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 modelo propuesto por el Ministerio de las Tecnologías de Información y las Comunicaciones, MSPI.

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 con el cual construyó la primera versión del Plan de Seguridad y Privacidad de la Información en el cual se contempló desde sus inicios el desarrollo de un plan de acción por fases con actividades a ejecutar desde enero 2019 siguiendo la metodologías propuesta por el Ministerio de Tecnologías de Información y Comunicaciones en el Modelo de Seguridad y Privacidad de la Información, MPSI.[1]

3 Alcance y Vigencia

Este plan tendrá vigencia a partir de diciembre de 2018 y su finalización se estima en 2025, su alcance es la implementación del Modelo de Seguridad y Privacidad de la Información en La Empresa.

4 Objetivo General

Elaborar el plan de seguridad y privacidad de la información siguiendo las recomendaciones de la norma ISO27001:2013 y del modelo definido por Ministerio de las Tecnologías de Información y las comunicaciones, alineado con el plan estratégico 2021- 2025 de La Empresa.

4.1 Objetivos Específicos

- Identificar la situación actual en materia de seguridad y privacidad de la información.
- Definir, implementar y socializar políticas, controles, lineamientos, buenas prácticas y recomendaciones frente a la Seguridad y Privacidad de la Información.
- Fortalecer la cultura de seguridad y privacidad de la información en los servidores Metro, aprendices, practicantes, proveedores y clientes.
- Fomentar la gestión de riesgos de seguridad de la información al interior de La Empresa.

[1] https://gobiernodigital.mintic.gov.co/seguridadyprivacidad/704/articles-162621_Modelo_de_Seguridad_y_Privacidad__MSPI.pdf

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 27001- 2013: 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

- Líder de seguridad de la información o quien haga sus veces
- Mesa de Seguridad y Privacidad de la Información, conformada por personal de las diferentes áreas definidas.

7 Responsables

Responsable	ROLES				Responsabilidades
	A	R	I	C	
Comité institucional de Gestión y Desempeño	X				Aprobar el diagnóstico del estado actual de seguridad y privacidad de la información en la empresa y actualizaciones de este. Aprobar Plan de Seguridad y Privacidad de la Información y los recursos requeridos para su ejecución.
Mesa de Política Gobierno Digital	X	X			Aprobar los entregables resultantes de la ejecución del plan de acción. Asignar los recursos necesarios para cumplir con las actividades establecidas en el plan de acción.
Mesa de Seguridad y Privacidad de la Información		X			Realizar el diagnóstico de seguridad y privacidad de la información y construir el plan de seguridad y privacidad de la información

A: Aprobador R: Responsable I: Informado C: Consultado

8 Metodología de Implementación

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.

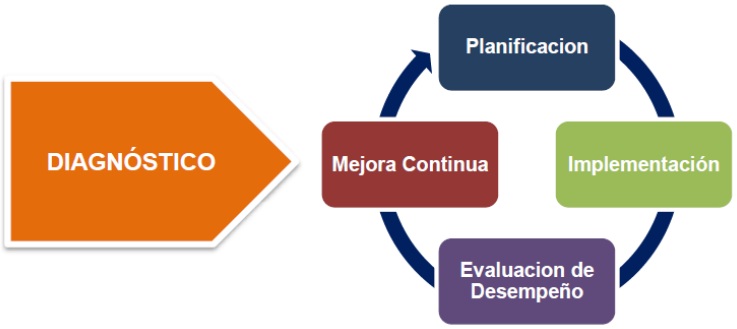

Imagen 1. Fases del modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de Información y Comunicaciones.

9 Diagnóstico Inicial

La Empresa en el año 2019 realizó el autodiagnóstico de seguridad y privacidad de la información apoyado en las herramientas que proporciona el MSPI, el cual arrojó una lista de oportunidades de mejora. En 2020 y con la conformación de la mesa técnica de seguridad y privacidad de la información, fue revisado nuevamente dicho diagnóstico y se validó su resultado, también fueron revisados los resultados de otros ejercicios de revisión y auditoría interna realizadas en La Empresa, así como los resultados de análisis de vulnerabilidades técnicas sobre los sistemas de información.

El resultado del anterior ejercicio fue la definición del plan de acción para la implementación del Modelo de Seguridad y Privacidad de la Información en el cual fueron priorizadas la definición o actualización de los lineamientos y controles para fortalecer aquellos dominios con calificaciones en INICIAL e INEXISTENTE.

El detalle del diagnóstico realizado y la actualización con corte a diciembre 2021 se encuentra registrado en el documento “Diagnóstico Seguridad y Privacidad de la Información Metro de Medellín.pdf”.

10 Cronograma

A continuación, se comparte el cronograma de alto nivel vigente para 2023:

Fase	Avance	Cronograma 2023	Observaciones y Principales Avances
Planeación	EN CURSO	Diciembre 2023	Durante el año 2022 se materializaron varios avances importantes para la implementación del Modelo de Seguridad y Privacidad de la Información, entre los cuales se resalta el TI001_Procedimiento seguridad activos información. Se crea plaza del perfil de Oficial de Seguridad y Privacidad de la Información del (CISO). Sigue como prioridad mantener controles existentes y fortalecer la postura de la empresa frente a los siguientes dominios del modelo propuesto por MINTIC: • Adquisición, desarrollo y mantenimiento de sistemas • Aspectos de seguridad de la información de la gestión de la continuidad del negocio • Control de acceso • Criptografía • Cumplimiento • Activos de información • Gestión de incidentes de seguridad de la información • Organización de la seguridad de la información • Políticas de seguridad de la información • Relaciones con los proveedores, clientes o aliado de negocio • Seguridad de los recursos humanos
Consultoría	Pendiente	2023	Se tiene programado para el 2023 una consultoría para el apoyo en la implementación del modelo de seguridad y privacidad de la información.
Implementación	PENDIENTE	2022 - 2025	Esta fase se adelantará en paralelo con la de Planeación a medida que la mesa de seguridad y privacidad avance y la mesa Política de Gobierno Digital apruebe las acciones propuestas y asigne los recursos para su desarrollo.
Evaluación de Desempeño	PENDIENTE	2022 - 2025	En febrero de 2023 se realizará nuevamente el autodiagnóstico para medir el avance respecto al modelo de seguridad y privacidad del MINTIC.
Plan de mejora continua	PENDIENTE	2022 - 2025	El plan de mejora continua es el consignado actualmente en el documento “plan de acción implementación MSPI.xlsx” el cual se actualiza durante todo el año, basado en: • Ejercicio de autodiagnóstico de modelo de seguridad y privacidad. • Resultados de auditorías internas. • Autodiagnóstico de la política de seguridad y gobierno digitales. • Requerimientos de ley.

10.1 Mesa de Seguridad y Privacidad de la Información

Durante el año 2020 y como parte del plan de acción para la implementación de la Política de Gobierno Digital del Modelo Integrado de Planeación y Gestión – MIPG, la empresa estableció varios organismos de coordinación entre los cuales se encuentra la Mesa de Seguridad y Privacidad de la Información descrita a continuación:

- **Propósito:** Diseñar el modelo del Sistema de Gestión de Seguridad y Privacidad de la Información en el marco del Modelo Integrado de Planeación y Gestión – MIPG y la Política de Gobierno Digital.

- **Alcance:** Diseñar el Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), alineado e integrado al modelo de Gestión y Gobierno de las Tecnologías de Información y comunicaciones de la Empresa, siendo este uno de los habilitadores transversales de la Política de Gobierno Digital.

- **Conformación:** El mecanismo estará conformado por los siguientes miembros permanentes:
  - Jefe de Área Gestión de Tecnologías de Información – responsable de la Seguridad de la Información
  - Profesional 1 Gestión de Tecnologías de Información - Outsourcing
  - Profesional 1 Gestión de Tecnologías de Información - Informática
  - Profesional 1 UEN Cívica – Habilitación
  - Profesional 1 UEN Cívica – Operaciones
  - Profesional 1 Investigación, Desarrollo e Innovación
  - Profesional 2 Sistema Operativo – Telemática Operativa
  - Profesional 1 Administración Documental
  - Profesional 1 Administración de Riesgos
  - Profesional 1 Oficial de Privacidad
  - Profesional 1 Asesoría en Gestión

- **Responsabilidades:**
  - Realizar los diagnósticos del estado de la seguridad y privacidad de la información.
  - Diseñar el plan de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)
  - Elaborar el plan de brechas para la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)
  - Identificar las necesidades de recursos para la implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)
  - Someter a aprobación de la Mesa de Política de Gobierno Digital el plan de implementación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI)

Serán invitados a esta mesa los participantes que se requieran de acuerdo con los temas necesarios para la implementación de la política de Gobierno Digital.

10.2 Política de Seguridad y Privacidad de la Información

El Metro de Medellín a través de la política de Seguridad y Privacidad de la Información se compromete a velar por la seguridad y la privacidad de los datos e información generados al interior de la organización y

recibidos de los grupos de interés, para ello establece lineamientos orientados a mitigar los riesgos asociados a los activos de información, mediante la creación y ejecución de iniciativas que promuevan el uso responsable de la información y los recursos tecnológicos, la adopción de buenas prácticas y la generación de una cultura organizacional de la seguridad de la información que involucre a los grupos de interés

10.2.1. Objetivo de la política

Establecer directrices orientadas a la conservación de la confidencialidad, integridad, disponibilidad y privacidad de la información, mediante la implementación de estrategias y ejecución de actividades que permitan la creación y mantenimiento de la cultura de seguridad y privacidad de la información en la Empresa.

El cumplimento de esta política se asocia al Modelo de Seguridad y Privacidad de la Información.

10.2.2. Marco de actuación

Con el desarrollo de esta política se establecerán lineamientos frente a los siguientes dominios del Modelo de Seguridad y Privacidad de la Información:

- Control de acceso
- Seguridad de los recursos humanos
- Ley 1581 de 2012, Decreto 1074 de 2015 y las demás normas o documentos que los modifiquen, adicionen, sustituyan o reglamenten.
- Gestión de activos de información
- Criptografía
- Seguridad física y del entorno
- Seguridad de las operaciones
- Seguridad de las comunicaciones
- Adquisición, desarrollo y mantenimiento de sistemas
- Relaciones con los proveedores, clientes o aliados de negocio
- Gestión de incidentes de seguridad de la información
- Seguridad de la información de la gestión de la continuidad del negocio
- Cumplimiento

11 Anexos

Plan de acción implementación MSPI.xlsx
Plan de formación y divulgación Modelo de Seguridad y Privacidad.xlsx
Diagnóstico Seguridad y Privacidad de la Información Metro de Medellín.pdf

12 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.[2]
- **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.
- **ISO/IEC 27001:2013:** 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.[3]

[2] https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf
[3] https://www.iso.org/standard/54534.html

13 Control de cambios

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

14 Responsabilidades

Documentador	Revisor	Aprobador
Mesa de Seguridad y Privacidad de la Información	Mesa de Política Gobierno Digital	Comité Institucional de Gestión y Desempeño