DERECHOS DE AUTOR

En el presente documento Metrolínea acoge como referencia el Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones y el Plan Marco de Seguridad y Privacidad de la Información diseñado por la Alcaldía Municipal de Bucaramanga, con la finalidad de implementar el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital, adaptándolo a las situaciones fácticas particulares y necesidades de la entidad.

INTRODUCCIÓN

El Marco para la seguridad y privacidad de la información fija los parámetros generales para la estructuración de un Sistema de Gestión de Seguridad de la Información (SGSI) para Metrolínea S.A., basado en las normas internacionales ISO 27000:2013 articulado con la normatividad colombiana para la reglamentación de la protección de datos personales (privacidad), ley 1581 de 2012 y decreto 1377 de 2013, lo anterior con el objetivo de aplicar lo dispuesto para la implementación de la Estrategia de Gobierno digital

Es importante tener en cuenta que es necesaria la participación activa del comité Institucional de Gestión y Desempeño, en articulación con las demás instancias y responsables del Modelo Integrado de Planeación y Gestión cuando las temáticas o funciones misionales lo requieran.

CONTENIDO

1. MARCO DE LA SEGURIDAD DE LA INFORMACIÓN DE METROLINEA S.A.

El presente documento fija los parámetros generales para la estructuración de un Sistema de Gestión de Seguridad de la Información SGSI para Metrolínea S.A. y así dar aplicabilidad al principio de la seguridad y privacidad de la información de la estrategia de Gobierno Digital, que *busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano*, en concordancia con el *principio de seguridad* de la Ley estatutaria para la protección de datos personales, favoreciendo el desarrollo transversal de los objetivos misionales y estratégicos de Metrolínea S.A.

1.1. DEFINICIÓN

El marco de seguridad y privacidad de la información (MSPI) es la guía para desarrollar los objetivos de la estrategia de Gobierno Digital donde se estable la necesidad de gestionar los riesgos de la seguridad y privacidad de la información de las entidades públicas, a través de la implementación de un sistema de gestión de seguridad de la información contando con los diferentes procesos de Metrolínea S.A. y otros modelos de gestión.

1.2. ÁMBITO

De conformidad con el informe anual de seguridad de Symantec que analiza un total de 157 países, Colombia en el 2017 se ubicó en el sexto lugar de Latinoamérica con el mayor número de ciberataques, siendo los más comunes en el territorio colombiano son los bots, spam, Phishing y Malware. Lo que genera una gran preocupación porque que gran cantidad de vulnerabilidades son detectadas en los sistemas informáticos que usan las entidades financieras, instituciones del gobierno y empresas todo el mundo, que se suponen deben ser los más seguros, lo anterior evidencia la necesidad de la gestión de riesgos digitales para proteger y asegurar la información.

Por lo anterior es indispensable que los funcionarios, directivos, contratistas y personal de Metrolínea S.A., que tengan acceso a la información con ocasión del desarrollo de sus funciones, adopte y ponga en práctica los diferentes mecanismos, herramientas, políticas y procedimientos creados para garantizar la seguridad y privacidad de la información, conforme las disposiciones legales.

1.3. ALIADOS ESTRATÉGICOS

Los aliados estratégicos para el funcionamiento del marco se consideran como actores que en cualquier momento pueden intervenir para la gestión, colaboración, reporte e investigación de incidentes de carácter informático para la gestión de la seguridad de la información, entre ellos se encuentran:

- **ColCERT**: Grupo de respuestas ante emergencias Cibernéticas de Colombia.
- CCP: Centro cibernético policial
- **Fiscalía general de la nación**: Órgano investigativo para delitos informáticos

- **SIC**: Superintendencia de industria y comercio, autoridad para la protección de datos personales.
    - **MINTIC**: Ministerio de Tecnologías de la información y Comunicaciones líder la implementación de estrategia de Gobierno en línea.
- **Universidades y otras entidades del sector tecnológico**.

1.4.CONTEXTO NORMATIVO Y ESTANDARIZACIÓN

1.4.1. ESTÁNDARES INTERNACIONALES

- **ISO 27001:2013:** Estándar internacional para la implementación de los sistemas de gestión de la seguridad de la información.
- **ITIL v3**: Es una librería de buenas prácticas para la gestión de servicios de tecnología de la información (TI), una de las librerías es la gestión de la seguridad de la información; actualmente en su versión 3.

1.4.2. NORMATIVIDAD COLOMBIANA

- **Constitución política de Colombia 1991,** Artículos 15 y 20.
- **Ley 599 de 2000,** código penal colombiano.
- **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 del Espectro y se dictan otras disposiciones".
- **Ley 1581 de 2012,** "Por la cual se dictan disposiciones generales para la protección de datos personales."
- **Decreto 1377 de 2013,** "Por el cual se reglamenta parcialmente la Ley 1581 de 2012".
- **Decreto 32 de 2013,** Por el cual se crea la Comisión Nacional Digital y de Información Estatal para la atención de incidentes de ciberdefensa y ciberseguridad.
- **Ley 1712 de 2014**, Ley de transparencia de la información pública.
- **Decreto 2573 de 2014**, Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea.
- **Decreto 1078 de 2015,** Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- **CONPES 3854**, Documento para la seguridad digital.

Otra normatividad vigente en derecho de autor propiedad intelectual y comercio electrónico.

1.5.POLÍTICAS

Con la necesidad de gestionar la seguridad y privacidad de la información se requiere crear, documentar y socializar las siguientes políticas:

- **Política de seguridad de la información**: Documento en el cual se establecen las indicaciones generales para el manejo de la seguridad de la información dentro de Metrolínea S.A, aprobada por el comité institucional de Gestión y Desempeño de Metrolínea S.A.

- **Política de protección de datos personales:** Documento por el cual se da cumplimiento a la ley 1581 de 2012 y el decreto reglamentario 1377 de 2013 para el manejo de datos personales.

1.6.ARTICULACIÓN ESTRATÉGICA

La gestión de la seguridad de la información es un deber de la entidad y por lo tanto es importante lograr la articulación e integración de diferentes puntos de acción de la organización:

1.7.CAPACITACIÓN, PROMOCIÓN Y SENSIBILIZACIÓN

Para articular las acciones y documentos alrededor del marco de seguridad y privacidad de la información es importante capacitar y sensibilizar a los funcionarios, contratistas y/o terceros sobre los riesgos digitales y tendencias en el manejo de la información. Los aspectos a priorizar inicialmente son:

- Capacitación en seguridad de la información, políticas y documentación asociada al SGSI
- Promoción de las herramientas de protección, tendencias y amenazas frecuentes.

1.8. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Se define como el conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de

seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.

1.8.1. OBJETIVO

Gestionar la toma de decisiones para la seguridad y privacidad de información articulando con los diferentes sistemas de gestión la implementación de políticas, controles y procedimientos, así como también la respuesta ante incidentes de seguridad.

1.8.2. ALCANCE

EL SGSI tendrá un alcance interno para las dependencias, funcionarios, contratistas y/o terceros de Metrolínea S.A.

1.8.3. LIMITES

El SGSI no hará control de incidentes a nivel de los usuarios del SITM de Metrolínea S.A., sin embargo, con los medios disponibles se sensibilizará sobre la existencia de la gestión de la seguridad dentro de la entidad a personal externo.

1.8.4. ORGANIZACIÓN DEL SGSI

El SGSI funcionará liderado por el Secretario General, quien articulará con las dependencias de la entidad a través del MIPG las actividades relacionadas en esta gestión. Las funciones o roles importantes para el SGSI son:

- **Seguridad y controles:** se establecerán los mecanismos o herramientas para el control de la seguridad de la información con base a la política de seguridad de la información.

- **Privacidad de datos:** La función es articular la gestión de la política de protección de datos personales mediante las herramientas, controles o procedimientos necesarios para el pleno cumplimiento de la legislación actual.

1.8.4.1. RESPONSABILIDADES

Las funciones específicas de cada rol en la organización del SGSI son:

Líder de SGSI

- Coordinar la implementación y gestión de las políticas relacionadas con la seguridad y privacidad.

- Supervisar el cumplimiento normativo.

- Garantizar la privacidad de los datos.

- Administrar al Equipo de Respuesta ante Incidentes de Seguridad de la información.

- Supervisar la administración de identidades y acceso.

- Coordinar y supervisar la arquitectura de seguridad de Metrolínea S.A.
- Llevar a cabo el descubrimiento electrónico y las investigaciones forenses digitales.
- Trabajar con los directivos de Metrolínea S.A. para establecer los planes de recuperación de desastres (DR) y continuidad del negocio.

Oficial de seguridad de la información:

- Apoyar la implementación y gestión del MSPI.
- Definir, revisar y evaluar la Política de seguridad de la información de Metrolínea S.A.
- Definir, revisar y evaluar los procedimientos para aplicar la Política de seguridad de la información.
- Seleccionar y gestionar los mecanismos y herramientas adecuados que permitan aplicar las políticas de seguridad de la información.
- Aplicar metodologías de análisis de riesgo en Metrolínea S.A.
- Promover la aplicación de auditorías enfocadas a la seguridad, para evaluar las prácticas de seguridad.
- Crear y vigilar los lineamientos necesarios que coadyuven a tener los servicios de seguridad.
- Coordinar el grupo de seguridad informática y la gestión de incidentes en la organización.
- Promover e impulsar la formación, educación y concienciación seguridad de la información.

Oficial de privacidad de datos:

- Apoyar la implementación y gestión del MSPI.
- Definir, revisar y evaluar la Política de privacidad y de protección de datos de Metrolínea S.A.
- Valorar el impacto sobre el marco de privacidad y la protección de los datos personales de nuevos proyectos o de normas que afecten a Metrolínea S.A.

- Coordinar la atención de los ejercicios de los derechos de los interesados en cuento a reclamaciones formuladas por los titulares de la información.

- Establecer relaciones con las autoridades en protección de datos (SIC).

- Supervisar la gestión de incidencias.

- Coordinar los planes de auditoría, de carácter interno o externo.

- Impulsar la adopción de medidas en conjunto a las políticas de seguridad de la información para asegurar el cumplimiento de la normativa de protección de datos.

- Impulsar y promover buenas prácticas en protección de datos.

- Promover e impulsar la formación, educación y concienciación en protección de datos.

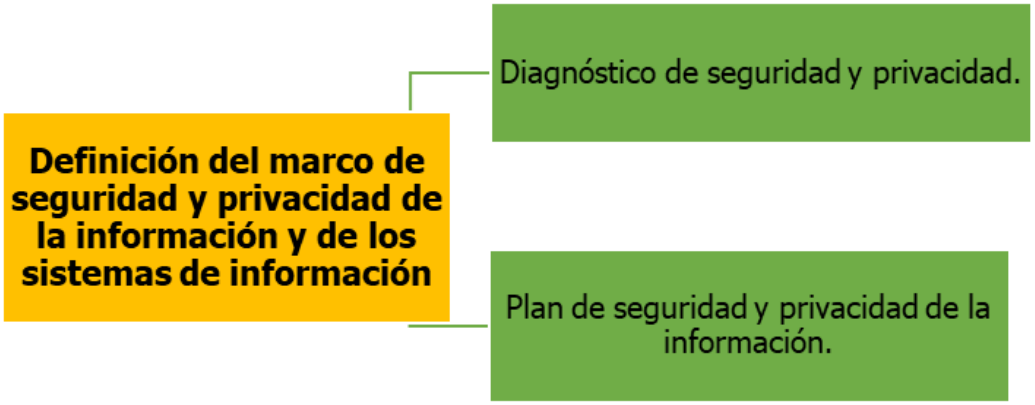
Nota: para llegar a implementar estas responsabilidades es importante concretar la estructura y organización de la actividad de TI al interior de Metrolínea S.A. como lo propone inicialmente el PETI, igualmente poder establecer gestión de mesa de servicio para la gestión de incidentes.

1.8.4.2. FASES DE IMPLEMENTACIÓN

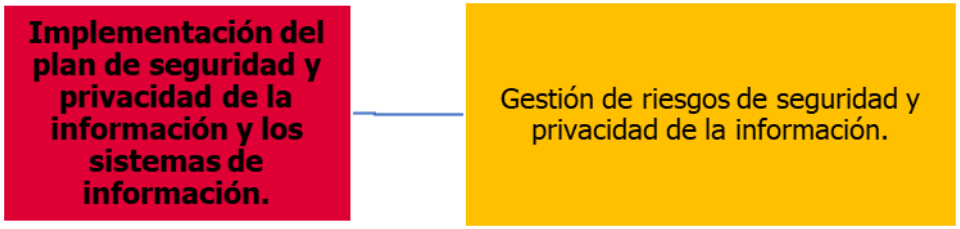
Mediante las cartillas publicadas por el MINTIC se establecen las siguientes fases que serán adoptadas por Metrolínea S.A:

- **Diagnóstico de seguridad y privacidad de la información:** Con el cual se podrá establecer el nivel actual de la entidad en este tema.

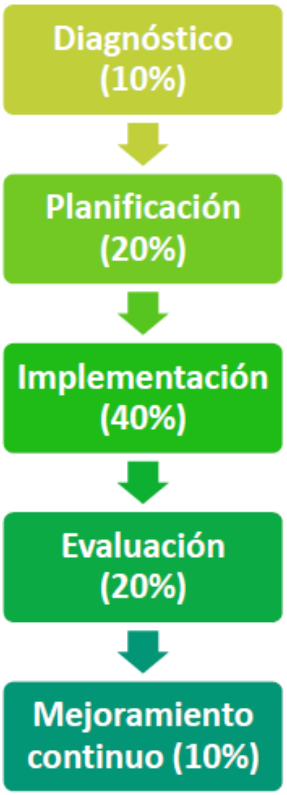
- **Planificación:** Donde se determinarán las acciones a tomar verificando la alineación estratégica de la entidad para la construcción de acciones objetivas.



- **Implementación:** Se busca la identificación valoración, tratamiento y mitigación de riesgos asociados al manejo de la información.



- **Evaluación y mejoramiento continuo:** para la revisión de acciones tomadas y la mejora continua a través de la gestión del conocimiento y lecciones aprendidas en la implementación.



Seguridad y Privacidad de la Información	**30%**	Definición de marco privacidad de la Entidad: La Entidad define el estado actual de privacidad y elabora su plan.	10%	Diagnóstico de Seguridad y Privacidad de la información: Busca que la entidad determine el nivel de seguridad y privacidad en el cual se encuentra.	10%	La Entidad cuenta con un diagnóstico de seguridad y privacidad.	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC 27001:2013 LI.ES.01 LI.ES.02 LI.GO.01
			20%	Propósito de seguridad y Privacidad de la información: Busca que la entidad organice las acciones a tomar, verificando que estén alineadas a la misión y visión de la entidad y construya de manera objetiva.	20%	La Entidad cuenta con un plan de seguridad e información.	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC LI.ES.02 27001:2013 LI.GO.01 LI.ES.08 LI.ES.06 LI.GO.04 LI.GO.09
	40%	Implementación del plan de seguridad y privacidad: La entidad desarrolla las acciones definidas en el plan de seguridad y privacidad de información.	40%	Gestión de Riesgos de seguridad y privacidad de la información: Busca la identificación, valoración,	20%	La entidad identifica y analiza los riesgos.	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC LI.ES.02 27001:2013 COBIT 5 LI.GO.04 LI.ST.14
				Mitigación de los riesgos.	20%	La entidad cuenta con un plan de tratamiento de riesgos, clasifica y gestiona controles	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC IEC 27001:2013 LI.INF.15 LI.SIS.22

	30%	Monitoreo y Mejoramiento continuo: La Entidad desarrolla actividades para la evaluación y mejora de los niveles de seguridad y privacidad de la información.	30%	Evaluación del desempeño Busca hacer las mediciones necesarias para calificar la operación y efectividad de los controles, estableciendo niveles.	20%	La entidad cuenta con actividades para el Seguimiento, medición, análisis y evaluación del desempeño de la seguridad y privacidad a efecto de generar los ajustes o cambios y oportunos pertinentes	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC 27001:2013 LI.ES.13 LI.GO.03
				de cumplimiento y de protección de los principios de seguridad y privacidad de la información	10%	La entidad revisa e implementa acciones de mejora continua que garanticen el cumplimiento del plan de seguridad y privacidad de la Información.	Modelo de Privacidad y seguridad de la Información. NTC-ISO-IEC 27001:2013 LI.ES.13 LI.GO.03

2. FASE DIAGNÓSTICO

Conocer el estado actual de la entidad es de vital importancia para establecer el punto de partida del componente de la seguridad y privacidad de la información, en este campo Metrolínea S.A. iniciará la gestión desde cero (0) porque hasta ahora se están diseñando los documentos y estrategias necesarias para el SGSI.

Para el cumplimiento de esta fase se establecen los siguientes lineamientos:

- **LI.ES.01:** Las instituciones de la administración pública deben contar con una estrategia de TI que esté alineada con las estrategias sectoriales, el Plan Nacional de Desarrollo, los planes sectoriales, los planes decenales -cuando existan- y los planes estratégicos institucionales. La estrategia de TI debe estar orientada a generar valor y a contribuir al logro de los objetivos estratégicos.

- **LI.ES.02:** Cada sector e institución, mediante un trabajo articulado, debe contar con una Arquitectura Empresarial que permita materializar su visión estratégica utilizando la tecnología como agente de transformación. Para ello, debe aplicar el Marco de Referencia de Arquitectura Empresarial para la gestión de TI del país, teniendo en cuenta las características específicas del sector o la institución.

- **LI.ES.03:** La dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir e implementar un esquema de Gobierno TI que estructure y direccione el

flujo de las decisiones de TI, que garantice la integración y la alineación con la normatividad vigente, las políticas, los procesos y los servicios del Modelo Integrado de Planeación y Gestión de la institución.

Los entregables de esta fase serán los siguientes:

FASE	**DIAGNÓSTICO**
CANTIDAD DE ENTREGABLES	**Tres (3)**
	1
FECHAS	2
	3

META	**ENTREGABLE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura de red de comunicaciones (IPv4/IPv6).	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección.
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad.	Documento con el resultado de la herramienta de la encuesta, revisado, aprobado y aceptado por la alta dirección.
Realizar pruebas que permitan a la Entidad medir la efectividad de los controles existentes.	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la dirección.

2.1.MAPA DE ACTIVIDADES FASE DIAGNÓSTICO

Meta	**Recursos Humano**		**Costo**		**Actividades**	**Tiempo**	**Entregables**
	Interno	**Externo**	**Interno**	**Externo**			
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad, teniendo en cuenta la infraestructura					Levantamiento de mapa de red de infraestructura Tecnológica.		Documento con el resultado de la autoevaluación realizada a la entidad, de la gestión de seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta
					Inventario de contraseñas gestionadas y Aseguradas.		
					Diagnóstico de auditoría Según		

de red de comunicaciones (IPv4/IPv6).					modelo Gobierno Digital.		Dirección.
					Revisión de políticas existentes de seguridad y Privacidad.		
Identificar el nivel de madurez de seguridad y privacidad de la información de la Entidad					Auditoría según norma ISO27001		Documento con el resultado de la herramienta de la encuesta, revisado, aprobado y aceptado por la entidad.
Realizar pruebas que permitan a la entidad medir la efectividad de los controles existentes.					Levantamiento de controles existentes		Documento con el resultado de la estratificación de la entidad, aceptado y aprobado y por la dirección.
					Evaluación de controles aplicados.		

3. FASE DE PLANIFICACIÓN

FASE	**PLANIFICACIÓN**	
CANTIDAD DE ENTREGABLES		**Ocho (8)**
FECHAS	1	
	2	
	3	
	4	
	5	
	6	
	7	
	8	

META	**ENTREGABLE**
Objetivos, alcance y límites del MSPI.	Documento con el alcance y límites de la seguridad de la información, debidamente aprobado y socializado al interior de la Entidad, por la alta Dirección.

Políticas de seguridad y privacidad de la información (Ver anexo 1 y 2) *	Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
Procedimientos de control documental del MSPI (Ver anexo 3) *	Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de gestión institucional.
Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección.
Inventario de activos de información.	Documento de inventario de activo de información, revisado y aprobado por la alta Dirección.
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de (Metodología, Reportes) o Tratamiento de riesgos (Selección de controles).	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección.
Toma de conciencia.	Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta dirección.
Plan y estrategia de transición de IPv4 a IPv6.	Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

3.1.MAPA DE ACTIVIDADES FASE DE PLANIFICACIÓN

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Objetivos, alcance y límites del MSPI.					Desarrollo de un marco de seguridad y privacidad de la información para Metrolínea S.A.		Documento con el alcance y límites de la seguridad de la información, debidamente aprobado y

					Revisión y ajustes del MSPI		socializado al interior de la Entidad, por la alta dirección
					Aprobación del MSPI		
					Publicación y socialización		
Políticas de seguridad y privacidad de la información					Desarrollo de las políticas de seguridad y privacidad de la información para Metrolínea S.A.		Documento con las políticas de seguridad y privacidad de la información, debidamente aprobadas y socializadas al interior de la Entidad, por la alta Dirección.
					Revisión y ajustes de las políticas de Seguridad y Privacidad de la Información		
					Aprobación de la política de Seguridad y Privacidad de la Información		
Procedimientos de control documental MSPI					Actualización y revisión del proceso de gestión e implementación y soporte de las TIC para articular con el MSPI		Formatos de procesos y procedimientos, debidamente definidos, establecidos y aprobados por el comité que integre los sistemas de Gestión Institucional
					Generación de formatos, guías, manuales, Instructivos asociados al SGC		
					Publicación y aprobación en el Sistema de Gestión de Calidad		
Asignación de recurso humano, comunicación de roles y responsabilidades de seguridad y privacidad de la					Verificar existencia de personal institucional para la asignación de roles.		Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (ó el que haga sus

información.							veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por
Inventario de activos de información.					Revisión de inventario de activos de información anteriores		Documento de inventario de activo de información, revisado y aprobado por la alta Dirección
					Verificación y actualización de activos de información.		
					Asociación de riesgos de Confidencialidad, Integridad, Disponibilidad y custodios.		
					Aprobación, publicación y socialización.		
					Diseño del sistema de gestión de activos de información del Metrolínea S.A.		
					Selección de activos de información con riesgo en privacidad de datos personales.		
					Caracterización de información pública para datos abiertos		
Acciones para tratar riesgos y oportunidades de seguridad de la					Análisis de metodología de riesgo aplicables a Metrolínea S.A.		Documento con el informe de análisis de riesgos, matriz de riesgos, plan de

información. Identificación y valoración de riesgos de (Metodología, Reportes). O Tratamiento de riesgos (Selección de controles).					Diseño de matriz de riesgo de seguridad y privacidad de activos de información.		tratamiento de riesgos y declaración de aplicabilidad, revisado y aprobado por la alta Dirección.
					Elaboración de aplicabilidad de norma ISO27000 (SoA)		
					Plan de tratamiento de riesgos.		
Toma de conciencia.					Plan de sensibilización de tendencias TI y alertas de virus entre otras.		Documento con el plan de comunicación, sensibilización y capacitación, con los respectivos soportes, revisado y aprobado por la alta Dirección
					Plan anual de capacitaciones en seguridad y privacidad de la información		
Plan y estrategia de transición de IPv4 a IPv6.					Estudio de aplicabilidad de Ipv6		Documento con el plan y estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

4. FASE DE IMPLEMENTACIÓN

FASE	**IMPLEMENTACIÓN**	
CANTIDAD DE ENTREGABLES		**Cuatro (4)**
FECHAS	1	
	2	
	3	
	4	

4.1. MAPA DE ACTIVIDADES FASE DE IMPLEMENTACIÓN

META	**ENTREGABLE**

Planificación y control operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
Implementación de controles.	Documento con el informe del plan de tratamiento de riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad, revisado y aprobado por la alta Dirección
Implementación del plan de tratamiento de riesgos	Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección.
Implementación del plan y estrategia de transición de IPv4 a IPv6	Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección.

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Planificación y control operacional.					Documento de procedimientos del SGSI.		Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
					Revisión y aprobación del documento de procedimientos y operaciones.		
					Revisión de la declaración de aplicabilidad.		
					Revisión de documentación asociada al SGC.		
					Diseño e implementación del sistema para la gestión de la seguridad de la información Reservada		
Implementación de controles.					Aplicación de controles por recursos humanos y áreas seguras.		Documento con el informe del plan de tratamiento de

					Aplicación de controles de red y servidores		riesgos, que incluya la implementación de controles de acuerdo con lo definido en la declaración de aplicabilidad, revisado y aprobado por la alta Dirección
					Aplicación de controles para evaluación y mejora continua.		
					Aplicación de normatividad legal de protección de datos personales		
					Elaboración de la documentación de controles aplicados.		
					Pruebas de efectividad de controles ejecutados para la seguridad y privacidad.		
Implementación del plan de tratamiento de riesgos					Diagnóstico Análisis de Impacto de Negocios BIA		Indicadores de gestión del MSPI, revisado y aprobado por la alta Dirección
					Elaboración del Plan de contingencia y continuidad del negocio		
					Elaboración de la guía para la gestión de incidentes de seguridad de la información		
					Elaboración e implementación de indicadores del MSPI		
Implementación del plan y estrategia de transición de IPv4 a IPv6					Aplicación del plan de transición a Ipv6		Documento con el informe de la implementación del plan y la estrategia de transición de IPv4 a IPv6, revisado y aprobado por la alta Dirección

5. FASE DE EVALUACIÓN

FASE	EVALUACIÓN
CANTIDAD DE ENTREGABLES	Tres (3)
FECHAS	1
	2
	3

META	ENTREGABLE
Plan de seguimiento, evaluación y análisis del MSPI.	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
Auditoria Interna	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.
Evaluación del plan de tratamiento de riesgos.	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección

5.1. MAPA DE ACTIVIDADES FASE DE EVALUACIÓN

Meta	Recursos Humanos		Costos		Actividades	Tiempo	Entregables
	Interno	Externo	Interno	Externo			
Plan de seguimiento, evaluación y análisis del MSPI.					Evaluación de indicadores de gestión del MSPI		Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
					Análisis de cumplimiento de la norma ISO 27000 (GAP)		
Auditoria Interna					Elaboración del plan de auditoria interna al SGSI		Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.
					Revisión de activos de información		
					Revisión de política de protección de datos		

					Evaluación de documentación y procedimientos.		
Evaluación del plan de tratamiento de riesgos.					Revisión del plan de riesgos.		Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.
					Revisión de riesgos asignados a activos de información.		

6. FASE DE MEJORA CONTINUA

FASE	**MEJORA CONTINUA**
CANTIDAD DE ENTREGABLES	**Dos (2)**
FECHAS	1
	2

META	**ENTREGABLE**
Plan de seguimiento, evaluación y análisis para el MSPI	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección
Auditoria Interna	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección
Comunicación de resultados y plan de mejoramiento.	
Revisión y aprobación por la alta Dirección.	

6.1. MAPA DE ACTIVIDADES FASE MEJORA CONTINUA

Meta	**Recursos Humanos**		**Costos**		**Actividades**	**Tiempo**	**Entregables**
	Interno	**Externo**	**Interno**	**Externo**			

Plan de seguimiento, evaluación y análisis del MSPI.					Evaluación de resultados de fase de evaluación. Revisión del análisis de cumplimiento de la norma ISO 27000 (GAP)		Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.
Auditoria Interna					Evaluación de hallazgos		Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta Dirección
					Elaboración de plan de mejoramientos del MSPI		
Comunicación de resultados y plan de mejoramiento					Plan de socialización y capacitación de mejoras y resultados		
Revisión y aprobación por la alta Dirección.					Actualización de documentación y correctivos de hallazgos de auditoría interna.		

7. CONCLUSIONES

- La información es el activo más importante para cualquier entidad, por lo tanto, es un factor clave protegerla de incidentes relacionados con la seguridad y privacidad que tienen que ver con los activos digitales de la entidad, abarcando los principios de confidencialidad, disponibilidad e integridad.

- Metrolínea S.A. busca a través de este documento implementar el componente de seguridad y privacidad de la información que es fundamental en los negocios que desean avanzar en la era digital y en las tecnologías de la información que cada vez más se implementan en las entidades, además de cumplir con las estrategias del gobierno nacional diseñadas para el sector público.

- Si bien día a día aparecen nuevos y complejos tipos de incidentes, aún se registran fallas de seguridad de fácil resolución técnica, las cuales ocurren en muchos casos por falta de conocimientos sobre los riesgos que acarrean. Por otro lado, los incidentes de seguridad impactan en forma cada vez más directa sobre las personas. En consecuencia, se requieren efectivas acciones de concientización, capacitación y difusión de mejores prácticas

- Es necesario mantener un estado de alerta y actualización permanente: la seguridad es un proceso continuo que exige aprender sobre las propias experiencias.

- Las organizaciones no pueden permitirse considerar la seguridad como un proceso o un producto aislado de los demás. La seguridad tiene que formar parte de las organizaciones.

- Debido a la constante amenaza en que se encuentran los sistemas, es necesario que los usuarios y las empresas enfoquen su atención en el grado de vulnerabilidad y en las herramientas de seguridad con las que cuentan para hacerle frente a posibles ataques informáticos que luego se pueden traducir en grandes pérdidas.

- Los ataques están teniendo el mayor éxito en el eslabón más débil y difícil de proteger, en este caso es la gente, se trata de uno de los factores que han incentivado el número de ataques internos. No importando los procesos y la tecnología, finalmente el evitar los ataques queda en manos de los usuarios.