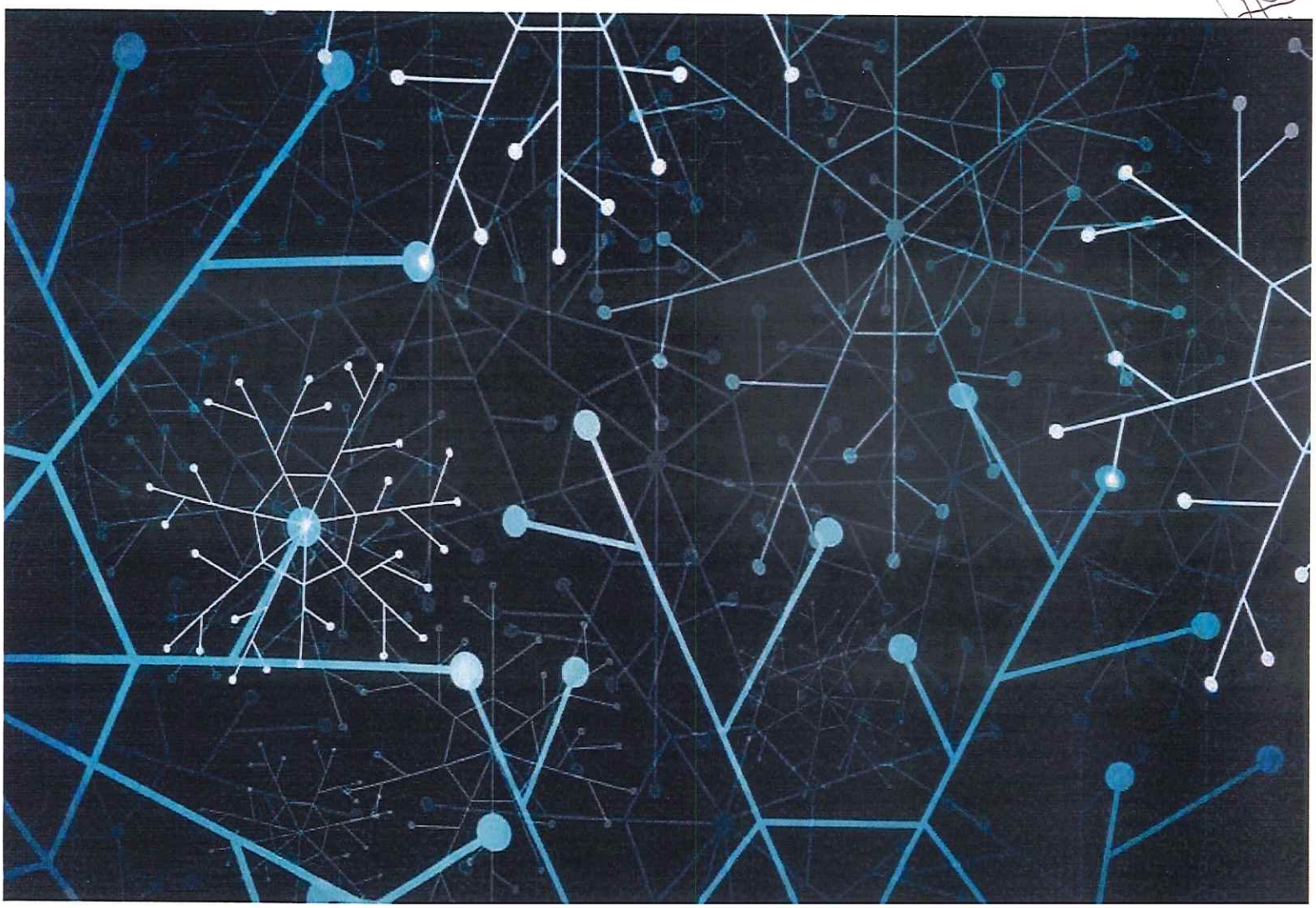
Plan de Seguridad, Privacidad de la Información y Ciberseguridad de Metro Cali S.A. Acuerdo de Reestructuración

Vigencia 2023 - 2026

metrocali



1. CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

2. INTRODUCCIÓN

La información es el activo de mayor valor en el entorno del servicio de transporte público esencial de la ciudad, como también lo es el conocimiento. Es un recurso vital y el buen uso de esta puede significar la diferencia en el servicio y el negocio, como también para proyectos que se emprendan dentro de su ámbito.

El gobierno y gestión de la información facilita la previsión, prospección y oportunidad para la reacción, mantener control sobre las fortalezas y debilidades, así como amenazas y oportunidades, permitiendo proteger los activos más vulnerables como entidad u organización. Un uso adecuado de la información, es fundamental para lograr un alto nivel competitivo dentro del mercado y obtener mayores niveles de capacidad de desarrollo.

La seguridad de la información, por tanto, alcanza niveles de la misma relevancia, pues también constituye un elemento fundamental para la protección efectiva de derechos, obligaciones y libertades del ciudadano con el transporte público esencial. Por ello, desde diferentes ámbitos, instancias y dimensiones, se han producido políticas públicas que posibilitan el uso de metodologías y marcos, que profiere el compromiso para el fortalecimiento de las entidades del estado, siendo menester en el contexto ampliado del ciberespacio involucrar a consumidores, individuos, organizaciones y proveedores, con la relevancia y oportunidad existente para mantener la ciberseguridad razonada de la sociedad en el ámbito del negocio.

Por su parte, la seguridad de la información permite construir y mantener las condiciones necesarias para su pleno ejercicio, aplicando la ley y ejerciendo la autoridad, lo que al mismo tiempo promueve la autorregulación ciudadana y la cohesión social alrededor de la gestión institucional.

El presente plan tiene como propósito, cerrar brechas frente a la seguridad de la información organizacional interna y establecer medidas para ampliar la confianza digital, mejorando la seguridad digital de la entidad en la operación del negocio público con participación privada y la definición del rol activo de los actores en el ámbito del ciberespacio. Contempla personas, procesos y tecnología; incluyente para las múltiples partes interesadas con

responsabilidad individual y conjunta en el desarrollo de las actividades socioeconómicas y servicios conexos del entorno del Sistema Inteligente e Integrado de Transporte Masivo de pasajeros de Santiago de Cali; que facilite una operación segura, confiable y competitiva, cerrando también las brechas de seguridad digital y avanzar en el futuro con mayor confianza ciudadana.

Se precisa que, las acciones referidas en el presente plan, se desarrollan de manera simultánea con el plan de tratamiento de riesgos de seguridad, privacidad de la información y ciberseguridad.

3. OBJETIVOS

3.1 Objetivo General

Implementar el Sistema del Gestión de Seguridad, Privacidad de la Información y Ciberseguridad definido por la entidad durante el periodo del 2023-2026, en función de la supremacía de los principios de disponibilidad, confidencialidad e integridad de la información organizacional interna, contribuyendo a la seguridad de la información en el negocio, la transparencia en la gestión pública y al incremento de la confianza ciudadana.

3.2. Objetivos Específicos

a. Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad, privacidad de la información y ciberseguridad, orientados al fortalecimiento institucional, la mejora continua y al alto desempeño del sistema de gestión seguridad, privacidad de la información y ciberseguridad.

b. Facilitar de manera integral la gestión de los riesgos de seguridad, privacidad de la información, ciberseguridad y continuidad de la operación de los servicios

c. Reducir vulnerabilidades frente a las amenazas existentes para reducir el número de incidentes de seguridad, privacidad de la información y ciberseguridad, de forma efectiva, eficaz y eficiente.

4. ALCANCE

Con base a las diferentes estrategias de negocio a las cuales le apuesta la entidad, el presente plan cuenta con aplicabilidad a todos los procesos de la entidad y en las partes interesadas del negocio, durante la vigencia 2023-2026 en función de los términos de la ISO 27001:2013.

Iniciando con la institucionalización del plan, seguido del desarrollo de las fases de diagnóstico, consolidación de la etapa de planeación (del plan anterior), se complementa con la implementación (contenida separadamente, en el plan de tratamiento de riesgos de seguridad, privacidad de la información y seguridad digital o ciberseguridad) y termina, con la completitud del ciclo, seguimiento, medición, evaluación y mejora continua; para que opere de manera recurrente.

5. NORMATIVIDAD

El presente normograma es alusivo a la Seguridad, Privacidad de la Información y Ciberseguridad de Metro Cali S.A. Acuerdo de restructuración en el contexto del negocio y del Servicio público esencial con el Sistema MIO, SIITP o el que se adopte por parte de la entidad.

- Constitución Política de Colombia 1991.
- Ley 23 de 1982: Ley de Propiedad Intelectual - Derechos de Autor
- Ley 527 de 1999: Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 1032 de 2006: Por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.

- Ley Estatutaria 1266 2008: Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Ley 1273 de 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Resolución 3066 de 2011: Comisión de Regulación de Comunicaciones Por la cual se establece el Régimen Integral de Protección de los Derechos de los Usuarios de los Servicios de Comunicaciones.
- CONPES 3701 de 2011: Lineamientos de política para Ciberseguridad y Ciberdefensa
- Ley 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales.
- Decreto 2364 de 2012: Por medio del cual se reglamenta el artículo 7° de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
- Decreto 032 de 2013: Crea una comisión intersectorial que se denominará "Comisión Nacional Digital y de Información Estatal".
- Ley 1712 de 2014: De transparencia y del derecho de acceso a la información pública nacional.
- Decreto 1074 de 2015: Decreto Único Reglamentario del Sector Comercio, Industria y Turismo. establece los objetivos y aspectos relacionados con la autorización del titular de la información, las políticas de tratamiento de los responsables y encargados, el ejercicio de los derechos de los titulares de la información, las transferencias de datos personales y la responsabilidad demostrada frente al tratamiento de datos personales.
- Decreto 1078 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
- Ley 1753 de 2015: se expide el Plan Nacional de Desarrollo 2014-2018.
- Decreto 415 de 2016 Fortalecimiento institucional con TIC

- CONPES 3854 de 2017: Política Nacional de Seguridad digital
- Resolución 5111 de 2017: Por la cual se establece el régimen de protección de los derechos de los usuarios de servicios de comunicaciones.
- Decreto 612 de 2018 Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto 1008 de 2018: Por el cual se establecen los lineamientos generales de la política de Gobierno Digital
- CONPES 3995 de 2020: Confianza y Seguridad Digital
- Decreto 620 de 2020 : establece los lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
- Resolución 1519 de 2020: Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos materia de acceso a la información pública, accesibilidad web, seguridad digital, y datos abiertos.
- Resolución No. 500 de 2021: 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.
- Decreto 338 de 2022: establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Resolución 746 de 2022: Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información.
- Resolución N° 912.110.284 2020: Por la cual se adopta la política general de seguridad y privacidad de la información de Metro Cali S.A. y se definen lineamientos frente al Gobierno, gestión y uso de la información.
- Resolución N° 912.110.204 2021: Por la cual se establece el proceso de arquitectura empresarial y la política de TI relacionada, se definen principios, roles, responsables, proyectos priorizados y procedimiento de calidad de la información.
- Resolución N° 912.110.241 2021: Por la cual se crea y se establece el comité operativo de TI o tecnologías de la información y las comunicaciones de la entidad,

se reglamenta su operación dentro del ámbito de planeación, operación, gobierno, gestión y control del Sistema MIO.

- Resolución N° 912.110.242 2021 Por la cual se crea y se establece el comité operativo de seguridad, privacidad de la información y ciberseguridad de la entidad, y se reglamenta su operación dentro del ámbito de planeación, operación, gobierno, gestión y control del Sistema MIO.

6. RESPONSABILIDAD Y AUTORIDAD

La autoridad del presente plan, es de quién ejerce el rol de dirección del Proceso Tecnológico, actualmente el jefe de la Oficina de Sistemas. La responsabilidad en el desarrollo y actualización del presente plan se produce a través de la persona que ejerce el rol de oficial de seguridad, privacidad de la información y ciberseguridad de la entidad, quién lo desarrolla para aprobación del arquitecto empresarial y el Comité de Seguridad, Privacidad de la Información y Ciberseguridad de la entidad establecido mediante la Resolución N° 912.110.242 de octubre 28 de 2021 o las normas internas que lo modifiquen y finalmente, aprobado y adoptado por el Comité Institucional de Gestión y Desempeño.

7. DEFINICIONES

Las definiciones empleadas en el presente documento hacen parte de las diferentes guías y Marco normativos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. A continuación, sin que se limite a ellas, se hace referencia de algunas definiciones al respeto

7.1 Acceso a la Información Pública: derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).

7.2 Activo: en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas…) que tenga valor para la organización. (ISO/IEC 27000).

7.3 Activo de Información: en relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal. También: Conocimiento o datos que tienen valor para la persona o para la organización.

7.4 Agente de amenaza: persona, grupo u organización que supuestamente está operando con intención maliciosa. (Adaptado de STIX)

7.5 Amenaza: causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

7.6 Ataque: intento de destruir, exponer, alterar, deshabilitar robar o lograr acceso no autorizado o hacer uso no autorizado de un activo.

7.7 Auditoría: proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

7.8 Autenticidad (authenticity): propiedad que consiste en que una entidad es lo que afirma ser. (ISO/IEC 27000:2018)

7.9 Aviso cibernético (cyber advisory): notificación de nuevas tendencias o de novedades acerca de una ciber amenaza contra sistemas de información o acerca de una vulnerabilidad de los sistemas de información. Dicha notificación puede abarcar un estudio analítico de tendencias, intenciones, tecnologías o tácticas empleadas para atacar sistemas de información. (Adaptado de NIST).

7.10 Ciber- o cibernético (cyber): relativo a una infraestructura tecnológica interconectada en la que interactúan personas, procesos, datos y sistemas de información. Fuente: (Adaptado de CPMI-IOSCO-cita de NICCS).

7.11 Ciberseguridad (cybersecurity / Cyberspace cybersecurity): preservación de la confidencialidad, la integridad y la disponibilidad de la información y/o de los sistemas de información a través del medio cibernético. Así mismo, pueden estar involucradas otras propiedades, tales como la autenticidad, la trazabilidad, el no repudio y la confiabilidad. (Adaptado de ISO/IEC 27032:2012).

7.12 Ciberespacio: es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de

telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

7.13 Compromiso (compromise): transgresión de la seguridad de un sistema de información. (Adaptado de ISO 21188:2018)

7.14 Confidencialidad (confidentiality): propiedad según la cual la información no está disponible para personas, entidades, procesos o sistemas no autorizados, ni se da a conocer a personas, entidades, procesos o sistemas no autorizados. (Adaptado de ISO/IEC 27000:2018).

7.15 Control de acceso (access control): medio para asegurar, que el acceso a los activos esté autorizado y restringido en función de requisitos relacionados con la actividad y la seguridad. (ISO/IEC 27000:2018)

7.16 Datos Abiertos: son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

7.17 Datos Personales: cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

7.18 Evento cibernético (cyber event): ocurrencia observable en un sistema de información. Los eventos cibernéticos a veces indican que se está produciendo un ciberincidente. (Adaptado de NIST - definición de "evento" ["event"]).

7.19 Plan de tratamiento de riesgos: documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

7.20 Riesgo: posibilidad de que una amenaza concreta, pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

7.21 Riesgo cibernético: combinación de la probabilidad de que se produzcan ciber incidentes y su impacto. (Adaptado de CPMI-IOSCO, ISACA Fundamentals (definición de "riesgo" ["risk"], e ISACA Full Glossary - definición de "riesgo" ["risk"])

7.22 Seguridad de la información: preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

7.23 Sistema de Gestión de Seguridad de la Información – SGSI: conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos), que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

8. DESARROLLO

8.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

8.1.1 DIAGNÓSTICO

La herramienta de diagnóstico de MinTIC[1] diligenciada, permite mostrar la situación actual de la Seguridad y Privacidad de la Información de la entidad, la cual contempla verificaciones en las fuentes de información del proceso "Gestión Tecnológica" de Metro Cali Acuerdo de Reestructuración y su relación con los distintos procesos de la empresa para la entrega de valor. A través de tabla 1 y figura 1. Avance ciclo de funcionamiento del Modelo de Operación (PHVA), se evidencia un resumen de los resultados del diagnóstico.

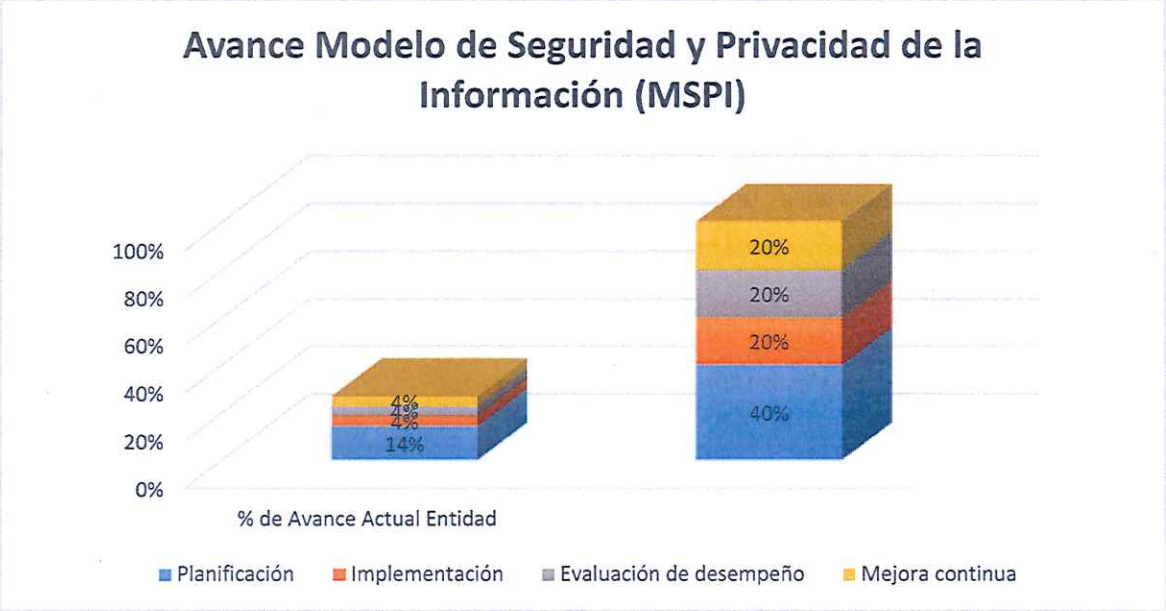
Tabla 1.Avance Modelo de Seguridad y Privacidad de la Información (PHVA

AÑO	AVANCE PHVA 2022	
	COMPONENTE	Avance 2022 (%)
2022	Planificación	14
	Implementación	4
	Evaluación de desempeño	4
	Mejora continua	4
TOTAL		27

Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

[1] MinTic, Ministerio de las Tecnologías de la Información y las Comunicaciones de Colombia

Figura 1.Modelo de seguridad y privacidad de la información (MSPI)



Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

8.1.2 Estructura funcional de Seguridad y Privacidad de la Información

Actualmente, la entidad realiza acciones que permiten el cierre de brechas operacionales en pro del planteamiento de una estructura funcional a través de políticas, procedimientos y acciones frente al Sistema de Gestión de Seguridad de la Información y la capacidad funcional que el SITM-MIO requiere.

8.1.3 Recursos

La entidad ha establecido recursos específicos a controles de mayor prioridad frente a la operación y referente a la seguridad informática, acorde con el presupuesto anual aprobado para la finalidad. Los recursos concebidos son para atender necesidades de mayor prioridad para la seguridad informática de conformidad con la definición y caracterización del proceso actual de la entidad, en cumplimiento de la legislación y fines de protección de datos personales.

Sin embargo, se mantiene el reto del fortalecimiento institucional frente a la definición y establecimiento, implementación, operación y mejora continua del sistema de gestión de seguridad, privacidad de la información y ciberseguridad propuesto en el presente plan.

8.2 DESARROLLO DE LA PLANIFICACIÓN

8.2.1 Planeación proyectada

Las acciones prioritarias planificadas, tanto, para la seguridad de la información interna, como prepararse para dar respuesta a los riesgos del ciberespacio, tienen relación con los avances logrados confrontado con los resultados del autodiagnóstico del modelo MSPI, con el perfil objetivo que se obtiene, a partir de la aplicación del marco de NIST CSF.

Coincidentemente con la priorización y el alcance identificado, se determina la necesidad de contar con un SGSPIC operativo y orientado a la mejora continua, que aplique para los sistemas y activos relacionados, los requisitos reglamentarios y el enfoque de riesgo general.

Con ello, la prioridad es la de revisar y establecer el SGSPIC, identificar las amenazas y vulnerabilidades aplicables a los sistemas y activos de mayor importancia y criticidad, por su aporte al negocio y a los objetivos estratégicos institucionales.

Así mismo como la identificación y priorización de brechas frente al perfil objetivo, dando lugar a la definición del plan, consecuentemente, de conformidad con la capacidad institucional y la disponibilidad de recursos. Lo anterior, con el fin de definir los programas y proyectos pertinentes que conlleven a priorizar, de manera estratégica y progresiva, el cierre de brechas frente a la seguridad de la información.

Como estrategia, se pretende avanzar en la capacitación y concientización de los requisitos de ciberseguridad para el cumplimiento paulatino del propósito, procurando que:

1. Sea extensivo a cada una de las empresas con responsabilidades en el negocio público concesionado, a los ciudadanos, y demás partes interesadas que forman parte del propósito institucional con el servicio público de transporte que se presta en la ciudad,

como agentes del sistema de transporte masivo (SITM-MIO, SIITP, o el que se establezca para la Ciudad).

2. La entidad reconozca modelos, estándares, marcos de trabajo y mejores prácticas en materia de seguridad de la información y ciberseguridad, con énfasis en nuevas tecnologías.
3. Se fortalezca el marco de gobernanza en materia de seguridad de la información y seguridad digital que conlleve aumentar su grado de desarrollo.
4. Se constituya un marco de intercambio y coordinación de la información entre los agentes del sistema de transporte masivo (SITM-MIO, SIITP, o el que se establezca para la ciudad) y demás partes interesadas, en términos de seguridad de la información y ciberseguridad.

Esta primera fase culmina con la revisión y adopción del proceso principal (caracterización del sistema de gestión) que habilite al sistema de gestión de seguridad, privacidad de la información y ciberseguridad propuesto en el ámbito del negocio del transporte público esencial que involucran a la entidad y a las organizaciones circunscritas, para el reconocimiento unificado de las partes interesadas.

La segunda fase y siguientes, darán continuidad y fortalecimiento a lo desarrollado en la primera fase, continua con la consolidación de la planeación mediante revisión, ajuste y complemento de los documentos del SGSPIC; articulados con los procesos de la entidad, objetivos de la seguridad de la información y ciberseguridad, y el sistema de gestión de calidad vigente; inventario de activos en el entorno de los procesos del alcance (procesos priorizados); apreciación de riesgos, definición y establecimiento de la declaración de aplicabilidad, implementación y planeación operacional del Sistema de Gestión de seguridad, privacidad de la información y ciberseguridad.

El ciclo del SGSPIC se complementa con la implementación del plan de tratamiento de riesgos de seguridad, privacidad de la información y ciberseguridad en base a lo establecido por la Res. N° 912.110.242 de oct.28.2021.

8.2.2 Líneas estratégicas del Plan

1. Promover el uso de mejores prácticas de seguridad de la información, como base de aplicación del concepto de Seguridad Digital.
2. Identificar infraestructuras críticas en el entorno del servicio público esencial de transporte y TIC en el ámbito del negocio liderado por Metro Cali Acuerdo de reestructuración. y su contexto para la definición de la aplicación del Modelo de Seguridad y Privacidad de la información, y el modelo de gestión de riesgos de seguridad digital.
3. Contribuir a mejorar los procesos de intercambio de información pública.
4. Orientar a las Áreas de Metro Cali S.A. Acuerdo de reestructuración en las mejores prácticas en seguridad, privacidad de la Información y ciberseguridad.
5. Optimizar la gestión de la seguridad de la información al interior de Metro Cali S.A. Acuerdo de reestructuración y las empresas del sistema MIO adscritas al propósito Estatal.
6. Desarrollo y transición de IPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
7. Mantener aplicación de la legislación relacionada con la protección de datos personales, y el cumplimiento de la política de tratamiento de datos personales respetuosa de los derechos de los titulares.
8. Contribuir en el desarrollo del plan estratégico institucional y del plan estratégico de tecnologías de la información y de las comunicaciones.
9. Contribuir en la transformación digital de la entidad mediante el desarrollo de ejercicios de arquitectura empresarial, sobre la base de la transformación institucional y el cumpliendo de los lineamientos del marco de referencia de arquitectura empresarial del estado colombiano, gobierno y gestión de TI, y, gestión de proyectos de TI.
10. Optimizar la labor de acceso a la información pública al interior de las áreas y entidades destinatarias.

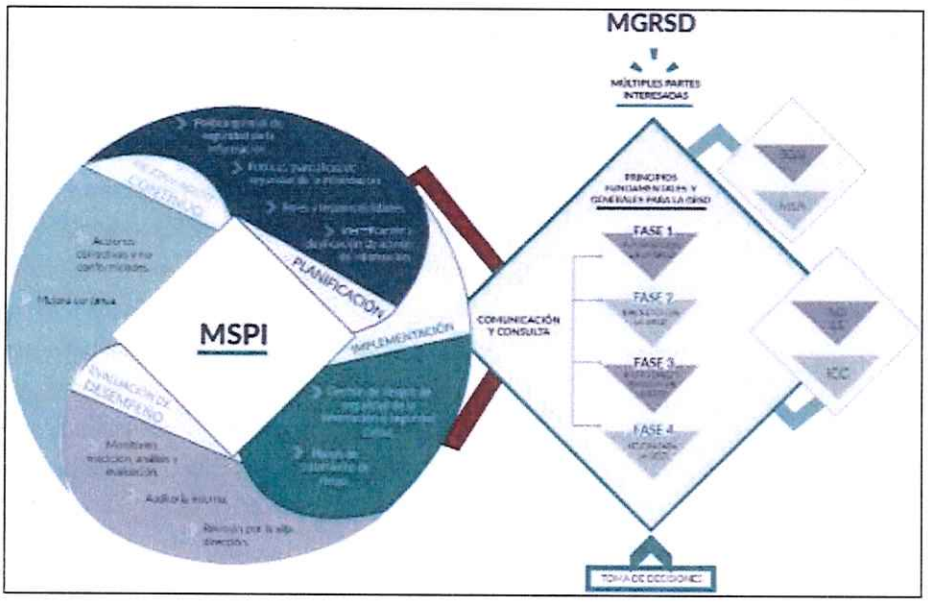
8.2 METODOLOGÍA DEL PLAN

La metodología procede de conformidad con el Modelo de Seguridad y Privacidad de la Información y el Modelo de Gestión de Riesgos de Seguridad Digital – MGRSD definida por MinTIC. Así mismo en concordancia con normas y estándares vigentes, especialmente la ISO/IEC 27001 y las fases del ciclo de operación (PHVA).

Los marcos de trabajo y metodologías de seguridad y privacidad de la información se integran a los métodos y mejores prácticas utilizadas para la gestión de TI y proyectos de TI, que abonen al gobierno y gestión de la información, la seguridad y ciberseguridad, creando condiciones se seguridad digital y confianza en la gestión y resultados institucionales, como también confianza de las partes interesadas y la Ciudadanía.

El SGSPIC (Sistema de Gestión de Seguridad, Privacidad de la Información y Ciberseguridad) propuesto para la entidad, abordarán las temáticas, acorde con el alcance de cada plan establecido. Para el presente plan, se mantiene la priorización con el cierre de brechas frente a la seguridad de la información, y, amparar a la entidad y al Stakeholders activos ante los riesgos en el ciberespacio.

Figura 2.Componentes MSPI y MGRSD (interacción)



Fuente: Modelo de Gestión de Riesgos de Seguridad Digital- MinTIC, 2018

8.3 ACTIVIDADES DEL PLAN

Las actividades del Plan se resumen en la tabla 2 y 3 que relaciona las fases del modelo de operación que será aplicado por Metro Cali S.A. Acuerdo de Reestructuración.

Tabla 2.Relación de objetivos y estrategias transversales

Objetivo transversal	ET	Estrategia transversal
OT-1 Generar un cambio organizacional a través de la concienciación y apropiación de la seguridad, privacidad de la información y la seguridad digital, orientados al fortalecimiento institucional, la mejora continua y al alto desempeño del Sistema de Gestión seguridad,	1	Mantener actualización de las normas, pautas o prácticas nuevas o revisadas, aportadas por las referencias informativas alusivas a las temáticas de seguridad, privacidad de la información y ciberseguridad.
	2	Formalizar e institucionalizar el sistema de gestión de seguridad, privacidad de la información y ciberseguridad de la entidad en desarrollo, creando condiciones para dar cumplimiento a los requisitos legales, reglamentarios, regulatorios, y a los de las normas técnicas colombianas en materia de seguridad y privacidad de la información, seguridad digital y protección de la información personal

Objetivo transversal	ET	Estrategia transversal
privacidad de la información y ciberseguridad.	3	Identificar competencias y actualizarlas adecuadas a las necesidades especializadas y subespecialidades en torno al desarrollo, implementación, operación y mejora continua del sistema de gestión de seguridad, privacidad de la información y ciberseguridad que sirvan de referencia para la entidad y partes interesadas en el evento de cubrir brechas de competencia, conocimiento y habilidades.
	4	Complementar, consolidar, actualizar y documentar las políticas y procedimientos desarrollados durante el plan 2019-2022 alusivo al sistema de gestión de seguridad y privacidad de la información en su desarrollo, e integrar y articularlos a requerimientos de ciberseguridad, en función de fortalecer y mantener la cultura institucional y la protección de la información en el ámbito interno y del ciberespacio.
	5	Fortalecer el marco de gobierno mediante la aplicación de la Resolución N° 912.110.242 de octubre 28 de 2021, conducente a la operación periódica del Comité de seguridad, privacidad de la información y ciberseguridad, para la toma de decisiones razonadas, mediante práctica de competencias alineadas a roles, responsabilidades y personas responsables en virtud del alcance y competencias de sus participantes.
	6	Construir el boletín trimestral, "Metro Cali S.A. Acuerdo de Reestructuración al día con la seguridad de la información y la ciberseguridad" con participación de las áreas, con entregas a todas las partes interesadas del negocio y el servicio; objeto del propósito institucional y la confianza ciudadana
	7	Construir y mantener un repositorio de seguridad de la información y ciberseguridad para referencia y consulta de las partes interesadas, que dinamicen un avance en la cultura de la seguridad de la información y seguridad digital de las partes interesadas
	8	Creación de la comunidad de ciberseguridad en el ámbito del servicio de transporte público esencial de Santiago de Cali y sus partes interesadas.

Objetivo transversal	ET	Estrategia transversal
	9	Definir, reformular y formalizar los elementos y herramientas para los temas de protección de la información.
OT-2 Facilitar de manera integral la gestión de los riesgos de seguridad y privacidad de la información y de seguridad digital y continuidad de la operación de los servicios	1	Desarrollar, adaptar y/o aplicar modelos, prácticas y herramientas, para la protección de la información, que sean de utilidad para el gobierno y gestión de los servicios y aporte a la supervisión de los contratos de concesión con fundamento en las mejores prácticas, herramientas, técnicas y estándares
	2	Mantener el cierre de brechas frente a la seguridad de la información y definir controles respecto a la seguridad digital de la entidad y las partes interesadas.
	3	Priorizar los controles de seguridad de la información mediante revisión paralela de la normatividad ISO 27001:2013 (Orientado a la transición de ISO 27001:2022); NIST SP 800-53 e ISO 27032 (Normas afines ISO 27110:2022)
OT-3 Reducir vulnerabilidades frente a las amenazas existentes para reducir el daño de los incidentes de seguridad y privacidad de la información y de seguridad digital, de forma efectiva, eficaz y eficiente.	1	Mantener actualizado e informado mediante repositorio de incidentes de la información y ciberseguridad
	2	Gestionar los controles de seguridad de la información y seguridad digital en el negocio y demás componentes críticos, estratégicos, sensibles priorizados de la entidad en el ámbito de operación, el entorno interno, externo y en el ciberespacio.
	3	Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, autenticidad, privacidad y no repudio de la información.
	4	Definir los lineamientos necesarios para el manejo de la información, tanto física como digital, en el marco de una gestión documental basada en seguridad y privacidad de la información.
	5	Definir, operar y mantener el plan de continuidad de la operación de los servicios de TI

Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

Tabla 3.Fases del Modelo de Seguridad y Privacidad de la Información de Metro Cali Acuerdo de Reestructuración.

Fase	Meta	Período del Plan	Instrumentos del MSPI	Alineación MRAE
Fase I – Actualizar el Diagnóstico (Actividad recurrente)	1. Actualizar el estado de seguridad y privacidad de la información y nivel de madurez de los controles	2023-2026	(i) Diligenciamiento de la herramienta. (ii) Diligenciamiento de la herramienta e identificación del nivel de madurez de Metro Cali S.A Acuerdo de Reestructuración. (iii) Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05 LI.GO.07 LI.ST.14
	2. Determinar la capacidad y asignación de recursos (roles y personas responsables)	2023-2026		
	3. Identificar vulnerabilidades técnicas y administrativas	2023-2026		
	4. Identificar el avance de la implementación del ciclo	2023-2026		
	5. Identificar el nivel de cumplimiento con la legislación vigente	2023-2026		
	6. Identificación del uso de buenas prácticas en ciberseguridad.	2023-2026		
Fase 2 – Planificación (Actividad recurrente)	7. Actualización de la política general	2023-2026	(i) Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08 LI.ES.09 LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09 LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09
	8. Revisión, ajuste y formalización de Procedimientos	2023-2026	(ii) Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	
	9. Designación de personas responsables.	2023	(iii) Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información	
	10. Inventario de activos de información.	2023-2026	(iv) Guía No 5 - Gestión De Activos	

Fase	Meta	Período del Plan	Instrumentos del MSPI	Alineación MRAE
			(v) Guía No 20 - Transición Ipv4 a Ipv6	LI.INF.10 LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14 LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
	11. Integración del MSPI con el Sistema de Gestión documental y ciberseguridad	2023-2026	(vi) Guía No 6 - Gestión Documental	
	1. Identificación, Valoración y tratamiento de riesgo.	2023-2026	(vii)Guía No 7 - Gestión de Riesgos (viii) Guía No 8 - Controles de Seguridad	
	2. Plan de Comunicaciones.	2023-2026	(ix) Guía No 14 - Plan de comunicación, sensibilización y capacitación	
	3. Plan de diagnóstico de IPv4 a IPv6.	2023-2026	(x) Guía No 20 - Transición IPv4 a IPv6	
Fase 3 – Implementación	1. Planificación y Control Operacional.	2023-2026	(i) Documento con el plan de tratamiento de riesgos. (ii) Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14 LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15 LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.09
	2. Implementación del plan de tratamiento de riesgos.	2023-2026	(iii) Documento con la declaración de aplicabilidad. (iv) Documento con el plan de tratamiento de riesgos.	
	3. Indicadores de Gestión.	2023-2026	(v) Guía No 9 - Indicadores de Gestión SI.	

Fase	Meta	Período del Plan	Instrumentos del MSPI	Alineación MRAE
	4. Plan de Transición de IPv4 a IPv6	2023-2026	(vi) Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6. (vii) Guía No 20 - Transición de IPv4 a IPv6 para Colombia. (viii) Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.10 LI.ST.12
Fase 4 – Evaluación Desempeño	1. Plan de revisión y seguimiento, a la implementación del MSPI.	2023-2026	(i) Guía No 16 – Evaluación del desempeño.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
	2. Plan de Ejecución de Auditorias	2023-2026	(ii) Guía No 15 – Guía de Auditoría.	
Fase 5 –Mejora Continua	1. Plan de mejora continua	2023-2026	(i) Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. (ii) Resultados del plan de ejecución de auditorías y revisiones	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

Fase	Meta	Período del Plan	Instrumentos del MSPI	Alineación MRAE
			independientes al MSPI. (iii) Guía No 17 – Mejora Continua	

Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

8.4 RECURSOS DEL PLAN

El sistema de gestión de seguridad, privacidad de la información y ciberseguridad – SGSPIC comprende la definición y establecimiento de los componentes y elementos que lo fundamentan, los cuales se constituyen como los recursos fundamentales que lo viabilice y habilite para la operación en un ciclo de mejora continua. Considerando lo establecido, el plan se concentrará en dichos elementos y componentes, son:

a) Roles
b) Revisión y ajuste de la política general (Seguimiento, extendida hacia la ciberseguridad)
c) Métodos
d) Procesos
e) Procedimientos (principales, acorde con la operación actual)
f) Controles técnicos aplicables (que fortalezca la operación actual)

8.4.1 Recurso Humano:

- Líderes de proceso y subproceso (directivos, jefes y quienes ejercen roles de coordinación y/o gestión de proyectos).
- Integrantes del Comité de Seguridad, Privacidad de la Información y Ciberseguridad
- Profesionales especializados en temáticas especificas frente a la seguridad de la información, ciberseguridad, controles a nivel de aplicación, protección del servidor, controles del usuario final, controles conta ataques de ingeniería social, entre otros.
- Profesionales especializados y Técnicos en tecnologías de la información y las comunicaciones.

- Usuarios finales, proveedores, consumidores, servidores públicos y organizaciones de los Concesionarios
- Ciudadano y usuario del Sistema de transporte de pasajeros

8.4.2 Recurso Físico:

- Hardware dedicado a la gestión, intercambio e interoperabilidad en la gestión de la entidad, del SGSPIC y agentes del sistema
- Instalaciones de la entidad
- Infraestructura de TI e Instalaciones del Sistema MIO (autobuses, edificaciones, estaciones, terminales, sedes operativas y administrativas, y demás dispuestas para la prestación del servicio público de transporte)
- Infraestructura de TI e instalaciones de los concesionarios, que comprenden infraestructura del Sistema MIO.
- Redes e infraestructura de red
- Controles de acceso físico

8.4.3 Recurso Tecnológico

- Servidores,
- Aplicaciones,
- Competencias y habilidades del equipo institucional
- Redes y equipos de cómputo,
- Sistemas gestores de bases de datos,
- Software y aplicaciones para la interoperabilidad e intercambio de información
- Página web
- Software dedicado y/o especializado a comunicaciones, a la seguridad y ciberseguridad e Infraestructura tecnológica, controles de acceso lógico.

8.5 PROYECCIÓN DE PRESUPUESTO

Para la presente vigencia 2023, se avanzará remedialmente de conformidad con los recursos disponibles asignados a la actual Oficina de Sistemas y los demás componentes, se implementarán progresivamente en la medida que se produzca la asignación de recursos

para el año 2024, 2025 y 2026. Tal como se describe en la situación actual, la Oficina de Sistemas tiene asignado un presupuesto para la vigencia 2023, cuya ejecución presupuestal es monitoreada de manera periódica de acuerdo con el Plan Anual de Compras.

Metro Cali S.A. Acuerdo de Reestructuración revisará periódicamente la proyección presupuestal correspondiente al presente plan, para dar cubrimiento en la presente y siguientes vigencias, de conformidad con sus ingresos, proyección de ingreso y definición de prioridades estratégicas definidas por la Alta Dirección.

Respecto a los costos del plan, para la vigencia 2023 se supedita dar cubrimiento al talento humano citado en los recursos del plan. Para las vigencias 2024-2026 se procederá a la solicitud de disponibilidad de recursos, que resulten consecuentes con la declaración de aplicabilidad que resulte aprobado en el desarrollo del sistema de gestión de seguridad, privacidad de la información y ciberseguridad, según corresponda a los programas y proyectos priorizados en busca del propósito y objetivos propuestos.

8.6 PROYECTOS Y ACTIVIDADES DE SEGURIDAD DE LA INFORMACIÓN

Acorde con la disponibilidad de recursos los proyectos y actividades citados, infieren continuar con la ejecución paulatina y progresiva, desde un alcance básico del MSPI, su complemento y formalización, para continuar avanzando en el desarrollo y madurez en las distintas fases y componentes del modelo, hasta su culminación y mejora continua, que también será progresiva.

La Tabla 4 siguiente, relaciona los proyectos y actividades que serán abordados con mayor prioridad. No obstante, el desarrollo de los mismos será supeditado a la priorización que defina la entidad y al apalancamiento respectivo.

Tabla 4.Proyectos de Seguridad y Privacidad de la Información de Metro Cali S.A. Acuerdo de reestructuración

ID	Proyecto / Actividad	Fecha
1	Actualización del diagnóstico de seguridad, privacidad de la información y ciberseguridad	Recurrente, cada año
2	Matriz de vulnerabilidades y amenazas	Recurrente, cada año 4

ID	Proyecto / Actividad	Fecha
3	Revisar, complementar, ajustar, documentar y formalizar el sistema de gestión de seguridad, privacidad de la información y ciberseguridad (SGSPIC)	Recurrente, hasta su completitud 2023-2026
4	Definir y/o ajustar políticas, manuales, procedimientos e instructivos asociados a la información	Recurrente, hasta su completitud 2023-2026
5	Inventario de activos de información y valoración	Recurrente, hasta su completitud 2023-2026
6	Definir las directrices frente a la conservación de la integridad, confidencialidad y disponibilidad de la información de la entidad.	Recurrente, hasta su completitud 2023-2026
7	Formalizar y socializar a los colaboradores de la entidad las políticas y lineamientos establecidos	Recurrente, hasta su completitud 2023-2026
8	Definir y elaborar la estrategia de Uso y Apropiación e implementarla	Recurrente, hasta su completitud 2023-2026
9	Realizar actividades tendientes a la Planeación, implementación, Gestión y mantenimiento del SGSI	Recurrente, hasta su completitud 2023-2026
10	Asistir a las reuniones de trabajo del MPIG V4 y apoyar en la articulación de sistemas de gestión	2023-2026
11	Gestionar los proyectos asociado a la implementación de controles	2023-2026
12	Revisar los controles propuestos por las dependencias, para mitigar los riesgos de seguridad de la información identificados.	2023-2026
13	Concertar mesas de trabajo con los líderes de proceso, para categorizar los tratamientos del riesgo propuestos en sus mapas de proceso.	2023-2026
14	Fortalecimiento de la infraestructura tecnológica de Metro Cali S.A. Acuerdo de reestructuración (Sistemas de información, Red, control de	2023-2026

ID	Proyecto / Actividad	Fecha
	acceso, servidores y almacenamiento, similares) para efectos de fortalecer los mecanismos de control actual.	

Fuente: Metro Cali Acuerdo de Reestructuración, 2023

8.7 PLAN PROYECTO DE INVERSIÓN

Los proyectos a ejecutar del plan, también están contemplados dentro del presupuesto de funcionamiento del componente de TI de la entidad para la vigencia 2023 -2025. Ante los recursos disponibles, se opta por la continuidad de las iniciativas en marcha y la incorporación de nuevos proyectos para solución a situaciones críticas que son necesarios para la continuidad de la operación.

Se produce como reto, cumplir con los proyectos citados en el presente plan, que darán lugar a la constitución de la declaración de aplicabilidad y su aprobación, sobre la cual, se producirá la ruta de ejecución de conformidad con nuevos proyectos, que se someterán a ejercicios de priorización, aprobación y solicitudes de disponibilidad de recursos.

Los costos de operación y está inmerso en los costos de funcionamiento de la Oficina de Sistemas.

Tabla 5.Presupuesto de funcionamiento aprobado para la para el componente Tecnológico año 2023

Item	Descripción	Valor total estimado	Valor estimado en la vigencia actual
1	Contratar la prestación de servicios tecnológicos y de comunicaciones requeridos por Metro Cali S.A. Acuerdo de Reestructuración.	155.736.000 COP	155.736.000 COP
2	Soporte de Sistema de Gestión Documental SEVENET y mantenimiento equipos de escaneo.	18.262.280 COP	18.262.280 COP
3	Soporte y mantenimiento Sistema Financiero (AWA y Talents)	66.920.132 COP	66.920.132 COP
4	Soporte y mantenimiento Sistema de Gestión de la Entidad (SIGEM)	25.048.788 COP	25.048.788 COP
5	Contratar servicio renovación antivirus corporativo	9.993.293 COP	9.993.293 COP
6	Renovación Licencia Soporte Emme - Compra Licencia Emme 3	15.079.680 COP	15.079.680 COP
7	Contratar servicio soporte de Firewall Corporativo Fortinet y de renovación de Hiper Visor VMWARE Vsphere	36.561.820 COP	36.561.820 COP
8	Contratar el servicio de Outsourcing de impresión, fotocopiado y escaneo de documentos, con inclusión de tóner, al igual que el alquiler de scanner y video proyectores, incluido mantenimiento preventivo y correctivo que se requiera.	38.192.571 COP	38.192.571 COP
9	Contratar el licenciamiento de Microsoft Windows Server 2023 con servicio de instalación y configuración, servicio de migración de datos, además del suministro de discos duros para HPE MSA 1050 SAN Storage y renovación soporte para 2 servidores HP ProLiantDL385 Gen10 y HPE MSA 1050 SAN Storage, según las especificaciones técnicas definidas por Metro Cali S.A. Acuerdo de Reestructuración.	135.000.000 COP	135.000.000 COP
10	Contratar servicios de alquiler de computadores de escritorio y portátiles incluido todos los servicios conexos necesarios de manera integral a fin de garantizar un correcto funcionamiento sin formula de reajuste, mediante sistema de precios fijos unitarios y servicio de asistencia técnica en sitio a los usuarios que se encuentren dentro de las instalaciones de Metro Cali S.A. (Pendiente Impuestos).	165.099.914 COP	165.099.914 COP
11	Contratar la compra y adquisicion de los equipos tecnológicos necesarios a utilizarse en las salas de Juntas y oficina de la Presidencia de la Entidad (3 pantallas de 65 pulgadas interactivas tactil 4K, 3 barras de sonido Smart 900, 2 arañas para videoconferencia).	55.000.000 COP	55.000.000 COP
12	Servicios en la nube; Servicio Disaster Recovery (DRP) y almacenamiento copia de respaldo (BACKUP) para servidores de aplicaciones misionales (Finanicero, Nomina, Sevenet, Sigem)	84.931.222 COP	84.931.222 COP
13	Adquirir Licencias de Autocad.	22.400.000 COP	22.400.000 COP
14	Sistema de copias de seguridad automatizado en Disco para salvaguardar la información de la entidad ajustándose a la política de la seguridad de la información.	33.011.308 COP	33.011.308 COP
15	Renovación de servicios en la nube de Correo Electrónico, Ofimática, Power BI, Visio y 2 licencias de project.	180.294.355 COP	180.294.355 COP
16	Mantenimiento de Licencias Arcgis	45.543.015 COP	45.543.015 COP
	TOTAL	1.087.074.378	1.087.074.378

Fuente: Plan Anual de Adquisiciones, Metro Cali S.A Acuerdo de Reestructuración, 2023

8.8 PLAN DE COMUNICACIONES

La entidad socializará con los grupos de interés el presente plan, mediante comunicación y publicación en el sitio web de la entidad.

De igual manera, el plan propone mantener de forma recurrente un proceso de concienciación, capacitación y comunicación para ser desarrollado por el área competente de la entidad. Propone avanzar remedialmente de conformidad con la disponibilidad de recursos y será recurrente para cada anualidad o vigencia fiscal subsiguiente: 2024, 2025 y 2026.

Durante el desarrollo del plan, se concibe ampliar el alcance de la sensibilización, divulgación y generación de conciencia, hasta producir competencias generales, especializadas y subespecializadas para soportar los roles en proyectos, actividades y operaciones concebidas que permitan el logro del propósito y objetivos del plan al mantener la seguridad de la información interna y respuesta a los riesgos en el ciberespacio.

Tabla 6.Metas y acciones del programa de concienciación y capacitación

Meta	Acciones	Período
Identificación de necesidades.	Métodos para identificación de necesidades	2024 - 2026
	Colaboración con otras áreas y algunas necesidades adicionales a identificar	
Diseño del plan de capacitación y sensibilización.	Definir prioridades (Temáticas)	2024 - 2026
	Definir la complejidad del material a desarrollar / adquirir / emplear	
	Financiamiento del plan de capacitaciones	
Desarrollo de materiales para el programa.	Desarrollo de material para sensibilización	2024 - 2026
	Desarrollo de material para entrenamiento	
Implementación del programa.	Temáticas de la capacitación presentadas	2024 - 2026
	Relación de entrega de valor institucional	
	Evidencias de la asistencia a Capacitaciones y el compromiso con la entidad	

Meta	Acciones	Período
Post-implementación	Evaluación del programa	2024 - 2026
Mejoramiento del plan de capacitaciones.	Análisis de las evaluaciones	2024 - 2026
	Recomendaciones para la mejora	
Indicadores del plan de capacitaciones.	Definición y estructura de indicadores	2024 - 2026

Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

Es necesario precisar que la sensibilización y la concienciación debe ser aplicada para toda la entidad. Entre los temas propuestos en el presente plan para ser incorporados se relacionan en la tabla 7.

Tabla 7.Temática inicial de sensibilización

Temática inicial para sensibilización de Seguridad y Privacidad en Metro Cali S.A. Acuerdo de reestructuración	
Administración de Contraseñas	Uso y manejo de inventario
Malware y sus diferentes tipos	Software permitido/prohibido en la entidad
Políticas Organizacionales Relacionadas con Seguridad de La Información	Uso de dispositivos de la entidad fuera de las instalaciones
Uso de correo electrónico e identificación de correos sospechosos	Seguridad en el puesto de trabajo
Uso apropiado de internet	Temas de control de acceso a los sistemas (privilegios, separación de roles)
Política de Escritorio Limpio.	Ingeniería social.
Sanciones por incumplimiento de las políticas.	Gestión de incidentes (cómo reportar, qué puedo reportar).
Administración de contraseñas.	Uso y manejo de inventario.
Malware y sus diferentes tipos.	Software permitido/prohibido en la entidad.
Políticas organizacionales relacionadas con seguridad de la información.	Uso de dispositivos de la entidad fuera de las instalaciones.

Fuente: Metro Cali S.A Acuerdo de Reestructuración, 2023

8.9 REFERENCIAS

- Modelo de Seguridad y Privacidad de la información – MSPI, versión 3.0.2 y Modelo de Gestión de riesgos de Seguridad Digital, Ministerio de Tecnologías de la Información, 2018. Arquitectura TI Colombia, MinTIC. Link: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf
- Guía del MSPI, Ministerio de Tecnologías de la Información y las comunicaciones, MinTIC.2018. Link: https://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan_comunicacion_sensibilizacion.pdf.
- Documentos del Estándar ISO/IEC 27000; 27001; 27032; 27005; 31000, entre otras
- Documentos de NIST CSF

9 ANEXOS

No aplica

10 OBSERVACIONES

La persona que desarrolló estructural y metodológicamente el documento fue:

Uriel de Jesús Ramírez Márquez Profesional Especializado Oficina de Sistemas.

Para la revisión de forma del documento se contó con la colaboración de:

Marlene Jennifer Hollaender Contratista de la Dirección de Planeación

Diana Marcela Gallego Santamaría Contratista de la Dirección de Planeación

Las personas que participaron en la construcción del presente plan fueron:

Uriel de Jesús Ramírez Márquez Profesional Especializado Oficina de Sistemas

Gabriel Federman Ortiz Segura Jefe de Oficina de Sistemas

Las personas que participaron en la revisión del presente plan fueron:

Uriel de Jesús Ramírez Márquez — Profesional Especializado Oficina de Sistemas

Gabriel Federman Ortiz Segura — Jefe de Oficina de Sistemas

Las personas que participaron de la documentación del presente plan fueron:

Gabriel Federman Ortiz Segura — Jefe de Oficina de Sistemas

Uriel Ramírez Márquez — Profesional Especializado Oficina de Sistemas

El presente plan fue aprobado por el Comité de Institucional de Gestión y Desempeño de Metro Cali Acuerdo de Reestructuración en la sesión sostenida el día 26 de enero de 2023.

Elaborado por:	Cargo:
Uriel Ramírez Márquez	Profesional Especializado Oficina de Sistemas
Revisado y Aprobado por:	**Cargo:**
Gabriel F. Ortiz Segura	Jefe de Oficina de Sistemas