SuperTransporte

VERSIÓN 5.0

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2025

PRESENTACIÓN

La evolución del gobierno electrónico en Colombia ha sido un pilar fundamental en la modernización del Estado. En este contexto, la implementación de la Política de Gobierno Digital representa una estrategia clave que redefine la interacción y gobernanza entre los diferentes niveles del Estado y sus grupos de interés. Esta política se articula a través de cuatro pilares fundamentales: una gobernanza efectiva basada en la colaboración entre los órdenes nacional y territorial, así como entre niveles centralizados y descentralizados; habilitadores clave que incluyen arquitectura tecnológica, seguridad y privacidad de la información, cultura digital y apropiación, y servicios ciudadanos digitales; líneas de acción definidas para orientar la implementación; e iniciativas dinamizadoras que impulsan la transformación digital.

La Superintendencia de Transporte de Colombia, consciente de su rol estratégico, asume esta política como un componente esencial para fortalecer la confianza de los ciudadanos, usuarios y grupos de interés. Este compromiso se materializa en un enfoque dirigido a asegurar y optimizar los procesos internos mediante una gestión integral de la seguridad de la información. Este enfoque abarca los procesos, trámites, servicios, sistemas de información, infraestructura y activos de información institucionales, con el objetivo de garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

Tomado de: MAE.G.AS - DOMINIO DE - ARQUITECTURA DE SEGURIDAD
Ministerio de Tecnologías de la Información y las Comunicaciones 2023

La implementación de esta política en la Superintendencia se sustenta en el Modelo de Seguridad y Privacidad de la Información (MSPI). Este modelo es una herramienta esencial que guía la gestión y asegura la implementación efectiva de medidas de seguridad en la entidad. Además de cumplir con los estándares nacionales, el modelo se alinea con las mejores prácticas internacionales, fortaleciendo así la posición de la Superintendencia como un actor clave en la transformación digital del sector transporte en Colombia.

Este documento se desarrolla en el marco de las directrices y lineamientos establecidos en la Guía General del Dominio de Arquitectura de Seguridad y se estructura siguiendo la metodología del Modelo de Arquitectura Empresarial (MAE) del MinTIC, garantizando su alineación con los requerimientos regulatorios, estratégicos y tecnológicos 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 vigilar, inspeccionar y controlar a los actores del sector transporte en Colombia, garantizando el cumplimiento de las normativas y promoviendo condiciones de confianza y seguridad para los ciudadanos y usuarios.

En este contexto, en el marco del Plan de Seguridad y Privacidad de la Información 2025, la Superintendencia refuerza su compromiso con la protección de los activos de información que son esenciales para el desarrollo de sus funciones misionales. Este plan tiene como objetivo principal asegurar la confidencialidad, integridad y disponibilidad de la información tanto en las operaciones internas como en la interacción con los sectores vigilados.

El Plan de Seguridad y Privacidad de la Información está alineado con la Resolución 5095 de 2024, que adopta la Política General de Seguridad y Privacidad de la Información. Este plan promueve iniciativas de transformación digital seguras y fortalece la capacidad institucional para garantizar la protección de los procesos, sistemas y datos críticos de la Superintendencia. De este modo, se asegura que la información se mantenga protegida frente a amenazas y vulnerabilidades, tanto en el entorno digital como físico.

2. OBJETIVO GENERAL.

Establecer el Plan de Seguridad y Privacidad de la Información mediante actividades que permitan definir, implementar, operar, monitorear, revisar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información (MSPI) y la estrategia de Seguridad Digital del Modelo de Arquitectura Empresarial (MAE) del MinTIC, asegurando su completa alineación con los requerimientos regulatorios, estratégicos y tecnológicos de la entidad.

2.1 Objetivos Específicos.

- ✓ Implementar y optimizar el Modelo de Seguridad y Privacidad de la Información, con el objetivo de mantener y elevar el nivel de madurez de la entidad en esta materia.
- ✓ Promover el fortalecimiento y la apropiación de prácticas de Seguridad Digital dentro de la Superintendencia de Transporte, asegurando su integración en las operaciones diarias.

- ✓ Reducir las brechas de seguridad y garantizar entornos de trabajo seguros, protegiendo los procesos, sistemas y datos institucionales.

3. ALCANCE.

El Plan de Seguridad y Privacidad de la Información 2025 de la Superintendencia de Transporte aplica a todos los funcionarios, contratistas, vigilados y terceros que interactúan con los activos de información de la entidad. Su alcance cubre los procesos y actividades institucionales, con el objetivo de garantizar la protección de la confidencialidad, integridad y disponibilidad de la información. Este plan asegura el cumplimiento de las normativas vigentes y fomenta una cultura organizacional orientada hacia la seguridad digital, fortaleciendo las capacidades de la entidad para gestionar de manera integral sus activos de información y los servicios asociados.

4. MARCO LEGAL.

- 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”
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012
- Decreto 886 de 2014. Por el cual se reglamenta el Registro Nacional de Bases de Datos.
- 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”
- Decreto 103 de 2015. Por medio del cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.

- Decreto 1074 de 2015. Por medio del cual se expide el Decreto Reglamentario del Sector Comercio, Industria y Turismo. Reglamenta parcialmente la Ley 1581 de 2012 e imparten instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 de 2015. Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones.
- Decreto 1083 de 2015 sustituido por el artículo 1º del Decreto 1499 de 2017 - políticas de Gestión y Desempeño Institucional, ("11. Gobierno Digital, antes Gobierno en Línea" y "12. Seguridad Digital)
- Decreto 1008 de 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.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano
- 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.
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.
- Resolución 500 del 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"
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP

5. DEFINICIONES.

- Activo de Información: Cualquier recurso que contiene o soporta información, incluyendo datos, sistemas informáticos, redes, aplicaciones, documentos físicos y personales relacionados con la entidad.

- Análisis de Vulnerabilidades: Identificación del nivel de exposición existentes en los sistemas, haciendo pruebas de intrusión, que sirven para verificar y evaluar la seguridad física y lógica de los sistemas de información, redes de computadoras, aplicaciones web, bases de datos y servidores.

- Amenaza: Evento o circunstancia con el potencial de causar daño a los activos de información o a la operación de los sistemas de una organización.

- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.

- Confidencialidad: Propiedad de la información que garantiza que el acceso a los datos sea autorizado únicamente a personas, procesos o sistemas debidamente identificados.

- CSIRT: Equipos de respuesta a incidentes de seguridad.

- Disponibilidad: Propiedad que asegura que la información y los servicios relacionados estén accesibles y utilizables cuando se requieran.

- Integridad: Propiedad que garantiza la exactitud y completitud de los datos, evitando su alteración no autorizada durante su almacenamiento, procesamiento o transmisión.

- Modelo de Seguridad y Privacidad de la Información (MSPI): Marco de gestión adoptado por las entidades públicas para implementar controles que garanticen la protección de los activos de información frente a amenazas físicas, digitales y organizacionales.

- Riesgo de Seguridad de la Información: Posibilidad de que una amenaza materialice vulnerabilidades sobre los activos de información, afectando su confidencialidad, integridad o disponibilidad.

- Política de Seguridad y Privacidad de la Información: Documento normativo que establece los lineamientos y principios básicos para proteger los activos de información de una organización en concordancia con los estándares legales y regulatorios aplicables.

- Seguridad Digital: Conjunto de medidas y estrategias implementadas para proteger los activos digitales de una organización, asegurando su funcionamiento óptimo frente a ataques cibernéticos, accesos no autorizados o fallas en los sistemas.

- Transformación Digital Segura: Proceso de adopción de tecnologías digitales que integra medidas de seguridad para garantizar la protección de datos e infraestructura tecnológica de la entidad.

- Usuario autorizado: Persona que, mediante autorización formal, tiene acceso legítimo a los activos de información para realizar tareas específicas.

- Vulnerabilidad: Debilidad o fallo en un sistema, proceso o control de seguridad que puede ser explotado por una amenaza para causar un impacto adverso.

6. DESARROLLO DEL PLAN.

Bajo el marco del Modelo de Seguridad y Privacidad de la Información (MSPI), y considerando el análisis del contexto institucional y estratégico, la Oficina TIC de la Superintendencia de Transporte define un conjunto de actividades técnicas diseñadas para implementar y fortalecer las estrategias de seguridad digital.

Estas actividades están alineadas con los lineamientos establecidos en la Resolución 500 de 2021, que norma la estrategia de seguridad digital como habilitador clave de la Política de Gobierno Digital. En este contexto, se prioriza la adopción de estándares y controles específicos que aseguren la protección integral de los activos de información, así como la integración eficiente de medidas de seguridad en los procesos digitales de la entidad.

Esta metodología asegura la ejecución de estrategias en conformidad con las buenas prácticas internacionales como ISO/IEC 27001 y NIST, optimizando los pilares fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad. Asimismo, fomenta una gobernanza digital robusta y tecnológicamente avanzada, alineada con la estrategia de Seguridad Digital del Modelo de Arquitectura Empresarial (MAE) del MinTIC, reforzando así la capacidad institucional frente a los retos del entorno digital actual.

6.1 Contexto institucional.

La Superintendencia de Transporte tiene como objetivo principal la vigilancia, inspección, y control que le corresponden al presidente de la República como suprema autoridad administrativa en materia de tránsito, transporte y su infraestructura de conformidad con la ley y la delegación establecida en este decreto

acceso, seguridad y legalidad, en aras de contribuir a una logística eficiente del sector.

Misión
Somos la Superintendencia encargada de supervisar la efectiva prestación del servicio público de transporte, su infraestructura y servicios conexos de forma incluyente, accesible y segura, propendiendo por el derecho fundamental a la vida y la protección a los usuarios.

Visión
Para el 2026, la Superintendencia de Transporte será reconocida como una entidad cercana e incluyente con sus grupos de valor e interés, a través, entre otros, del uso de tecnologías digitales, fomentando la legalidad, la construcción de la paz, la protección de los usuarios y la vida, en todo el territorio nacional.

6.2 Contexto Estratégico.

CONTEXTO ESTRATÉGICO ARTICULADO	
Objetivo Estratégico al que Contribuye	OE02 Fortalecer las Tecnologías de la Información y las Telecomunicaciones
Modelo Integrado de Planeación y Gestión - MIPG	Política Gobierno Digital Política de Seguridad Digital Política de Gestión Documental Política de Transparencia, acceso a la información pública y lucha contra la corrupción

6.3 Metodología.

La implementación del Plan de Seguridad y Privacidad de la Información de la Superintendencia de Transporte se basa en una gestión integral del Modelo de Seguridad y Privacidad de la Información (MSPI), complementada con los lineamientos establecidos en el Modelo de Arquitectura Empresarial (MAE) por el MinTIC. Esta metodología garantiza que los procesos relacionados con la seguridad y privacidad de la información estén alineados con los estándares de buenas prácticas, asegurando además su coherencia con los objetivos estratégicos de la entidad. Este enfoque permite una implementación estructurada y eficaz, asegurando la protección de los activos de información y la correcta integración con las políticas tecnológicas y organizacionales de la entidad.

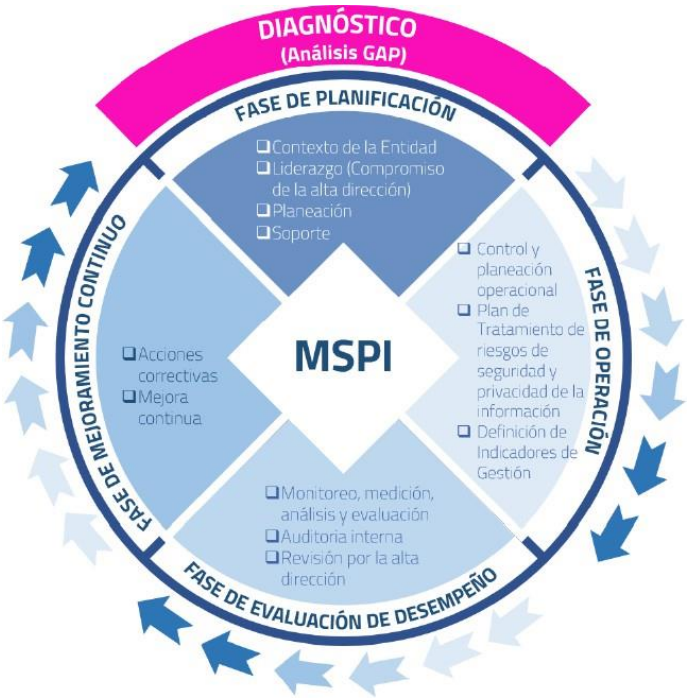

Ilustración 1. Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.

6.4 Actividades de Implementación.

Planificación – Gestión de activos de información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Actualización activos de información 2025	Generar estrategia de sensibilización y reconocimiento de los activos de información	Pieza gráfica
	Charla de sensibilización de conceptos sobre activos de información – socialización manual en su versión TIC-MA-004	Actas de sesiones de sensibilización y capacitación
	Enviar por correo electrónico MEMORANDO INTERNO solicitando la actualización de activos de información a los líderes de proceso.	Correo electrónico Memorando interno
	Revisar de los activos de información reportados en el formato TIC-FR-010	Correo electrónico
	Retroalimentar y corregir de los activos reportados.	Correo electrónico / actas de mesa de trabajo

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	Recibir de formato final y Memorando de entrega final por parte de los líderes de proceso.	Oficio de aceptación y entrega de activos
	Generar informe del proceso de actualización de los activos	Informe Final de Proceso
	Publicar en la página web de la entidad la Matriz de activos Anonimizada.	Matriz Publicada en la página web

Planificación – Gestión de riesgos de seguridad de la información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Actualización de documentación de riesgos de seguridad de la información	Evaluar la estrategia de seguridad digital para integrar a la política de riesgo de la entidad	Política gestión del riesgo actualizada en cadena valor
	Socializar documentos actualizados	Correo electrónico y pieza gráfica.
Identificación, consolidación de riesgos de seguridad de la información y seguridad digital	Identificar, analizar, actualizar y evaluar los riesgos de Seguridad de la Información	Matriz de riesgos publicada en página web
Seguimiento planes de tratamiento	Realizar Seguimiento a los planes de manejo de riesgo de seguridad de la información.	Formato de seguimiento de planes de riesgos.
	Emitir informes cuatrimestrales de seguimiento a los riesgos con las respectivas evidencias.	Informes de riesgos Cuatrimestrales entregados y publicados en página web.
Evaluación de riesgos residuales	Evaluar el riesgo residual de los riesgos identificados	Matriz de riesgo / actas sesiones.

Planificación – Toma de conciencia y comunicación

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Conciencia y comunicación	Elaborar matriz de cultura y apropiación con los temas relacionados a seguridad de la información	Documento con actividades de cultura y apropiación

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Ejecución de la estrategia de cultura y apropiación en seguridad de la información	Llevar a cabo las acciones que fomenten la cultura organizacional en materia de seguridad de la información	Correo electrónico, piezas gráficas
Medición de apropiación en seguridad de la información	Ejecutar acción programada que permita medir la apropiación de los conceptos/procedimientos de seguridad en la Entidad, a través de eventos controlados de phishing e ingeniería social	Correo electrónico, actas mesa de trabajo, informes
	Incorporar simulaciones de hacking ético en entornos controlados para aumentar la conciencia sobre seguridad y detectar vulnerabilidades.	Simulaciones y ejercicios de Hacking Ético.

Operación - Implementación

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
MSPI	Autodiagnóstico MSPI	Actualizar autodiagnóstico del MSPI	Autodiagnóstico
Controles NTC/IEC ISO 27001:2022	Creación Declaración de aplicabilidad de controles de seguridad de la información	Definir y actualizar de controles aplicados en la Entidad.	Matriz de Declaración de Aplicabilidad
	Implementación de controles de seguridad de la información	Implementar las políticas de seguridad definidas.	Reportes
Gestión de Vulnerabilidades	Estructuración y ejecución del plan de análisis de vulnerabilidades -interno y externo-	Elaborar el plan de análisis de vulnerabilidades, alcance y coordinar ejecución pruebas.	Plan de análisis de vulnerabilidades Informe d ejecución del plan
	Plan remediación de vulnerabilidades -interno y externo-	Establecer plan de remediación de vulnerabilidades	Correo electrónico / actas
	Re-testeo	Ejecutar pruebas sobre las actividades de parcheo	Documentos con nuevo análisis
	Ejercicios de Análisis de Vulnerabilidades de las aplicaciones críticas, con apoyo del CSIRT y COLCERT.	Ejecutar análisis de vulnerabilidades con apoyo del CSIRT y COLCERT	Reporte e informes de los análisis de vulnerabilidades

Operación - Gestión de incidentes

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Sensibilización sobre incidentes de seguridad.	Socializar la documentación creada/actualizada.	Actas sesiones Pieza gráfica
CSIRT PONAL / CSIRT / Comando Conjunto Cibernético - CCOC	Socializar con el equipo TI los boletines informativos y de gestión para la prevención de incidentes de seguridad.	Correo electrónico
	Ejecutar ejercicios preventivos de análisis de vulnerabilidades en conjunto, con el fin de mantener la página web, las aplicaciones y la infraestructura tecnológica de la entidad segura.	Reporte de los ejercicios de análisis de vulnerabilidades realizados
Eventos/vulnerabilidades	Realizar seguimiento a las herramientas de seguridad informática validando comportamientos sospechosos sobre la infraestructura TI	Correo electrónico / actas sesiones

Operación - Continuidad de seguridad de la información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Prueba, mantenimiento y revisión de continuidad	Ejecutar pruebas sobre las estrategias definidas e implementadas	Plan de pruebas de continuidad, Informe ejecución de pruebas
	Alinear las estrategias de seguridad con Plan de continuidad de negocio (BCP), Plan de recuperación ante desastres (DRP), Plan de manejo de la crisis (CMP)	Plan de continuidad de negocio (BCP), Plan de recuperación ante desastres (DRP), Plan de manejo de la crisis (CMP) actualizados

Evaluación de desempeño

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Indicadores MSPI	Actualización de Indicadores	Revisar y actualizar de acuerdo con los objetivos del MSPI.	Seguimiento de indicadores
	Gestión de indicadores	Reportar seguimiento de los indicadores	Reportes

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	Implementación de la Hoja de ruta del PESI. Plan Estratégico de Seguridad de la Información	Ejecutar las acciones contenidas en el PESI de acuerdo con el cronograma establecido	Acciones efectuadas e indicadores de avances trimestrales.

Mejoramiento continuo

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Mejora	Visitas de inspección	Revisar el cumplimiento de los procedimientos y políticas implementadas en materia de seguridad.	Informe
	Reporte de oportunidades de mejora	Generar oportunidades de mejora que se requieran, derivadas de las visitas de inspección y revisión de la documentación del MSPI	Oportunidades de mejora
	Apoyarse en entidades del sector y expertos a través de mesas intersectoriales para fortalecer los parámetros de seguridad, promoviendo la colaboración y el intercambio de mejores prácticas.	Participar en las mesas intersectoriales y acoger las recomendaciones que se emitan	Participación en mesas y ejercicios de seguridad informática

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 Oficina de Tecnologías de la información y las comunicaciones.

8. CONTROL DE CAMBIOS DEL DOCUMENTO.

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	30-Nov-2020	Creación del documento
2	20-Ene-2022	Actualización del plan de seguridad digital y desagregación de actividades por componente que se desarrollaran durante el año y de acuerdo con el anexo 1 de la resolución 500 del 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"
3	20-Dic-2022	Actualización de la presentación y actividades a ejecutar en el 2023
4	20-Dic-2023	Actualización de introducción Actualización de actividades
5	09-Dic-2024	Actualización general del documento, presentación, objetivos, alcance, marco legal, desarrollo del plan, inclusión de actividades en cada ítem del capítulo 6.4

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
Aprobó:	Miembros con voto Comité Institucional de Gestión y Desempeño