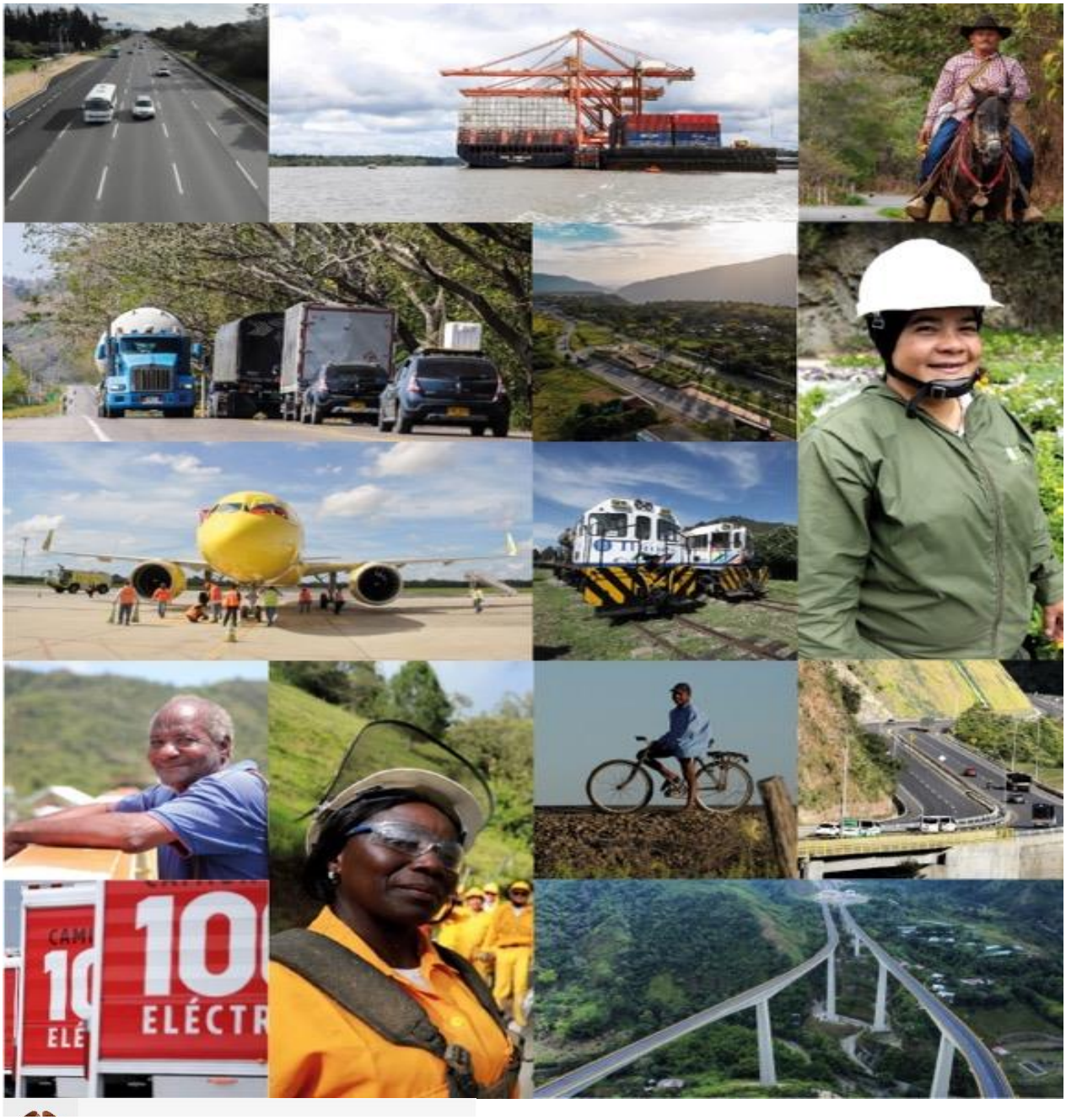

# Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información 2023

## 1. CONTENIDO

## 2. INTRODUCCION

*El Ministerio de Transporte, cumpliendo con su compromiso con la protección de la información, identifica, valora, gestiona y trata los riesgos de seguridad de la información que se puedan presentar en la entidad y que pueden afectar el cumplimiento de la misión y visión del Ministerio de Transporte.*

*Para lo anterior, ha establecido su esquema de gestión de riesgos basado en la "Guía para la administración del riesgo y el diseño de controles en entidades públicas – Versión 2020" definida por el DAFP (Departamento Administrativo de la Función Pública) donde se realiza una gestión unificada de los riesgos de gestión, corrupción y seguridad digital (Seguridad de la Información). Brindando un enfoque preventivo y anticipándose a las posibles vulnerabilidades o eventos que puedan afectar el logro de los objetivos institucionales y a la ciudadanía.*

## 3. GENERALIDADES

*El Ministerio de Transporte, realiza la gestión de riesgos de seguridad de la información en el último cuatrimestre de la vigencia 2022, alineado a los lineamientos definidos por Función Pública, a través de la "Guía para Administración de Riesgos y el Diseño de Controles versión 2020". Se tiene realizada la identificación de los activos de información en cada proceso, una matriz de riesgos debidamente estructurada y se plantean los planes de tratamiento para mitigar las vulnerabilidades y amenazas identificadas para reducir su probabilidad de ocurrencia.*

*Se realizó un levantamiento especifico de activos y riesgos para cada uno de los veinte (20) procesos de la entidad, obteniendo un total de 108 riesgos a nivel institucional, este análisis se presentará con mayor detalle en secciones posteriores del documento.*

*Para la vigencia 2023, se tiene proyectada una actividad de acompañamiento a los procesos para la revisión de todos los catálogos de activos, así mismo, una revisión de nuevas posibles amenazas y vulnerabilidades para enriquecer y complementar los análisis de riesgos realizados hasta el momento. De estas actividades, se espera tener una reducción en la cantidad de riesgos ubicados en la zona no aceptable para la entidad.*

*De estos nuevos riesgos identificados, se proyectarán nuevos planes de tratamiento de riesgo tanto a mediano como a largo plazo (misma vigencia o siguientes) de acuerdo con las necesidades o controles que se planteen y de la disponibilidad presupuestal de la entidad.*

## 4. MARCO NORMATIVO

*El presente Plan de Tratamiento de Riesgos de Seguridad y Privacidad se genera con base a los requisitos enmarcados en el decreto 612 de 2018 "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."*

## 5. ALINEACIÓN INSTITUCIONAL

*El presente plan de alinea con el Modelo Integrado de Planeación y Gestión (MIPG) en la dimensión "Gestión con valores para resultados" – Políticas de Gobierno Digital y Seguridad Digital, como se describe a continuación:*

| DIMENSIÓN MIPG<br>POLÍTICA DE GESTIÓN Y DESEMPEÑO | DESCRIPCIÓN DE RELACIÓN |
|---|---|
| *POLÍTICA DE GOBIERNO DIGITAL* | *El presente plan de acción contribuye a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI).* |
| *POLÍTICA DE SEGURIDAD DIGITAL* | *El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, se alinea a lo establecido en la política de seguridad digital, donde prima el enfoque basado en riesgos y a su tratamiento, para mejorar el entorno digital tanto para la ciudadanía como las demás partes interesadas.* |

## 6. OBJETIVO GENERAL

*Establecer y detallar el Plan de Tratamiento de los Riesgos de Seguridad y Privacidad de la Información del Ministerio de Transporte de acuerdo con los resultados obtenidos en la valoración y planes de acción definidos para su tratamiento.*

## 7. ALCANCE

*El presente plan contempla todos los procesos de la entidad (Misionales, Estratégicos, Apoyo y de Evaluación), acorde al alcance definido en el Modelo de Seguridad y Privacidad de la Información (MSPI) establecido por el Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC).*

## 8. RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

*Para la gestión de riesgos de seguridad de la información del 2023 (Último Trimestre de*

*2022), se ejecutó un proceso detallado de gestión de riesgos sobre los activos específicos de los veinte (20) procesos de la entidad.*

*Respecto al inventario y clasificación de activos de información, se definieron los inventarios para los veinte (20) procesos, identificando un total de seiscientos noventa y seis (696) activos, los cuales posterior a su identificación y valoración, fueron analizados en las respectivas matrices de riesgo de cada proceso empleando la metodología de Función Pública de la versión 2018.*

*Con base a este análisis de riesgos de seguridad digital, enfocado a vulnerabilidades y amenazas, se identificaron las siguientes cantidades de riesgos clasificados por cada uno de los procesos de la entidad.*

| ***DESCRIPCIÓN*** | ***DISTRIBUCIÓN*** |
|---|---|
| *Extremo* | *4* |
| *Alto* | *23* |
| *Moderado* | *60* |
| *Bajo* | *21* |
| ***TOTAL DE RIESGOS*** | *108* |

*En la presente etapa de gestión de riesgos a nivel institucional, se observa una cantidad moderada de riesgos en niveles Altos y Extremos (25%) aproximadamente. Los riesgos restantes, hacen parte de la zona de riesgo aceptable para la entidad.*

***Nota:** Las vulnerabilidades, amenazas, o descripción detallada de los riesgos de seguridad de la información son **información pública clasificada,** teniendo en cuenta que pueden poner en riesgo la operación y activos de información de la entidad.*

## 9. RESULTADO DEL PLAN DE TRATAMIENTO DE RIESGOS

*Para los riesgos identificados se establecieron planes de tratamiento con base a la cantidad de vulnerabilidades asociadas a cada uno, sin embargo, la proyección del año 2023 se realizará una vez se actualicen las matrices de riesgos de los procesos. Lo cual se tiene establecido para el primer semestre de 2023.*

*En adición a lo anterior, se contemplan las siguientes actividades a ejecutar en la vigencia 2023:*

- *Reuniones con los procesos para reinducción sobre de la "Guía para Administración de Riesgos y el Diseño de Controles versión 2020" orientada a los riesgos de seguridad digital.*
- *Acompañamiento en la actualización de los catálogos de activos de cada proceso (20 catálogos de activos).*

- *Verificación y análisis de amenazas y vulnerabilidades con base a posibles nuevos activos encontrados en cada proceso.*
- *Determinación de nuevos planes de tratamiento de riesgos, extensión o modificación, con base a las revisiones requeridas.*

*De forma paralela además de las actividades de identificación, análisis y evaluación de los riesgos, se gestionarán los siguientes controles para la mitigación de los riesgos:*

- *Generación/Actualización de documentos con lineamientos y políticas de seguridad de la información.*
- *Asignación de roles en el grupo TIC.*
- *Concientización de personal.*
- *Aprovechamiento de las herramientas o recursos de ciberseguridad con los que cuenta el Ministerio de Transporte.*
- *Inversión en controles tecnológicos que permitan el adecuado resguardo y protección de los activos de información.*

## 10. MONITOREO Y SEGUIMIENTO DEL PLAN DE TRATAMIENTO DE RIESGOS

*Es responsabilidad de los dueños de los procesos realizar el monitoreo de los riesgos y sus tratamientos, así como analizar los resultados trimestralmente conforme a la Política Integral de Gestión de Riesgos de la Entidad, así como reportar periódicamente los resultados del monitoreo y su análisis, el cual debe enviarse a la oficina Asesora de planeación para su análisis y consolidación.*

*El Responsable de Gestión de Seguridad de la Información (Oficial de Seguridad) asesora y apoya a los lideres de proceso en la identificación de riesgos y planteamiento de tratamiento de estos. De igual forma, revisará la ejecución de los tratamientos referentes a riesgos de seguridad de la información y brindará retroalimentación al coordinador del Grupo TIC y jefe de la Oficina Asesora de Planeación para que sea informado a la alta dirección del Ministerio.*

## 11. GLOSARIO

- ***Riesgo de seguridad de la información:*** *Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.*
- ***Confidencialidad:*** *Propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.*
- ***Integridad:*** *Propiedad de la información relativa a su exactitud y completitud.*
- ***Disponibilidad:*** *Propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.*

- ***Seguridad de la Información:*** *Preservación de la confidencialidad, integridad y disponibilidad de la información.*
- ***MSPI:*** *Modelo de Seguridad y Privacidad de la Información*
- ***Vulnerabilidad:*** *Debilidad de un activo o control que puede ser explotada por una o más amenazas.*
- ***Amenaza:*** *Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.*
- ***Tratamiento del Riesgo:*** *Es la respuesta establecida por la primera línea de defensa para la mitigación de los diferentes riesgos. Existen 4 categorías para "tratar" los riesgos: aceptar el riesgo, reducir el riesgo, evitar el riesgo y compartir el riesgo.*

## 12. RESPONSABLE DEL PLAN

*Nombre completo: Catalino Posso Arboleda*
*Cargo: Coordinador (e) Grupo TIC*
*Dependencia: Grupo de Tecnologías de la Información y las Comunicaciones*
*Elaboró: Hugo Alejandro Casallas Larrotta*
*Elaboró: Juan Carlos Valenzuela Buitrago*