Contenido

1 Propósito

El **Plan Estratégico de Seguridad de la Información (PESI)** establece el marco estratégico para proteger los activos de información del Metro de Medellín durante el periodo 2026–2029, garantizando su confidencialidad, integridad, disponibilidad y resiliencia.

El plan articula la seguridad y privacidad de la información con los objetivos corporativos y la evolución tecnológica de la Empresa, integrando la gestión de activos y riesgos de información, el cumplimiento normativo y las mejores prácticas internacionales, en coherencia con las Políticas de Gobierno y Seguridad digital del Modelo Integrado de Planeación y Gestión **(MIPG)** y los lineamientos institucionales, para fortalecer la confianza de los grupos de interés y asegurar la continuidad del servicio.

2 Justificación

El Metro de Medellín Ltda., en cumplimiento de lo dispuesto en el **Decreto 612 de 2018**, expedido por el Departamento Administrativo de la Función Pública, mediante el cual se establecen directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades del Estado, la Empresa incorporó en su **Plan Estratégico 2021–2025** la iniciativa estratégica denominada **"Excelencia organizacional en la era de la transformación digital"**, mediante la cual se reconoce la seguridad y privacidad de la información como un habilitador clave para la transformación digital y la sostenibilidad del negocio, estableciendo la implementación, sostenibilidad y mejora del Modelo de seguridad y privacidad de la información **(MSPI)** como una acción estratégica institucional.
Como resultado de este proceso evolutivo, el Metro de Medellín ha consolidado un **modelo de gobierno de seguridad de la información** estructurado en tres niveles claramente definidos y formalmente aprobados, que garantizan la sostenibilidad y mejora continua del modelo:

- **Nivel operativo**, a través de la Mesa Técnica de Seguridad de la Información
- **Nivel táctico**, mediante el Comité de Seguridad de la Información.
- **Nivel estratégico**, a través del Comité Institucional de Gestión y Desempeño.

Este esquema de gobierno se encuentra respaldado por la definición clara de responsabilidades, liderando de manera transversal la planeación, implementación y mejora del Plan de Seguridad y Privacidad de la Información, asegurando la gestión de riesgos, el cumplimiento normativo y la adopción de buenas prácticas, en coherencia con el Modelo Integrado de Planeación y Gestión **(MIPG),** la Política de Gobierno y seguridad Digital y los lineamientos internos.

3 Alcance y Vigencia

Este plan tendrá vigencia a partir de diciembre de 2025 y su finalización se estima en diciembre 2026, su alcance estará enmarcado en la totalidad de las actividades descritas en las fases de operación, evaluación del desempeño y mejoramiento continuo del modelo de seguridad de la información del metro de Medellín.

4 Objetivo General

Garantizar la protección y resiliencia de los activos de información del Metro de Medellín, mediante un modelo de seguridad de la información alineado con la estrategia corporativa, que permita gestionar los riesgos, asegurar la continuidad del servicio y fortalecer la confianza de los grupos de interés.

4.1 Objetivos Específicos

- Gestionar de manera sistemática los riesgos sobre los activos de información, mediante la identificación, análisis, tratamiento y seguimiento de los riesgos de seguridad y privacidad, alineados con los objetivos corporativos y el apetito de riesgo de la Empresa.
- Implementar y mantener controles de seguridad de la información que garanticen la confidencialidad, integridad, disponibilidad, privacidad y resiliencia de los activos de información, en coherencia con las mejores prácticas internacionales.
- Fortalecer la seguridad de los sistemas de información y de la infraestructura tecnológica, incorporando prácticas de ciberseguridad que reduzcan la probabilidad e impacto de incidentes y aseguren la continuidad de los servicios críticos.
- Promover el uso seguro y responsable de la información, mediante acciones de sensibilización, formación y apropiación de la seguridad y privacidad de la información en todos los niveles de la Empresa.
- Asegurar el cumplimiento normativo y la protección de los datos personales, integrando los lineamientos legales, regulatorios e institucionales en la gestión de la seguridad y privacidad de la información.
- Establecer un esquema de seguimiento, medición y mejora continua del PESI, a través de indicadores, evaluaciones de madurez y reportes periódicos a las instancias de gobierno, que permitan la toma de decisiones informadas.

5 Marco Normativo

Decreto 612 de 2018 – Integración de planes institucionales al Plan de Acción.
Modelo Integrado de Planeación y Gestión – MIPG (Decreto 1499 de 2017).
Política de Gobierno Digital – Decreto 1008 de 2018 y normas complementarias.
Decreto 338 de 2022 – Gobernanza en seguridad digital.
CONPES 3854 – Política Nacional de Seguridad Digital.
CONPES 3995 – Política Nacional de Confianza y Seguridad Digital.
Resolución 500 de 2021 (actualizada por Resolución 02277 de 2025) – Lineamientos y estándares del Modelo de Seguridad y Privacidad de la Información – MSPI.
ISO/IEC 27001:2022 – Buenas prácticas aplicables a SGSI.
Otros decretos del sector TIC (1078 de 2015) y Función Pública (1083 de 2015) para contexto regulatorio general.

6 Recursos

- Profesional 1 (oficial de seguridad de la información)
- Mesa de Seguridad y Privacidad de la Información.
- Comité de seguridad de la información.

7 Responsables

Responsable	ROLES				Responsabilidades
	A	R	I	C	
Rol estratégico	X	X			• Asegurar la implementación, desarrollo, supervisión y mejora de las políticas de gestión y desempeño, así como las directrices impartidas por la presidencia de la república y el ministerio de tecnología de la información y las comunicaciones en materia seguridad digital y de la información. • Aprobar el Modelo y la Política de Seguridad de la Información, y asegurar su implementación, desarrollo, supervisión y mejora continua, garantizando su alineación con el Sistema de Planeación de la Empresa, en cumplimiento de las directrices nacionales desde la política de seguridad digital.
Rol táctico	X	X			• Planear, coordinar, supervisar y evaluar todas las acciones relacionadas con la implementación y mantenimiento del Modelo de Seguridad de la Información (MSI). • Acompañar la implementación de estrategias y proyectos enfocados en fortalecer el Modelo de Seguridad de la Información, asegurando el cumplimiento de la política de seguridad digital del Modelo Integrado de Planeación y Gestión (MIPG). • Coordinar y alinear el Plan Estratégico de Seguridad de la Información (PESI) con el Plan Estratégico de Tecnologías de la Información (PETI) • Aprobar las metodologías, procedimientos y mejores prácticas que aseguren la

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					implementación efectiva y la sostenibilidad del modelo de seguridad de la Información. • Revisar las políticas y lineamientos de seguridad de la información y entregar recomendaciones claras al Comité Institucional de Gestión y Desempeño para su aprobación. • Evaluar y revisar los roles y responsabilidades en materia de seguridad de la información, proporcionando una postura clara para su aprobación por parte del Comité Institucional de gestión y desempeño. • Realizar un seguimiento continuo al desempeño del modelo de seguridad de la Información, asegurando su efectividad y evolución. • Velar por la implementación de acciones derivadas de incidentes de seguridad de la Información, análisis de riesgos y resultados de auditorías, garantizando una respuesta oportuna y adecuada. • Velar por el cumplimiento de las normativas relacionadas con seguridad de la información, asegurando su alineación con las leyes y regulaciones vigentes.
Rol operativo		X			• Apoyar técnicamente al responsable del Modelo de seguridad de la información en cada una de las tareas descritas en el plan de implementación, así como también en las actividades que busque apoyar la sostenibilidad del modelo de seguridad de la información. • Participar en la definición del alcance de los controles de seguridad de la información dentro de la declaración de aplicabilidad. • Hacer seguimiento a la ejecución de los controles de acuerdo con su rol para seguridad de la información, obteniendo evidencia con la

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					periodicidad que se defina desde la gestión de riesgos de seguridad de la información • Gestionar incidentes de seguridad, así como la posterior investigación para determinar causas y recomendaciones de mejora.
Oficial de seguridad de la información		X	X		• Velar por el cumplimiento y ejecución del plan estrategico de seguridad de la información PESI. • Implementar mecanismos de monitoreo dentro del ciclo de vida del Modelo de Seguridad de la Información (MSI). • Asesorar a los procesos y/o proyectos en materia de seguridad de la información. • Liderar la gestión de riesgos de seguridad de la información incluyendo los riesgos en proyectos, contratos y cambios que involucren activos de información. • Definir e implementar en coordinación con los procesos de la Empresa, las estrategias de sensibilización, divulgación, fortalecimiento de la cultura y competencia de seguridad de la información para los servidores y terceros. • Velar por el mejoramiento continuo del Modelo de Gestión de Seguridad de la Información (MSI). • Presentar informes y reportes a los órganos de gobierno, órganos de control, autoridades y proceso internos respecto al Modelo de Gestión de Seguridad y de la Información (MSI). • Proponer medidas preventivas, correctivas o disuasorias necesarias para la gestión del Modelo de Gestión de Seguridad de la Información (MSI). • Identificar la brecha entre el Modelo de seguridad de la información y la situación actual de la Empresa.

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					• Realizar la estimación, planificación y seguimiento de proyectos relacionados con seguridad de la información (MSI). • De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad de la información. • Apoyar a los procesos de la Empresa en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad de la información. • Definir, socializar y hacer seguimiento el plan de respuesta a Incidentes de seguridad de la información en la Empresa articulándolo con la gestión de continuidad de negocios y la gestión de riesgos. • Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la Empresa.
A: Aprobador R: Responsable I: Informado C: Consultado					

8 Estrategia de seguridad y privacidad de la información

El Plan de Seguridad y Privacidad de la Información se desarrollará de forma estructurada, progresiva y articulada, conforme a las cuatro fases del Modelo de Seguridad de la Información del Metro de Medellín y a los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones, con el fin de garantizar una implementación consistente, sostenible y orientada a resultados.

Así mismo, el plan habilitará y acompañará en materia de seguridad y privacidad de la información la ejecución de las 48 iniciativas definidas en la hoja de ruta digital del PETI, asegurando que su desarrollo y operación se realicen bajo criterios de gestión de riesgos, cumplimiento normativo y resiliencia institucional.

9 Proyectos

Gestión Integral de Activos de Información

Propósito: Garantizar visibilidad, control y trazabilidad de los activos de información.

Incluye:

- Inventario unificado de activos de información por procesos
- Clasificación de los activos de información

Gestión de Riesgos de Seguridad y Privacidad de la Información

Propósito: Reducir el impacto de los riesgos sobre los activos de información.

Incluye:

- Integración con riesgos de proceso y estratégicos
- Estructura para la entrega de evidencias de los controles de seguridad de la información.
- Planes de tratamiento y seguimiento

Gestión de Incidentes de Seguridad de la Información

Propósito: Mejorar la capacidad de respuesta y recuperación ante incidentes.

Incluye:

- Documentación y socialización del plan de respuesta a incidentes de seguridad de la información.
- Ejercicios y simulacros

10 Cronograma

A continuación, se comparte el cronograma de alto nivel vigente para 2026:

Fase	Estado	Fecha de implementación	Observaciones
Operación	En proceso	Agosto 2026	Identificación de activos sobre todos los procesos
Operación	En curso	Agosto 2026	Clasificación de activos de información
Operación	En curso	Febrero 2026	Integración con riesgos de proceso y estratégicos
Operación	En curso	Marzo 2026	Entrega de estructura para la entrega de evidencias de los controles
Planificación	En curso	Marzo 2026	Entrega del plan de tratamiento de riesgos de seguridad de la información
Implementación	En curso	Marzo 2026	Socialización del plan de respuesta a incidentes de seguridad de la información.
Implementación	En curso	Abril 2026	Ejecución de ejercicios y simulacros

11 Análisis presupuestal

En la **fase de operación**, se dará ejecución a los **controles definidos en la matriz de aplicabilidad**, de acuerdo con su alcance y priorización, los cuales estarán **respaldados por la asignación presupuestal de los procesos responsables**, garantizando su implementación efectiva, sostenibilidad y adecuada gestión.

Las **auditorías internas** asociadas a la fase de evaluación del desempeño del modelo de seguridad de la información se integrarán al **Plan Anual de Auditoría de la Empresa** y se ejecutarán con los **recursos asignados a las áreas o procesos responsables**, asegurando una evaluación sistemática y eficiente.

12 Anexos

- Plan detallado del MSI.xlsx

13 Control de cambios

Versión modificada	Descripción del cambio
NA	NA

14 Responsabilidades

Documentador	Revisor	Aprobador
Profesional 1 Oficial de seguridad de la información	Comité de Seguridad de la Información	Comité Institucional de Gestión y Desempeño