MINISTERIO DE TRANSPORTE
SUPERINTENDENCIA DE TRANSPORTE

RESOLUCIÓN NÚMERO 5095 **DE** 20/05/2024

"Por medio de la cual se actualiza la Política General de Seguridad y Privacidad de la Información de la Superintendencia de Transporte y se deroga la Resolución 7386 de 09 de septiembre de 2022"

LA SUPERINTENDENTE DE TRANSPORTE

En ejercicio de facultades constitucionales y legales, en especial las conferidas mediante el Decreto 2409 de 2018 y demás normas concordantes,

CONSIDERANDO

Que en el artículo 15 de la Constitución Política de Colombia se consagró el derecho de todas las personas a la intimidad personal, familiar y a su buen nombre, así como el derecho a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas, por lo que el Estado debe respetarlos y hacerlos respetar.

Que mediante la Ley 1581 de 2012, se expidió el Régimen General de Protección de Datos Personales, el cual amplia el derecho constitucional consagrado en el artículo 15 de la Constitución Política. Este derecho garantiza a todas las personas la posibilidad de conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

Que en sentencia de constitucionalidad 748 del 6 de octubre de 2011, la Corte Constitucional declaró exequible el marco normativo de la Ley 1581 de 2012 y estableció que el ámbito de aplicación de la ley, relaciona el tratamiento de base de datos tanto por entidades públicas como privadas.

Que en el artículo 227 de la Ley 1450 de 2011, estableció la obligatoriedad de suministro de información para las entidades públicas y los particulares que ejerzan funciones públicas, bajo la sujeción de los principios y normas de protección de datos personales y demás normas que regulan la materia.

Lo anterior, en línea con lo previsto en el artículo 15 de la Constitución Política, y estipulando que "(…) para los casos de inspección, vigilancia e intervención del Estado podrá exigirse la presentación de libros de contabilidad y demás documentos privados en los términos que señale la ley". Asimismo, en la Ley 1755 de 2015, artículo 27, se previó que "el carácter reservado de una información o de determinados documentos, no será oponible a (…) las autoridades administrativas que, siendo constitucional o legalmente competentes para ello, los soliciten para el debido ejercicio de sus funciones".

De igual manera, en el artículo 10 de la Ley 1581 de 2012, ley estatutaria para la protección de datos personales, y en concordancia con lo previsto en la Ley 594 de 2000, se estableció que no se requerirá autorización del titular de los

datos para entregarlos, cuando los requiera una entidad administrativa en ejercicio de sus funciones.

Que en el artículo 12 del Decreto 2609 de 2012, se requirió la protección de la información y los datos personales de conformidad con la Ley 1273 de 2009 y la Ley 1581 de 2012 en el Programa de Gestión Documental de las entidades públicas de conformidad con los lineamientos del Manual de Gobierno en Línea.

Que en el artículo 6 del Decreto 2693 de 2012, se definió el principio de interoperabilidad y el Modelo de Seguridad para el desarrollo del Programa de Gobierno en línea. Así pues, los sujetos obligados deben implementar mecanismos que garanticen el acceso e intercambio de información con observancia de lo establecido en la Ley 1581 de 2012, la Ley 1437 de 2011, la Ley 1450 de 2011 y el Decreto 19 de 2012.

Que en el Decreto 1377 de 2013, se estableció que los responsables deben desarrollar Políticas para el Tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas. En particular, el artículo 26 señaló respecto del principio de responsabilidad demostrada que los responsables del tratamiento de datos deben demostrar que han implementado las medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.

Que en el Decreto 886 de 2014, que reglamentó el artículo 25 de la Ley 1521 de 2012, se estableció la información mínima que debe contener el Registro Nacional de Bases de Datos y los términos y condiciones bajo las cuales se deben inscribir en éste los responsables del Tratamiento. En tal sentido, el artículo 2 extiende el ámbito de aplicación a personas naturales o jurídicas, de naturaleza pública o privada, en el territorio colombiano o fuera de él.

Que en la Ley 1712 de 2014, se definió el principio de transparencia y se reguló el derecho de acceso a la información pública, los procedimientos para el ejercicio, garantía del derecho y las excepciones a la publicidad de información.

Que en los capítulos 25 y 26 del Decreto 1074 de 2015, se consagró el Régimen General de Protección de Datos en el Sector Comercio, Industria y Turismo.

Que en el Decreto 1078 de 2015, por medio del cual se adoptan los lineamientos generales en el uso y operación de los servicios ciudadanos digitales en el marco del aparato normativo del Sector de Tecnologías de la Información y las Comunicaciones, se estableció que además de los lineamientos de la Ley 1437 de 2011, la Ley 1753 de 2015, la Ley 1955 de 2019 y el Decreto 2106 de 2019, el aparato administrativo del Estado debe implementar los principios de privacidad por diseño y por defecto, así como el de seguridad, privacidad y circulación restringida de la información.

Que en el Libro 2, Parte VIII, Título IV del Decreto 1080 de 2015, con relación a la inspección, vigilancia y control a los archivos de las entidades del estado y a los documentos de carácter privado declarados de interés cultural, se establecieron directrices para la calificación de información pública en la gestión documental.

Que en el artículo 159 de la Ley 1753 de 2015, se reiteró el acatamiento de la Ley 1581 de 2012 y la Ley 1712 de 2014, para el desarrollo de los planes, programas y proyectos en las entidades públicas y los particulares que ejerzan funciones públicas en cumplimiento y ejercicio de su objeto misional.

Que en el Titulo III, Capitulo 1 del Decreto 1743 de 2016, se delimitó el procesamiento, operación e información del Sistema Estadístico Nacional, refiriéndose a los objetivos, el Consejo Asesor y la anonimización de microdatos.

Que en el Documento CONPES 3854 de 2016, se delimitó la Política Nacional de Seguridad Digital en la República de Colombia, presentando el plan de acción para el fortalecimiento de la seguridad de los individuos y del Estado en el entorno digital, a nivel nacional y trasnacional, con un enfoque de gestión de riesgos.

Que en el Documento CONPES 3854 del 7 de marzo de 2017, se estableció la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y generando mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

Que en el Decreto 1499 de 2017, se definió el Modelo Integrado de Planeación y Gestión (MIPG), como el marco de referencia para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de las entidades y organismos públicos, con el fin de generar resultados que atiendan los planes de desarrollo y resuelvan las necesidades y problemas de los ciudadanos, con integridad y calidad en el servicio.

Que en el Decreto 1008 de 2018, se determinó que uno de los principios de la Política de Gobierno Digital es el de Seguridad de la Información, a través del cual se buscó crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado y de los servicios que prestan al ciudadano. De igual manera, se estableció que la Política de Gobierno Digital se desarrolla a través de componentes y habilitadores transversales y que la seguridad de la información, la arquitectura y los servicios ciudadanos digitales son los elementos fundamentales que permiten el desarrollo y el logro de los propósitos de la Política de Gobierno Digital.

Que en el Documento CONPES 3920 del 17 de abril de 2018, sobre la Política Nacional de Explotación de Datos (Big Data), se definió a los datos como representación primaria de variables cualitativas y cuantitativas que son almacenables, transferibles, pueden ser visualizadas, controladas y entendidas, los cuales se someten a un conjunto de reglas que gobiernan el ciclo de vida y flujo de los datos de acuerdo con su tipología. Igualmente, en el Documento se expuso la importancia de articular la normativa en la materia con la política pública, con el fin de aumentar los niveles de datos públicos digitales.

Que en la Circular Externa 01 del 16 de enero de 2019 de la Superintendencia de Industria y Comercio, se exhortó a los responsables y encargados del tratamiento de datos personales de las entidades de la rama ejecutiva del orden nacional a realizar el registro de bases de datos.

Que en la Resolución 462 del 26 de abril del 2019, expedida por la Procuraduría General de la Nación, se establecieron las funciones de la Procuraduría Delegada para la Defensa del Patrimonio Público, la Transparencia y la Integridad, entre las que se encuentran adelantar en primera instancia las actuaciones disciplinarias que correspondan a conductas relacionadas en el incumplimiento de las obligaciones contenidas en la Ley 1581 de 2012 y demás disposiciones que la desarrollen, modifiquen y reglamenten, a cargo de los sujetos vinculados con las autoridades públicas.

Que en el artículo 147 de la Ley 1955 de 2019, sobre la transformación digital pública, se incorporó el componente de transformación digital en las entidades estatales del orden nacional, siguiendo los estándares establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones. A su vez, indica la norma que los proyectos estratégicos de transformación digital se deben orientar al principio de inclusión y actualización permanente de políticas de seguridad y confianza digital.

Que en el Decreto 2106 de 2019, cuyo objetivo es simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la Administración Pública, se estableció que las autoridades deben disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

Que en la Circular Externa Conjunta No. 4 del 5 de septiembre de 2019, la Superintendencia de Industria y Comercio y la Agencia Nacional de Defensa Jurídica del Estado, manifestaron la importancia de los principios orientadores para que las entidades púbicas adopten las medidas necesarias para el aprovechamiento de las tecnologías de la información y las comunicaciones, de cara a la interoperabilidad en la transformación digital del Estado. El instructivo señalado por la Circular, refiere que los sistemas de información hacen uso de datos personales, y por ende, no se requiere expedir normas adicionales, sino adecuar el componente documental a la Ley 1581 de 2012.

Que en el Documento CONPES 3995 del 1 de julio de 2020, sobre la Política Nacional de Confianza y Seguridad Digital, se busca fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país.

Que en el Decreto 620 de 2020, se reglamentaron los lineamientos generales en el uso y operación de los servicios ciudadanos digitales, que deben cumplir con los estándares de privacidad en el diseño, arquitectura y configuración predeterminada del proceso de gestión de información y de la infraestructura que lo soporta. Así mismo, la adopción de seguridad, privacidad y circulación restringida de la información cuando se genere, almacene, transmita o trate en

el marco de los servicios ciudadanos digitales, por lo que requiere ser protegida y custodiada bajo los más estrictos esquemas de seguridad digital y privacidad con miras a garantizar la autenticidad, integridad, disponibilidad, confidencialidad, el acceso y circulación restringida de la información.

Que en la Resolución 500 del 10 de marzo del 2021, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, se establecieron los lineamientos y estándares para la estrategia de seguridad digital y se adoptó el modelo de seguridad y privacidad como habilitador de la Política de Gobierno Digital.

Que el Decreto 767 de 2022, mediante el cual se actualizó la política de Gobierno Digital del país, "establece los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio."

Que el Decreto 338 de 2022, mediante el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, dispone: "Título 21 lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital".

Que e Decreto 088 de 2022, mediante el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, dispone: "Título 20 conceptos, lineamientos, plazos y condiciones técnicas transversales para la digitalización y automatización de trámites y su realización en línea".

Que la Resolución 01117 de 5 de abril de 2022, expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, tiene por objeto establecer los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco de la Política de Gobierno Digital.

Que de acuerdo con el acta de sesión extraordinaria del Comité Institucional de Gestión y Desempeño efectuada el 29 de abril de 2024, se aprobó la actualización de la Política General de Seguridad y Privacidad de la Información de la Superintendencia de Transporte, la cual esta ajustada a los cambios estipulados en la Política de Gobierno Digital y Seguridad Digital.

Que dado lo anterior, se hace necesario adoptar mediante acto administrativo la nueva Política de Seguridad y Privacidad de la Información, que permitirá

salvaguardar la seguridad de los activos de información de la Superintendencia de Transporte.

Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1. Objeto. La presente resolución tiene como objeto actualizar y adoptar la nueva Política General de Seguridad y Privacidad de la Información de la Superintendencia de Transporte.

Artículo 2. Ámbito de aplicación. La política de seguridad y privacidad de la información aplica a todos los procesos de la Superintendencia de Transporte y la deben cumplir todos sus funcionarios, contratistas, vigilados y los terceros que presten algún servicio a la entidad, así como aquellas personas o terceros que debido al cumplimiento de sus funciones y las de la Superintendencia de Transporte compartan, utilicen, recolecten, procesen, intercambien o consulten su información.

Artículo 3. Política general 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. Lo anterior, enmarcado en los procesos de transformación digital que se vienen trabajando en 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.
- 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.

Artículo 4. Compromiso. La Superintendencia de Transporte se compromete a implementar el SGSI en cada uno de sus procesos a fin de identificar y gestionar la seguridad de los activos de información y adicionalmente a:

- Divulgar y verificar el cumplimiento de la Política de Seguridad y Privacidad de la Información a los funcionarios y contratistas de la entidad.
- Promover la cultura en Ciberseguridad y privacidad de la información al interior de la Superintendencia.
- Aprobar la asignación de funciones, roles y responsabilidades de cada dependencia en el sistema de gestión de seguridad de la información.
- Asignar los recursos para la implementación y mejora continua del sistema de gestión de seguridad de la información.
- Apoyar la innovación tecnológica acorde con los lineamientos del Ministerio de las Tecnologías y las Comunicaciones MINTIC, con el fin de contribuir en la implementación de la Política de Gobierno Digital.
- Minimizar y mitigar los riesgos de seguridad digital, acorde con lo establecido en la política de administración del riesgo de la entidad.
- Incluir las buenas prácticas y las políticas de seguridad en los proyectos y acciones de transformación digital que se lleven a cabo en la entidad.

Artículo 5. Objetivos. La Política General de Seguridad y Privacidad de la Información tendrá los siguientes objetivos:

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.

Objetivos Específicos

1. 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.
2. Reducir el índice de incidentes de Seguridad de la Información que afecten el normal funcionamiento de la entidad.
3. 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.
4. Incluir los lineamientos establecidos en las políticas de seguridad y privacidad de la información en todos los proyectos de innovación y transformación digital que se lleven a cabo en la entidad.

Artículo 6. Lineamiento de Seguridad. Proteger la información significa garantizar el cumplimiento de los tres principios fundamentales de la seguridad de la información, que son la confidencialidad, la integridad y la disponibilidad de la información, además de establecer los lineamientos que deben cumplir los funcionarios, contratistas y terceros. Para lograr este propósito se definen los lineamientos que permitirán salvaguardar la seguridad de los activos de información de la Superintendencia de Transporte así:

1. Organización de la seguridad de la información.
2. Seguridad de los recursos humanos.
3. Gestión de activos de información.
4. Control de acceso
5. Criptografía
6. Seguridad física y del entorno
7. Seguridad de las operaciones
8. Seguridad de las comunicaciones
9. Desarrollo y mantenimiento de sistemas de información
10. Relación con los proveedores
11. Gestión de incidentes de seguridad de la información y digital.
12. Seguridad de la información en la continuidad de negocio.
13. Cumplimiento.

Artículo 7. Responsables. En la política de seguridad y privacidad de la información se establecen los diferentes roles, asignación de responsabilidades y principales actividades a desarrollar a fin de ejecutar la implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, así como la Política de Seguridad y Privacidad de la Información.

Artículo 8. Actualización. La actualización de la política de seguridad y privacidad de la información estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones en cabeza del oficial de seguridad con la colaboración de las demás dependencias de la entidad.

Artículo 9. Aprobación. El Comité Institucional de Gestión y Desempeño tendrá la potestad de aprobar la actualización y/o modificación de la Política de Seguridad y Privacidad de la Información.

Artículo 10. implementación y Seguimiento: La implementación, ejecución y seguimiento de la Política, procedimientos, funciones de software y hardware e instructivos en materia de seguridad y privacidad de la información estará a cargo de la Oficina de Tecnologías de la Información y las Comunicaciones con la colaboración de las demás dependencias de la entidad acorde con los procesos y procedimientos en los cuales interactúen; así mismo será parte integral el cumplimiento de lo definido en el manual de políticas de seguridad de la información.

Artículo 11. Obligatoriedad. La Política de Seguridad y Privacidad de la Información y sus lineamientos deberán ser adoptadas como herramientas de obligatorio cumplimiento, estas determinan la información necesaria que permite a los funcionarios y contratistas hacer un acceso y uso apropiado de los recursos informáticos de la Superintendencia de Transporte.

Artículo 12. Incumplimiento. El incumplimiento de la Política de Seguridad y Privacidad de la Información y los lineamientos establecidos dará lugar a las acciones administrativas que se consideren necesarias de acuerdo con la normatividad vigente aplicable.

Artículo 13. Vigencia y derogatoria. La presente resolución rige a partir de la fecha de su publicación y deroga la Resolución 7386 de 09 de septiembre de 2022.

Artículo 14. Publíquese en la página web oficial de la Superintendencia de Transporte.

Dada en Bogotá, D.C., a los

PUBLÍQUESE Y CÚMPLASE

Firmado digitalmente por OSPINA ARIAS AYDA LUCY

AYDA LUCY OSPINA ARIAS
Superintendente de Transporte

Proyectó: Sebastián López Ciro – Contratista Oficina TIC
Revisó: Urías Romero – Jefe Oficina TIC
Luis Gabriel Serna Gámez – Jefe Oficina Asesora Jurídica

TIC-PO-001

V4

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

2024

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 (OTIC) 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 SGSI.
- Incluir los lineamientos establecidos en las políticas de seguridad y privacidad de la información en todos los proyectos de innovación y transformación digital que se lleven a cabo en la entidad.

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 documento de política 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.
- MSPI: Modelo de Seguridad y Privacidad de la Información.
- Política de Seguridad de la Información: es un documento de alto nivel que denota el compromiso de la administración 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.
- 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.
- Vulnerabilidad: Debilidad de un activo que puede ser explotada por una o más amenazas.

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”
- CONPES 3701 de 14 de julio de 2011: Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- 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”.
- 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)

- CONPES 3854 de 7 de marzo de 2017: Política de Seguridad Digital del Estado Colombiano.
- 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.”
- Guía para la administración de los riesgos de gestión, corrupción y seguridad digital del Departamento Administrativo para la Función Pública - DAFP
- 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”.
- CONPES 3995 del 1 de julio de 2020: Política Nacional de Confianza y Seguridad Digital.
- Resolución 500 de 10 de marzo 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”.
- Decreto 767 del 16 de mayo de 2022: 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.
- En el Decreto 767 de 2022: mediante el cual se actualizó la política de Gobierno Digital del país. “establece los lineamientos generales de la Política de Gobierno Digital, entendida como el uso y aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el objetivo de impactar positivamente la calidad de vida de los ciudadanos y, en general, los habitantes del territorio nacional y la competitividad del país, promoviendo la generación de valor público a través de la transformación digital del Estado, de manera proactiva, confiable, articulada y colaborativa entre los Grupos de Interés y permitir el ejercicio de los derechos de los usuarios del ciberespacio.”
- En el Decreto 338 de 2022: mediante el cual se adiciona el Título 21 a la Parte 2 del Libro 2 del Decreto Único, Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, el cual quedará así: "Título 21 lineamientos generales para fortalecer la gobernanza de la seguridad digital, la identificación de infraestructuras críticas cibernéticas y servicios esenciales, la gestión de riesgos y la respuesta a incidentes de seguridad digital”.
- En el Decreto 088 de 2022: mediante el cual se adiciona el Título 20 a la Parte 2 del Libro 2 del Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015 el cual quedará así: “Título 20 conceptos, lineamientos, plazos y condiciones técnicas transversales para la digitalización y automatización de trámites y su realización en línea”.
- La Resolución, 01117 de 5 de abril de 2022: expedida por el Ministerio de Tecnologías de la Información y las Comunicaciones, tiene por objeto establecer los lineamientos de transformación digital para las estrategias de ciudades y territorios inteligentes de las entidades territoriales, en el marco 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 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 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.

La integración de la seguridad de la información en la gestión de los proyectos independiente del tipo, es decir, tiene carácter transversal entre las diferentes dependencias de la entidad.

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 SGSI 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 SGSI, soportado en lineamientos claros alineados a las necesidades institucionales, y los requerimientos regulatorios.
- Incluir las buenas prácticas y las políticas de seguridad en los proyectos y acciones de transformación digital que se lleven a cabo en la entidad.
- Como parte integral para la implementación de la política, se establece el Manual de Políticas de Seguridad de la Información - código TIC-MA-009

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

La presente política se desarrolla en 11 lineamientos para el cumplimiento de los objetivos planteados, los cuales se describen a continuación:

9.1. GESTIÓN DE ACTIVOS DE INFORMACIÓN

La Superintendencia de Transporte con el liderazgo de la alta dirección y el trabajo articulado de la OTIC, 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 OTIC definirá los lineamientos para la gestión de activos de información institucionales. Es por esto que se ha definido un proceso de actualización de activos de información por vigencia, que busca garantizar que este proceso se realice de manera ágil mediante el módulo de activos de información del sistema DARUMA, dentro del marco de los procesos de transformación digital que se están llevando en la entidad.

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 OTIC a través del procedimiento establecido para tal fin.

La OTIC 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 OTIC 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 OTIC 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 OTIC 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.
- Asegurar 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 OTIC.
- 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 OTIC 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.
- Establecer los canales de comunicación y reportes directos con el Csirt y ColCert para realizar el reporte de los incidentes de seguridad de acuerdo a las estrategia de gobierno digital.

9.10. SEGURIDAD DE LA INFORMACIÓN EN LA CONTINUIDAD DE NEGOCIO

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.

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 31 de julio de 2023, 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
3	31-Jul-2023	Ajuste en la redacción del alcance Se complementa marco normativo Incorporación de responsabilidad en el numeral 6.4 Se complementa el numeral 8, incorporando el Manual de las políticas de seguridad. Actualización del numeral 9.5, seguridad de las operaciones por operaciones seguras, de acuerdo con la resolución 00500 de marzo 10 de 2021
4	29-Abr-2024	Ajuste incorporación de Objetivo específico. Incorporación de nuevos términos en el capítulo Definiciones. Se complementa marco normativo Se complementa el numeral 8, Declaración de la política institucional de seguridad y privacidad de la información, incluyendo los proyectos de transformación digital de la entidad Se incorpora en el ítem 9.1 el proceso de actualización de activos y la transformación del proceso. Se incorpora en el ítem 9.9 el proceso de reporte de gestión de incidentes a Csirt y ColCert.

* El elaborador que figurá en el documento es quien cargó la Política en el Sistema de Gestión de Calidad, sin embargo, quien la realizó fue **Sebastian López Ciro**. Dicha persona no pudo cargarla en el DARUMA teniendo en cuenta las limitantes de usuario.

Etapa	Nombre y cargo
Elaboró	Andrea del Pilar Bermudez Sierra Contratista(OAP)
Revisó	Luz Angela Maria Mora Cubillos ProfesionalEspecializado(OAP) Urias Romero Hernandez Contratista(TIC)
Aprobó	Martha Patricia Aguilar Copete Jefe(OAP)

Sebastian Lopez Ciro @ 2024-11-13, 8:50:50

TIC-MA-009

VERSIÓN 3

MANUAL DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

2024

PRESENTACIÓN

La Superintendencia de Transporte, considera la información como un activo de alta importancia que permite el desarrollo continuo de la misión y el cumplimiento de los objetivos institucionales, razón por la cual se adoptan e implementan controles y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El documento que se desarrolla a continuación es complemento integral de la Política de Seguridad y Privacidad de la Información TIC-PO-001, en donde se adoptan las responsabilidades y políticas que deben ser aplicadas por los funcionarios, contratistas, visitantes y proveedores que presten sus servicios o tengan algún tipo de relación con la entidad; estas se encuentran enfocadas al cumplimiento de la normatividad Colombiana vigente y las buenas prácticas de seguridad de la información, basadas en la norma ISO serie 27000 y al modelo de seguridad y privacidad de la información de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia.

TABLA DE CONTENIDO

1. INFORMACIÓN DE LA ENTIDAD

La Supertransporte, es la entidad que vigila, inspecciona y controla el servicio público de transporte, la actividad portuaria y la infraestructura, por una Colombia conectada, incluyente y competitiva; así mismo, tiene como visión lograr ser reconocida 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.

Para el cumplimiento de su misión y visión ha definido cinco objetivos estratégicos:

- Brindar protección a los usuarios
- Fortalecer la presencia en las regiones
- Fortalecer la vigilancia
- Fortalecer las tecnologías de la información y las telecomunicaciones
- Fortalecimiento institucional

Para aportar al fortalecimiento institucional, la entidad tiene definida en su cadena de valor 16 procesos, el proceso de Gestión de TIC busca “proveer, gestionar y mantener los sistemas de información, infraestructura y los servicios”.

2. OBJETIVO GENERAL

Establecer las condiciones para la implementación de las políticas de seguridad de la información, ciberseguridad y protección de la privacidad en la entidad.

3. MARCO LEGAL

- 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”
- 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 imparten 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)
- 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.
- 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”
- Decreto 767 del 16 de mayo de 2022. 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.

4. DEFINICIONES

Las definiciones detalladas a continuación, se encuentran conforme a los términos y definiciones de la ISO 27002:2022

- **Activo:** cualquier cosa que tenga valor para la organización.
- **Ataque:** intento no autorizado exitoso o fallido de destruir, alterar, deshabilitar, obtener acceso a un activo o cualquier intento de exponer, robar o hacer uso no autorizado de un activo.

- **Autenticación:** provisión de seguridad de que una característica declarada de una entidad es correcta.
- **Autenticidad:** propiedad de que una persona natural o jurídica es lo que dice ser
- **Cadena de custodia:** posesión demostrable, movimiento, manejo y ubicación del material desde un punto en el tiempo hasta otro.
- **Evaluación de impacto de la privacidad:** proceso general de identificación, análisis, evaluación, consulta, comunicación y planificación del tratamiento de posibles impactos en la privacidad con respecto al procesamiento de información de identificación personal, enmarcado dentro de la gestión de riesgos.
- **Gestión de incidentes de seguridad de la información:** ejercicio de un enfoque coherente y eficaz para el manejo de incidentes de seguridad de la información.
- **Incidente de seguridad de la información:** uno o varios eventos de seguridad de la información relacionados e identificados (3.1.14) que pueden dañar los activos de una organización (3.1.2) o comprometer sus operaciones
- **No repudio:** capacidad para probar la ocurrencia de un evento o acción alegado y sus entidades de origen
- **Objetivo de punto de recuperación-RPO:** tiempo en el que se recuperarán los datos después de que se haya producido una interrupción.
- **Objetivo de tiempo de recuperación-RTO:** período de tiempo dentro del cual se recuperarán los niveles mínimos de servicios y/o productos y los sistemas, aplicaciones o funciones de soporte después de que haya ocurrido una interrupción
- **Parte interesada:** persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad
- **Procedimiento:** forma especificada de llevar a cabo una actividad o un proceso
- **Proceso:** conjunto de actividades interrelacionadas o que interactúan que usa o transforma entradas para entregar un resultado
- **Sistema de información:** conjunto de aplicaciones, servicios, activos de tecnología de la información u otros componentes.
- **SGSI:** Sistema de Gestión de Seguridad de la Información
- **Vulnerabilidad:** debilidad de un activo o control que puede ser explotado por una o más amenazas

5. DESARROLLO DEL MANUAL

A continuación, se relacionan las políticas que se deben implementar como parte integral de la implementación del Sistema de Gestión de Seguridad de la Información (SGSI) y cumplimiento de la Política General de Seguridad y Privacidad de la Información.

Políticas organizacionales

Política de estructura organizacional de seguridad de la información

- La Superintendencia de Transporte, en cumplimiento al compromiso de implementar el SGSI, establece un esquema de seguridad de la información definiendo roles y responsabilidades que involucren las actividades de operación, gestión y administración de la seguridad de la información a través de su “Política de Seguridad y Privacidad de la información código TIC-PO-001.
- A través de un acto administrativo de carácter general se adoptará la estrategia de seguridad digital, identificando el alcance y responsable de su implementación.
- Las políticas que componen el SGSI deben ser aprobadas por la Alta Dirección, en Comité Institucional de Gestión y Desempeño.
- El CIO (jefe de la Oficina de Tecnologías de la Información y las Comunicaciones - OTIC) y el oficial de seguridad tendrán la responsabilidad de proyectar, actualizar y/o modificar la Política de Seguridad y Privacidad de la Información, si a ello hubiere lugar y ser presentada al Comité Institucional de Gestión y Desempeño; para su aprobación.

- Todos los procedimientos y lineamientos que formen parte del SGSI deben ser aprobados y publicados en la cadena de valor.

Política de gestión de activos de Información

- La entidad debe documentar y divulgar un procedimiento formal para la gestión de activos de información, lo cual debe hacer parte de la cadena de valor.
- Los procesos institucionales deben identificar y mantener actualizados los activos de información que tengan a cargo.
- Los activos de información serán responsabilidad de los líderes de cada dependencia o proceso.
- Es responsabilidad de cada dependencia o proceso informar las novedades que puedan afectar la integridad, disponibilidad o confidencialidad de los activos de información.
- Los activos de información son propiedad de la Superintendencia de Transporte, por tal motivo, los servidores al finalizar su contrato o acuerdo deberán devolverlos.
- Se debe identificar y documentar la devolución de los activos, como, por ejemplo: información física, hardware de autenticación -token-, tarjetas de acceso a las instalaciones de la entidad, equipos y dispositivos tecnológicos.

Política de uso de los activos

- La entidad implementará las directrices para mantener la protección adecuada y uso de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo con sus roles y funciones.
- La asignación de los activos de información es para uso exclusivo del desarrollo de las actividades misionales y contractuales que le sean asignadas en la entidad, por tal motivo la entidad no se hace responsable de la información personal que sea almacenada en los activos institucionales.
- El usuario de los recursos tecnológicos asignados por la entidad se debe comprometer a dar buen uso, de acuerdo con las políticas y lineamientos definidos por el SGSI.
- Todos los servidores que hagan uso de los activos de información institucionales tienen la responsabilidad de seguir las políticas establecidas para el uso adecuado de los activos de información, entendiendo que el uso no adecuado de los recursos puede poner en riesgo la disponibilidad de los servicios tecnológicos institucionales y la confidencialidad de la información y además generar acciones disciplinarias de ser el caso.
- Se debe capacitar a los servidores cuando ingresen por primera vez a la entidad, en el manejo de los sistemas de información institucionales y las herramientas tecnológicas.
- No se debe consumir alimentos y bebidas mientras se esté haciendo uso o manipulación de los activos de información.

Política de uso de los recursos tecnológicos.

- Todos los servidores deben hacer buen uso de los activos de información a los cuales tienen acceso y que son propiedad de la entidad, de igual forma, son responsables de cualquier uso que se les dé.
- Los equipos de cómputo solo deben ser destapados y actualizados por el personal autorizado en la OTIC.
- Los usuarios no deben almacenar en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, fotos o cualquier tipo de archivo que no sean de carácter institucional.
- No está permitido realizar conexiones o derivaciones eléctricas que pongan en riesgo la disponibilidad de la información por fallas en el suministro eléctrico a los equipos de cómputo.
- La pérdida o daño de elementos o recursos tecnológicos, o de alguno de sus componentes, debe ser informada de inmediato a la Dirección administrativa, de acuerdo con el procedimiento establecido para tal fin.
- El traslado de los recursos tecnológicos físicos estará a cargo de la Dirección Administrativa y su configuración se realizará a través de la OTIC.
- Todo incidente de seguridad que comprometa la disponibilidad, integridad o confidencialidad de la información debe ser reportado a la OTIC en la mayor brevedad posible, a través de la herramienta establecida para tal fin.
- La OTIC es la única dependencia autorizada para la instalación del software, el cual no debe ser copiado, suministrado a terceros o utilizado para fines personales.
- Las estaciones de trabajo de usuario final deben quedar apagados cada vez que el colaborador no se encuentre en la entidad y no requiera realizar actividades vía remota.
- Definir y documentar la gestión de cambios en la infraestructura tecnológica y los sistemas de información, en el Catálogo de Elementos de Infraestructura Tecnológica.
- La OTIC debe establecer los procedimientos de reutilización, eliminación y borrado de información de equipos de cómputo no funcionales.
- La OTIC debe validar mensualmente las actualizaciones de los parches de seguridad de toda la plataforma tecnológica como bases de datos, aplicaciones o software instalados. Deberá realizar de forma oportuna las actualizaciones una vez se publiquen o estén disponibles, especialmente las de los sistemas operativos, navegadores y programas antivirus, no obstante, previamente se deberá identificar el efecto de estas actualizaciones.
- La entidad a través de la OTIC debe identificar y clasificar todo el software en el Catálogo de Sistemas de Información identificando y clasificando (obsolescencia, soporte) los más críticos, para que se les dé un tratamiento prioritario para actualizar, migrar o desconectar de la red, mitigando así los riesgos.

Política de uso del correo electrónico

- El correo electrónico institucional es una herramienta de apoyo a las funciones y responsabilidades de los servidores de la entidad.
- El servicio de correo electrónico institucional debe ser empleado únicamente para enviar y recibir mensajes de carácter institucional. En consecuencia, no puede ser utilizado con fines personales, económicos, comerciales y/o cualquier otro ajeno a los propósitos de la Superintendencia de Transporte.
- En cumplimiento de la iniciativa del uso aceptable del papel y la eficiencia administrativa, se debe optar por el uso del correo electrónico al envío de documentos físicos, siempre que las disposiciones legales lo permitan. Esto teniendo en cuenta que, los mensajes de correo están respaldados por la Ley 527 de 1999 (por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.), en tal caso se funda la legalidad de los mensajes de datos y las implicaciones legales que conlleva el mal uso de estos.

- No se permite el uso de correos masivos tanto internos como externos, salvo a través de las cuentas autorizadas para tal fin.
- Todo mensaje sospechoso, SPAM o Cadena debe ser inmediatamente reportado a la OTIC como incidente/evento de seguridad de la información. No está permitido el envío y/o reenvío de mensajes en cadena, debido a que puede ser contentivo de virus, en especial si contiene archivos adjuntos con extensiones .exe, .bat, .prg, .bak, .pif,
- La cuenta de correo institucional no debe ser registrada en páginas o sitios publicitarios, de comercio electrónico, deportivos, casinos, o a cualquier otra ajena a los fines institucionales.
- No se permite el uso del correo para la transferencia de contenidos insultantes, ofensivos, injuriosos, obscenos, violatorios de los derechos de autor y/o que atenten contra la integridad moral de las personas o instituciones.
- No se dará uso del correo electrónico institucional para distribuir información de carácter reservado o clasificado, sin el previo análisis y autorización del líder de la dependencia y/ o proceso.
- El envío de mensajes desde el correo electrónico debe contener una leyenda de confidencialidad y aplicarse en la firma institucional de todos los usuarios institucionales.
- El único servicio de correo electrónico autorizado para el manejo de la información institucional en la Entidad es el asignado por la OTIC, y que cuente con el dominio @supertransporte.gov.co, el cual cumple con todos los requerimientos técnicos y de seguridad.

Política de uso de internet

- La entidad permite el acceso al servicio de internet, estableciendo las medidas técnicas que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones web.
- La OTIC implementará los controles necesarios para evitar el acceso a redes sociales, sistemas de mensajería instantánea, páginas con contenido ofensivo, insultante, injurioso y violatorio de los derechos de autor; así como el acceso a sistemas de almacenamiento en la nube y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud con la respectiva justificación a la OTIC, para que sea evaluado, autorizado y realice los cambios según corresponda.
- La OTIC implementará los controles técnicos para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales así mismo controla el acceso a la información contenida en portales de almacenamiento publicados en internet para prevenir la fuga de información.
- La Superintendencia de Transporte se reserva el derecho de monitorear los accesos, y por tanto el uso del servicio de internet de todos los servidores, además de limitar el acceso a determinadas páginas de internet, los servicios ofrecidos por la red, la descarga de archivos y cualquier otro ajeno a los fines de la entidad.

Política para uso de dispositivos móviles

- Todo dispositivo móvil -equipo portátil y tabletas- que ingrese o se retire de la entidad deberá ser registrado por el personal encargado de la seguridad física, en donde se pueda identificar lo siguiente:
    - Fecha y hora de ingreso.
    - Fecha y hora de salida.
    - Identificación y nombre de la persona que ingresa o retira el elemento
    - Dependencia a la que se dirige
    - Descripción del dispositivo (serial y marca)
- Los dispositivos móviles que sean asignados por la entidad deberán mantener la configuración respectiva para restringir la instalación de software, así como un mecanismo que impida el robo o perdida dentro de las instalaciones institucionales.
- Los dispositivos móviles deben estar configurados para acceder a través de credenciales de acuerdo con la asignación.
- Los dispositivos móviles de la entidad que sean retirados de las instalaciones deben contener mecanismo de cifrado de tal forma que evite divulgación de información en caso de pérdida o robo.
- Todos los dispositivos móviles asignados deben tener instalado el antivirus institucional.
- El uso de conexión a la red para los dispositivos móviles ajenos a la entidad deberá estar segmentada para proveer únicamente el servicio de internet, restringiendo el acceso a la data y navegación interna.

Política de uso de mensajería instantánea y redes sociales

La Superintendencia de Transporte define los lineamientos generales para asegurar la protección de la información, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

- La información que se publique o divulgue por cualquier medio de Internet, de cualquier colaborador de la entidad, que sea creado a nombre personal en redes sociales como -pero sin limitarse a los siguientes: Twitter®, Facebook®, YouTube®, blogs, Instagram, se considera fuera del alcance del SGSI y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que lo genere.
- Toda información distribuida en las redes sociales que sea originada por la entidad debe ser autorizada por los líderes de la dependencia y/o proceso para ser socializadas y divulgada por el grupo de comunicaciones de la entidad.
- No se debe utilizar el nombre de la Superintendencia de Transporte en redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la entidad.
- Las personas designadas para el manejo y gestión de contenido en las redes sociales de la entidad deben acatar las directrices dadas en el presente documento.

- Los responsables de cada red social deberán aplicar complejidad en las contraseñas de las cuentas institucionales, acatando los protocolos de seguridad de estas y realizando el cambio periódicamente.
- El Oficial de Seguridad de la Información realizará la verificación de las medidas y controles implementados de seguridad, encaminadas a evitar el acceso abusivo a la plataforma, que puedan afectar la imagen y la credibilidad de la entidad.
- No se deben vincular cuentas de correo electrónico personales en las redes sociales que se apertura bajo el dominio de la Superintendencia de Transporte.
- No se debe administrar y configurar las redes sociales la entidad en dispositivos móviles personales.
- Con el fin de evitar la fuga de información y descarga de contenido que pueda generar un riesgo de seguridad para la entidad, se restringirá el acceso de mensajería instantánea como -pero sin limitarse a los siguientes: WhatsApp, Telegram y/o Signal- que no se encuentre licenciada por la Superintendencia de Transporte. En caso de ser requerida alguna, se debe hacer la solicitud a la OTIC a través de la herramienta de mesa de ayuda para la respectiva viabilidad de uso.

Política de clasificación de la información

La Superintendencia de Transporte consiente de aplicar el nivel de protección apropiada de acuerdo con el tipo de calificación establecido por las disposiciones legales, define lo siguiente:

- Las categorías de calificación de la información que se adoptaran son: INFORMACIÓN PÚBLICA, INFORMACIÓN PÚBLICA RESERVADA e INFORMACIÓN PÚBLICA CLASIFICADA.
- Todos los activos de información indiferente de su medio de almacenamiento deben ser clasificados de acuerdo con los lineamientos institucionales creados para tal fin. Esta actividad debe ser realizada por los responsables sobre la gestión de los activos de información, es decir los líderes de cada dependencia o proceso.
- Toda la documentación o información generada en la entidad debe ser clasificada en alguna de las categorías adoptadas.
- Desarrollar e implementar los lineamientos para el etiquetado de la información de acuerdo con las categorías definidas y adoptadas, las cuales permitirán reconocer fácilmente la clasificación del activo de información.
- La información que se intercambie en cumplimiento de acuerdos institucionales con otras entidades debe incluir la clasificación e informar al destinatario la interpretación de la clasificación con el fin de que este le asigne las protecciones requeridas.
- En el caso de los sistemas de información que contienen información sensible o crítica se deben implementar mecanismos que indiquen la clasificación e identificación del contenido.

Política para la transferencia de información

- Proteger la información transferida al interior y exterior de la entidad.
- La OTIC, realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

- Los canales de red usados para la transferencia de información deberán contar con un mecanismo que no permita la fuga o interceptación de información, en su defecto la información que viaja por estos deberá estar cifrada.
- Las transferencias de información deben estar amparadas por acuerdos interinstitucionales o de confidencialidad que permitan mantener los estándares de seguridad sobre esta.

Política de control y gestión de acceso a los activos de información

- La OTIC establecerá los lineamientos para la gestión de usuarios dónde se detalle el uso de credenciales únicas, así mismo, para el uso de identificaciones compartidas o grupales por razones justificadas, establecer los tiempos de bloqueo o modificación de cuentas por inactividad, intentos fallidos, cambio de roles o retiro.
- Se debe mantener un registro centralizado de los accesos suministrados.
- Los accesos remotos se deben realizar por las herramientas autorizadas, no se permiten el uso de software de acceso remoto no licenciado por la entidad.
- Todo software debe ser comprado o aprobado por la OTIC.
- El control de acceso a la Información se realiza aplicando el principio de mínimo privilegio necesario para la realización de las actividades asignadas.
- El acceso a la información se realiza de acuerdo con los niveles de calificación de la información y perfil asignado al usuario.
- Los accesos con privilegios especiales deben contar con la aprobación de la OTIC y estar debidamente justificados por el solicitante.
- Los responsables del manejo de usuarios privilegiados deben aceptar su responsabilidad frente al uso del usuario asignado.
- Los administradores funcionales de los sistemas de información deben realizar revisiones periódicas por lo menos una semestral de los usuarios activos en los diferentes sistemas de información, dominio y red.
- Es responsabilidad de los servidores institucionales notificar a los administradores de TI la desvinculación de un funcionario, cesiones y terminaciones anticipadas del contratista para que sean retirados los accesos de todos los sistemas incluidos los accesos físicos a las diferentes instalaciones de la entidad, teniendo en cuenta el procedimiento establecido para tal fin.
- En el caso de los contratistas se debe realizar la configuración automática en la consola de administración del directorio activo, para que el día de la terminación del contrato sean inhabilitadas las credenciales asignadas.
- Para el acceso a los espacios de archivo tanto en las dependencias como el Archivo Central, se debe dar aplicación a los controles y lineamientos establecidos por la dependencia y/o proceso encargado.
- Los servidores que, tengan bajo su responsabilidad la custodia de información física almacenada en archivadores que se encuentren en las oficinas, deben mantener el control de acceso a esta información; por lo tanto, debe estar bajo llave, la cual se debe guardar en un sitio seguro, dando cumplimiento a lo establecido en el presente manual.

- Se debe controlar que la información física clasificada como reservada o confidencialidad no se encuentre expuesta en sitios tales como cajones sin llave o sobre el escritorio, esto con el fin de mantener la confidencialidad.
- La OTIC y el grupo de Gestión Documental deberá definir los lineamientos para la creación de repositorios de información dentro las herramientas que dispone la entidad, con el fin de establecer la estructura de la información generada y procesada de cada dependencia que se debe almacenar.

Política de establecimiento, uso y protección de claves de acceso

- Ningún usuario deberá acceder a la red o a los servicios de la entidad utilizando una cuenta de usuario o credenciales de otro usuario.
- Toda acción realizada usando la clave de acceso es responsabilidad directa del usuario al que se le asignaron las credenciales.
- La OTIC suministrará a los usuarios las claves iniciales respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados. Las claves son de uso personal e intransferible.
- La OTIC Implementará mecanismos para que los usuarios cambien su contraseña de acceso al usarla por primera vez en los sistemas de información o servicios a los que se les permita el acceso; así como implementar una política de red que solicite cambio de credenciales en periodos definidos.
- El desbloqueo y asignación de nueva contraseña solo debe ser solicitado por el titular de la cuenta, comunicándose a la OTIC, en donde se llevará a cabo la validación de los datos personales, y se asignará una contraseña temporal.
- Los servidores no deben dejar visibles las credenciales asignadas.
- Las claves o contraseñas de acceso deben contener los siguientes requisitos de seguridad:
  - Tener mínimo ocho (8) caracteres alfanuméricos y especiales.
  - Cada vez que se cambien estas deben ser distintas por lo menos de las últimas cinco anteriores.
  - La contraseña debe ser cambiada máximo cada noventa (90) días.
  - No debe contener el nombre de usuario y caracteres consecutivos como -abcd,123456

Manejo de contraseñas para administradores de TI

- Se debe preferir en las plataformas de tecnología que, el ingreso a la administración se realice con la vinculación directa de las credenciales del directorio activo.
- Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. De no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.
- Los administradores de TI pertenecientes a la OTIC no deben dar a conocer sus credenciales institucionales de acceso a los sistemas de información a terceros, sin previa autorización escrita del OTIC.

- Los Administradores de TI pertenecientes a la OTIC deben emplear obligatoriamente contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación que posee la entidad de acuerdo con el rol asignado.

Política en la relación con proveedores

- Mantener la seguridad de la información y de los servicios de procesamiento, a los cuales tienen acceso las terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.
- Se deben establecer obligaciones dentro de los contratos con terceros que contemplen aplicación de estándares y mejores prácticas de gestión de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la entidad, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.
- En los contratos o acuerdos con los proveedores y/o contratistas se debe considerar una causal de incumplimiento del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.
- Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la entidad.
- Los servidores de la entidad que tengan responsabilidad como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas, propendiendo por el cumplimiento de las políticas de seguridad de la información.
- Todo proveedor y/o contratista debe informase de las políticas y lineamientos que componen el SGSI y establecerse como una obligación contractual.
- Todo proveedor y/o contratista debe realizar la devolución de los activos de información asignados por la entidad para el cumplimiento de las obligaciones contractuales.
- Se deben establecer mecanismos o condiciones con los contratistas y proveedores en donde estos informen y puedan realizar la gestión de cambios en los servicios suministrados.

Política para el uso de servicios en la nube

- En el uso de servicios en la nube contratados por la entidad se deben gestionar los riesgos de seguridad.
- Se debe identificar y definir la responsabilidad compartida de la seguridad de la información y los esfuerzos de colaboración entre el proveedor del servicio y la Superintendencia de Transporte. En caso de que los acuerdos de servicios estén predefinidos y no están abiertos a negociación la entidad debe revisar los definidos y validar que se contemplen los requisitos de confidencialidad, integridad, disponibilidad y manejo de la información institucional.

- La entidad, actuando como cliente del servicio en la nube definirá si debe exigir al proveedor de servicio que se notifique antes de realizar cambios sustanciales que afecten la continuidad del servicio contratado, como los relacionados a continuación, pero sin limitarse:
    - Cambios de hardware o software, reconfiguraciones y demás que afecten o cambien la oferta de servicios en la nube.
    - Realizar tratamiento de información en una nueva jurisdicción geográfica o legal.
    - Uso de proveedores de servicios similares o subcontratados.

Política de gestión de los incidentes de la seguridad de la información

- Garantizar que los eventos e incidentes de seguridad que se presenten con los activos de información sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de tomar oportunamente las acciones correctivas.
- Establecer los respondientes para la atención de incidentes de seguridad dentro de la Superintendencia de Transporte.
- Identificar y documentar contacto con autoridades, grupos de interés que manejen temas relacionados con seguridad de la información e incidentes.
- Asegurar una gestión consistente y eficaz de la evidencia relacionada con incidentes de seguridad de la información para efectos de acciones disciplinarias y legales.
- Fortalecer y mejorar los controles de seguridad de la información a través de la documentación y conocimiento de los incidentes de seguridad que se presenten en la entidad.

Política de seguridad de la información durante la interrupción de los servicios institucionales

- La entidad debe definir el conjunto de procedimientos y estrategias para contrarrestar las interrupciones en las actividades misionales de la entidad, proteger sus procesos críticos contra fallas mayores en los sistemas de información o contra desastres y asegurar que las operaciones se recuperen oportuna y ordenadamente, generando un impacto mínimo o nulo ante una contingencia.
- Prevenir interrupciones en las actividades de la plataforma informática de la entidad que, van en detrimento de los procesos críticos de TI afectados por situaciones no previstas o desastres.
- Los proveedores de servicios TI críticos deberán contar con planes de continuidad, los cuales deben ser de conocimiento de la OTIC.
- Se debe desarrollar e implementar un Plan de Continuidad para asegurar que los procesos misionales de la entidad los cuales serán restaurados dentro de escalas de tiempo razonables. El plan de acción que permitirá mantener la continuidad se desarrollará teniendo en cuenta los siguientes aspectos como mínimo:
    - Identificación y asignación de prioridades a los procesos críticos de la entidad de acuerdo con su impacto en el cumplimiento de la misión de la entidad.
    - Documentación de la estrategia de continuidad.
    - Documentación del plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente.
    - Plan de pruebas de la estrategia de continuidad.
- Los requisitos de seguridad de la información deben incluirse en los procesos de gestión de la continuidad del negocio.

Política de cumplimiento de requisitos legales, estatutarios, reglamentarios y contractuales

- La entidad debe gestionar riesgos para prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.
- Todos los sistemas de información que capturen datos personales deben cumplir con la política de protección de datos personales definida por la entidad.
- La entidad debe identificar, documentar y actualizar los requisitos legales y reglamentados relacionados con seguridad de la información.
- La OTIC deberá garantizar que todo el software que se ejecute esté protegido por derechos de autor o en su defecto contenga licencia de uso o software de libre distribución y uso.
- La entidad debe mantener prueba y evidencia de propiedad del licenciamiento adquirido.
- Los servidores institucionales deben cumplir con las Leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software y documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la Ley.

Política de tratamiento de datos personales

En cualquiera sea el caso el tratamiento de datos personales se realizará conforme la Ley 1581 de 2012, sus Decretos reglamentarios y la Política de Tratamiento de Datos Personales definida por la Superintendencia de Transporte.

Política de revisión independiente de la seguridad de la información.

- Garantizar el funcionamiento del SGSI de acuerdo con las políticas y procedimientos implementados en la Entidad.
- A través de la Oficina de Control Interno se realizarán las verificaciones del cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
- Todos los líderes de proceso y dependencias deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información con el personal a cargo.
- La OTIC a través del SGSI realizará revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones de la entidad.

Política de cumplimiento

- Los diferentes aspectos contemplados en esta política son de obligatorio cumplimiento para todos los servidores de la Superintendencia de Transporte. En caso de que se infrinjan las políticas de seguridad de forma intencional o por desconocimiento, la entidad tomará las acciones disciplinarias y legales correspondientes.
- Con la aplicabilidad de las políticas establecidas se debe prevenir el incumplimiento de las leyes, estatutos, regulaciones y obligaciones contractuales que se relacionen con los controles de seguridad.

Política de seguridad del recurso humano

- Se debe asegurar que los servidores, adopten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir los riesgos.
- Los acuerdos laborales y contractuales deben establecer la responsabilidad del colaborador en cuanto a seguridad de la información -derechos de autor, confidencialidad y no divulgación de la información durante y después del empleo; así como el conocimiento y cumplimiento de las políticas del SGSI.
- Establecer estrategias para que los servidores tomen conciencia con lo relacionado a los temas de seguridad de la información.
- Articular los procedimientos disciplinarios en situaciones de incumplimiento y/o violaciones de las políticas de seguridad de la información, conforme a las normas que lo reglamenten en el sector público.
- Implementar procedimientos que permitan identificar las novedades, desvinculaciones, terminaciones o cesiones de contrato y demás, con el fin de retirar o modificar los accesos físicos y lógicos en la entidad.

Política de trabajo a distancia

- La OTIC velará por la identificación de necesidad y licenciamiento de la VPN - Virtual Private Network
- Las actividades de acceso remoto (uso de VPN - Virtual Private Network) a los activos de información electrónicos/digitales de la entidad, se autorizan de acuerdo con las necesidades específicas de la dependencia solicitante.
- Se recomienda que mientras se haga uso de VPN desde un equipo personal, éste tenga instalado y actualizado el antivirus y que el sistema operativo cuente con las actualizaciones de seguridad y esté licenciado.
- La OTIC realizará las configuraciones de seguridad, aprovisionamientos y revocación de acceso a la VPN según corresponda.

Política de reporte de eventos e incidentes de seguridad de la información

- Los servidores y terceros deben reportar cualquier evento sospechoso observado en los activos de información.
- La OTIC definirá y socializará los canales para el reporte de eventos de seguridad detectados.

Política de seguridad física

Política de perímetros y entrada física

- La entidad debe implementar un sistema de seguridad física para las instalaciones de la entidad.
- Se deben implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la entidad u otros mecanismos que permitan mantener alertas.
- Definir y usar perímetros de seguridad para proteger las dependencias de procesamiento de información sensible o critica, teniendo en cuenta:
    - Todas las puertas externas deberían tener mecanismos de control que eviten el acceso no autorizado.
    - Las puertas y ventanas se deben mantener cerradas con llave cuando no hay supervisión.
    - Prohibir el uso de equipo fotográfico, de video, audio u otro equipo de grabación cuando no se cuente con autorización para ello.
- Los visitantes deben registrarse en la entrada, ser autorizados por un colaborador para ingresar y durante su estancia y hasta su retiro deben estar acompañados por el funcionario o contratista con el cual están desarrollando su actividad.
- Los controles de acceso físico a las instalaciones deben permitir el acceso únicamente al personal autorizado.
- Documentar el registro de ingresos y salidas del centro de datos y cableado.
- Todos los servidores deben portar el carné en lugar visible, en caso de ser visitante se debe portar una escarapela que lo identifique, se debe notificar al personal de vigilancia cualquier caso de visitantes solos y sin identificación visible.
- Para el caso de las dependencias del despacho y carga se debe:
    - Inspeccionar el material que ingresar para detectar presencia de materiales peligrosos.
    - Restringir para el personal identificado y autorizado

Política de escritorio despejado y pantalla limpia

- Los servidores y terceros que tienen algún vínculo con la entidad deben conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- Todos los equipos y sistemas de información deben configurarse con una función de tiempo de espera o cierre de sesión automático.
- Los usuarios de los sistemas de información institucionales deben bloquear la pantalla de su computador, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información deben cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Al imprimir documentos con información pública reservada y/o pública clasificada, deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Política de protección contra amenazas físicas y ambientales

La entidad debe:

- Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.
- Contar con herramientas que permitan registrar y restringir el acceso de los servidores a estas dependencias.
- En las instalaciones del centro de datos o de los centros de cableado, No está permitido:
  - Fumar dentro de las instalaciones.
  - Introducir alimentos o bebidas.
  - El porte de armas de fuego, corto punzantes o similares.
  - Mover, desconectar y/o conectar equipos de cómputo sin autorización.
  - Modificar la configuración del equipo o intentarlo sin autorización.
  - Alterar software instalado en los equipos sin autorización.
  - Alterar o dañar las etiquetas de identificación de los elementos tecnológicos o sus conexiones físicas.
  - Extraer información de los equipos en dispositivos externos sin previa autorización.
  - Abuso y/o mal uso de los recursos tecnológicos físicos.
  - Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.
- Revisar y actualizar periódicamente los derechos de acceso.
- Cada gabinete o armario contiene llave de ingreso y/o tarjeta de acceso, las cuales deben permanecer custodiadas por el colaborador designado para tal fin.
- Considerar la implementación de controles contra incendios, inundaciones, sobretensiones eléctricas y en general de las posibles amenazas físicas y ambientales.
- Los medios y equipos donde se almacena procesan o comunica la información (física o electrónica), deben mantenerse con las medidas de protección físicas y lógicas.

Política de medios de almacenamiento

- Los medios de almacenamiento extraíble pueden generar riesgos para la entidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- Está restringida la copia de archivos en medios removibles de almacenamiento, por lo cual se deshabilita la opción de escritura en dispositivos USB, unidades ópticas de grabación en todos los equipos de cómputo institucionales; la autorización de uso de los medios removibles debe ser tramitada a través de la OTIC y será objeto de auditorías de seguridad mediante las herramientas consideradas para tal fin.
- Solo se habilitarán los puertos de conexión de medios de almacenamiento extraíbles si existe una razón institucional para su uso y es autorizado por el jefe inmediato.
- Se debe realizar monitoreo a la transferencia de información cuando sea necesario utilizar medios de almacenamiento extraíble.

Política de seguridad del cableado

- Se debe implementar controles que permitan proteger las líneas eléctricas y de telecomunicaciones de cortes accidentales.
- Los cables de alimentación y comunicación deben estar separados para evitar interferencias.
- Implementar conductos blindados, cajas cerradas y alarmas en los puntos de terminación.
- Establecer mecanismos de acceso controlado a los paneles de conexión y centros de cableado.
- Se debe propender por el uso de cables de fibra óptica.

Política de mantenimiento de equipos

- Se debe establecer un cronograma para el mantenimiento de los equipos tecnológicos (UPS, routers, computadores, aires, switch, servidores)
- Solo las personas autorizadas realizaran las reparaciones y mantenimientos respectivos.
- Cada mantenimiento debe contar con una ficha técnica que permita establecer el mantenimiento realizado, fecha, reparaciones, persona que realiza la actividad y quien recibe a satisfacción.
- En caso de ser requerido un mantenimiento remoto, se solicitará la autorización de La OTIC a través de un mecanismo seguro y licenciado por la Entidad.

Política de eliminación segura o reutilización de equipos

- En los casos en los que se almacene información en equipos que se encuentran en las salas de reuniones de la entidad, salas de juntas y salones de capacitación; las personas que han realizado la reunión, en el momento que no se requiera su uso en estos dispositivos, deben eliminarla de forma permanente; con el fin de evitar que personas no autorizadas puedan conocerla.
- Cuando no se requiera la información contenida en un medio de almacenamiento reusable, se debe borrar para que no sea recuperable y registrar los resultados como prueba de la eliminación. En caso de los equipos en condición de alquiler, se debe realizar el borrado antes de la devolución.
- La información almacenada con nivel alto de confidencialidad o integridad en medios removibles debe contar con técnicas de cifrado para evitar accesos no autorizados.
- Para los medios que contienen información confidencial, se deben almacenar y disponer de forma segura, mediante incineración, destrucción a través de máquinas destinadas para tal fin o proceso de borrado seguro, de acuerdo con las directrices de la OTIC .
- En cualquiera sea el caso de realizar destrucción de algún componente tecnológico, se ejecutará bajo los lineamientos del Sistema de Gestión Ambiental.

Política de las operaciones TIC

Política de dispositivos tecnológicos y redundancias

- Definir y documentar las actividades operacionales especificando los lineamientos para:
  - Copias de respaldo
  - Reinicio y recuperación del sistema en caso de falla
  - Manejo de errores y otras condiciones.
  - Contactos de soporte en caso de dificultades técnicas inesperadas.
- Realizar seguimiento al uso de recursos y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema, considerando documentar planes de gestión de capacidad para los sistemas críticos de la misionalidad.
- Los servicios y dispositivos tecnológicos deben estar monitoreados en cuanto a: seguimiento de intentos de accesos fallidos y compartimientos anómalos.
- Los servidores no deben instalar ningún tipo de canal de transmisión, módems, ni cambiar la configuración de sus equipos sin la previa aprobación de la OTIC.
- Los servidores no tienen permitido descargar, utilizar e instalar software externo en los recursos tecnológicos institucionales a menos que sea aprobado e instalado por la OTIC.
- Implementar controles de detección, prevención y recuperación para proteger los activos de información contra ataques de código malicioso.
- La asignación de dispositivos tecnológicos deberá realizarse a través de registro y entregar con las configuraciones de: dominio, cifrado de disco, restricción de instalación de software, protección contra malware, bloqueo remoto -en caso de no requerirse accesibilidad a través de VPN, partición del disco duro y demás consideradas en las políticas anteriores.
- La OTIC velará por:
  - Adquirir y mantener actualizadas las licencias de software de protección contra código malicioso en todos sus servidores, equipos de cómputo y los archivos intercambiados por correo electrónico tanto entrantes como salientes.
  - Establecer mecanismos para mantener actualizados todos los sistemas de procesamiento de información (parches de software y actualizaciones).
  - Presentar las necesidades tecnológicas en materia de seguridad digital ante las instancias correspondientes.
- Identificar los servicios tecnológicos más críticos y considerar la implementación de redundancias necesarias para garantizar la continuidad del servicio.

Política de accesos con privilegios elevados.

- La asignación de los accesos con privilegios debe controlarse a través de un procedimiento.
- Las solicitudes deben ser realizadas y aprobadas por el responsable del activo de información.
- Los accesos con privilegios deben estar limitadas por un rango de tiempo específico.

- Revisar regularmente los accesos con privilegios otorgados.
- Se debe tener en cuenta que los accesos con privilegios elevados son exclusivamente para realizar tareas de gestión y administración de los componentes tecnológicos y en ningún momento para realizar actividades de uso personal del usuario.
- Los accesos con privilegios deben estar asociados a un usuario específico, si la cuenta contiene una identificación genérica no se debe hacer uso por varios administradores.

Política de acceso a sistemas y aplicaciones

- El acceso a la información y a las funcionalidades de las aplicaciones se debe restringir, de acuerdo, con los niveles de autorización para cada usuario o grupo de usuarios.
- El acceso a los sistemas de información se debe iniciar con el principio de accesos mínimos.
- Los sistemas y aplicaciones deben mantenerse monitoreados y auditados.
- Las credenciales para acceder a los ambientes de pruebas y producción se deben diferenciar de forma que permitan identificar cada usuario para cada ambiente.
- Se debe controlar el acceso a códigos fuente de programas y elementos asociados (diseños, especificaciones, planes de prueba, resultados), para evitar la introducción de funcionalidades no autorizadas o cambios involuntarios, así mismo, para mantener la confidencialidad de la propiedad intelectual, por tal motivo:
    - Las librerías de programas fuente deben reposar en el repositorio de control de versiones dispuesta por la entidad para tal fin, no deberían estar contenidas en los ambientes de producción.
    - Establecer un repositorio formal para el almacenamiento de código fuente y control de versiones.
    - Controlar los cambios para el mantenimiento y copia de las librerías de fuentes de programas.
    - Mantener un registro de auditoría de todos los accesos con su respectiva acción.
- Se debe mantener los siguientes lineamientos, pero sin limitarse;
    - Validar las credenciales de acceso al completar todos los datos de entrada, en caso de error el sistema no deberá informar cual es el dato correcto o incorrecto.
    - Proteger contra intentos de ingreso mediante ataques de fuerza bruta.
    - Mantener registro de intentos exitosos y fallidos de acceso.
    - No mantener visible la contraseña que se está ingresando.
    - Todos los sistemas de información expuestos públicamente o en el portal web de la entidad deben contar con certificado de sitio seguro.
    - No transmitir contraseñas en texto claro en las redes o medios de comunicación.
    - No dar la opción al usuario de recordar las credenciales
    - Datos de acceso (fecha y hora de inicio de sesión exitoso)
    - Finalizar las sesiones inactivas después de un periodo de inactividad de tiempo, con especial rigurosidad para lugares públicos, externos o dispositivos móviles.
    - Bloqueo de credenciales tras 3 intentos máximos erróneos.
    - Bloqueo de los equipos de cómputo tras 5 minutos de inactividad.

Política de gestión de vulnerabilidades

- Identificar y definir las estrategias de monitoreo de vulnerabilidades técnicas.
- Se debe exigir a los proveedores de servicios tecnológicos la notificación y plan de remediación de vulnerabilidades
- Realizar pruebas planificadas y documentadas para evaluar vulnerabilidades mínimo una vez al año.
- Validar riesgos del despliegue de actualizaciones de firmware o sistemas operativos antes de su instalación

Política de controles criptográficos

- Implementar controles para proteger activos de información reservados, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.
- La entidad no establece un lineamiento de ciclo de vida de llaves criptográficas, toda vez que, la asignación de la clave para el cifrado de la información en la herramienta, la establece el usuario que genera o administra la información a cifrar, teniendo siempre presente que, en caso de olvidar la clave, la información cifrada no es recuperable.
- Se debe contar con herramientas que permitan el cifrado de información en medios de almacenamiento.
- Se debe instalar y configurar herramientas de cifrado de información en los portátiles institucionales.

Política de respaldo y restauración de información

- Proporcionar medios de respaldo adecuados para asegurar que toda la información misional y el software, se pueda recuperar después de una falla, garantizando que la información y la infraestructura de software crítica de la entidad, sean respaldadas y puedan ser restauradas en caso de una falla y/o desastre.
- Los administradores de la plataforma que realizan las copias de seguridad verificarán la correcta ejecución de estos procesos.
- Los administradores de la plataforma de copias de respaldo de la entidad, mensualmente deben generar tareas de restauración aleatorias de la información, quedando registradas en el formato definido para tal fin, incluidas las bases de datos definidas por la OTIC; estas restauraciones deben ser documentadas, con el fin de garantizar la continuidad de las actividades realizadas en la entidad, usando las herramientas tecnológicas en caso de presentarse la no disponibilidad de la información almacenada en las bases de datos.
- Es responsabilidad de los servidores almacenar la información en los medios dispuestos por la OTIC, el medio contará con un límite de espacio de almacenamiento. Cuando la información almacenada supere la capacidad de almacenamiento limite asignado, el usuario deberá revisar y depurar su información.
- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, sin autorización del responsable del activo de información.
- Teniendo en cuenta que, la información generada, producida y tratada por el colaborador es producto de la ejecución de actividades institucionales no se entregaran copias de respaldo de la información

contenida en correos electrónicos, sistemas de información, estaciones de trabajo y unidades de almacenamiento; en todo caso se validará la autorización de entrega de la información previa solicitud del responsable del activo indicando el motivo, tipo de información se requiere, la clasificación establecida en la matriz de activos de información. Es responsabilidad del usuario entregar el medio de almacenamiento en el cual será entregada la información.

- Mantener custodiadas copias idénticas de sistemas operativos que respondan a eventos de contingencia y disminuyan el impacto en caso de falla irreversible.
- La entidad debe evaluar mecanismos externos para generar copias de seguridad.

Política de seguridad de las comunicaciones

- Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la entidad.
- Segmentar los servicios de información, usuarios y sistemas, controlando así el tráfico.
- Los servicios de red deben estar protegidos a través de medios de autenticación.
- Implementar los mecanismos técnicos requeridos para la conexión segura con los servicios de red.
- Disponer de zona desmilitarizada en inglés demilitarized zone (DMZ) entre la red interna y externa con el objetivo limitar conexiones desde la red interna hacia Internet y conexiones desde internet hacia la red interna.
- Restringir la conectividad de la red cableada a los equipos que no son propiedad de la entidad.
- Se debe disponer de servicio de Internet para visitantes de la entidad.
- La entidad debe garantizar que las pasarelas de pago dispuestas para los vigilados a través de comercio electrónico (pagos por PSE) cumpla con los protocolos de seguridad como lo son SSL/TLS.

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

- Identificar los sistemas críticos de la entidad y documentar una metodología de revisión y escritura de eventos (event logs), que permita identificar las actividades por usuario, excepciones, fallas y eventos de seguridad que no den espacio a la alteración, uso no autorizado o repudio, en caso de presentarse materialización del riesgo y ser utilizados como medio probatorio.
- Mantener los relojes de todos los dispositivos tecnológicos con una única fuente de referencia, esto con el fin de mantener la exactitud del tiempo y permita correlacionar los eventos y logs.

Política de adquisición, desarrollo y mantenimiento de sistemas de información

- Garantizar que la seguridad es parte integral del ciclo de vida de los sistemas de información.
- Documentar lineamiento de control de instalación y cambios de los sistemas, para mantener operativas las aplicaciones basadas en estos y que permitan procedimientos de retroceso (RollBack) exitosos.
- Definir y documentar los requisitos de seguridad para la adquisición, desarrollo de los sistemas y mejoras de los existentes.

- Se debe aplicar mecanismos de auditoría a todos los sistemas de información en producción y se evaluara su tiempo de retención teniendo en cuenta la capacidad de almacenamiento institucional, en todo caso, este no debe ser inferior a 3 meses.
- Garantizar la separación de los entornos de desarrollo, pruebas y producción de los sistemas de información.
- Definir y documentar los entornos para el almacenamiento de los códigos y sus versiones.
- Ejecutar revisiones periódicas al licenciamiento de software y desinstalar de los equipos de cómputo, el software que no se encuentre licenciado.
- Establecer, documentar y ejecutar las prácticas seguras, criterios de solicitud y pruebas de calidad y aceptación sobre el desarrollo
- Las solicitudes para uso de software libre serán avaladas previo concepto del oficial de seguridad.
- Asegurar en la medida de lo posible que las bases de datos utilizadas en ambientes de pruebas sobre las etapas de desarrollo de soluciones de información no corresponden a información real o la misma debe ser modificada para tales fines.
- El desarrollo de aplicativos o sistemas de información diseñado por terceros debe estar bajo estándares de desarrollo de la OTIC y alineado a las políticas de seguridad de la información.
- Los datos de prueba no deben contener datos personales o información sensible, de ser necesario este contenido se deben utilizar mecanismos de enmascaramiento o sustitución de datos.

Política de protección de la información durante auditorias

Cuando se considere realizar auditorías a los sistemas de información y demás componentes de almacenamiento de esta, se debe tener en cuenta lo siguiente:

- La auditoría debe contemplar de manera específica el sistema al cual requiere acceso.
- Los accesos solo serán autorizados en modo lectura.
- Si se requiere un acceso diferente al modo lectura, se otorgará para copias aisladas del sistema con todos los parámetros de seguimiento de seguridad -logs.
- Si las pruebas afectan la disponibilidad estas deben realizarse fuera del horario laboral.

Política de Apagado de Servidores

El apagado de servidores puede clasificarse en las siguientes categorías:

- Apagado programado (mantenimiento): Para actividades rutinarias de mantenimiento, actualización de software, parches de seguridad o mantenimiento del hardware.
- Apagado de emergencia: En respuesta a incidentes críticos, fallos de hardware o software, amenazas de seguridad o desastres naturales.
- Apagado no planificado: Situaciones imprevistas que requieren la intervención inmediata.

Apagado Programado

- Planificación: El apagado programado debe planificarse con anticipación y debe ser aprobado por el Jefe de la OTIC y el equipo de infraestructura TI.
- Se deberá establecer una ventana de mantenimiento que cause la menor interrupción posible a las operaciones de la organización.
- Se debe notificar a los usuarios y equipos afectados con al menos 48 horas de antelación, indicando el motivo, la fecha y hora del apagado, la duración esperada y el impacto en los servicios.
- Antes de iniciar el apagado, se deben verificar todos los sistemas y procesos críticos, garantizando que no haya operaciones en curso que puedan verse interrumpidas o afectadas.
- Es necesario realizar copias de seguridad de todos los datos críticos antes del apagado. Los backups deben verificarse para asegurarse de que sean correctos y completos.
- Se deben Cerrar todas las aplicaciones y servicios no críticos. Desconectar los usuarios activos o migrar servicios a otros servidores redundantes si aplica. Apagar los servidores siguiendo el orden recomendado (servicios de aplicación, bases de datos, luego el sistema operativo).
- Reinicio y verificación: Después del apagado y la finalización del mantenimiento, se debe reiniciar el servidor y realizar una verificación exhaustiva de los servicios para garantizar que todos los sistemas estén funcionando correctamente.

Apagado de Emergencia

- En caso de un apagado de emergencia, el personal autorizado debe evaluar rápidamente la situación y decidir si el apagado es necesario para proteger los sistemas.
- Prioridades: Se deben priorizar los servidores críticos y los sistemas que contienen datos sensibles o que afectan la operación central.
- Comunicación inmediata: Se debe notificar inmediatamente, a los responsables de seguridad de la información y, si es necesario, a la dirección, describiendo la causa y los posibles impactos.
- Desconexión segura: Si es posible, se deben seguir los pasos de apagado programado para detener los servicios de manera controlada. Sin embargo, en casos extremos, se puede proceder al apagado forzoso, siempre documentando el proceso y las razones.

- Evaluación post-emergencia: Una vez resuelta la emergencia, se debe realizar una evaluación de los daños potenciales y restaurar los servicios tan pronto como sea posible. Se deben verificar los logs y las copias de seguridad para identificar cualquier pérdida de datos o daños en los sistemas.

Apagado No Planificado

- En caso de que ocurra un apagado no planificado debido a fallos eléctricos, fallos de hardware u otros factores imprevistos, se deben seguir los protocolos de emergencia para minimizar el impacto.
- Los servidores deben estar conectados a sistemas de respaldo de energía, como UPS (Sistemas de Alimentación Ininterrumpida), que permitan mantener los servidores activos el tiempo suficiente para apagarlos de forma controlada.
- Evaluación posterior: Después de que ocurra un apagado no planificado, se debe realizar una evaluación completa de los servidores, verificar la integridad de los datos y corregir cualquier problema resultante del apagado abrupto.

Roles y responsabilidades

- El Jefe de la Otic realizará la asignación de roles y responsabilidades, ademas, el equipo de Infraestructura TI será el encargado de administrar y gestionar todas las acciones que se realicen con relación a los servidores físicos y virtualizados de la entidad.

Registro y documentación

Todo apagado de servidor, ya sea programado, de emergencia o no planificado, debe ser registrado por el equipo de Infraestructura TI de la entidad. La documentación debe incluir:

- Fecha y hora del apagado.
- Causa del apagado.
- Servidores afectados.
- Responsable del apagado.
- Procedimiento seguido para el apagado y reinicio.
- Evaluación post-apagado y cualquier incidencia registrada.

Política de Actualización de Servidores y Aplicación de Parches de Seguridad

Esta política tiene como propósito establecer directrices claras para la actualización periódica de servidores y la aplicación de parches de seguridad con el objetivo de proteger la infraestructura tecnológica contra vulnerabilidades conocidas, minimizando los riesgos de ciberataques y garantizando la continuidad operativa.

Clasificación de Parches:

- Críticos: Parches que corrigen vulnerabilidades explotadas o que presentan un alto riesgo para la seguridad. Deben ser aplicados de forma inmediata.
- Importantes: Parches que corrigen vulnerabilidades con potencial de ser explotadas. Deben aplicarse en un plazo no mayor a una semana.
- Menores: Actualizaciones que no afectan directamente la seguridad. Deben aplicarse dentro del ciclo de mantenimiento programado.

Frecuencia de Actualización:

- Servidores críticos: Actualizaciones de seguridad se revisarán semanalmente y se aplicarán en un plazo de 24 horas tras su lanzamiento si son críticas.
- Servidores no críticos: Revisión de actualizaciones mensualmente, aplicando parches críticos dentro de las 72 horas y parches importantes dentro de la semana.
- Aplicaciones: Las actualizaciones deben aplicarse según las recomendaciones del proveedor, priorizando las que solucionen vulnerabilidades.

Pruebas de Actualización: Antes de aplicar un parche en el entorno de producción, debe realizarse una prueba en un entorno controlado para asegurar que la actualización no afecta la operatividad de los sistemas.

Monitoreo y Notificación: El equipo de infraestructura TI será responsable de monitorear las actualizaciones y parches disponibles, utilizando herramientas automatizadas cuando sea posible para asegurar que no se omita ninguna actualización crítica. Además, deberá notificar a los equipos afectados antes y después de aplicar los parches.

Excepciones: Si, por razones técnicas o operativas, no es posible aplicar un parche en el tiempo estipulado, se debe implementar una medida de mitigación temporal y notificar al Oficial de Seguridad de la Información, documentando el caso y los riesgos asociados.

DECLARACIÓN DE APLICABILIDAD

La declaración de aplicabilidad en ingles statement of applicability (SOA), es un documento que lista los controles que se van a implementar en la Superintendencia de Transporte, así como las justificaciones de aquellos controles que no serán implementados.

En el caso específico de la entidad, este tipo de análisis se hace evaluando el cumplimiento de la norma ISO 27002, para cada uno de los controles establecidos en los dominios o temas relacionados con la gestión de la seguridad de la información que este estándar especifica.

6. CONTROL Y SEGUIMIENTO

La OTIC será la encargada de realizar el monitoreo, seguimiento y control del manual de políticas de seguridad de la información de acuerdo con la competencia y la normatividad vigente

Control de Cambios del Documento

Control de cambios		
Versión	**Fecha**	**Descripción del cambio**
1	31/05/2022	Creación del documento
2	06-dic-2023	Incorporación de ítem en la política de seguridad física.
3	30-09-2024	Se incorpora la Política de Apagado de Servidores con cada uno de los lineamientos según la situación presentada. Se incorpora la Política de Actualización de Servidores y Aplicación de Parches de Seguridad.

Aprobación del documento		
Etapa	**Nombres y apellidos**	**Cargo**
Elaboró	Sebastián López Ciro	Contratista OTIC
Revisó	Andrea del Pilar Bermudez Sierra	Contratista OTIC
Aprobó	Urias Romero Hernandez	Jefe OTIC