Contenido

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 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 institucionales y estratégicos 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 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 una iniciativa estratégica denominada, "excelencia organizacional en la era de la transformación digital", la cual establece la implementación del modelo de seguridad y privacidad de la información como una acción estratégica, lo que lleva a la empresa a incorporar el rol del oficial de seguridad de la información buscando obtener las competencias adecuadas 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 2024 y su finalización se estima en diciembre 2025, su alcance estará enmarcado en la totalidad de las actividades descritas en las fases de planificación, operación, evaluación del desempeño y mejoramiento continuo de la estrategia adoptada por la empresa desde del ciclo de operación del modelo se seguridad y privacidad de la información entregado por MINTIC.

4 Objetivo General

Apoyar al cumplimiento de los objetivos de la empresa desde la iniciativa "excelencia organizacional en la era de la transformación digital" que se encuentra en el plan estratégico 2021-2025

4.1 Objetivos Específicos

- Identificar el estado actual en materia de seguridad y privacidad de la información, así como también el nivel de madurez y hacer el levantamiento de la información requerida para la fase de planificación.
- Identificar el contexto 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.
- Establecer las políticas necesarias y requeridas por el modelo de seguridad y privacidad de la información, así como también los roles y responsabilidades.
- Implementar 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 documental 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 auditorias 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 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 1499 de 2017: Sistema Integrado de Planeación y Gestión y actualización del modelo para su implementación, denominado “Modelo Integrado de Planeación y Gestión –MIPG”.
- 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)
- Mesa de Seguridad y Privacidad de la Información.
- Mesa de Política Gobierno Digital

7 Responsables

Responsable	ROLES				Responsabilidades
	A	R	I	C	
Comité institucional de Gestión y Desempeño	X				Asegurar la implementación, desarrollo, supervisión y mejora de las políticas de gestión y desempeño, así como las directrices impartidas por la presidencia de la república y el ministerio de tecnología de la información y las comunicaciones en materia seguridad digital y de la información Aprobación y seguimiento de las políticas de seguridad y privacidad de la información. Aprobar acciones, metodologías, procesos específicos y mejores prácticas para la implementación y sostenibilidad del modelo de seguridad y privacidad de la información. Aprobación y seguimiento a los planes, programas, proyectos, estrategias y herramientas necesarias para garantizar la aplicación de la normatividad vigente y que haga referencia al cumplimiento, control, protección y gestión de la información de datos personales administrados por la empresa.
Mesa de Política Gobierno Digital	X	X			Revisar los informes de cumplimiento a las políticas, controles y procedimientos referentes a seguridad y privacidad de la información. Revisar los diagnósticos del estado de la seguridad de la información y apoyar el cierre de brechas. Acompañar e impulsar el desarrollo de proyectos de seguridad y privacidad de la información. 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. Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos Fomentar la implementación de la Política de Gobierno Digital Promover la difusión y sensibilización de la seguridad de la información dentro de la empresa. Definir la estrategia informática que permita lograr los objetivos y minimizar los riesgos de la empresa Seguir y controlar la estrategia de TI, que permita el logro de los objetivos y la minimización de los riesgos del componente de TI. Monitorear la prestación del servicio y la adquisición de bienes y/o servicios relacionados y requeridos para garantizar la seguridad de información.
Profesional 1 (Oficial de seguridad de la información)		X			Liderar la implementación del Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Implementar mecanismos de monitoreo respecto a la implementación y funcionamiento del

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Definir, elaborar e implementar las políticas, procedimientos, estándares o documentos para la operación del Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Asesorar a los procesos y/o proyectos en materia de seguridad y privacidad de la información. Liderar la gestión de riesgos de seguridad y privacidad de la información, así como la definición de los controles correspondientes para su mitigación y seguimiento al plan de tratamiento de riesgos, de acuerdo con las metodologías establecidas. Definir e implementar en coordinación con los procesos de la Empresa, las estrategias de sensibilización, divulgación y fortalecimiento de la cultura de seguridad y privacidad de la información para los empleados y contratistas. Velar por el mejoramiento continuo del Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Presentar informes y reportes a los órganos de gobierno, órganos de control, autoridades y procesos internos respecto al Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Tramitar el diseño y la implementación de la estrategia de seguridad de la información y protección de la privacidad alineadas con los objetivos estratégicos. Tomar las medidas preventivas, correctivas o disuasorias necesarias para la gestión del Modelo de Gestión de Seguridad y Privacidad de la Información (MSPI). Asesorar a la empresa en el diseño, implementación y mantenimiento del Modelo de Seguridad y privacidad de la Información de conformidad con la regulación vigente. Poner en conocimiento de la empresa, las políticas aprobadas por el comité que impacten de manera transversal a la misma. Identificar la brecha entre el Modelo de seguridad y privacidad de la información y la situación actual de la empresa. Realizar la estimación, planificación y seguimiento cronograma de la implementación del MSPI. De acuerdo con las solicitudes realizadas por los proyectos y/o procesos, realizar el acompañamiento correspondiente en materia de seguridad y privacidad de la información.

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					Apoyar a los procesos de la empresa en los planes de mejoramiento para dar cumplimiento a los planes de acción en materia de seguridad y privacidad de la información. Definir, socializar el procedimiento de Gestión de Incidentes de seguridad de la información en la empresa. Poner en conocimiento de las dependencias con competencia funcional cuando se detecten irregularidades, incidentes o prácticas que atentes contra la seguridad y privacidad de la información de acuerdo con la normativa vigente. Supervisar la respuesta a incidentes, así como la investigación de violaciones de la seguridad, ayudando con las cuestiones disciplinarias y legales necesarias Supervisar pruebas de vulnerabilidad sobre los diferentes servicios tecnológicos para detectar vulnerabilidades y oportunidades de mejora a nivel de seguridad de la información. Establecer los requerimientos mínimos de seguridad que deberán cumplir los sistemas de información a desarrollar, actualizar o adquirir dentro de la empresa. Apoyar la implementación segura de los sistemas de información, de acuerdo con el modelo de seguridad y privacidad de la información. Supervisar que se garantice la confidencialidad, integridad y disponibilidad de la información a través de los distintos componentes de información implementados. Supervisar los resultados del plan de formación y sensibilización establecido para la empresa, con el fin de identificar oportunidades de mejora. Participar en la elaboración de los planes de gestión de cambio, garantizando la inclusión del componente de seguridad de la información en la implementación de los proyectos de TI.
Mesa de Seguridad y Privacidad de la Información		X	X		Oficiar como consultores de primer nivel en cuanto a las dudas técnicas y de procedimiento que se puedan suscitar en el desarrollo del proyecto. Participar en la identificación de necesidades en recursos para la implementación del Modelo de Gestión de Seguridad y Privacidad de la Información (MGSPI). Participar en el diseño de las metodologías y procesos específicos para la seguridad de la información. Participar en la identificación, formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.

Responsable	ROLES				Responsabilidades
	A	R	I	C	
					Participar en las revisiones periódicas del MSPI y sus acciones de mejora continua Promover la difusión y sensibilización del MSPI dentro de la Empresa. Apoyar al líder de proyecto en cada una de las tareas descritas en el plan de implementación Ayudar al líder de proyecto designado, en la gestión de proveedores de tecnología e infraestructura. Asistir a las reuniones de seguimiento o de cualquier otra naturaleza planeadas por el líder de proyecto
A: Aprobador R: Responsable I: Informado C: Consultado					

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.

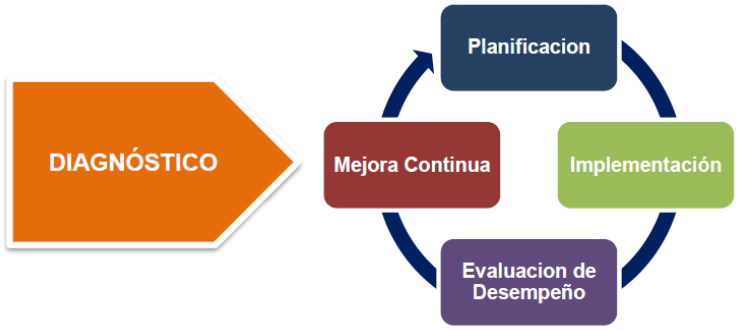

Imagen 1. Fases del modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de Información y Comunicaciones.

9 Diagnóstico Inicial

En el año 2024 se actualiza 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 Modelo de seguridad y privacidad de la información.

El detalle del diagnóstico realizado y la actualización con corte a diciembre 2024 se encuentra registrado en el documento interno “Diagnóstico Seguridad y Privacidad de la Información Metro de Medellín 2024”.

10 Proyectos

- Identificación y clasificación de activos de información de forma transversal en todos los procesos y áreas de la empresa.
- Matriz de riesgos y controles de seguridad de la información.
- Plan de sensibilización y comunicación del Modelo de seguridad y privacidad de la información.

11 Cronograma

A continuación, se comparte el cronograma de alto nivel vigente para 2024:

Fase	Estado	Fecha de implementación	Observaciones
Planificación	En proceso	Febrero 2025	Actualización del Documento donde se establecen las políticas generales de seguridad de la información para la empresa.
Planificación	En curso	Febrero 2025	Actualización de roles y responsabilidades de seguridad y privacidad de la información.
Planificación	En curso	Febrero 2025	Definición y documentación del alcance del modelo de seguridad y privacidad de la información.
Planificación	En curso	Junio 2025	Definición de objetivos de seguridad y privacidad de la información.
Planificación	En curso	Enero 2025	Construcción y ejecución del plan de sensibilización y comunicación, tomando como referencia las necesidades de cada parte interesada.
Implementación	En curso	Diciembre 2025	Ejecución del ciclo completo para la gestión de riesgos de seguridad de la información sobre los activos de información críticos registrados en el inventario de activos de información.
Implementación	En curso	Julio 2025	Definición de indicadores de gestión

12 Análisis presupuestal

Se define que la fase de planificación se puede realizar con recursos que ya se tienen desde el capital humano y que se encuentran asignados a la mesa técnica de seguridad de la información, para la fase de operación tendremos como prioridad aquellos controles que se puedan realizar con tecnologías y procesos existentes en la Empresa, para aquellos que requieran inversión o gasto y que estén registrados como planes de tratamiento a los riesgos serán analizados y planificados en el presupuesto 2026.

13 Anexos

- Plan detallado del MSPI.xlsx
- Plan sensibilización y comunicación MSPI.xlsx
- Diagnóstico Seguridad y Privacidad de la Información Metro de Medellín 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:** Es la 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:** Es una 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.
- **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.[1]
- **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:** es la 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.[2]

15 Control de cambios

Versión modificada	Descripción del cambio
NA	Se crea el plan estratégico de seguridad y privacidad de la información para el año 2025.

16 Responsabilidades

Documentador	Revisor	Aprobador
Profesional 1 Oficial de seguridad de la información	Jefe de Administración de Riesgos	Comité Institucional de Gestión y Desempeño