No. INFORME: OCI-2022-055

PROCESO/SUBPROCESO/ACTIVIDAD

Seguridad de la información al subsistema de recaudo.

EQUIPO AUDITOR

José Luis Soto Dueñas, Contratista - Líder de Auditoría

Diana Elizabeth Patiño Sabogal, Contratista

LÍDERES DEL PROCESO: Dirección Técnica de TIC y Subgerencia Económica.

INFORME DISTRIBUIDO A: Gerente General e integrantes del Comité Institucional de Coordinación del Sistema de Control Interno de TRANSMILENIO S. A.

FECHA REUNIÓN DE APERTURA: 19 de agosto de 2022.

FECHA REUNIÓN DE CIERRE: 6 de septiembre de 2022.

OBJETIVOS

1. Evaluar la administración de los riesgos de gestión y corrupción que aplican a las actividades de seguridad de la información al subsistema de recaudo.
2. Verificar el cumplimiento de las obligaciones del contrato de interventoría al Sistema Integrado de Recaudo, Control e Información y Servicio al Usuario, SIRCI, en especial las obligaciones de seguridad de la información al subsistema de recaudo.
3. Evaluar la efectividad operativa de los controles internos de la actividad auditada.
4. Evaluar el cumplimiento de la normativa externa e interna, considerando las políticas y procedimientos aplicables a la actividad auditada.
5. Identificar posibles riesgos que puedan llegar afectar la consecución de los objetivos estratégicos de la entidad y las actividades relevantes de la actividad auditada.

ALCANCE

La auditoría se realizó con base en las actividades definidas en los contratos número CTO552-21 y CTO533-22 los cuales tienen por objeto la realización de la interventoría al

contrato de concesión No. 001 de 2011 «Diseño, suministro, implementación, operación y mantenimiento del subsistema de recaudo, del subsistema de información y servicio al usuario y del subsistema de integración y consolidación de información; el diseño, suministro, implementación, gestión y mantenimiento del subsistema de control de flota; el suministro de la conectividad; la integración entre el subsistema de recaudo el subsistema de control de flota el subsistema de información y servicio al usuario y el subsistema de integración y consolidación de la información, que conforma el SIRCI, para el sistema integrado de transporte publico de Bogotá D.C.».

Específicamente se revisó la supervisión que realizó TRANSMILENIO S. A. a las actividades reportadas por las interventorías al subsistema de recaudo en relación con las pruebas de vulnerabilidad y seguridad informática, integridad y consistencia de los datos, realización de backups y copias de respaldo y la realización de auditorías sobre políticas de seguridad a las bases de datos, de acuerdo con el anexo 2 «Guia para establecer la metodología ejecución del contrato de interventoría» de los contratos de interventoría en su cláusula 3.2.3. Seguridad de la información en los siguiente literales:

- La interventoría deberá realizar anualmente dos (2) pruebas de vulnerabilidad y seguridad informática sobre el 100% de la infraestructura y aplicaciones de los medios de pago, de los sistemas de información de recaudo y de la infraestructura que los soporta. Así mismo, las pruebas deberán incluir la infraestructura computacional y de comunicaciones del concesionario SIRCI y SISU. El resultado deberá consignarse en un informe ejecutivo y técnico donde se documenten las vulnerabilidades identificadas, su nivel de clasificación, la acción para remediar la vulnerabilidad, los tiempos recomendados de remediación y demás información pertinente técnica necesaria para entender los resultados y su remediación. De igual forma, el informe deberá ser socializado a las partes interesadas de parte del concesionario SIRCI y a TRANSMILENIO S. A. inmediatamente se culmine cada ejercicio de pruebas.
- La interventoría deberá realizar dos (2) veces al año la verificación de copia y restauración de backups de la infraestructura y aplicaciones del concesionario SIRCI. Para esto se debe validar el proceso integridad y consistencia de los datos respaldados

por el concesionario SIRCI y determinar si dicho proceso se lleva a cabo correctamente. Como entregable se deberá construir un informe de resultados de las pruebas realizadas. La revisión deberá realizarse sobre todas las bases de datos de los sistemas de información.

- La interventoría deberá realizar dos (2) auditorías sobre los procedimientos de identificación, autenticación y autorización de usuarios sobre el 100% de la infraestructura y aplicaciones del concesionario SIRCI. De igual forma esta auditoría deberá contemplar la revisión de las políticas de seguridad sobre otros aspectos que se cobijen bajo el control de acceso lógico, tales como el registro de eventos, auditoría y trazabilidad, la administración de seguridad, el monitoreo de accesos al software, sistemas de información, bases de datos y sistema operativo, entre otros. El resultado deberá consignarse en un informe de resultados de auditoría donde se indiquen los hallazgos identificados y el plan de acción para su corrección.

LIMITACIONES AL ALCANCE

No se revisaron informes de auditoría basados en la norma ISO 27001 «Sistemas de Gestión de la seguridad de la información», toda vez que la Dirección Técnica de TIC informó que, en el contrato de concesión del Sistema Integrado de Recaudo, Control e Información y Servicio al Usuario, SIRCI, no se especificó contractualmente que el concesionario debía certificarse en dicha norma. Por lo anterior, no se ejecutaron auditorías que validaran su cumplimiento, por lo que no se consideró objeto de verificación para el presente ejercicio auditor.

DECLARACIÓN

Esta auditoría fue realizada en el análisis de diferentes muestras aleatorias seleccionadas y, la adopción de varios criterios establecidos por los auditores a cargo de la realización del trabajo. Una consecuencia de lo anterior 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

1. Contrato de concesión número. 001 de 2011. Diseño, suministro, implementación, operación y mantenimiento del subsistema de recaudo, del subsistema de información y servicio al usuario y del subsistema de integración y consolidación de información; el diseño, suministro, implementación, gestión y mantenimiento del subsistema de control de flota; el suministro de la conectividad; la integración entre el subsistema de recaudo el subsistema de control de flota el subsistema de información y servicio al usuario y el subsistema de integración y consolidación de la información, que conforma el SIRCI, para el sistema integrado de transporte publico de Bogotá D. C.
2. Contrato número 552 de 2021. Contratar la realización de la interventoría al contrato de concesión no. 001 de 2011.
3. Contrato número 533 de 2022. Contratar la realización de la interventoría al contrato de concesión no. 001 de 2011.
4. Caracterización del proceso, manuales, procedimientos, protocolos, indicadores, mapas de riesgos y demás documentos del Modelo Integrado de Planeación y Gestión - MIPG de TRANSMILENIO S. A. vigente.
5. Manual de supervisión e interventoría, M-DA-015 versión 3 de septiembre de 2019.
6. Políticas de seguridad y privacidad de la información, M-DT-001 versión 5 de diciembre de 201
7. La demás normativa interna y o externa asociada a la actividad auditada.
8. Ley 1474 de 2011- artículo 83 -Supervisión e interventoría contractual-

ABREVIATURAS

CTO: Contrato

DTIC: Dirección de TIC

OCI: Oficina de Control Interno

RB: Recaudo Bogotá

SGE: Subgerencia Económica

SIRCI: Sistema Integrado de Recaudo, Control, Información y Servicio al Usuario

SITP: Sistema Integrado de Transporte Público

TISC: Tarjetas Inteligentes Sin Contacto

TMSA: Empresa de Transporte del Tercer Milenio - TRANSMILENIO S. A.

RIESGOS CUBIERTOS

El trabajo auditor se basó en los riesgos identificados por TRANSMILENIO S. A., y la verificación de gestión de estos por partes de las áreas. Por lo anterior, se presenta algunos riesgos mapeados en las diferentes matrices que ha adoptado la entidad en su Sistema de Gestión de Riesgos.

Riesgos identificados en la entidad

1. Imposibilidad de apoyar técnicamente las necesidades relacionadas con TIC y que afectan los procesos críticos de la entidad.
2. Inadecuada estructuración de los procesos de selección.
3. Cálculo erróneo de la liquidación previa a los agentes del sistema

ESTADO PLAN DE MEJORAMIENTO

La revisión de la información de recaudo involucra dos áreas, la Subgerencia Económica (SGE) encargada de validar la conciliación de ventas y consignaciones de tarjetas inteligentes sin contacto, TISC y, la Dirección de TIC encargada de validar el cumplimiento de estándares de seguridad de la información del subsistema de recaudo a través de la supervisión de las interventorías que TMSA contrata para realizar seguimiento al cumplimiento del contrato de concesión del SIRCI. Por tal razón, a continuación, se relaciona el estado del plan de mejoramiento que tienen vigentes las áreas relacionadas.

La Subgerencia Económica registra, con corte a 30 de junio de 2022, once acciones en estado de ejecución y una acción incumplida, las cuales fueron consignadas en el plan de mejoramiento interno derivado de las auditorías realizadas por la Oficina de Control Interno en la vigencia 2019, 2020 y 2022.

Respecto al plan de mejoramiento de la Dirección de TIC, se evidenciaron siete acciones en ejecución y tres acciones incumplidas.

RESUMEN EJECUTIVO DE LA AUDITORÍA

El desarrollo de la presente auditoría consistió en la validación del cumplimiento de obligaciones contractuales de los contratos de interventoría CTO552-21 y CTO533-22, en los componentes de seguridad de la información al subsistema de recaudo en relación con pruebas de vulnerabilidad y seguridad informática, integridad y consistencia de los datos, realización de backups y copias de respaldo y la realización de auditorías sobre políticas de seguridad a las bases de datos.

Como resultado de lo anterior, no se evidenció el cumplimiento de las actividades revisadas, lo que conllevó a formular recomendaciones que se visualizan al final del presente informe con el propósito de que sean analizadas por las áreas auditadas para la formulación de acciones que aporten a la mejora continua de los procesos.

DESARROLLO DE AUDITORÍA

En la auditoría se verificó el seguimiento a las actividades de validación de la seguridad de la información del subsistema de recaudo del sistema TransMilenio, específicamente se desarrollaron los siguientes pasos:

- **Entendimiento de la actividad auditada**: Se realizaron consultas basadas en la documentación existente de la actividad (manuales, guías, procedimientos, instructivos, mapas de riesgos, contratos de concesión y de interventorías etc.), así como la búsqueda de distintos controles que apliquen las áreas para la gestión de sus riesgos.
- **Revisión de la normativa vigente aplicable**: Se verificó la normativa vigente aplicable para constatar su cumplimiento.
- **Identificación de riesgos y controles**: A través del ejercicio de auditoría se revisaron actividades y controles operativos que se ejecutan para preservar y garantizar la seguridad de la información del subsistema de recaudo del sistema

TransMilenio, así como también algunos de los registrados en los diferentes documentos del MIPG.

- **Elaboración y ejecución del plan de trabajo**: Se llevó a cabo con base en el entendimiento adquirido de las actividades auditadas**,** el cual, durante su desarrollo permitió determinar la existencia, funcionalidad y aplicación de controles.
- **Identificación de hallazgos, recomendaciones y observaciones:** Como resultado de la comparación entre el criterio (la norma o procedimiento aplicable) y la condición (es decir el estado actual), durante el ejercicio auditor se encontraron diferencias entre ambos, lo cual se convirtió en insumo para la elaboración del informe.

Breve descripción de las pruebas de auditoría realizadas

La Oficina de Control Interno durante la ejecución del trabajo de auditoría adelantó las siguientes pruebas:

1. Vulnerabilidad y seguridad informática.

Para el desarrollo de esta prueba se tuvieron en cuenta los 12 informes de supervisión presentados por la interventoría «C&M asesoría y consultoría» mediante el contrato 522 de 2011, que fueron publicados en el SECOP II.

Igualmente, se revisó la información entregada por la Dirección de TIC y se evidenció que la interventoría, de manera formal, solicitó realizar mesas de trabajo con Recaudo Bogotá con el fin de ejecutar las pruebas de vulnerabilidad a la infraestructura tecnológica. Sin embargo, esta última no autorizó las actividades planteadas bajo el argumento de que en el contrato 001 del 2011 quedó establecido que se ejecutarían mediante la herramienta Qualys y se presentarían los resultados obtenidos en las mesas de trabajo.

Teniendo en cuenta lo anterior, Recaudo Bogotá entrega los resultados únicamente de las dos pruebas realizadas a la página web (vínculo: consulte la página de tullave), dejando de evaluar el 100% de la infraestructura, las aplicaciones de los medios de pago, los sistemas de información de recaudo y de la infraestructura que los soporta. Explicando que no está explicito en sus obligaciones ejecutar este tipo de pruebas.

La anterior situación ha impedido que la interventoría C&M pueda dar cumplimiento a 100% de las obligaciones establecidas por Transmilenio, en cuanto a la vulnerabilidad y seguridad informática a las bases de datos del subsistema de recaudo.

Por otra parte, en la información entregada por Recaudo Bogotá se evidenciaron vulnerabilidades clasificadas en un nivel medio y alto, en consecuencia, la interventoría solicitó un plan de acción el cual no fue entregado por Recaudo Bogotá.

Así las cosas, se evidencio un cumplimiento parcial a lo establecido en el anexo 2, guía para establecer la metodología de ejecución del contrato de interventoría del contrato CTO552-21 numeral 3.2.3 seguridad de la información literal 1: «La interventoría deberá realizar anualmente dos (2) pruebas de vulnerabilidad y seguridad informática sobre el 100% de la infraestructura y aplicaciones de los medios de pago, de los sistemas de información de Recaudo y de la infraestructura que los soporta. Así mismo, las pruebas deberán incluir la infraestructura computacional y de comunicaciones del concesionario SIRCI y SISU. El resultado deberá consignarse en un informe ejecutivo y técnico donde se documenten las vulnerabilidades identificadas, su nivel de clasificación, la acción para remediar la vulnerabilidad, los tiempos recomendados de remediación y demás información pertinente técnica necesaria para entender los resultados y su remediación. De igual forma, el informe deberá ser socializado a las partes interesadas de parte del concesionario SIRCI y a TRANSMILENIO S. A. inmediatamente se culmine cada ejercicio de pruebas.»

2. Integridad y consistencia de los datos, realización de backups y copias de respaldo

En la formulación y desarrollo de esta prueba se planteó validar el cumplimiento de la cláusula 3.2.3. correspondiente al componente de seguridad de la información del anexo 2, de la guia para establecer la metodología de ejecución del contrato de interventoría para los contratos 522 de 2021 y 533 de 2022, específicamente del numeral que define:

- La interventoría deberá realizar dos (2) veces al año la verificación de copia y restauración de backups de la infraestructura y aplicaciones del concesionario SIRCI.

Para esto se debe validar el proceso integridad y consistencia de los datos respaldados por el concesionario SIRCI y determinar si dicho proceso se lleva a cabo correctamente. Como entregable se deberá construir un informe de resultados de las pruebas realizadas. La revisión deberá realizarse sobre todas las bases de datos de los sistemas de información.

Una vez definido el criterio a validar el equipo auditor solicitó a la Dirección de TIC, la cual funge como supervisor del contrato de interventoría en su componente de seguridad de la información, los soportes que demostraran el cumplimiento de dicho criterio. La información fue suministrada el 23 de agosto de 2022 y anexaron los informes mensuales detallados en el componente de seguridad de la información para la ejecución de los contratos 522 de 2021 y 533 de 2022. Del análisis de los documentos referenciados se presenta el siguiente resumen:

Tabla 1. Validación de cumplimiento cláusulas contractuales

Número de informe	**Observaciones de los informes de interventoría al componente de seguridad de la información**	**Observaciones OCI**	**¿cumple el criterio?**
1	Para mayo de 2021 la interventoría programó una reunión para el levantamiento de información relacionada con backups y copias de respaldo.	Sin observaciones	No
2	Para junio de 2021 se solicitó a Recaudo Bogotá el procedimiento de copias de respaldo. Como respuesta compartió el documento M-MN016 Backups, quedando pendiente la entrega de los soportes de los meses de mayo y junio 2021.	Sin observaciones	No
3	Para julio de 2021 la interventoría realizó verificación y validación del manual backups. Solicitó, por medio de oficio, los soportes de la realización de backups y soportes de mantenimiento a las bases de datos. Señalaron que previamente los había solicitado por correo electrónico, pero no se tuvo respuesta.	Transcurrido los meses de mayo, junio y julio de 2021, el único avance que tuvo la interventoría en temas de backups y copias de respaldo consistió en obtener el manual de backups de RB	No

Número de informe	Observaciones de los informes de interventoría al componente de seguridad de la información	Observaciones OCI	¿cumple el criterio?
4	Para agosto de 2021 la interventoría solicitó, por medio de oficio, los soportes de realización de backups y soportes mantenimiento a bases de datos. En respuesta Recaudo Bogotá solicitó que se convocara una mesa de trabajo para el 14 de septiembre con las partes interesadas para definir la manera como se debería entregar los soportes.	Para el mes de agosto aún no se ha realizado la verificación de las copias y restauración de backups de la infraestructura y aplicaciones del concesionario del SIRCI.	No
5	Para septiembre de 2021 se realizó la mesa de trabajo. La interventoría le expuso a Recaudo Bogotá las obligaciones contractuales que indican la entrega de las evidencias y soportes de realización de backups y soportes mantenimiento a bases de datos. Recaudo Bogotá indica que el cambio de tecnología hizo que la forma como se generaba y realizaba este procedimiento cambiara y se comprometió a hacer una propuesta de la forma como se puede entregar dicha información.	Para septiembre no se logró evidenciar el cumplimiento de la verificación de las copias y restauración de backups de la infraestructura y aplicaciones del concesionario del SIRCI ya que Recaudo Bogotá informó cambio de tecnología	No
6	Para octubre de 2021 no se reportó avance en el tema de las evidencias y soportes de realización de backups y soportes mantenimiento a bases de datos.	Para octubre tampoco se logró evidenciar el cumplimiento de la verificación de las copias y restauración de backups de la infraestructura y aplicaciones del concesionario del SIRCI, ya que Recaudo Bogotá informó el cambio de tecnología.	No

Número de informe	Observaciones de los informes de interventoría al componente de seguridad de la información	Observaciones OCI	¿cumple el criterio?
7	Para noviembre de 2021 no se reportó avance en el tema de las evidencias y soportes de realización de backups y soportes mantenimiento a bases de datos. Se describen actividades de planes de continuidad (pruebas verificación interfaces, verificación de dispositivos de validación troncal).	Para noviembre no se logró evidenciar el cumplimiento de la verificación de las copias y restauración de backups de la infraestructura y aplicaciones del concesionario del SIRCI ya que Recaudo Bogotá informa cambio de tecnología.	No
8	Para diciembre de 2021 la interventoría solicitó nuevamente los backups de las bases de datos suministradas al ente gestor. Recaudo Bogotá respondió que los backups de las DB de FMS se entregaron a TMSA. El último backups entregado corresponde de enero-marzo de 2019. La Dirección de TIC informa que la fecha de entrega de último backups a TMSA se realizó para marzo de 2022 y corresponde a los datos de mayo y junio de 2019.	Los backups que se relacionan son del año 2019, cumpliendo parcialmente con la obligación del contrato de interventoría revisada, ya que la interventoría no reporta las actividades de restauración de dichas copias de la infraestructura y aplicaciones del concesionario del SIRCI	*SI
9	Para enero de 2022 la interventoría solicitó nuevamente los backups de las bases de datos suministradas al ente gestor. Recaudo Bogotá cuestionó si las restauraciones de copias de respaldo obedecían a una obligación contractual entre RB y TMSA. Ante dicho cuestionamiento la interventoría le indicó que, si bien no estaba explícitamente en el contrato 001 de 2011, ni en sus anexos, si hace parte de las buenas prácticas al momento de realizar una copia de respaldo.	Para enero de 2022 la interventoría no reporta las actividades de restauración de los backups de la infraestructura y aplicaciones del concesionario del SIRCI.	*SI

Número de informe	Observaciones de los informes de interventoría al componente de seguridad de la información	Observaciones OCI	¿cumple el criterio?
10	Para febrero la interventoría solicitó nuevamente los backups de las bases de datos suministradas al ente gestor. Recaudo Bogotá cuestionó si las restauraciones de copias de respaldo obedecían a una obligación contractual entre RB y TMSA. Nuevamente la interventoría le indicó que, si bien no estaba explícitamente en el contrato 001 de 2011, ni en sus anexos, si hace parte de las buenas prácticas al momento de realizar una copia de respaldo.	Para febrero de 2022 la interventoría no reporta las actividades de restauración de los backups de la infraestructura y aplicaciones del concesionario del SIRCI.	*SI
11	Para marzo se realizó una reunión con el área de infraestructura de Recaudo Bogotá, quien explicó a la interventoría el procedimiento de realización de las copias de respaldo de la información generada en el SIRCI y la manera como se realiza la entrega de estas copias de respaldo al ente gestor. De acuerdo con esto, se recibió y validó el acta correspondiente a la última entrega de backups realizada por el concesionario a TMSA el día 17 de marzo de 2022 y que relaciona las copias de respaldo correspondientes a los meses de abril, mayo y junio de 2019 es decir 36 meses atrás. Tal y como se encuentra indicado en el contrato 001 de 2011, con las anteriores verificaciones la interventoría da por aprobada y cerrada la obligación correspondiente.	Para marzo de 2022 la interventoría no reporta las actividades de restauración de los backups de la infraestructura y aplicaciones del concesionario del SIRCI.	*SI

Número de informe	Observaciones de los informes de interventoría al componente de seguridad de la información	Observaciones OCI	¿cumple el criterio?
12	Para abril la interventoría realizó la solicitud de evidencia de entrega de las copias de respaldo de las bases de datos a TMSA con el fin de hacer la última verificación del periodo, preguntando: • ¿En qué tipo de medio reciben las copias de respaldo? • ¿Ustedes verifican la integridad de los archivos recibidos? • ¿Cómo se almacenan estas copias de seguridad?	Para abril de 2022 la interventoría no reporta las actividades de restauración de los backups de la infraestructura y aplicaciones del concesionario del SIRCI.	*SI

Fuente: Evaluación realizada con base en los informes de interventoría del contrato contratos 522 de 2021

*SI: Se evidencia cumplimiento parcial de la obligación del contrato de interventoría del anexo 2 que menciona: «La interventoría deberá realizar dos (2) veces al año la verificación de copia y restauración de backups de la infraestructura y aplicaciones del concesionario SIRCI. Para esto se debe validar el proceso integridad y consistencia de los datos respaldados por el concesionario SIRCI y determinar si dicho proceso se lleva a cabo correctamente. Como entregable se deberá construir un informe de resultados de las pruebas realizadas. La revisión deberá realizarse sobre todas las bases de datos de los sistemas de información».

Lo anterior debido a que Recaudo Bogotá si suministró al ente gestor backups de información de operación correspondiente a marzo, abril, mayo y junio de 2019, transcurridos tres años de consulta en línea, esto de acuerdo con lo establecido en el numeral 5.8 del anexo 2 literal b del contrato de concesión del SIRCI. Sin embargo, no fueron suministrados por Recaudo Bogotá o por la interventoría los soportes para validar la restauración de dichas copias y la validación de la integridad y consistencia de los datos de respaldo.

En igual sentido, se observa en la tabla anterior que la interventoría inició la ejecución de

su contrato realizando un entendimiento y aprendizaje del contrato del SIRCI lo cual le llevó un periodo de cuatro meses, situación que se identifica para mayo, junio y julio de 2021, y el único avance que obtuvo en temas de backups y copias de respaldo fue el de obtener el manual de backups de Recaudo Bogotá.

Para el periodo comprendido entre agosto de 2021 y abril de 2022, esto es nueve meses, la gestión de la interventoría se basó en la solicitud de soportes para dar cumplimiento a la verificación de las copias y restauración de backups de la infraestructura y aplicaciones del concesionario del SIRCI, soportes que no fueron suministrados por Recaudo Bogotá.

En conclusión, el concesionario de Recaudo Bogotá evadió y dilató lo solicitado por la interventoría, hasta que, en el mes de diciembre de 2021, transcurrido aproximadamente ocho meses del contrato de interventoría, lo único que suministró al ente gestor fueron backups de la información de la operación correspondiente a marzo, abril, mayo y junio de 2019, transcurridos tres años de consulta en línea.

3. Auditorías sobre políticas de seguridad de la información a las bases de datos.

Para el desarrollo de esta prueba, el equipo auditor solicitó a la Dirección de TIC los informes remitidos por la interventoría «C&M asesoría y consultoría» respecto las dos auditorías realizadas a los procedimientos de identificación, autenticación y autorización de usuarios sobre el 100% de la infraestructura y aplicaciones del concesionario SIRCI. Así mismo, respecto de la revisión de las políticas de seguridad, entre otros, el control de acceso lógico, el registro de eventos, auditoría y trazabilidad, la administración de seguridad, el monitoreo de accesos al software, sistemas de información, bases de datos y sistema operativo, como se encuentra establecido en el anexo 2 ya citado.

Los informes fueron remitidos por el área auditada y revisados por la Oficina de Control Interno, observando que en estos se encuentran descritos los resultados obtenidos de las validaciones realizadas al procesamiento de los datos relacionados a los procesos de transacción de ventas, transacciones de recarga, transacciones de validación, transacciones de transbordo, transacción de entrada y salida, transacción de viaje a

crédito, transacciones de pasajes vendidos y no utilizados, listas negras y la verificación de la integridad y consistencia de las transacciones de venta.

La información contenida en dichos informes fue avalada por la interventoría «C&M asesoría y consultoría» y reportada para demostrar cumplimiento ante la Dirección de TIC, quien funge como supervisor del contrato de interventoría, de lo establecido en el anexo 2, guía para establecer la metodología de ejecución del contrato de interventoría del contrato CTO552-21, numeral 3.2.3, seguridad de la información literal 11: «La interventoría deberá realizar 2 veces al año, una auditoría técnica que permita revisar el manejo de errores de procesamiento (cambios de fechas, cambios de valores, saltos en consecutivos de transacciones, transacciones erradas, entre otras), sobre el 100% de la infraestructura y sistemas de información del concesionario SIRCI El resultado deberá consignarse en un informe de resultados de auditoría donde se indiquen los hallazgos identificados y el plan de acción para su corrección.»

DESCRIPCIÓN DE LOS RESULTADOS EVIDENCIADOS

Como resultado de las pruebas realizadas y del análisis de la información suministrada por las áreas auditadas, como soporte de la ejecución de controles y de la gestión de las actividades de la supervisión a los contratos de interventoría al SIRCI, se formuló el siguiente hallazgo:

Hallazgo No 1

Debilidad en la supervisión del contrato de interventoría al SIRCI, Sistema Integrado de Recaudo, Control, Información y Servicio al Usuario, debido al cumplimiento parcial en las obligaciones contractuales, en cuanto al componente de seguridad de la información al subsistema de recaudo en dos de tres ítems evaluados:

1. Pruebas de vulnerabilidad y seguridad informática (cumplimiento parcial)
2. Integridad y consistencia de los datos, realización de backups y copias de respaldo. (cumplimiento parcial)
3. Realización de auditorías sobre políticas de seguridad a las bases de datos. (ítem

cumplido)

Descripción del hallazgo o situación encontrada:

Con el propósito de validar el cumplimiento de las obligaciones establecidas en el contrato 522 del 2021, suscrito con la interventoría «C&M asesoría y consultoría» dentro anexo técnico número 2, guía para establecer la metodología de ejecución del contrato de interventoría, en la cláusula 3.2.3. seguridad de la información, de las trece obligaciones definidas en esta cláusula se evaluaron tres. Una vez revisadas las actividades reportadas por la interventoría en los informes de supervisión al componente de seguridad de la información, como se detalló la descripción de las pruebas de auditoría realizadas, se logró evidenciar el cumplimiento para una de ellas consistente en:

- La interventoría deberá realizar dos auditorías sobre los procedimientos de identificación, autenticación y autorización de usuarios sobre el 100% de la infraestructura y aplicaciones del concesionario SIRCI. De igual forma esta auditoría deberá contemplar la revisión de las políticas de seguridad sobre otros aspectos que se cobijen bajo el control de acceso lógico, tales como el registro de eventos, auditoría y trazabilidad, la administración de seguridad, el monitoreo de accesos al software, sistemas de información, bases de datos y sistema operativo, entre otros. El resultado deberá consignarse en un informe de resultados de auditoría donde se indiquen los hallazgos identificados y el plan de acción para su corrección.

Para las dos obligaciones restantes que se evaluaron, se evidenció un cumplimiento parcial. Estas corresponden a:

- La interventoría deberá realizar anualmente dos pruebas de vulnerabilidad y seguridad informática sobre el 100% de la infraestructura y aplicaciones de los medios de pago, de los sistemas de información de Recaudo y de la infraestructura que los soporta. Así mismo, las pruebas deberán incluir la infraestructura computacional y de comunicaciones del concesionario SIRCI y SISU. El resultado deberá consignarse en un informe ejecutivo y técnico donde se documenten las vulnerabilidades identificadas, su nivel de clasificación, la acción para remediar la vulnerabilidad, los tiempos

recomendados de remediación y demás información pertinente técnica necesaria para entender los resultados y su remediación. De igual forma, el informe deberá ser socializado a las partes interesadas de parte del concesionario SIRCI y a TRANSMILENIO S. A. inmediatamente se culmine cada ejercicio de pruebas.

- La interventoría deberá realizar dos veces al año la verificación de copia y restauración de backups de la infraestructura y aplicaciones del concesionario SIRCI. Para esto se debe validar el proceso integridad y consistencia de los datos respaldados por el concesionario SIRCI y determinar si dicho proceso se lleva a cabo correctamente. Como entregable se deberá construir un informe de resultados de las pruebas realizadas. La revisión deberá realizarse sobre todas las bases de datos de los sistemas de información.

Criterios evaluados:

1. Manual de supervisión e interventoría M-DA-15, en su versión 3 de septiembre de 2019, en el numeral 9. Funciones del interventor y o supervisor, 9.1. actividades generales, literales a). Exigir al contratista el cumplimiento de las obligaciones previstas en el contrato, g). Identificar las necesidades de cambio o ajuste y sugerir las medidas que considere necesarias para la mejor ejecución del objeto pactado. o). Originar, apoyar y sustentar los procesos de incumplimiento parcial o total, la caducidad del contrato, la imposición de multas de conformidad con el procedimiento establecido por la ley y TRANSMILENIO S. A.
2. Ley 1474 de 2011- artículo 83 -Supervisión e interventoría contractual.

RECOMENDACIONES

1. Evaluar la participación que tiene la Dirección de TIC en su rol de supervisor, en las mesas de trabajo que se realice entre la interventoría y Recaudo Bogotá, esto con el fin de conocer de manera directa el efectivo cumplimiento de las obligaciones establecidas en cada uno de los contratos.
2. Fortalecer el acompañamiento por parte del ente gestor al cumplimiento de las actividades que adelante la interventoría del contrato de concesión del SIRCI y de los

posibles inconvenientes que se conozcan en las mesas de trabajo en que participe la Dirección de TIC, esto con el fin de dirimir las situaciones dónde el concesionario no suministre o impida el acceso a la información.

3. Analizar las obligaciones contractuales establecidas con Recaudo Bogotá y, a partir de estas definir la manera más efectiva en que la interventoría puede desarrollar las obligaciones de supervisión al contrato del SIRCI, respecto del componente de seguridad de la información.
4. Consolidar las lecciones aprendidas en materia de seguridad de la información, derivadas de la supervisión al contrato de concesión del SIRCI a través de las diferentes interventorías. Lo anterior, con el propósito de plantear nuevas estrategias que puedan ser consignadas en el clausulado de un futuro contrato del SIRCI en pro del buen servicio al usuario y de poder validar cualquier información que sea gestionada por el concesionario de recaudo, brindando la oportunidad de realizar auditorías permanentes en temas seguridad de la información con estándares de las mejores prácticas y normas técnicas existentes.
5. Evaluar la posibilidad de realizar la supervisión al contrato de concesión del SIRCI directamente por TRANSMILENIO S. A., ya que las interventorías contratadas emplean un gran porcentaje del periodo del contrato para entender las actividades de recaudo y, una vez culmina la curva de aprendizaje se encuentran con prácticas evasivas del concesionario del SIRCI y al final del contrato se presentan incumplimientos o cumplimientos parciales de algunas de las obligaciones contractuales. En caso de considerar necesaria la contratación de la interventoría a la concesión del SIRCI, analizar la posibilidad de que dicho contrato tenga vigencia superior a un año.

SOLICITUD PLAN DE MEJORAMIENTO

De acuerdo con lo establecido en el procedimiento formulación y seguimiento a planes de mejoramiento internos, con código P-CI-010, versión 3 de septiembre de 2019, las áreas responsables deberán suscribir, dentro de los ocho días hábiles siguientes a la recepción

del informe, el respectivo plan de mejoramiento consolidado con acciones correctivas, preventivas y de corrección que eliminen las causas de los hallazgos.

Para lo anterior, si las áreas responsables de las actividades auditadas lo consideran, la Oficina de Control Interno dentro del rol de asesoría puede acompañar en la formulación metodológica del plan de mejoramiento.

Los resultados y recomendaciones relacionados en el presente informe corresponden a la evaluación de una muestra realizada conforme a la planeación del trabajo de auditoría dentro del alcance establecido, como se comentó inicialmente, es responsabilidad del área auditada efectuar una revisión de carácter general sobre los aspectos evaluados.

El presente informe fue socializado el 2 y 5 de septiembre de 2022 a la Dirección de TIC y sus respectivos equipos de trabajo.

Bogotá D. C., 09 de septiembre de 2022

SANDRA JEANNETTE CAMARGO ACOSTA

Jefe Oficina de Control Interno

Elaboró: José Luis Soto Dueñas, Contratista - Oficina de Control Interno.
Diana Elizabeth Patiño Sabogal, Contratista - Oficina de Control Interno.

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