



Contenido

1	Propósito	2
2	Alcance y Vigencia	2
3	Objetivo General	2
3.1	Objetivos Específicos	2
4	Responsables	2
5	Requisitos técnicos	3
6	Documentos asociados	3
7	Seguimiento al cronograma	3
8	Control de cambios	4
9	Responsabilidades	4

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 y monitoreo de los riesgos relacionados a los activos de información de la Empresa.

2 Alcance y Vigencia

Este plan tendrá vigencia a partir enero del año 2024 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 - Riesgos de gestión, corrupción y seguridad digital de la Función Pública.

3.1 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 del 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.

7 Seguimiento al cronograma

Durante el año 2020 el área de Gestión de Tecnologías de la Información como parte de una de sus acciones para la implementación de la Política de Gobierno Digital del Modelo Integrado de Planeación y Gestión (MIPG), estableció la Mesa de Seguridad y Privacidad de la Información, cuyo propósito era 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 abordaron acciones como:

- 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.

En 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 incorporó 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 seguridad de la información.

El siguiente es el cronograma definido para el año 2024:

Cronograma 2024		
Actividad	Cronograma	Responsable
Actualización de la metodología para la gestión de activos de información	Enero 2024	Oficial de seguridad de la información
Creación del inventario de activos de información	Diciembre 2024	Oficial de seguridad de la información
Identificación de riesgos a los activos del inventario	Diciembre 2024	Oficial de seguridad de la información
Asignación de controles a las causas de los riesgos identificados	Diciembre 2024	Oficial de seguridad de la información
Monitorear y gestionar los riesgos identificados y valorados en el Modelo de Seguridad y Privacidad que definió la Empresa	Permanente	Administración de Riesgos y líderes de riesgos de los procesos

8 Control de cambios

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

9 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