Plan de Seguridad y Privacidad de la Información

Tabla de contenido

1. DERECHOS DE AUTOR 3
2. INTRODUCCIÓN 3
3. JUSTIFICACIÓN 3
4. GLOSARIO 4
5. OBJETIVO 6
6. OBJETIVO ESPECIFICOS 6
7. ALCANCE 6
8. MARCO LEGAL 6
9. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE METROLÍNEA S.A. (ADOPTADA EN COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE DICIEMBRE 3 DE 2018) 8
10. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN –SGSI 9
11. COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO 9
12. MODELO DE SEGURIDAD Y PRIVACIDAD – MSPI 9
12.1 METODOLOGIA ESTABLECIMIENTO MODELO DE SEGURIDAD 10
12.2 Fase Diagnostico: 10
12.3 Fase Planificación (Planear) 10
12.4 Fase Implementación (Hacer) 11
12.5 ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION 11
12.6 PLAN DE SEGURIDAD DE LA INFORMACION 14

1. DERECHOS DE AUTOR

Metrolínea S.A. para la elaboración del documento acoge como referencia la Guía para el plan de seguridad de la información artículo 74968 del Ministerio de Tecnologías de la Información y las Comunicaciones, con la finalidad de aportar al 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.

2. INTRODUCCIÓN

Metrolínea S.A. es consciente que la protección y aseguramiento de su información es fundamental para garantizar su debida gestión financiera, administrativa y operativa, razón por la cual ha establecido un marco normativo que contempla políticas, límites, responsabilidades y obligaciones frente a la seguridad y privacidad de la información y ciberseguridad de la entidad.

El objetivo primordial del sistema es garantizar que los riesgos asociados a la seguridad de la información, seguridad digital y ciberseguridad sean conocidos, gestionados y tratados de forma documentada, sistemática, estructurada, repetible y eficiente, con el fin de gestionar los riesgos a los cuales están expuestos los activos de información de Metrolínea S.A. y establecer las opciones apropiadas para su tratamiento.

A través del sistema, Metrolínea S.A. gestiona y administra los riesgos, eventos, amenazas, vulnerabilidades y situaciones que pueden afectar la seguridad de la información, la seguridad digital y la ciberseguridad de la entidad, lo anterior de acuerdo con el Decreto 1078 de 2015 modificado por el Decreto 1008 de 2018, en el artículo 2.2.9.1.1.3. Principios. Define la seguridad de la información como principio de la Política de Gobierno Digital, de igual manera en el artículo 2.2.9.1.2.1 define la estructura de los Elementos de la Política de Gobierno Digital a través de componentes y habilitadores transversales los cuales son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital

3. JUSTIFICACIÓN

El Plan de seguridad y privacidad busca que Metrolínea S.A. sea una entidad que contribuya a la construcción de un estado más eficiente, transparente y participativo a través de la implementación del MSPI, de igual forma busca estar alineado por lo establecido desde el Plan Nacional de desarrollo, aportando a los pactos de legalidad, equidad, etc. También a lo determinado en el componente de seguridad y privacidad de la información de la estrategia de Gobierno Digital, así como lo propuesto desde los Conpes de Ciberseguridad y Ciberdefensa, Seguridad Digital y ahora Transformación Digital.

4. GLOSARIO

- **Activo de información.**
  Aquello que es de alta validez y que contiene información vital de la empresa que debe ser protegida.

- **Amenaza.**
  Es la causa potencial de un daño a un activo de información.

- **Análisis de riesgos.**
  Utilización sistemática de la información disponible, para identificar peligros y estimar los riesgos.

- **Causa**
  Razón por la cual el riesgo sucede.

- **Ciberiesgo o riesgo cibernético**
  Posibles resultados negativos derivados de fallas en la seguridad de los sistemas tecnológicos o asociados a ataques cibernéticos

- **Ciberseguridad**
  Es el desarrollo de capacidades empresariales para defender y anticipar las amenazas cibernéticas con el fin de proteger y asegurar los datos, sistemas y aplicaciones en el ciberespacio o nube.

- **Colaborador**
  Es toda persona que realiza actividades directa o indirectamente en las instalaciones de la entidad, servidores públicos, contratistas y/o terceros.

- **Confidencialidad**
  Propiedad que determina que la información no esté disponible a personas no autorizados

- **Controles**
  Son aquellos mecanismos utilizados para monitorear y controlar acciones que son consideradas sospechosas y que pueden afectar de alguna manera los activos de información.

- **Disponibilidad**
  Propiedad que determina que la información sea accesible y utilizable por aquellas personas debidamente autorizadas.

- **Dueño del riesgo sobre el activo**
  Persona responsable de gestionar el riesgo.

- **Impacto**
  Consecuencias de que la amenaza ocurra. Nivel de afectación en el activo de información que se genera al existir el riesgo.

- **Incidente de seguridad de la información**

  Evento no deseado o inesperado, que tiene una probabilidad de amenazar la seguridad de la información.

- **Oficial de Seguridad**

  Persona encargada de administrar, implementar, actualizar y monitorear el Sistema de Gestión de Seguridad de la Información.

- **Probabilidad de ocurrencia**

  Posibilidad de que se presente una situación o evento específico.

- **Responsables del Activo**

  Personas responsables del activo de información.

- **Riesgo**

  Grado de exposición de un activo que permite la materialización de una amenaza.

- **Riesgo Inherente**

  Nivel de incertidumbre propio de cada actividad, sin la ejecución de ningún control.

- **Riesgo Residual**

  Nivel de riesgo remanente como resultado de la aplicación de medidas de seguridad sobre el activo.

- **Seguridad de la Información**

  Preservación de la confidencialidad, la integridad y la disponibilidad de la información (ISO 27000:2014).

- **SGSI**

  Siglas del Sistema de Gestión de Seguridad de la Información.

- **Sistema de Gestión de Seguridad de la información SGSI**

  Permite establecer, implementar, mantener y mejorar continuamente la gestión de la seguridad de la información de acuerdo con los requisitos de la norma NTC-ISO-IEC 27001.

- **Vulnerabilidad**

  Debilidad de un activo o grupo de activos de información que puede ser aprovechada por una amenaza. La vulnerabilidad de caracteriza por ausencia en controles de seguridad que permite ser explotada.

Autopista Floridablanca N° 86-30, Estación Provenza Occidental, Barrio Diamante II
Teléfono: 6929824 Bucaramanga.
www.metrolinea.gov.co

5. OBJETIVO

Establecer las actividades que están contempladas en el Modelo de Seguridad y Privacidad de la Información que apoyen el establecimiento, operación, mejora continua y sostenibilidad de la Entidad, acorde con los requerimientos del negocio y alineados con la estrategia de Gobierno digital y NTC/IEC ISO 27001:2013 que establece el Sistema de Gestión de seguridad y privacidad de la información.

6. OBJETIVO ESPECIFICOS

- Apoyar la operación, mejora continua y sostenibilidad del Sistema de gestión de seguridad de la información.
- Fortalecer la cultura de seguridad de la información.
- Definir, reformular y formalizar los elementos normativos sobre los temas de protección de la información.
- Gestionar los riesgos de seguridad y privacidad de la información, Seguridad Digital de manera integral.
- Mitigar los incidentes de Seguridad y Privacidad de la Información, Seguridad Digital de forma efectiva, eficaz y eficiente.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad, continuidad y no repudio de la información del Ministerio.
- Definir los lineamientos necesarios para el manejo de la información tanto física como digital en el marco de una gestión documental basada en Seguridad y Privacidad de la Información.
- Generar conciencia para el cambio organizacional requerido para la apropiación de la Seguridad y Privacidad de la Información como eje transversal del Ministerio.
- Dar cumplimiento a los requisitos legales y normativos en materia de Seguridad y Privacidad de la información, seguridad digital y protección de la información personal.
- Atender los requerimientos de seguridad de la información, de los diferentes órganos gubernamentales.

7. ALCANCE

El Plan de Seguridad y Privacidad de la información identifica e incluye los lineamientos para la gestión del ciclo (PHVA) de operación del modelo de seguridad y privacidad de la información (MSPI), el cual debe ser aplicado por todos los servidores públicos, contratistas y/o terceros de Metrolínea S.A.

8. MARCO LEGAL

Norma	Descripción
Política de seguridad y privacidad de la información de Función Pública – 2018.	La Política de Seguridad de la Información de (MIPG Administración Pública), con respecto a la protección de los activos de que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad dela Información.

Norma	Descripción
Manual de política de seguridad y privacidad de la información de Función pública – 2018.	Compendio de políticas aplican para todos los servidores públicos y contratistas de las entidades que procesan y/o manejan información de las entidades. Política pública de Seguridad Digital.
Decreto 103 de 2015,	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Manual Gobierno Digital.	Para la Implementación de la Estrategia de Gobierno Digital, entidades del orden nacional; Modelo de Seguridad de la Información para la Estrategia de Gobierno Digital.
Ley 1712 de 2014;	Por medio de la cual se crea la Ley de Transparencia y del derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
NTC/IEC ISO 27001:2013	Norma internacional que suministra los requisitos para implementar y mantener un sistema de gestión de seguridad de la información
Anexo A	Controles de seguridad de la información de la gestión de continuidad de negocio¨ de la norma ISO 27001
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581de 2012.
Decreto 2609 de 2012.	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 2693 de 2012	Estrategia de Gobierno en Línea. Ministerio de Tecnologías de la Información y las comunicaciones
Ley estatutaria 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales. Congreso de la República
Ley 1474 de 2011	Por la cual se dictan normas orientadas a fortalecer los mecanismos de prevención, investigación y sanción de actos de corrupción y la efectividad del control de la gestión pública. Disponible en Línea
Decreto 4632 de 2011	Por medio del cual se reglamenta parcialmente la Ley
1474 de 2011	Se refiere a la Comisión Nacional para la Moralización y la Comisión Nacional Ciudadana para la Lucha contra la Corrupción y se dictan otras disposiciones.
Ley 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.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado

Norma	Descripción
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.

9. POLÍTICA GENERAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE METROLÍNEA S.A. (ADOPTADA EN COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO DE DICIEMBRE 3 DE 2018)

La Política de Seguridad y Privacidad de la Información es la declaración general que representa la posición de METROLINEA S.A. respecto a la protección de los activos de información (los servidores públicos, contratistas, terceros, la información, los procesos, las tecnologías de información incluido el hardware y el software), que soportan los procesos de la Entidad y apoyan la implementación del Sistema de Gestión de Seguridad de la Información, por medio de la generación y publicación de sus políticas, procedimientos e instructivos, así como de la asignación de responsabilidades generales y específicas para la gestión de la seguridad de la información.

Para Metrolínea S.A. la información es un activo valioso para la toma de decisiones, la gestión del cambio y el conocimiento; así como la apropiación de la política de Gobierno Digital, para establecer una política de seguridad de la información que ha de brindar a los usuarios y ciudadanos las herramientas para la defensa de lo público.

La necesidad de mitigación de riesgos alrededor de la información requiere planes de manejo de incidentes y herramientas para respaldar las actividades ejecutadas en Metrolínea S.A considerando que las TIC son un proceso de apoyo a toda la entidad. Además de incentivar la cultura de seguridad de la información a los usuarios ante ataques informáticos, virus, robos o pérdidas de información.

Es de vital importancia la gestión del conocimiento y las revisiones de la política que lleven a una mejora continua para lograr un mejor desempeño de las actividades y la articulación de la normatividad colombiana e internacional en protección de datos, delitos informáticos y seguridad de la información además de tendencias tecnológicas que puedan ser implementadas entorno a la eficacia de las actividades relacionadas, considerando siempre los tres principios de la seguridad de la información: Confidencialidad, disponibilidad e integridad

10. OPERACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN –SGSI

11. COMITÉ INSTITUCIONAL DE GESTION Y DESEMPEÑO

Según la RESOLUCION 1905 DE 2019 de agosto 1 del Min TIC, el Comité Institucional de Gestión y Desempeño en el ARTÍCULO 9. FUNCIONES DEL COMITÉ MIG en su numeral 14. Dice "Son funciones del comité, Aprobar y hacer seguimiento a la implementación de políticas de gestión y directrices en materia de Estrategia de Gobierno Digital y Seguridad de la Información en la Entidad y al Plan Estratégico de Tecnologías Información" esto dentro del marco del Modelo Integrado de Gestión (MIG) el cual se alinea con el Modelo Integrado de Planeación y Gestión (MIPG) de acuerdo a sus cinco (5) dimensiones.

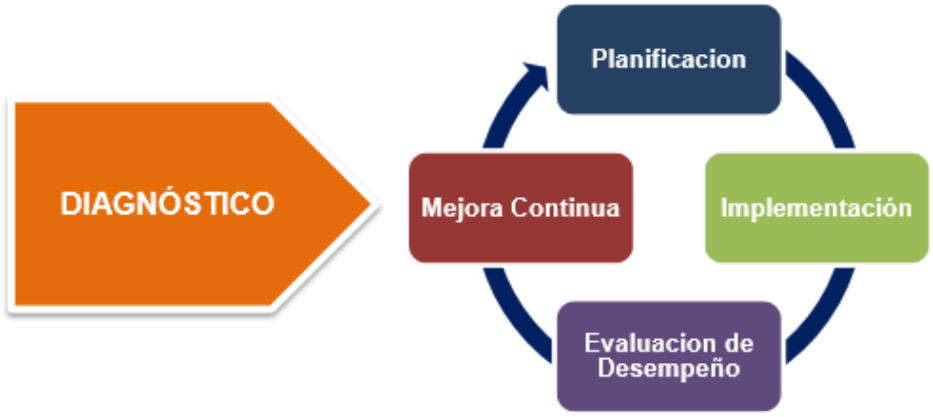
12. MODELO DE SEGURIDAD Y PRIVACIDAD – MSPI

El Modelo de Seguridad y Privacidad es un lineamiento publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, este es entregado a las entidades del Estado colombiano con el fin de que su adopción permita estar acorde con las buenas prácticas de seguridad y privacidad de la información, basado en norma 27001 del 2013, 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 una correcta gestión de la información. Metrolínea S.A. a través del comité Institucional de Gestión y Desempeño, impulsará la implementación del Modelo de Seguridad y Privacidad de la Información MSPI, en el contexto de las actividades globales de la entidad y de los riesgos que enfrenta.

Autopista Floridablanca N° 86-30, Estación Provenza Occidental, Barrio Diamante II
Teléfono: 6929824 Bucaramanga.
www.metrolinea.gov.co

12.1 METODOLOGIA ESTABLECIMIENTO MODELO DE SEGURIDAD

El modelo de seguridad de la información Metrolínea S.A. se estableció teniendo en cuenta las cinco (5) fases definidas en el ciclo de operación del Modelo de Seguridad y Privacidad de la Información, sin embargo para efectos de este plan de seguridad, se trabajaran las primeras tres etapas del modelo.



Ciclo de operación Modelo de Seguridad y Privacidad de la Información

12.2 Fase Diagnostico:

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.

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.	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.
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.

12.3 Fase Planificación (Planear)

En esta fase se establecen los objetivos a alcanzar y las actividades del proceso susceptibles de mejora, así como los indicadores de medición para controlar y cuantificar los objetivos.

META	ENTREGABLE
Objetivos, alcance y límites.	Documento con el alcance y límites de la seguridad de la información.
Políticas de seguridad de la información y tratamiento de la información personal	Documento con las Políticas de seguridad de la información y tratamiento de la información personal
Inventario de activos de información de TI.	Documento de inventario de activo de información de TI.
Acciones para tratar riesgos y oportunidades de seguridad de la información. Identificación y valoración de riesgos de o Tratamiento de riesgos.	Documento con el informe de análisis de riesgos, matriz de riesgos, plan de tratamiento de riesgos y declaración de aplicabilidad, revisado.
Toma de conciencia.	Documento plan de sensibilización, comunicación y capacitación de seguridad y privacidad de la información.

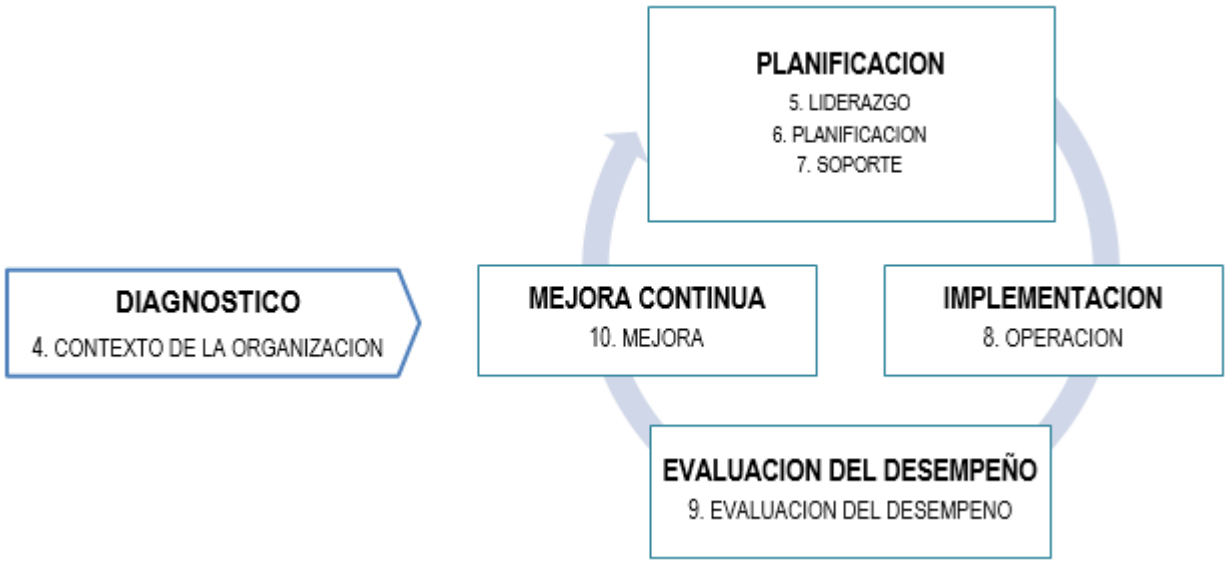
12.4 Fase Implementación (Hacer)

En esta fase se ejecuta el plan establecido que consiste en implementar las acciones para lograr mejoras planteadas.

META	ENTREGABLE
Planificación y control operacional.	Documento de Procedimientos De Seguridad De La Información
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
Implementación del plan de tratamiento de riesgos	Indicadores de gestión del MSPI.

12.5 ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION

Aunque en la norma ISO 27001:2013 no se determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de las modelos de gestión de la siguiente forma:



Norma ISO 27001:2013 alineado al Ciclo de mejora continua

A continuación, se muestra la relación entre las fases del ciclo de operación del Modelo de Seguridad y Privacidad de la Información (Diagnostico, Planificación e Implementación y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Fase	Capitulo ISO 27001:2013
Diagnostico	4. Contexto de la Organización
Planificación	5. Liderazgos 6. Planificación 7. Soporte
Implementación	8. Operación

- **Fase DIAGNOSTICO en la norma ISO 27001:2013.** En el capítulo 4 - Contexto de la organización de la norma ISO 27001:2013, se determina la necesidad de realizar un análisis de las cuestionas externas e internas de la organización y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesas de la organización en el alcance del modelo de seguridad de la información.

- **Fase PLANEACION en la norma ISO 27001:2013.** En el capítulo 5 - Liderazgo, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la organización asegure la asignación de los recursos para la seguridad de la información y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen. En el capítulo 6 - Planeación, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento. En el capítulo 7 - Soporte se establece que la

Autopista Floridablanca N° 86-30, Estación Provenza Occidental, Barrio Diamante II
Teléfono: 6929824 Bucaramanga.
www.metrolinea.gov.co

organización debe asegurar los recursos necesarios para el establecimiento, implementación y mejora continua del modelo de seguridad de la Información.

- **Fase IMPLEMENTACION en la norma ISO 27001:2013.** En el capítulo 8 - Operación de la norma ISO 27001:2013, se indica que la organización debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

12.6 PLAN DE SEGURIDAD DE LA INFORMACION

Fase	Actividad	Estado	feb	Mar	abr	may	jun	jul	ago	sep	oct	nov	dic
Diagnostico	1. Levantamiento de mapa de red de infraestructura Tecnológica.		x										
	2. Inventario de contraseñas gestionadas y Aseguradas.		x										
	3. Revisión de políticas existentes de seguridad y Privacidad.		x										
	4. Levantamiento de controles existentes		x										
Planificación	1. Elaborar el inventario de activos de información de TI		x										
	2. Selección de activos de información con riesgo en privacidad de datos personales.		x										
	3. Diseño de matriz de riesgo de seguridad y privacidad de activos de información de TI			x	x								
	4. Elaboración de aplicabilidad de norma ISO27000 (SoA)			x	x								
	5. Plan de tratamiento de riesgos.			x	x								
	6. plan de sensibilización, comunicación y capacitación de seguridad y privacidad de la información.			x	x								
Implementación	1. Elaboración y Revisión del documento de procedimientos y operaciones del SGSI.			x	x								
	2. Revisión de la declaración de aplicabilidad.			x	x								
	3. Aplicación de controles por recursos humanos y áreas seguras.				x	x							
	4.Aplicación de controles de red y servidores				x	x							
	5. Aplicación de normatividad legal de protección de datos personales				x	x							
	8. Análisis de impacto de los servicios de TI en el área administrativa que afectan el negocio				x	x							
	9. Elaboración del Plan de continuidad de los servicios de TI en el área Administrativa					x	x						
	10. Elaboración de la guía para la gestión de incidentes de seguridad de la información					x	x						
	11. Elaboración de indicadores del MSPI					x	x						

Autopista Floridablanca N° 86-30, Estación Provenza Occidental, Barrio Diamante II
Teléfono: 6929824 Bucaramanga.
www.metrolinea.gov.co