

RESOLUCIÓN NÚMERO

DE 2016

(# 4905)

13 MAY 2016

Por medio de la cual se adopta el Sistema de Gestión de la Seguridad de la Información, para la realizar el seguimiento de seguridad a nivel integral sobre procesos, procedimiento y sistemas de Información.

EL SUPERINTENDENTE DE NOTARIADO Y REGISTRO

En ejercicio de sus facultades legales establecidas en especial las que le confiere y

CONSIDERANDO:

Que el ARTÍCULO 230 de la Ley 1450 de 2011 establece que todas las entidades de la Administración pública deberán adelantar acciones señaladas en la Estrategia de Gobierno en Línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, a través del cumplimiento de los lineamientos que establezca.

Que mediante Decreto 2693 de 2012, se establecieron los lineamientos generales de la Estrategia de Gobierno en Línea y se reglamentan parcialmente las leyes 1341 de 2009 y 1450 de 2011.

Que el Ministerio de Tecnologías de la Información y las Comunicaciones, mediante documento de fecha junio de 2011, actualizó el Manual para la Implementación de las Estrategias de Gobierno en Línea en las entidades del orden nacional, en el que señaló los lineamientos y criterios a que estas deben sujetarse para la implementación de la estrategia y la definición de las políticas y estándares respectivos.

Que mediante Decreto 2573 de 2014, se establece los lineamientos generales de la Estrategia de Gobierno en Línea y se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.

Que el referido requiere la implementación de un Sistema de Gestión de Seguridad de la Información que permita ejercer controles y gobernabilidad sobre la seguridad integral en los procesos, procedimientos, sistemas de información y/o documentación física que genere la Entidad.

Que el Manual requiere la creación del Comité de Seguridad de la Información como órgano operativo y de apoyo para efectos de garantizar la adecuada implementación del Sistema de Gestión de Seguridad de la Información, el cual será conformado por el Comité Administrativo y Desarrollo.

En mérito de lo expuesto,

RESUELVE:

ARTÍCULO PRIMERO: Implementar el Sistema de Gestión de la Seguridad de la Información diseñado por la Entidad en el cual se compromete a implementar y aplicar las políticas de seguridad de la información para proteger la información capturada, usada y producida para efectos de los servicios que se prestan a los ciudadanos.

ARTÍCULO SEGUNDO: El Sistema de Gestión de Seguridad de la Información contiene el manual de seguridad de la información, la política de seguridad de la información corporativa y será

RESOLUCIÓN NÚMERO

DE 2016

(# 4905)

13 MAY 2016

complementada por un conjunto de políticas por dominios basadas en ISO 27000, normas, procedimientos, decretos necesarios para garantizar aplicación y seguimiento correspondiente.

ARTÍCULO TERCERO: Es deber de todo funcionario de la Superintendencia de Notariado y registro cumplir con los lineamientos establecidos en la política de seguridad de la información, los procedimientos, normas y/o decretos adyacentes.

ARTÍCULO CUARTO: La Oficina de Tecnologías de la información desarrollará las actividades necesarias para la implementación, seguimiento, evaluación y mejoramientos del Sistema de Gestión de la Seguridad de la Información.

ARTÍCULO QUINTO: El incumplimiento de las políticas establecidas en el Sistema de Gestión de Seguridad de la Información será causal de mala conducta y se tomarán medidas disciplinarias al interior de la Entidad.

ARTÍCULO SEXTO: Se adoptará el Sistema de Gestión de Seguridad de la Información en conjunto y serán de obligatorio cumplimiento al interior de la Entidad las diferentes políticas, normas y documentos subsidiarios tales como procedimientos y protocolos relacionados a continuación:

1. Políticas de Seguridad de la Información SNR
 - 1.1. Organización de la Seguridad
 - 1.2. Aspectos relacionados con recurso humano
 - 1.3. Gestión de Activos de Información
 - 1.4. Control de Acceso
 - 1.5. Criptografía
 - 1.6. Seguridad Física y Ambiental
 - 1.7. Seguridad de las Operaciones
 - 1.8. Seguridad de las Comunicaciones
 - 1.9. Adquisición, Desarrollo y Mantenimiento de Software
 - 1.10. Relaciones con los proveedores
 - 1.11. Gestión de incidentes de seguridad
 - 1.12. Administración de la continuidad de negocio
 - 1.13. Cumplimiento de requerimientos
2. Política de dispositivos móviles personales propios
3. Políticas para el uso adecuado de recursos informáticos

ARTÍCULO SEPTIMO: El Comité Administrativo y Desarrollo debe coordinar la formulación y la implementación del Sistema de Gestión de Seguridad de la Información, de acuerdo a los lineamientos establecidos por Gobierno en línea y la ley Antitramites, para el interior de la Entidad y para las Oficinas de Registro.

ARTÍCULO OCTAVO: El Comité Administrativo y Desarrollo, creado estará conformado por los siguientes servidores públicos:

- Superintendente Delegado para Registro
- Superintendente Delegado para Notariado
- Superintendente Delegado para la protección, restitución y formalización de Tierras
- Secretario General

RESOLUCIÓN NÚMERO

DE 2016

13 MAY 2016

(# 4905)

- Director Técnico de Registro
- Directora Vigilancia y Control Notarial
- Director Administrativo y financiero
- Jefe Oficina de Tecnologías de la Información
- Jefe Oficina Asesora de Planeación
- Jefe Oficina Control Interno de Gestión
- Jefe Oficina de Control Disciplinario Interno
- Jefe Oficina Asesora Jurídica

ARTÍCULO NOVENO: Funciones del Comité Institucional de Administrativo y Desarrollo referentes a Seguridad de la Información. Como parte de las funciones y responsabilidades, el Comité de Seguridad de la Información debe realizar las siguientes actividades:

- Ser un ente asesor en materia de seguridad para la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.
- Revisar y aprobar la operación del Sistema de Gestión de Seguridad de la Información (SGSI), y definir responsabilidades para su implementación y mantenimiento en el tiempo.
- Definir los roles y responsabilidades relacionados con seguridad a través de la Entidad.
- Definir y revisar las Políticas de Seguridad de la Información de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.
- Asegurar que se identifiquen las metas e indicadores de gestión de seguridad, y que se encuentren alineadas con los objetivos de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.
- Garantizar que los aspectos relacionados con la seguridad de la información estén incluidos dentro del proceso de planeación estratégica de la Entidad.
- Monitorear los cambios significativos en el Sistema de Gestión de la Seguridad de la Información (SGSI).
- Definir y priorizar proyectos de seguridad y servir de soporte gerencial para su desarrollo.
- Aprobar las iniciativas para mejorar la gestión de la seguridad.
- Definir los requerimientos y la inversión necesaria en los proyectos críticos sobre seguridad de la información.
- Aprobar cambios importantes en la infraestructura tecnológica y de seguridad, así como los nuevos desarrollos de aplicaciones que afecten significativamente la Entidad.

RESOLUCIÓN NÚMERO

DE 2016

(# 4905)

13 MAY 2016

- Efectuar el seguimiento a la Matriz de Riesgos de Seguridad de la Información y al Plan de Tratamiento de Riesgos, de manera que permita definir los requerimientos de seguridad para los procesos de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.
- Ser un facilitador para la implementación y puesta en práctica del Sistema de Gestión de Seguridad de la Información y del Plan de Continuidad del Negocio.
- Revisar y monitorear las investigaciones de los incidentes de seguridad.
- Definir, impulsar y promover las estrategias de los planes de concientización en seguridad de la información.
- Establecer las políticas y apoyar la implementación de las estrategias de continuidad del negocio para los servicios prestados por la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.

ARTÍCULO DECIMO: Oficial de Seguridad y/o Profesional Asignado. La SUPERINTENDENCIA DE NOTARIADO Y REGISTRO contará con un Oficial de Seguridad y/o Profesional Asignado, quien lidera un grupo dedicado a la gestión de la seguridad de la información dentro de la Entidad.

ARTÍCULO DECIMO PRIMERO: Funciones del Oficial de Seguridad. El Oficial de Seguridad y/o Profesional Asignado de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO es el responsable de la gestión y/o administración del SGSI. Con base en esto, su función es la de realizar el diseño, implementación, revisión y mantenimiento del SGSI. Adicionalmente, una de sus principales funciones es ser el responsable del funcionamiento del Comité de Seguridad.

Dentro de las responsabilidades directas del Oficial de Seguridad y/o Profesional Asignado, se encuentran:

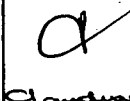
- Administrar el Sistema de Gestión de la Seguridad de la Información de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO (ISO/IEC 27001:2013). Estructurar y mantener un Sistema de Gestión de la Seguridad de la Información y asegurar que es debidamente operado, implementado y mantenido, en concordancia con los objetivos de la Entidad.
- Apoyar al Comité de Seguridad en la medición de la efectividad del Sistema de Gestión en Seguridad de la Información, mediante el reporte permanente de los resultados de las revisiones de seguridad.
- Asegurar que se establezcan e implementen las políticas y procedimientos de seguridad de la información, acordes con los objetivos estratégicos, la planeación estratégica, y las definiciones dadas por el Comité de Seguridad.

RESOLUCIÓN NÚMERO

DE 2016

(**# 4905**)**13 MAY 2016**

- Definir, revisar, divulgar y verificar el cumplimiento del Modelo de Seguridad de la Información.
- Coordinar la aplicación de los controles de seguridad en los sistemas, procesos y servicios, existentes o nuevos, que se definan para la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.
- Liderar los diferentes grupos de apoyo para la gestión de la seguridad de la información.
- Mantener actualizados los requerimientos de seguridad de los sistemas de información.
- Coordinar el Comité de Seguridad de la Información.
- Definir y dar soporte a las iniciativas de seguridad en la Entidad.
- Definir los requisitos de seguridad para las soluciones tecnológicas, de manera que se cumpla con los requerimientos de seguridad de la Entidad.
- Verificar que las soluciones tecnológicas cumplen con las especificaciones de seguridad establecidas por el Modelo de Seguridad de la Información establecido por la Entidad.
- Organizar y mantener los requerimientos de seguridad y procesos relacionados que deba cumplir la Entidad para responder a los entes de control internos y externos que corresponda.
- Elaborar y gestionar el procedimiento de análisis, tratamiento y gestión del riesgo, para lograr los niveles de riesgo aceptables establecidos por la Entidad.
- Elaborar, administrar y realizar la gestión del proceso de manejo de incidentes.
- Liderar la investigación de los incidentes de seguridad.
- Definir, indicar y evaluar los requerimientos de seguridad del Plan de Continuidad del Negocio, en coordinación con el área o dependencia responsable, asignada por el Superintendente de Notariado y Registro.
- Desarrollar y aplicar el plan de concientización, entrenamiento y capacitación en seguridad de la información para la Entidad.
- Ser punto de contacto para todos los temas relacionados con seguridad de la información de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO. Ser un recurso permanente de consultoría interno.
- Establecer los mecanismos de clasificación e identificación de activos de información de la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO.



RESOLUCIÓN NÚMERO

DE 2016

(**# 4905**)

13 MAY 2016

- Establecer lineamientos para definir los requerimientos y los mecanismos de control de acceso a la información según su nivel de clasificación.
- Revisar los requerimientos y niveles de seguridad que deban ser incluidos en los contratos con terceros.
- Organizar y mantener los procesos de certificación en seguridad de la información y procesos similares relacionados con el área, que sea exigencia para la Entidad.
- Consultar con el área jurídica las implicaciones a nivel legal sobre la implementación de las medidas de seguridad de la información aplicadas en cada uno de los proyectos que la SUPERINTENDENCIA DE NOTARIADO Y REGISTRO requiera como Entidad.

ARTÍCULO DECIMO SEGUNDO: Reuniones. El Comité Institucional de Desarrollo Administrativo deberá reunirse periódicamente cada tres (3) meses y en forma extraordinaria cuando se amerite. Previa convocatoria del Oficial de Seguridad y/o Profesional Asignado.

Las sesiones podrán realizarse de forma presencial o virtual a través de medios electrónicos, informáticos, telefónicos, audiovisuales o cualquier otro medio que permita el intercambio de información entre los miembros del comité.

PARÁGRAFO UNO. Para realizar las deliberaciones y toma de decisiones del Comité Institucional de Desarrollo Administrativo, se requerirá mínimo la mitad más uno de los integrantes asistentes a la reunión.

PARÁGRAFO DOS. De cada una de las reuniones se levantará la respectiva acta, la cual deberá estar firmada por quien presida la reunión y el Oficial de Seguridad de la Información y/o Profesional Asignado, previa aprobación de los miembros participantes en la reunión. Las actas deben registrar los compromisos para hacer seguimiento y serán numeradas consecutivamente durante la vigencia anual.

ARTÍCULO DECIMO TERCERO: La presente resolución rige a partir de su publicación.

COMUNIQUESE Y CÚMPLASE

Dada en Bogotá, D.C. a

13 MAY 2016

EL SUPERINTENDENTE DE NOTARIADO Y REGISTRO


JORGE ENRIQUE VELEZ GARCÍA

Elaboró: Ing. Juan Carlos Ramirez Valderrama – Asesor Oficina de TI
Revisó: Ing. Elba Lucia Corredor - Jefe Oficina de TI
Dr. Marcos Jaher Parra Oviedo – Jefe Oficina Asesora Juridica
Dra. Claudia Alvarez – Asesora Despacho Superintendente