REPUBLICA DE COLOMBIA

MINISTERIO DE TRANSPORTE
SUPERINTENDENCIA DE TRANSPORTE

RESOLUCIÓN NÚMERO **14134 DE 31/12/2020**

"Por medio de la cual se actualiza la Política General de Seguridad y Privacidad de la Información de la Superintendencia de Transporte"

EL 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

1. 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 las informaciones que se hayan 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.

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

3. 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.

4. 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 las normas que regulan la materia.

Lo anterior, en línea con lo previsto en el artículo 15 de la Constitución Política, en donde se estipuló 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 (…) 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, la 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.

5. 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.

6. 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.

7. 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 el principio de responsabilidad demostrada como aquella capacidad de demostrar que se han implementado medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012.

8. 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 este 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.

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

10. 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.

11. 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.

12. 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.

13. 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.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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.

19. 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.

20. 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.

21. En la Resolución 462 del 26 de abril del 2019, expedida por la Procuraduría General de la Nación, se establecieron funciones de la Procuraduría Delegada para la Defensa del Patrimonio Público, la Transparencia y la Integridad para adelantar en primera instancia las actuaciones disciplinarias que correspondan por 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.

22. 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, se 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.

23. 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 dispongan de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

24. 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.

25. 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.

26. 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 las infraestructuras 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.

27. De acuerdo con el acta del Comité Institucional de Gestión y desempeño efectuada el 13 de octubre de 2020, 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.

28. 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.

En mérito de lo expuesto,

RESUELVE

ARTÍCULO 1. *Objeto*. La presente resolución tiene como objeto actualizar y adoptar la 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 mediante la adopción e implementación del Modelo de Seguridad y Privacidad de la Información - MSPI enmarcado en el Sistema de Gestión de Seguridad de la información - SGSI, protege, preserva y administra la 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 funcionamiento y operaciones de la entidad, la prevención de incidentes de seguridad y la reducción de su impacto potencial dentro de un proceso de mejora continua.

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.

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

5.1 Objetivo General: Establecer las reglas, 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.

5.2 Objetivos Específicos

1. Gestionar y mantener la seguridad de la información que se gestiona y procesa dentro de la entidad y de los servicios y trámites dispuestos para los grupos de interés externos.

2. Establecer, implementar y mantener la protección adecuada de los activos de información de la entidad.

3. Asegurar que los funcionarios, contratistas, y empresas prestadoras de servicios en la entidad, conozcan sus responsabilidades y deberes, además que estén informados de las amenazas respecto a la seguridad de la información con el fin de reducir los riesgos de seguridad.

4. Evitar el acceso no autorizado a los sistemas de información, servicios de información e infraestructura tecnológica de la entidad, así como el daño o interceptación no autorizada a la información de la entidad.

5. Impedir la pérdida, daño, robo o puesta en riesgo de los activos de información y la interrupción de las actividades de la entidad.

6. Asegurar la operación correcta y segura de los servicios de almacenamiento y de procesamiento de la información.

7. Establecer la inclusión de controles de seguridad en los sistemas de información desarrollados por la entidad o por terceros, o adquiridos.

8. Dar directrices para contrarrestar las interrupciones en las actividades de la entidad y proteger los procesos más críticos en caso de fallas importantes de los sistemas de información o la infraestructura tecnológica y asegurar su recuperación oportuna.

9. Definir los roles y perfiles dentro de la entidad para la gestión y seguridad de la información.

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. Lineamientos para la organización de la seguridad de la información

2. Lineamientos para la gestión de activos de información.

3. Lineamientos de seguridad de los funcionarios y contratistas

4. Lineamientos para la seguridad física y del entorno

5. Lineamientos de seguridad de los equipos de cómputo

6. Lineamientos para la gestión de comunicaciones y operaciones

7. Lineamientos de copias de seguridad

8. Lineamientos para el control de acceso a sistemas de información, servicios de información e infraestructura tecnológica de la entidad

9. Lineamientos para el trabajo remoto

10. Lineamientos de seguridad para la adquisición, desarrollo y mantenimiento de sistemas de información

11. Lineamientos para la gestión de incidentes de la seguridad de la información

12. Lineamientos para la gestión de la continuidad del negocio

13. Lineamientos de interoperabilidad e intercambio de información

14. Lineamientos para terceros u outsourcing

15. Lineamientos para correo y documentos electrónicos

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 7. *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 8. *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 9. *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.

ARTÍCULO 10. O*bligatoriedad.* 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.

Todos los funcionarios y contratistas que laboran en la Superintendencia de Transporte se comprometen a cumplir con la Política de Seguridad y Privacidad de la Información y dar el manejo adecuado a los activos de información a su cargo.

ARTÍCULO 11. Incumplimiento. El incumplimiento de la Política de Seguridad y Privacidad de la Información y los lineamientos establecidos dará lugar a la aplicación acciones disciplinarias incluyendo la terminación del contrato, acción civil y penal, que, en su caso, puedan resultar aplicables.

ARTÍCULO 12. *Vigencia y derogatoria:* La presente resolución rige a partir de la fecha de su publicación y deroga la Resolución 60362 del 21 de noviembre de 2017.

PUBLÍQUESE Y CÚMPLASE
Dada en Bogotá D.C., a los

14134 DE 31/12/2020

Firmado digitalmente por: PABON ALMANZA CAMILO
Motivo: Firmado por el Superintendente de Transporte * CP
Fecha y hora: 31.12.2020 11:07:05

CAMILO PABÓN ALMANZA
SUPERINTENDENTE DE TRANSPORTE

Proyectó: Ing. Milena Malagon – Oficina de Tecnologías de la Información y las Comunicaciones- Oficial de Seguridad
Revisó/Aprobó: Ing. Claudia M. Rodríguez - Asesor despacho del superintendente de Transporte
Ing. Javier Pérez Pérez – Jefe Oficina de Tecnologías de la Información y las Comunicaciones
Dra. Maria Fernanda Sema Quiroga – Jefe Ofician Asesora Jurídica
Dr. Diego Felipe Diaz Burgos – Jefe de la Oficina Asesora de Planeación