SuperTransporte

VERSIÓN 5.0

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

2026

PRESENTACIÓN

La Superintendencia de Transporte, comprometida con el fortalecimiento de un entorno institucional seguro, confiable y resiliente frente a los riesgos digitales, presenta su Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2026. Este instrumento orienta la gestión integral de los riesgos que pueden afectar los activos de información, mediante un enfoque preventivo, estratégico y basado en la mejora continua, que garantiza la identificación, análisis, valoración, tratamiento, comunicación y monitoreo permanente de los riesgos que puedan impactar la confidencialidad, integridad y disponibilidad de la información institucional.

La implementación de este plan se enmarca en la Política General de Seguridad y Privacidad de la Información, adoptada mediante la Resolución Interna 5095 de 2024, y se alinea con la normativa nacional vigente, entre la que se destacan: CONPES 3995 de 2020, que define la Política Nacional de Confianza y Seguridad Digital; Decreto 1008 de 2018, que establece lineamientos para la gestión de la seguridad de la información y la privacidad; la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones, que actualizan y fortalecen el Modelo de Seguridad y Privacidad de la Información (MSPI); y el Modelo Integrado de Planeación y Gestión (MIPG), que articula los procesos institucionales de control, planeación y gestión del riesgo. Asimismo, este plan incorpora las mejores prácticas internacionales, como los lineamientos de las normas ISO/IEC 27001:2022 e ISO 31000:2018, garantizando que la gestión del riesgo sea objetiva, medible y auditable.

El Plan 2026 adopta un enfoque cuantitativo y trazable para la valoración del riesgo, estableciendo criterios uniformes de probabilidad, impacto y nivel residual que permiten priorizar acciones de tratamiento según su criticidad y efectividad. Asimismo, fortalece la cultura de seguridad digital, promoviendo la corresponsabilidad institucional en la protección de la información, la implementación de controles proactivos, la actualización de políticas y procedimientos, la automatización de procesos y la formación continua del talento humano en ciberseguridad y privacidad. Su ejecución, liderada por la OTIC en coordinación con las áreas misionales, estratégicas y de apoyo, busca mantener un sistema de seguridad dinámico, medible y alineado con los lineamientos del MinTIC, consolidando un entorno digital confiable y seguro para la entidad y la ciudadanía.

TABLA DE CONTENIDO

PRESENTACIÓN 2
1. INFORMACIÓN DE LA ENTIDAD 4
2. OBJETIVO GENERAL 4
2.1 OBJETIVOS ESPECIFICOS: 4
4. MARCO LEGAL 5
5. DEFINICIONES 6
6. DESARROLLO DEL PLAN 8
7. CONTROL Y SEGUIMIENTO 13
8. CONTROL DE CAMBIOS DEL DOCUMENTO 13
9. APROBACION DEL DOCUMENTO 14

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 2026, 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 durante el primer semestre de la vigencia 2026, garantizando que todos cuenten con un nivel de criticidad asignado, conforme al procedimiento TIC-PR-015 y al manual TIC-MA-004, y en cumplimiento de la nueva normativa establecida en los Lineamientos para el Inventario y Clasificación de Activos de Información e Infraestructura Crítica Cibernética Nacional del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).
- Dar Continuidad 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.
- Consolidar la gobernanza de la seguridad y privacidad de la información, articulando el Plan de Tratamiento de Riesgos con el Modelo Integrado de Planeación y Gestión (MIPG), el Modelo de Seguridad y Privacidad de la Información (MSPI), el Modelo de Referencia de Arquitectura Empresarial (MRAE 3.0) y el Formulario Único de Reporte de Avances de Gestión (FURAG), con el fin de asegurar la coherencia institucional, la trazabilidad y la alineación estratégica en la gestión del riesgo y la seguridad digital.

3. ALCANCE:

El Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2026 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.

- 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.

- Resolución 2277 de 2025 del MinTIC: Actualiza y fortalece el Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando nuevos lineamientos sobre gestión de riesgos, clasificación de activos de información, infraestructura crítica cibernética, protección de datos personales y monitoreo de la seguridad digital en las entidades del Estado.

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 6.2

6.1 METODOLOGÍA: La metodología del Plan de Tratamiento de Riesgos en Seguridad y Privacidad de la Información 2026 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.

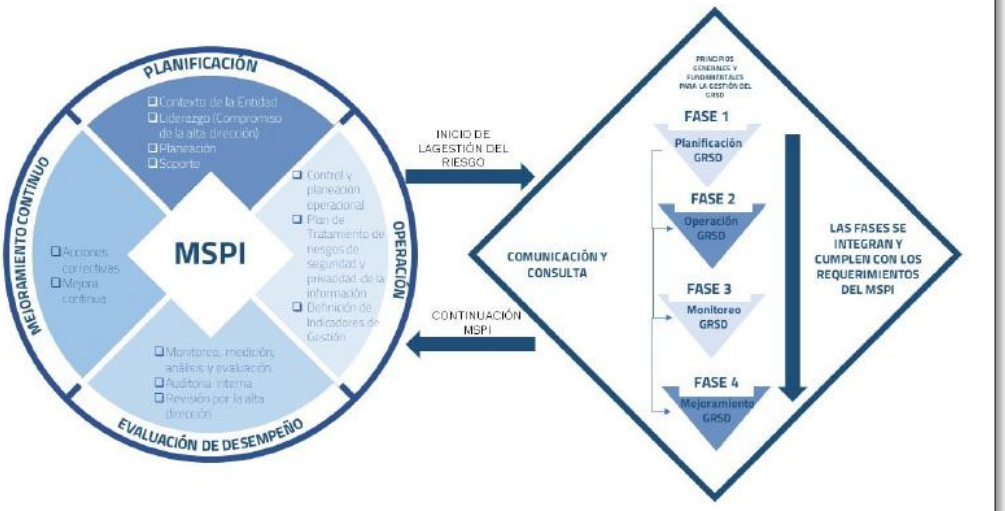

Ilustración 1 Interacción MSPI - Modelo Gestión de Riesgo de seguridad de la información

Fuente: Ministerio de Tecnologías de la Información y las Comunicaciones

6.1.1 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.

6.1.2 Identificación de riesgos

La identificación de riesgos se realiza en el Mapa de Riesgos de Seguridad de la Información (DE-FR-001), donde se registran de manera sistemática los activos de información, junto con las amenazas y vulnerabilidades que podrían comprometer su confidencialidad, integridad o disponibilidad. Este proceso permite analizar el contexto interno y externo, identificar los eventos que pueden afectar los procesos misionales y determinar las condiciones que originan los riesgos, constituyendo la base para su análisis, valoración y tratamiento, en coherencia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

6.1.3 Valoración y análisis del riesgo

En esta etapa se definen los criterios y metodologías necesarios para analizar los riesgos identificados y evaluar su impacto y probabilidad de ocurrencia. El proceso permite determinar la probabilidad de materialización de cada riesgo y el nivel de consecuencia o impacto asociado, con el fin de estimar la zona de riesgo inherente correspondiente. Esta valoración facilita la priorización de los riesgos y orienta la implementación de controles y acciones de tratamiento adecuados, garantizando una gestión objetiva y alineada con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

6.1.4 Control y Tratamiento del riesgo

De acuerdo con los riesgos identificados, se establecen los controles necesarios para su mitigación o tratamiento, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC. Para su definición, la Entidad se apoya en los controles establecidos en la norma NTC-ISO/IEC 27001:2022, orientados a reducir la probabilidad de materialización de los riesgos y a minimizar el impacto de posibles incidentes de seguridad.

Estos controles se diseñan para fortalecer la protección de la información institucional, garantizando la confidencialidad, integridad y disponibilidad de los activos de información, así como la continuidad de las operaciones y la resiliencia de los servicios tecnológicos de la Superintendencia de Transporte.

6.1.5 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.

6.1.6 Documentación y Trazabilidad

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece que la gestión del riesgo debe ser documentada, auditada y trazable, con soporte verificable en cada una de sus etapas. En cumplimiento de ello, la Superintendencia de Transporte mantiene un repositorio para el almacenamiento y gestión de los registros, formatos y evidencias relacionados con la identificación, análisis, valoración, tratamiento y monitoreo de los riesgos, incluyendo informes de seguimiento, planes de acción, actas y registros de aceptación o transferencia. Este repositorio garantiza la transparencia, la trazabilidad de las decisiones y la efectividad del sistema de gestión, facilitando los procesos de auditoría y promoviendo la mejora continua, en concordancia con los lineamientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del MinTIC.

6.1.7 Integración con Otros Modelos

El Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) establece que la gestión de riesgos en seguridad digital debe integrarse con los modelos de gestión institucional, garantizando coherencia y alineación entre las estrategias organizacionales. En este marco, el Modelo de Seguridad y Privacidad de la Información (MSPI) se articula con el Modelo Integrado de Planeación y Gestión (MIPG) y con los instrumentos de evaluación del desempeño institucional, como el Formulario Único de Reporte de Avances de Gestión (FURAG) y el Modelo

de Referencia de Arquitectura Empresarial (MRAE 3.0). Esta integración consolida una estructura unificada de control, planeación y mejora continua, asegurando que los riesgos de seguridad digital se gestionen de manera transversal, trazable y coherente, en alineación con los objetivos estratégicos institucionales.

6.2 ACTIVIDADES DE IMPLEMENTACION 2026

En el marco del Plan de Tratamiento de Riesgos en Seguridad de la Información 2026, 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 el Manual de Gestión de Riesgos de Seguridad de la Información (TIC-MA-007), alineándolo con los lineamientos del MinTIC y la Resolución 2277 de 2025.	Documento: Manual De Gestión De Riesgos De Seguridad De La Información TIC-MA-007 publicado y aprobado.
Inventario y clasificación de activos de información	Identificar, clasificar y actualizar los activos de información, asignando niveles de criticidad conforme al procedimiento TIC-PR-015, al manual TIC-MA-004 y a los lineamientos del MinTIC sobre infraestructura crítica cibernética.	Inventario de activos actualizado y aprobado; evidencia de clasificación y asignación de criticidad.

Estrategia	Actividades	Evidencia
Concienciación sobre conceptos y bases para la identificación de riesgos	Diseñar y ejecutar campañas de sensibilización, piezas gráficas y jornadas informativas sobre el Mapa de Riesgos y la gestión de seguridad digital.	Piezas gráficas, listados de asistencia, grabación de charlas y correo electrónico con envío masivo.
Identificación de riesgos de seguridad de la información	Realizar la revisión, identificación, análisis y actualización de los riesgos de seguridad, registrando los resultados en el Mapa de Riesgos (DE-FR-001).	Mapa de Riesgos Actualizado y publicado.
Plan de tratamiento de riesgos de seguridad de la información	Documentar e implementar las acciones y controles definidos en el plan de tratamiento, conforme al nivel de riesgo residual y los controles ISO/IEC 27001:2022.	Evidencias de los controles, seguimiento y monitoreo de los riesgos. Informes de Seguimiento de Riesgos SDI Cuatrimestrales.
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, Evidencias de los controles, seguimiento y monitoreo de los riesgos. Informes de Seguimiento de Riesgos SDI Cuatrimestrales.

Estrategia	Actividades	Evidencia
Mejoramiento	Identificar oportunidades de mejora conforme los resultados de la evaluación del riesgo residual.	Correo electrónico, Actas de sesiones
Monitoreo	Realizar el seguimiento cuatrimestral a los indicadores del plan, evaluando la efectividad de los controles implementados.	Publicación de informes de seguimiento a los riesgos de manera cuatrimestral.
Mejoramiento continuo	Identificar oportunidades de mejora derivadas del análisis del riesgo residual y de los resultados de auditorías internas.	Actas de sesiones, informes de auditoría y correos de seguimiento.
Integración con modelos de gestión institucional	Articular la matriz de riesgos SDI con el MIPG, el FURAG y el MRAE 3.0, garantizando coherencia con la planeación y evaluación institucional.	Matriz de riesgos institucional actualizada, reportes FURAG y documentación de integración con MRAE.

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, dando los reportes respectivos y evidencias a la oficina de planeación de la entidad.

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
5	01-Dic-2025	Actualización de la presentación y enfoque del documento, de acuerdo con las nuevas directrices de la resolución 2277 de 2025. Se actualizan los objetivos específicos. Se actualiza el marco normativo, se agrega en la metodología los ítems 6.1.6 Documentación y Trazabilidad y 6.1.7 Integración con Otros Modelos dando cumplimiento a la nueva normatividad. En las actividades de implementación se agrega Inventario y clasificación de activos de información. Se incluyen actividades de Mejoramiento continuo e Integración con modelos de gestión institucional.

9. APROBACION DEL DOCUMENTO

Aprobación del documento	
Etapa	**Nombres y cargo**
Elaboró:	Sebastian López Ciro - Contratista Sebastián López C.
Revisó:	Urías Romero Hernández – Jefe OTIC SuperTransporte Firmado digitalmente por URIAS ROMERO HERNANDEZ
Aprobó:	Miembros con voto Comité Institucional de Gestión y Desempeño