SuperTransporte

VERSIÓN 6.0

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2026

PRESENTACIÓN

La evolución del Gobierno Digital en Colombia ha constituido un pilar esencial en la modernización del Estado y en la consolidación de una administración pública más eficiente, transparente e innovadora. En este contexto, la Política de Gobierno Digital se erige como una estrategia integral que redefine la interacción entre las entidades públicas, los ciudadanos y los grupos de interés, promoviendo la confianza y la colaboración entre los diferentes niveles de gobierno.

Esta política se fundamenta en cuatro pilares interdependientes:

- Una gobernanza efectiva, basada en la articulación entre los órdenes nacional y territorial, y entre las estructuras centralizadas y descentralizadas.
- Habilitadores claves, como la arquitectura tecnológica, la seguridad y privacidad de la información, la cultura y apropiación digital, y los servicios ciudadanos digitales.
- Líneas de acción que orientan la implementación de políticas, estrategias y proyectos institucionales.
- Iniciativas dinamizadoras que impulsan la innovación y la transformación digital en el sector público.

En coherencia con lo anterior, la Superintendencia de Transporte de Colombia, consciente de su papel estratégico en la vigilancia y control del sector transporte, adopta esta política como un componente esencial para consolidar la confianza de los ciudadanos, usuarios y actores del sistema. Este compromiso se refleja en la implementación de un enfoque integral de gestión de la seguridad y privacidad de la información, orientado a proteger los activos institucionales y garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos de sus vigilados.

La aplicación de este enfoque se desarrolla mediante la adopción del Modelo de Seguridad y Privacidad de la Información (MSPI), el cual constituye una herramienta fundamental para guiar la gestión de la seguridad de la información en la entidad. Dicho modelo permite establecer, implementar, operar, monitorear y mejorar las medidas técnicas, administrativas y organizacionales necesarias para proteger los activos de información de la Superintendencia, en alineación con los estándares nacionales e internacionales.

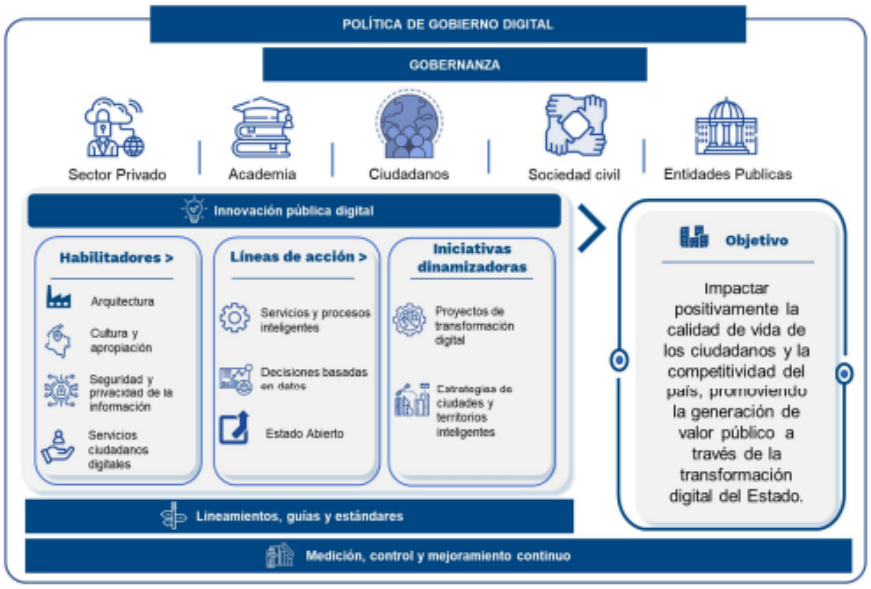

Ilustración 2. Habilitador de Arquitectura en la estructura de la Política de Gobierno Digital (Fuente: propia)

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.

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

TABLA DE CONTENIDO

PRESENTACIÓN 2
1. INFORMACIÓN DE LA ENTIDAD. 5
2. OBJETIVO GENERAL. 5
2.1 Objetivos Específicos. 6
4. MARCO LEGAL. 7
5. DEFINICIONES 8
6. DESARROLLO DEL PLAN. 10
6.1 Contexto institucional. 10
6.2 Contexto Estratégico. 11
6.3 Metodología. 11
6.4 Actividades de Implementación. 13
7. CONTROL Y SEGUIMIENTO. 17
8. CONTROL DE CAMBIOS DEL DOCUMENTO. 17
9. APROBACION DEL DOCUMENTO. 18

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 2026, 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 se encuentra alineado con la nueva Resolución 2277 de 2025, mediante la cual el Ministerio de Tecnologías de la Información y las Comunicaciones adopta la Política General de Seguridad y Privacidad de la Información y establece los lineamientos para su implementación en las entidades públicas. Este plan orienta las acciones de la Superintendencia de Transporte hacia la consolidación de un entorno digital confiable, promoviendo la adopción de prácticas seguras en el desarrollo de la transformación digital institucional. Asimismo, fortalece la capacidad operativa y tecnológica de la entidad para garantizar la protección de sus procesos, sistemas y datos críticos, asegurando que la información permanezca resguardada frente a amenazas, vulnerabilidades y riesgos que puedan comprometer su confidencialidad, integridad, disponibilidad y privacidad, tanto en el entorno físico como digital.

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.
- ✓ Fortalecer la gestión de riesgos de seguridad y privacidad de la información, mediante la identificación, evaluación, tratamiento y monitoreo continuo de los riesgos asociados a los activos de información.
- ✓ Asegurar el cumplimiento normativo frente a la Política General de Seguridad y Privacidad de la Información, la Política de Gobierno Digital y demás disposiciones vigentes aplicables a la entidad.
- ✓ Garantizar la continuidad del negocio y la resiliencia institucional, mediante la implementación de medidas preventivas y correctivas que permitan mantener la operación de los servicios críticos ante incidentes de seguridad.
- ✓ Consolidar la mejora continua del Sistema de Gestión de Seguridad y Privacidad de la Información, a través del seguimiento, evaluación y actualización permanente de los controles implementados.

3. ALCANCE.

El Plan de Seguridad y Privacidad de la Información 2026 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: Modifica el Código Penal, crea el bien jurídico de la protección de la información y de los datos, y establece medidas para preservar la seguridad de los sistemas que utilizan tecnologías de la información y las comunicaciones.
- CONPES 3701 de 2011: Lineamientos de política para la Ciberseguridad y la Ciberdefensa en Colombia.
- Ley 1581 de 2012: Dicta disposiciones generales para la protección de datos personales.
- Decreto 1377 de 2013: Reglamenta parcialmente la Ley 1581 de 2012 en materia de autorización y tratamiento de datos personales.
- Decreto 886 de 2014: Reglamenta el Registro Nacional de Bases de Datos (RNBD).
- Ley 1712 de 2014: Crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional.
- Decreto 103 de 2015: Reglamenta parcialmente la Ley 1712 de 2014 sobre transparencia y acceso a la información pública.
- Decreto 1078 de 2015: Expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones (TIC), que integra las disposiciones de Gobierno Digital, seguridad de la información y servicios ciudadanos digitales.
- Decreto 1074 de 2015: Expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo; reglamenta parcialmente la Ley 1581 de 2012 en materia de protección de datos personales.
- Decreto 1083 de 2015, modificado por el Decreto 1499 de 2017: Define las políticas de Gestión y Desempeño Institucional, incluyendo los componentes de Gobierno Digital y Seguridad Digital.
- CONPES 3854 de 2016: Establece la Política de Seguridad Digital del Estado Colombiano.
- Decreto 612 de 2018: Fija directrices para la integración de los planes institucionales y estratégicos al Plan de Acción de las entidades públicas.
- Decreto 1008 de 2018: Establece los lineamientos generales de la Política de Gobierno Digital, subrogando el capítulo 1 del título 9 del Decreto 1078 de 2015.
- CONPES 3995 de 2020: Adopta la Política Nacional de Confianza y Seguridad Digital.

- Ley 2108 de 2021: Declara el acceso a Internet como servicio público esencial y regula aspectos de conectividad y seguridad digital.
- Guía para la administración de riesgos de gestión, corrupción y seguridad digital, del Departamento Administrativo de la Función Pública (DAFP).
- Decreto 088 de 2024: Actualiza disposiciones sobre Servicios Ciudadanos Digitales y lineamientos del ecosistema de confianza digital.
- Resolución 2277 de 2025 del MinTIC: Adopta la Política General de Seguridad y Privacidad de la Información y actualiza el Modelo de Seguridad y Privacidad de la Información (MSPI), incorporando lineamientos sobre gestión de riesgos, clasificación de activos, infraestructura crítica cibernética, protección de datos personales y monitoreo continuo de la seguridad digital en las entidades públicas.
- Norma Técnica ISO/IEC 27001:2022: Establece los requisitos para la implementación y mejora continua de los sistemas de gestión de seguridad de la información (SGSI), en armonía con el MSPI.

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, normativo y estratégico, la Oficina TIC de la Superintendencia de Transporte define un conjunto de actividades técnicas, administrativas y de gestión orientadas a fortalecer la seguridad y privacidad de la información, en cumplimiento de los lineamientos establecidos en la Resolución 2277 de 2025 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Esta resolución adopta la Política General de Seguridad y Privacidad de la Información y establece los lineamientos para la implementación, seguimiento y mejora continua del MSPI en las entidades públicas. En este marco, el presente plan promueve la adopción de controles, estándares y buenas prácticas internacionales que garanticen la protección integral de los activos de información, la gestión efectiva de los riesgos y la incorporación de medidas de seguridad en los procesos digitales, servicios, sistemas y plataformas tecnológicas de la entidad.

La metodología empleada se basa en el ciclo de mejora continua (PHVA) y en la aplicación de referentes internacionales como las normas ISO/IEC 27001:2022 y los lineamientos del NIST, orientados a optimizar los pilares fundamentales de la seguridad de la información: confidencialidad, integridad, disponibilidad y privacidad. Asimismo, fomenta una gobernanza digital sólida y proactiva, articulada con la estrategia de Seguridad Digital definida en el Modelo de Arquitectura Empresarial (MAE) del MinTIC, fortaleciendo la capacidad institucional de la Superintendencia frente a los desafíos del entorno digital actual y asegurando la sostenibilidad del modelo de gestión.

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
Política de Gobierno Digital	Alinea las acciones del plan con los habilitadores tecnológicos y los servicios ciudadanos digitales definidos por el MinTIC, garantizando el uso seguro, eficiente y confiable de las tecnologías en la prestación de los servicios institucionales.
Política de Seguridad Digital	Se enmarca en los lineamientos de la **Resolución 2277 de 2025**, que adopta la Política General de Seguridad y Privacidad de la Información, orientando las actividades hacia la gestión integral de riesgos, la protección de los activos de información y la mejora continua del MSPI.

6.3 Metodología.

La implementación del Plan de Seguridad y Privacidad de la Información de la Superintendencia de Transporte se fundamenta en una gestión integral del Modelo de Seguridad y Privacidad de la Información (MSPI), conforme a los lineamientos establecidos en la Resolución 2277 de 2025 del Ministerio de Tecnologías de la

Información y las Comunicaciones (MinTIC). Este modelo se complementa con la metodología definida en el Modelo de Arquitectura Empresarial (MAE), asegurando la alineación entre los componentes estratégicos, tecnológicos, organizacionales y de seguridad digital de la entidad.

La metodología adoptada se basa en el ciclo de mejora continua (Planear – Hacer – Verificar – Actuar, PHVA), lo que permite planificar, implementar, monitorear y optimizar las acciones orientadas a la protección de la información institucional. Este enfoque garantiza la coherencia entre la planeación estratégica, la gestión del riesgo, la definición de controles de seguridad y la evaluación de resultados, promoviendo un proceso sistemático y sostenible de fortalecimiento institucional.

De igual forma, la metodología se articula con los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y con los componentes de control interno, gobierno digital y seguridad digital, garantizando que las acciones desarrolladas contribuyan al cumplimiento de los objetivos estratégicos de la entidad y a la protección efectiva de los activos de información en todo su ciclo de vida.

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 2026	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
	Cargar, clasificar y valorar los activos de acuerdo con su nivel de confidencialidad, integridad, disponibilidad y privacidad, conforme a la metodología MSPI, en el Sistema Daruma.	Activos cargados y clasificados según el MSPI en el Modulo de Daruma.
	Revisar de los activos de información reportados en el formato TIC-FR-010 o en el sistema DARUMA, módulos de Activos de Información.	Correo electrónico
	Retroalimentar y corregir de los activos reportados.	Correo electrónico / actas de mesa de trabajo
	Recibir de formato final y Memorando de entrega final por parte de los líderes de proceso.	Oficio de aceptación y entrega de activos
	Tener los activos cargados y actualizados en el Modulo de Activos de Información Daruma.	Información cargada / actualizada Modulo Activos Daruma.
	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 de activos 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 Daruma.

ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	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 controles asociados con 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
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, Boletines.
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 ciberseguridad.	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	Definir y actualizar de controles aplicados en la Entidad.	Matriz de Declaración de Aplicabilidad

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	controles de seguridad de la información		
	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, restauraciones y monitoreos.
	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 del cumplimento del PESI (Plan estratégico de Seguridad de la información)
	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	Revisiones periódicas	Revisar el cumplimiento de los procedimientos y políticas implementadas en materia de seguridad.	Evidencias, monitoreos
	Reporte de oportunidades de mejora	Generar oportunidades de mejora que se requieran, derivadas de las auditorias, y revisión de la documentación del MSPI	Oportunidades de mejora

FASE	ESTRATEGIA	ACTIVIDADES	EVIDENCIA
	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 Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) es responsable del monitoreo, seguimiento y control del Plan de Seguridad y Privacidad de la Información, conforme a la normativa vigente. Podrá solicitar apoyo a otras dependencias para consolidar avances, validar controles y asegurar la articulación del plan con los instrumentos institucionales, garantizando la mejora continua y la rendición de cuentas en materia de seguridad y privacidad de la información.

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
6	01-Dic-2025	Actualización de la presentación y enfoque del documento, de acuerdo con las nuevas directrices de la resolución 2277 de 2025. Se complementan los objetivos específicos alineados con las nuevas guías y documentos normativos. (Res 2277 de 2025). Se ajusta el Marco Legal, de acuerdo con los nuevos lineamientos normativos. Se reestructura el capitulo del Desarrollo del Plan alineándolo con otros estándares. Se completa el contexto estratégico, incorporando las políticas de gobierno y seguridad digital. Se modifica la metodología, conforme a los nuevos lineamientos normativos. Se incluye en la actividad de Actualización activos de información 2026, el Módulo de Activos del Daruma, y el cargue, la clasificación y valoración los activos de acuerdo con su nivel de confidencialidad, integridad, disponibilidad y privacidad, conforme a la metodología MSPI.Se incluyen las revisiones de los indicadores del del PESI (Plan estratégico de Seguridad de la información). En mejoramiento continuo, se incluyen Revisiones periódicas de los procedimientos y políticas implementadas en materia de seguridad. Se ajusta el Capitulo de Control y Seguimiento.

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