REGISTRADURÍA
NACIONAL DEL ESTADO CIVIL

RESOLUCIÓN No. 3308 DE 2024

(11 ABR. 2024)

"Por la cual se adopta la Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil y se dictan otras disposiciones"

EL REGISTRADOR NACIONAL DEL ESTADO CIVIL

En ejercicio de las atribuciones establecidas en los numerales 1 y 2 del artículo 25 del Decreto 1010 de 2000, y

CONSIDERANDO:

Que, el artículo 120 de la Constitución Política de Colombia establece que: "*(...) la Organización Electoral está conformada por el Consejo Nacional Electoral, por la Registraduría Nacional del Estado Civil y por los demás organismos que establezca la Ley. Tiene a su cargo las elecciones, su dirección y vigilancia, así como lo relativo a la identidad de las personas (...)*".

Que, de conformidad con el artículo 266 de la Constitución Política, modificado por el Acto Legislativo 02 de 2015, corresponde a la Registraduría Nacional del Estado Civil ejercer "(...) *las funciones que establezca la ley, incluida la dirección y organización de las elecciones, el registro civil y la identificación de las personas (...)*".

Que, la Constitución Política señala en su artículo 1° que Colombia es un Estado social de derecho, fundado en la prevalencia del interés general; en su artículo 2.°, se indica que servir a la comunidad es un fin esencial del Estado; y en su artículo 209, que la función administrativa está al servicio de los intereses generales y se desarrolla con fundamento en los principios de igualdad, moralidad, eficacia, economía, celeridad, imparcialidad y publicidad.

Que, a su turno, la Carta Superior incorporó en el catálogo de derechos fundamentales el derecho a la intimidad; en este orden de ideas, el artículo 15 *ibidem* indicó: *"Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen 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. (...)*".

Que, el Congreso de la República expidió la Ley 527 de 1999, por medio de la cual se definió y reglamentó el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictaron otras disposiciones,

Que, la Ley Estatutaria 1581 de 2012, desarrollo "*(...) el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma*"; norma que fue reglamentada en el Decreto 1377 de 2013..

Que, a su turno, la Ley 1712 de 2014 reguló "*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*", estableciendo, entre otras cosas, que

su aplicación sería para "*a) Toda entidad pública, incluyendo las pertenecientes a todas las Ramas del Poder Público, en todos los niveles de la estructura estatal, central o descentralizada por servicios o territorialmente, en los órdenes nacional, departamental, municipal y distrital*" y "*b) Los órganos, organismos y entidades estatales independientes o autónomos y de control*". Esta Ley fue reglamentada mediante el Decreto Reglamentario 103 de 2015,

Que, la Registraduría Nacional del Estado Civil reglamentó las condiciones y el procedimiento para el acceso a las bases de datos de la información que produce y administra la Entidad, mediante la Resolución No. 5633 del 29 junio de 2016, suscrita por el Registrador Nacional del Estado Civil.

Que, mediante la Resolución No. 4173 de 2016, suscrita por el Registrador Nacional del Estado Civil se adoptó la Políticas de Seguridad de la Información, en la que se estableció la normatividad y políticas de seguridad al interior de la Entidad.

Que, el Decreto 1010 de 2000 establece la organización interna de la Registraduría Nacional del Estado Civil y fija las funciones de cada una de sus dependencias, por tanto, es responsabilidad de todos los funcionarios dar estricto cumplimiento a las políticas de seguridad de la información, las cuales se constituyen la base de creación del Sistema de Gestión de Seguridad de la Entidad.

Que, teniendo en cuenta que las tecnologías en la última década han tenido un avance vertiginoso en todas las principales áreas del conocimiento, en especial la de los servicios en internet; los ciberdelincuentes perfeccionado sus métodos y técnicas de ataques para infiltrarse en los nuevos sistemas desarrollados, hurtar y secuestrar información confidencial y causar daños significativos a las plataformas informáticas que no están lo suficientemente actualizadas y con los controles de seguridad mínimos necesarios para su defensa; exigiendo a las empresas privadas y las entidades del sector público mantener sus infraestructuras constantemente actualizadas, con controles, lineamientos y políticas de seguridad para estar a la vanguardia de los retos que estos avances tecnológicos demandan.

Que, ante la situación actual, la Registraduría Nacional del Estado Civil requiere protegerse de las técnicas cada vez más sofisticadas que usan los ciberdelincuentes, como el uso de inteligencia artificial y aprendizaje automático, para eludir las defensas tradicionales y evadir la detección en ataques dirigidos y campañas de ciber espionaje que se han vuelto cada día más comunes, lo que pone en riesgo la información confidencial de genera, administra, custodia y/o procesa.

Que, la Registraduría Nacional del Estado Civil identifica la información como un componente indispensable para sus funciones, razón por la cual, se deben establecer unas políticas, estrategias y acciones que aseguren la información y esta sea protegida de una manera adecuada, independientemente de la forma en la que esta sea manejada, procesada, transportada y/o almacenada.

Que, en atención con lo anteriormente mencionado, se requiere adoptar una nueva política de seguridad y un manual de políticas internas y controles de seguridad de la información, para que, a través de éste, se adelanten el seguimiento de mejora continua que apoye y de soporte al cumplimiento de la política general de seguridad de la información al interior de la Entidad.

Que, a su turno, se hace necesario implementar, dirigir, promover, asegurar, mantener, revisar y comunicar los requisitos del sistema de gestión de seguridad de la información de la organización, a intervalos planificados, para asegurar su continua idoneidad, suficiencia y eficacia conforme lo señala la norma ISO 27001:2013.

Que, la política de seguridad de la información es objeto de actualización y que para su elaboración se deberá tener en cuenta cada uno de los 14 grupos de control con sus respectivos objetivos, los cuales se encuentran identificados en el estándar ISO/ IEC 27001 de 2013.

Que, las mejores prácticas de seguridad del mercado y los estándares de seguridad tales como la norma ISO 27001 en su versión 2013, indican qué, la política general de seguridad de la información debe actualizarse regularmente en periodos no mayores a un año, de acuerdo con la velocidad con la que se está desarrollando la tecnología y constante evolución de las amenazas cibernéticas.

Que, la seguridad y privacidad de los datos e Información es una prioridad para la Registraduría Nacional del Estado Civil, por tanto, es responsabilidad de todos los servidores públicos, contratistas, proveedores y colaboradores velar por que no se realicen actividades que atenten contra la confidencialidad, integridad, disponibilidad y no repudio sobre los datos e información en cualquiera de las presentaciones que esta pueda tener, e independientemente de la forma que esta pueda revestir.

Que la Registraduría Nacional del Estado Civil, en línea con los lineamientos del Plan Estratégico 2024-2027, ha delineado los objetivos estratégicos que definen la dirección de la entidad. Estos objetivos están orientados hacia la generación de valor público mediante la mejora de la calidad en la prestación de servicios, lo que implica la salvaguarda de la información concerniente a los procesos misionales, como la identificación y la gestión electoral. En aras de mantener la continuidad en el cumplimiento de este plan, se hace necesaria la implementación de una nueva política de seguridad de la información.

Que, el Registrador Nacional del Estado Civil podrá crear y conformar comités al interior de la Entidad, lo anterior, de acuerdo con lo establecido en el artículo 51 del Decreto 1010 de 2000 que establece: *"Los objetivos, la conformación y las funciones de los consejos, comités, comisiones y juntas estarán establecidos por las disposiciones legales correspondientes. El Registrador Nacional del Estado Civil podrá reglamentar estos aspectos tanto para los órganos de creación legal como para los que él decida conformar para suplir las necesidades del servicio. (...)".*

En mérito de lo expuesto, se

RESUELVE:

Título 1.
De la Política de Seguridad de la Información

Artículo 1: Adopción de la Política de Seguridad de la Información. Adoptar la Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil, estableciendo que los requisitos de seguridad y privacidad de los datos e información y de todos sus activos de información tangibles e intangibles son prioridad para la Entidad y, por lo tanto, son responsabilidad y compromiso del nivel directivo, de todos los servidores públicos, proveedores, contratistas y partes interesadas, quienes garantizarán el continúo cumplimiento tanto de la presente política, como de lo descrito en el manual de políticas internas y controles de seguridad de la información, definidos en este documento.

Artículo 2: Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil. La información es un activo fundamental para la Registraduría Nacional del Estado Civil y, por tanto, la Entidad está comprometida con proteger la confidencialidad, integridad, disponibilidad y no repudio, siendo esta parte de una estrategia orientada al cumplimiento de sus procesos estratégicos, misionales, de apoyo, de evaluación, control y continuidad del negocio, entendiendo como tal los procesos de registro civil, identificación y electoral, la administración de riesgos y la consolidación de una cultura de seguridad y privacidad de los datos e información, acorde con lo indicado en este acto administrativo y Manual de Políticas Internas y Controles de Seguridad de la Información.

Por tanto, han sido socializadas tanto las políticas internas como los controles que apoyan el desarrollo, no sólo de éstas, sino de la presente política y que se encuentran desarrolladas en el manual de políticas internas y controles de seguridad de la información, acorde al cumplimiento de los procesos administrativos y operativos, de identificación y realización de eventos electorales, y por tanto, se encuentran ajustadas a los cambios tecnológicos y marcos jurídicos vigentes de orden supranacional, constitucional, legal y reglamentario, protegiendo los datos e información contra las amenazas y vulnerabilidades internas o externas, intencionales o accidentales, en las diferentes formas en las cuales se pueda encontrar la información.

Artículo 3. Objetivo General de la Política de Seguridad de la Información. Garantizar la seguridad de los datos e información con respecto a la normas actuales asociadas a la ISO/IEC 27001 junto con su Anexo A y a la recomendación indicada como mejor práctica que ha sido dispuesta por el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, la cual se basa en orientar la protección tanto de los activos de información como de los datos e información que almacena la Registraduría Nacional del Estado Civil, los cuales constituyen el soporte y apoyo para los procesos misionales, estratégicos, de apoyo y de evaluación que se encuentran definidos e identificados en la Entidad.

Artículo 4. Alcance de la Política de Seguridad de la Información. Inicia con la identificación y definición de los parámetros que debe tener en cuenta la Política de Seguridad de la Información para la protección de la confidencialidad, integridad, disponibilidad y no repudio de los datos, información y activos de información que almacenan y custodian los registros de la Registraduría Nacional del Estado Civil, pasando por el diseño, construcción de las políticas internas y controles entre los cuales se encuentra la gestión de vulnerabilidades técnicas que apoyan a la protección de lo mencionado y termina con la generación documental, socialización y apropiación del Modelo de Seguridad y Privacidad de la Información, la cual aplica

a todos los servidores públicos, contratistas, proveedores o partes interesadas que posean cualquier vínculo legal o contractual de la Registraduría Nacional del Estado Civil.

Artículo 5. Ámbito de aplicación. La presente política va dirigida a los servidores públicos, contratistas, proveedores y terceros que tengan acceso a los datos e información de la Registraduría Nacional del Estado Civil quienes serán los responsables de la aplicación y cumplimiento de ésta, y así mismo, garantizar la confidencialidad, integridad, disponibilidad y no repudio a los datos e información y activos de información que almacenan y custodian, como resultado de los procesos misionales, estratégicos, de apoyo y seguimiento, dando cumplimiento a la misionalidad de la Entidad.

Artículo 6. Definiciones. Para efectos de la Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil se tendrán las siguientes definiciones:

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a individuos, Entidades o procesos no autorizados.[1]

Disponibilidad: Propiedad de la información de estar accesible y utilizable cuando lo requiera una Entidad autorizada.[2]

Integridad: Propiedad de la información relativa a su exactitud y completitud.[3]

Mejor Práctica: Establecida para asegurar que las características de seguridad de los sistemas utilizados con regularidad estén configurados y administrados de manera uniforme, garantizando un nivel consistente de seguridad a través de la entidad.

Modelo de Seguridad y Privacidad de la Información: El Modelo de Seguridad y Privacidad de la Información – MSPI, conduce a la preservación de la confidencialidad, integridad, disponibilidad de la información, permitiendo garantizar la privacidad de los datos, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos.[4]

Registro: Un registro es un conjunto de campos que contienen los datos que pertenecen a una misma unidad de información, es decir, es la unidad de información que se asocia a un proceso de entrada y salida; también designa el sustento físico de esas unidades.

Riesgo: Efecto de la incertidumbre sobre los objetivos. Un efecto es una desviación de lo esperado: positivo o negativo. La incertidumbre es el estado, incluso parcial, de deficiencia de información relacionada con la comprensión o conocimiento de un evento, su consecuencia o probabilidad. El riesgo a menudo se caracteriza por la referencia a posibles "eventos" (Guía ISO 73: 2009) y "consecuencias" (Guía ISO 73: 2009) o una combinación de estos. El riesgo a menudo se expresa en términos de una combinación de las consecuencias de un evento (incluyendo cambios en las

[1] https://www.iso27000.es/glosario.html
[2] https://www.iso27000.es/glosario.html
[3] https://www.iso27000.es/glosario.html
[4] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf

circunstancias) y la "probabilidad" asociada (Guía ISO 73: 2009) de ocurrencia. En el contexto de los sistemas de gestión de seguridad de la información, los riesgos de seguridad de la información pueden expresarse como un efecto de incertidumbre sobre los objetivos de seguridad de la información. El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización.[5]

Seguridad de la información: Preservación de la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, otras propiedades como la autenticidad, la responsabilidad, el no repudio y la confiabilidad también pueden estar involucradas.[6]

Sistema de Gestión: Conjunto de elementos interrelacionados o interactivos de una organización para establecer políticas y objetivos y procesos para alcanzar esos objetivos. Un sistema de gestión puede abordar una sola disciplina o varias disciplinas. Los elementos del sistema incluyen la estructura, roles y responsabilidades, planificación y operación de la organización. El alcance de un sistema de gestión puede incluir la totalidad de la organización, funciones específicas e identificadas de la organización, secciones específicas e identificadas de la organización, o una o más funciones en un grupo de organizaciones.[7]

Sistema de Gestión de la Seguridad de la Información: Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión del riesgo y de mejora continua.[8]

Artículo 7. Desarrollo de la Política de Seguridad de la Información. En el marco de la Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil, la Entidad ha decidido definir, establecer, implementar, operar y mejorar de forma continua un Modelo de Seguridad y Privacidad de la Información, el cual se apoya en lineamientos claros enfocados a las necesidades de la prestación del servicio sobre la identificación personal de la ciudadanía y la transparencia del proceso electoral, acordado en el cumplimiento de las funciones de la Registraduría Nacional del Estado Civil y a los requerimientos regulatorios que le puedan aplicar según a su naturaleza.

Para tal efecto, se establecen las once (11) políticas internas de seguridad que soportan el Modelo de Seguridad y Privacidad de la Información en la Registraduría Nacional del Estado Civil:

- Política para dispositivos móviles.
- Política para trabajo en casa.
- Política para control de acceso.
- Política para uso controles criptográficos.

---

[5] https://img1.wsimg.com/
[6] https://www.iso27000.es/glosario.html
[7] https://www.iso27000.es/glosario.html
[8] https://www.iso27000.es/glosario.html

- Política para gestión de llaves.
- Política para seguridad física y del entorno.
- Política para escritorio y pantalla limpia.
- Política para transferencia de información.
- Política de uso de software.
- Política para relación con proveedores.
- Política para protección de datos personales.

El cumplimiento de las mencionadas políticas garantizará que:

a. Los deberes y las responsabilidades frente a la seguridad y privacidad de los datos e información serán definidos, establecidos, compartidos, publicados y aceptados por cada uno de los servidores públicos, contratistas, proveedores o partes interesadas que posean cualquier vínculo legal y/o contractual con la Registraduría Nacional del Estado Civil.

b. La Registraduría Nacional del Estado Civil protegerá y salvaguardará la información que genere, administre, procese, modifique, transmite y/o custodie, a través de los procesos para la prestación del servicio a la ciudadanía asociados con la identificación personal y procesos electorales, en el cumplimiento de las funciones de la Entidad, con el fin de minimizar impactos de marca, financieros, operativos y/o legales debido a un uso incorrecto de esta, por lo cual, se hace fundamental la aplicación de los controles diseñados y aplicados de acuerdo con la clasificación de la información, ya sea de su propiedad o que se encuentre en custodia de ésta.

c. La Registraduría Nacional del Estado Civil protegerá los datos e información de las amenazas originadas por parte del personal custodio, responsable o usuario de esta.

d. La Registraduría Nacional del Estado Civil protegerá las instalaciones donde se procesan los datos e información, la infraestructura tecnológica y las redes de datos que soporta los procesos críticos, misionales, de apoyo y de evaluación y control.

e. La Registraduría Nacional del Estado Civil definirá e implementará control de acceso tanto lógico como físico a los datos e información, sistemas, bases de datos, aplicaciones y recursos de red.

f. La Registraduría Nacional del Estado Civil definirá e implementará controles para garantizar que la seguridad sea parte integral del ciclo de vida de los sistemas de información y aplicaciones respectivas.

g. La Registraduría Nacional del Estado Civil definirá e implementará controles para garantizar adecuada gestión, tanto de las vulnerabilidades encontradas como de los eventos e incidentes de seguridad y las debilidades encontradas y asociadas con los sistemas de información, bases de datos y aplicaciones, para una mejora efectiva del Modelo de Seguridad y Privacidad de la Información – MSPI.

h. La Registraduría Nacional del Estado Civil definirá e implementará controles para garantizar la disponibilidad de los procesos en la prestación del servicio a la ciudadanía relacionados con la identificación y los procesos electorales, dando

cumplimiento a las funciones constitucional y legalmente asignadas a la Entidad y la continuidad de su operación basada en el impacto que pueden generar los eventos que se presenten con relación a la disponibilidad de los servicios mencionados.

i. La Registraduría Nacional del Estado Civil garantizará el cumplimiento por parte de los servidores públicos, contratistas, proveedores y terceros que interactúen con los sistemas de información y demás recursos informáticos en el marco de leyes, estatutos, regulaciones u obligaciones contractuales que se deriven del manual de políticas internas, los controles de seguridad de la información y la presente Resolución.

Artículo 8. Seguimiento de la Política de Seguridad de la Información. El seguimiento a la política es responsabilidad del Comité de Seguridad y Privacidad de la Información, así como lo es mantener el Modelo de Seguridad y Privacidad de la Información – MSPI actualizado mediante mecanismos de control y seguimiento de manera periódica o al menos una (1) vez por año, los cuales permitirán medir el nivel de cumplimiento en la implementación de las medidas de seguridad y los seguimientos acordes a las definiciones establecidas en el plan de trabajo del mencionado modelo y en el cual se identificarán las respectivas fases del ciclo P-H-V-A.

TÍTULO 2
Del Comité de Seguridad y Privacidad de la Información de la Registraduría Nacional del Estado Civil

Artículo 9: Comité de Seguridad y Privacidad de la Información. Crear el Comité de Seguridad y Privacidad de la Información de la Registraduría Nacional del Estado Civil, instancia en la cual se debatirán, analizarán y aprobarán los planes y proyectos que conlleven a la Entidad al cumplimiento legal y normativo relacionado con la protección de los datos e información y garantizar la confidencialidad, integridad y disponibilidad de éstos.

Artículo 10: Integrantes del Comité de Seguridad y Privacidad de la Información. Los integrantes del Comité de Seguridad y Privacidad de la Información serán:

1. El Secretario General,
2. El Registrador Delegado en lo Electoral,
3. El Registrador Delegado para el Registro Civil y la Identificación,
4. El Gerente de Informática,
5. El Jefe de la Oficina Jurídica,
6. El Jefe Oficina de Planeación

A las sesiones del Comité de Seguridad y Privacidad de la Información de la Registraduría Nacional del Estado Civil asistirán con voz pero sin voto: el Jefe de la Oficina de Control Interno y el Oficial de Gobierno y Cumplimiento del Modelo de Seguridad y Privacidad de la Información – MSPI.

Artículo 11. Funciones del Comité de Seguridad y Privacidad de la Información. El Comité de Seguridad y Privacidad de la Información tendrá las

siguientes funciones generales:

a. Liderar la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI al interior de la Registraduría Nacional del Estado Civil.

b. Aprobar las políticas de Seguridad y Privacidad de la Información

c. Realizar seguimiento al estado de la implementación y gestión del Modelo de Seguridad y Privacidad de la Información – MSPI en la Registraduría Nacional del Estado Civil.

d. Revisar y proponer mejoras para el cumplimiento tanto de la política de seguridad de la información, como de las políticas internas y controles que garanticen acciones preventivas y correctivas para la salvaguarda de los datos, información y activos de información de la Registraduría Nacional del Estado Civil.

e. Revisar los diagnósticos del estado de la seguridad de la información de la Registraduría Nacional del Estado Civil.

f. Realizar seguimiento a las acciones tomadas para implementar la cultura de cumplimiento de las políticas de seguridad y privacidad de la información.

Artículo 12. Sesiones del Comité de Seguridad y Privacidad de la Información. El Comité de Seguridad y Privacidad de la Información de la Registraduría Nacional del Estado Civil se reunirá ordinariamente 2 veces al año, 1 por cada semestre, y extraordinariamente cuando sea convocado por su presidente o por alguno de sus miembros.

Artículo 13. Presidente del Comité de Seguridad y Privacidad de la información. El Comité de Seguridad y Privacidad de la Información será presidido por el Secretario General de la Entidad.

Artículo 14. Presidencia del Comité de Seguridad y Privacidad de la información. El Presidente del Comité de Seguridad y Privacidad de la Información y cumplirá las siguientes funciones:

a. Citar a las reuniones del Comité de Seguridad y Privacidad de la Información con la respectiva agenda y temas a tratar tanto en las reuniones ordinarias como extraordinarias.

b. Fomentar y fortalecer la cultura del Modelo de Seguridad y Privacidad de la Información – MSPI en la Entidad.

c. Articular esfuerzos institucionales, recursos, metodologías y estrategias para asegurar la implementación, cumplimiento, sostenibilidad y mejora del Modelo de Seguridad y Privacidad de la Información en la Entidad.

Artículo 15. Secretario del Comité de Seguridad y Privacidad de la información. El Secretario del Comité de Seguridad y Privacidad de la Información será el Gerente de Informática o quien haga sus veces en la Gerencia de Informática

a cargo de temas de seguridad, ciberseguridad y privacidad informática de la Entidad.

Artículo 16. Secretaría del Comité de Seguridad y Privacidad de la información. La Secretaría del Comité de Seguridad y Privacidad de la Información y cumplirá las siguientes funciones:

a. Verificar la asistencia de los integrantes del Comité de Seguridad y Privacidad de la Información a las reuniones ordinarias y extraordinarias programadas.

b. Consignar en las respectivas actas los pronunciamientos y decisiones que emitan los miembros del Comité de Seguridad y Privacidad de la Información.

c. Realizar el seguimiento a los compromisos adquiridos en el marco del Comité de Seguridad y Privacidad de la Información.

d. Llevar el control, organización y respectivo archivo de las actas y documentos que emita el Comité de Seguridad y Privacidad de la Información

e. Las demás que le sean asignadas por el Comité de Seguridad y Privacidad de la Información y sean consignadas en el manual del comité de seguridad y privacidad de la información.

TÍTULO 3
Del Oficial de Seguridad y Privacidad de la Información de la Registraduría Nacional del Estado Civil

Es el encargado de implementar, mantener y administrar la seguridad de la información, así como de establecer los mecanismos de corto, mediano y largo, plazo que permita el desarrollo armónico de las políticas de seguridad de la información con la estrategia de la Registraduría Nacional del Estado Civil

Artículo 17: Funciones y Responsabilidades del Oficial de Seguridad y Privacidad de la Información

a. Establecer la alineación estratégica del modelo de con los planes, programas, proyectos y objetivos estratégicos de la Entidad.

b. Identificar el alcance, objetivos y estrategias del Modelo de Seguridad y Privacidad de la Información – MSPI (SGSI).

c. Proponer políticas y controles en lo relativo a la seguridad de la información.

d. Definir y Construir los Manuales, Modelos, Procedimientos, Instructivos y Formatos requeridos para implementar el Modelo de Seguridad y Privacidad de la Información – MSPI.

e. Asesorar el establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y mejoramiento continuo del SGSI

f. Apoyar y asesorar la implementación de los controles del SGSI, de acuerdo con las responsabilidades que para uno de ellos este definida.

g. Realizar socialización y capacitación a las dependencias de la Entidad para el conocimiento de las políticas de seguridad y privacidad de la información

h. Realizar reportes periódicos al comité de Seguridad y Privacidad de la Información de los avances en la implementación del SGSI de la Registraduría Nacional del Estado Civil.

i. Apoyar al equipo auditor en las auditorías internas y externas con el suministro de la información asociada al SGSI.

k. Apoyar en la definición de indicadores y riesgos asociados al SGSI

i. Promover el mejoramiento continuo del SGSI a través de la generación de los planes de mejoramiento y proyectos que se identifiquen a partir de las revisiones del comité y de las auditorías al Sistema de Gestión de Seguridad

l. Comprobar los requisitos de seguridad de la información con los proveedores y/ tercero que tengan relación con la RNEC, gestionando las acciones necesarias tanto interna como externamente.

m. Realizar seguimiento a la gestión de incidentes de seguridad de la información.

n. Implementar un programa de auditorías para la revisión de la seguridad de la información, revisando y comunicando oportunamente los resultados a las partes interesadas.

o. Asegurar la inclusión de la continuidad de seguridad de la información en el plan de continuidad del negocio.

TÍTULO 4
Otras disposiciones

Artículo 18: Incumplimiento a la Política de Seguridad de la Información. El incumplimiento tanto de la Política de Seguridad de la Información como de las políticas internas y controles de seguridad de la información se considerará como un incidente de seguridad y privacidad que, y de acuerdo con el caso, cuando sea un servidor público que incumpla, se compulsaran copias a los operadores disciplinarios para lo de su competencia, y en caso de contratistas o proveedores, aplicará lo establecido en las leyes relacionadas con la contratación estatal definidas en la legislación colombiana, sin perjuicio de las demás acciones administrativas, penales, fiscales y/o civiles que procedan contra las personas que incumplan estás disposiciones.

Parágrafo: Se deberá incorporar, como obligación en los contratos y convenios que suscriba la Registraduría Nacional del Estado Civil, el imperativo cumplimiento de la Política de Seguridad de la Información y las políticas internas y controles de seguridad de la información de los contratistas y terceros que tengan acceso a los datos e información que genere, almacene, administre y/o custodie la Entidad,

precisando expresamente que cualquier incumplimiento dará lugar a la terminación unilateral de la relación contractual, previo agotamiento del debido proceso, sin perjuicio del inicio de acciones judiciales a que haya lugar.

Artículo 19: Manuales, procedimientos y formatos de la Política de Seguridad de la Información de la Registraduría Nacional del Estado Civil. El oficial de Seguridad y Privacidad de la Información, con apoyo de la Oficina de Planeación, dentro de los dos meses siguientes a la expedición de este acto administrativo, expedirán y socializaran los manuales en donde se desarrollará la Política de Seguridad de la Información y sus once (11) políticas internas y controles de seguridad de la información que la componen; al igual que establecerá y/o actualizará los procedimientos y formatos necesarios para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI.

Artículo 20: Comunicaciones. Comunicar este acto administrativo a todos los servidores públicos de la Registraduría Nacional del Estado Civil y a los contratistas, proveedores y partes interesadas por intermedio de los supervisores de contratos y convenios en donde sea parte la Entidad.

Artículo 21. Publicación. Publicar este acto administrativo en el Diario Oficial y en la página web de la Registraduría Nacional del Estado Civil.

Artículo 22: Vigencia y derogatoria. El presente acto administrativo rige a partir de su publicación en la gaceta oficial y deroga las resoluciones número 13860 de 13 de diciembre de 2011, modificatorio Resoluciones No. 4154 del 19 de mayo de 2016, No. 4173 del 20 de mayo de 2016 y No. 27161 del 22 de noviembre de 2023.

NOTIFIQUESE, PUBLÍQUESE Y CÚMPLASE

Dada en Bogotá D.C., 11 ABR. 2024

HERNAN PENAGOS GIRALDO
Registrador Nacional del Estado Civil

Aprobó: Maria Eugenia Areiza Frieri – Secretaria General (EF)

Revisó: Hoslander Adlai Saenz Barrera - Registrador Delegado para el Registro Civil y la Identificación
Alejandro Alberto Campo Valero – Gerente de Informática.
Renato Contreras Ortega - Jefe Oficina Jurídica.

Proyectó: Eduardo Emilio Calderón Narváez – Coordinador Grupo de Administración e Infraestructura Tecnológica
Andrea Rosas Tobito - Coordinadora Grupo de Integración y Gestión – Gerencia de Informática.