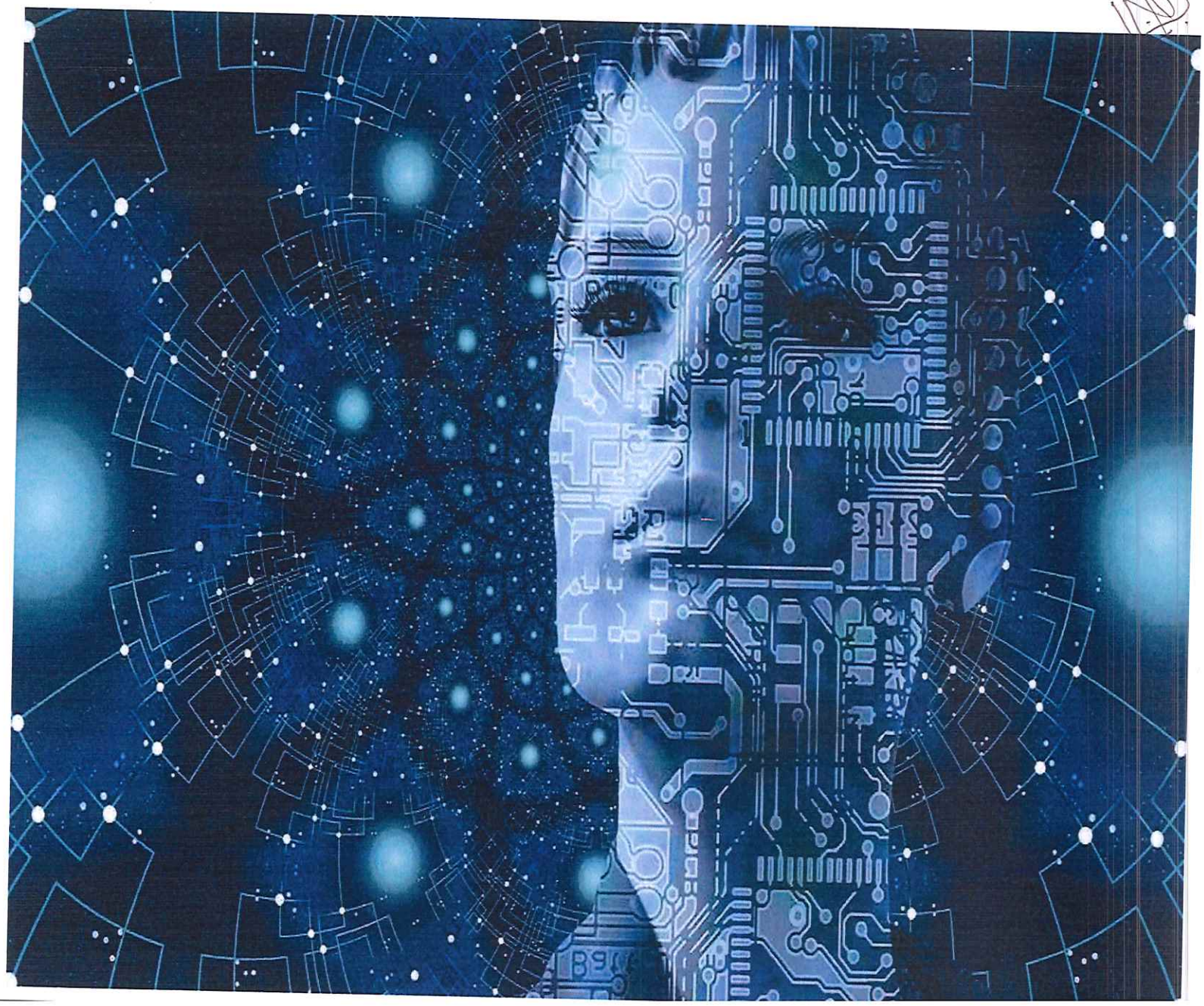
Plan de Tratamiento de Riesgos de Seguridad, Privacidad de la Información y Ciberseguridad

Vigencia 2023 – 2026



1. CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

2. INTRODUCCIÓN

En las bases de las políticas de gobierno y seguridad digital, fundamentales para la transformación empresarial y digital de la entidad, la seguridad de la información es parte esencial para el logro de los objetivos institucionales. De igual manera, las amenazas en el ciberespacio son cada vez más frecuentes y sofisticados. En consecuencia, los ataques e incidentes de seguridad digital son complejos y con mayor experticia de sus autores, que implican graves consecuencias de tipo económico o social, conllevando al deterioro de la confianza digital y la desaceleración del desarrollo en el futuro digital con afectación reputacional.

Lo anterior exige que, la entidad cuente con suficiente capacidad institucional y una gestión adecuada y oportuna de sus activos de información y de su infraestructura crítica. Por su parte, los gobiernos alrededor del mundo han venido atendiendo los nuevos retos para la detección y manejo de amenazas, ataques e incidentes cibernéticos mediante la formulación y actualización de estrategias o políticas relacionadas con la seguridad digital como en el caso de Colombia con el CONPES 3995 de 2020. Este avance en la política pública dinamiza a que se amplié el espectro, considerado en el plan de seguridad y privacidad de la información del periodo anterior (2019-2022), al incluir los aspectos de la ciberseguridad o seguridad digital en el plan 2023-2026 con fortalecimiento de su Sistema de Gestión de seguridad, Privacidad de la Información y Ciberseguridad (SGSPIC). En su desarrollo propone condiciones para mantener la confidencialidad, integridad y disponibilidad de activos de información y activos de mayor criticidad, mediante la protección contra el acceso, uso, divulgación, interrupción, modificación o destrucción no autorizados u otras amenazas resultantes.

La decisión estratégica de adoptar un enfoque de seguridad basado en el riesgo, conduce a una evaluación integral de las amenazas que enfrenta la entidad y las vulnerabilidades en su entorno operativo actual.

Para el logro de los objetivos institucionales el Plan de Seguridad, Privacidad de la Información y Ciberseguridad 2023-2026 operará en conjunto con el actual, como instrumentos para la adecuación y actualización del sistema de gestión de seguridad, privacidad de la información y ciberseguridad, que obre de conformidad con los requisitos de ley normativos y técnicos a través de sus modelos MSPI y MGRSD.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Disminuir la probabilidad y el impacto de riesgos de seguridad y privacidad de la información que puedan afectar a Metro Cali S.A. Acuerdo de Reestructuración, mediante el cierre de brechas de seguridad interna y en el ciberespacio y la implementación de controles y su seguimiento. Proporcionar una seguridad e integridad razonable que genere una base confiable para la toma de decisiones y la planificación institucional, orientada a la entrega de valor público por parte de la entidad y organizaciones circunscritas al servicio público esencial del sistema de transporte masivo de pasajeros.

3.2 OBJETIVOS ESPECÍFICOS

a. Cerrar progresivamente las brechas existentes de seguridad de la información y ciberseguridad, mediante la gestión de procesos de apreciación y tratamiento de riesgos de seguridad digital.

b. Revisar la declaración de aplicabilidad que se obtenga del plan de seguridad, privacidad de la información y ciberseguridad para someterlo a ejercicios de priorización, acorde con las prioridades de la entidad, la capacidad institucional y la participación. Todo este trabajo a través del comité de TI y/o de seguridad, privacidad de la información y ciberseguridad, según corresponda.

c. Consolidar los proyectos que resultan de la declaración de aplicabilidad del SGSPIC y orientarlos hacia el área de la entidad que corresponda para su gestión, acorde con las competencias institucionales requeridas, la priorización y la definición de recursos.

d. Revisar y adoptar, según su pertinencia, los dominios, objetivos y controles referidos en la Norma ISO/IEC 27001:2013 en procura de la transición hacia la Norma ISO/IEC 27001:2022, para garantizar los controles necesarios elegidos del tratamiento de riesgos de seguridad de la información.

4. ALCANCE

El presente plan cuenta con aplicabilidad basada a la Declaración de Aplicabilidad – SoA-, como resultado de la fase de planeación del SGSPIC a todos los procesos de la entidad y en las partes interesadas del negocio, durante la vigencia 2023-2026.

Incluye la implementación de controles priorizados, teniendo en cuenta los dominios definidos en la Norma ISO 27001:2013, con progresividad y transición a la ISO 27001:2022, según aplique. De igual manera, busca una evaluación integral de las amenazas y las vulnerabilidades del entorno operativo actual en el ciberespacio, a las cuales se enfrenta la entidad. Además, del cumplimiento de los requisitos de la Política de Gobierno Digital y los lineamientos de la arquitectura empresarial, adoptados por la entidad mediante Resolución N° 912.110.284 de 28 de diciembre de 2020.

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 la cual se dictan disposiciones generales del hábeas 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: "Por el cual se crea la Comisión Nacional Digital y de Información Estatal".
- Ley 1712 de 2014: Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 1074 de 2015: por medio del cual se expide instrucciones sobre el registro nacional de bases de datos.
- 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: Política Nacional de 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: 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 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 quien ejerce el rol de Director del Proceso Tecnológico, actualmente el Jefe de la Oficina de Sistemas. La responsabilidad en el desarrollo y actualización del plan es la persona que ejerce el rol de oficial de seguridad, privacidad de la información y ciberseguridad de la entidad. Persona que desarrolla el plan para la 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. Finalmente, es 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 marcos 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. Asimismo, 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. Estos facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas, que cumplen con funciones públicas. 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. 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 y su relación con los distintos procesos de la empresa para la entrega de valor. A continuación, se evidencia un resumen los resultados del diagnóstico.

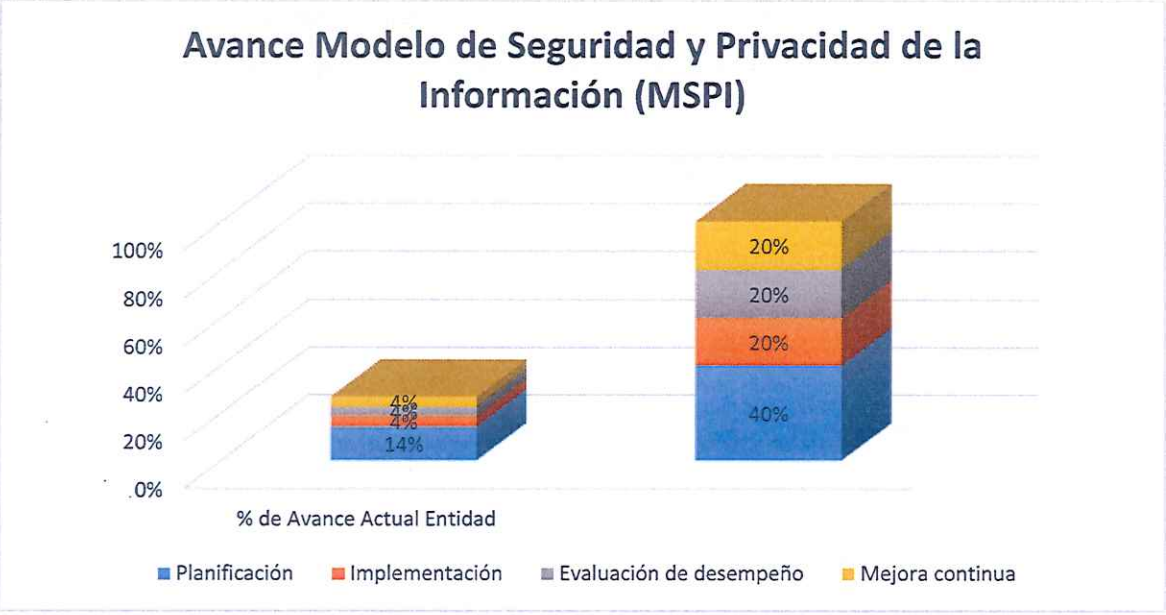
Tabla 1.Avance Modelo de Seguridad y Privacidad de la Información (PHVA).

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.

Figura 1.Modelo de Seguridad y Privacidad de la Información (MSPI).

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



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

8.1.2 ESTRUCTURA FUNCIONAL PARA EL TRATAMIENTO DE RIESGOS

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. El tratamiento de riesgos de seguridad digital se mantiene con las acciones concebidas por la operación de TI en la entidad.

8.2 ACTIVIDADES PARA LA CONTINUIDAD DE LA OPERACIÓN ACTUAL

Con la identificación y priorización de brechas frente al perfil objetivo, se da lugar a la definición del Plan de Seguridad, Privacidad de la Información y Ciberseguridad 2023-2026. Se definen los programas y proyectos pertinentes que conlleven a la priorización, frente a la seguridad de la información y la respuesta a los riesgos en el ciberespacio. A continuación, se muestran las acciones desarrolladas durante el 2021 y 2022 y, las actividades de la operación.

Tabla 2.Actividades 2021- 2022. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Alcance	Actividad	Vigencia	Estado 2021	Estado 2022
Continuidad de la operación de la entidad según su modelo actual, y de la Oficina de Sistemas.	Servicio renovación antivirus corporativo.	2021	Renovación con la firma INFORTEC. Contrato N° 917.108.8.03.2021.	Contratado, ejecutado y liquidado.
	Soporte y mantenimiento Sistema Financiero (AWA y Talents).	2021	Soporte y mantenimiento con la firma AFQ. Contrato N° 917.104.2.174.2021.	Contratado, ejecutado y liquidado.
	Soporte y mantenimiento Sistema de Gestión de la entidad (SIGEM).	2021	Soporte y mantenimiento con la firma BINAPS. Contrato N° 917.104.2.176.2021.	Contratado, ejecutado y liquidado.
	Servicio soporte de Firewall Corporativo Fortinet y de renovación de Hiper Visor VMWARE Vsphere.	2021	Soporte y mantenimiento con la firma Controles Empresariales. Contrato proceso mínima cuantía N° 917.108.8.05.2021.	Contratado, ejecutado y liquidado.
	Implementar servicios de infraestructura de red Microsoft Active Directory Domain Services y Windows	2021	Implementación con la firma The Best Experience in Technology S.A. Contrato	Contratado, ejecutado y liquidado.

Alcance	Actividad	Vigencia	Estado 2021	Estado 2022
	Server Update Services, y adquirir servicios en la nube de correo electrónico, ofimática, Power BI y Visio.		N° 917.104.1.01.2021.	
	Soporte de Sistema de Gestión Documental SEVENET, compra de impresora de códigos de barra y mantenimiento equipos de escaneo.	2021	Soporte y mantenimiento, compra de impresora y mantenimiento de equipos con la firma LEXCO. Contrato N° 917.104.2.464.2021.	Contratado, ejecutado y liquidado.
	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.	2021	Debido a la difícil situación económica de la entidad quedó para la vigencia 2022.	No contratado.
	Discos para HPE MSA 2050 (Discos SAS 10.000 rpm / 2.4TB), incluida instalación, que permitan contar con capacidad de almacenamiento para	2021	Se recibieron cotizaciones de los discos. Sin embargo, vía telefónica los proveedores informaron que no ofrecían mano de	Para la vigencia 2021 no se llevó a cabo el proceso de contratación. En la vigencia

Alcance	Actividad	Vigencia	Estado 2021	Estado 2022
	las labores diarias de los funcionarios de la entidad.		obra porque es muy especializada para este equipo y que no disponían del personal calificado para este servicio. Se evaluará en el 2022 adquirir un equipo NAS para el almacenamiento de archivos institucionales y liberar espacio de la HPE MSA 1050 dejándola solo para guardar las aplicaciones misionales.	2022 el proceso fue declarado desierto en dos ocasiones.
	Service Disaster Recovery As A Service (DRaaS).	2021	Debido a la difícil situación económica de la entidad, quedó para la vigencia 2022.	En la vigencia 2021 no se llevó a cabo el proceso de contratación. En la vigencia 2022 se inició la proyección de la documentación del proceso de contratación,

Alcance	Actividad	Vigencia	Estado 2021	Estado 2022
				pero no se finalizó.
	Soporte y garantía Switches Alcatel.	2021	Debido a la difícil situación económica de la entidad, quedó para la vigencia 2022.	No se recibió viabilidad financiera, en las dos vigencias.
Fuente: Metro Cali S.A. Acuerdo de Reestructuración, 2023.				

Tabla 3.Actividades 2022 – 2023. Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información.

Alcance	Actividad	Estado 2022
Continuidad de la operación de la entidad según su modelo de operación actual, y de la Oficina de Sistemas.	Contratar servicio renovación antivirus corporativo.	En ejecución.
	Contratar la prestación de servicios tecnológicos y de comunicaciones requeridos por Metro Cali S.A. Acuerdo de Reestructuración.	Finalizado sin liquidar.
	Renovación licencia Soporte Emme - Compra Licencia Emme 3.	Finalizado sin liquidar.
	Contratar servicio soporte de Firewall Corporativo Fortinet y de renovación de Hiper Visor VMWARE Vsphere.	En ejecución.
	Mantenimiento de licencias Arcgis.	En ejecución.
	Software de monitoreo de datos.	No se recibió viabilidad financiera.
	Soporte de Sistema de Gestión Documental SEVENET y mantenimiento equipos de escaneo.	Finalizado sin liquidar.
	Mantenimiento preventivo video proyectores y compra de video proyector.	No se recibió viabilidad financiera.
	Adquirir Soporte y garantía para los equipos de la red inalámbrica Cisco (1 Controladora "AIR-CT2504-25-K9Z" + 20 Aps "AIR-AP1852I-A-K9") - Smart Net Total Care 8 x 5 x Siguiente día laborable.	No se recibió viabilidad financiera.

Alcance	Actividad	Estado 2022
	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.	No se recibió viabilidad financiera.
	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.	En ejecución por prorroga solicitada por 2 meses, para la vigencia 2023.
	Renovación de servicios en la nube de correo electrónico, ofimática, Power BI, Visio y 2 licencias de Project.	En ejecución.
	Servicios en la nube: Servicio Disaster Recovery (DRP) y almacenamiento copia de respaldo (BACKUP), para servidores de aplicaciones misionales (financicero, nómina, Sevenet y Sigem).	Se inició la proyección de la documentación del proceso de contratación, pero no se finalizó.
	Contratar servicios de alquiler de computadores de escritorio y portátiles. Incluidos todos los servicios conexos necesarios de manera integral, para garantizar un correcto funcionamiento sin fórmula 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. (Pendiente impuestos).	En ejecución por prorroga solicitada por 3 meses, para la vigencia 2023.
	Soporte y mantenimiento Sistema Financiero (AWA y Talents).	Finalizado sin liquidar.
	Soporte y mantenimiento Sistema de Gestión de la entidad (SIGEM).	Finalizado sin liquidar.

Fuente: Metro Cali Acuerdo de Reestructuración, 2023.

8.3 PRESUPUESTO

Para la vigencia 2023 la entidad revisará periódicamente la proyección presupuestal correspondiente al plan. Todo encaminado a 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. Así mismo, estará sujeto a los resultados de la declaración de aplicabilidad que resulte 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.

8.4 PROYECTOS Y ACTIVIDADES DEL PLAN

Para el 2023 se mantiene el desarrollo de las actividades que tienen relación con los proyectos y procesos priorizados, como se muestra en la tabla 4.

Tabla 4.Proyectos y actividades 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

8.5 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 dar 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 este 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 están inmersos en los costos de funcionamiento al proceso tecnológico.

Tabla 5.Presupuesto de funcionamiento aprobado el proceso tecnológico año 2023.

Objeto de gasto	Presupuesto 2023 publicado
Funcionamiento y fortalecimiento institucional	$ 1.087.074.378,00
Infraestructura	
Servicios externos	
Total asignado	$ 1.087.074.378,00
Fuente: Metro Cali S.A. Acuerdo de Reestructuración, 2023.	

8.6 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 año 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 sub-especializadas para soportar los roles en proyectos, actividades y operaciones concebidas. De esta manera, alcanzar el 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.	
Post-implementación.	Evaluación del programa.	2024 - 2026
Mejoramiento del plan de capacitaciones.	Análisis de las evaluaciones.	2024 - 2026
	Recomendaciones para la mejora.	

Meta	Acciones	Período
Indicadores del plan de capacitaciones.	Definición y estructura de indicadores.	2024 - 2026

Es necesario precisar que, la sensibilización y la concienciación deben ser aplicadas para toda la entidad. Los temas propuestos en el presente plan para se relacionan en la tabla 7.

Tabla 7.Temática inicial de sensibilización.

Temática inicial para sensibilización de Seguridad y Privacidad en Metro Cali	
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).

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

8.7 REFERENCIAS

- Anexo 4: lineamientos para la gestión de riesgos de seguridad digital en entidades públicas, MinTic, Viceministerio de Economía Digital, Dirección de Gobierno en Línea 2018.
- Documentos del estándar ISO/IEC 27000; 27001; 27032; 27005; 31000, entre otras.
- Documentos de NIST CSF.
- 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.

- 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, 2017. Arquitectura TI Colombia, Mintic. Link: https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

9 ANEXOS

No aplica.

10 OBSERVACIONES

Desarrollo estructural y metodológico del documento:

Uriel de Jesús Ramírez Márquez	Profesional Especializado Oficina de Sistemas.

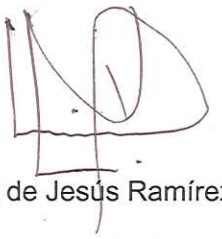
Revisión contenido del documento:

Marlene Jennifer Hollaender	Profesional contratista de la Dirección de Planeación.
Diana Marcela Gallego Santamaría	Profesional contratista de la Dirección de Planeación.

Participantes en la construcción del documento:

Luís Javier Uribe Villaquirán	Contratista de la Oficina de Sistemas.
Uriel de Jesús Ramírez Márquez	Profesional Especializado Oficina de Sistemas.
Holman Jimmy Rodríguez	Técnico Administrativo Oficina de Sistemas.
Gabriel Federman Ortiz Segura	Jefe de Oficina de Sistemas.

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

Elaborado por:	Cargo:
 Uriel de Jesús Ramírez Márquez	Profesional Especializado Oficina de Sistemas
Revisado y aprobado por:	Cargo:
 Gabriel Federman Ortiz Segura	Jefe de Oficina de Sistemas