



Libertad y Orden

Ministerio de Vivienda, Ciudad y Territorio
República de Colombia

RESOLUCIÓN NÚMERO

()

“Por la cual se adopta el Sistema de Gestión de la Seguridad de la Información – SGSI - y se conforma el Comité de Seguridad de la Información”

EL MINISTRO DE VIVIENDA CIUDAD Y TERRITORIO

En uso de las facultades legales y en desarrollo del artículo 2º de la Ley 962 de 2005, el Decreto 1151 de 2008 y,

CONSIDERANDO:

Que el Decreto 2573 de diciembre 12 de 2014, “*Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea, se reglamenta parcialmente la Ley 1341 de 2009 y se definen los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad, mediante el aprovechamiento de las TIC*” obliga a todas las entidades del estado a crear un Modelo de Seguridad y Privacidad de la Información.

Que el Decreto 1078 de Mayo 26 de 2015, “*Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones*” en su artículo 2.2.9.1.1.1. define los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones.

Que según el Decreto 2573 de diciembre 12 de 2014 en el componente de seguridad y privacidad de la información para las entidades del Estado colombiano, la prestación de servicios a los ciudadanos a través de las tecnologías de la información, deberá ser respaldada por la gestión, políticas y procedimientos adecuados, en la protección de los activos de información, orientados a preservar los pilares fundamentales de la seguridad de la información, confidencialidad, integridad y disponibilidad.

Que la Ley 1341 de 2009 “*Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones –TIC- se crea la Agencia Nacional de Espectro y se dictan otras disposiciones*”, señala en su artículo segundo, como aspectos fundamentales para el comercio electrónico, “la protección a los derechos de los usuarios de las TIC, el acceso y uso de las TIC, la garantía de los derechos de los ciudadanos y la masificación del Gobierno en Línea”.

Que de acuerdo a la Ley 1753 de 2015 “*Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 “Todos por un nuevo país”*” en el Artículo quinto “*Plan Nacional de Inversiones Públicas*”, en el ítem *Estrategias Transversales y Objetivos*, incluye a las Tecnologías de Información y Comunicaciones –TIC- como plataforma para la equidad, la educación y la competitividad. Adicionalmente circunscribe las TIC como herramienta de gerencia pública para el buen gobierno y la gestión óptima de la información. Adicionalmente en el Artículo 45. Estándares, Modelos y Lineamientos de Tecnologías de la Información y las Comunicaciones para los Servicios al Ciudadano, señala la implementación de la estrategia de Gobierno en Línea y el marco de referencia de arquitectura empresarial para la gestión de las tecnologías de información en el Estado.

Que el Gobierno Nacional, a través del documento CONPES 3701 del 14 de julio de 2011, estableció la Estrategia Nacional de Ciberseguridad y Ciberdefensa, con el fin de desarrollar medidas que aseguren la información de los ciudadanos frente a las amenazas informáticas, igualmente, estableció los compromisos a cargo del Ministerio de las

TIC, y demás entidades del estado, relacionados con el diseño e implementación de planes, políticas, estrategias, gestión, capacitación y sensibilización en lo referente a seguridad de la información.

Que la Ley 1273 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”*. Trata de los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos.

Que la Ley Estatutaria 1581 de 2012 *“Por la cual se dictan disposiciones generales para la protección de datos personales”*, regula el derecho fundamental de hábeas data, buscando proteger los datos personales registrados en cualquier base de datos que permite realizar operaciones, tales como recolección, almacenamiento, uso, circulación o tratamiento por parte de entidades de naturaleza pública y privada.

Que el Decreto 1377 del 27 de junio de 2013 define la implementación y el cumplimiento de la ley 1581 reglamentando aspectos relacionados con la autorización del titular de la información para el tratamiento de sus datos personales, las políticas de tratamiento de los responsables y encargados, y el ejercicio de los derechos de los titulares de la información.

Que la Ley 1266 de 2008 dicta disposiciones generales del hábeas data y regula el manejo de la información contenida en bases de datos personales, financieras, crediticias, comerciales, de servicios y las provenientes de terceros países.

Que la Ley 1712 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”*, regula el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información. Establece que toda información en posesión, bajo control o custodia de un sujeto obligado es pública y no podrá ser reservada o limitada sino por disposición constitucional o legal.

Que la Ley 527 de Agosto 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 el Artículo noveno señala *“Integridad de un mensaje de datos”, “se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación”*. En el Artículo decimo señala *“Admisibilidad y fuerza probatoria de los mensajes de datos”*. *“Los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Capítulo VIII del Título XIII, Sección Tercera, Libro Segundo del Código de Procedimiento Civil”*.

Que la Ley 594 de 2000 *“Por medio de la cual se dicta la Ley General de Archivos y se dictan otras disposiciones”* Ley General de Archivos del Sector Público, regula la obligación que tienen las entidades públicas y privadas que cumplen funciones públicas, de elaborar programas de gestión documental, independientemente del soporte en que se produzca la información para su cometido estatal, y del objeto social para el que fueron creadas, y que en el Anexo 11.2 *Seguridad de la Información, establece: que la conservación en condiciones seguras de estos documentos se efectúe en locales especialmente habilitados, al amparo de desastres naturales o accidentales, de robos o usos indebidos, de campos magnéticos o de diferencias térmicas o hidrométricas excesivas*.

Que la Ley 603 de 2000 establece que la Dirección de Impuestos y Aduanas Nacionales -DIAN trabaja con entidades públicas y privadas que hacen parte del comité antipiratería del software y de la producción intelectual, con el fin de extender las auditorías al tema de la informática.

Que la Norma ISO 27001 de 2013, en el numeral 5.1 *Liderazgo y Compromiso*, indica: que *“La Alta Dirección debe demostrar liderazgo y compromiso con el establecimiento, operación, revisión, mantenimiento y mejora del SGSI”* desarrollándolo en los siguientes literales, así: literal (A) *“Asegurando que se establezca una Política de Seguridad de la Información y los objetivos del SGSI”*, literal (B) *“Asegurando la integración de los requisitos del Sistema de Gestión de Seguridad de la Información en los procesos de la entidad”*, literal (C) *“Asegurando que los recursos necesarios para el Sistema de Gestión de Seguridad de la Información estén disponibles”*, literal (E) *“Asegurando que el Sistema de Gestión de Seguridad de la Información logre los resultados previstos”*, y literal (F) *“Dirigiendo y Apoyando a las personas, para contribuir a la eficacia del Sistema de Gestión de Seguridad de la Información”*.

RESUELVE:

ARTÍCULO PRIMERO. ADOPCIÓN DE LA NORMA DEL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN –SGSI–. Adóptese en el Ministerio de Vivienda Ciudad y Territorio –MVCT- y el Fondo Nacional de Vivienda – Fonvivienda, la Norma Técnica NTC-ISO-IEC 27001 de 2013, referente a Sistemas de Gestión de la

Seguridad de la Información, como mecanismo de implementación del componente Modelo de Seguridad y Privacidad de la Información establecido en el Decreto 2573 de diciembre 12 de 2014 *por el cual se definen los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones.*

ARTÍCULO SEGUNDO. OBLIGATORIEDAD. Como premisa que garantice la apropiación en el desarrollo, implementación, mantenimiento, revisión y perfeccionamiento del Sistema de Gestión de la Seguridad de la Información –SGSI-, éste se realizará con la participación activa de cada uno de los funcionarios del Ministerio. Esto implica el compromiso de todas y cada una de las personas que hacen parte de la entidad en el desarrollo de las diferentes acciones que se adelantarán para la implementación de dicho sistema, las cuales son de obligatorio cumplimiento.

ARTÍCULO TERCERO. REPRESENTANTE DEL MINISTRO PARA EL SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN. Como representante del Ministro para el Sistema de Gestión de la Seguridad de la Información –SGSI-, se designa al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones –TIC-, quien tiene la responsabilidad de liderar, impulsar y garantizar el desarrollo del proceso, por lo cual, podrá requerir la información que considere necesaria y citar a las reuniones pertinentes para el cumplimiento de los objetivos propuestos.

ARTÍCULO CUARTO. FUNCIONES DEL REPRESENTANTE DEL MINISTRO. Son funciones del Representante del Ministro las siguientes:

- 1) Coordinar el desarrollo, implementación, mantenimiento, revisión y mejora del Sistema de Gestión de la Seguridad de la Información – SGSI, con base en la misión y visión del Ministerio y Fonvivienda, sus objetivos y funciones y la política y objetivos de seguridad de la información en la Entidad.
- 2) Asegurar que se establezcan, ejecuten y mantengan los procesos necesarios para la implementación del Sistema de Gestión de la Seguridad de la Información - SGSI.
- 3) Procurar que todos los procesos y procedimientos definidos en el Sistema Integrado de Gestión del Ministerio y Fonvivienda, estén alineados con la política, propósitos y objetivos del Sistema de Gestión de la Seguridad de la Información – SGSI, y con los objetivos generales que definen las normas y guías técnicas adoptadas.
- 4) Generar en el Ministerio las acciones necesarias para un adecuado desarrollo, implementación, mantenimiento, revisión y mejora del Sistema de Gestión de la Seguridad de la Información – SGSI, para lo cual podrá requerir a las dependencias la información que considere necesaria.
- 5) Informar al Ministro, al Comité de Seguridad de la Información y a la alta dirección, según corresponda, sobre el desempeño del Sistema de Gestión de la Seguridad de la Información -SGSI, así como informar sobre las necesidades de mejora y proponer acciones para la mejora continua.
- 6) Asegurar que se promueva la toma de conciencia y el cumplimiento de las políticas de seguridad de la información en todos los niveles de la Entidad, a través de mecanismos de formación y divulgación a los servidores del Ministerio.
- 7) Asegurar la promoción de una cultura de gestión integrada de seguridad de la información en funcionarios, contratistas y visitantes acorde con las políticas y directrices del Sistema de Gestión de la Seguridad de la Información.
- 8) Orientar y coordinar permanentemente con las instancias necesarias el adecuado desarrollo, implementación, mantenimiento, revisión y mejora del Sistema de Gestión de la Seguridad de la Información - SGSI en el Ministerio y Fonvivienda.
- 9) Representar al Ministerio en asuntos relacionados con el Sistema de Gestión de la Seguridad de la Información, ante Ministerios y entidades externas.

PARAGRAFO. Con el objeto de divulgar y aplicar las políticas, objetivos, y estrategias definidas en el Sistema de Gestión de la Seguridad de la Información –SGSI, el representante de la dirección podrá conformar los comités o equipos de trabajo que se considere necesarios para apoyar el desarrollo e implementación del SGSI y citar a las reuniones pertinentes para el cumplimiento de los objetivos propuestos.

ARTÍCULO QUINTO. CREACION DEL COMITÉ DE SEGURIDAD DE LA INFORMACION. Créase el Comité de Seguridad de la Información, el cual indicará las acciones de orientación, promoción, mejoramiento, y supervisión del desarrollo e implementación del Sistema de Gestión de la Seguridad de la Información –SGSI en el Ministerio de Vivienda Ciudad y Territorio –MVCT- y el Fondo Nacional de Vivienda –Fonvivienda.

ARTÍCULO SEXTO. CONFORMACION DEL COMITÉ DE SEGURIDAD DE LA INFORMACION. El Comité de Seguridad de la Información estará integrado por:

- 1) El Ministro de Vivienda Ciudad y Territorio o su delegado, quien lo presidirá.
- 2) El Viceministro de Vivienda o su delegado
- 3) El Viceministro de Agua y Saneamiento o su delegado
- 4) El Secretario General o su delegado.
- 5) El Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones
- 6) El Jefe de la Oficina Asesora de Planeación o su delegado.

- 7) El Subdirector de Servicios Administrativos.
- 8) El Jefe de la Oficina Asesora Jurídica.
- 9) El Líder de Seguridad de la Información.

PARAGRAFO. El Jefe de la oficina de Control Interno, será invitado permanente al Comité de Seguridad de la Información, con voz pero sin voto.

ARTÍCULO SEPTIMO. FUNCIONES DEL COMITÉ DE SEGURIDAD DE LA INFORMACION. Son funciones del Comité de Seguridad de la Información las siguientes:

- 1) Apoyar y asesorar al Ministerio de Vivienda, Ciudad y Territorio en la formulación y aplicación de la Política, el Manual de Políticas de Seguridad de la Información y los objetivos del Sistema de Gestión de la Seguridad de la Información –SGSI y su aplicación.
- 2) Establecer las estrategias necesarias, apoyar y dar lineamientos para la implementación, mantenimiento y mejora del Sistema de Gestión de la Seguridad de la Información –SGSI del Ministerio de Vivienda, Ciudad y Territorio y el Fondo Nacional de Vivienda –Fonvivienda.
- 3) Apoyar la gestión con las áreas competentes, para la obtención de los recursos necesarios y requeridos para el desarrollo, implementación, gestión, mantenimiento y mejoramiento del Sistema de Gestión de la Seguridad de la Información –SGSI.
- 4) Fomentar la adopción de un enfoque de gestión basado en procesos y procurar su implementación.
- 5) Definir estrategias y mecanismos que propicien en los servidores públicos, la interiorización, apropiación, comunicación y divulgación de la filosofía del Sistema de Gestión de la Seguridad de la Información –SGSI.
- 6) Propiciar un clima de compromiso hacia el Sistema de Gestión de la Seguridad de la Información –SGSI, en toda la Entidad.
- 7) Revisar y analizar los eventos e incidentes de seguridad detectados y evidenciados al interior del Ministerio y Fonvivienda, y el tratamiento dado a los mismos.
- 8) Proponer acciones preventivas, correctivas y de mejora del Sistema de Gestión de la Seguridad de la Información –SGSI.
- 9) Revisar y actualizar anualmente la política de Seguridad de la Información y el Manual de Políticas de Seguridad de la Información con base en la nueva legislación o reglamentación expedida.
- 10) Las demás funciones que le asigne el Ministro de Vivienda, Ciudad y Territorio, relacionadas con el Sistema de Gestión de la Seguridad de la Información –SGSI.

ARTÍCULO OCTAVO. PRESIDENTE DEL COMITÉ. Actuará como presidente del comité el Ministro o su delegado y a falta de este por la persona que designen los asistentes a la reunión del Comité de Seguridad de la Información.

Son funciones del Presidente del Comité de Seguridad de la Información las siguientes:

- 1) Impulsar y velar porque se cumplan los objetivos y políticas del Comité de Seguridad de la Información.
- 2) Convocar y presidir de ordinario las reuniones del Comité de Seguridad de la Información.
- 3) Autorizar con su firma las Actas del Comité de Seguridad de la Información, las cuales deben llevar la firma del Secretario.
- 4) Proponer las medidas que estime conducentes para el logro de los objetivos del Comité de Seguridad de la Información.

ARTÍCULO NOVENO. SECRETARÍA TÉCNICA. Actuará como Secretario del Comité el Jefe de la Oficina TIC de manera indelegable.

Son funciones de la secretaría técnica las siguientes:

- 1) Enviar por medio físico o electrónico a los miembros del Comité la convocatoria realizada por el presidente a las sesiones ordinarias y extraordinarias, indicando el día, la hora y el lugar de la reunión.
- 2) Elaborar el orden del día y las actas de cada una de las reuniones del Comité.
- 3) Enviar las comunicaciones con las recomendaciones dadas por el Comité a las diferentes dependencias de la entidad.
- 4) Citar a reuniones y solicitar los soportes requeridos para hacer seguimiento al cumplimiento de los compromisos adquiridos al interior del Comité.
- 5) Elaborar informes trimestrales sobre la gestión del comité.
- 6) Llevar el archivo de las actas y asuntos tratados al interior del comité.

ARTÍCULO DECIMO. SESIONES. El Comité de Seguridad de la Información se reunirá ordinariamente cada tres (3) meses y extraordinariamente las veces que se requiera, previa convocatoria del Presidente del Comité. La convocatoria se hará con tres (3) días calendario de anticipación a la fecha de la reunión, anexando la documentación requerida para

el análisis de los temas a tratar. Las sesiones constaran en Actas que deberán ser suscritas por el Presidente y el Secretario del Comité.

PARAGRAFO. La asistencia y participación en este comité es de carácter obligatorio.

ARTÍCULO DECIMO PRIMERO. QUORUM Y DECISIONES. El Comité de Seguridad de la Información solo podrá deliberar con la asistencia de la mitad más uno de sus integrantes y las decisiones serán tomadas por la mayoría de sus asistentes.

A las reuniones del Comité de Seguridad de la Información, podrán asistir con voz pero sin voto, personas invitadas cuando esta instancia lo considere conveniente.

ARTÍCULO DECIMO SEGUNDO. VIGENCIA. La presente resolución rige a partir de la fecha de su publicación.

COMUNÍQUESE Y CÚMPLASE

Dada en Bogotá, D.C., a los

LUIS FELIPE HENAO CARDONA
Ministro de Vivienda, Ciudad y Territorio

Proyectó: Pedro Enrique Cortés Sánchez.
Revisó: Edgar Omar Rubiano Rodríguez - Jefe Oficina TIC
: German Alberto Diaz Pinto – Jefe (E) de la Oficina Asesora de Planeación
Aprobó: Armando Gomez Rayo – Secretario General.