Contenido

1 Propósito

Presentar el Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información para la Empresa de Transporte Masivo del Valle de Aburrá Limitada, que contiene el cronograma de trabajo para la identificación, análisis, valoración, tratamientos y monitoreo de los riesgos relacionados a los activos de información de la Empresa.

2 Alcance y Vigencia

Este plan tendrá vigencia a partir del año 2026 y su alcance es a todos los activos relacionados en el inventario de activos de información.

3 Objetivo General

Elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información de acuerdo con las mejores prácticas del modelo definido por Ministerio de las Tecnologías de Información y las comunicaciones, la guía para la administración del riesgo y el diseño de controles en entidades públicas.

Objetivos Específicos

- Establecer los lineamientos que propendan por la unificación de criterios en la administración de los riesgos de seguridad y privacidad de la información.
- Fortalecer la gestión de riesgos de la Empresa incorporando controles y tratamientos de seguridad y privacidad de la información que estén acordes con la metodología de riesgos utilizada.
- Vincular al mapa de riesgos de procesos de la Empresa, los riesgos de seguridad y privacidad de la información identificados, analizados y valorados.
- Generar una cultura y apropiación de trabajo enfocada a la gestión de los riesgos de seguridad y privacidad de la información.

4 Responsables

Área de Administración de Riesgos

5 Requisitos técnicos

Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información, guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital de la Función Pública.

6 Documentos asociados

DR1381 Manual Gestión de Riesgos y sus anexos.
Anexo 3_Identificación, análisis y valoración de riesgos asociados a los activos de información
Anexo 9_Metodología riesgos de protección de datos personales

7 Seguimiento al cronograma

- **Durante el año 2020** el área de Gestión de Tecnologías de la Información y como parte de una de sus acciones para la implementación de la Política de Gobierno Digital del Modelo Integrado de Planeación y Gestión (MIPG), se estableció la Mesa de Seguridad y Privacidad de la Información, cuyo propósito es realizar el diagnóstico y establecer el plan de acción para implementación del Modelo de Seguridad y Privacidad de la Información establecido por el Ministerio de las Tecnologías de Información y las Comunicaciones

- **Durante el año 2021** se avanza en la alineación de la metodología de riesgos de La Empresa con el modelo definido por Ministerio de las Tecnologías de Información y las comunicaciones y la guía para la administración del riesgo y el diseño de controles en entidades públicas, riesgos de gestión, corrupción y seguridad digital de la Función Pública.

  Ajustes en las matrices para la gestión de riesgos de seguridad y privacidad de la información.

- **Durante el año 2022** se avanzó en la documentación del procedimiento para la identificación, clasificación y valoración de los activos de información en la Empresa.

- **Durante el 2023** se incorpora el oficial de seguridad de la información mostrando el compromiso

de la empresa para el cumplimiento de sus objetivos y trayendo la competencia adecuada para la identificación de los activos y riesgos asociados a estos.

- **Durante el año 2024** Se crea y se documenta la metodología para la gestión de activos de información, así como también se actualiza el inventario de activos de información, clasificándolos y agrupándolos, así como también fua asignada la criticidad a cada uno de ellos, lo que permitió la identificación de riesgos para cada grupo de activos e información.

- **Durante el año 2025** Se crea y se documenta la metodología de riesgos de protección de datos personales, se culmina la documentación de la declaración de aplicabilidad donde se establece el alcance de cada control asociado al estándar adoptado que para el Metro de Medellin es ISO27002.

El siguiente es el cronograma definido para el año 2026:

Cronograma 2026		
Actividad	**Cronograma**	**Responsable**
Integración de riesgos de proceso y estratégicos con los riesgos de seguridad de la información.	Febrero 2026	Oficial de seguridad de la información
Actualización metodología de riesgos sobre contratos	Febrero 2026	Oficial de seguridad de la información
Entrega de estructura para la entrega de evidencias de los controles asociados a los riesgos de seguridad de la información	Marzo 2026	Oficial de seguridad de la información

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