SuperTransporte

GUIA DE IMPLEMENTACION DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION MSPI

2025

PRESENTACION

La Superintendencia de Transporte reconoce la necesidad imperante de establecer, mantener y actualizar las medidas y controles de seguridad y privacidad de la información que garanticen la integridad, disponibilidad y confidencialidad de los datos en su ámbito de acción. Es en este contexto donde se da alcance a la implementación del Modelo de Seguridad y Privacidad de la Información (MSPI). La era digital, marcada por la cuarta revolución industrial ha traído consigo la aparición de nuevas tecnologías como el IoT (Internet de las Cosas), la IA (Inteligencia Artificial), la automatización, la nanotecnología, la gestión masiva de datos, la transformación digital, entre otras innovaciones, desempeñan un papel crucial en el manejo y tratamiento de la información.

El MSPI no solo establece directrices claras para la protección de la información, sino que también define un marco integral para la gestión de la seguridad digital, proporcionando las herramientas necesarias para establecer un sistema de gestión de seguridad de la información (SGSI) efectivo, adaptado a los requerimientos legales, técnicos, normativos y operativos pertinentes. Así es como desde la Oficina TIC de la Superintendencia de Transporte se lleva a cabo el desarrollo de la Guía de Implementación del MSPI, la cual proporciona un enfoque estructurado que permite a la entidad abordar de manera efectiva los desafíos en materia de seguridad y privacidad de la información. Para ello, se implementarán los controles establecidos en el Anexo A del estándar ISO/IEC 27001:2013, asegurando así un marco sólido y confiable para la protección de la información.

TABLA DE CONTENIDO

PRESENTACION 2
1. OBJETIVO GENERAL 4
2. ALCANCE 4
3. DEFINICIONES 4
4. ASPECTOS GENERALES 7
4.1 AUTODIAGNOSTICO MSPI 8
4.2 PLANIFICACION 9
4.3 OPERACIÓN 10
4.4 EVALUACION DE DESEMPEÑO 11
4.5 MEJORAMIENTO CONTINUO 11
4.6 DOMINIOS DE REFERENCIA 12
5. LINEAMIENTOS 15
6. CONTROL Y SEGUIMIENTO 16
7. CONTROL DE CAMBIOS DEL DOCUMENTO 16

1. OBJETIVO GENERAL

Ofrecer una herramienta que facilite la aplicación del Modelo de Seguridad y Privacidad de la Información (MSPI) en la Superintendencia de Transporte, en conformidad con los lineamientos normativos establecidos en la política de Gobierno Digital, cuyo propósito sea asegurar la continuidad de las operaciones y al mismo tiempo minimizar los riesgos asociados a los activos tecnológicos de la entidad.

2. ALCANCE

La presente guía aplica a todos los procesos de la Superintendencia de Transporte donde se debe garantizar la seguridad y privacidad de la información, inicia con la fase de autodiagnóstico y finaliza en la fase de mejoramiento continuo, sin embargo, es un proceso vivo, sujeto a constante monitoreo, control y actualización.

3. DEFINICIONES

- Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de ésta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización. (ISO/IEC 27000).
- Activos de Información y recursos: se refiere a elementos de hardware y de software de procesamiento, almacenamiento y comunicaciones, bases de datos y procesos, procedimientos y recursos humanos asociados con el manejo de los datos y la información misional, operativa y administrativa de cada entidad, órgano u organismo.
- Amenazas: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).
- Análisis de Riesgo: Proceso para comprender la naturaleza del riesgo y determinar el nivel de dicho riesgo. (ISO/IEC 27000).
- Archivo: Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o Entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la

gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3).

- Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).
- Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3).
- Ciberespacio: Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios.
- Ciberseguridad: Protección de activos de información, mediante el tratamiento de las amenazas que ponen en riesgo la información que se procesa, almacena y transporta mediante los sistemas de información que se encuentran interconectados.
- Control: Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.
- Acceso a la Información Pública: Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceso a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4).
- 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).

- Internet de las cosas (IoT): se refiere a la red de dispositivos físicos que están conectados a internet y pueden recopilar y compartir datos entre ellos sin intervención humana directa, permite que estos dispositivos sean controlados de forma remota, recopilen información del entorno en el que se encuentran y realicen acciones en función de esos datos.
- Inteligencia Artificial: se refiere a la capacidad de las máquinas para realizar tareas que normalmente requieren inteligencia humana. Esto incluye la capacidad de aprender de la experiencia, adaptarse a nuevas situaciones, comprender y procesar lenguaje natural, reconocer patrones y realizar decisiones con base en datos, puede ser implementada a través de algoritmos y modelos matemáticos complejos que permiten a las máquinas simular ciertos aspectos de la inteligencia humana. La inteligencia artificial está en constante evolución y tiene el potencial de transformar numerosos aspectos de la sociedad y la industria.
- MIPG: Modelo Integrado de Planeación y Gestión.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- PESI: Plan Estratégico de Seguridad de la Información.
- Propietario del riesgo: Persona o Entidad con la responsabilidad de rendir cuentas y la autoridad para gestionar un riesgo.
- 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.
- Riesgo: Efecto de la incertidumbre sobre los objetivos.
- 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.

4. ASPECTOS GENERALES

La implementación del MSPI (Modelo de Seguridad de la Información) en la Superintendencia de Transporte, está enmarcado en el alcance del Anexo A del estándar ISO/IEC 27001:2013, que implica una serie de fases y aplicación de diversos dominios de seguridad de la información, establecidos en la política de Gobierno digital y las buenas prácticas informáticas.

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

La implementación del Modelo de Seguridad y Privacidad de la Información en la Superintendencia de Transporte ha sido un proceso continuo y evolutivo a lo largo de diversas vigencias, donde se han llevado a cabo una serie de pasos y acciones con el objetivo de alcanzar el nivel de madurez actual en materia de seguridad y privacidad de la información. Todas las evidencias del trabajo realizado se encuentran publicadas en el SharePoint de la Oficina OTIC de la entidad.

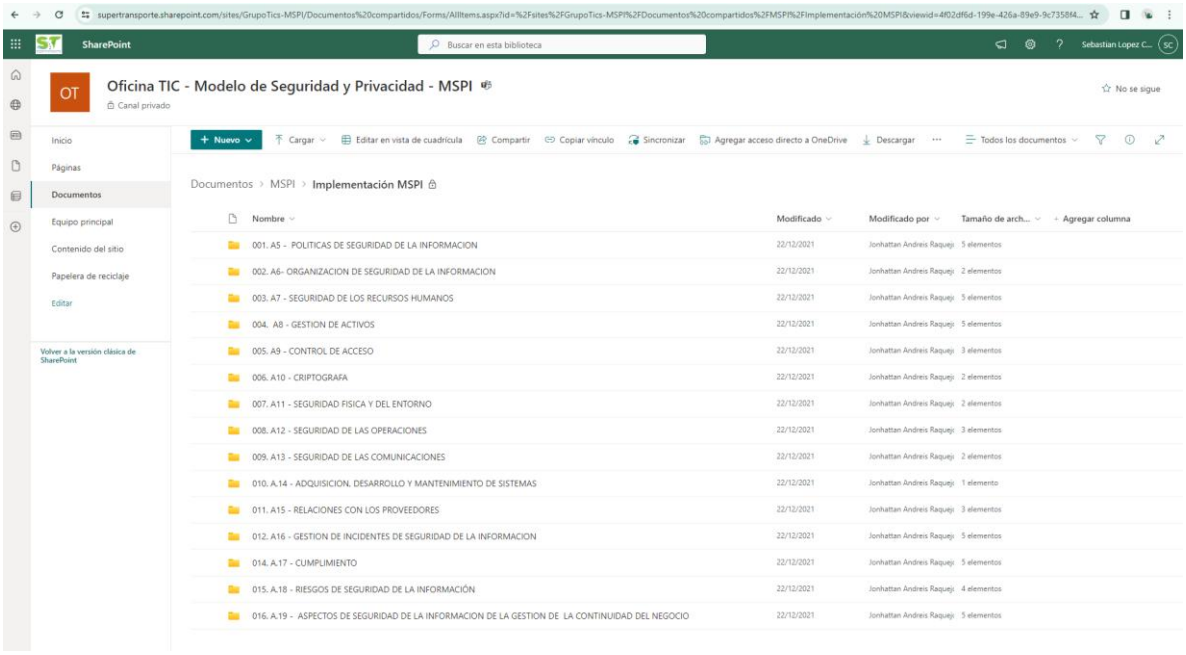

Ilustración 2. Evidencias de Implementación del MSPI modelo de seguridad y privacidad de la información, Fuente: SuperTransporte OTIC.

A continuación, se mencionan los procesos claves realizados en cada vigencia:

4.1 AUTODIAGNOSTICO MSPI

La fase de diagnóstico en cada período ha permitido a la Superintendencia de Transporte establecer el estado actual de la implementación de la seguridad y privacidad de la información. Para lograrlo, se ha empleado la herramienta de "Diagnóstico" utilizando el "instrumento de evaluación MSPI". Este instrumento identifica de manera específica los controles implementados y los faltantes, proporcionando insumos fundamentales para la fase de planificación.

Es crucial realizar este autodiagnóstico cada vigencia antes de iniciar la fase de planificación y actualizarlo al finalizar la fase de evaluación de desempeño. Esto con el propósito de identificar los avances en la implementación del Modelo en la entidad. El resultado obtenido después de la fase de evaluación de desempeño se incorporará como un insumo en la fase de mejoramiento continuo.

La información histórica de este proceso se encuentra publicada en el SharePoint de la OTIC

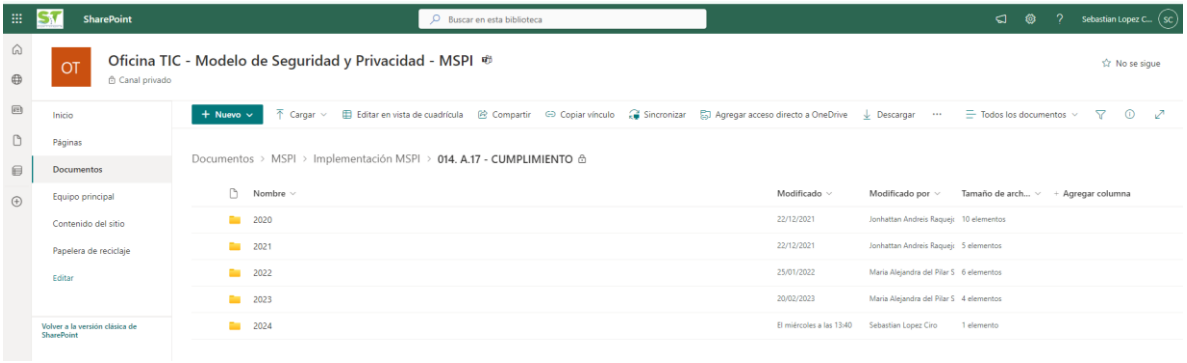

Ilustración 3. Evidencias de Implementación del MSPI modelo de seguridad y privacidad de la información, Dominio A.17 Cumplimiento Fuente: Superintendencia de Transporte OTIC.

4.2 PLANIFICACION

En esta etapa, se emplean los resultados anteriores para abordar las acciones del Plan de Seguridad y Privacidad de la Información, con el objetivo de que la entidad pueda realizar una planificación efectiva del tiempo, los recursos y el presupuesto para las actividades relacionadas con el MSPI. Los documentos generados en este proceso comprenden el Alcance MSPI, el Acto administrativo que establece las funciones de seguridad y privacidad de la información, la Política correspondiente, el Documento de roles y responsabilidades asociadas, los Procedimientos para el inventario y clasificación de la información e infraestructura crítica, la Metodología pertinente, el Procedimiento de gestión de riesgos, el Plan de tratamiento de riesgos, la Declaración de aplicabilidad, el Manual de políticas de Seguridad de la Información, y el Plan de capacitación, sensibilización y comunicación en materia de seguridad de la información.

La Superintendencia de transporte utiliza la herramienta del PESI, Plan Estratégico de Seguridad de la Información para establecer el cronograma y las acciones a ejecutar.

La información de este proceso se encuentra publicada en el SharePoint de la OTIC

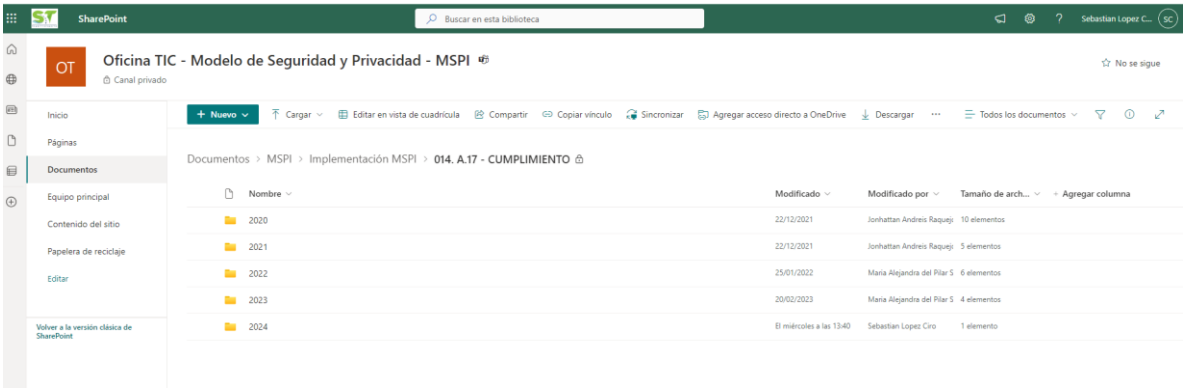

Ilustración 5. Evidencias de Implementación del MSPI modelo de seguridad y privacidad de la información, dominio A.17 Cumplimiento. Fuente: SuperTransporte OTIC.

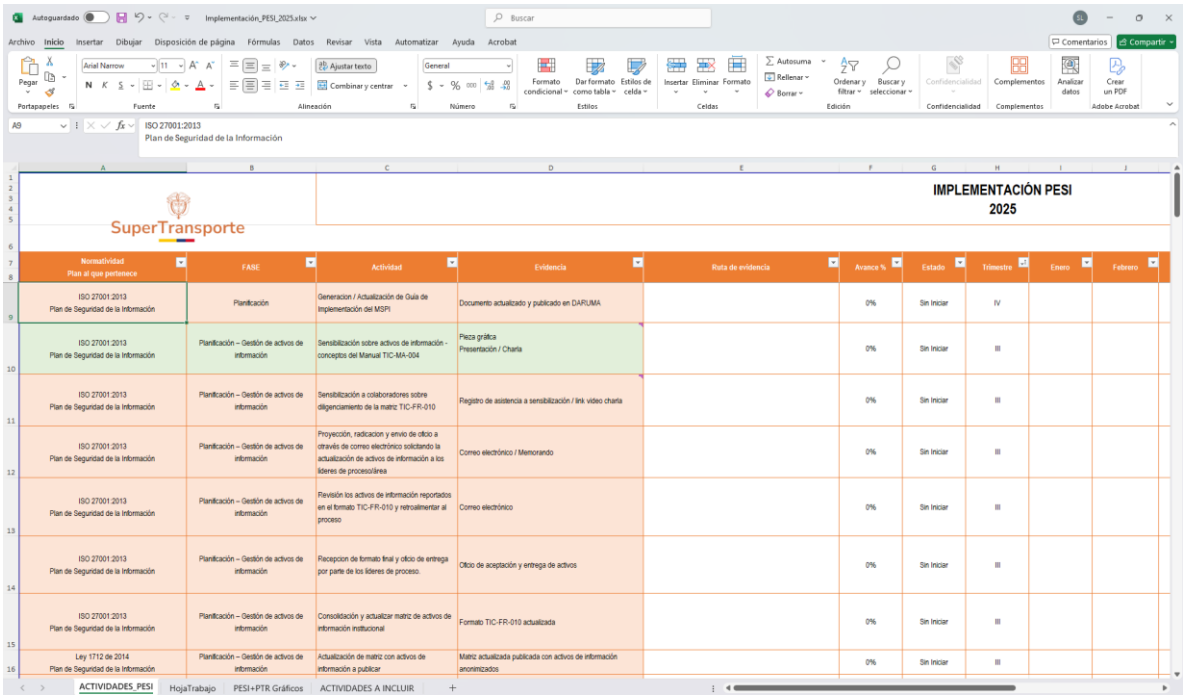

Ilustración 6. Evidencias de Implementación del MSPI modelo de seguridad y privacidad de la información, Herramienta del PESI, Plan Estratégico de Seguridad. Fuente: SuperTransporte OTIC.

4.3 OPERACIÓN

Una vez concluidas las actividades de la fase de Planificación del MSPI (Modelo de Seguridad y Privacidad de la Información), se procede a la ejecución de los controles para satisfacer los requisitos del MSPI. Esto implica la elaboración del

Plan de Tratamiento de Riesgos de Seguridad y Privacidad de la Información, así como la definición de indicadores de gestión, estos planes se actualizan y revisan cada vigencia.

La entidad lleva a cabo la planificación e implementación de las acciones establecidas en el Plan de Tratamiento de Riesgos, así mismo, esta información hace parte de las evidencias de los controles establecidos y los indicadores de cumplimiento del plan estratégico de seguridad de la información PESI.

Estos planes en cada vigencia deben recibir la aprobación del Comité Institucional de Gestión y Desempeño. El objetivo es poner en práctica los planes y controles necesarios para alcanzar los objetivos del MSPI, garantizando así la seguridad y privacidad de la información en la entidad.

4.4 EVALUACION DE DESEMPEÑO

Una vez finalizadas las actividades del MSPI, se evalúa la efectividad de las acciones tomadas mediante los indicadores definidos en la fase de implementación. Esto debe incluir la correcta integración entre el MSPI, MIPG y los requisitos normativos.

A través de este proceso de medición, la Superintendencia de Transporte puede determinar su nivel de madurez respecto a las acciones implementadas y ejecutadas. Asimismo, permite monitorear continuamente los avances en su gestión, los logros de los resultados y metas establecidas para la implementación de la Política de Gobierno Digital.

Para ello, es crucial establecer cronogramas y asignar recursos para el monitoreo, desempeño, resultados y aceptación en el comité de gestión institucional y desempeño, según lo establecido por el MIPG. El objetivo es evaluar el rendimiento de la seguridad de la información y la eficacia del MSPI.

4.5 MEJORAMIENTO CONTINUO

Una vez finalizadas las actividades del MSPI en la fase de evaluación y desempeño, es fundamental consolidar los resultados obtenidos y desarrollar un plan de mejoramiento continuo de seguridad y privacidad de la información. Esto

implica tomar medidas oportunas para abordar las debilidades identificadas. La Superintendencia de Transporte elabora este plan con el propósito de implementar acciones correctivas, optimizar procesos o controles, y elevar el nivel de madurez del MSPI. Es esencial actualizar el autodiagnóstico anualmente, así como implementar las acciones correctivas y los planes de mejora continua.

Dado que el proceso es cíclico, como se define en la ilustración 1 del Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTic), es crucial garantizar la toma y priorización adecuada de las acciones respectivas en cada ciclo para seguir mejorando el nivel de madurez del MSPI.

4.6 DOMINIOS DE REFERENCIA

La implementación del Anexo A del estándar ISO/IEC 27001:2013 en la Superintendencia de Transporte reviste una importancia técnica sustancial en el contexto del Modelo de Seguridad y Privacidad de la Información (MSPI), proporciona a la entidad una guía clara y estructurada para dirigir sus acciones hacia la adopción de buenas prácticas en seguridad de la información.

Este Anexo proporciona un conjunto exhaustivo de controles de seguridad de la información que son esenciales para salvaguardar los activos críticos de información de la entidad.

Los dominios a los que pertenecen estos controles, dentro del MSPI, abarcan áreas vitales como la gestión de riesgos, la seguridad de la información, la continuidad del negocio y el cumplimiento normativo, la aplicación de estos controles garantiza que la entidad pueda mitigar riesgos, proteger la integridad, confidencialidad y disponibilidad de su información, así como cumplir con las exigencias regulatorias de la estrategia de Gobierno Digital y el Modelo Integrado de Planeación y Gestión MIPG.

A continuación, se enumeran los dominios de referencia:

Anexo A del estándar ISO/IEC 27001:2013 y dominios a los que pertenece

Núm.	Nombre	Selección / Excepción	Descripción / Justificación

A.5	Políticas de seguridad de la información		
A.5.1	Directrices establecidas por la dirección para la seguridad de la información		Objetivo: Brindar orientación y apoyo por parte de la dirección, para laseguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
A.6	Organización de la seguridad de la información		
A.6.1	Organización interna		Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
A.6.2	Dispositivos móviles y teletrabajo		Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
A.7	Seguridad de los recursos humanos		
A.7.1	Antes de asumir el empleo		Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que seconsideran.
A.7.2	Durante la ejecución del empleo		Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información ylas cumplan.
A.7.3	Terminación o cambio de empleo		Objetivo: Proteger los intereses de la organización como parte delproceso de cambio o terminación del contrato.
A.8	Gestión de activos		
A.8.1	Responsabilidad por los activos		Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
A.9	Control de acceso		
A.9.1	Requisitos del negocio para control de acceso		Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
A.9.2	Gestión de acceso de usuarios		Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
A.9.3	Responsabilidades de los usuarios		Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
A.10	Criptografía		
A.10.1	Controles criptográficos		Objetivo: Asegurar el uso apropiado y eficaz de la criptografía paraproteger la confidencialidad, la autenticidad y/o la integridad de la información.
A.11	Seguridad física y del entorno		
A.11.1	Áreas seguras		Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
A.11.2	Equipos		Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
A.12	Seguridad de las operaciones		
A.12.1	Procedimientos operacionales y responsabilidades		Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
A.12.2	Protección contra códigos maliciosos		Objetivo: Asegurarse de que la información y las instalaciones deprocesamiento de información estén protegidas contra códigos maliciosos.
A.12.3	Copias de respaldo		Objetivo: Proteger contra la perdida de datos.
A.12.4	Registro y seguimiento		Objetivo: Registrar eventos y generar evidencia.
A.12.5	Control de software operacional		Objetivo: Asegurar la integridad de los sistemas operacionales.
A.12.6	Gestión de la vulnerabilidad técnica		Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.

A.12.7	Consideraciones sobre auditorias de sistemas de información		Objetivo: Minimizar el impacto de las actividades de auditoría sobrelos sistemas operacionales.
A.13	Seguridad de las comunicaciones		
A.13.1	Gestión de la seguridad de las redes		Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
A.14	Adquisición, desarrollo y mantenimientos de sistemas		
A.14.1.1	Requisitos de seguridad de los sistemas de información		Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
A.14.2	Seguridad en los procesos de desarrollo y soporte		Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
A.14.3	Datos de prueba		Objetivo: Asegurar la protección de los datos usados para pruebas.
A.15	Relación con los proveedores		
A.15.1	Seguridad de la información en las relaciones con los proveedores		Objetivo: Asegurar la protección de los activos de la organización quesean accesibles a los proveedores.
A.15.2	Gestión de la prestación de servicios con los proveedores		Objetivo: Mantener el nivel acordado de seguridad de la información yde prestación del servicio en línea con los acuerdos con los proveedores.
A.16	Gestión de incidentes de seguridad de la información		
A.16.1	Gestión de incidentes y mejoras en la seguridad de la información		Objetivo: Asegurar un enfoque coherente y eficaz para la gestión deincidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
A.17	Aspectos de seguridad de la información de la gestión de continuidad de negocio		
A.17.1	Continuidad de seguridad de la información		Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de laorganización.
A.18	Cumplimiento		
A.18.1	Cumplimiento de requisitos legales y contractuales		Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
A.18.2	Revisiones de seguridad de la información		Objetivo: Asegurar que la seguridad de la información se implementey opere de acuerdo con las políticas y procedimientos organizacionales.

5. LINEAMIENTOS

No.	Situación presentada	Descripción de la acción a desarrollar (orientación)
1	Se necesita presentar reporte de avance de la implementación del MSPI alineado con el PESI 	El funcionario o contratista que cuenta con el permiso de acceso al repositorio podrá presentar los avances de la implementación basado en las acciones y actividades llevadas a cabo y que están alineadas con el cronograma de implementación del Plan Estratégico de Seguridad de la Información PESI. Las evidencias se encuentran en sharepoint, en una carpeta principal denominada “Implementación del MSPI” y allí encontrara subcarpetas con cada uno de los dominios del Anexo A del estándar ISO/IEC 27001:2013. A su vez dentro de cada dominio están los históricos de las vigencias.
2	Se requiere desarrollar acciones y actividades en torno con los 18 dominios del Anexo A del estándar ISO/IEC 27001:2013. Dejando evidencia y trazabilidad de la implementación.	El funcionario o contratista encargado del proceso debe asegurar la ejecución de acciones específicas en cada uno de los dominios, documentando de manera clara y verificable cada actividad realizada. Esto permitirá dar cumplimiento a los requerimientos normativos y atender de manera oportuna cualquier solicitud de información que pueda surgir.
3	Se requiere socializar las acciones adelantadas y generar una cultura de apropiación en seguridad y privacidad de la información.	El funcionario o contratista responsable del proceso deberá diseñar e implementar un programa de capacitación continúa enfocado en buenas prácticas de seguridad y privacidad, sensibilizar al personal sobre su rol en la protección de la información institucional y promover una cultura organizacional orientada a la seguridad y privacidad de la información.

6. CONTROL Y SEGUIMIENTO

La Oficina de las tecnologías y las Comunicaciones OTIC, junto con su equipo de trabajo, será responsable de liderar la implementación de la guía, así como de proporcionar las acciones y evidencias necesarias. Sin embargo, es importante destacar que la implementación, seguimiento y control del MSPI corresponde al ámbito de competencia del Comité de Gestión y Desempeño de la Superintendencia de Transporte.

7. CONTROL DE CAMBIOS DEL DOCUMENTO

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
001	16-06-2025	Creación del documento Guía de la implementación del modelo de seguridad y privacidad de la información MSPI.

8. APROBACIÓN DEL DOCUMENTO

Aprobación del documento	
Etapa	**Nombres y cargo**
Elaboró:	Sebastián López Ciro – Contratista OTIC
Revisó:	
Aprobó:	Urias Romero Hernández – Jefe OTIC