



# PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION DE METROPLÚS VIGENCIA 2020 – 2023





## Contenido

<b>1. INTRODUCCION</b> .....	3
<b>2. OBJETIVOS</b> .....	5
2.1. Objetivo General.....	5
2.2. Objetivos Específicos .....	5
<b>3. ALCANCE</b> .....	6
<b>4. NORMATIVIDAD</b> .....	7
<b>5. RESPONSABILIDAD Y AUTORIDAD</b> .....	10
<b>6. DEFINICIONES</b> .....	10
<b>7. DESARROLLO</b> .....	10
7.1. Análisis de la situación actual.....	10
<b>7.1.2. Estructura Funcional de Seguridad y Privacidad de la Información</b> ....	12
<b>7.1.3. Recursos</b> .....	13
7.2. Metodología del Plan .....	13
7.3. Actividades del Plan .....	14
7.4. Recursos del Plan.....	19
<b>7.4.1. Recursos Humanos</b> .....	19
<b>7.4.2. Recursos Físicos</b> .....	19
<b>7.4.3. Recurso Tecnológico</b> .....	19
7.5. Responsabilidad.....	19
7.6. Proyección de Presupuesto para TICS en la Dirección Administrativa .....	19
7.7. Proyectos y Actividades de Seguridad de la Información .....	20
7.8. Plan Proyecto de Inversión .....	22
7.9. Plan de Comunicaciones .....	22
<b>8. REFERENCIAS</b> .....	26



## 1. INTRODUCCION

A través del decreto único reglamentario 1078 de 2015, del sector de Tecnologías de Información y las Comunicaciones, se define el componente de seguridad y privacidad de la información, como parte integral de la Política de Gobierno Digital (antes estrategia Gobierno en Línea-GEL). Forma parte del componente de Seguridad y Privacidad de la Información, acorde con las mejores prácticas de seguridad y estándares internacionales como ISO 27001 e ISO 31000 y COSO.

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, bajo la modalidad de transporte terrestre automotor así como ejercer la titularidad sobre el mismo, buscando promover y beneficiar la prestación de servicio de transporte público masivo, se concibe el Plan de Seguridad y Privacidad de la Información de Metroplús S.A - SIT, en el cual, la gestión de la seguridad propone ser concebidas en el marco de la gestión de la organización determinado por las necesidades, objetivos, los requisitos de seguridad, los procesos misionales, estratégicos y de apoyo, el tamaño y estructura de Metroplús S.A. y su contexto, de manera que resulte acorde con las características y necesidades institucionales para la disponibilidad, confidencialidad e integridad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.

El Modelo de Seguridad y Privacidad de la Información se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Política de Gobierno Digital (antes Estrategia de Gobierno en Línea-GEL): TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión) para efecto de dar cubrimiento a los macro componentes TIC para el Estado y TIC para la Sociedad. El presente modelo pretende facilitar la comprensión del proceso de construcción de una política de privacidad por parte de Metroplús S.A., que permita fijar los criterios que seguirán para proteger la privacidad de la información y los datos, así como de los



procesos y las personas vinculadas con dicha información. Por tal motivo, su desarrollo e implementación se concibe en coherencia y articulación con la Arquitectura de TI.

El presente Plan se concibe para ser actualizado periódicamente; de conformidad con los cambios técnicos de la norma, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información; de otro lado el Plan concibe al MSPI específica, a los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano.

Finalmente, a nivel metodológico se consideran los distintos lineamientos y guías en cada una de las fases del modelo definido por Mintlc para que los destinatarios del mismo tengan claridad de cuáles son los resultados a obtener y como desarrollarlos.

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



## **2. OBJETIVOS**

### **2.1. Objetivo General**

Generar el horizonte de planeación, implementación, seguimiento, evaluación y mejora continua para la seguridad y privacidad de la información de Metroplús S.A. con aplicación de las mejores prácticas en Seguridad y Privacidad para las entidades del Estado, que contribuya al incremento de la transparencia en la gestión pública.

### **2.2. Objetivos Específicos**

- Promover el uso de mejores prácticas de seguridad de la información, para ser la base de aplicación del concepto de Seguridad Digital.
- Identificar infraestructuras críticas en Metroplús S.A. y su contexto para la definición de la aplicación del Modelo de Seguridad y Privacidad de la información.
- Contribuir a mejorar los procesos de intercambio de información pública.
- Orientar a las Áreas de Metroplús S.A. en las mejores prácticas en seguridad y privacidad de la Información.
- Optimizar la gestión de la seguridad de la información al interior de Metroplús S.A.
- Facilitar la transición de IPv4 a IPv6 con la utilización de las guías disponibles para tal fin.
- Mantener aplicación de la legislación relacionada con la protección de datos personales.
- Contribuir en el desarrollo del plan estratégico institucional y la elaboración del plan estratégico de tecnologías de la información y de las comunicaciones.
- Contribuir en el desarrollo del ejercicio de arquitectura empresarial apoyando en el cumplimiento de los lineamientos del marco de referencia de arquitectura empresarial para la gestión de TI del estado colombiano.
- Mantener la política de tratamiento de datos personales respetuosa de los derechos de los titulares.



- Optimizar la labor de acceso a la información pública al interior de las áreas y entidades destinatarias.
- Revisar los roles relacionados con la privacidad y seguridad de la información al interior de la entidad para optimizar su articulación.

### **3. ALCANCE**

El presente Plan fue concebido para una frontera de aplicación de cuatro años entre el 2020 al 2024. Inicia con el apalancamiento de la Gerencia de la Entidad y la Alta Dirección para la definición e implementación de los habilitadores transversales, como, la Arquitectura Empresarial, Arquitectura de TI, Arquitectura de Información, así como la definición e implementación de un 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 establecido por MinTic – MSPI, y, con la Política de Gobierno Digital del Estado Colombiano (antes Estrategia de Gobierno en Línea – GEL).

Comprende el uso de las mejores prácticas y estándares internacionales como ISO 27001 e ISO 31000 y COSO que trata de requisitos para el diagnóstico, planificación, implementación, gestión y evaluación, y, mejoramiento continuo, fases de su modelo de operación y seis (6) niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación.

Tiene aplicación para el cumplimiento de las políticas de seguridad y privacidad de la información, y seguimiento a una adecuada gestión de la información por parte de cada Líder de proceso de la empresa, en el contexto del servicio de Sistema de Transporte Masivo de Pasajeros -SIT- de mediana capacidad, en el Valle de Aburra y su respectiva área de influencia. Comprende para cada Líder de proceso de la Entidad, mantener una adecuada gestión de riesgos de seguridad y privacidad de la información y su seguimiento, y se desarrolla al abordar los pasos metodológicos, lineamientos, guías, herramientas y mejores prácticas para el cubrimiento de brechas de seguridad y privacidad de la información.



La seguridad y privacidad de la información, como componente transversal a la Política de Gobierno Digital (antes Estrategia de Gobierno en línea), permite alinearse al componente de TIC para la Gestión para preservar la confidencialidad, integridad y disponibilidad de la información. Se alinea al componente de TIC para Servicios apoyando el tratamiento de la información utilizada en los trámites y servicios que ofrece Metroplús S.A., y se alinea al componente de TIC para Gobierno Abierto que permite la construcción de un estado más transparente, colaborativo y participativo al garantizar que la información que se provee tenga controles de seguridad y privacidad de tal forma que los ejercicios de interacción de información con el ciudadano, otras entidades y la empresa privada sean confiables.

#### 4. NORMATIVIDAD

La normatividad que cubre el Plan 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 de Transporte Masivo de Pasajeros -SIT- de mediana capacidad.

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

<i>Normograma de Seguridad y Privacidad de la Información de Metroplús S.A</i>	
<b>NORMA</b>	<b>DESCRIPCION</b>
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, 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. Actualmente está a cargo de la Profesional Universitaria Gestión TIC y Servicios Administrativos; quien podrá editar el contenido de cada una de las secciones que lo conforman, previa autorización del Director Administrativo.

## 6. DEFINICIONES

Las definiciones pueden ser consultadas en la sección Glosario del documento “Modelo de Seguridad y Privacidad de la Información” del portal del Ministerio de las Tecnologías de la información y las comunicaciones de Colombia – MINTIC: Para ver el documento, consultar: [https://www.mintic.gov.co/gestioniti/615/articles-5482\\_Modelo\\_de\\_Seguridad\\_Privacidad.pdf-ira5](https://www.mintic.gov.co/gestioniti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf-ira5)  
Glosario

## 7. DESARROLLO

### 7.1. Análisis de la situación actual

#### 7.1.1. Diagnostico



La situación actual referente a la Seguridad y Privacidad de la Información en Metroplús S.A. se analizó teniendo en cuenta la herramienta de diagnóstico de MinTIC1; 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., como ejemplo: La implementación de las estrategias de TI contenidos en el PETI de la Entidad, definición, implementación, seguimiento y evaluación de las Políticas de seguridad de la información en Metroplús S.A., Arquitectura de información comprendida dentro de la Arquitectura de TI y este a su vez dentro del contexto de la arquitectura empresarial y servicios ciudadanos digitales en consonancia con el propósito Estatal, como lo es, el servicio de Transporte Masivo de Pasajeros -SIT- de mediana capacidad, en el Valle de Aburra y su respectiva área de influencia y sus agentes responsables.

El diagnóstico realizado contempla verificaciones en las fuentes de información del proceso “Sistema integral de gestión” 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, 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 con su área de Gestión TIC.

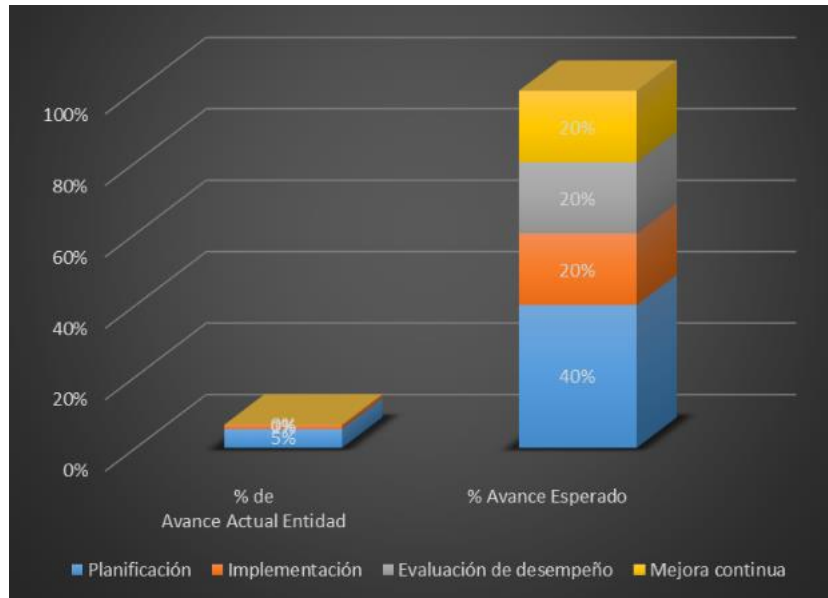
El resultado del diagnóstico, según la herramienta facilitada por MinTic, se resume en la tabla 2 y figura 1. Avance ciclo de funcionamiento del Modelo de Operación (PHVA), como sigue:



Tabla No. 2. Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)

AÑO	AVANCE PHVA		
	COMPONENTE	% AVANCE ACTUAL	% AVANCE ESPERADO
2020	Planificación	5%	40%
2021	Implementación	1%	20%
2022	Evaluación de Desempeño	0%	20%
2023	Mejora Continua	0%	20%
<b>TOTAL</b>		<b>6%</b>	<b>100%</b>

Figura No. 1. Avance Ciclo de Funcionamiento del Modelo de Operación (PHVA)



### 7.1.2. Estructura Funcional 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 que permita ejercer las funciones que el Sistema de Transporte Masivo de Pasajeros -SIT- de mediana capacidad, en el Valle de Aburra y su respectiva área de influencia requiere. Como se hace alusión en el “PETI 2018 versión 1.0 de Metroplús S.A.

### **7.1.3. Recursos**

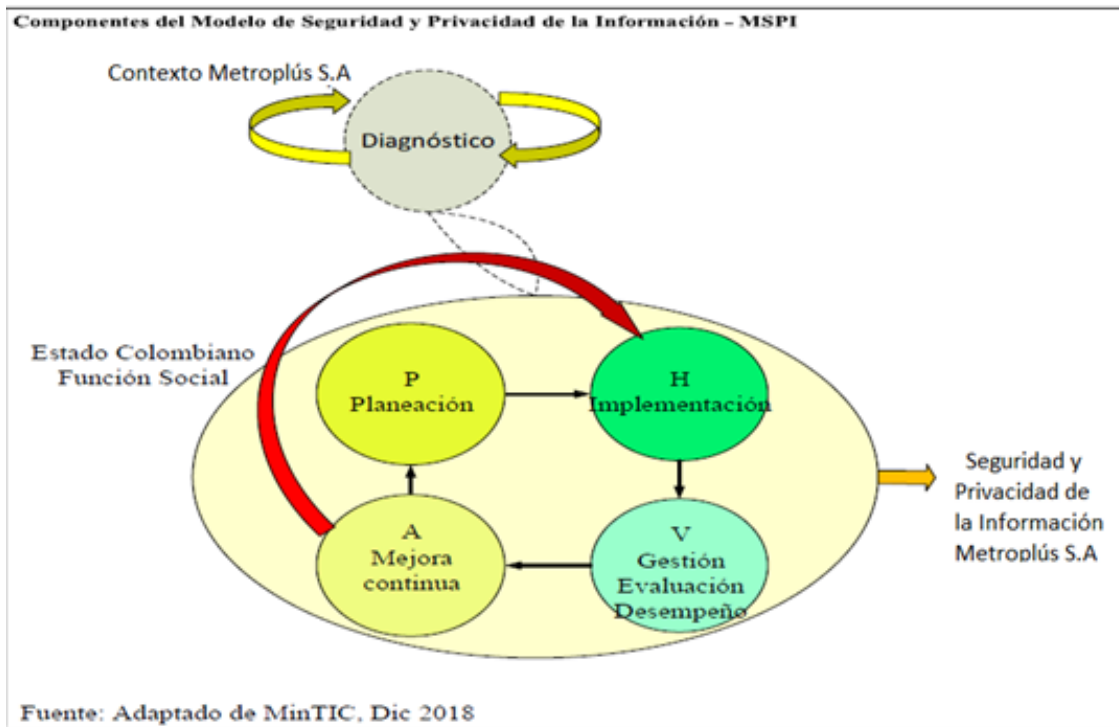
La Profesional Universitaria Gestión TIC y Servicios Administrativos, no ha contado con recursos específicos para la definición, diseño, implementación, gestión y operación de un sistema de Gestión de Seguridad de la Información. Los recursos aforados han sido concebidos para atender necesidades de infraestructura tecnológica de la Entidad de conformidad con la definición y caracterización del proceso de Gestión Tecnológica actual de la Entidad, tampoco ha destinado recursos para el cumplimiento de la legislación para fines de protección de datos personales.

## **7.2. Metodología del Plan**

La metodología procede de conformidad con el Modelo de Seguridad y Privacidad de la Información definida por MinTIC en concordancia con la norma ISO 27001 e ISO 27002, contempla las fases del ciclo de operación.

Las fases de operación serán aplicadas para el desarrollo y ejecución del presente Plan. La figura 2. Componentes del Modelo de Seguridad y Privacidad de la Información – MSPI, permite mostrar la aplicación del ciclo PHVA y las distintas fases del modelo de operación del MSIP propuesto.

*Figura No. 2. Componentes del Modelo de Seguridad y Privacidad de la Información MSPI*



### 7.3. Actividades del Plan

Las actividades del Plan se resumen en la tabla 3 que relaciona las fases del modelo de operación que será aplicado por Metroplús S.A.

Tabla No. 3. Fases del Modelo de Seguridad y Privacidad de la Información de Metroplús S.A.

Fase	Meta	Periodo del Plan	Instrumento del MSPI
	1. Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	2020- 2023	



FASE DIAGNOSTICO	1	2. Determinar el nivel de madurez de los controles de seguridad de la información.	2020 – 2023	Diligenciamiento de la herramienta.  Diligenciamiento de la herramienta e identificación del nivel de madurez de Metroplús S.A.
		3. Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	2020 – 2023	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad
		4. Identificar el avance de la implementación del ciclo de operación al interior de la entidad.	2020 – 2023	
		5. Identificar el nivel de cumplimiento con la legislación vigente relacionada con protección de datos personales.	2020 – 2023	
		6. Identificación del uso de buenas prácticas en ciberseguridad.	2020 – 2023	
FASE PLANIFICACION	2	1. Política de Seguridad y Privacidad de la Información.	2020 - 2023	DA400-MA-GIN-02 Manual de Política de Seguridad de la Información V2
		2. Procedimientos de seguridad y	2020 - 2023	DA400-PR-INT-08 Procedimiento de



	privacidad de la información.		Restauración de Datos V1 DA-400-PR-INT-04 Procedimiento Incidentes de Seguridad  DA-400-PR-INT-10 Procedimiento generación Acceso Servicios TIC V1
	3. Roles y responsabilidades de seguridad y privacidad de la información.	2020 - 2023	DA-400-PR-INT-03 Manual Modelo de Estructuras de Sistemas de Información
	4. Inventario de activos de información.	2020 – 2023	DA-400-PR-GIN-02 Administración Plataforma Tecnológica V5 DA-400-PR-INT-05 Mantenimiento preventivo TICS V2  Da-400-FT-INT-33 Formato de Mantenimiento Preventivo de equipos V2  DA-400-PR-INT-06 Procedimiento alistamiento de equipos V2  DA-400-FT-INT-29 Lista de Chequeo





			Equipos de Cómputo V2  DA-400-FT-INT-34 Formato Mantenimiento Preventivo de Impresoras, Scanner V2  DA-400-FT-INT-36 Formato de Entrega y Devolución de Elementos V2
	5. Integración del MSPI con el Sistema de Gestión documental.	2020 – 2023	DA-430-MA-INT-01 Programa de Gestión Documental V2
	6. Identificación, Valoración y tratamiento de riesgo.	2020 – 2023	Matriz de Riesgos Gestión TIC 2018  GG-100-MA-GRI-01 Manual de Gestión de Riesgos V2
	7. Plan de Comunicaciones.	2020 - 2023	CO-130-MA-COM-01 Manual de Políticas comunicacionales V2
	8. Plan de diagnóstico de IPv4 a IPv6.	2020 - 2023	No existe, pues de acuerdo a la infraestructura tecnológica actual no soporta el trabajo con este protocolo
	1. Planificación y Control Operacional.	2020 - 2023	



<b>FASE 3 IMPLEMENTACION</b>	2. Implementación del plan de tratamiento de riesgos.	2020 - 2023	Documento con el Plan de Tratamiento de Riesgos.  Declaración de Aplicabilidad
	3. Indicadores de Gestión.	2020 - 2023	
	4. Plan de Transición de IPv4 a IPv6	2020 - 2023	En diciembre 1 de 2020, Metroplús, renueva la Infraestructura Tecnológica, lo que posibilita la construcción de este Diagnóstico y su implementación.
<b>FASE 4 EVALUACIÓN DESEMPEÑO</b>	1. Plan de revisión y seguimiento, a la implementación del MSPI.	2020 – 2023	GG120-FT-EYC-01 Programas de Auditorías V7
	2. Plan de Ejecución de Auditorías	2020 - 2023	GG120-FT-EYC-09 Plan de Auditoría V2 Final
<b>FASE 5 MEJORA CONTINUA</b>	Plan de Mejora Continua	2020 - 2023	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI.  Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI.



			GG420-FT-EYC-02 Mejoramiento (seguimiento acciones) V2
--	--	--	---

## **7.4. Recursos del Plan**

### **7.4.1. Recursos Humanos**

- 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.

### **7.4.2. Recursos Físicos**

Edificaciones e Instalaciones de la Entidad (arrendadas)

### **7.4.3. Recurso Tecnológico**

- Infraestructura Tecnológica

## **7.5. 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.

## **7.6. 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. Metroplús S.A. revisará periódicamente la proyección presupuestal correspondiente al presente Plan de Seguridad y Privacidad de la Información, para dar cubrimiento en la presente o siguientes vigencias, de conformidad con sus ingresos, proyección de ingreso y definición de prioridades estratégicas.

### **7.7. Proyectos y Actividades de Seguridad 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 prevista en el presente Plan.

Para la presente vigencia 2020, se avanzará remedialmente de conformidad con los recursos disponibles asignados para la gestión TI, y los demás componentes se implementarán 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 un alcance básico del MSPI, para avanzar en el desarrollo y madurez en las distintas fases y componentes del modelo, hasta su culminación y mejora continua, que también será progresiva.

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

*Tabla No. 4. Proyectos de Seguridad y Privacidad de la Información de Metroplús S.A.*

<b>ID</b>	<b>PROYECTO/ACTIVIDAD</b>	<b>RESPONSABLE</b>	<b>CORRESPONSABLE</b>	<b>FECHA</b>
1	Automatización de Procesos para la Optimización de la	DIRECTOR ADMINISTRATIVO	Asistente CAD – Tecnólogo de	2021



	Gestión Documental de Metroplús S.A.		Soporte de Metroplús	
2	Adquisición, implementación y puesta en producción de una Solución ERP para Metroplús S.A.	DIRECTOR FINANCIERO	Profesional Universitaria Planificación Financiera y Gestión Contable y Tributaria - Tecnólogo de Soporte de Metroplús	2021
3	Adquisición de Licencias de Software de Aplicaciones de Apoyo para la Dirección de Transporte	DIRECTOR DE TRANSPORTE	Profesional Especializado Estructuración Técnica de los Proyectos de Metroplús	2021
4	Adquisición de Licencias de Software de Aplicaciones de Apoyo para la Dirección de Infraestructura	DIRECTOR DE INFRAESTRUCTURA	Profesional Universitario Gestión de Proyectos de Infraestructura	2021
5	Actualización Gráfica del Portal Web corporativo y Desarrollo de la Intranet para Metroplús S.A.	COMUNICACIONES	Profesional de Comunicaciones	2021
6	Adquisición, implementación y puesta en producción de una Solución para la Administración de los Sistemas de Gestión de Metroplús S.A.	DIRECTOR ADMINISTRATIVO	Profesional Universitario de Calidad	2022
7	Crecimiento y Mejoramiento de la	DIRECTOR ADMINISTRATIVO	Profesional Universitaria Gestión TIC y	2020



	Infraestructura Tecnológica		Servicios Administrativos	
8	Implementar un SGSI para METROPLÚS S.A.	DIRECCION ADMINISTRATIVA	Profesional Universitaria Gestión TIC y Servicios Administrativos – Profesional de Calidad	2022 - 2023

### **7.8. Plan Proyecto de Inversión**

Los proyectos a ejecutar para todo el componente de TI de la empresa para la vigencia 2020 y siguientes, contemplan la continuidad de las iniciativas en marcha y la incorporación de nuevos proyectos necesarios para cumplir con el Plan de Seguridad y Privacidad de la Información definido en el presente documento.

Los costos de operación y funcionamiento de la Dirección Administrativa, en lo que tiene que ver con la Tecnología de la Información para la vigencia 2020 y que fueron contemplados en el Plan Estratégico de TI (PETI) y en el Plan Estratégico Institucional 2018 – 2021.

### **7.9. Plan de Comunicaciones**

La Dirección Administrativa, por intermedio de la Profesional Universitaria Gestión TIC y Servicios Administrativos socializará con los grupos de interés el Plan de Seguridad y Privacidad de la Información para la vigencia 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 Director Administrativo y publicado en el sitio web de Metroplús S.A. [www.metroplus.gov.co](http://www.metroplus.gov.co)

Para la presente vigencia 2020, se avanzará remedialmente de conformidad con los recursos disponibles asignados a la Dirección Administrativa para la Tecnología de la Información, y los demás componentes del Plan de Comunicaciones se implementarán



progresivamente en la medida que se produzca la asignación de recursos para el año 2021, 2022 y 2023.

Se propone establecer un programa de sensibilización, capacitación y comunicación en seguridad de la información para explicar de manera apropiada las reglas de comportamiento adecuadas para el uso de los sistemas y la información, que estarán plasmadas en las políticas y procedimientos de seguridad de la información que la Entidad, requiere que sean cumplidos por parte de todos los usuarios del sistema.

El presupuesto para este programa se sugiere concebir en el plan de capacitación institucional que lidera la Oficina de Talento Humano, para el Uso y apropiación de TI y para Seguridad y Privacidad de la Información.

El programa de se definirá de conformidad con la Guía N° 14 del MSPI establecida por MinTIC, el cual considera en primera instancia definir el modelo como se administrará el programa de sensibilización, y contemplará las siguientes actividades o etapas, como se indica en la tabla No. 5.

*Tabla No. 5. Metas y acciones del programa de sensibilización, entrenamiento, educación y desarrollo profesional para la Seguridad y Privacidad de la Información de Metroplús S.A.*

<b>META</b>	<b>ACCIONES</b>	<b>RESPONSABLES</b>	<b>CORRESPONSABLES</b>	<b>PERIODO</b>
Identificación de necesidades	Métodos de identificación de Necesidades	Tecnólogo de Soporte – Profesional Universitaria Gestión TIC y Servicios Administrativos – Coordinador de Control Interno	Gerencia – - Secretaría General - Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
	Colaboración con otras áreas y algunas necesidades adicionales a identificar			
	Definir prioridades	Tecnólogo de Soporte – Profesional Universitaria		2020 - 2023
	Definir la complejidad del material			



Diseño del Plan de Capacitación y Sensibilización	desarrollar / adquirir / emplear	Gestión TIC y Servicios Administrativos – Oficina de Talento Humano	Gerencia – Secretaría General - Dirección Administrativa – Coordinación de Control Interno	
	Financiamiento del plan de capacitaciones			
Desarrollo de Materiales para el programa	Desarrollo de material para sensibilización	Tecnólogo de Soporte – Profesional Universitaria	Gerencia – Secretaría General – Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
	Desarrollo de material para entrenamiento	Gestión TIC y Servicios Administrativos		
Implementación del programa	Socialización del plan con la alta Dirección			202 - 2023
	Técnicas recomendadas para comunicación de información de sensibilización	Tecnólogo de Soporte – Profesional Universitaria	Gerencia – Secretaría General - Dirección Administrativa – Coordinación de Control Interno	
	Técnicas recomendadas para la comunicación de material de entrenamiento	Gestión TIC y Servicios Administrativos		
	Evidencias de la asistencia a Capacitaciones y el compromiso con la entidad			
Post- implementación (evaluación y mejoramiento continuo del programa).	Monitoreo del plan de capacitaciones	Tecnólogo de Soporte – Profesional Universitaria	Gerencia – Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
	Evaluación de las actividades de sensibilización / entrenamiento	Gestión TIC y		





		Servicios Administrativos		
Mejoramiento del plan de capacitaciones.	Análisis de las evaluaciones	Tecnólogo de Soporte Profesional Universitaria	Gerencia – Secretaría General – Dirección Administrativa – Coordinación de Control Interno	2020 - 2023
	Recomendaciones para la mejora	Gestión TIC y Servicios Administrativos		
Indicadores del plan de capacitaciones.	Definición y estructura de indicadores	Tecnólogo de Soporte Profesional Universitaria	Gerencia – Secretaría General – Dirección Administrativa – Coordinación de Control Interno	2020 - 2023

Es necesario precisar que la sensibilización aplicará para toda la Entidad por igual. Todos los servidores y contratistas podrán ver la información entregada de sensibilización como una responsabilidad compartida en seguridad de la información y que todos son importantes en esa labor. Entre los temas más importantes de sensibilización que serán considerados se encuentran descritos en la tabla 6., sin embargo, podrán variar de acuerdo a las necesidades identificadas.

*Tabla No. 6 Temática inicial de sensibilización*

<b>Temática inicial para sensibilización de Seguridad y Privacidad en Metroplús S.A.</b>	
Administración de contraseñas	Uso y manejo de inventario
Malware y sus diferentes tipos	Software permito/no permitido por la entidad
Políticas organizacionales relacionadas con Seguridad de la Información	Uso de dispositivos de la entidad fuera de las instalaciones
Uso de correo electrónico e identificación de correos sospechosos	Seguridad en el puesto de trabajo
Uso apropiado de internet	Temas de control acceso a los sistemas (privilegios, separación de roles)
Política de escritorio limpio	Ingeniería social



Sanciones por incumplimiento de las políticas	Gestión de incidentes (como reportar, que puedo reportar)
---	---

## 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](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](https://www.mintic.gov.co/gestionti/615/articles5482_G14_Plan_comunicacion_sensibilizacion.pdf).

El presente Documento fue elaborado por:

MITSY ALBANY MEJIA MEDINA

Profesional Universitario Gestión TIC y Servicios Administrativos