# PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DEL SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S

Tabla de contenido

## RESUMEN EJECUTIVO

El Plan de Tratamiento de Riesgos tiene como propósito establecer estrategias específicas para minimizar los riesgos identificados en el análisis, tales como la pérdida de confidencialidad, integridad y disponibilidad de los activos de información. Esto contribuye a reducir la incertidumbre y garantiza el cumplimiento de los objetivos estratégicos del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.

Este plan busca evaluar y organizar las acciones necesarias para mitigar los riesgos detectados en los procesos de la entidad. Cada acción se detalla en actividades concretas que incluyen la asignación de responsables, tareas específicas y plazos de ejecución, asegurando su implementación dentro del período definido para el plan.

Las actividades diseñadas se fundamentan en el análisis de riesgos, considerando las necesidades y el contexto particular de los procesos de la organización. Además, ofrecen un enfoque estructurado que facilita la identificación de sus características y la definición de los pasos requeridos para su ejecución, priorizando la seguridad y la privacidad de la información.

## INTRODUCCIÓN

El Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. está orientado estratégicamente hacia el desarrollo de una cultura preventiva. Esto implica una comprensión integral del concepto de riesgo y su relación con el contexto organizacional, lo que permite planificar acciones destinadas a mitigar impactos potenciales en caso de que los riesgos se materialicen. Asimismo, el plan busca fortalecer las estrategias de identificación, análisis, tratamiento, evaluación y monitoreo de los riesgos con un enfoque más objetivo, asegurando que se identifiquen y gestionen situaciones que puedan comprometer los objetivos de la entidad en el ámbito TIC.

Este enfoque preventivo se alinea con las recomendaciones del Documento CONPES 3995 de 2020, que establece lineamientos clave para la seguridad digital en Colombia, y con el Decreto Único Reglamentario del Sector TIC (Decreto 1078 de 2015), en particular en lo que respecta al habilitador de seguridad y privacidad de la información. Además, integra las disposiciones de la Resolución 500 de 2021, que define estándares para implementar estrategias de seguridad digital y adopta el modelo de seguridad y privacidad.

El plan también incorpora las buenas prácticas internacionales definidas en los estándares ISO 27001, que especifica los requisitos para establecer y mantener un sistema de gestión de seguridad de la información, y ISO 31000:2018, que proporciona directrices para la gestión del riesgo en cualquier contexto organizacional. De igual manera, sigue las directrices del Modelo Integrado de Planeación y Gestión (MIPG), que establece una guía específica para la administración del riesgo y el diseño de controles en entidades públicas.

Con base en estas normativas y estándares, el documento se actualiza para garantizar que las acciones propuestas estén alineadas con los marcos regulatorios y las mejores prácticas aplicables, consolidando un enfoque robusto y adaptado a las necesidades específicas de una entidad pública como el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.

## 1. OBJETIVOS

Implementar un marco integral de gestión de riesgos en Seguridad y Privacidad de la Información en del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S., que permita garantizar el cumplimiento de los requisitos normativos, la continuidad operativa y la protección de la información gestionada.

Esto se logrará mediante la aplicación de lineamientos estratégicos, la identificación y tratamiento de riesgos, y la promoción de una cultura organizacional basada en la prevención y mitigación de amenazas, asegurando la confidencialidad, integridad y disponibilidad de los datos en concordancia con los estándares y regulaciones vigentes

### 1.1. Objetivos Específicos

- Establecer y aplicar lineamientos que permitan tratar de manera integral los riesgos relacionados con la Seguridad y Privacidad de la Información a los que el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. pueda estar expuesta. Esto tiene como objetivo garantizar el cumplimiento de los objetivos estratégicos, así como la misión y visión de la entidad, preservando la confidencialidad, integridad y disponibilidad de la información gestionada.

- Asegurar el cumplimiento de los requisitos legales, reglamentarios y normativos, así como de las normas técnicas colombianas aplicables en materia de seguridad y privacidad de la información, seguridad digital y protección de datos personales, en concordancia con el marco jurídico vigente.

- Gestionar de manera eficiente los riesgos asociados a la Seguridad y Privacidad de la Información, la Seguridad Digital y la Continuidad Operacional, considerando los contextos específicos de los procesos internos de la entidad. Esto incluye la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos, alineándose con los estándares y modelos aplicables.

- Promover la formación y apropiación de conocimientos relacionados con la gestión de riesgos en estos ámbitos, fortaleciendo las capacidades del personal del SETP y fomentando una cultura organizacional basada en la prevención y mitigación de riesgos.

## 2. ALCANCE

Implementar una gestión eficiente de los riesgos relacionados con la Seguridad y Privacidad de la Información, integrando en los procesos de la entidad buenas prácticas que fortalezcan la toma de decisiones y permitan prevenir incidentes que puedan comprometer el cumplimiento de los objetivos estratégicos.

Además, establecer lineamientos claros para identificar, analizar, tratar, evaluar y monitorear los riesgos asociados a la seguridad y privacidad de la información, asegurando un enfoque sistemático y preventivo que facilite su gestión en el contexto del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.

El Plan de Tratamiento de Riesgos estará orientado a abordar prioritariamente aquellos riesgos clasificados en niveles Moderado, Alto y Extremo, de acuerdo con los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Los riesgos clasificados en niveles inferiores serán gestionados mediante una aceptación formal por parte de la entidad, siempre que su impacto sea considerado manejable dentro de las capacidades operativas y estratégicas del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.

## 3. TERMINOLOGIA Y DEFINICIONES

- **Riesgo:** Efecto que se causa sobre los objetivos de las entidades, debido a eventos potenciales.

- **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. (ISO/IEC 27000).

- **Amenaza:** es un ente o escenario interno o externo que puede hacer uso de una vulnerabilidad para generar un perjuicio o impacto negativo en la institución (materializar el riesgo).

- **Vulnerabilidad:** es una falencia o debilidad que puede estar presente en la tecnología, las personas o en las políticas y procedimientos.

- **Probabilidad:** se entiende la posibilidad de ocurrencia del riesgo. Estará asociada a la exposición al riesgo del proceso o actividad que se esté analizando.

- **Impacto:** consecuencias que puede ocasionar a la organización la materialización del riesgo.

- **Control o Medida:** Medida que permite reducir o mitigar un riesgo.

## 4. NORMATIVIDAD

- Ley 1978 de 2019. Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único y se dictan otras disposiciones.
- Ley 1753 de 2015. Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAIS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
- Ley 1341 de 2009. Por la cual se definen Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
- Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
- Ley 1221 del 2008. Por la cual se establecen normas para promover y regular el Teletrabajo y se dictan otras disposiciones.
- Decreto 0767 de 2022. Por el cual se establecen los 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.
- Decreto 338 de 2022. Por el cual se adiciona el Titulo 21 a la Parte 2 del Libro 2 del Decreto Único 1078 de 2015, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, con el fin de establecer los lineamientos generales para fortalecer la gobernanza de la seguridad digital, se crea el Modelo y las instancias de Gobernanza de Seguridad Digital y se dictan otras disposiciones.
- Decreto 1008 del 2018. Por el cual se establecen los 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.
- 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.
- Decreto 415 de 2016. Definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones.
- Decreto 2573 de 2014. Reglamenta parcialmente la Ley 1341 de 2009 y que en el mismo decreto se define el componente de Privacidad y Seguridad de la información que incluye el modelo de seguridad y privacidad de la información - MSPI.
- Decreto 886 de 2014. Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012, relativo al Registro Nacional de Bases de Datos, que permitirá cumplir con la obligación legal de dar publicidad a la existencia de bases de datos de carácter personal y servirá de herramienta de supervisión para la efectiva protección de los derechos de los titulares.

- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012 o Ley de Datos Personales.
- Decreto Ley 019 de 2012, por el cual se dictan normas para suprimir o reformar regulaciones, procedimientos y trámites innecesarios existentes en la Administración Pública.
- Resolución 746 de 2022. Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución No. 500 de 2021
- Resolución 460 de 2022. Por el cual expide el Plan Nacional de Infraestructura de Datos y su hoja de ruta en el desarrollo de la Política de Gobierno Digital, y se dictan los lineamientos generales para su implementación
- Resolución 500 de 2021. Por la cual se establecen los lineamientos y estándares para la estrategia de Seguridad Digital y se adopta el Modelo de Seguridad y Privacidad como habilitador de la Política de Gobierno Digital.
- Resolución N 2710 de 2017, por la cual se establecen lineamientos para la adopción del protocolo IPv6
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- CONPES 3701 de 2011, Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016, Política Nacional de Seguridad digital.

## 5. MARCO REFERENCIAL

El sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S., ratifica su compromiso con la promoción de una cultura de gestión del riesgo que fortalezca las medidas de prevención, monitoreo y control necesarias para mitigar la posible ocurrencia de riesgos en las actividades desarrolladas por la entidad. Este compromiso abarca el diseño, adopción, ejecución y promoción de políticas, planes, programas e iniciativas alineadas con los objetivos estratégicos del SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S, asegurando que los mecanismos, sistemas y controles implementados detecten y gestionen de manera integral riesgos asociados con:

- Estrategia organizacional y transparencia.
- Ética en la gestión pública.
- Seguridad y privacidad de la información.
- Seguridad digital y continuidad operativa.
- Riesgo fiscal.
- Aspectos ambientales.
- Seguridad y salud en el trabajo.

Estas acciones están orientadas a prevenir situaciones que puedan afectar el cumplimiento de los objetivos institucionales, garantizar el uso eficiente de los recursos asignados y atender de manera adecuada las expectativas de los grupos de interés.

El propósito de esta política es establecer los lineamientos necesarios para una adecuada gestión de los riesgos relacionados con la Seguridad y Privacidad de la Información, buscando minimizar la probabilidad de que se materialicen. Para ello, se adoptan los parámetros establecidos en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas emitida por el Departamento Administrativo de la Función Pública (DAFP). Este enfoque permite tomar decisiones oportunas, reducir los efectos adversos y garantizar la continuidad de la gestión institucional, cumpliendo los compromisos adquiridos con los grupos de interés.

El tratamiento de los riesgos constituye la respuesta implementada por la primera línea de defensa, es decir, el líder o responsable del proceso junto con su equipo de trabajo, quienes son los encargados de diseñar y ejecutar las acciones necesarias para mitigar los riesgos identificados.

El tratamiento o respuesta dada al riesgo, se enmarca en las siguientes categorías:

**Aceptar el riesgo:** No se adopta ninguna medida que afecte la probabilidad o el impacto del riesgo. (Ningún riesgo de corrupción es aceptado). La aceptación del riesgo puede ser una opción viable en la entidad, para los riesgos bajos, pero también pueden existir escenarios de riesgos a los que no se les puedan aplicar controles y, por ende, se acepta el riesgo. En ambos escenarios debe existir un seguimiento continuo del riesgo.

**Reducir el riesgo:** Se adoptan medidas para reducir la probabilidad o el impacto del riesgo, o ambos; por lo general conlleva a la implementación de controles. Deben seleccionarse controles apropiados y con una adecuada segregación de funciones, de manera que el tratamiento al riesgo adoptado logre la reducción prevista sobre este.

**Evitar el riesgo:** Se abandonan las actividades que dan lugar al riesgo, es decir, no iniciar o no continuar con la actividad que lo provoca.

**Compartir el riesgo:** Se reduce la probabilidad o el impacto del riesgo transfiriendo o compartiendo una parte de este. Los riesgos de corrupción se pueden compartir, pero no se puede transferir su responsabilidad. Los dos principales métodos de compartir o transferir parte del riesgo son: seguros y tercerización.

La gestión de riesgos relacionados con la Seguridad y Privacidad de la Información permite a el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. identificar, analizar y tratar los riesgos que puedan afectar el cumplimiento de los objetivos de sus procesos. Este enfoque contribuye a una toma de decisiones más informada y a la prevención de la materialización de eventos adversos.

La administración de estos riesgos se centra en identificar, analizar, valorar y mitigar las amenazas y vulnerabilidades asociadas a los activos de información de la entidad, considerando su nivel de criticidad y las medidas necesarias para garantizar su protección.

Este enfoque integral asegura que cada etapa de la gestión de riesgos esté alineada con los objetivos estratégicos y las políticas corporativas de la organización, logrando establecer un nivel de riesgo que sea aceptable o asumible por la Alta Dirección.

## 6. METODOLOGIA

El Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información de el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.. se enfoca en establecer acciones concretas para mitigar los riesgos identificados, alineándose con normativas como la ISO/IEC 27001, la Política Pública de Seguridad Digital y el Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Sin embargo, en su estado actual, el plan no incluye metodologías específicas para la gestión de activos de seguridad digital, análisis y valoración de riesgos, ni tratamiento de riesgos, debido a que estas no han sido desarrolladas ni implementadas en la entidad.

La ausencia de estas metodologías se justifica en que el proceso de gestión de riesgos en el SETP. se encuentra en una fase inicial, donde el foco principal ha sido la identificación e inventario de activos de seguridad. Esta fase, aunque esencial, no abarca las etapas posteriores de la gestión de riesgos, como el análisis, la valoración y el tratamiento de los mismos. La falta de recursos técnicos, humanos y financieros especializados ha limitado la capacidad de la entidad para desarrollar metodologías completas que integren estas fases.

Adicionalmente, la entidad ha priorizado la implementación de controles básicos y la sensibilización del personal en temas de seguridad de la información, lo cual es un primer paso fundamental para avanzar hacia una gestión integral de riesgos. La no inclusión de metodologías específicas en el plan no implica un desconocimiento de su importancia, sino que responde a una estrategia gradual de implementación, donde se busca consolidar primero una base sólida en la identificación de activos y riesgos, para posteriormente desarrollar y aplicar metodologías más avanzadas.

En este sentido, se reconoce la necesidad de avanzar en la elaboración de estas metodologías, las cuales serán incorporadas en futuras actualizaciones del plan. Este enfoque progresivo garantiza que la entidad cumpla con los estándares internacionales y normativas locales de manera sostenible, priorizando la efectividad y la adecuada gestión de los riesgos de seguridad y privacidad de la información

El Plan de Tratamiento de Riesgos del SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S establece un conjunto de actividades diseñadas para mitigar los riesgos que afectan los activos identificados en la entidad. Estas actividades se han estructurado siguiendo las recomendaciones de la Guía de Gestión de Riesgos de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC, 2016), con el objetivo de asegurar que se adopten las mejores prácticas en la gestión de los riesgos relacionados con la seguridad y privacidad de la información.

| Gestión | Actividades | Tareas | Responsable de la Tarea | Evidencia | Fechas Programación Tareas | | Fecha de seguimiento |
|---|---|---|---|---|---|---|---|
| | | | | | Fecha Inicio | Fecha Final | |
| Gestión de Riesgos | Actualización de lineamientos de riesgos | Apoyar cuando se requiera la actualización de la política, metodología y lineamientos de la gestión de riesgos | Planeación Estrategica | Correos electrónicos, Documentación actualizada en Sistema de Gestión Página web | 01-jul-25 | 30-jul-25 | 30-dic-25 |
| | Identificación de Riesgos de Seguridad y Privacidad de la Información | Contexto, Identificación, Análisis y Evaluación de Riesgos - Seguridad y Privacidad de la Información y Seguridad Digital | Planeación Estrategica | Correos electrónicos Mapas de riesgos | 1-ago-25 | 30-ago-25 | 30-dic-25 |
| | | Realimentación, revisión y verificación de los riesgos identificados (Ajustes) | Planeación Estrategica | Correos electrónicos Mapas de riesgos | 1-ago-25 | 30-ago-25 | 30-dic-25 |
| | Aceptación de Riesgos Identificados | Aceptación, aprobación riesgos identificados y planes de tratamiento | Planeación Estrategica | Memorandos de aceptación mapas de riesgos | 1-sept-25 | 11-sept-25 | 30-dic-25 |
| | Publicación | Publicación mapas de riesgos de los procesos Sistema de Gestión | Planeación Estrategica | Mapas de riesgos publicados Sistema de Gestión | 15-sept-25 | 30-sept-25 | 30-dic-25 |

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| | Seguimiento Fase de Tratamiento | Seguimiento implementación de controles y planes de tratamiento de riesgos los identificados (verificación de evidencias) | Planeación Estrategica | Seguimiento mapas de riesgo | 01-dic-25 | 30-dic-25 | 30-dic-25 |

### 1.1. Desarrollo metodológico


### Establecimiento del Contexto

El establecimiento del contexto se refiere a la identificación y análisis de los aspectos externos, internos y del proceso que deben ser considerados para gestionar los riesgos de Seguridad y Privacidad de la Información, en el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.

Este análisis permite comprender las posibles causas de los riesgos que podrían afectar el cumplimiento de los objetivos institucionales. A partir de este contexto, se establecerán las bases para identificar y evaluar los riesgos relevantes, siguiendo las metodologías y procedimientos establecidos por la entidad. Estas metodologías están orientadas a asegurar una identificación precisa de los riesgos y a determinar las acciones más efectivas para su tratamiento.

### Identificación del Riesgo

La identificación de riesgos relacionados con la Seguridad y Privacidad de la Información, en el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. debe considerar diversos factores, como la infraestructura física, las áreas de trabajo, el entorno y el ambiente en

general. Es fundamental que cada proceso dentro de la entidad tenga identificados los activos de información y que se reconozcan las situaciones potenciales que puedan causar daño a la organización, comprometiendo así el logro de los objetivos establecidos.

La falta de apropiación de la seguridad de la información o la ausencia de controles adecuados puede ser aprovechada por una amenaza, lo que derivaría en la materialización de un riesgo o incidente. Para ello, es esencial identificar, a través del mapa de riesgos, los siguientes atributos: el impacto en la triada de la información (Confidencialidad, Integridad, Disponibilidad), el propietario del riesgo (líder del proceso), el activo de información afectado, las amenazas, las vulnerabilidades y las consecuencias potenciales.

La identificación de los activos afectados se realiza mediante la validación en el inventario de activos de información del proceso correspondiente. En esta validación se considera la criticidad, la clasificación de la información y otros atributos relevantes para el análisis del posible riesgo. La identificación de los activos se lleva a cabo conforme a los lineamientos establecidos en los documentos Manual de Activos de Información y Procedimiento de Activos de Información.

Además, la identificación de las amenazas y vulnerabilidades se apoya en el catálogo definido en el Anexo 4: Lineamientos para la Gestión del Riesgo en Entidades Públicas, el cual es analizado y validado en las mesas de trabajo con los diferentes procesos. Con base en este análisis, se determinan las posibles consecuencias de los riesgos identificados.

**Valoración del Riesgo**

La valoración de los riesgos relacionados con la Seguridad y Privacidad de la Información, en el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. se llevará a cabo siguiendo la metodología para la administración de riesgos descrita en la Guía para la Administración del Riesgo y el Diseño de Controles en Entidades Públicas, emitida por el Departamento Administrativo de la Función Pública (DAFP). Esta metodología se adopta como referencia principal para garantizar un análisis integral y estructurado, utilizando además las tablas de impacto y probabilidad establecidas por la entidad.

En mesas de trabajo con los diferentes procesos de la organización, se analiza el contexto y se identifican los riesgos relevantes. Posteriormente, se realiza un análisis de probabilidad e impacto como valoración preliminar para determinar el nivel del riesgo inherente. Este análisis incluye la asociación de las amenazas, vulnerabilidades y consecuencias, además de identificar los controles necesarios para mitigar dichos riesgos. Los controles se alinean con los establecidos en el Anexo A de la Norma ISO/IEC 27001, cubriendo las siguientes variables clave para garantizar su adecuado diseño y efectividad:

Asignación de responsables: Definición clara de quién es responsable de la implementación y monitoreo del control.

- **Segregación y autoridad:** Determinación de los roles y límites de autoridad de los responsables.
- **Tipo de control:** Clasificación como preventivo, detectivo o correctivo.
- **Implementación:** Especificación de si el control es manual o automatizado.
- **Periodicidad:** Frecuencia con la que debe ejecutarse el control.

- **Propósito:** Objetivo específico del control dentro del sistema de gestión de riesgos.
- **Actividad de control:** Detalle de cómo se realiza el control y cómo se gestionan las observaciones o desviaciones.
- **Evidencia:** Registro documental que demuestre la ejecución efectiva del control.

Se verifica que los controles diseñados sean consistentes en su ejecución para garantizar que cumplan con su propósito de mitigación. La valoración final del riesgo se realiza siguiendo las tablas y metodología especificadas en la guía del DAFP, ajustándose a las necesidades y particularidades del SISTEMA ESTRATÉGICO DE TRANSPORTE PÚBLICO SETP TRANSFEDERAL S.A.S.

**Definición y aprobación de mapas de riesgos y planes de tratamiento.**

Una vez finalizadas las etapas del proceso de administración de riesgos y obtenida la valoración correspondiente de los riesgos relacionados con la Seguridad y Privacidad de la Información, los líderes de los procesos, con el apoyo de los gestores de riesgos, deberán proceder a la formalización y aprobación de los resultados.

Para ello, se utilizará la plataforma del sistema integrado de gestión definida por el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S., donde se registrarán los mapas de riesgos y los planes de tratamiento. Estos documentos incluirán las actividades específicas necesarias para mitigar aquellos riesgos cuyo nivel residual se encuentre clasificado en las categorías Moderada, Alta o Extrema, según los lineamientos y criterios de valoración establecidos por la entidad.

El proceso de formalización garantiza que cada riesgo identificado sea debidamente documentado, asignando responsabilidades claras y definiendo plazos específicos para la implementación de las medidas de mitigación. Además, se asegura que los planes de tratamiento sean revisados y aprobados por las instancias correspondientes, promoviendo un enfoque proactivo y eficiente para la gestión integral de riesgos.

**Materialización**

En caso de que un riesgo identificado se materialice, deberá ser reportado de manera inmediata conforme al procedimiento establecido para la gestión de incidentes de seguridad y privacidad de la información en el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. Este reporte permitirá una respuesta oportuna y el inicio de las acciones correctivas correspondientes.

Posteriormente, será necesario analizar el impacto del incidente y determinar el nuevo nivel de riesgo residual tras su materialización. Los cambios relevantes deberán ser documentados y actualizados en el mapa de riesgos de la entidad, asegurando que la información refleje la realidad de los activos y sus vulnerabilidades.

En caso de que se materialice un riesgo previamente no identificado, este deberá ser reportado y gestionado inmediatamente para iniciar su correspondiente identificación, análisis y valoración en el mapa de riesgos. Esto garantizará que el incidente quede formalizado dentro del sistema

de gestión de riesgos de EL SETP, permitiendo adoptar las medidas necesarias para prevenir su recurrencia y reforzar los controles existentes.

### 1.1. Oportunidad de Mejora

El sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S.., la gestión de riesgos no debe limitarse únicamente a la identificación y mitigación de riesgos existentes. Este análisis debe servir como base para identificar y aprovechar oportunidades de mejora que puedan surgir durante el proceso.

La oportunidad debe interpretarse como una consecuencia positiva derivada del tratamiento eficaz de los riesgos. Por ejemplo, la implementación de controles de seguridad más robustos no solo reduce las vulnerabilidades existentes, sino que también puede abrir caminos hacia una mayor eficiencia operativa, el fortalecimiento de la confianza de los grupos de interés y el cumplimiento de estándares internacionales que posicionen a el sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. como líder en gestión de seguridad de la información y continuidad operativa.

Estas oportunidades, identificadas a partir del análisis de riesgos, deben ser documentadas y evaluadas con el mismo rigor que los riesgos, de modo que puedan traducirse en acciones concretas que contribuyan al logro de los objetivos estratégicos de la entidad.

## 7. RECURSOS

El sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S., en el marco de la gestión de riesgos de Seguridad y Privacidad de la información, dispone de los siguientes recursos.

| RECURSOS | VARIABLE |
|---|---|
| Humanos | Equipo de trabajo del sistema estratégico de transporte público SETP TRANSFEDERAL S.A.S. |
| Técnicos | Guía para la administración del riesgo y el diseño de controles en entidades públicas - Riesgos de gestión, corrupción y seguridad digital del DAFP<br>Herramienta para la gestión de riesgos |
| Logísticos | Gestión de recursos para realizar socializaciones, transferencia de conocimientos y seguimiento a la gestión de riesgos. |
| Financieros | Recursos para la adquisición de conocimiento, recursos humanos, técnicos, y desarrollo de auditorías con un costo aproximado de 81.400.000 |

## 8. PRESUPUESTO APARA LA IMPLEMENTACIÓN DE CONTROLES

La estimación y asignación del presupuesto para el plan de tratamiento de riesgos de Seguridad y Privacidad de la Información identificados en la entidad, corresponderá al dueño del riesgo (líder del proceso), quien es el responsable de contribuir con el seguimiento y control de la gestión, además de la implementación de los controles definidos y del plan de tratamiento