N° INFORME: OCI-2026-026

DENOMINACIÓN DEL TRABAJO: Seguimiento al cumplimiento del Modelo de Seguridad y Privacidad de la Información - MSPI

EQUIPO AUDITOR:

- Diana Elizabeth Patiño Sabogal – Contratista

DESTINATARIOS:

Integrantes Comité Institucional de Coordinación de Control Interno (CICCI)

Responsable de la(s) actividad(es) auditada(s): Director de TIC

OBJETIVO(S)

- Verificar el cumplimiento de los lineamientos establecidos en la Resolución 500 de 2021 y su Anexo 1 (versión 5), relacionados con la adopción e implementación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad.

MARCO NORMATIVO

Normativa Externa

- Resolución 500 de 10 de marzo de 2021 - Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) “Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital”.
- Norma ISO 27001:2013 Sistema de Gestión de Riesgos y Seguridad de la Información.
- Documento Maestro de Los Lineamientos del Modelo de Seguridad y Privacidad de la Información. Versión 5 del 21/04/2025, emitido por el Ministerio de Tecnologías de la Información y las Comunicaciones.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Normativa Interna

- Política de seguridad y privacidad de la información (Código L-DT-002) versión 7 de abril de 2025.
- Manual para la gestión del riesgo en TRANSMILENIO S.A. Anexo 3 riesgos de seguridad de la información (Código M-OP-002) versión 7 de julio de 2024.
- Manual del sistema de gestión de seguridad de la información (SGSI) (Código M-DT-004) versión 0 de marzo de 2022.
- Plan de cultura y sensibilización del Sistema de Gestión de Seguridad de la Información - SGSI (Código T-DT-007) versión 1 de diciembre de 2021.
- Resolución 133 de 02 de mayo de 2024 “Por la cual se actualiza el Comité Institucional de Gestión y Desempeño de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A”, vigente hasta el 17 de marzo de 2026.
- Resolución 095 de 18 de marzo de 2026 “Por la cual se actualiza el Comité Institucional de Gestión y Desempeño de la Empresa de Transporte del Tercer Milenio TRANSMILENIO S.A”
- Instructivo para la identificación, valoración y clasificación de activos de información (Código I-DT-001) versión 1 de octubre de 2021.

ALCANCE

El alcance del presente trabajo de cumplimiento se definió con fundamento en los lineamientos establecidos para el Modelo de Seguridad y Privacidad de la Información (MSPI), contenidos en la Resolución 500 de 2021 y demás instrumentos expedidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Período auditado: 01 de enero de 2025 al 30 de abril de 2026

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Nota: El establecimiento de este período no limitaba la facultad de la Oficina de Control Interno para pronunciarse sobre hechos previos o posteriores que, por su nivel de riesgo o materialidad, deban ser revelados.

LIMITACIONES AL ALCANCE

No se presentaron limitaciones en el alcance determinado para esta auditoría interna.

METODOLOGÍA

En atención a los lineamientos normativos y procedimentales aplicables a las Oficinas de Control Interno, en la realización de este trabajo de cumplimiento se aplicó un enfoque sistemático y disciplinado que abarcó tres (3) fases: planeación del trabajo, desempeño o ejecución de pruebas de auditoría y comunicación de resultados, en las cuales se llevaron a cabo las siguientes actividades:

Planeación del trabajo

Durante el desarrollo de la etapa de planeación se realizaron solicitudes de información relacionadas con los siguientes temas:

Tabla 1. Trazabilidad Fase de Planeación

Actividad Realizada	Fecha de solicitud	Fecha de respuesta
Riesgos de seguridad identificados por la Dirección TIC.	12-may-2026	15-may-2026
Plan Institucional de Capacitaciones – PIC para la vigencia 2025 y 2026	27-may-2026	25-may-2026

Fuente: *Elaboración propia con datos generados u obtenidos en la fase de planeación.*

Desempeño o ejecución

En desarrollo de la etapa de ejecución, el equipo auditor verificó y analizó la información suministrada por la Dirección TIC y la Dirección Corporativa, contrastándola con la normativa

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

aplicable, los procedimientos internos y demás documentos soporte relacionados con el Modelo de Seguridad y Privacidad de la Información (MSPI), con el propósito de determinar el nivel de cumplimiento de los criterios objeto de evaluación, a través de la verificación y/o validación de los siguientes datos o información:

Tabla 2. Trazabilidad Fase de Ejecución

Actividad Realizada	Fecha de inicio	Fecha fin
Diagnóstico de seguridad de la información documentado en el Instrumento de Identificación de la Línea Base de Seguridad, conforme a los lineamientos del MSPI.	19-may-2026	20-may-2026
Adopción, aprobación y divulgación de la Política de Seguridad y Privacidad de la Información.	21-may-2026	21-may-2026
Formulación, implementación y seguimiento del Plan de Tratamiento de Riesgos de seguridad y privacidad de la información.	21-may-2026	23-may-2026
Roles y responsabilidades asociados al MSPI.	25-may-2026	26-may-2026
Formulación, ejecución y seguimiento del Plan de Comunicación, Capacitación, Sensibilización y Concientización en seguridad y privacidad de la información.	26-may-2026	29-may-2026
Definición, documentación y formalización de los límites, alcance y aplicabilidad del MSPI.	29-may-2026	30-may-2026
Asignación, formalización y divulgación de las funciones de seguridad y privacidad de la información.	01-jun-2026	01-jun-2026
Identificación, valoración, tratamiento y seguimiento de los riesgos de seguridad y privacidad de la información.	01-jun-2026	02-jun-2026
Identificación, actualización y clasificación de los activos de información e infraestructura crítica, conforme a los lineamientos del MSPI.	03-jun-2026	05-jun-2026

Fuente: *Elaboración propia con datos generados u obtenidos en la fase de ejecución.*

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Comunicación de resultados

Mediante correo electrónico del 11 de junio de 2026, se comunicó a la Dirección de TIC el contenido del informe preliminar, con el fin de poner en su conocimiento los resultados preliminares obtenidos en el Seguimiento y, asimismo, conceder el derecho a réplica, a través de la formulación de respuestas, comentarios u observaciones que fueran consideradas por dicha dirección como responsable de la unidad auditada. Al respecto, la Dirección TIC no emitió observaciones o respuestas frente a los resultados entregados en el informe preliminar.

DESCRIPCIÓN DE LOS RESULTADOS Y RECOMENDACIONES

Como resultado del ejercicio de seguimiento al cumplimiento del Modelo de Seguridad y Privacidad de la Información (MSPI), y con base en las pruebas de auditoría realizadas y el análisis de la información suministrada por las dependencias involucradas, a continuación, se presentan los resultados obtenidos en cada una de las siguientes temáticas:

1. DIAGNÓSTICO

Observación 1: Debilidades en la aplicación y soporte del diagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI)

De conformidad con lo establecido en la Resolución 500 de 2021 y en el Anexo 1 “Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información”, la fase de diagnóstico constituye un elemento fundamental para determinar el estado real de implementación de la seguridad y privacidad de la información en la entidad, mediante la aplicación del instrumento de evaluación MSPI, la identificación de los controles implementados y la medición objetiva de su nivel de madurez.

En desarrollo del presente seguimiento, la Oficina de Control Interno realizó la revisión integral de la matriz de autodiagnóstico MSPI correspondiente a la vigencia 2025, remitida por la Dirección TIC mediante correo electrónico del 15 de mayo de 2026, con el propósito

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

de verificar la integridad, disponibilidad, trazabilidad, consistencia y soporte de la información reportada. Como resultado de la validación efectuada, se evidenciaron debilidades relacionadas con la ausencia de soportes documentales verificables, información desactualizada respecto de responsables y áreas involucradas, registro de enlaces o rutas de acceso que no permitían visualizar la documentación relacionada y reportes de porcentajes de cumplimiento sin evidencias que demostraran la ejecución de las actividades correspondientes a las fases del ciclo PHVA (Planear, Hacer, Verificar, Actuar).

Adicionalmente, se evidenció que durante el Comité Institucional de Gestión y Desempeño realizado el 27 de octubre de 2025, la Dirección TIC informó que la entidad había alcanzado un nivel de madurez “Optimizado”, con una calificación de 82 sobre 100. No obstante, la revisión realizada por la Oficina de Control Interno permitió establecer que dicho resultado correspondía exclusivamente a la evaluación de efectividad de los controles definidos en la norma ISO 27001:2013, Anexo A, sin que se informara que el avance reportado para las cláusulas del modelo de operación bajo el enfoque PHVA correspondía al 41 % y que la evaluación del componente de ciberseguridad basado en el marco del Instituto Nacional de Estándares y Tecnología (NIST, por sus siglas en inglés) presentaba un resultado de 0 %, situación que no reflejaba de manera integral el nivel de implementación del MSPI en la entidad.

Para la vigencia 2026, la Dirección TIC implementó el nuevo instrumento de autodiagnóstico definido por el Ministerio de Tecnologías de la Información y las Comunicaciones, reportando un nivel de cumplimiento del 73 % en la evaluación de efectividad de controles asociados a la ISO 27001:2022. Con el fin de verificar la razonabilidad de este resultado, la Oficina de Control Interno seleccionó una muestra aleatoria de cuatro controles y realizó la validación de las evidencias reportadas frente a los criterios de evaluación establecidos en el instrumento. Como resultado de esta revisión

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

se identificaron inconsistencias entre las evidencias suministradas, las pruebas exigidas por el Ministerio y las calificaciones asignadas por la Dirección TIC.

Frente al componente correspondiente a las cláusulas del modelo de operación bajo el ciclo PHVA, la Dirección TIC reportó un avance del 68 %, resultado superior al 41 % informado en la vigencia 2025. No obstante, se observó que dicho incremento obedece principalmente a la modificación de la ponderación de los componentes evaluados en el instrumento de autodiagnóstico para la vigencia 2026. En efecto, el componente de Planificación pasó de representar el 40 % al 56 % de la calificación total, mientras que los componentes restantes redujeron su participación del 20 % al 14 %, situación que incidió directamente en el resultado final reportado. Por lo anterior, el incremento observado no necesariamente refleja una mejora proporcional en la implementación de los requisitos evaluados.

Adicionalmente, persistieron debilidades relacionadas con la ausencia de soportes suficientes que permitieran verificar el cumplimiento de los criterios reportados. Como ejemplo de ello, en el numeral 6.1 “Acciones para tratar los riesgos” se registró como evidencia únicamente la existencia de riesgos identificados sin aportar documentación que permitiera verificar su implementación, seguimiento o tratamiento. Situaciones similares fueron evidenciadas en los numerales 7.1 “Recursos” y 8.2 “Apreciación de riesgos”, donde la información reportada no contó con soportes suficientes o incluyó responsabilidades que no corresponden a las funciones de las dependencias mencionadas.

De igual manera, se observó una inconsistencia en la valoración reportada para el numeral 10 “Mejora”, al asignarse un nivel de cumplimiento del 60 %, pese a que la evidencia registrada indicaba que el sistema aún se encontraba en fase de implementación, situación que no guarda correspondencia con los criterios de evaluación definidos en el instrumento de autodiagnóstico.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Finalmente, respecto al componente de mejores prácticas de ciberseguridad basado en el marco NIST, la Dirección TIC reportó un nivel de cumplimiento del 69 %. No obstante, la estructura del instrumento no contempla el registro de evidencias que soporten las respuestas consignadas, situación que limitó a la Oficina de Control Interno para verificar la veracidad, consistencia y razonabilidad de los resultados reportados.

En consecuencia, se evidencian debilidades en la aplicación, documentación, soporte y validación del diagnóstico del Modelo de Seguridad y Privacidad de la Información, lo que afecta la confiabilidad de los resultados reportados y limita la capacidad de la entidad para determinar de manera objetiva su nivel real de madurez y avance en la implementación de los controles de seguridad de la información y ciberseguridad.

Recomendación:

Fortalecer la aplicación del instrumento de autodiagnóstico del Modelo de Seguridad y Privacidad de la Información (MSPI), garantizando que los resultados reportados se encuentren soportados mediante evidencias verificables, actualizadas, trazables y suficientes, de manera que reflejen objetivamente el nivel de implementación, madurez y efectividad de los controles de seguridad de la información y ciberseguridad en la entidad.

2. ADOPCIÓN DE LA POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Observación 2: Desactualización del acto administrativo de adopción del Modelo de Seguridad y Privacidad de la Información (MSPI)

La Dirección TIC, mediante correo electrónico del 14 de mayo de 2026, remitió la Resolución No. 355 de 2022, mediante la cual TRANSMILENIO S.A. adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) como habilitador de la Política de Gobierno Digital y la estrategia de seguridad digital de la entidad.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Al verificar el contenido del artículo primero de dicho acto administrativo, se evidenció que la adopción del modelo se fundamentó en la Resolución No. 500 del 10 de marzo de 2021 expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones y en el Anexo No. 1 vigente para ese momento. No obstante, se observó que posteriormente el marco normativo del MSPI fue actualizado mediante la Resolución No. 746 del 11 de marzo de 2022 y, más recientemente, mediante la Resolución No. 7722 de 2025, que actualizó el documento maestro de lineamientos del modelo.

Pese a las modificaciones efectuadas por el Ministerio de Tecnologías de la Información y las Comunicaciones, no se evidenció la actualización del acto administrativo adoptado por la entidad ni la realización de acciones orientadas a revisar y ajustar formalmente la adopción del modelo frente a los cambios normativos vigentes, situación que genera una brecha entre el marco regulatorio actualmente aplicable y el instrumento mediante el cual la entidad formalizó la adopción del MSPI.

Lo anterior evidencia debilidades en las actividades de revisión, actualización y mantenimiento del Modelo de Seguridad y Privacidad de la Información, incumpliendo lo establecido en el Documento Maestro de los Lineamientos del Modelo de Seguridad y Privacidad de la Información (en adelante, documento maestro MSPI), numeral 7.2.1 “Liderazgo y compromiso”, que dispone la realización de revisiones periódicas de la adopción del modelo, así como lo señalado en el numeral 7.2.2 “Política de seguridad y privacidad de la información”, relacionado con la observancia de la normatividad vigente y la actualización periódica de las medidas de seguridad para garantizar su adecuación frente a los cambios normativos, tecnológicos y de riesgos.

Así mismo, la situación observada no se encuentra alineada con lo establecido en el documento interno L-DT-002 “Política de Seguridad y Privacidad de la Información”, versión 7 de abril de 2025, el cual establece que las políticas de seguridad de la

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

información deben revisarse al menos una vez al año o cuando se presenten cambios significativos, con el fin de garantizar su conveniencia, adecuación y eficacia continua.

Recomendación

Actualizar el acto administrativo mediante el cual se adoptó el Modelo de Seguridad y Privacidad de la Información (MSPI) en la entidad, incorporando las disposiciones contenidas en la normatividad vigente emitida por el Ministerio de Tecnologías de la Información y las Comunicaciones, y establecer mecanismos periódicos de revisión normativa que permitan asegurar la actualización oportuna de los instrumentos, políticas y lineamientos asociados al modelo.

3. PLAN DE TRATAMIENTO DE RIESGOS

Observación 3: Debilidades en la valoración, tratamiento y seguimiento de los riesgos de seguridad de la información

La Dirección TIC, mediante correo electrónico del 15 de mayo de 2026, remitió la matriz denominada “Matriz de Riesgos de Seguridad Digital Dirección TIC 2025”, la cual fue considerada por la Oficina de Control Interno como el instrumento vigente para la administración de los riesgos de seguridad de la información, teniendo en cuenta que correspondió a la única matriz suministrada en respuesta al requerimiento realizado para verificar la información vigente al 30 de abril de 2026.

Con base en la revisión efectuada a los dieciséis (16) riesgos documentados en dicha matriz y su contraste con los lineamientos establecidos en el numeral 7.3.2 “Valoración de los riesgos de seguridad de la información” del documento maestro MSPI, se evidenciaron debilidades que afectan la adecuada identificación, valoración, administración y seguimiento de los riesgos de seguridad de la información, toda vez que, se observó que los riesgos identificados no se encuentran asociados a procesos específicos de la entidad,

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

lo que dificulta establecer de manera clara la responsabilidad sobre su gestión, monitoreo y tratamiento.

Adicionalmente, se evidenciaron inconsistencias en la identificación de los activos relacionados con los riesgos, en razón a que se incluyeron sistemas de información que ya no hacen parte de la entidad, como VIHANET, así como profesionales, contratistas y activos de hardware registrados de forma genérica, sin especificar los elementos objeto de protección. Lo anterior afecta la calidad de la información utilizada para la valoración y administración de los riesgos de seguridad de la información.

De igual forma, no se evidenció la definición del apetito de riesgo de la entidad ni la comparación entre los resultados obtenidos en el análisis de riesgos y los criterios de riesgo establecidos en el MSPI, elementos necesarios para determinar la aceptabilidad de los riesgos identificados y establecer prioridades para su tratamiento. Así mismo, no se observó un ejercicio de priorización de riesgos que permitiera orientar la toma de decisiones y la asignación de recursos para su mitigación.

Respecto de la asignación de responsabilidades, se identificó que la matriz no contempla un responsable integral para cada riesgo, registrando únicamente responsables asociados a algunos controles. Esta situación se ve agravada por el hecho de que, de los ciento dos (102) controles definidos para los dieciséis (16) riesgos identificados, setenta y tres (73) controles (71,56% del total) no cuentan con responsable asignado. Adicionalmente, se evidenció que algunos responsables correspondían a funcionarios o contratistas que ya no hacían parte de la Dirección TIC o de la entidad, así como dependencias que no han sido actualizadas conforme a la estructura organizacional vigente, afectando la trazabilidad y la gestión efectiva de los controles definidos.

Por otra parte, no se evidenciaron actividades de monitoreo o seguimiento a los controles implementados, situación que impide determinar su efectividad y limita la capacidad de la

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

entidad para identificar oportunamente desviaciones o fallas en la gestión de los riesgos de seguridad de la información.

En relación con el tratamiento de los riesgos, la Dirección TIC suministró como soporte el documento M-OP-001 “Manual para la Gestión del Riesgo en TRANSMILENIO S.A.” y su Anexo 1 “Metodología para la Administración de los Riesgos de Gestión”. No obstante, de acuerdo con lo establecido en dicho documento, los riesgos clasificados en nivel alto o extremo deben contar con un plan de tratamiento que incluya acciones, responsables y fechas de implementación. Frente a este requisito, se evidenció que diez (10) de los dieciséis (16) riesgos registrados en la matriz presentan una valoración “Alta”; sin embargo, no se observaron planes de tratamiento formulados para dichos riesgos ni evidencias de su aprobación por parte del Comité Institucional de Gestión y Desempeño, tal como lo exigen los lineamientos del MSPI.

Las situaciones descritas evidencian debilidades en la gestión integral de los riesgos de seguridad de la información, particularmente en las etapas de identificación, valoración, asignación de responsabilidades, seguimiento, tratamiento y aprobación de los riesgos, limitando la capacidad de la entidad para administrar de manera efectiva los riesgos de seguridad digital y garantizar la implementación de controles orientados a su mitigación.

Recomendación

Fortalecer el proceso de gestión de riesgos de seguridad de la información mediante la actualización integral de la matriz de riesgos, la definición del apetito de riesgo institucional, la asignación formal de responsables para los riesgos y controles, la implementación de mecanismos de seguimiento periódico y la formulación, aprobación y monitoreo de los planes de tratamiento requeridos para los riesgos clasificados en niveles altos o extremos, conforme a los lineamientos establecidos en el Modelo de Seguridad y Privacidad de la Información (MSPI).

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

4. ROLES Y RESPONSABLIDADES

Observación 4: Fortalecimiento de la gestión documental asociada a los roles y responsabilidades de seguridad de la información

De acuerdo con la información suministrada por la Dirección TIC mediante correo electrónico del 14 de mayo de 2026, se evidenció que la entidad cuenta con documentación orientada a la definición de roles asociados a la seguridad y privacidad de la información. En particular, el documento L-DT-002 “Política de Seguridad y Privacidad de la Información”, versión 7 de abril de 2025, establece en su numeral 6 “Autoridades y roles de seguridad de la información” los siguientes roles: Comité Institucional de Gestión y Desempeño, Profesional Especializado Seguridad Informática, Profesional Especializado Procesos Corporativos, Operador de Seguridad de la Información, Propietarios de Activos de Información y Usuarios de la Información.

Por otra parte, se evidenció que el documento M-DT-004 “Manual del Sistema de Gestión de Seguridad de la Información (SGSI)” sí contempla responsabilidades específicas para diferentes actores involucrados en la operación y gestión de la seguridad de la información, entre ellos trabajadores oficiales y contratistas de la Dirección TIC, administradores de infraestructura, técnicos de mesa de ayuda, propietarios de activos de información, usuarios de la información y el Director TIC como responsable del Modelo de Seguridad y Privacidad de la Información.

Adicionalmente, se verificó que la entidad dispone de personal de planta y contratistas que apoyan la implementación y operación del MSPI, evidenciándose la existencia de capacidades institucionales para el desarrollo de las actividades relacionadas con la seguridad de la información.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Recomendación

Fortalecer la gestión documental asociada a los roles y responsabilidades de seguridad y privacidad de la información, asegurando la consistencia, actualización y articulación de la información contenida en los diferentes documentos que conforman el Sistema de Gestión de Seguridad de la Información, con el fin de facilitar su consulta, comprensión y aplicación por parte de los actores involucrados en la implementación y operación del MSPI**.**

5. PLAN DE COMUNICACIÓN, CAPACITACIÓN, SENSIBILIZACIÓN Y CONCIENTIZACIÓN

Observación 5: Debilidades en la ejecución del Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información

Durante la revisión realizada se evidenció que la Subdirección de Talento Humano incorporó en los Planes Institucionales de Capacitación de las vigencias 2025 y 2026 diferentes temáticas relacionadas con tecnología, transformación digital e inteligencia artificial. No obstante, estas actividades corresponden a procesos de formación institucional y no sustituyen las actividades de sensibilización, concientización y fortalecimiento de la cultura de seguridad de la información definidas en el documento T-DT-007 “Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información”, cuya ejecución es responsabilidad de la Dirección TIC.

De acuerdo con la información suministrada por la Dirección TIC mediante correo electrónico del 15 de mayo de 2026, para la vigencia 2025 se programaron seis (6) charlas de sensibilización, con una duración de una (1) hora cada una, y cinco (5) microcharlas de treinta (30) minutos. Sin embargo, se evidenció que únicamente fue desarrollada una (1) charla de sensibilización el 20 de mayo de 2025, mientras que las demás actividades fueron reprogramadas debido a cambios internos de actividades y personal. Igualmente, la programación de microcharlas con una duración de treinta (30) minutos no se encuentra

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

alineada con lo establecido en el numeral 3.6.1 del documento T-DT-007, el cual dispone que las sesiones de sensibilización deben contar con una duración mínima de una (1) hora.

Para la vigencia 2026 se programaron siete (7) charlas de sensibilización y nueve (9) microcharlas; no obstante, se evidenció que una de las actividades programadas para el mes de mayo de 2026 no había sido ejecutada al momento de la verificación, situación que refleja retrasos frente al cronograma definido por la dependencia.

Por otra parte, la revisión realizada permitió evidenciar la no ejecución o falta de desarrollo integral de los temas definidos en el numeral 3.3 del Plan de Cultura y Sensibilización, entre ellos la Política de Gobierno Digital y el MSPI, la Política de Seguridad de la Información de TRANSMILENIO S.A., la gestión de incidentes de seguridad, los delitos informáticos y la ingeniería social. Tampoco se observó la realización de la actividad “Día de la Seguridad de la Información” durante la vigencia 2025, la cual debió ser ejecutada el 28 de noviembre de 2025, ni la ejecución de actividades complementarias de divulgación contempladas en el plan, tales como la publicación de piezas de papel tapiz institucional y la utilización del eslogan institucional “La seguridad de la información está en tus manos” dentro de las estrategias de sensibilización y concientización.

Las situaciones descritas evidencian debilidades en la ejecución, seguimiento y cumplimiento del Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información, limitando el fortalecimiento de la cultura de seguridad de la información y la toma de conciencia de funcionarios, contratistas y demás partes interesadas frente a sus responsabilidades en la protección de la información institucional.

Recomendación

Ejecutar y monitorear de manera integral las actividades definidas en el Plan de Cultura y Sensibilización del Sistema de Gestión de Seguridad de la Información, garantizando el cumplimiento de la programación aprobada, el desarrollo de los temas establecidos, la

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

realización de las actividades de divulgación previstas y la implementación de acciones que permitan medir su efectividad y cobertura dentro de la entidad.

6. MSPI: LÍMITES, ALCANCE Y APLICABILIDAD

Observación 6: Ausencia de definición formal del alcance del Modelo de Seguridad y Privacidad de la Información (MSPI)

De acuerdo con la información suministrada por la Dirección TIC el 15 de mayo de 2026, para el cumplimiento de este requisito la entidad remitió el documento M-DT-004 "Manual del Sistema de Gestión de Seguridad de la Información (SGSI)", versión 0 de marzo de 2022.

Durante la revisión realizada se evidenció que dicho documento se encuentra orientado a la gestión y operación del Sistema de Gestión de Seguridad de la Información (SGSI), incorporando elementos relacionados con el contexto de la entidad, la política y objetivos de seguridad de la información, la gestión de riesgos, la declaración de aplicabilidad, los roles y responsabilidades, así como el alcance definido para el SGSI; no obstante, el requisito establecido en los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) exige la definición formal de los límites, alcance y aplicabilidad del modelo dentro del esquema de operación por procesos de la entidad, especificando los procesos y los recursos humanos, financieros, técnicos y tecnológicos sobre los cuales aplica su implementación.

Frente a este requisito, no se evidenció un documento formal que establezca el alcance del MSPI ni la identificación específica de los procesos, recursos y activos que se encuentran cubiertos por el modelo. En consecuencia, no fue posible verificar la delimitación del alcance del MSPI conforme a los criterios definidos en la Resolución 500 de 2021 y en el documento maestro MSPI.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Como información complementaria, la Dirección TIC remitió los documentos en estado borrador correspondientes al proyecto de resolución para la adopción del “Plan de Control Operacional del Modelo de Seguridad y Privacidad de la Información (MSPI)” y el documento T-DT-014 “Plan de Control Operacional del Modelo de Seguridad y Privacidad de la Información (MSPI)”. La revisión efectuada permitió evidenciar avances orientados a la implementación de los lineamientos del modelo, incorporando componentes relacionados con gestión de riesgos, evaluación de madurez, controles de seguridad y enfoque PHVA; no obstante, se identificaron debilidades en aspectos relacionados con la definición específica del alcance del modelo, la diferenciación conceptual entre SGSI y MSPI, la formalización de la gobernanza y la identificación concreta de los procesos, recursos y activos cubiertos por su implementación.

Lo anterior evidencia que la entidad no cuenta formalmente con la definición del alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), situación que limita la determinación de los procesos, recursos y activos sobre los cuales aplica el modelo y dificulta la implementación, seguimiento y evaluación de sus lineamientos.

Recomendación

Definir, documentar y formalizar el alcance del Modelo de Seguridad y Privacidad de la Información (MSPI), estableciendo de manera clara sus límites, aplicabilidad, procesos, recursos humanos, financieros, técnicos y tecnológicos involucrados, conforme a los lineamientos establecidos en la Resolución 500 de 2021 y el documento maestro MSPI, garantizando su articulación con el Sistema de Gestión de Seguridad de la Información de la entidad.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

7. ASIGNACIÓN FUNCIONES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Observación 7: Oportunidades de fortalecimiento en la formalización de las funciones de gobernanza del Modelo de Seguridad y Privacidad de la Información (MSPI)

En cumplimiento del numeral 7.2.1 “Liderazgo y Compromiso” del Anexo 1 de la Resolución 500 de 2021, la Oficina de Control Interno verificó la Resolución 095 del 18 de marzo de 2026, mediante la cual se actualizó el Comité Institucional de Gestión y Desempeño de TRANSMILENIO S.A.

Como resultado de la revisión efectuada, se evidenció que el acto administrativo establece la conformación, funcionamiento y responsabilidades generales del Comité Institucional de Gestión y Desempeño, así como aspectos relacionados con la implementación de las políticas del Modelo Integrado de Planeación y Gestión (MIPG). De igual forma, se observó que la Dirección TIC lidera la Política de Seguridad Digital y que el Director de Tecnologías de la Información y Telecomunicaciones hace parte del mencionado comité.

No obstante, aunque el acto administrativo incorpora disposiciones generales relacionadas con seguridad digital y seguridad de la información, no se evidenció la asignación específica de funciones orientadas a la adopción, implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a lo establecido en los lineamientos definidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

Así mismo, no se observó la designación expresa del responsable de seguridad de la información o de quien haga sus veces como miembro permanente del Comité Institucional de Gestión y Desempeño, ni la definición formal de su participación dentro de la estructura de gobernanza del modelo.

Lo anterior evidencia oportunidades de fortalecimiento en la formalización de las responsabilidades y mecanismos de gobernanza asociados al MSPI, con el fin de asegurar

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

que las funciones requeridas por los lineamientos del modelo se encuentren claramente definidas, asignadas y articuladas dentro de las instancias institucionales de dirección y seguimiento.

Recomendación

Actualizar los actos administrativos y demás instrumentos de gobernanza relacionados con el Comité Institucional de Gestión y Desempeño, incorporando de manera expresa las funciones asociadas a la adopción, implementación, seguimiento y mejora continua del Modelo de Seguridad y Privacidad de la Información (MSPI), así como la participación formal del responsable de seguridad de la información o su equivalente, conforme a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones.

8. GESTIÓN DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Observación 8: Debilidades en la aprobación y divulgación de los lineamientos de seguridad y privacidad de la información

De acuerdo con la información suministrada por la Dirección TIC, la entidad cuenta con el documento M-OP-001 “Manual para la Gestión del Riesgo en TRANSMILENIO S.A.” y su Anexo 3 “Metodología para la administración de los riesgos de seguridad de la información”, mediante los cuales se establecen lineamientos para la identificación, valoración y tratamiento de los riesgos de seguridad y privacidad de la información. Así mismo, se evidenció la existencia del documento L-DT-002 “Políticas de Seguridad y Privacidad de la Información”, versión 7 de abril de 2025, el cual define los lineamientos y compromisos orientados a garantizar la confidencialidad, integridad y disponibilidad de la información institucional.

Con el fin de verificar el cumplimiento de los lineamientos establecidos en el Anexo 1 de la Resolución 500 de 2021, la Oficina de Control Interno revisó las cuatro (4) actas del Comité

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

Institucional de Gestión y Desempeño correspondientes a la vigencia 2025 y el acta de la sesión realizada en enero de 2026. Como resultado de dicha revisión, se evidenció que únicamente en la sesión del 30 de enero de 2026 fue presentada para aprobación la actualización de las Políticas de Seguridad y Privacidad de la Información.

No obstante, no se evidenció que los lineamientos relacionados con la gestión de riesgos de seguridad y privacidad de la información, ni la documentación asociada para la administración y gestión de dichos riesgos, hubieran sido presentados al Comité Institucional de Gestión y Desempeño y aprobados por éste, conforme a lo establecido en la viñeta 5 del numeral 7.2.2 del Anexo 1 de la Resolución 500 de 2021.

Así mismo, aunque la Dirección TIC informó que durante el mes de mayo de 2026 la política fue socializada a ciento cuarenta y nueve (149) profesionales y contratistas, no se evidenciaron soportes que permitieran verificar su comunicación a la totalidad de los servidores, contratistas y demás partes interesadas a quienes aplica, conforme a lo requerido en la viñeta 6 del lineamiento antes mencionado.

Las situaciones descritas evidencian debilidades en los mecanismos de aprobación y divulgación de los lineamientos de seguridad y privacidad de la información, limitando la trazabilidad frente a su adopción institucional y la verificación de su conocimiento por parte de todos los actores involucrados en la gestión y protección de la información.

Recomendación

Mejorar los mecanismos de aprobación, divulgación y trazabilidad de los lineamientos asociados a la seguridad y privacidad de la información, garantizando su presentación ante el Comité Institucional de Gestión y Desempeño cuando corresponda, así como la comunicación y conservación de evidencias que permitan verificar su conocimiento por parte de todos los servidores, contratistas y demás interesados a quienes les aplique.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

9. INVENTARIO Y CLASIFICACIÓN DE LA INFORMACIÓN E INFRAESTRUCTURA CRÍTICA

Observación 9: Debilidades en la actualización y administración del inventario de activos de información

De acuerdo con la información suministrada por la Dirección TIC el 15 de mayo de 2026, se evidenció que la entidad cuenta con el instructivo I-DT-001 “Para la identificación, valoración y clasificación de activos de información”, versión 1 de octubre de 2021, mediante el cual se establecen los lineamientos para la identificación, registro, valoración y clasificación de los activos de información de la entidad. Así mismo, el documento define criterios de clasificación de la información y responsabilidades para el diligenciamiento y actualización del formato R-DT-010 “Inventario de Activos de Información”.

Con el fin de verificar la aplicación de la metodología definida por la entidad, la Oficina de Control Interno revisó la matriz de inventario de activos de información suministrada por la Dirección TIC, identificando las siguientes situaciones:

- El inventario no presenta una fecha de actualización que permita determinar la vigencia de la información registrada, observándose únicamente la anotación “en proceso de actualización 2025”.
- En la hoja denominada “Información” se encuentra documentada principalmente información asociada al proceso Gestión TIC y registros de información publicada o disponible para consulta ciudadana, sin evidenciarse la identificación integral de los activos de información correspondientes a los demás procesos de la entidad.
- La valoración registrada para los activos no corresponde a la escala definida en el instructivo I-DT-001, generando inconsistencias entre la metodología establecida y la información reportada en el inventario.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

- Para los activos clasificados como software se identificaron cincuenta y dos (52) registros, de los cuales, dos (2) no cuentan con información sobre el tipo de licenciamiento, dieciséis (16) no registran la cantidad de licencias asociadas, doce (12) no incluyen la justificación de la necesidad del software, algunos registran como propietario o responsable del activo un usuario identificado como “desconocido”, dos (2) se encuentran asociados a contratistas que ya no tienen vínculo con la entidad, ocho (8) no tienen responsable identificado y doce (12) no registran dependencia custodio.
- Para los activos clasificados como hardware se identificaron ciento sesenta y cinco (165) registros, de los cuales, trece (13) se encuentran asignados a contratistas que ya no tenían vínculo con la entidad.
- Respecto de los activos clasificados como servicios, únicamente se identificaron once (11) registros asociados al proceso Gestión TIC.
- En el inventario de activos de conocimiento se observó que varios registros corresponden a cargos o roles que no se encuentran alineados con la estructura organizacional vigente de la entidad.
- Para los activos clasificados como ubicación únicamente se identificó un (1) registro correspondiente a la sede principal de TRANSMILENIO S.A., sin evidenciarse la totalidad de las sedes, ubicaciones o infraestructura tecnológica crítica de la entidad.

Las situaciones identificadas evidencian debilidades en la aplicación, mantenimiento y actualización del inventario de activos de información, así como en la identificación de propietarios, custodios y responsables de los activos. De igual forma, no fue posible evidenciar la identificación integral de los activos de información asociados a todos los procesos de la entidad, ni la administración completa de la infraestructura crítica y los

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

servicios esenciales requeridos por los lineamientos del Modelo de Seguridad y Privacidad de la Información.

Por lo anterior, se evidenció un cumplimiento parcial del numeral 7.3.1 “Identificación de activos de información” del Anexo 1 de la Resolución 500 de 2021, toda vez que, la entidad cuenta con una metodología formal para la identificación y clasificación de activos; sin embargo, persisten debilidades en su aplicación, actualización y seguimiento, así como en la gestión integral del inventario de activos de información, infraestructura crítica y servicios esenciales.

Recomendación

Actualizar y reforzar el inventario de activos de información de la entidad, garantizando la aplicación uniforme de la metodología definida, la identificación integral de los activos asociados a todos los procesos, la asignación de propietarios, custodios y responsables, así como la actualización periódica de la información relacionada con infraestructura crítica, servicios esenciales y demás elementos requeridos para una adecuada gestión y protección de los activos de información.

DECLARACIONES GENERALES:

- La evidencia recopilada para propósitos de la evaluación efectuada versa en información suministrada por las áreas indicadas en el presente informe, responsables de la actividad objeto de evaluación y seguimiento. Nuestro alcance no pretende corroborar la precisión de la información y su origen.
- La naturaleza de la labor de auditoría interna ejecutada por la Oficina de Control Interno, al estar supeditada al cumplimiento del Plan Anual de Auditoría, se encuentra limitada por restricciones de tiempo y alcance, razón por la que, procedimientos más detallados podrían develar asuntos no abordados en la ejecución de esta actividad.

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co

- La respuesta ante las situaciones observadas por la Oficina de Control Interno es discrecional de la administración de TRANSMILENIO S.A., más se incentiva la consideración de las “Recomendaciones” en la construcción de los planes de mejora a que haya lugar para el mejoramiento del Sistema de Control Interno y el Modelo Integrado de Planeación y Gestión de la entidad.

ANGELA JOHANNA MARQUEZ MORA

Firmado digitalmente por ANGELA JOHANNA MARQUEZ MORA
Fecha: 2026.06.18 08:49:29 -05'00'

ANGELA JOHANNA MÁRQUEZ MORA

Jefe Oficina de Control Interno

Elaboró: Diana Elizabeth Patiño Sabogal, Contratista de apoyo, Oficina de Control Interno

Revisó: Claudia Patricia Quintero Cometa, Contratista de apoyo, Oficina de Control Interno

TRANSMILENIO S.A.
Avenida Calle 26 # 69-76
Edificio Elemento - Torre 1 Piso 5
Código postal: 111071
Teléfono: (601) 2203000
Información: línea (601) 4824304
www.transmilenio.gov.co