SuperTransporte

VERSIÓN 4.0

PLAN DE TRATAMIENTO DE RIESGOS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

PRESENTACIÓN

La Superintendencia de Transporte, comprometida con el fortalecimiento de condiciones seguras en los entornos digitales y físicos, presenta su Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2025. Este plan tiene como propósito garantizar la protección de los activos de información mediante un enfoque preventivo y estratégico que permita la identificación, análisis, tratamiento, evaluación y monitoreo continuo de los riesgos. La implementación de este plan responde a las disposiciones de la nueva Política General de Seguridad y Privacidad de la Información aplicada mediante la resolución interna 5095 de 2024, y alineada con la normativa vigente, como el CONPES 3995 de 2020, el Decreto 1008 de 2018, la Resolución 500 de 2021 y el Modelo de Seguridad y Privacidad del Ministerio de Tecnologías de la Información y las Comunicaciones (MINTIC). Además, integra estándares internacionales como la ISO 27001 e ISO 31000:2018, que fortalecen la gestión de riesgos y garantizan la continuidad operativa de los procesos institucionales.

Este plan prioriza acciones estratégicas para minimizar el impacto de los riesgos que puedan materializarse, con énfasis en áreas como el desarrollo digital, el empoderamiento ciudadano en entornos digitales, la transformación digital sectorial y territorial, y la inclusión social digital.

En este sentido, se promueve la continuidad en la ejecución de proyectos de transformación digital que refuercen la infraestructura tecnológica, la interoperabilidad entre sistemas, la automatización de trámites y el uso seguro de herramientas digitales para la gestión de la información.

Entre los componentes esenciales del plan se encuentra la gestión integral de los riesgos que afectan la confidencialidad, integridad y disponibilidad de la información. Asimismo, contempla la implementación de controles proactivos para mitigar vulnerabilidades, fomentar una cultura de seguridad de la información y garantizar que todos los proyectos de transformación digital cuenten con lineamientos sólidos de ciberseguridad. La ejecución del Plan de Tratamiento de Riesgos 2025 será liderada por la Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) en coordinación con las demás dependencias, asegurando su mejora continua y su alineación con las necesidades estratégicas de la entidad.

TABLA DE CONTENIDO

1. INFORMACIÓN DE LA ENTIDAD

La Superintendencia de Transporte, como entidad pública del orden nacional, tiene la misión de ejercer la vigilancia, inspección y control sobre los actores del sector transporte en Colombia, asegurando el cumplimiento de las normativas y promoviendo condiciones de confianza y seguridad para los ciudadanos y usuarios. En el marco del Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2025, la Superintendencia refuerza su compromiso con la protección de los activos de información críticos que soportan sus funciones misionales. Este compromiso está orientado a garantizar la confidencialidad, integridad y disponibilidad de la información, respaldando tanto las operaciones internas como la interacción con los sectores vigilados. Su enfoque se alinea con la Política General de Seguridad y Privacidad de la Información, impulsando iniciativas de transformación digital seguras y fortaleciendo la capacidad institucional frente a riesgos en el entorno digital y físico.

2. OBJETIVO GENERAL

Establecer una ruta estratégica para la gestión integral de riesgos de seguridad de la información y digital, que garantice la confidencialidad, integridad y disponibilidad de los activos de información institucionales, mediante la identificación, análisis, tratamiento y monitoreo continuo de riesgos, asegurando su alineación con los objetivos misionales de la entidad y promoviendo un entorno digital seguro y confiable.

2.1 OBJETIVOS ESPECIFICOS:

- Identificar, clasificar y actualizar los activos de información de la entidad en el primer semestre de la vigencia 2025, asegurando que la totalidad cuente con un nivel de criticidad asignado de acuerdo con el procedimiento TIC-PR-015 y el manual TIC-MA-004.
- Continuar con la implementación de controles que preserven la confidencialidad, integridad y disponibilidad de los activos de información, garantizando que las áreas institucionales estén cubiertas por medidas efectivas de seguridad digital.
- Monitorear y evaluar continuamente los riesgos de manera periódica, emitiendo informes y evidenciando los controles efectuados.

- Sensibilizar y capacitar a los funcionarios y contratistas en buenas prácticas de ciberseguridad, promoviendo una cultura institucional de seguridad de la información.

3. ALCANCE:

El Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2025 de la Superintendencia de Transporte abarca a todos los funcionarios, contratistas, vigilados y terceros que interactúan con los activos de información institucionales. Su alcance incluye todos los procesos y actividades de la entidad, garantizando la gestión integral de los riesgos y la protección de la confidencialidad, integridad y disponibilidad de la información, en cumplimiento de las normativas aplicables y fomentando una cultura organizacional enfocada en la seguridad digital.

4. MARCO LEGAL

Describir la normatividad que le aplica al plan, de forma cronológica como ha influido en el tema, con el formato de día, mes y año completo.

- Constitución Política de Colombia, Artículo 15: Reconoce el derecho fundamental a la intimidad y a la protección de los datos personales, estableciendo la obligación del Estado de garantizar su respeto.

- Ley 1581 de 2012: Régimen General de Protección de Datos Personales, que regula el tratamiento de datos y la implementación de políticas para su protección en entidades públicas y privadas.

- Ley 1712 de 2014: Ley de Transparencia y del Derecho de Acceso a la Información Pública, que regula el acceso y protección de la información pública.

- Decreto 1083 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Función Pública”, el cual establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea” y “12. Seguridad Digital”.

- Decreto 1008 de 2018: Establece los lineamientos para la Política de Gobierno Digital, incluyendo principios de seguridad de la información y gestión de riesgos digitales.

- Resolución 500 de 2021: Adopta los estándares y lineamientos para la estrategia de seguridad digital y el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

- Documento CONPES 3995 de 2020: Política Nacional de Confianza y Seguridad Digital, que promueve la protección de datos e infraestructura crítica, fortaleciendo la gestión de riesgos en el entorno digital.

- Guía para la Administración de los Riesgos de Gestión, Corrupción y Seguridad Digital del Departamento Administrativo de la Función Pública (DAFP): Define lineamientos para gestionar riesgos de seguridad digital en entidades públicas.

- Decreto 767 de 2022: Lineamientos generales de la Política de Gobierno Digital, promoviendo la transformación digital con inclusión de estándares de ciberseguridad.

5. DEFINICIONES

Listar el significado de términos técnicos que se desarrollan a lo largo del plan y que contribuyen a facilitar la comprensión del lector.

- **Aceptación del riesgo**: Decisión informada de tomar un riesgo particular.
- **Análisis de riesgo**: Proceso para comprender la naturaleza del riesgo y determinar el nivel de este.
- **Causa:** Origen, comienzo de una situación determinada que genera un efecto o consecuencia.
- **Consecuencia:** Resultado de un evento que afecta los objetivos.
- **Control:** Medida que modifica el riesgo.
- **Evaluación de riesgos:** Proceso de comparación de los resultados del análisis del riesgo con los criterios del riesgo, para determinar si el riesgo, su magnitud o ambos son aceptables o tolerables.

- **Gestión del riesgo:** Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **Incidente de seguridad de la información:** Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información (Confidencialidad, Integridad y Disponibilidad).
- **MSPI:** Modelo de Seguridad y Privacidad de la Información
- **Propietario del riesgo:** Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos.
- **Riesgo de Seguridad de la Información:** Probabilidad de ocurrencia de un evento que genere un impacto sobre la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Riesgo Residual:** El riesgo que permanece tras el tratamiento del riesgo o nivel resultante del riesgo después de aplicar los controles.
- **Tratamiento del Riesgo:** Proceso para modificar el riesgo.
- **Triada de la información:** Conjunto de las propiedades derivadas de la Confidencialidad, Integridad y Disponibilidad de la Información.
- **Valoración del riesgo:** Proceso global de identificación del riesgo, análisis del riesgo y evaluación de los riesgos.
- **Vulnerabilidad:** Debilidad de un activo que puede ser explotada por una o más amenazas.

6. DESARROLLO DEL PLAN

A continuación, se describe el ciclo que se ejecutará para la gestión de riesgos de seguridad de la información, siguiendo las metodologías publicadas por el DAFP y Min Tic, la cual será desarrollada a través de la ejecución de las actividades propuestas en el numeral 4.2

6.1 METODOLOGÍA: La metodología del Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2025 estará alineada con la interacción entre el Modelo de Seguridad y Privacidad de la Información (MSPI) y el Modelo de Gestión de Riesgos de Seguridad Digital (MGRSD), tal como lo establece el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC). Este enfoque integrado permitirá abordar de manera coherente y estructurada la identificación, evaluación y tratamiento

de los riesgos, tanto en el ámbito de la seguridad de la información como en la privacidad de los datos. La metodología garantizará que todos los procesos institucionales de la Superintendencia de Transporte estén enfocados en la clasificación y priorización de los activos de información, considerando los riesgos asociados a cada uno, y promoviendo una cultura organizacional sólida en ciberseguridad y privacidad, en cumplimiento de las normativas vigentes y de las mejores prácticas internacionales.

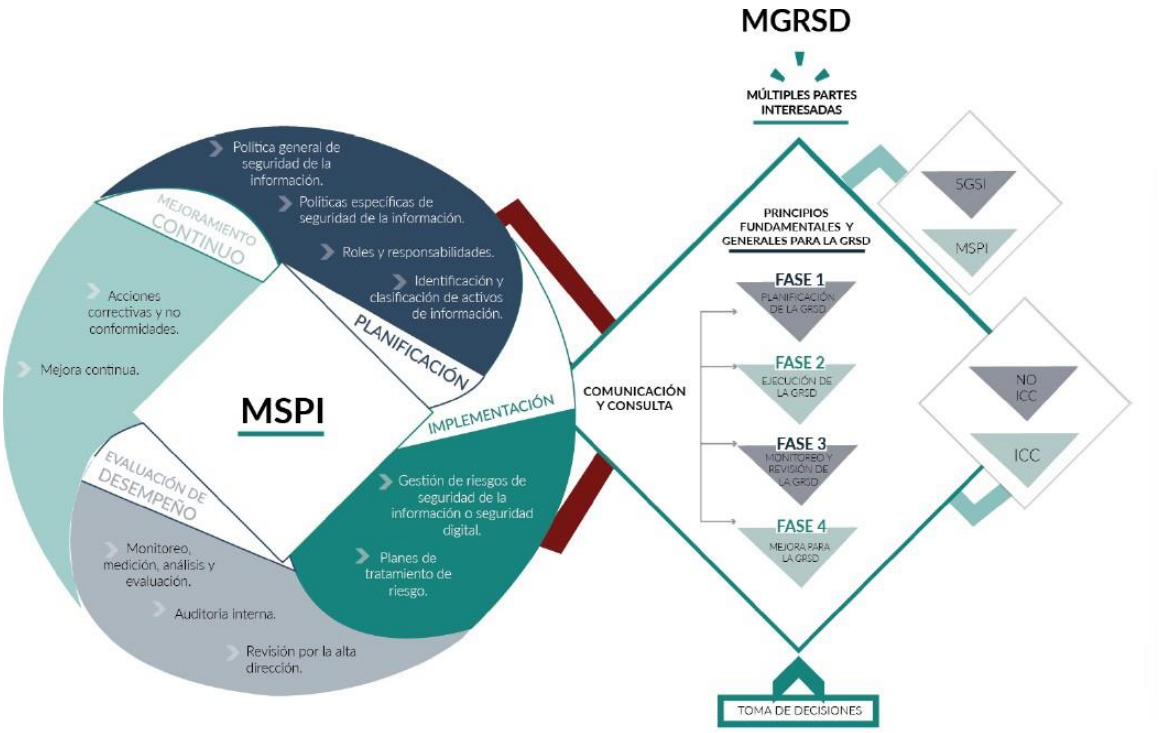

Ilustración 1 Interacción entre el MSPI y el MGRSD. Fuente: MinTIC

Análisis de información

La actividad inicial para la identificación de riesgos, conforme al procedimiento TIC-PR-015 y al manual TIC-MA-004, consistirá en el levantamiento, clasificación y actualización de los activos de información en cada proceso institucional. El líder del proceso será responsable de priorizar los activos calificados con un nivel de riesgo alto, registrados en el formato TIC-FR-010, así como aquellos adicionales que considere relevantes para la generación de los riesgos. Este enfoque garantizará una identificación adecuada y completa de los activos críticos, alineada con las políticas y procedimientos establecidos para la gestión de riesgos en la entidad.

Identificación de riesgos

En el nuevo mapa de riesgos institucional, se han identificado las amenazas y vulnerabilidades asociadas a los activos de información. Para cada activo, se analizan las posibles consecuencias de su materialización y se determina la probabilidad e impacto que pueden afectar la confidencialidad, integridad o disponibilidad de la información, interrumpiendo alguno de los elementos clave de la triada de seguridad. Este análisis permite priorizar los riesgos y establecer medidas preventivas y correctivas para mitigar su impacto en la entidad.

Valoración y análisis del riesgo

Se definen los criterios para:

- Analizar los riesgos identificados.
- Evaluar su impacto y probabilidad de ocurrencia.

Este proceso permite determinar la probabilidad de materialización del riesgo y el nivel de consecuencia o impacto asociado, con el objetivo de estimar la zona de riesgo inherente a cada situación, facilitando la priorización de acciones y la implementación de controles adecuados.

Control del riesgo

De acuerdo con los riesgos identificados, se establecerán los controles necesarios para mitigar o tratar cada uno de ellos, alineados con el Modelo de Seguridad y Privacidad de la Información (MSPI). Para ello, la Entidad se basará en los controles propuestos por la NTC-ISO/IEC 27001:2022, con el fin de reducir la probabilidad de materialización de los riesgos y minimizar el impacto de los incidentes de seguridad.

Estos controles estarán diseñados para fortalecer la protección de la información, garantizar la confidencialidad, integridad y disponibilidad de los activos de información, y asegurar la continuidad de las operaciones.

Monitoreo de riesgos

Se debe dar continuidad al proceso de seguimientos cuatrimestrales del Plan de Tratamiento de Riesgos en Seguridad de la Información, durante los cuales se analizan y verifican los avances de las actividades establecidas. Estos seguimientos incluyen la emisión y publicación de informes detallados, los cuales permiten evaluar el cumplimiento de las acciones previstas y garantizar la efectividad de las medidas implementadas en la mitigación de los riesgos identificados. Además, cada

seguimiento cuenta con evidencias documentales que respaldan el proceso de análisis y verificación, asegurando la transparencia y la correcta aplicación de las medidas de seguridad. Este proceso debe seguir aplicándose de manera continua para asegurar la mejora constante y el cumplimiento de los objetivos del plan.

6.2 ACTIVIDADES DE IMPLEMENTACION 2025

En el marco del Plan de Tratamiento de Riesgos en Seguridad de la Información 2025, se desarrollará un conjunto de actividades estratégicas orientadas a fortalecer la gestión integral de riesgos y garantizar la protección de los activos de información institucionales. Estas acciones incluyen la actualización de documentos clave, la concienciación del personal, la identificación y evaluación de riesgos, la implementación de controles, y el monitoreo y mejora continua del plan. A continuación, se presentan las actividades específicas, sus respectivas estrategias y las evidencias que respaldarán su ejecución.

Estrategia	Actividades	Evidencia
Revisión/actualización de documentación	Actualizar manual de gestión de riesgos de seguridad digital.	Documento: Manual De Gestión De Riesgos De Seguridad De La Información TIC-MA-007 publicado y aprobado
Concienciación sobre conceptos y bases para la identificación de riesgos	Elaborar piezas gráficas y charlas relacionadas con el mapa riesgos.	Piezas gráficas, listados de asistencia, grabación de charlas y correo electrónico con envío masivo.
Identificación de riesgos de seguridad de la información	Realizar revisión, identificación, gestión y actualización sobre los riesgos de seguridad de la información.	Mapa de Riesgos Actualizado y publicado.

Estrategia	Actividades	Evidencia
Plan de tratamiento de riesgos de seguridad de la información	Documentar las actividades relacionadas para implementar los controles establecidos.	Evidencias de los controles, seguimiento y monitoreo de los riesgos.
Aceptación del riesgo de seguridad de la información	Revisar periódicamente de las aprobaciones de las matrices de riesgos de seguridad por el propietario del riesgo (líder del proceso) como declaración formal de la aceptación.	Correo electrónico/memorando
Seguimiento planes de tratamiento de riesgos de seguridad de la información	Revisar la documentación y evidencias de los seguimientos realizados al plan de tratamiento.	Correo electrónico, Actas de sesiones
Mejoramiento	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual.	Correo electrónico, Actas de sesiones
Monitoreo	Reportar actividades de seguimiento a través del plan e indicadores.	Publicación de informes de seguimiento a los riesgos de manera cuatrimestral.

7. CONTROL Y SEGUIMIENTO

La dependencia encargada de realizar el monitoreo, seguimiento y control del plan de acuerdo con la competencia y la normatividad vigente es la Oficina de Tecnologías de la información y las comunicaciones.

8. CONTROL DE CAMBIOS DEL DOCUMENTO

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	20-Ene-2022	Creación del documento
2	20-Dic-2022	Actualización de actividades
3	20-Dic-2023	Actualización de introducción y actividades; se incorpora estrategia de monitoreo.
4	09-Dic-2024	Actualización general del documento, presentación, objetivos, alcance, marco legal, desarrollo del plan, actividades

9. APROBACION DEL DOCUMENTO

Aprobación del documento	
Etapa	**Nombres y cargo**
Elaboró:	Sebastian López Ciro - Contratista
Revisó:	Urías Romero Hernández – Jefe OTIC
Aprobó:	Miembros con voto Comité Institucional de Gestión y Desempeño