



## Contenido

<b>1</b>	<b>Propósito .....</b>	<b>2</b>
<b>2</b>	<b>Alcance y Vigencia .....</b>	<b>2</b>
<b>3</b>	<b>Objetivo General .....</b>	<b>2</b>
3.1	Objetivos Específicos .....	2
<b>4</b>	<b>Responsables .....</b>	<b>3</b>
<b>5</b>	<b>Requisitos técnicos .....</b>	<b>3</b>
<b>6</b>	<b>Documentos asociados .....</b>	<b>3</b>
<b>7</b>	<b>Seguimiento al cronograma .....</b>	<b>3</b>

## **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 con sistema de gestión de seguridad de la información en los procesos de la Empresa.

## **2 Alcance y Vigencia**

Este plan tendrá vigencia a partir del año 2019 y su alcance es a todos los procesos de la Empresa en concordancia con la implementación del Modelo de Seguridad y Privacidad de la Información en La Empresa.

## **3 Objetivo General**

Elaborar el plan de tratamiento de riesgos de seguridad y privacidad de la información de acuerdo con las mejores prácticas de la norma ISO27001:2013, 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.

### **3.1 Objetivos Específicos**

- Realizar un diagnóstico de la situación actual de la Empresa materia de riesgos de seguridad y privacidad de la Información, con base en la norma ISO27001:2013, 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.
- Establecer los lineamientos que propendan por la unificación de criterios para 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.

## **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 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, una vez se publique dicho procedimiento en el Sistema de Gestión Integral, se iniciará la identificación de dichos activos.
- El siguiente es el cronograma definido para el año 2023:

<b>Cronograma 2023</b>		
<b>Actividad</b>	<b>Cronograma</b>	<b>Responsable</b>
Identificación de los activos de información y calificación de su criticidad en los procesos priorizados.	Febrero a Diciembre de 2023	Mesa de Seguridad y Privacidad de la Información
Apoyar la identificación, análisis y valoración de los riesgos de seguridad y privacidad de la información, de acuerdo con los activos de información identificados y calificados.	Febrero a Diciembre de 2023	Administración de Riesgos y líderes de riesgos de los procesos
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

<b>Versión modificada</b>	<b>Descripción del cambio</b>
NA	NA
NA	NA
NA	NA
NA	NA

## 9 Responsabilidades

<b>Documentador</b>	<b>Revisor</b>	<b>Aprobador</b>
Profesional 1 Administración de Riesgos, Didier Pérez Giraldo	Jefe Administración de Riesgos, María Duque Quintero	Jefe Administración de Riesgos, María Duque Quintero