Contenido

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

1 Propósito

Presentar el Plan de Seguridad y Privacidad de La Información para el Metro de Medellín Ltda., el cual contiene la hoja de ruta para la implementación y sostenibilidad del Modelo de Seguridad y Privacidad de la Información, alineado con el estándar propuesto por el Ministerio de las Tecnologías de Información y las Comunicaciones.

2 Justificación

El Metro de Medellín Ltda., a partir de la publicación del Decreto 612 de 2018 por parte del Departamento Administrativo de Función Pública y por el cual se fijan directrices para la integración de los planes estratégicos institucionales al Plan de Acción por parte de las entidades del Estado, conformó un equipo de trabajo interdisciplinario el cual inicia desde el año 2020 a trabajar en el plan inicial para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, siguiendo la metodologías propuesta por el Ministerio de Tecnologías de Información y Comunicaciones, durante la ejecución del plan inicial la Empresa establece en su plan estratégico 2021-2025 el objetivo estratégico “Fortalecer la excelencia organizacional en la era de la transformación digital”, en el cual se establece iniciativa estratégica de implementar del Modelo de Seguridad y Privacidad de la Información, lo que lleva a la Empresa a incorporar el rol del oficial de seguridad de la información, buscando obtener las competencias requeridas para la implementación y actualización del Plan de Seguridad y Privacidad de la Información de forma transversal .

3 Alcance y Vigencia

Este plan tendrá vigencia a partir de diciembre de 2023 y su finalización se estima en diciembre 2024, esto teniendo en cuenta que el presente documento es actualizado cada año y se incluyen solo las actividades que están planeadas para el año vigente, no obstante el plan general para el funcionamiento de todo el ciclo del MSPI se estima para el año 2025, su alcance para el año 2024 estará enmarcado en la totalidad de las actividades descritas en las fases de planificación e implementación de la estrategia adoptada por la Empresa desde del ciclo de operación del Modelo de Seguridad y Privacidad de la Información entregado por MINTIC.

4 Objetivo General

Apoyar al cumplimiento de los objetivos de la Empresa desde la iniciativa estratégica Seguridad y privacidad de la información que se encuentra en el Direccionamiento Estratégico 2021-2025.

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

4.1 Objetivos Específicos

- Identificar el estado actual en materia de seguridad y privacidad de la información, como también el nivel de madurez y hacer el levantamiento de la información requerida para la fase de planificación.

- Identificar el contexto actual de la Empresa referente a seguridad y privacidad de la información, identificando las necesidades y expectativas de las partes interesadas y el alcance del MSPI.

- Actualizar las políticas necesarias y requeridas por el Modelo de Seguridad y Privacidad de la Información, como también los roles y responsabilidades.

- Implementar la metodología de gestión de activos de información.

- Implementar metodología de gestión de riesgos para los activos de información.

- Integrar el MSPI en el Sistema de Gestión Integral de la Empresa.

- Fortalecer la cultura de seguridad y privacidad de la información en los Servidores Metro, aprendices, practicantes, proveedores y clientes.

- Implementar controles asociados a cada una de las causas de los riesgos identificados en los activos de información.

- Definir indicadores de gestión.

- Hacer monitoreo, medición, análisis y evaluación del desempeño del MSPI

- Planear las auditorías internas al Modelo de Seguridad y Privacidad de la Información MSPI.

- Entregar resultados a la alta dirección.

- Implementar las acciones correctivas resultantes de seguimientos internos o externos al Modelo de Seguridad y Privacidad de la Información.

5 Marco Normativo

- Decreto 1499 de 2017: Sistema Integrado de Planeación y Gestión y actualización del modelo para su implementación, denominado “Modelo Integrado de Planeación y Gestión –MIPG”.

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

- Decreto 612 de 2018 del Departamento Administrativo de Función Pública.
- Manual para la Implementación de la Política de Gobierno Digital.
- Decreto 1078 de 2015: Decreto Único Reglamentario del sector TIC.
- Decreto 1083 de 2015: Decreto Único Reglamentario del Sector de Función Pública.
- Decreto 1413 de 2017: Servicios ciudadanos digitales.
- Decreto 1008 de 2018: Lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3854 Política Nacional de Seguridad Digital.
- CONPES 3995 Política Nacional de Confianza y Seguridad Digital.
- Resolución 00500 del 10 de marzo de 2021 del Ministerio de las TIC cuyo objeto es "establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital".
- ISO/CEI 27001- 2022: Es un estándar para los Sistemas Gestión de la Seguridad de la Información que permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos.

6 Recursos

- Profesional 1 (Oficial de seguridad de la información)
- Profesionales 1 Gestión de Tecnologías de Información (Ciberseguridad)
- Profesional 1 de Sistema Operativo
- Mesa de Seguridad y Privacidad de la Información.
- Mesa de Política Gobierno Digital

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

7 Responsables

A: Aprobador R: Responsable I: Informado C: Consultado					
Responsable	**ROLES**				**Responsabilidades**
	A	**R**	**I**	**C**	
Comité Institucional de Gestión y Desempeño	X				• Aprobar las políticas y el plan general de seguridad y privacidad de la información y todos los entregables que por normatividad se requieran.
Mesa de Política Gobierno Digital	X				• Aprobar los entregables resultantes de las actividades registradas en el plan detallado del MSPI
Profesional 1 (Oficial de seguridad de la información)		X			• Realizar los diagnósticos del estado del Modelo de Gestión de Seguridad y Privacidad de la Información. • Diseñar el plan detallado del MSPI • Identificar las necesidades de recursos para la implementación del Modelo de Gestión de Seguridad y Privacidad de la Información (MGSPI). • Definir y coordinar el plan de trabajo para la implementación del Modelo de Gestión de Seguridad y Privacidad de la Información. • Planear y ejecutar los proyectos de seguridad y privacidad de la información en búsqueda del cumplimiento de los objetivos. • Coordinar y dirigir acciones específicas que ayuden a proveer un ambiente seguro y establecer los recursos de información que sean consistentes con las metas y objetivos de la Empresa. • Diseñar metodologías y procesos específicos para la seguridad de la información. • Promover y coordinar la identificación, formulación y evaluación de planes de acción para mitigar los riesgos. • Hacer seguimiento periódico al MSPI y según los resultados de este seguimiento definir las acciones pertinentes. • Identificar e implementar las acciones para el mejoramiento continuo del MSPI.
Mesa de Seguridad y Privacidad de la Información		X	X		• Revisar y hacer observaciones a los diagnósticos del estado del Modelo de Gestión de Seguridad y Privacidad de la Información. • Revisar y hacer observaciones al plan detallado del MSPI • Identificar las necesidades de recursos para la implementación del Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI).

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

					• Participar en la definición y coordinación del plan de trabajo para la implementación del Modelo de Gestión de Seguridad y privacidad de la Información. • Acompañar e impulsar el desarrollo de proyectos de seguridad y privacidad de la información. • Revisar y apoyar en la definición de metodologías y procesos específicos para la seguridad de la información. • Participar en la identificación, formulación y evaluación de planes de acción y acciones de mejora que busquen la mitigación del riesgo y la mejora continua.

8 Estrategia de seguridad y privacidad de la información

El Plan de Seguridad y Privacidad de la Información se desarrollará con base en las cinco fases planteadas en el modelo propuesto por el Ministerio de las Tecnologías de Información y las Comunicaciones - MINTIC.

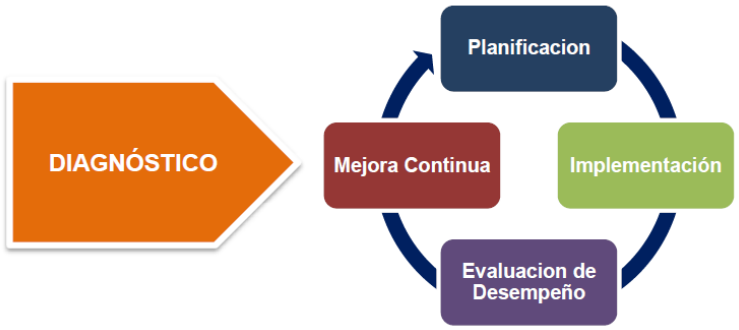

Imagen 1. Fases del modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de Información y Comunicaciones.

9 Diagnóstico Inicial

En el año 2023 con la incorporación del Oficial de seguridad de la información se realizó nuevamente el autodiagnóstico del estado actual a nivel de seguridad de la información incluyendo requisitos de ciberseguridad, buscando complementar la lista de actividades que se incluyen en el plan detallado del MSPI

El detalle del diagnóstico realizado con corte a enero 2024 se encuentra registrado en el documento interno de la Empresa denominado “GAP del MSPI 2024”.

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

10 Proyectos

- Identificación y clasificación de activos de información de forma transversal.
- Matriz de riesgos y controles de seguridad de la información.
- Plan de sensibilización y comunicación del MSPI.
- Automatización de la gestión de las vulnerabilidades en las Tecnologías de la Operación “OT” y las Tecnologías de la Información “IT”.

11 Cronograma

A continuación, se detalla el cronograma vigente para el año 2024:

Fase	Estado	Fecha de implementación	Observaciones
Planificación	En curso	Diciembre 2024	Actualización de las necesidades y expectativas de las partes interesadas.
Planificación	En curso	Diciembre 2024	Actualización de las políticas de seguridad de la información para la Empresa, así como también los roles y responsabilidades
Planificación	En curso	Diciembre 2024	Implementación de la metodología de gestión de riesgos para los activos de información.
Planificación	En curso	Diciembre 2024	Actualización de objetivos de seguridad y privacidad de la información.
Planificación	En curso	Diciembre 2024	Actualización y ejecución del plan de sensibilización y comunicación, para las partes interesadas.
Implementación	En curso	Diciembre 2024	Asignación de controles a las causas registradas dentro de la matriz de riesgos de seguridad y privacidad de la información
Implementación	En curso	Diciembre 2024	Actualización del plan de tratamiento de riesgos según la metodología definida.
Implementación	En curso	Diciembre 2024	Definición de indicadores de gestión

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

12 Análisis presupuestal

Se define que la fase de planificación estimada para el año 2024 se puede realizar con recursos que ya se tienen desde el capital humano y que se encuentran asignados al mecanismo de coordinación Mesa de seguridad y privacidad de la información, para la fase de implementación se tendrá como prioridad aquellos controles que se puedan realizar con tecnologías y procesos que ya se tengan, para aquellos que requieran inversión o gasto serán planificados en el presupuesto del siguiente periodo para el año 2025.

El proyecto automatización de la gestión de las vulnerabilidades en las tecnologías de la operación "OT" y las tecnologías de la información "IT", ya cuenta con presupuesto asignado para el año 2024.

13 Anexos

La Empresa cuenta con una documentación interna asociada al Plan de Seguridad y Privacidad de la Información que son:

- Plan detallado del MSPI.xlsx
- Plan sensibilización y comunicación MSPI.xlsx
- GAP del MSPI 2024 .xlsx

14 Definiciones

- **Activos de información:** cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Riesgo:** probabilidad de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.
- **Evento de seguridad de la información:** situación no deseada que involucra uno o varios activos de información que si no es atendido de forma oportuna puede afectar la disponibilidad, integridad o confidencialidad de la información corporativa y comprometer las operaciones del negocio.
- **Incidente de seguridad de la información:** uno o varios eventos indeseados o inesperados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información.
- **Integridad:** característica de la información por la cual solo es modificada por personas o sistemas autorizados y de una forma permitida.

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

- **Disponibilidad:** característica de la información por la cual solo pueden acceder las personas autorizadas cuando sea necesario.

- **Confidencialidad:** propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados.

- **Información:** cualquier forma de registro, sea electrónico, óptico, magnético, impreso o en otros medios, previamente procesado a partir de datos u otra información, que puede ser almacenado, procesado y distribuido, utilizado para análisis, estudios, toma de decisiones, ejecución de una transacción o entrega de un servicio.

- **Seguridad:** capacidad de las redes o de los sistemas de información para resistir, con un determinado nivel de confianza, a los accidentes o acciones ilícitas o malintencionadas que comprometan la disponibilidad, integridad y confidencialidad de los datos almacenados o transmitidos y de los servicios que dichas redes y sistemas ofrecen o hacen accesibles.

- **Seguridad de la información:** preservación de la confidencialidad, integridad y disponibilidad de la información.

- **Activo de información:** recurso que genera, procesa, transporta y/o resguarda datos necesarios para la operación y el cumplimiento de los objetivos del negocio.

- **MINTIC:** Ministerio de Tecnologías de la Información y las Comunicaciones.

- **ISO/IEC 27001:2022:** Especifica los requisitos para establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información dentro del contexto de la organización. También incluye requisitos para la evaluación y el tratamiento de los riesgos de seguridad de la información adaptados a las necesidades de la organización. Los requisitos establecidos en ISO/IEC 27001:2013 son genéricos y están destinados a ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

15 Control de cambios

Versión modificada	Descripción del cambio
NA	NA.
NA	NA.
NA	NA.
NA	NA.

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.

16 Responsabilidades

Documentador	Revisor	Aprobador
Profesional 1 Oficial de Seguridad de la Información, Carlos Alberto Sepúlveda Ramírez	Mesa de Política Gobierno Digital	Comité Institucional de Gestión y Desempeño

Prohibida la copia y reproducción total o parcial del presente documento sin autorización expresa de Administración Documental del Metro de Medellín Ltda.