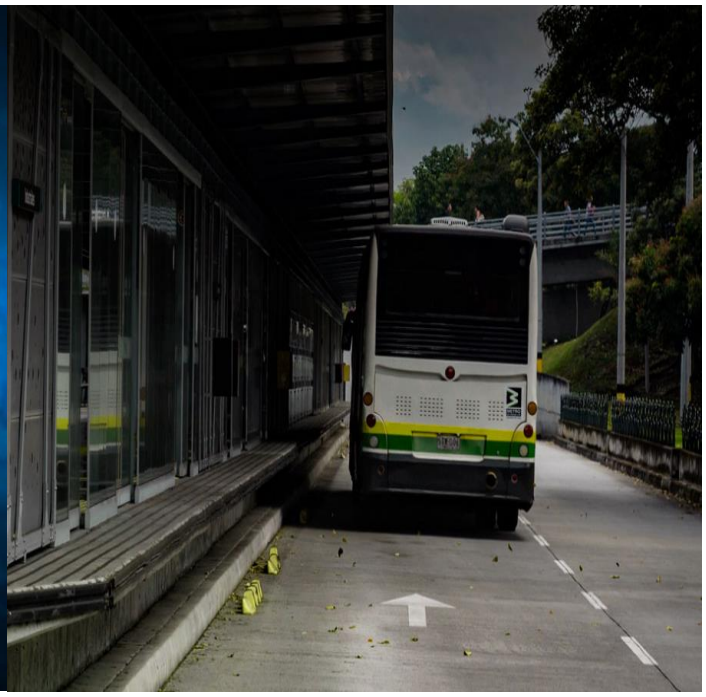
PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION VIGENCIA 2020 – 2023



1. INTRODUCCION

En el ámbito del propósito de la empresa Metroplús S.A., del Sistema de Transporte Masivo de Pasajeros -SIT- de mediana capacidad, en el Valle de Aburra y su respectiva área de influencia, Metroplús S.A. ha iniciado acciones para la definición e implementación de los habilitadores transversales, como Arquitectura Empresarial, Arquitectura de TI, lo cual involucra, la definición, estructura y operación de una arquitectura de información, en el cual, la gestión de la información infiere a la necesidad de mecanismos, estrategias y herramientas para la gestión 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, Metroplús S.A. ha establecido planes de mediano plazo, como el PETI y el Plan de Seguridad y Privacidad de la Información en un período de cuatro (4) años (2020-2023), 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.

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 proceder a 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 da lineamientos sencillos y claros para su adecuada gestión.

El tratamiento del riesgo involucra la selección de una o más opciones para modificar los riesgos y la implementación de tales opciones y la gestión de riesgos es intrínseco a Metroplús S.A., por medio del liderazgo, la cultura, la integración con los procesos y la implicación de los servidores públicos, contratistas y empleados de la entidad.

Una vez implementado, el Sistema de Gestión de riesgos, el tratamiento suministra controles o los modifica"[1]. De las opciones de tratamiento sugeridas por la norma ISO 31000:2018, Metroplús S.A. ha incluido 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.

2. OBJETIVOS

2.1. Objetivo General

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

2.2. Objetivos Específicos

- Alinear los objetivos de cada proceso y subproceso en torno a la Política de seguridad y privacidad de la información de Metroplús 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 cuyo alcance está delimitado por la capacidad institucional del proceso actual de gestión tecnológica y del área

[1] Icontec 2011

actualmente responsable, Oficina de sistemas, 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 Metroplús 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 Metroplús 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[2] e ISO[3] respectivamente en seguridad y riesgo de la información, para Metroplús 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.

[2] Departamento Administrativo de la Función Pública de Colombia
[3] International Organization for Standardization, que en español traduce, Organización Internacional de Normalización

3. ALCANCE

El presente Plan concibe una frontera de aplicación de cuatro años entre el 2020 al 2023. Inicia con la definición y establecimiento, por parte del Gerente y la Alta Dirección, de la "Declaración de Aplicabilidad – SOA", 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 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 del Sistema de Transporte Masivo de Pasajeros -SIT- de mediana capacidad, en el Valle de Aburra y su respectiva área de influencia. Tiene aplicación con los resultados de la operación de los componentes y habilitadores transversales; 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 Metroplús 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 (antes Estrategia de Gobierno en Línea – GEL), lineamientos, legislación, normas, guías y marcos de referencia definidos por el DAFP e ISO 27001, ISO 27002 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.

Para su mantenimiento y mejora continua cada vez que Metroplús S.A. realice un ejercicio o proyecto de Arquitectura Empresarial, Arquitectura de información, y/o gestión de riesgos, su resultado debe ser integrado al PTR-SPI-MC.

4. NORMATIVIDAD

La normatividad en el cual se enmarca el Plan Tratamiento de Riesgos de Seguridad y Privacidad de la Información de Metroplús 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 Metroplús S.A. en el contexto del Sistema SIT.

Tabla No. 1. Normograma de Seguridad y Privacidad de la Información de Metroplús S.A

Normograma de Seguridad y Privacidad de la Información de Metroplús S.A	
NORMA	**DESCRIPCION**
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 sus 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 de 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 2000	Código Disciplinario Único.
Ley 906 de 2004	Código de Procedimiento Penal

Decreto 1599 de 2002	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.
Ley 1150 de 2007 y sus 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.
Decreto 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.
Campes 3701 de 2011	Lineamientos de política para Ciberseguridad y Ciberdefensa
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
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
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 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.

5. RESPONSABILIDAD Y AUTORIDAD

El desarrollo y actualización del presente plan está bajo la autoridad de la Dirección Administrativa, responsable del proceso de Gestión de Tecnologías de la Información, o quién haga sus veces dentro del contexto de las Tecnologías de la Información y las

Comunicaciones que establezca oficialmente Metroplús S.A. para tal finalidad, o quién lo reemplace o sustituya.

6. DEFINICIONES

Las definiciones se retoman de la norma ISO 31000:2018 e ISO 31010, y se complementan de la Guía ISO/CEI 73 Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas, en el capítulo 3. “Términos y definiciones”. La Guía puede ser consultada: https://mybmt.org/wp-content/uploads/2017/10/Cap-1-8-2-a-6-Guia_ISO-IEC-73.pdf

7. DESARROLLO

7.1. Análisis de la Situación Actual

7.1.1. Diagnostico

La situación actual referente al Tratamiento de Riesgos de Seguridad y Privacidad de la Información en Metroplús S.A. se analizó teniendo los resultados obtenidos para la gestión de la 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-MC – 2020 – 2023 versión 1.0”, en relación con el contexto de la Entidad que resultan necesarios y compatibles con las necesidades institucionales.

Este análisis permite contar con una línea base para proyectar el presente Plan, de tal forma, que inicialmente procure por identificar la capacidad institucional 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 Metroplús S.A.

El diagnóstico realizado contempla verificaciones en las fuentes de información del proceso “Gestión de Tecnologías de la Información de Metroplús S.A. y su relación con los distintos procesos de la empresa para la entrega de valor. Se procedió a la consulta de los expertos que forman parte de la Entidad y memoria institucional, y se consideraron las encuestas a los tomadores de decisiones de la Entidad y a los colaboradores de TI, cuyo enfoque específico comprende a los dominios de información, sistemas de información y uso y apropiación de TI. Lo anterior, con el propósito de conocer la percepción de la Gestión de la Seguridad de la Información de Entidad y/o la Dirección Administrativa, por intermedio de la Profesional Universitaria Gestión TIC y Servicios Administrativos 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 de Tecnologías de la Información Actual; (iii) Capacidad Organizacional de la Oficina de Sistemas Actual; (iv) Recursos.

7.1.2. Estructura Funcional para el Tratamiento de Riesgos de Seguridad y Privacidad de la Información

No se cuenta con una división del trabajo en Metroplús S.A., ni en la Oficina de Sistemas 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 que permita ejercer las funciones que el SIT requiere. Como se hace alusión en el “PETI 2019 versión 1.0 de 2019” y en el “PSPI-MC 2020-2023” de Metroplús S.A. que se aluden en el presente documento.

El tratamiento de riesgos en este componente específico no se ha realizado de manera estructurada o formalizada en la Entidad, sin embargo, se ha cubierto de manera previsiva y recursiva por parte de los Líderes de proceso, durante la gestión de riesgos de gestión y la Gestión de Riesgos de Corrupción. No obstante, la normatividad actual delimita su tratamiento específico que pretende ser cubierto en el presente plan.

7.1.3. Alcance del Sistema de Gestión de Seguridad de la Información Actual

Al revisar el objetivo, caracterización, proceso actual y procedimientos del proceso de Gestión de Seguridad de la Información, frente al propósito de la Entidad y su correlación con las líneas estratégicas, objetivos estratégicos, programas y proyectos, se encuentra que no existe 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. Tampoco se observa coherencia en el contexto estratégico, al no estar inmerso en una posición estratégica en el mapa.

7.1.4. Capacidad Organizacional de la Dirección Administrativa en lo que concierne a las Tecnologías de la Información

Se cuenta solo con el contrato de soporte de TI, con un tecnólogo de apoyo técnico, quien esta permanente en la empresa; además se cuenta con una Profesional Universitaria Gestión TIC y servicios Administrativos, quien tiene a su cargo el proceso de Gestión tecnológico. Aunque se cuenta con el Plan Estratégico Institucional, no se tiene alcance a la arquitectura empresarial exigida por el Estado colombiano.

Como también se observa en la estructura de organización de TI con una estructura y un equipo humano mínimo y necesario, personal que cubre algunas acciones de la gestión, con un rumbo recursivo frente a las necesidades del negocio y de las partes interesadas.

7.1.5. Recursos

La Dirección Administrativa no ha contado con recursos específicos para la definición, diseño, implementación, gestión y operación de un sistema de Gestión de Seguridad de la Información.

El Tratamiento de riesgos tecnológicos se ha tratado de manera recursiva, con implementación de acciones o proyectos de infraestructura tecnológica que demanda la necesidad recurrente.

Los recursos aforados se han establecido en el rubro de "Gastos Generales" y han sido concebidos de manera limitada para atender necesidades específicas, sin que tenga alcance para la seguridad y privacidad de la información de la Entidad, lo anterior, de conformidad con la definición y caracterización del proceso de Gestión Tecnológica actual de la Entidad, y para el cumplimiento de la legislación para fines de protección de datos personales.

7.2. Metodología del Plan

Comprende los componentes del modelo de seguridad y privacidad de la información – MSPI, completando el ciclo mediante el seguimiento y control a la gestión de los proyectos resultantes de la "Declaración de Aplicabilidad" del citado modelo, como se define en el citado Plan de seguridad y Privacidad de la Información. Por lo anterior, el tratamiento de riesgos de seguridad de la información, con su ciclo PHVA, considera la metodología de gestión de riesgos del Estado Colombiano definido por el DAFP y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC a través de los Decretos y Guías, y también procede en concordancia con la norma ISO 27001, ISO 27002 e ISO 31000 y COSO (Para efectos del sistema de Control interno).

El MSPI se dinamiza y materializa con la definición, establecimiento y operación del Sistema de Gestión de Seguridad y Privacidad de la Información, y con los resultados obtenidos, se procede a desarrollar sistemática y estratégicamente el tratamiento de riesgos respectivo, es decir, cuando se haya producido el establecimiento de la "Declaración de Aplicabilidad - SOA[4] " y los proyectos para el prevalecimiento de la

[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).

seguridad y privacidad de la información, aprobados y apalancados por parte de la Alta Gerencia.

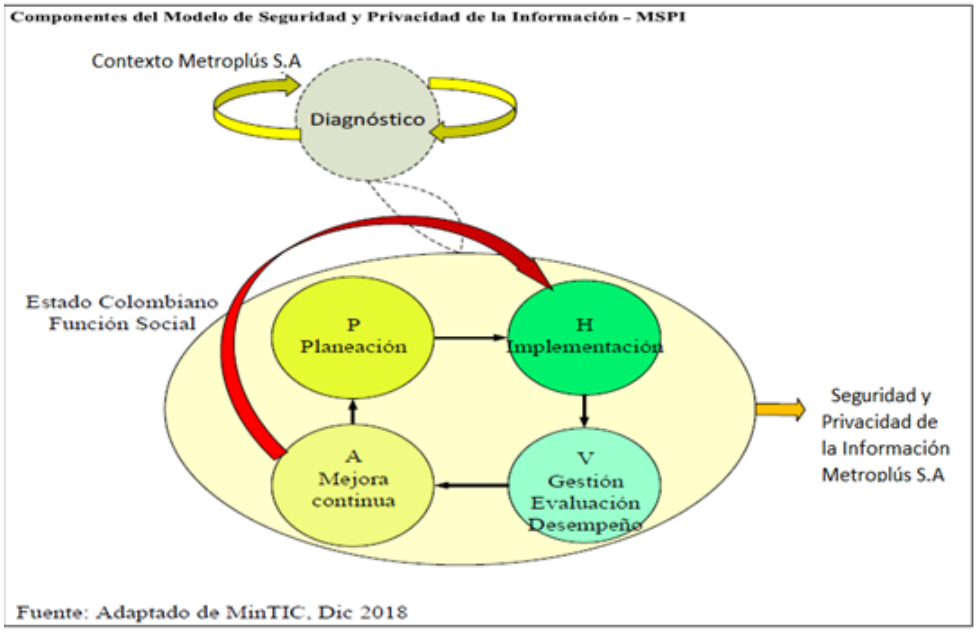
La tabla 2. Opciones para el tratamiento de riesgos, permite observar la caracterización de cada opción para el tratamiento de riesgos de seguridad y privacidad de la información en el contexto del presente Plan.

Tabla No. 2. Opciones para el Tratamiento de Riesgos

OPCIONES DE 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 Metroplús 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 SIT 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 Metroplús S.A.

Las fases del ciclo de operación del ciclo PHVA del MSIP se relacionan en la figura 1. Componentes del Modelo de Seguridad y Privacidad de la Información – MSPI.

Figura No. 1. Componentes del Modelo de Seguridad y Privacidad de la Información - MSPI



7.3. 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 No. 3. Líneas Estratégicas del Plan

LINEAS ESTRATEGICAS 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

7.4. Actividades del Plan

Las actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información se resumen en la tabla 4 que será aplicado por Metroplús S.A. se relacionan a continuación:

Tabla No. 4. Líneas Estratégicas del Plan

FASE	META	PERIODO DEL PLAN	RESPONSABLE	CORRESPONSABLE
Fase 1. Diagnostico	Determinar el estado actual de la gestión de tratamiento de riesgos de seguridad y privacidad de la información al interior de la Entidad.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Determinar el nivel de madurez de los controles de seguridad de la información.	2020 – 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Identificar el avance y desarrollo del Plan de Seguridad y Privacidad de la Información.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno

	Verificar el cumplimiento de la legislación vigente	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar el uso de buenas prácticas en ciberseguridad.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
Fase 2 Planificación	Revisión, ajuste y/o validación de la Política de Seguridad y Privacidad de la Información	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificación de Procedimientos de seguridad y privacidad de la información, y su cumplimiento.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificación la definición de Roles y responsabilidades de seguridad y privacidad de la información, y su cumplimiento	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar la gestión de inventario de activos de información	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar la integración		Dirección Administrativa –	Gerencia – Secretaría General –Dirección Administrativa –

	del MSPI con el Sistema de Gestión Documental	2020 - 2023	Todos los líderes del proceso	Coordinación de Control Interno
	Verificar la aplicación de la metodología para la Gestión del riesgo de las normas aludidas y establecimiento de la “Declaración de Aplicabilidad”	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar el apalancamiento e implementación del Plan de Comunicaciones en todos los niveles de la organización.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar el desarrollo y evolución del Plan de diagnóstico de IPv4 a IPv6.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar la Planificación y Control Operacional del Sistema de Gestión de Seguridad y Privacidad de la Información	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar la implementación proyectos de seguridad y			

	privacidad frente a las acciones críticas, altas, y los resultados obtenidos en la Declaración de Aplicabilidad	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
Fase 3 Implementación	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.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar los resultados del Plan de Transición de IPv4 a IPv6	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
Fase 4 Evaluación del Desempeño	Análisis de la información de la operación del Plan de revisión y seguimiento, a la implementación del MSPI.	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno
	Verificar la implementación de Auditorías y el análisis de la información resultados de Auditorias	2020 - 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno

Fase 5 Mejora Continua	Verificar y controlar que se ejecute el Plan de mejora continua	2020 – 2023	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno

7.5. Recursos del Plan

7.5.1. Recurso Humano

- Profesionales en tecnologías de la información y las comunicaciones del área responsable de la Gestión Tecnológica de Metroplús S.A., o quién haga sus veces. Para el 2020,
- Los líderes de proceso,
- Coordinador de control interno.

7.5.2. Recurso Físico

- Edificaciones e Instalaciones de la Entidad (arrendadas)

7.5.3. Recurso Tecnológico

- Infraestructura Tecnológica

7.6. Responsabilidad

- La alta Dirección de la Entidad
- La Dirección Administrativa de la Entidad y su sector de Gestión TIC, o quién haga sus veces, actualmente la Profesional Universitaria Gestión TIC y Servicios Administrativos.
- Líderes de proceso

7.7. Proyección de Presupuesto para TICS en la Dirección Administrativa

Tal como se describe en la situación actual, la Dirección Administrativa para el tema de TICs tiene asignado un presupuesto para la vigencia 2020, cuya ejecución presupuestal es monitoreada de manera periódica de acuerdo con el Plan Anual de Adquisiciones.

7.8. Proyectos y Actividades del Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información

Dentro del ejercicio de arquitectura empresarial que adelante Metroplús S.A., se ha concebido la definición de la Arquitectura de TI incorporado en el PETI versión 1.0 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 Plan de Seguridad y Privacidad de la Información, específicamente lo alusivo al desarrollo e implementación del Sistema de Gestión de Seguridad de la Información prevista en el Plan respectivo, 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 Dirección Administrativa para lo referente a la Tecnología de la Información consecuente con el contexto y alcance del proceso actual. Los demás componentes se implementaran progresivamente en la medida que se produzca la asignación de recursos para el año 2021, 2022 y 2023. Por consiguiente, los proyectos y actividades citados, infieren una ejecución progresiva para Metroplús S.A., desde el alcance actual y el avance en el desarrollo e implementación del MSPI[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, relaciona los proyectos y actividades que serán abordados 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, 2022 y 2023 se avanzarán en la medida del avance de la

[5] Modelo de Seguridad y Privacidad de la información del Estado Colombiano definido por el Ministerio de las Tecnologías de la información y las Comunicaciones de Colombina, MINTIC

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 No. 5. Proyectos y Actividades Tratamiento de Riesgos de Seguridad y Privacidad de la Información

PROYECTO/ACTIVIDAD	RESPONSABLE	CORRESPONSABLE	FECHA
Seguimiento y revisión a la definición e implementación de la Arquitectura Empresarial de la Entidad	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Seguimiento y revisión a la definición e implementación de la Arquitectura de TI de la Entidad	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Seguimiento y revisión a la definición e implementación de la Arquitectura de información de la Entidad	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Seguimiento y revisión a la definición e implementación del Plan de Tecnologías de la Información y las comunicaciones de la Entidad (PETI)	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Seguimiento y revisión a la definición e implementación del Plan de Seguridad y Privacidad de la Información de la entidad	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
Seguimiento a la definición e			

implementación del Sistema de Gestión de Seguridad de la Información de Metroplús S.A.	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Revisar y verificar la definición e implementación del Plan de Comunicaciones del Plan de Seguridad y Privacidad de la Información de Metroplús S.A	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Seguimiento a la Operación del Sistema de Gestión de Seguridad de la Información de Metroplús S.A.	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
Asistir a las reuniones de trabajo del MPIG V2 y definir reuniones con cada líder de proceso y subproceso	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
Ejecución de Proyecto de Infraestructura tecnológica	Dirección Administrativa – Todos los líderes del proceso	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
Identificación de los riesgos con los líderes de procesos	Dirección Administrativa	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
Valoración del riesgo residual.	Dirección Administrativa	Gerencia – Secretaría General –Dirección Administrativa –	2020 - 2023

		Coordinación de Control Interno	
Socialización del plan de tratamiento de riesgo aprobado por los líderes.	Dirección Administrativa	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 – 2023
Monitoreo y control	Dirección Administrativa	Gerencia – Secretaría General –Dirección Administrativa – Coordinación de Control Interno	2020 - 2023

7.9. 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 Dirección Administrativa, en lo referente a la tecnología de la información) 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 Dirección Administrativa en lo referente a la tecnología de la información para la vigencia 2020 aprobado por el presupuesto anual de Metroplús S.A. y que fueron contemplados en el Plan Estratégico de TI (PETI).

7.10. Plan de Comunicaciones

El Plan de comunicaciones para el Tratamiento de riesgos de Seguridad y Privacidad de la Información de Metroplús S.A. está contemplado en el documento del Plan de Seguridad y Privacidad de la Información para la vigencia 2020 – 2023, versión 1, de conformidad con la Estrategia de Uso y apropiación que defina en conjunto con la oficina de Talento Humano de la Entidad, una vez aprobado por el Director Administrativo y publicado en el sitio web de Metroplús S.A. www.metroplus.gov.co Para la presente vigencia 2020, se avanzará remedialmente de conformidad con los recursos disponibles

asignados a Dirección Administrativa en lo referente a la tecnología de Información actual, y los demás componentes del Plan de Comunicaciones se implementaran progresivamente en la medida que se produzca la asignación de recursos para el año 2021, 2022 y 2023.

8. 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

Ministerio de Tecnologías de la Información, Arquitectura TI Colombia, Guía N° 14. Plan de Capacitación, Sensibilización y Comunicación de Seguridad de la Información, consultado diciembre de 2018 https://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan_comunicacion_sensibilizacion. pdf - Guía para la administración del riesgo y el diseño de controles en entidades públicas, versión 4, Departamento Administrativo de la función Pública, Octubre de 2018 https://www.google.com.co/search?q=-+Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controle s+en+entidades+p%C3%BAblicas%2C+versi%C3%B3n+4%2C+Departamento+Administrativo +de+la+funci%C3%B3n+P%C3%BAblica%2C+Octubre+de+2018&oq=-+Gu%C3%ADa+para+la+administraci%C3%B3n+del+riesgo+y+el+dise%C3%B1o+de+controle s+en+entidades+p%C3%BAblicas%2C+versi%C3%B3n+4%2C+Departamento+Administrativo +de+la+funci%C3%B3n+P%C3%BAblica%2C+Octubre+de+2018&aqs=chrome..69i57.1222j0j7 &sourceid=chrome&ie=UTF-8 - ISO/IEC 31000:2018 ISO 31000:2018, Risk management -- Guidelines - ISO.IEC 31010:2009 – Risk management – Risk assessment techniques. - ISO/IEC 27001:2013, Information technology - Security techniques - Information security management systems - Requirements - ISO IEC

2702:2013, Information technology — Security techniques — Code of practice for information security controls (second edition) - Guía ISO/CEI 73, Gestión de riesgos – Terminología – Líneas directrices para el uso en las normas: https://mybmt.org/wp-content/uploads/2017/10/Cap-1-8-2-a-6-Guia_ISO-IEC-73.pdf

El documento fue elaborado por

MITSY ALBANY MEJIA MEDINA
Profesional Universitaria Gestión TIC y Servicios Administrativos