TIC-PO-001

V2

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2022

Tabla de contenido

PRESENTACION

La implementación del sistema de gestión de seguridad de la información-SGSI, busca preservar la confidencialidad, integridad y disponibilidad de los activos de información de la Superintendencia de Transporte, garantizando su buen uso y la privacidad de los datos, a través del Modelo de Seguridad y Privacidad de la Información – MSPI.

Por tal motivo, la Superintendencia de Transporte consciente de cumplir la normatividad que le aplica a las entidades del Estado Colombiano, define los lineamientos de la política de Seguridad y privacidad de la Información, y a través de la Oficina de Tecnologías de la Información y las Comunicaciones se liderará su planeación, implementación, capacitación y ejecución, con el fin de mitigar las vulnerabilidades de la información durante el ciclo de vida del dato, a través de herramientas y mecanismos que permitan garantizar la confidencialidad, integridad, confiabilidad y disponibilidad de los datos e información.

Este documento se estructura teniendo en cuenta la guía técnica colombiana ISO 27001 y los lineamientos emitidos por el Ministerio de Tecnologías de la Información y las Comunicaciones – MINTIC desde el Modelo de Seguridad y Privacidad de la Información – MSPI.

1. OBJETIVO GENERAL

Establecer los lineamientos y principios para la gestión de la seguridad de los activos de información, con el fin de preservar la confidencialidad, integridad y disponibilidad durante todo el ciclo de vida de la información en la Superintendencia de Transporte.

2. OBJETIVOS ESPECÍFICOS

- Orientar la gestión de los riesgos de seguridad de la información de forma oportuna por medio de su identificación y formulación de controles, mitigando los impactos negativos ante una eventual materialización.
- Reducir el índice de incidentes de Seguridad de la Información que afecten el normal funcionamiento de la entidad.
- Fomentar una cultura y apropiación de seguridad y privacidad de la información en los servidores de la Entidad frente al Sistema de Gestión de Seguridad de la Información -SGSI.

3. ALCANCE

Esta política se encuentra alineada a los objetivos institucionales y es transversal a todos los procesos institucionales

4. DEFINICIONES

- **Activo de información:** en relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Análisis de riesgos:** proceso que permite comprender la naturaleza del riesgo y determinar su nivel de riesgo.
- **Colaborador:** empleado, contratista, practicante, proveedor y en general cualquier persona que tenga acceso a información de la entidad y tenga un vínculo contractual con el mismo.
- **Confidencialidad:** propiedad de la información de no ponerse a disposición o ser revelada a individuos, entidades o procesos no autorizados.
- **Control:** comprenden las políticas, procedimientos, prácticas y estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido. Control también es utilizado como sinónimo de salvaguarda o contramedida, es una medida que modifica el riesgo.
- **Disponibilidad:** propiedad de la información de estar accesible y utilizable cuando lo requiera una entidad autorizada.
- **Evento de seguridad de la información:** ocurrencia identificada de estado en un sistema de información, servicio o red que indica una posible brecha de seguridad, falla de un control o una condición no identificada que puede ser relevante para la seguridad de la información.

- **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.
- **Información**: se refiere a un conjunto organizado de datos contenido en cualquier medio la entidad genere, obtenga, adquiera, transforme o controle.
- **Integridad:** la propiedad de salvaguardar la exactitud y complejidad de la información.
- **Modelo Integrado de Planeación y Gestión- MIPG:** el Sistema de Gestión que deben aplicar las entidades públicas el cual integra y articula los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad con el Sistema de Control Interno.
- **Política de Seguridad de la Información**: es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene el conjunto de lineamientos y procedimientos que deben ser implementados para gestionar la seguridad de la información.
- **Seguridad informática:** conjunto de medidas técnicas que son implementadas para asegurar los recursos e información contenida en los componentes tecnológicos institucionales.
- **Seguridad de la información:** conjunto de medidas que buscan la protección de la información física, electrónica, digital del acceso, uso, divulgación o destrucción no autorizada.
- **Sistema de Gestión de Seguridad de la Información (SGSI):** conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer la política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basando en un enfoque de gestión y de mejora a un individuo o entidad.

5. MARCO NORMATIVO

La Superintendencia de Transporte por ser una entidad pública del orden Nacional de la rama ejecutiva, debe cumplir con la regulación y la normativa que establece el Estado Colombiano en materia de:

- Ley 1273 del 05 de enero 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 Estatutaria 1581 del 17 octubre de 2012, “Por la cual se dictan disposiciones generales para la protección de datos personales”
- Ley 1712 del 06 de marzo 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”.
- Ley 1915 del 12 de julio de 2018, “Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos”.

- Decreto 1074 del 26 de mayo 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 imparte instrucciones sobre el Registro Nacional de Bases de Datos. Artículos 25 y 26.
- Decreto 1078 del 26 de mayo de 2015. "Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones ".
- Decreto 1083 del 26 de mayo 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 4 de abril 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."
- Decreto 1008 del 14 de junio 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 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política de Seguridad Digital del Estado Colombiano.
- CONPES 3995 del 1 de julio de 2020. Política Nacional de Confianza y Seguridad Digital.
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- Resolución 500 de 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".

6. RESPONSABILIDADES

Para la debida implementación de la Política de Seguridad y Privacidad de la información se establecen las siguientes responsabilidades:

6.1. ALTA DIRECCIÓN

Asignar y aprobar los recursos humanos y económicos para la implementación del Sistema de Gestión de Seguridad de la Información (SGSI); así como apoyar el desarrollo de las actividades que sean requeridas para su mejora continua.

6.2. COMITÉ INSTITUCIONAL DE GESTIÓN Y DESEMPEÑO

Es la instancia encargada de realizar la revisión, seguimiento y aprobación de la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información (SGSI).

6.3. OFICIAL DE SEGURIDAD DE LA INFORMACIÓN

Responsable de presentar al Comité Institucional de Gestión y Desempeño la documentación, estrategias y propuestas para el mantenimiento y fortalecimiento del SGSI, así como liderar la implementación, mantenimiento y mejora de este con el fin de fomentar una cultura de la seguridad de la información en la Entidad. Adicionalmente tiene la misión de acompañar a las dependencias y/o procesos en la administración de los riesgos de seguridad de la información, realizando la revisión, análisis y consolidación de la información.

6.4. DEPENDENCIAS

De acuerdo con las establecidas en la estructura organizacional bajo el Decreto 2409 de 2018 a partir del Articulo 6 hasta el Artículo 22.

7. PRINCIPIOS DE LA POLÍTICA

La política de seguridad y privacidad de la información de la Supertransporte se rige por los siguientes principios:

- **Integridad:** propiedad de exactitud y completitud.
- **Confidencialidad:** propiedad de la información que la hace no disponible o divulgada a individuos, entidades o procesos no autorizados.
- **Disponibilidad:** propiedad de ser accesible y utilizables a demanda por los autorizados.
- **No repudio:** capacidad para corroborar que es cierta la reivindicación de que ocurrió un evento o una acción y las instancias que lo originaron.

8. DECLARACIÓN DE LA POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La Superintendencia de Transporte entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando establecer confianza en el ejercicio de sus deberes con el Estado y los ciudadanos, todo enmarcado en el cumplimiento de la normatividad vigente y en concordancia con la misión y visión institucional.

Por tal motivo adopta su Política de Seguridad y Privacidad de la Información orientada en el modelo de seguridad y privacidad de la información con el fin de asegurar la protección, confidencialidad, integridad, disponibilidad de los activos de información (procesos, hardware, software, infraestructura, información, funcionarios, contratistas, terceros) que soportan los procesos de la entidad, mediante la implementación de los lineamientos, procedimientos e instructivos y la asignación de responsabilidades generales y específicas, los cuales están orientados a preservar la continuidad del negocio, la prevención de incidentes de seguridad y la reducción de su impacto potencial dentro de un proceso de mejora continua.

Para la Entidad, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados, permitiendo propender por la integridad, confidencialidad y la disponibilidad de esta, acorde con las necesidades de los diferentes grupos de interés identificados y teniendo en cuenta lo siguiente:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Mantener la confianza ciudadanos y servidores.
- Proteger los activos de información.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información
- Fortalecer la cultura de seguridad de la información en los servidores (funcionarios, contratistas), proveedores, aprendices y demás actores que tengan vínculo con la Superintendencia de Transporte.
- Garantizar la continuidad de los servicios misionales frente a incidentes de seguridad de la información.
- La Superintendencia de Transporte, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades institucionales, y los requerimientos regulatorios.

9. COMPONENTES O LINEAMIENTOS DE POLÍTICA INSTITUCIONAL DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

9.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Superintendencia de Transporte con el liderazgo de la alta dirección y el trabajo articulado de la Oficina de Tecnologías de la Información y las Comunicaciones, a través del Oficial de Seguridad, y los procesos institucionales, brindará herramientas y metodologías para la identificación, clasificación y etiquetado de los activos de información de la entidad.

La Oficina de Tecnologías de la Información y las Comunicaciones definirá los lineamientos para la gestión de activos de información institucionales.

Los servidores (funcionarios y contratistas) no deberán divulgar, extraer, modificar y/o destruir información almacenada en los medios accesibles sin que medie autorización del dueño de la información

Todos los servidores (funcionarios y contratistas) que se desvincule temporal o definitivamente de la entidad deberá realizar la devolución de activos de información que tenga asignada y en custodia, físico o virtual, al supervisor o jefe inmediato.

Es de exclusiva responsabilidad de cada servidor tomar las medidas adecuadas para el almacenamiento y resguardo de los medios removibles, evitando accesos no autorizados, daños, pérdida de información o extravío del medio.

La información que reposa en los dispositivos móviles asignados por la Entidad (Directivos) es responsabilidad de quien tiene en uso el dispositivo móvil. Cuando se entreguen estos dispositivos, la dependencia encargada deberá eliminar los datos contenidos en este.

9.2. CONTROL DE ACCESO

La creación, reactivación o desactivación de usuarios de la red o sistemas de información; al igual que los roles y permisos otorgados, los realizará la Oficina de Tecnologías de la Información y Comunicaciones a través del procedimiento establecido para tal fin.

La Oficina de Tecnologías de la Información y las Comunicaciones gestionará mecanismos de control de acceso a través de usuario y contraseña, a la red de la Entidad, correo electrónico y a los sistemas de información que administre.

La Oficina de Tecnologías de la Información y Comunicaciones debe mantener actualizada la documentación relacionada con la administración de usuarios y monitoreará la asignación de permisos y roles otorgados a los usuarios.

Las contraseñas serán de uso personal e intransferible, por tal motivo se deben implementar mecanismos para ser cambiadas periódicamente. Se debe evitar que las contraseñas sean fáciles de recordar; no estén basadas en algo que otra persona pueda adivinar fácilmente u obtener usando información relacionada con la persona, (nombres, números de teléfono y fechas de nacimiento, etc.); que no sean vulnerables a ataques de diccionario (es decir, no contienen palabras incluidas en los diccionarios de credenciales); contener combinaciones de caracteres numéricos, alfabéticos y especiales con longitud mínima que se determine; si son temporales, cambiarlos la primera vez que se ingrese.

Es responsabilidad del funcionario o contratista el uso dado a su usuario y contraseña.

9.3. CRIPTOGRAFIA

La Oficina de Tecnologías de la Información y Comunicaciones deberá identificar, definir e implementar los controles criptográficos que se considere para proteger la confidencialidad, autenticidad e integridad de la información institucional.

9.4. SEGURIDAD FÍSICA Y DEL ENTORNO

La Superintendencia de Transporte velará por:

- Prevenir el acceso físico no autorizado, el daño y la interferencia de la información en la infraestructura de procesamiento de esta.
- Diseñar y aplicar la protección contra desastres naturales, ataques maliciosos y accidentes para evitar daños a causa de incendios, inundaciones, terremotos, explosiones, disturbios civiles y otras formas de desastres naturales o causados por el hombre.

9.5. SEGURIDAD DE LAS OPERACIONES

La Superintendencia de Transporte a través de la Oficina de Tecnologías de la Información y Comunicaciones velará por:

- Documentar, poner a disposición y aplicar los procedimientos de operación de los servicios tecnológicos.
- Hacer seguimiento y gestión a los cambios en las instalaciones y sistemas de procesamiento de información que afectan la seguridad de la información.
- Separar los ambientes de desarrollo, prueba y producción, para reducir los riesgos de acceso o cambios no autorizados al ambiente de producción.
- Hacer seguimiento al uso de los recursos, ajustes y proyecciones de los requisitos sobre la capacidad de gestión tecnológica futura.
- Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
- Implementar controles de detección, prevención y recuperación ante incidentes de seguridad, combinados con la toma de conciencia apropiada de los usuarios.
- Hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política o procedimiento de copias de respaldo aceptada.
- Elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
- Implementar procedimientos para controlar la instalación de software en sistemas operativos.
- Obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.

9.6. SEGURIDAD DE LAS COMUNICACIONES

Asegurar la protección de la información en las redes de comunicación y la infraestructura de procesamiento de información, a través de documentación y controles efectivos que permitan conexiones seguras para los fines institucionalmente establecidos; así como los lineamientos para la transferencia de información.

9.7. DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

De manera armónica durante la adquisición, desarrollo y mantenimiento de los sistemas de información, se deben considerar los siguientes aspectos:

- Conocer e implementar la guía de estilo e imagen institucional en aspectos en los que aplique para el desarrollo de los sistemas de información.
- Garantizar ambientes seguros de desarrollo, pruebas y producción.
- Todo sistema de información o desarrollo de software debe poseer un plan de pruebas de calidad que incluya pruebas de seguridad.

- Especificar las carpetas y archivos a los cuales se les debe generar copias de seguridad de acuerdo con los lineamientos que defina la Oficina de Tecnologías de la Información
- Mantener actualizada la documentación de los desarrollos realizados y estándares que se emplearan.
- Establecer un plan para el análisis y tratamiento de vulnerabilidades en los sistemas de información.
- Establecer como obligación específica contractual la entrega de la documentación necesaria para la administración y funcionamiento de los sistemas o aplicativos.
- Realizar transferencia de conocimiento, obligación específica que debe estar consignada en el contrato cuando así sea el caso.

9.8. RELACIÓN CON LOS PROVEEDORES

La Superintendencia de Transporte debe:

- Establecer y documentar los requisitos de seguridad de la información con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la entidad.
- Cuando sea el caso, requerir al proveedor planes de continuidad y recuperación de desastres que le permitan prestar en forma continua el servicio contratado; dichos planes deberán estar avalados por un tercero experto.
- Realizar seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

9.9. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN Y DIGITAL

La Superintendencia de Transporte debe:

- Establecer las responsabilidades y procedimientos de gestión para una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información. Todos los servidores deben reportar los incidentes de seguridad de la información a La Oficina de Tecnologías de la Información y Comunicaciones tan pronto como tengan conocimiento de este o sospechen de alguno mediante los mecanismos establecidos para tal fin.
- Definir y aplicar procedimientos para preservar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información con el fin de ser usado en la reducción de la posibilidad o el impacto de incidentes futuros.
- Definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información de los incidentes de seguridad de la información que pueda servir como evidencia.

9.10. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

La Superintendencia de Transporte debe:

- Determinar los aspectos de la continuidad de la gestión de la seguridad de la información en situaciones adversas, durante una crisis o desastre entre ellas el cumplimiento de los requisitos de disponibilidad, confidencialidad e integridad.
- Identificar, documentar, implementar y mejorar de manera continua los procesos y procedimientos para asegurar el nivel de continuidad requerido por la entidad.
- Verificar a intervalos planificados los controles de continuidad definidos e implementados, validando su adecuado funcionamiento.

9.11. CUMPLIMIENTO

La Superintendencia de Transporte debe:

- Propender por la identificación, documentación y cumplimiento de las obligaciones legales, estatutarias y demás normatividad vigente relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
- Implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
- Asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación en materia.
- Realizar revisión del SGSI, con el fin de identificar su adecuada implementación y operación conforme a las políticas definidas.

VIGENCIA

Esta Política Institucional de Seguridad y Privacidad de la Información ha sido aprobada por el Comité Institucional de Gestión y Desempeño o la instancia que haga sus veces en sesión del 03 de agosto de 2022, será adoptada mediante resolución del despacho del Superintendente y tendrá vigencia desde su adopción.

CONTROL DE CAMBIOS

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	13-Oct-2020	Versión Original en Formato del Sistema de Gestión creado para tal efecto.
2	03-ago-2022	Se suprimen los siguientes numerales: Lista de figuras, Numeral 1. 1.1, 1.2, 1.3, 1.3.1, 1.3.2, 1.3.3, 1.3.3, 7, 8.2, Actualización de los siguientes ítems: redacción presentación, objetivo general, marco normativo, concatenación de los objetivos específicos, alcance, responsabilidades, declaración de la política de seguridad y privacidad de la información