de 2019, no fue realizado el aporte a la Afiliación de Riegos Laborales, sin embargo, las cuentas de cobro fueron avaladas por parte del Supervisor y pagadas por parte de la Entidad.

					Pago Planilla				
No.	**Número Contrato**	**Nombre Contratista**	**C.C.**	**No. Proceso**	**IBC Pagado**	**Salud**	**Pensión**	**ARL**	**Meses**
6 Soi	CTO347-19	VILLAMIL PAEZ RUTH MARCELA	51754054	TMSA-CD-375-2019	4.230.000	528.800	676.800	-	Abril
					4.473.496	559.200	715.800	-	Mayo
					4.473.496	559.200	715.800	-	Junio
					4.473.496	559.200	715.800	-	Julio

Posibles causas identificadas por la Oficina de Control Interno:

2) Inadecuada aplicación de controles definidos por el manual de supervisión e Interventoría M-DA-015.

2) Desconocimiento de los controles definidos en el manual de supervisión e Interventoría M-DA-015, por parte del supervisor del contrato.

Descripción del riesgo:

1) Incumplimiento a los lineamientos internos de la Entidad en cuanto a la supervisión de contratos.

Descripción del impacto:

1) Sanciones e investigaciones

Recomendaciones:

1. Dar efectivo cumplimiento al manual de supervisión e Interventoría M-DA-015.

2. Solicitar a la Dirección Corporativa, asesoría, sensibilización y/o capacitación en la correcta aplicación del Manual de Supervisión en interventoría, de los supervisores de contratos designados en la Dirección de TIC.

RESUMEN DE HALLAZGOS:

No.	Título de Hallazgo	Repetitivo
1	Software no autorizado instalado en los equipos de TRANSMILENIO S.A.	No
2	Acceso no autorizado al sistema directorio activo y actividad en correo corporativo después de desvinculación con TRANSMILENIO S.A.	Si
3	Incumplimiento a los lineamientos para el control de Medios Removibles (copiado de información por medio de puertos USB).	No
4	Incumplimiento a los lineamientos del control de acceso de áreas seguras.	No
5	Incumplimiento a los lineamientos definidos en el Manual M-DT-001: Políticas de la Seguridad y Privacidad de la Información, Numeral 9.6: Políticas de Copias de Respaldos.	No
6	Incumplimiento al procedimiento: P-DT-013: Construcción de Sistemas de Información.	No
7	Incumplimiento al procedimiento P-DT-008: Mantenimiento Equipos de Cómputo.	No
8	Incumplimiento al procedimiento P-DT-009: Soporte Técnico a Usuarios Finales.	No
9	Incumplimiento al manual: M-DT-001: Manual de las Políticas de la Seguridad y la Privacidad de la Información, numeral: 9.2.1.1: Inventario de Activos.	No
10	Incumplimiento a la ejecución de la Planeación Estratégica de la Seguridad de la Información: PESI, del "Mapa de Ruta del SGSI - Gel 2019 - 2020.	No
11	Debilidad en la publicación de los documentos del proceso contractual del Megaproyecto: Centro de Gestión, en el SECOP II.	No
12	Debilidad en la supervisión de los contratos relacionada con los aportes al sistema de Seguridad Social para contratos de prestación de servicios personales adscritos a la Dirección de TIC.	No

RECOMENDACIONES y OPORTUNIDADES DE MEJORA.

1. Definir y/o formalizar un procedimiento de cambios para la plataforma del SIRCI que incorpore todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción.

   - No se cuenta con lineamientos claramente definidos y estructurados para los cambios en la Plataforma del SIRCI. Todos los cambios, incluyendo el mantenimiento de emergencia y parches, relacionados con la infraestructura y las aplicaciones dentro del ambiente de producción, no son administrados formal y controladamente. Los cambios (incluyendo

procedimientos, procesos, sistemas y parámetros del servicio) se deben registrar, evaluar y autorizar previo a la implantación y revisar contra los resultados planeados después de la implantación. Esto garantiza la reducción de riesgos que impactan negativamente la estabilidad o integridad del ambiente de producción, según lo definido en la Norma NTC-ISO-IEC 27001, Numeral A.12.1.2: "Gestión de Cambios".

- Sobre la formalización de requerimientos a las modificaciones para el control de cambios a la plataforma tecnológica del SIRCI, la Oficina de Control Interno revisó los informes de Interventoría del SIRCI, de los meses de agosto y noviembre del 2018 y los meses de marzo y mayo del 2019. En el informe de Interventoría del mes de Agosto de 2018, se evidenció, que el concesionario realizó cambios a la plataforma del SIRCI, que no fueron enviados con el tiempo suficiente para su revisión y respectiva toma de acciones, dificultando que la interventoría pueda realizar su labor para emitir concepto al Ente Gestor para garantizar la gestión de cambios conforme a lo indicado en el contrato. Lo anterior, en razón a que no existe formalizado un procedimiento para que el Concesionario realice la gestión de Cambios apropiada.

2. Gestionar adecuadamente los riesgos asociados al proceso Gestión de TIC, teniendo en cuenta las debilidades evidenciadas y solicitar la respectiva asesoría a la Oficina Asesora de Planeación, como segunda línea de defensa.

La matriz de riesgos versión 3 del proceso Gestión TIC cuenta con tres (3) riesgos, los cuales son muy generales y están calificados desde su etapa inherente en una zona moderada, lo cual no se relaciona con el nivel de importancia e impacto que genera el proceso de Gestión de TIC a la Entidad. Una vez aplicados los controles a los tres (3) riesgos, pasan a una zona de importancia baja, denotando la necesidad de reevaluar un análisis específico al proceso.

Con relación a la matriz de riesgos versión 2 (versión anterior), el proceso Gestión TIC, presentaba veinte (20) controles y se cubría el tema de "La continuidad o integridad en las tecnologías de la información", actualmente la versión 3 presenta ocho (8) controles y no cubre específicamente el tema mencionado. Como resultado de este ejercicio de auditoría dos (2) de los tres (3) riesgos de gestión del proceso equivalentes al 67% se materializaron, lo cual denota la debilidad en el diseño y la aplicación de los controles establecidos. Por otra parte, se evidenció debilidad por parte de la Dirección TIC, como proceso técnico para la implementación y divulgación y publicación en el Micrositio de la Entidad MIPG para todos los procesos de la

Entidad en materia de Seguridad Digital, de conformidad con los lineamientos del Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), del Ministerio de Tecnologías de la Información y las Comunicaciones. (Numeral 4.1.3 Alineación o creación de la política de gestión de riesgo de seguridad digital.) Lo anterior se documentó en la recomendación No. 3

CONCLUSIÓN

Se evidenció que algunas de las desviaciones evidenciadas durante el ejercicio auditor, fueron corregidas al corte del presente documento, no obstante, resulta necesario tomar acciones correctivas tendientes a eliminar la causa de los problemas detectados.

El presente informe fue socializado con el Director de TIC y su equipo de trabajo el pasado 22 de noviembre de 2019.

Los hallazgos y observaciones relacionados en el presente informe corresponden a la evaluación realizada a muestras tomadas, 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.

Se considera importante precisar que al corte del presente informe la Dirección de TIC no ha enviado a la Oficina de Control Interno cinco (5) Planes de mejoramiento derivados de la presente auditoría, teniendo en cuenta que tales documentos fueron enviados por ésta Oficina en noviembre 20, se sobre pasó el tiempo límite de ocho (8) días hábiles, definido en el procedimiento formulación y seguimiento a planes de mejoramiento internos, con código P-CI-010 versión 3, por lo tanto se solicita el envío de dichos documentos a la mayor brevedad posible.

Cualquier información adicional con gusto será suministrada.

Bogotá D.C., 04 de diciembre del 2019.

LUIS ANTONIO RODRÍGUEZ OROZCO

Jefe Oficina de Control Interno

Elaboró: Jorge Iván Flórez Franco – Contratista, German Ortiz Martin – Contratista y Luz Marina Díaz Ramírez, Contratista

Revisó: Luz Marina Díaz Ramírez, Contratista – Oficina de Control Interno.