Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Metro Cali S.A.

Vigencia 2019 – 2022

Seguimiento 2020

Terminal de Calipso - Cali

1. CONTENIDO

LISTADO DE FIGURAS

LISTADO DE TABLAS

2. INTRODUCCIÓN

El tratamiento de riesgos de seguridad y privacidad de la información de la Entidad conlleva a la implementación de controles y su seguimiento para efecto de generar confianza en el desarrollo misional de la empresa, la interoperabilidad y el intercambio de información entre estado-ciudadanos-entidades. Para efecto de aplicar las mejores prácticas establecidas por el Estado colombiano, determina acciones previas, consecuentes y articuladas de la Entidad en el ámbito del propósito de la empresa y propósito misional con el sistema MIO, como la definición e implementación de los habilitadores transversales de la Política de Gobierno Digital, como son: Arquitectura Empresarial y el sistema de Gestión para la Seguridad y Privacidad de la información, y por supuesto las actividades definidas con la Arquitectura de TI, que involucra, la definición, estructura, implementación, gobierno y gestión de la arquitectura de información de la entidad.

El Gobierno y gestión de la información implica la necesidad de mantener mecanismos, estrategias y herramientas de la seguridad de la información y sus controles. En consecuencia con lo anterior y con los lineamientos de Gobierno Digital y en consideración a su transversalidad en la definición e implementación de la Política, Metro Cali S.A. ha establecido planes de mediano plazo, como el Plan Estratégico de Tecnologías de la Información y las Comunicaciones – PETI y el Plan de Seguridad y Privacidad de la Información – PSPI en un período de cuatro (4) años (2019-2022), que coadyuve dentro del ámbito de la Empresa, al fortalecimiento de la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, políticas y normas, y la identificación de soluciones a problemáticas de interés común. De igual forma, ha concebido su seguimiento para el 2020 que articula las acciones desarrolladas durante el 2019 para efecto de continuidad de la estrategia, lo cual requiere del entendimiento Estratégico por parte de los actores de la Entidad y el apalancamiento necesario y suficiente para el desarrollo y evolución hasta la consecución de los objetivos propuestos, para velar por su mejora continua.

En el desarrollo de las acciones en búsqueda de su propósito institucional, en cumplimiento de sus funciones, permanentemente, todas las áreas, procesos, personas y activos de la Entidad

están sometidos a riesgos de seguridad y privacidad de la información que pueden limitar o hacer fracasar una gestión; por lo tanto, es necesario tomar las medidas, para identificar las causas y consecuencias de la materialización de dichos riesgos para evitarlo procediendo con un tratamiento adecuado. Lo anterior introduce como objetivo orientar y facilitar la implementación y desarrollo de una eficaz, eficiente y efectiva gestión del riesgo, desde la identificación hasta el monitoreo; usando como base, fundamentos teóricos y lineamientos, para facilitar su identificación, reconocimiento de las causas, efectos, definición de controles y de lineamientos sencillos y claros para su adecuada gestión.

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Generar un Plan que permita disminuir la probabilidad y el impacto de los riesgos de seguridad y privacidad de la información que puedan afectar a Metro Cali S.A. para proporcionar una seguridad e integridad razonable que genere una base confiable para la toma de decisiones y la planificación institucional.

3.2 OBJETIVOS ESPECÍFICOS

- Alinear los objetivos de cada proceso y subproceso en torno a la Política de seguridad y privacidad de la información de Metro Cali S.A. y frente a la gestión de la información con base en las mejores prácticas.
- Identificar y sensibilizar a la entidad para la construcción de acciones que conlleven al fortalecimiento de la Entidad frente a la seguridad y privacidad de la información.
- Fortalecer los recursos tecnológicos en torno al tratamiento de riesgos de seguridad y privacidad de la información, con el enfoque de facilitar su alineación con un sistema de Gestión de Seguridad de la Información una vez, este se encuentre en desarrollo en la Entidad.
- Coadyuvar en la priorización de la definición e implementación de la Arquitectura de Información de la Entidad,
- Revisar, ajustar y/o validar la Política de la Entidad de Gestión de Riesgos de seguridad y privacidad de la información.

- Definir y desarrollar estrategias para el seguimiento, definición y ejecución de proyectos orientados al tratamiento de riesgos de seguridad y privacidad de la información con priorización de aspectos críticos identificados por los Líderes de los distintos procesos de la Entidad, y los riesgos de mayor probabilidad o impacto identificados por el Sistema de Gestión de riesgos que se implemente en la Entidad, validando los recursos con los que se cuentan actualmente en Metro Cali S.A.
- Minimizar efectos no deseados ante potenciales amenazas y vulnerabilidades existentes, que sea objetivo, progresivo, escalable y gradual.
- Identificar y reportar de manera oportuna los eventos generadores de riesgos y sus causas, de seguridad y privacidad de la Información en el contexto de Metro Cali S.A.
- Generar un panorama de la Entidad para la implementación de controles ante los riesgos valorados en una adecuada gestión de riesgos en una frontera de tiempo para un adecuado tratamiento de riesgo de seguridad y privacidad de la información
- Aplicar las metodologías del DAPF[1] e ISO[2] respectivamente en seguridad y riesgo de la información, para Metro Cali S.A.
- Implementar acciones correctivas y preventivas orientadas a reducir el riesgo a niveles aceptables de acuerdo a lo definido por el comité de Seguridad de la Información.

4. ALCANCE

El presente Plan fue concebido para una frontera de aplicación de cuatro años desde el 2019 hasta el 2022. Implica la articulación de las acciones remediales desarrolladas en el año 2019, de acuerdo con la capacidad actual de la Oficina de Sistemas frente al modelo de operación de la empresa, acompañando en su evolución para la definición e implementación del Plan de Seguridad y Privacidad de la Información de la Entidad. Inicia con la definición y establecimiento, por parte del Presidente y la Alta Dirección, de la “Declaración de Aplicabilidad – SOA” del Sistema de Gestión de Seguridad y Privacidad de la Información que se defina e implemente, y las acciones de cada proceso para la gestión y seguimiento de riesgos de seguridad y privacidad de la información, complementado con los resultados de los Proyectos de TI para tratamiento de riesgos de seguridad y privacidad de la información. Lo anterior, como resultado de la

[1] *DAPF es el Departamento Administrativo de la Función Pública de Colombia*

[2] *ISO es International Organization for Standardization, que en español traduce, Organización Internacional de Normalización*

implementación y operación en la empresa del modelo de seguridad y privacidad de la información del Estado Colombiano definido por MinTic. Se activa con la identificación, caracterización, valoración de los riesgos de seguridad y privacidad de la información y priorización de acciones para el tratamiento por parte de cada Líder de proceso de la empresa, en el contexto del servicio de transporte público masivo de pasajeros de Santiago de Cali y el Sistema MIO. Tiene aplicación con los resultados de la operación de los componentes y habilitadores transversales de la Política de Gobierno Digital; Arquitectura de información en la Entidad, articulada con la Arquitectura Empresarial, la Arquitectura de TI, la aplicación y seguimiento de: la Política de TI, Política de Seguridad y Privacidad de la Información. Exige la definición de roles y responsabilidades de la información en cada proceso de la Empresa en el contexto descrito. Para ser implementado por Metro Cali S.A., se enmarca en los ámbitos, lineamientos y guías de conformidad con el Modelo de Seguridad y Privacidad de la Información - MSPI de conformidad con la Política de Gobierno Digital del Estado Colombiano, lineamientos, legislación, normas, guías y marcos de referencia definidos por el DAFP e ISO 27001, ISO 27002, 27005 e ISO 31000 y/o COSO para cerrar el ciclo de la gestión de la seguridad y privacidad de la información de la Entidad, mediante un adecuado tratamiento de riesgos de seguridad y privacidad de la información, evaluación y mejora continua.

Para su mantenimiento y mejora continua cada vez que Metro Cali S.A. realice un ejercicio o proyecto de Arquitectura Empresarial, o avance en el tratamiento de riesgos e implementación de controles, o revisión ante cambio de normatividad y/o legislación, su resultado debe ser integrado al presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información - PTR-SPI de la Entidad.

5. NORMATIVIDAD

La normatividad en el cual se enmarca el Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Metro Cali S.A. se encuentra dentro del marco de la legislación alusiva al Sistema de gestión pública del Estado Colombiano, especialmente de la Política de Gobierno Digital (antes Estrategia de Gobierno en Línea – GEL) y articulada con la reglamentación y lineamientos producidos por la legislación Colombiana, Decreto reglamentarios, el Departamento Administrativo de la Función Pública y el Ministerio de las TIC, como, Habeas DATA, Propiedad

Intelectual, Seguridad Digital, Servicios Ciudadanos Digitales, Participación Democrática, Transparencia, Acceso a la Información Pública y Anticorrupción, entre otros.

En la tabla 1, se muestra el Normograma alusivo a la Seguridad y Privacidad de la Información de Metro Cali S.A. en el contexto del Sistema MIO.

Tabla 1. Normograma de Seguridad y Privacidad de la Información de Metro Cali S.A.

Normograma Seguridad y Privacidad de la Información de Metro Cali S.A.	
NORMA	DESCRIPCIÓN
Ley 23 de 1982	Ley de Propiedad Intelectual - Derechos de Autor
Carta Magna de Colombia	Constitución Política de Colombia 1991.
Ley 80 de 1993 y Decretos reglamentarios	Por la cual se expide el Estatuto General de Contratación de la Administración Pública
Ley 87 de 1993	Por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
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.
Directiva presidencial 02 del año 2000	Presidencia de la República de Colombia, Gobierno en línea.
Ley 594 de 2000	Ley General de Archivos.
Decreto 599 de 2000	Código Penal Colombiano
Ley 734 de 2002	Código Disciplinario Único.
Ley 906 de 2004	Código de Procedimiento Penal.
Decreto 1599 de 2005	Por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
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.

Normograma Seguridad y Privacidad de la Información de Metro Cali S.A.	
NORMA	DESCRIPCIÓN
Ley 1150 de 2007 y Decretos reglamentarios	Por medio de la cual se introducen medidas para la eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos.
Ley Estatutaria 1266 de 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 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC–, se crea la Agencia Nacional de Espectro 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"
Decreto 235 de 2010	Intercambio de información entre entidades para el cumplimiento de funciones públicas.
Ley 1437 de 2011	Código de procedimiento administrativo y de lo contencioso administrativo.
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 1474 de 2011	Fortalece los mecanismos **de** prevención, investigación y sanción **de** actos **de** corrupción y la efectividad del control **de** la gestión pública.
Ley 1581 de 2012	"Protección de Datos personales".
Decreto 2609 de 2012	Por la cual se reglamenta la ley 594 de 2000 y ley 1437 de 2011

Normograma Seguridad y Privacidad de la Información de Metro Cali S.A.	
NORMA	DESCRIPCIÓN
Decreto 032 de 2013	Crea una comisión intersectorial que se denominará "Comisión Nacional Digital y de Información Estatal", cuyo objeto será la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para la interacción con los ciudadanos y el uso efectivo de la información en el Estado Colombiano.
Decreto 1377 de 2013	Por la cual se reglamenta la ley 1581 de 2012
Ley 1712 de 2014	De transparencia y del derecho de acceso a la información pública nacional.
Decreto 886 de 2014	Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos.
Decreto 2573 de 2014	Establece los componentes GEL
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”
Ley 1755 de 2015	Reglamenta el derecho de petición
Ley 1757 de 2015	Por la cual se dictan disposiciones en materia de promoción y protección del derecho a la participación democrática.
Decreto 415 de 2016	Fortalecimiento institucional con TIC
Conpes 3854 de abril 11 de 2016	Política Nacional de Seguridad Digital del Estado Colombiano
Resolución 5111 de 2017, Comisión de Regulación de Comunicaciones	Por la cual se establece el régimen de protección de los derechos de los usuarios de servicios de comunicaciones, se modifica el capítulo 1 del título II de la Resolución CRC 5050 de 2016 y se dictan otras disposiciones.
Decreto 1413 de 2017	Por el cual se adiciona el Título 17 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el Capítulo IV del Título III de la Ley 1437 de 2011 y el

Normograma Seguridad y Privacidad de la Información de Metro Cali S.A.	
NORMA	DESCRIPCIÓN
	artículo 45 de la Ley 1753 de 2015, estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.
Decreto 1299 de 2018	Por medio del cual se modifica el Decreto 1083 de 2015, Único Reglamentario del Sector Función Pública, en lo relacionado con la integración del Consejo para la Gestión y Desempeño Institucional y la incorporación de la política pública para la Mejora Normativa a las políticas de Gestión y Desempeño Institucional.
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.
Directiva Presidencia 2 de Abril de 2019	Simplificación de la interacción digital entre los Ciudadanos y el Estado
Ley 1955 del 25 de mayo de 2019	“Por el cual se expide el Plan Nacional de Desarrollo 2018 – 2022. “Pacto por Colombia, Pacto por la Equidad”.
Ley 1978 del 25 de Julio de 2019 - “Ley de las TIC”	“Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencia, se crea un regulador único y se dictan otras disposiciones”.

6. RESPONSABILIDAD Y AUTORIDAD

El desarrollo y actualización del presente plan está bajo la autoridad de la Dirección o área responsable del proceso de Gestión Tecnológica, o quién haga sus veces dentro del contexto de las Tecnologías de la Información y las Comunicaciones que establezca oficialmente Metro Cali S.A. para tal finalidad, o quién lo reemplace o sustituya. Actualmente es la Oficina de Sistemas quien podrá editar el contenido de cada una de las secciones que lo conforman.

7. DEFINICIONES

Las definiciones se retoman del Modelo de Seguridad y Privacidad de la información del Estado colombiano – "MSPI", capitulo "Glosario", que puede ser consultado en el enlace:

https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf – ir a 5

De igual forma, es preciso resaltar las definiciones que se retoman del modelo de gestión de riesgos de seguridad digital del Estado Colombiano – "MGRSD" en consecuencia con los estándares internacionales ISO 31000:2018 e ISO 31010, la Guía ISO/CEI 73 Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas, y otros, como se relaciona a continuación

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).

Actitud hacia el riesgo: Enfoque de la organización para evaluar y eventualmente buscar, retener, tomar o alejarse del riesgo. (NTC ISO 31000:2011).

Activo: Se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo. (CONPES 3854:2016, pág.56).

Activo cibernético: En relación con la privacidad de la información, se refiere al activo que contiene información que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Amenaza: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización. (ISO 2700:2016).

Amenaza cibernética: Aparición de una situación potencial o actual donde un agente tiene la capacidad de generar una agresión cibernética contra la población, el territorio y la organización política del Estado. (CONPES 3854).

Análisis del riesgo: Proceso sistemático para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (NTC ISO 31000:2011).

Apetito de riesgo: Es el máximo nivel de riesgo que los accionistas están dispuestos a aceptar. (Componente COSO ERM II)

Ataque cibernético: Acción organizada y premeditada de una o más personas para causar daño o problemas a un sistema informático a través del ciberespacio. (Ministerio de Defensa de Colombia).

CCOC: Comando Conjunto Cibernético, grupo de ciberseguridad y ciberdefensa creado por el Ministerio de Defensa para apoyar todos los aspectos relacionados con seguridad cibernética en conjunto con el CCP y el Grupo de Respuestas a Emergencias Cibernéticas de Colombia ColCERT.

CERT: Computer Emergency Response Team (Equipo de respuesta a emergencias cibernéticas). (Universidad Carnegie-Mellón).

Cibercrímen (Delito cibernético): Conjunto de actividades ilegales asociadas con el uso de las tecnologías de la información y las comunicaciones, como fin o como medio. (CONPES 3854, pág. 87).

Ciberdefensa: Es el empleo de las capacidades militares ante amenazas cibernéticas, ataques cibernéticos o ante actos hostiles de naturaleza cibernética que afecten la sociedad, la soberanía nacional, la independencia, la integridad territorial, el orden constitucional y los intereses nacionales. (CONPES 3854, pág. 88).

Ciberseguridad: Es el conjunto de recursos, políticas, conceptos de seguridad, salvaguardas de seguridad, directrices, métodos de gestión del riesgo, acciones, investigación y desarrollo, formación, prácticas idóneas, seguros y tecnologías que pueden utilizarse buscando la disponibilidad, integridad, autenticación, confidencialidad y no repudio, con el fin de proteger a los usuarios y los activos de la organización en el ciberespacio. (CONPES 3854, pág. 87).

Ciberterrorismo: Es el uso del ciberespacio, como fin o como medio, con el propósito de generar terror o miedo generalizado en la población, nación o Estado trayendo como consecuencia una violación a la voluntad de las personas. (CONPES 3854, pág. 88).

Ciberdelincuencia: Acciones ilícitas que son cometidas mediante la utilización de un bien o servicio informático. (Ministerio de Defensa de Colombia).

Ciberdelito/Delito cibernético: Actividad delictiva o abusiva relacionada con los ordenadores y las redes de comunicaciones, bien porque se utilice el ordenador como herramienta del delito, bien porque sea el sistema informático (o sus datos) el objetivo del delito. (Ministerio de Defensa de Colombia).

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).

Cibernética: Ciencia o disciplina que estudia los mecanismos automáticos de comunicación y de control o técnica de funcionamiento de las conexiones de los seres vivos y de las máquinas. (Diccionario de la lengua española).

Cibernético: Adjetivo masculino y femenino para denominar todo cuanto tiene relación con la cibernética: órgano cibernético, proceso cibernético o que está especializado en cibernética, así como también a la persona que se dedica a ella. (Diccionario de la lengua española).

Convergencia: Evolución coordinada de redes que antes eran independientes hacia una uniformidad que permita el soporte común de servicios y aplicaciones. (Rec. UIT-T Q.1761, 3.1).

CSIRT: Por su sigla en inglés: Computer Security Incident Response Team (Equipo de respuesta a incidentes de seguridad cibernética). (http:// www.first.org).

Comunicación y consulta: Procesos continuos y reiterativos que una organización lleva a cabo para suministrar, compartir u obtener información e involucrarse en un diálogo con las partes involucradas con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Consulta: La consulta es un proceso de doble vía de la comunicación informada entre una organización y sus partes involucradas, acerca de algún tema, antes de tomar una decisión o determinar una dirección para dicho tema. La consulta es: un proceso que tiene impacto en la decisión a través de la influencia más que del poder; y: una entrada para la toma de decisiones, no para la toma conjunta de decisiones. (NTC ISO 31000 definición 2.12.).

Compartir el riesgo: Compartir con otra de las partes el peso de la pérdida o el beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Conocimiento, capacidades y empoderamiento: Las múltiples partes interesadas deben entender los riesgos de seguridad digital. Deben ser conscientes de que el riesgo de seguridad

digital puede afectar el logro de sus objetivos económicos y sociales, y el de otros. Deben estar educados al respecto, poseer las habilidades necesarias para entender el riesgo, administrarlo y evaluar su impacto. (CONPES 3854, pág. 25).

Consecuencia: Resultado o impacto de un evento que afecta a los objetivos. (NTC ISO 31000:2011).

Contexto externo: Ambiente externo en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Contexto interno: Ambiente interno en el cual la organización busca alcanzar sus objetivos. (NTC ISO 31000:2011).

Control: Medida que modifica al riesgo. (NTC ISO 31000:2011), medios para gestionar el riesgo e incluye políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

Cooperación: Las múltiples partes interesadas deben cooperar, incluso más allá de sus fronteras, a nivel regional e internacional.

Criterios del riesgo: Términos de referencia frente a los cuales se evalúa la importancia de un riesgo. (NTC ISO 31000:2011).

Derechos humanos y valores fundamentales: Las múltiples partes interesadas deben gestionar los riesgos de seguridad digital de manera transparente y compatible con los derechos humanos y los valores fundamentales. La implementación de la gestión de riesgos de seguridad digital debe ser compatible con la libertad de expresión, el libre flujo de la información, la confidencialidad de la información, la protección de la privacidad y los datos personales. Las organizaciones deben tener una política general de transparencia acerca de sus prácticas y procedimientos para la gestión de riesgos de seguridad digital.

Entorno digital: Ambiente, tanto físico como virtual, sobre el cual se soporta la economía digital. Siendo esta última la economía basada en tecnologías, cuyo desarrollo y despliegue se produce en un ecosistema caracterizado por la creciente y acelerada convergencia entre diversas tecnologías, que se concreta en redes de comunicación, equipos de hardware, servicios de procesamiento y tecnologías web. (CONPES 3854, pág. 87).

Entorno digital abierto: En el que no se restringe el flujo de tecnologías, de comunicaciones o de información, y en el que se asegura la provisión de los servicios esenciales para los ciudadanos y para operar la infraestructura crítica. (CONPES 3854, pág. 87).

Establecimiento del contexto: Definición de los parámetros internos y externos que se han de tomar en consideración cuando se gestiona el riesgo y establecimiento del alcance y los criterios del riesgo para la política para la gestión del riesgo. (NTC ISO 31000:2011).

Evaluación del control: Revisión sistemática de los procesos para garantizar que los controles son adecuados y eficaces. (NTC ISO 31000:2011).

Evaluación del riesgo: Proceso de comparación de los resultados del análisis del riesgo, con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables. (NTC ISO 31000:2011).

Evento de seguridad de la información: Ocurrencia que indica una posible brecha de seguridad de la información o falla de los controles. (ISO/IEC 27035:2016).

Evitar el riesgo: Decisión de no involucrarse o de retirarse de una situación de riesgo. (NTC ISO 31000:2011).

Evento: Presencia o cambio de un conjunto particular de circunstancias. (NTC ISO 31000:2011).

Fuente de riesgo: Elemento que solo o en combinación tiene el potencial intrínseco de originar un riesgo. (NTC ISO 31000:2011).

Frecuencia: Medición del número de ocurrencias por unidad de tiempo. (NTC ISO 31000:2011).

Gestión del riesgo: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo. (NTC ISO 31000:2011).

Gestión de riesgos de seguridad digital: Es el conjunto de actividades coordinadas dentro de una organización o entre organizaciones para abordar el riesgo de seguridad digital, mientras se maximizan oportunidades. Es una parte integral de la toma de decisiones y de un marco de trabajo integral para gestionar el riesgo de las actividades económicas y sociales. Se basa en un conjunto flexible y sistemático de procesos cíclicos lo más transparente y lo más explícito posible. Este conjunto de procesos ayuda a asegurar que las medidas de gestión de riesgos de seguridad digital (medidas de seguridad) sean apropiadas para el riesgo y los objetivos económicos y sociales en juego. (CONPES 3854, pág. 24).

ICC: Es la denominación de lo que el CCOC ha definido como infraestructuras críticas cibernéticas en el ámbito colombiano.

Identificación del riesgo: Proceso para encontrar, reconocer y describir el riesgo. (NTC ISO 31000:2011).

Incidente digital: Evento intencionado o no intencionado que puede cambiar el curso esperado de una actividad en el medio digital y que genera impactos sobre los objetivos. (CONPES 3854, pág. 87).

Incidente de seguridad de la información: Uno o múltiples eventos de seguridad de la información relacionados e identificados que pueden dañar los activos de información de la organización o comprometer sus operaciones. (ISO/IEC 27035:2016).

Infraestructura crítica cibernética nacional: Aquella soportada por las TIC y por las tecnologías de operación, cuyo funcionamiento es indispensable para la prestación de servicios esenciales para los ciudadanos y para el Estado. Su afectación, suspensión o destrucción puede generar consecuencias negativas en el bienestar económico de los ciudadanos o en el eficaz funcionamiento de las organizaciones e instituciones, así como de la administración pública. (CONPES 3854, pág. 29).

Inventario de activos: Sigla en inglés: Assets inventory. Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, intangibles, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten, por tanto, ser protegidos de potenciales riesgos (ISO 27000.ES).

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización, cuyo objetivo es establecer, promocionar y gestionar estándares. (http://www.iso.org).

Marco de referencia para la gestión del riesgo: Conjunto de componentes que brindan las bases y las disposiciones de la organización para diseñar, implementar, monitorear, revisar y mejorar continuamente la gestión del riesgo, a través de toda la organización. (NTC ISO 31000:2011).

Monitoreo: Verificación, supervisión, observación crítica o determinación continúa del Estado con el fin de identificar cambios con respecto al nivel de desempeño exigido o esperado. (NTC ISO 31000:2011).

Múltiples partes interesadas: El Gobierno nacional y los territoriales, las organizaciones públicas y privadas, la fuerza pública, los propietarios u operadores de las infraestructuras críticas cibernéticas nacionales, la academia y la sociedad civil, quienes dependen del entorno digital para todas o algunas de sus actividades, económicas y sociales, y quienes pueden ejercer distintos roles y tener distintas responsabilidades. (CONPES 3854, pág. 29).

Nivel de riesgo: Magnitud de un riesgo o de una combinación de riesgos expresada en términos de la combinación de las consecuencias y su probabilidad. (NTC ISO 31000:2011).

Organización: Grupo de personas e instalaciones con distribución de responsabilidades, autoridades y relaciones. (NTC ISO 31000:2011).

Parte involucrada: Persona u organización que puede afectar, verse afectada o percibirse a sí misma como afectada, por una decisión o una actividad. (NTC ISO 31000:2011).

Peligro: Una fuente de daño potencial. (NTC ISO 31000:2011).

Pérdida: Cualquier consecuencia negativa o efecto adverso, financiero u otro. (NTC ISO 31000:2011).

Perfil del riesgo: Descripción de cualquier conjunto de riesgos. (NTC ISO 31000:2011).

Política: Intenciones y dirección de una organización como las expresa formalmente su alta dirección. (ISO/IEC 27000:2016).

Política para la gestión del riesgo: Declaración de la dirección y las intenciones generales de una organización con respecto a la gestión del riesgo. (NTC ISO 31000:2011).

Posibilidad: Se utiliza como descripción general de la probabilidad o la frecuencia. (NTC ISO 31000:2011).

Plan para la gestión del riesgo: Esquema dentro del marco de referencia para la gestión del riesgo que especifica el enfoque, los componentes y los recursos de la gestión que se van a aplicar a la gestión del riesgo. (NTC ISO 31000:2011).

Probabilidad: Oportunidad de que algo suceda. (NTC ISO 31000:2011).

Proceso para la gestión del riesgo: Aplicación sistemática de las políticas, los procedimientos y las prácticas de gestión a las actividades de comunicación, consulta, establecimiento del contexto, y de identificación, análisis, evaluación, tratamiento, monitoreo y revisión del riesgo. (NTC ISO 31000:2011).

Propietario del riesgo: Persona o entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo. (ISO GUIA 73:2009).

Responsabilidad: Las múltiples partes interesadas deben asumir la responsabilidad de la gestión del riesgo de seguridad digital. Deben rendir cuentas sobre la base de sus funciones y su capacidad para actuar, teniendo en cuenta el posible impacto de sus decisiones sobre los demás. Deben también reconocer que un cierto nivel de riesgo de seguridad digital tiene que ser aceptado para lograr los objetivos económicos y sociales. (CONPES 3854, pág. 25).

Revisión: Acción que se emprende para determinar la idoneidad, conveniencia y eficacia de la materia en cuestión para lograr los objetivos establecidos. (NTC ISO 31000:2011).

Reducción del riesgo: Acciones que se toman para disminuir la posibilidad, las consecuencias negativas o ambas, asociadas con un riesgo. (NTC ISO 31000:2011).

Resiliencia: Es la capacidad de un material, mecanismo o sistema para recuperar su estado inicial cuando ha cesado la perturbación a la que había estado sometido. (CONPES 3854, pág. 87).

Retención del riesgo: Aceptación del peso de la pérdida o del beneficio de la ganancia proveniente de un riesgo particular. (NTC ISO 31000:2011).

Riesgo: Efecto de la incertidumbre sobre los objetivos. (NTC ISO 31000:2011).

Riesgo inherente: Es aquel al que se enfrenta una entidad en ausencia de acciones de la dirección para modificar su probabilidad o impacto. (NTC ISO 31000:2011).

Riesgo residual: Remanente después del tratamiento del riesgo. (NTC ISO 31000:2011).

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no repudio y confiabilidad pueden estar involucradas. (ISO/IEC 27001:2016).

Seguridad digital: Es la situación de normalidad y de tranquilidad en el entorno digital (ciberespacio), derivada de la realización de los fines esenciales del Estado mediante (i) la gestión del riesgo de seguridad digital; (ii) la implementación efectiva de medidas de ciberseguridad; y (iii) el uso efectivo de las capacidades de ciberdefensa; que demanda la voluntad social y política de las múltiples partes interesadas y de los ciudadanos del país. (CONPES 3854, pág. 29).

Servicios esenciales: Los necesarios para el mantenimiento de las funciones sociales básicas, la salud, la seguridad, el bienestar social y económico de los ciudadanos, o el eficaz funcionamiento de las instituciones del Estado y las administraciones públicas (Tomado del documento ICC del CCOC).

SGC: Sistema de gestión de calidad.

SGSI: Sistema de gestión de seguridad de la información.

Sistema para la gestión del riesgo: Conjunto de elementos del sistema de gestión de una organización involucrados en la gestión del riesgo. (NTC ISO 31000:2011).

Telecomunicaciones: Toda transmisión y recepción de signos, señales, escritos, imágenes y sonidos, datos o información de cualquier naturaleza por hilo, radiofrecuencia, medios ópticos u otros sistemas electromagnéticos. (Resolución MinTIC 202 de 2010).

TI: Tecnologías de la información.

TO: Tecnología de operación

TIC (Tecnologías de la información y las comunicaciones): Conjunto de recursos, herramientas, equipos, programas informáticos aplicaciones, redes y medios que permiten la compilación, procesamiento, almacenamiento, transmisión de información como voz, datos, texto, video e imágenes. (Ley 1341/2009 TIC).

Tratamiento del riesgo: Proceso para modificar el riesgo. (ISO/IEC Guía 73:2009).

Valoración del riesgo: Proceso global de identificación del riesgo, análisis del riesgo y evaluación del riesgo. (ISO GUÍA 73:2009).

Vulnerabilidad: Es una debilidad, atributo o falta de control que permitiría o facilitaría la actuación de una amenaza contra información clasificada, los servicios y recursos que la soportan. (CONPES 3854, pág. 87).

8. DESARROLLO

8.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

8.1.1 DIAGNÓSTICO

La situación actual en el 2020, referente al Tratamiento de Riesgos de Seguridad y Privacidad de la Información en Metro Cali S.A. se analizó teniendo en cuenta los resultados obtenidos con la gestión de la Entidad frente a la mejora producida frente a los riesgos de seguridad digital, y a la evolución de la estrategia para la definición e implementación del sistema de Gestión de seguridad y privacidad de la información contenida en el Plan de Seguridad y Privacidad de la Información de la Entidad (Ver documento “Plan de Seguridad y Privacidad de la Información – PSPI - 2019-2022 versión 1.0 – Seguimiento 2020”, en relación con el contexto de la Entidad que resultan necesarios y compatibles con las necesidades institucionales.

Este análisis permite evolucionar frente a la línea base obtenida del diagnóstico de 2019 para proyectar el presente Plan, de tal forma, que inicialmente procure por fortalecer la capacidad institucional identificada y se posibiliten las condiciones para el desarrollo e implementación de los habilitadores transversales de la información y seguridad de la información, como mecanismos y/o elementos fundamentales o necesarios que conforman la columna vertebral de la Seguridad de la Información en la Entidad y para la gestión y gobierno de los proyectos, seguimiento de riesgos y controles para lograr los objetivos propuestos en el Plan de Seguridad de la Información en Metro Cali S.A.

El diagnóstico contempló verificaciones en las fuentes de información del proceso “Gestión Tecnológica” en el SIGEM[3] de Metro Cali S.A. y su relación con los distintos procesos de la empresa para la entrega de valor, así como los avances del 2019. Se mantiene consulta a los expertos que forman parte de la Entidad y memoria institucional, y a los tomadores de

[3] *SIGEM es, Sistema de Información Gerencial de Metro Cali S.A. en Plataforma Web que permite realizar la gestión de calidad de Metro Cali S.A.*

decisiones de la Entidad y a los colaboradores de TI, cuyo enfoque especifico comprende a los dominios de información, sistemas de información y uso y apropiación de TI. Lo anterior, con el propósito de mantener bajo observación la percepción de la Gestión de la Seguridad de la Información de la Entidad y/o la Oficina de Sistemas y el tratamiento de riesgos en seguridad y privacidad de la información respectiva.

El resultado del diagnóstico contenido en el Plan de Seguridad y Privacidad de la Información se obtiene según la herramienta facilitada por MinTic, y se resume en los siguientes acápites: (i) Estructura funcional para el tratamiento de riesgos de seguridad y privacidad de la información; (ii) Alcance del proceso de Gestión Tecnológica Actual; (iii) Capacidad Organizacional de la Oficina de Sistemas Actual; (iv) Recursos.

8.1.2 ESTRUCTURA FUNCIONAL PARA EL TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Durante el año 2019 se avanzó en cerrar brechas frente a restricciones y limitaciones de capacidad, el reto es avanzar hacia el fortalecimiento institucional con una división del trabajo en Metro Cali S.A. para el tratamiento de riesgos de seguridad digital que permitan satisfacer las necesidades actuales de la Entidad para el Gobierno y Gestión de un sistema de Gestión de Seguridad de la Información, y su consecuente gestión y tratamiento de riesgos de Seguridad y Privacidad de la Información. Lo anterior con la finalidad de mayor certidumbre y confianza ciudadana frente al desarrollo, evolución y operación de la entidad en el contexto misional requerido en el SITM-MIO. Como se hace alusión en el “PETI 2019-2022 versión 2.0 – Seguimiento 2020” y en el “PSPI-MC 2019-2022 – Seguimiento 2020” de Metro Cali S.A. que se aluden en el presente documento.

El tratamiento de riesgos en este componente específico se ha cubierto de manera remedial por parte de los Líderes de proceso, para lo cual se ha avanzado con el establecimiento de la Política la administración de riesgos de gestión, corrupción y seguridad digital. No obstante, la implementación de la Política se procede de manera progresiva, manteniendo los principios de gradualidad y capacidad institucional conforme con la normatividad actual, la cual delimita su tratamiento específico que pretende ser cubierto en el presente plan.

8.1.3 ALCANCE DEL PROCESO DE GESTIÓN TECNOLÓGICA ACTUAL

Al revisar el objetivo, caracterización, proceso actual y procedimientos del proceso de Gestión Tecnológica frente al propósito de la Entidad y su correlación con las líneas estratégicas, objetivos estratégicos, programas y proyectos, el reto es producir la correlación del proceso de TI actual con el mapa de procesos que cubra las necesidades de la Entidad y valide institucionalmente la gestión tecnológica desde el proceso establecido con cubrimiento de los distintos dominios de la Arquitectura empresarial. Para ello es preciso avanzar con el entendimiento estratégico facilitando y manteniendo coherencia con el contexto de la entidad y su plataforma estratégica. Actualmente el proceso de Gestión Tecnológica se encuentra en el mapa de procesos a cargo de la Oficina de Sistemas, el reto es lograr cubrimiento de los distintos dominios de TI, como: Implementación de la Estrategia de TI, Gobierno de TI, Información, Sistemas de Información, Infraestructura tecnológica (Servicios Tecnológicos), y, Uso y Apropiación, que satisfaga las necesidades de la Entidad en el contexto del servicio de transporte público con el Sistema MIO en cumplimiento de la normatividad vigente.

De igual manera, se procurar la consistencia necesaria entre el objetivo del proceso y la denominación en las etapas referidas para el ciclo PHVA, frente al alcance sobre el cual está supeditado dicho proceso.

8.1.4 CAPACIDAD ORGANIZACIONAL DE LA OFICINA DE SISTEMAS ACTUAL

Frente a los requisitos de Gestión Tecnológica y las Políticas del sistema de Gestión Pública definido por el Estado Colombiano, Metro Cali S.A. ha establecido mediante el PETI, las acciones conducentes al fortalecimiento institucional, de manera progresiva y gradual.

Actualmente se cuenta solo con el jefe de sistemas y un profesional de apoyo técnico, únicos que están en la estructura permanente de cargos de la empresa, y con personal contratista por prestación de servicios netamente para soporte de sistemas, cubriendo algunas acciones de la gestión, con un rumbo recursivo frente a las necesidades del negocio y de las partes interesadas.

Aunque se cuenta con el Plan Estratégico Institucional, el reto es darle alcance y articulación con la arquitectura empresarial exigida por el Estado colombiano, como también cubrir el requisito de

fortalecer la estructura de organización de TI con el equipo humano mínimo y necesario, que soporte las actividades resultantes de la definición e implementación de los Planes de Seguridad y Privacidad y de tratamiento de riesgos de seguridad y privacidad de la información.

8.1.5 RECURSOS

La Oficina de Sistemas cuenta con recursos específicos para la operación actual de soporte de sistemas en la Entidad. El Tratamiento de riesgos tecnológicos se ha supeditado de forma recurrente a la incorporación de procedimientos e implementación de acciones o proyectos de mejora de infraestructura tecnológica que demanda la necesidad de la Entidad.

Los recursos aforados se han establecido en el rubro de “Gastos Generales” para atender necesidades específicas. El reto comprende dar alcance a la seguridad y privacidad de la información de la Entidad. Lo anterior, para el cumplimiento de la legislación y fines de protección de la privacidad de la información.

8.2 METODOLOGÍA DEL PLAN

Metro Cali S.A. con el Plan de Seguridad y Privacidad de la Información incluye en su metodología de gestión de riesgos, las opciones de evitar, reducir, asumir y compartir o transferir para el tratamiento de los riesgos de seguridad y privacidad de la información, y seguridad digital.

El presente Plan se desarrolla sobre la base de la definición de la fase de Planeación del Sistema de Gestión de Seguridad y Privacidad de la Información que establezca la entidad.

Con la planeación del Sistema de Gestión de Seguridad y Privacidad de la Información se dinamiza y materializa la definición, establecimiento y operación del Plan de tratamiento, y con los resultados obtenidos, se procede a desarrollar sistemática y estratégicamente la madurez de la Entidad frente al tratamiento de riesgos respectivo, para lo cual, la “Declaración de

Aplicabilidad - SOA[4]", se constituye en la base sobre la cual, en la mesa técnica de Gobierno Digital y Seguridad Digital se priorizaran los proyectos para el prevalecimiento de la seguridad y privacidad de la información y seguridad digital, como sean aprobados y apalancados por parte de la Alta Dirección.

Los componentes del Sistema de gestión de seguridad y privacidad de la información – SGSPI complementan el ciclo PHVA con la implementación de controles, así como el seguimiento y evaluación de los mismos mediante la gestión e implementación de los proyectos priorizados resultantes de la "Declaración de Aplicabilidad" del citado sistema, que se define como estrategia del citado Plan de seguridad y Privacidad de la Información y el avance desarrollado en 2019.

El tratamiento del riesgo involucra la selección de una o más opciones identificadas en cada uno de los procesos y subprocesos, y priorizados a través de la mesa técnica de la Política de Gobierno Digital y Seguridad Digital gestionada por el Líder del presente Plan, en consideración de la capacidad y/o mejora tecnológica a implementar, lo que permitirá modificar los riesgos y la implementación priorizada de tales opciones. Por tanto, la gestión de riesgos y la madurez del Sistema de gestión es intrínseco a Metro Cali S.A. por medio del liderazgo, la cultura, la integración con los procesos y la implicación de los servidores públicos, contratistas y empleados de las empresas adscritas al Sistema MIO.

Con la implementación del Sistema de Seguridad y Privacidad de la información, bajo los principios de proporcionalidad y gradualidad, tendrá lugar la aplicación del presente Plan, el cual se producirá de manera progresiva en consideración a las guías y modelos del Estado Colombiano, como son: la Guía de Administración del riesgo y diseño de controles en Entidades Públicas, riesgos de gestión, corrupción y seguridad digital, en su versión más actualizada, y consecuentemente, la implementación del modelo de Gestión de riesgo de seguridad digital – MGRSD de conformidad con el Modelo Nacional de Gestión de Riesgos de Seguridad Digital del Gobierno de Colombia. No obstante, que, desde el contexto de la Oficina de Sistemas actual, se

[4] Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

implemente de manera paralela y complementaria el Sistema de administración de riesgos de gestión, corrupción y seguridad digital obedeciendo a la dinámica actual de la Entidad.

La tabla 2. Opciones para el tratamiento de riesgos, permite observar la caracterización de cada opción para el tratamiento de riesgos de seguridad y privacidad de la información en el contexto del presente Plan.

Tabla 2. Opciones para el tratamiento de riesgos

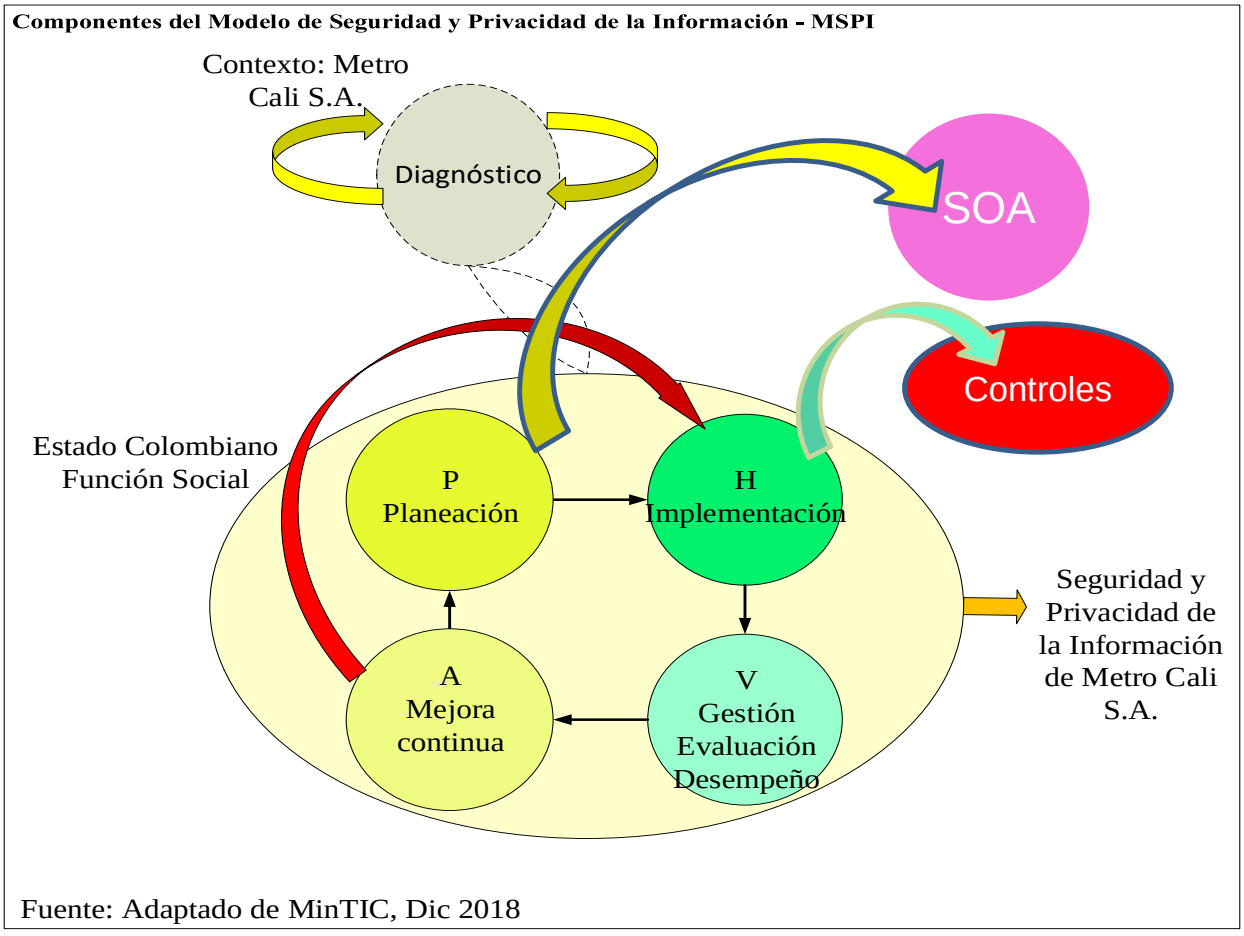
Opciones para el tratamiento de riesgos	
Evitar el riesgo	Conlleva a tomar medidas encaminadas a prevenir su materialización. Es siempre la primera alternativa a seguir, se logra cuando al interior de los procesos se genera cambios sustanciales para mejoramiento, rediseño o eliminación, resultado de unos adecuados controles y acciones emprendidas.
Reducir el riesgo	Conlleva a tomar medidas encaminadas a disminuir, tanto la probabilidad, como el impacto, a través de la optimización de los procedimientos y la implementación de controles eficientes, eficaces y efectivos,
Compartir y transferir el riesgo	Conlleva a reducir su efecto a través del traspaso de posibles impactos a otras organizaciones, o a través de otros medios que permitan distribuir el riesgo o parte de el con otra, u otras empresas involucradas o, a involucrar con Metro Cali S.A. Por ejemplo: (i) El caso de Garantías por Seguros; (ii) Empresa anexa al servicio de transporte público con mayor control del componente, y/o que por su naturaleza, o actividad en el sistema MIO tiene mayor acceso o control del proceso o activo.
Asumir el riesgo	Es la última alternativa a considerar. Puede ocurrir después que el efecto del riesgo haya sido reducido o transferido (Probabilidad o impacto) quedando un riesgo residual, que a consideración del Comité de Seguridad de la información pueda ser aceptado y asumido por la Metro Cali S.A.

En síntesis, la evolución de la Entidad en el tratamiento de riesgos articulado con los modelos del Estado Colombiano alcanzará su mayor efecto, con el tratamiento de riesgos de seguridad y privacidad de la información con su ciclo PHVA de conformidad con los Planes respectivos, según la metodología de gestión de riesgos del Estado Colombiano definido por el DAFP, y el Modelo establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones –

MinTIC como se refiere en la normatividad en concordancia con la norma ISO 27001, ISO 27002 e ISO 31000 y COSO (Para efectos de articulación con el Sistema de Control interno).

El tratamiento de riesgos se genera de manera periódica mediante la revisión continúa y mejora de los controles con la verificación de los riesgos y el seguimiento a los riesgos, su evolución y los resultados de los controles procediendo a ser calificados al revisar y evaluar su nivel de incidencia en la mitigación o materialización producida. Ante ello, se procede nuevamente a generarse el ciclo PHVA, que permita identificar desde el contexto, si el riesgo residual o nuevo se ubica en una zona de riesgo que requiera tratamiento en función de las cuatro opciones de tratamiento de riesgos. La aplicación e implementación de las fases del ciclo de operación PHVA del Sistema de Gestión de Seguridad y Privacidad de la Información se relacionan en la figura 1.

Figura 1. Ciclo del Sistema de Seguridad y Privacidad de la Información – SGSPI



Fuente: Adaptado de MinTIC, Dic 2018

8.3 LÍNEAS ESTRATÉGICAS DEL PLAN

Las líneas de acción frente a los planes que se implementen para fines de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se pueden observar en la tabla 3.

Tabla 3. Líneas Estratégicas del Plan

Líneas Estratégicas del Plan
1. Integrado en todas las actividades
2. Estructurado
3. Adaptado a la organización
4. Inclusivo de todas las partes interesadas.
5. Dinámico y con respuesta a cambios
6. Basado en la mejor información disponible
7. Considera factores humanos y culturales
8.Enfocado a la mejora continua

8.4 ACTIVIDADES DEL PLAN

Las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información prevista 2019 – 2022 se mantienen para el año 2020, las cuales se resumen en la tabla 4 que se relaciona a continuación:

Tabla 4. Actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Fase	Meta	Período del Plan	Responsable	Corresponsable
Fase I – Diagnóstico	1.Determinar el estado actual de la gestión de tratamiento de riesgos de seguridad y privacidad de la información al interior de la Entidad.	2019 - 2022	1. Oficina de sistemas 2. Dirección de Planeación 3. Líderes de Proceso y Subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño

Fase	Meta	Período del Plan	Responsable	Corresponsable
				5. Oficina de Control interno
	2. Determinar el nivel de madurez de los controles de seguridad de la información.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	3. Identificar el avance y desarrollo del Plan de Seguridad y Privacidad de la Información	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	4. Verificar el cumplimiento de la legislación vigente	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno

Fase	Meta	Período del Plan	Responsable	Corresponsable
	5. Verificar el uso de buenas prácticas en ciberseguridad.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
Fase 2 – Planificación	1. Revisión, ajuste y/o validación de la Política de Seguridad y Privacidad de la Información	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	2. Verificación de Procedimientos de seguridad y privacidad de la información, y su cumplimiento.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	3. Verificación la definición de Roles y	2019 - 2022	1. Oficina de sistemas	1. Presidencia 2. Directivos

Fase	Meta	Período del Plan	Responsable	Corresponsable
	responsabilidades de seguridad y privacidad de la información, y su cumplimiento		2. Todos los líderes de proceso y subproceso	3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	4. Verificar la gestión de inventario de activos de información.	2019 - 2022	1. Todos los líderes de proceso y subproceso 2. Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	5. Verificar la integración del MSPI con el Sistema de Gestión documental	2019 - 2022	1. Oficina de sistemas 2. Secretaría General y Asuntos Jurídicos 3. Dirección Financiera y Administrativa	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	6. Verificar la aplicación de la metodología para la Gestión del riesgo de las normas aludidas y	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital

Fase	Meta	Período del Plan	Responsable	Corresponsable
	establecimiento de la "Declaración de Aplicabilidad"		proceso y subproceso	4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	7. Verificar el apalancamiento e implementación del Plan de Comunicaciones en todos los niveles de la organización.	2019 - 2022	1. Oficina de sistemas 2. Oficina de Gestión Humana 3. Dirección Financiera y Administrativa	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	8. Verificar el desarrollo y evolución del Plan de diagnóstico de IPv4 a IPv6.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
Fase 3 – Implementación	1. Verificar la Planificación y Control Operacional del Sistema de Gestión de Seguridad y Privacidad de la Información.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de

Fase	Meta	Período del Plan	Responsable	Corresponsable
				Gestión y Desempeño 5. Oficina de Control interno
	2. Verificar la implementación proyectos de seguridad y privacidad frente a las acciones críticas, altas, y los resultados obtenidos en la Declaración de Aplicabilidad	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	3. Verificar el seguimiento producido a los Indicadores de Gestión del Plan de Seguridad y Privacidad y a la implementación de controles definidos en la Declaración de Aplicabilidad.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	4. Verificar los resultados del Plan de Transición de IPv4 a IPv6	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño

Fase	Meta	Período del Plan	Responsable	Corresponsable
				5. Oficina de Control interno
Fase 4 – Evaluación Desempeño	1. Análisis de la información de la operación del Plan de revisión y seguimiento, a la implementación del SGSPI.	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
	2. Verificar la implementación de Auditorías y el análisis de la información resultados de Auditorias	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno
Fase 5 –Mejora Continua	1. Verificar y controlar que se ejecute el Plan de mejora continua	2019 - 2022	1. Oficina de sistemas 2. Todos los líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno

8.5 RECURSOS DEL PLAN

Está comprendido por los recursos requeridos y aforados que han presupuestado para conformidad en el desarrollo del PETI, el PSPI y el PTR-SPI-MC articulado con la gestión y los recursos asignados por parte de todos los Líderes de proceso y subproceso durante las vigencias 2020, 2021 y 2022. Su evolución está circunscrita a la capacidad de la entidad y a los recursos que se dispongan para los años 2020, 2021 y 2022. Para el 2020 se generan las acciones y recursos de conformidad con la capacidad actual de la Oficina de Sistemas:

8.5.1 RECURSO HUMANO:

- Profesionales especializados y expertos en tecnologías de la información y las comunicaciones del área responsable de la Gestión Tecnológica de Metro Cali S.A., o quién haga sus veces. Para el 2020, comprendidos en la Oficina de Sistemas,
- Los líderes de proceso,
- Líder del sistema de Gestión de Seguridad y Privacidad de la Información de la Entidad
- Líder de Seguridad y Privacidad de la Información
- Líder de control interno.

8.5.2 RECURSO FÍSICO:

- Edificaciones e Instalaciones de la Entidad
- Edificaciones e Instalaciones del Sistema MIO
- Edificaciones e Instalaciones de los Concesionarios, que comprenden infraestructura del Sistema MIO.
- Desarrollo e implementación del Sistema de Gestión de seguridad y privacidad de la información de Metro Cali S.A.
- Documento que contemple la definición de las acciones prioritarias para el tratamiento de riesgos, según la evaluación, Crítico o Alta, y resultados del Sistema de Gestión de Seguridad y Privacidad de la Información.
- Documento que comprende la “Declaración de Aplicabilidad – SOA”

8.5.3 RECURSO TECNOLÓGICO:

- Infraestructura tecnológica, controles de acceso físico.

8.6 RESPONSABILIDAD

- La Alta Dirección de la Entidad
- La Dirección de tecnologías de la información y las comunicaciones de la Entidad, o quién haga sus veces, actualmente la Oficina de Sistemas
- Líderes de proceso.
- Profesional Especializado del Sistema de Gestión de Seguridad y privacidad de la información
- Profesional Especializado en seguridad informática del cual disponga la Entidad
- Profesional Especializado de la Gestión de Proyectos de TI
- Oficina de Control Interno

8.7 PROYECCIÓN DE PRESUPUESTO DE LA OFICINA DE SISTEMAS

Tal como se ha descrito en la situación actual, la Oficina de Sistemas tiene asignado un presupuesto para la vigencia 2020 para los requerimientos de operación primaria en el contexto actual, y su ejecución presupuestal es monitoreada de manera periódica de acuerdo con el Plan Anual de Compras.

Metro Cali S.A. revisará periódicamente la proyección presupuestal correspondiente al presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, para dar cubrimiento en la presente o siguientes vigencias, de conformidad con sus ingresos, proyección de ingreso, definición de prioridades estratégicas y definición de las acciones prioritarias para el tratamiento de riesgos por parte de la Entidad.

8.8 PROYECTOS Y ACTIVIDADES DEL PLAN TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dentro del ejercicio de arquitectura empresarial que adelante Metro Cali S.A., se ha concebido la definición de la Arquitectura de TI incorporado en el PETI versión 2.0 – Seguimiento 2020 aludido, y, con ello, la Arquitectura de Información como principal habilitador para el alcance y definición de un Sistema de Gestión de Seguridad de la Información. El presente Plan toma como

referencia los avances en la ejecución del Sistema de Gestión de Seguridad y Privacidad de la Información que se adopte e implemente por la Entidad, para ser ejecutado de manera paralela y progresiva, con aplicación de los proyectos asociados con los controles que resulten prioritarios.

Para la presente vigencia 2020, el tratamiento de riesgos avanzará con los proyectos en avance, y remedialmente de conformidad con los recursos disponibles asignados a la oficina de sistemas actual consecuente con el contexto y alcance del proceso actual. Los demás componentes se implementan progresivamente en la medida que se produzca la asignación de recursos para el año 2020, 2021 y 2022.

Por consiguiente, los proyectos y actividades citados, infieren una ejecución progresiva para Metro Cali S.A., desde el alcance y avance en el desarrollo e implementación de la estrategia con el SGSPI[5], en pro de avanzar en el desarrollo y madurez en las distintas fases y componentes del modelo de manera segura, hasta su culminación y mejora continua, que también será progresiva.

La Tabla 5 siguiente, continúa de conformidad con los avances del 2019, para lo cual se relacionan los proyectos y actividades que se han presentado para implementar con mayor prioridad en la vigencia de 2020 para el tratamiento de riesgos de seguridad y privacidad de la información y los que actualmente vienen en ejecución. Para las siguientes vigencias, 2021 y 2022, se avanzará en la medida del avance de la implementación del sistema de Gestión de Seguridad y Privacidad de la Información. No obstante, el desarrollo de los mismos será supeditado a la priorización que defina la entidad y al apalancamiento respectivo.

Tabla 5. Proyectos y Actividades Tratamiento de Riesgos de Seguridad y Privacidad de la Información

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
TR-SPI-01	Seguimiento y revisión a la definición e implementación	1. Oficina de sistemas	1. Presidencia 2. Directivos	2020 - 2022

[5] SGSPI es, Sistema de Gestión de Seguridad y Privacidad de la información de conformidad con el Modelo de Seguridad y Privacidad de la Información del Estado Colombiano – MSPI definido por el Ministerio de las Tecnologías de la información y las Comunicaciones de Colombina, MINTIC.

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
	de la Arquitectura Empresarial de la Entidad	2. Dirección de Planeación 3. Líderes de Proceso y Subproceso	3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	
TR-SPI - 02	Seguimiento y revisión a la definición e implementación de la Arquitectura de TI de la Entidad	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 03	Seguimiento y revisión a la definición e implementación de la Arquitectura de información de la Entidad	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 04	Seguimiento y revisión a la definición e implementación del Plan de Tecnologías de la Información y las comunicaciones de la Entidad (PETI)	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 – 2022
TR-SPI 05	Seguimiento y revisión a la definición e implementación del Plan de Seguridad y Privacidad de la información de la Entidad	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño	2020 - 2022

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
			5. Oficina de Control interno	
TR-SPI 06	Seguimiento a la definición e implementación del Sistema de Gestión de Seguridad de la Información de Metro Cali S.A.	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 07	Revisar y verificar la definición e implementación del Plan de Comunicaciones del Plan de Seguridad y Privacidad de la Información de Metro Cali S.A.	1. Oficina de sistemas 2. Oficina de Gestión Humana 3. Dirección Financiera y Administrativa	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 08	Seguimiento a la Operación del Sistema de Gestión de Seguridad de la Información de Metro Cali S.A.	1. Oficina de sistemas 2. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 09	Asistir a las reuniones de trabajo del MPIG V2 y definir reuniones con cada líder de proceso y subproceso	1. Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
TR-SPI 10	Seguimiento a la operación de la nueva infraestructura de TI adquirida	Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 11	Seguimiento a la mejora de la infraestructura de TI	Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 12	Mantenimiento de las redes e infraestructura de TI (switches y topología)	Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 13	Seguimiento a los planes de acción específicos por vigencia del Tratamiento de Riesgo de Seguridad y Privacidad de la Información	1. Líderes de proceso y subproceso 2. Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 14	Identificación de los riesgos de proceso y subproceso	1. Líderes de proceso y subproceso	1. Presidencia 2. Oficina de Sistemas 3. Directivos	2020 - 2022

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
			4. Mesa Técnica de Gobierno Digital 5. Comité Institucional de Gestión y Desempeño 6. Oficina de Control interno	
TR-SPI 15	Valoración del riesgo residual.	Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 16	Realizar Mapas de calor donde se ubican los riesgos.	Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 17	Socialización del plan de tratamiento de riesgo aprobado por los líderes.	1. Oficina de sistemas 2. Oficina de Gestión Humana 3. Líderes de proceso y subproceso	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital 4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	2020 - 2022
TR-SPI 18	Monitoreo y control.	Oficina de sistemas	1. Presidencia 2. Directivos 3. Mesa Técnica de Gobierno Digital	2020 - 2022

ID	Proyecto / Actividad	Responsable	Co-Responsable	Fecha
			4. Comité Institucional de Gestión y Desempeño 5. Oficina de Control interno	

8.9. PLAN PROYECTO DE INVERSIÓN

Los proyectos a ejecutar para todo el componente de TI de la empresa (según el alcance del proceso de TI y capacidad actual de la Oficina de Sistemas) para la vigencia 2020 y siguientes, contemplan la continuidad de las iniciativas en marcha y la incorporación de nuevos proyectos necesarios para cumplir con todos los requisitos y necesidades de la Entidad, desde su capacidad y alcance actual en la entidad, los distintos planes de TI y el Plan de Tratamiento de riesgos de Seguridad y Privacidad de la Información definido en el presente documento.

Los costos de operación (en la Entidad se conoce como Gastos Generales) y funcionamiento de la Oficina de Sistemas para la vigencia 2020 publicado por Metro Cali S.A. y que fueron contemplados en el Plan Estratégico de TI (PETI), como se resume en la siguiente tabla 6.

Tabla 6. Presupuesto de funcionamiento aprobado para la Oficina de Sistemas año 2019

Objeto de Gasto	Presupuesto 2020 presentado	Presupuesto 2020 publicado
Funcionamiento y fortalecimiento institucional	$2.852.132.131,36	$716.410.350,0
Infraestructura		
Servicios externos		
Total Asignado	$716.410.350,0	
Nota tomada del presupuesto presentado por la Oficina de Sistemas: (ii) El Item "FORTALECIMIENTO INSTITUCIONAL DEL ÁREA DE TI" incorpora las necesidades mínimas de operación frente a los distintos dominios de TI y las necesidades de implementación del PETI (Plan Estratégico de Tecnologías de la Información y las Comunicaciones) en su componente de habilitadores de Gobierno digital, política transversal del MIPG v2.		

8.10 PLAN DE COMUNICACIONES

El Plan de comunicaciones para el Tratamiento de riesgos de Seguridad y Privacidad de la Información de Metro Cali S.A. está contemplado en el documento del Plan de Seguridad y Privacidad de la Información para la vigencia 2019 – 2022, versión 2.0, enero de 2020, de conformidad con la Estrategia de Uso y apropiación que defina en conjunto con la oficina de Gestión Humana de la Entidad, una vez aprobado por el Jefe de la Oficina de Sistemas y publicado en el sitio web de Metro Cali S.A., enlace: www.metrocali.gov.co

Para la presente vigencia 2020, manteniendo los principios de gradualidad y proporcionalidad, avanzará remedialmente y progresivamente de conformidad con los recursos disponibles asignados a la oficina de sistemas actual, y los demás componentes del Plan de Comunicaciones, se implementan progresivamente en la medida que se produzca la asignación de recursos para el año 2020, 2021 y 2022.

8.11 REFERENCIAS

- Ministerio de Tecnologías de la Información, Arquitectura TI Colombia, Modelo de Seguridad y Privacidad de la información – MSPI, consultado diciembre de 2018.

  https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

- Guía de Administración del riesgo y diseño de controles en Entidades Públicas, riesgos de gestión, corrupción y seguridad digital, Versión 4, 2018, Departamento Administrativo de la Función Pública
- Modelo de Gestión de riesgo de seguridad digital, documento: Modelo Nacional de Gestión de Riesgos de Seguridad Digital, Gobierno de Colombia, 2017.

9. ANEXOS

No aplica.

10. OBSERVACIONES

— La persona que apoyó metodológicamente en la gestión del documento fue:

Marlene Jenifer Hollaender Profesional Contratista de la Dirección de Planeación

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

Juan José Muriel Agudelo	Jefe de Oficina de Sistemas
Uriel Ramírez Márquez	Profesional Especializado Evaluación de la Operación Adscrito a la Oficina de Sistemas

Elaborado por:  Uriel de Jesús Ramírez Márquez	Cargo: Profesional Especializado Evaluación de la Operación Adscrito a la Oficina de Sistemas
Revisado y Aprobado por:  Juan José Muriel Agudelo	Cargo: Jefe de Oficina de Sistemas