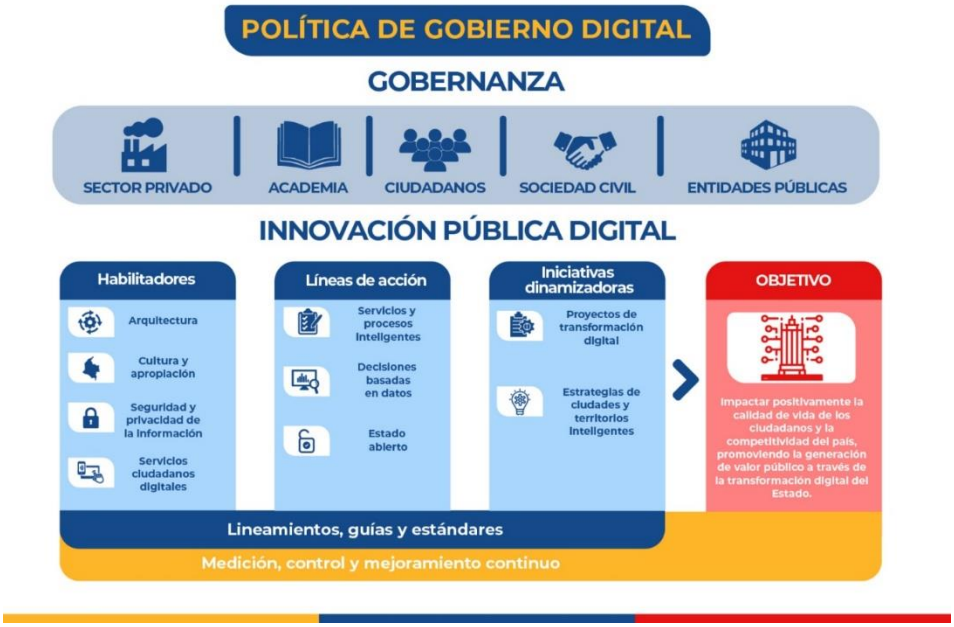
PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

PRESENTACIÓN

La evolución del gobierno electrónico en Colombia ha llevado a la implementación de la Política de Gobierno Digital, una estrategia que redefine la interacción y gobernanza entre los diferentes niveles del Estado y los grupos de interés. Esta política se articula a través de cuatro pilares fundamentales: (i) una gobernanza efectiva, basada en la colaboración entre el orden nacional y territorial, y entre niveles centralizados y descentralizados, (ii) habilitadores clave que incluyen arquitectura tecnológica, seguridad y privacidad de la información, cultura digital y apropiación, y servicios ciudadanos digitales, (iii) líneas de acción definidas para guiar la implementación y (iv) iniciativas dinamizadoras para impulsar la transformación digital.



En este contexto, la Superintendencia de Transporte de Colombia asume un papel activo al adoptar este plan como un componente esencial para reforzar la confianza de ciudadanos, usuarios y grupos de interés. El enfoque se centra en asegurar y eficientar los procesos internos a través de una rigurosa gestión de la seguridad de la información. Este enfoque abarca todos los procesos, trámites, servicios, sistemas de información, infraestructura y demás activos de información institucionales. El objetivo es garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos.

La implementación de esta política en la Superintendencia se basa en el Modelo de Seguridad y Privacidad de la Información, una herramienta clave que orienta la gestión y la implementación efectiva de la seguridad de la información en la entidad. Este modelo no solo cumple con los estándares nacionales, sino que también se alinea con las mejores prácticas internacionales, fortaleciendo la posición de la Superintendencia como un actor clave en la transformación digital del sector del transporte en Colombia.

TABLA DE CONTENIDO

1. OBJETIVO GENERAL

Establecer el Plan de Seguridad y Privacidad de la información a través de actividades que permitan establecer, implementar, operar, monitorear, revisar y mejorar continuamente el Modelo de Seguridad y Privacidad de la Información – MSPI y la estrategia de Seguridad Digital.

1.1 Objetivos Específicos

- Avanzar en la implementación del modelo de seguridad y privacidad de la información, con el propósito de mantener y mejorar el nivel de madurez de la entidad en materia de seguridad y privacidad de la información.
- Fortalecer el uso y apropiación en materia de Seguridad Digital en la Superintendencia de Transporte.

2. 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”
- Ley 1581 de 2012. “Por la cual se dictan disposiciones generales para la protección de datos personales”.
- 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 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.
- 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 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.
- 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 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.

- 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”
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- CONPES 3995 de 2020. Política Nacional de Confianza y Seguridad Digital.

3. DEFINICIONES

- Activos de información: es: “algo que una organización valora y por lo tanto debe proteger”. Se puede considerar como un activo de información a: los datos creados o utilizados por un proceso de la organización en medio digital, en papel o en otros medios. Es importante precisar que el concepto de activos de información definido en la ley 1712 de 2014 es diferente al concepto que maneja el MSPI – ISO 27001.
- 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
- CSIRT: Equipos de respuesta a incidentes de seguridad.
- COLCERT: Grupo de Respuesta a Emergencias Cibernéticas de Colombia.
- MSPI: Modelo de Seguridad y Privacidad de la Información

4. DESARROLLO DEL PLAN

A través del contexto institucional, estratégico y la metodología definida del Modelo de Seguridad y Privacidad de la Información – MSPI, la oficina TIC define una serie de actividades que permiten ejecutar las estrategias de gobierno digital establecidas en 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”

4.1. 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 que supervisa el servicio público de transporte, la actividad portuaria y la infraestructura, por una Colombia conectada, incluyente y competitiva.

Visión

En 2022 seremos reconocidos en el País, como la Superintendencia que de manera efectiva y transparente ejerce sus funciones de supervisión, protege a los usuarios y contribuye al fortalecimiento del sector transporte.

4.2. 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

4.3. Metodología

Es gestión propia del Modelo de Seguridad y Privacidad de la Información:

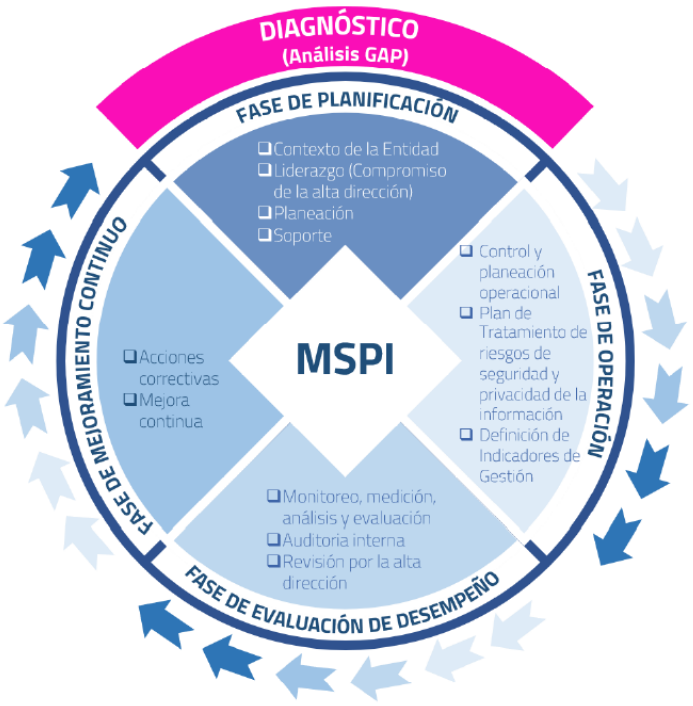


Ilustración 1. Ciclo de operación del modelo de seguridad y privacidad de la información, Fuente: MinTic.

4.4. Actividades de Implementación

Planificación – Gestión de activos de información

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
Actualización activos de información 2024	Generar de pieza gráfica para sensibilización	Pieza gráfica
	Charla de sensibilización de conceptos sobre activos de información – socialización manual en su nueva versión TIC-MA-004	Actas de sesiones de sensibilización y capacitación
	Enviar de correo electrónico solicitando la actualización de activos de información a los líderes de proceso.	Correo electrónico
	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
	Recibir de formato final y oficio de entrega por parte de los líderes de proceso.	Oficio de aceptación y entrega de activos

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 y evaluar los riesgo de todos los procesos.	Matriz de riesgos
	Aceptación y aprobación de los riesgos identificados en cada uno de los procesos	Matriz de riesgos publicada en cadena de valor.
	Elaborar planes de tratamiento de riesgos	Matriz de riesgos publicada en cadena de valor.
Seguimiento planes de tratamiento	Realizar Seguimiento a los planes de manejo de riesgo de seguridad de la información establecidos por cada uno de los procesos y subprocesos, con sus respectivas evidencias.	Formato de seguimiento de planes de riesgos.
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
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

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.	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

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
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

Evaluación de desempeño

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

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

4. 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.

5. 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

6. APROBACIÓN DEL DOCUMENTO

Aprobación del documento		
Etapa	**Nombres y apellidos**	**Cargo**
Elaboro	Maria Alejandra Suarez	Contratista
Aprobó	Miembros con voto	Comité Institucional de Gestión y Desempeño