PLAN ESTRATÉGICO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN 2024

METROLÍNEA S.A.

Tabla de contenido

1. OBJETIVO

Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables, a partir de la implementación de las estrategias de seguridad digital definidas en este documento para las vigencias 2024-2025.

1.1 OBJETIVOS ESPECÍFICOS

- Definir y establecer la estrategia de seguridad digital de la entidad.
- Definir y establecer las necesidades de la entidad para la implementación del Sistema de Gestión de Seguridad de la Información.
- Priorizar los proyectos a implementar para la correcta implementación del SGSI.
- Planificar la evaluación y seguimiento de los controles y lineamientos implementados en el marco del Sistema de Gestión de Seguridad de la Información.

2. ALCANCE

El Plan Estratégico de Seguridad de la Información al buscar la implementación del Sistema de Gestión de Seguridad de la Información y la estrategia de seguridad digital de la entidad, comparte el alcance definido dentro de la Política General de Seguridad de la Información, donde se indica que se tendrán en cuenta comprende a los siguientes procesos de la entidad; Gerencia del talento Humano, Gestión Documental, Servicio al Ciudadano, Gestión Presupuestal, Tesorería, Gestión Contable, Gestión Contractual, Gestión Jurídica.

3. DOCUMENTOS DE REFERENCIA

El Plan Estratégico de Seguridad de la Información se basa en los siguientes documentos, normas y lineamientos para su estructura y funcionamiento:

- 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", donde se encuentra el presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.
- Resolución 500 de 2021. "Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital".
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

4. ESTADO ACTUAL DE LA ENTIDAD RESPECTO AL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

(En esta sección, se debe indicar y documentar de la forma más estratégica posible el estado actual de la entidad respecto a la implementación de los lineamientos de seguridad de la información requeridos por el MSPI.

Esto permitirá a la entidad establecer la línea base de donde se encuentra la entidad y así proyectar hacía que punto desea llegar con base a las actividades definidas dentro del PESI.

Para esto, la entidad puede tomar como base la sección PORTADA del INSTRUMENTO DE EVALUACIÓN MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN. También podrá emplear insumos como el AUTODIAGNÓSTICO DE GOBIERNO DIGITAL o la MEDICIÓN FURAG para los temas de SEGURIDAD DE LA INFORMACIÓN).

5. ESTRATEGIA DE SEGURIDAD DIGITAL

Metrolinea S.A. establecerá una estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información, teniendo como premisa que dicha estrategia gira entorno a la implementación del Modelo de Seguridad y Privacidad de la Información -MSPI, así como de la guía de gestión de riesgos de seguridad de la información y del procedimiento de gestión de incidentes que debe establecerse (Ver Resolución 500 de 2021).

Por tal motivo, LA ENTIDAD define las siguientes 5 estrategias específicas, que permitirán establecer en su conjunto una estrategia general de seguridad digital:

5.1 DESCRIPCIÓN DE LAS ESTRATEGIAS ESPECÍFICAS (EJES)

A continuación, se describe el objetivo de cada una de las estrategias específicas a implementar, alineando las actividades a lo descrito dentro del MPSI y la resolución 500 de 2021:

- **Liderazgo de seguridad de la información**

Asegurar que se establezca el Modelo de Seguridad y Privacidad de la Información (MSPI) a través de la aprobación de la política general y demás lineamientos que se definan buscando proteger la confidencialidad, integridad y disponibilidad de la información teniendo como pilar fundamental el compromiso de la alta dirección y de los líderes de las diferentes dependencias y/o procesos de la Entidad a través del establecimiento de los roles y responsabilidades en seguridad de la información.

- **Gestión de riesgos**

Determinar los riesgos de seguridad de la información a través de la planificación y valoración que se defina buscando prevenir o reducir los efectos indeseados tendiendo como pilar fundamental la implementación de controles de seguridad para el tratamiento de los riesgos.

- **Concientización**

Fortalecer la construcción de la cultura organizacional con base en la seguridad de la información para que convierta en un hábito, promoviendo las políticas, procedimientos, normas, buenas prácticas y demás lineamientos, la transferencia de conocimiento, la asignación y divulgación de responsabilidades de todo el personal de la entidad en seguridad y privacidad de la información.

- **Implementación de controles**

Planificar e implementar las acciones necesarias para lograr los objetivos de seguridad y privacidad de la información y mantener la confianza en la ejecución de los procesos de la Entidad, se pueden subdividir en controles tecnológicos y/o administrativos.

- **Gestión de incidentes**

Garantizar una administración de incidentes de seguridad de la información con base a un enfoque de integración, análisis, comunicación de los eventos e incidentes y las debilidades de seguridad en pro de conocerlos y resolverlos para minimizar el impacto negativo de estos en la Entidad.

5.2 PORTAFOLIO DE PROYECTOS / ACTIVIDADES:

Para cada estrategia específica, Metrolinea S.A. define los siguientes proyectos y productos esperados, que tienen por objetivo lograr la implementación y mejoramiento continuo del Sistema de Gestión de Seguridad de la Información (SGSI):

Liderazgo de seguridad de la información

PROYECTO 1:
Desarrollar e implementar una política de seguridad

PROYECTO 2:
Definición de Roles y Responsabilidades de Seguridad de la Información.

Gestión de riesgos

PROYECTO 1:
Identificar, valorar y clasificar los riesgos asociados a los activos de información.

PROYECTO 2:
Definir planes de tratamiento de riesgos de seguridad.
Matriz de riesgos de seguridad digital.

Concientización

PROYECTO 1:
Establecer desde el inicio de cada año la planeación de sensibilización para todo el año.

PROYECTO 2:
Realizar jornadas de sensibilización a todo el personal.

PROYECTO 3:
Realizar trasferencia de conocimiento a colaboradores de la Entidad a través de cursos especializados en diferentes temas.

PROYECTO 4:
Medir el grado de sensibilización a toda la Entidad.

5.3 CRONOGRAMA DE ACTIVIDADES:

El responsable de seguridad de la información, con base a los proyectos definidos en la sección anterior, deberá establecer un cronograma de actividades donde se evidencie como se llevarán a cabo cada uno de los proyectos previstos. Las actividades podrán desarrollarse de forma secuencial o paralela según se considere.

AÑO 2023			
TRIMESTRE 1	**TRIMESTRE 2**	**TRIMESTRE 3**	**TRIMESTRE 4**
		Definir y formalizar un procedimiento de Gestión de Incidentes seguridad de la información.	Capacitar al personal en la gestión de incidentes de seguridad de la información.
Realizar diagnóstico seguridad y privacidad			
Identificación de activos procesos misionales	Implementación de solución WAF		Gestión de Riesgos de Seguridad
Desarrollo Plan de Sensibilización 2024	Adquisición e implementación Sistema de Análisis de Vulnerabilidades		

CUADRO DE APROBACIÓN			
	CARGOS	**NOMBRE**	**FECHA**
ELABORADO POR:	Directora Administrativa	Natalia Lucía Rodríguez	01/2024
REVISADO POR:	Directora Administrativa	Natalia Lucía Rodríguez	01/2024
APROBADO POR:		Comité Institucional de Gestión y Desempeño	30/01/2024

CONTROL DE CAMBIOS

VERSIÓN	FECHA DE REVISIÓN	SOLICITUD NO.	DESCRIPCIÓN DEL CAMBIO
00	01/2024	01	Emisión inicial. El Plan Estratégico de Seguridad y Privacidad de la Información de la vigencia 2024 Fortalecer la integridad, confidencialidad y disponibilidad de los activos de información de la Entidad, para reducir los riesgos a los que está expuesta la organización hasta niveles aceptables. Solicitud Realizada por Natalia Lucía Rodríguez Moreno, Directora Administrativa