Superintendencia de Notariado y Registro

MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código: SIG - SSI - PO - 04 - MN - 01	**Versión: 01**	**Fecha:29 de Octubre de 2024**

JOSÉ RICARDO ACEVEDO SOLARTE
JEFE OFICINA DE TECNOLOGIA DE LA INFORMACIÓN
JUAN CARLOS VALENZUELA BUITRAGO
PROFESIONAL OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN
HUGO ALEJANDRO CASALLAS LARROTTA
PROFESIONAL OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN
MAURICIO ALEJANDRO RODRÍGUEZ GONZÁLEZ
JEFE DE LA OFICINA ASESORA DE PLANEACIÓN
MÓNICA YANETH GALVIS GARCÍA
COORDINADORA GRUPO ARQUITECTURA ORGANIZACIONAL Y MEJORAMIENTO CONTINUO DE LA OFICINA ASESORA DE PLANEACIÓN

PROFESIONALES GRUPO ARQUITECTURA ORGANIZACIONAL Y MEJORAMIENTO CONTINUO DE LA OFICINA ASESORA DE PLANEACIÓN OFICINA ASESORA DE PLANEACIÓN

Octubre 2024

Libertad y Orden

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

TABLA DE CONTENIDO

1. INTRODUCCIÓN

La información es el recurso más valioso para las entidades, siendo esencial para el desempeño de sus funciones y la realización de sus procesos. Dada su importancia en la toma de decisiones, creación de políticas y prestación de servicios, entre otros usos, la información está expuesta a diversos riesgos, tanto internos como externos, que pueden provocar graves consecuencias negativas para la entidad si se materializan.

Poseer información conlleva responsabilidades, especialmente en la gestión adecuada de las amenazas potenciales. Esto implica protegerla mediante los principios fundamentales de confidencialidad, integridad y disponibilidad.

Por esta razón, la Superintendencia de Notariado y Registro ha reconocido la necesidad y la importancia de implementar un Sistema de Gestión de Seguridad de la Información (SGSI) para asegurar adecuadamente sus trámites, servicios, sistemas de información, plataforma tecnológica, infraestructura física y, en general, su información y como base fundamental, se establece el presente Manual de Políticas del Sistema de Gestión de Seguridad, que define lineamientos generales para la protección de la información en diversas áreas. Cabe señalar que este manual se enfoca en proporcionar directrices generales, las cuales serán desplegadas de forma detallada en los diferentes procedimientos, manuales, guías y documentos que componen el SGSI.

2. MARCO LEGAL

La política general de seguridad de la información se implementa y se basa.

- Resolución 1978 DE 2023 “por la cual se adopta la Versión 3 del Marco de Referencia de Arquitectura Empresarial para el Estado Colombiano como el instrumento para implementar el habilitador de arquitectura de la Política de Gobierno Digital y se dictan otras disposiciones” – Donde se establece la guía general MAE.G.AS - DOMINIO DE ARQUITECTURA DE SEGURIDAD.
- Resolución 500 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 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*”, donde se encuentra el

presente Plan Estratégico de Seguridad de la Información (PESI) como uno de los requisitos a desarrollar para cumplir con esta normativa.

- Decreto 767 de 2022 - Política de Gobierno Digital, "*Por el cual se establecen los lineamientos generales de la Política de Gobierno Digital*".
- Decreto 1499 de 2017, que establece el Modelo Integrado de Planeación y Gestión - MIPG, el cual surge de la integración de los Sistemas de Desarrollo Administrativo y de Gestión de la Calidad en un solo Sistema de Gestión, y de la articulación de este con el Sistema de Control Interno.
- Manual de Gobierno Digital – MINTIC.
- Modelo de Seguridad y Privacidad de la Información – MINTIC.

3. GLOSARIO DE TÉRMINOS

- **Activos de seguridad de la Información:** se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, documentos, soportes, edificios, personas, etc.) que tenga valor para la organización.
- **Amenazas:** Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización.
- **Confidencialidad:** Propiedad de la información que la hace no disponible o que no sea divulgada a individuos, entidades o procesos no autorizados.
- **Controles:** Medida que permite reducir o mitigar un riesgo.
- **Disponibilidad:** Propiedad de la información de ser accesible y utilizable a demanda por una parte interesada.
- **Incidentes de Seguridad:** Un evento o serie de eventos no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones del negocio y de amenazar la seguridad de la información
- **Integridad:** Propiedad de la información que busca preservar su exactitud y completitud.
- **Líderes de Proceso:** responsables de planear, dirigir, organizar, ejecutar, definir herramientas de seguimiento, medición, análisis y evaluar la operación y, además, quienes toman la decisión final en la gestión de los procesos.
- **Partes interesadas:** Persona u organización que puede afectar, verse afectada o percibirse como afectada por una decisión o actividad.
- **Política:** Intenciones y dirección de una organización, como las expresa formalmente su alta dirección (ISO 9001:2015).
- **Proveedor o Contratista:** Persona jurídica o natural con la que se celebra un contrato o convenio para la ejecución de obras, la prestación de servicios, la adquisición de bienes o la realización de cualquier otro tipo de actividad específica.

- **Riesgo:** Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias.
- **Sistema de Gestión de Seguridad de la Información:** Es el conjunto de manuales, procedimientos, controles y técnicas utilizadas para controlar y salvaguardar todos los activos que se manejan dentro de una entidad.
- **Streaming:** Distribución o descarga de datos desde un proveedor o servidor en internet mientras el usuario hace uso de los datos en cuanto estos son descargados, por ejemplo escuchar música directamente desde una página de internet o consumir una página de reproducción de videos.**Uso Aceptable:** Se refiere a los normas y lineamientos que describen cómo deben ser utilizados los activos de información de una organización.
- **Webproxy:** Página, software o servidor intermediario que se utiliza como túnel, permitiendo saltar reglas o políticas de navegación.

4. OBJETIVO DEL DOCUMENTO – MANUAL DE POLÍTICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Establecer lineamientos claros, detallados para cada dominio de seguridad, basado en el Modelo de Seguridad y Privacidad de la Información (MSPI) y la norma ISO/IEC 27001, en articulación con todos los procesos de la Entidad, con el fin de garantizar la confidencialidad, integridad y disponibilidad de la información y el buen uso de los activos de información propiedad de la Superintendencia de Notariado y Registro.

5. CAPÍTULO I – POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN

5.1. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) Y SU RELACIÓN CON EL SISTEMA INTEGRADO DE GESTIÓN (SIG)

El Sistema de Gestión de Seguridad de la Información (SGSI) forma parte del Sistema Integrado de Gestión (SIG), por lo tanto, el SGSI contribuye en el cumplimiento de los objetivos que el SIG establezca desde la perspectiva y alcance de la seguridad de la información. Los lineamientos establecidos en este documento profundizan y detallan todo lo relacionado con el SGSI.

5.2. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información define su declaración de política, en la Política Integral del Sistema Integrado de Gestión Para lo anterior, se podrá consultar el documento Política General del

Sistema Integrado de Gestión, en los aspectos que corresponde al aseguramiento de la confidencialidad, integridad y disponibilidad de los activos de seguridad de la información de la Entidad.

5.3. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La política del Sistema Integrado define en su contenido el objetivo general del sistema de Gestión de Seguridad de la Información *"Gestionar de manera eficiente la información de la Superintendencia de Notariado y Registro a través de la implementación de planes, procedimientos y protocolos que den cumplimiento a las condiciones de confidencialidad, integridad y disponibilidad en el óptimo desarrollo de los procesos de la Entidad."* Con lo anterior para el logro del mismo, se definen los siguientes objetivos específicos:

- Definir y apropiar los lineamientos para la protección de la información, de conformidad a estándares internaciones en seguridad de la información, normatividad vigente y contemplando las necesidades y expectativas de las partes interesadas identificadas para el SGSI.
- Gestionar los riesgos de seguridad de la información (Riesgos de seguridad digital) estableciendo planes de tratamiento orientados a las prevención y mitigación de los riesgos, hasta llevarlos a niveles aceptables por la alta dirección.
- Fortalecer la cultura de seguridad y privacidad de la información de los colaboradores y terceros que tienen una relación directa con la Superintendencia.
- Gestionar eficientemente los incidentes de seguridad de la información, para mitigar los posibles impactos a los procesos de la entidad.
- Realizar mejora continua del Sistema de Gestión de Seguridad de la Información, a través de la gestión de los riesgos, reporte de incidentes, eventos o debilidades y ejercicios de auditoría.

5.4. ALCANCE DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información (SGSI), también denominado Modelo de Seguridad y Privacidad de la Información por el MINTIC y conforme a las disposiciones normativas de la política de Gobierno Digital y su implementación, establece que el alcance del sistema y aplicación de sus controles tenga alcance para todos los procesos de la entidad y partes interesadas identificadas que puedan afectar o ser afectadas por el SGSI de la Entidad.

5.5. COMPROMISO DE LA ALTA DIRECCIÓN

La alta dirección establece los siguientes compromisos, con el fin de fijar el liderazgo y apoyo en la implementación, mantenimiento y logro de los objetivos del Sistema de Gestión de Seguridad de la Información:

- Establecer y fomentar la adopción de la política general, los objetivos y las políticas específicas de seguridad y privacidad de la información.
- Impulsar la adopción y cumplimiento de los requisitos y políticas del sistema de Gestión de Seguridad de la Información en los procesos de la entidad.
- Proveer los recursos necesarios (presupuesto, personal, recursos tecnológicos) para la implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información.
- Incluir y tener en cuenta dentro de la planeación estratégica los aspectos asociados a seguridad de la información.
- Realizar revisiones del estado del Sistema de Gestión de Seguridad de la Información mínimo una vez al año.
- Apoyar en la toma de decisión y ejecución de planes de acción frentes a eventos críticos que puedan afectar la operación de la entidad.

5.6. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (ROLES Y RESPONSABILIDADES)

La Superintendencia, dentro de su organización establece dos niveles principales en la toma de decisiones de alto nivel, dentro estos dos niveles se encuentra la Alta Dirección y el Comité Institucional de Gestión y Desempeño. Así mismo, se establecen los roles y responsabilidades de cada uno de los actores y áreas involucrados que hacen parte y contribuyen en la construcción y mantenimiento del Sistema de Gestión de Seguridad de la Información.

Tabla 1. Roles y responsabilidades del SGSI

ROL / RESPONSABLE	RESPONSABILIDADES
Alta Dirección	• Garantizar la adopción y cumplimiento de las políticas de seguridad de la información, para que los colaboradores a su cargo conozcan y apliquen las políticas de seguridad de la información. • Proveer los recursos necesarios (presupuesto, personal, recursos tecnológicos) para la adopción y mantenimiento del Sistema de Gestión de Seguridad de la Información. • Incluir y tener en cuenta dentro de la planeación estratégica y decisiones que toma la entidad los aspectos asociados a seguridad de la información.

ROL / RESPONSABLE	RESPONSABILIDADES
	• Liderar y direccionar los planes estratégicos de seguridad de la información propuestos por el Oficial de Seguridad de la Información. • Aprobar o denegar las solicitudes para excepciones al cumplimiento de las políticas de seguridad de la información. • Apoyar en la toma de decisión y ejecución de planes de acción frente a eventos críticos que puedan afectar la operación de la entidad.
Comité Institucional de Gestión y Desempeño	• Revisar y aprobar la política general de seguridad de la información y los objetivos de seguridad de la información. • Aprobar los recursos correspondientes para la implementación y el mantenimiento del Sistema de gestión de seguridad de la información. • Aprobar lineamientos o políticas de seguridad de la información. • Realizar revisión del estado de los riesgos de seguridad digital a nivel gerencial y aprobar las decisiones para su tratamiento o aceptación. • Apoyar en la toma de decisión y ejecución de planes de acción frente a eventos críticos que puedan afectar la operación de la entidad. • Revisar y aprobar los cambios y estructura de roles definido para el Sistema de Gestión de Seguridad de la Información. • Revisar y aprobar los cambios de infraestructura críticos para la entidad, conforme a lo dispuesto en el control de cambios de TI. • Aprobar o denegar las solicitudes para excepciones al cumplimiento de las políticas de seguridad de la información. • Realizar la verificación y aprobación de políticas que tengan afectación significativa para la entidad como para el Sistema de Gestión de seguridad de la información. • Validar el cumplimiento de las políticas y procedimientos de seguridad de la información.
Comité Institucional de Coordinación de Control Interno	• Aprobar el Plan Anual de Auditoría de la Superintendencia de Notariado y Registro presentado por el Jefe de Control Interno, donde se incluyan las auditorías programadas por la 2da. Línea de defensa, en relación con la seguridad y privacidad de la información; hacer sugerencias y seguimiento a las recomendaciones producto de la ejecución del plan, de acuerdo con lo

ROL / RESPONSABLE	RESPONSABILIDADES
	dispuesto en el estatuto de auditoría, basado en la priorización de los temas críticos y según la gestión de riesgos de la administración.
Oficial de Seguridad de la Información	• Formular, documentar y gestionar el Plan Estratégico de Seguridad de la Información (PESI) y proponer planes de trabajo que permitan gestionar la seguridad de la información en el marco del cumplimiento de la política y los lineamientos definidos y aprobados por la entidad. • Identificar oportunidades para mejorar las políticas y los lineamientos de seguridad de la información en función de las necesidades de la entidad y de los riesgos identificados. • Participar en las reuniones de los equipos de mejoramiento de los procesos, evidenciando los riesgos, controles y planes de mitigación que deben establecerse para la mitigación de los riesgos de seguridad de la información. • Proponer los objetivos de seguridad de la información, las métricas asociadas y las estrategias para conseguir el cumplimiento de estos. • Asesorar a los procesos en las actividades de identificación de activos y riesgos de seguridad de la información. • Verificar que los controles y planes de seguridad hayan sido implementados adecuadamente, realizando las actividades de seguimiento correspondientes. • Consolidar y entregar la información necesaria para la revisión por la alta dirección. • Asesorar a la alta dirección en aspectos de seguridad de la información. • Apoyar en la definición y mejora de los procedimientos de seguridad de la información.
Jefe de Tecnologías de la Información	• Realizar la aprobación respecto a los cambios de infraestructura propuestos. • Informar a la alta dirección sobre el avance, necesidades o aspectos que puedan ser relevantes del Sistema de Gestión de Seguridad de la Información, con apoyo del Oficial de Seguridad de la Información.

ROL / RESPONSABLE	RESPONSABILIDADES
	• Socializar los incidentes de seguridad de la información de alto impacto a la alta dirección. • Definir y asignar roles de seguridad de la información dentro de la Oficina de Tecnologías de la Información de acuerdo con las actividades correspondientes. • Dirigir la implementación de los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Validar solicitudes para excepciones al cumplimiento de las políticas de seguridad de la información e informar a la alta dirección sobre las mismas.
Oficina de Tecnologías de la información	• Implementar los controles de tipo tecnológico que ayuden a mitigar los riesgos de seguridad de la información. • Desarrollar los procedimientos e instructivos necesarios para la correcta operación y administración de la seguridad informática de la entidad, debidamente verificados junto al Oficial de Seguridad de la Información y la Oficina de Planeación. • Evaluar y seleccionar herramientas tecnológicas que faciliten y aumenten la protección de los activos de la entidad. • Apoyar con la apropiación, divulgación y socialización de las Políticas a todo el personal y los cambios que en ellas se produzcan a través de los diferentes medios de comunicación. • Apropiar, cumplir y realizar mejora continua a los procedimientos establecidos en el Sistema de Gestión de Seguridad de la Información, de acuerdo con los roles de seguridad de la información establecidos para el personal de la Oficina de Tecnología de la Información.
Oficina Asesora de Planeación	• Establecer, mantener e implementar la política de protección de datos personales de la Superintendencia de Notariado y Registro. • Apoyar en el establecimiento y mantenimiento de la metodología integral de riesgos donde se incluya los riesgos de seguridad digital (Seguridad de la información). • Apoyar en el establecimiento y mantenimiento de las cláusulas de cumplimiento transversal de los sistemas de gestión, incluyendo el Sistema de Gestión de Seguridad de la Información.

ROL / RESPONSABLE	RESPONSABILIDADES
Oficina de Control Interno	• Consolidar el Plan Anual de Auditorías Interna PAAI para cada vigencia, donde se evidencie entre otros, la programación realizada por la 2da. Línea de Defensa para las auditorías de seguridad y privacidad de la información, este plan debe estar aprobado por el Comité Institucional de Coordinación de Control Interno. • Apoyar en el seguimiento a la gestión de riesgo de seguridad de la información y los planes de mejoramiento derivados de estos análisis, conforme a su rol de tercera línea de defensa.
Dirección de Contratos	• Incluir dentro de los contratos o convenios con contratistas o terceras partes las obligaciones correspondientes con el cumplimiento de las políticas de seguridad de la información definidas por la entidad. • Exigir el diligenciamiento de los contratistas del formato de Conocimiento de Políticas de Seguridad de la Información de la SUPERINTENDENCIA. • Apoyar con la aplicación y cumplimiento de la Política de Seguridad de la Información para la relación con los proveedores. • Reportar a la Oficina de Tecnologías de la Información de forma inmediata, cancelaciones de contrato, terminaciones, cesiones o suspensiones, para realizar las gestiones en los sistemas de información de manera oportuna, evitando posibles incidentes de seguridad.
Dirección Administrativa y Financiera	• Establecer políticas y procedimientos para proteger los activos físicos de la organización, como instalaciones, equipos y documentos. • Gestionar y controlar el acceso a las instalaciones de la Superintendencia mediante diversos sistemas de control de acceso, como tarjetas de identificación, cerraduras electrónicas, controles biométricos, cámaras de seguridad entre otros. • Establecer las medidas para la protección de las áreas seguras de la Superintendencia.

ROL / RESPONSABLE	RESPONSABILIDADES
Dirección de Talento Humano	• Asegurar que los empleados durante el proceso de selección comprendan sus responsabilidades, los términos y las condiciones de contratación y que son idóneos en los roles para los que se contratan. • Asegurar que los empleados tomen conciencia de sus responsabilidades en seguridad de la información y las cumplan, además de dar aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos. • Contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información. • Capacitar continuamente en materia de seguridad de la información de acuerdo con los planes estipulados y coordinados previamente con el Oficial de Seguridad de la Información. • Incorporar dentro de sus procedimientos la firma de un acuerdo de confidencialidad definido por el Oficial de Seguridad de la Información, la Oficina de Jurídica y aprobado por la Oficina de Tecnología de la Información. • Verificar los antecedentes y experiencia de los candidatos durante los procesos de vinculación con la entidad. • Reportar a la Oficina de Tecnologías de la Información de forma inmediata, sobre desvinculaciones, traslados o vacaciones del personal, para realizar las gestiones en los sistemas de información de manera oportuna, para mitigar el riesgo de posibles incidentes de seguridad.
Oficina Jurídica	• Apoyar con la verificación de la normatividad que la entidad debe cumplir respecto a la seguridad de la información y la protección de datos personales. • Apoyar desde el punto de vista jurídico en la revisión de los acuerdos de confidencialidad o los instrumentos que generen los procesos, que tengan por objetivo proteger la SUPERINTENDENCIA en temas de privacidad y seguridad de la información.

ROL / RESPONSABLE	RESPONSABILIDADES
Líderes de Proceso	• Implementar y cumplir las políticas y procedimientos de seguridad de la información que se definan como parte del Sistema de Gestión de Seguridad de la Información. • Apoyar a la entidad en los planes de mejoramiento para dar cumplimiento a los planes de acción, en materia de seguridad y privacidad de la información • Asegurar que los funcionarios bajo su cargo conozcan, entiendan y apliquen las políticas y lineamientos definidos para la seguridad de la información. • Al ser ellos los propietarios de los activos en su proceso, deben velar por que existan las medidas de protección necesarias para preservar su seguridad. • Realizar la identificación y valoración de los activos de seguridad de la información y riesgos de seguridad digital que están a cargo del proceso. Así como, formular y hacer seguimiento al tratamiento de los riesgos.
Todos los funcionarios y contratistas.	• Conocer y cumplir a cabalidad con las políticas y procedimientos de seguridad de la información definidos y aprobados. • Reportar todos los eventos, incidentes o debilidades que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información de los procesos. • Apoyar a los líderes de proceso en el desarrollo de tareas como gestión de activos y gestión de riesgos de seguridad de la información. • Usar los activos de información de la entidad de forma responsable y únicamente para los propósitos autorizados, protegiendo la respectiva confidencialidad de estos.
Proveedores	• Reportar todos los eventos, incidentes o debilidades que puedan afectar la confidencialidad, integridad o disponibilidad de los activos de información de la Superintendencia. • Conocer las políticas de seguridad de la información, y firmar los formatos de inducción del Subsistema de Gestión de Seguridad de la Información previo al inicio de la ejecución de las obligaciones para lo cual fue contratado. • Aplicar las políticas de Seguridad de la Información de la Superintendencia, mientras se encuentre en las instalaciones de la Superintendencia o ejecutando las obligaciones establecidas para lo cual fue contratado.

ROL / RESPONSABLE	RESPONSABILIDADES
	• Cumplir con todos los lineamientos de seguridad establecidos para la relación con los proveedores.

6. CAPÍTULO II – POLÍTICAS ESPECÍFICAS DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

6.1. SEGURIDAD DE LOS RECURSOS HUMANOS

La superintendencia debe garantizar a través de su área de talento humano que durante el proceso de vinculación y desvinculación de sus empleados, cualquier funcionario, gerente o cualquier persona aplique medidas de seguridad de la información tales como, y sin limitarse a: verificaciones e investigaciones sobre referencias personales, laborales, experiencia laboral, pruebas complementarias, estudio de seguridad, examen de aptitud y conocimientos, de tal manera que apoyen las políticas de seguridad y en cumplimiento de las regulaciones locales.

6.2. GESTIÓN DE ACTIVOS

Se debe identificar la información y los recursos de valor asociados a la información que la Organización utilice para el desarrollo de sus objetivos misionales; la información y demás recursos asociados deben tener asignado un responsable, quien debe tomar las decisiones que son pertinentes para su protección, de acuerdo con los requerimientos internos y regulaciones aplicables a la entidad.

6.3. CONTROL DE ACCESO

Para la protección de los activos de seguridad de la información, la entidad establece lineamientos, procedimientos y controles de acceso a la red y sistemas de información con el fin de mitigar riesgos asociados al acceso no autorizado tanto a la información como a la infraestructura tecnológica.

6.4. CRIPTOGRAFÍA

La Superintendencia dispondrá de lineamientos, herramientas y controles para garantizar la confidencialidad, autenticidad e integridad de la información, aplicando controles criptográficos a los activos que, por su

exposición, así lo requieran. Así mismo, realizara seguimiento y gestión de los controles criptográficos implementados.

Los procesos de la entidad serán responsables de identificar los activos que, por su contexto y exposición a diversas amenazas, requerirán la aplicación o implementación de cifrado y los mismos deberán ser comunicados a la Oficina de Tecnologías de la Información, para de conformidad a las herramientas con las que se cuentan en la Entidad, se implementen los controles necesarios, o se establezcan posibles tratamientos para mitigación de los riesgos.

6.5. SEGURIDAD FÍSICA Y DEL ENTORNO

La Superintendencia adopta lineamientos para el control de acceso y la protección del perímetro de seguridad de sus instalaciones físicas. Así mismo establece los criterios para la identificación y definición de los controles para la protección de las áreas seguras, con el fin de mitigar los riesgos y amenazas externas y evitar afectación a la confidencialidad, disponibilidad e integridad de la información de la Entidad.

Todos los colaboradores y personal externo que ingresen a las instalaciones de la Superintendencia deben cumplir con los lineamientos establecidos para el control de acceso físico.

6.6. SEGURIDAD DE LAS OPERACIONES

La Superintendencia, con el fin de asegurar la operación de los recursos tecnológicos, planea, gestiona, mantiene, controla, respalda, protege y monitorea la infraestructura tecnológica de la Entidad, por medio de los diversos lineamientos y políticas establecidos en los procedimientos del Sistema de Gestión de Seguridad de la Información.

6.7. SEGURIDAD DE LAS COMUNICACIONES

La Oficina de Tecnologías de la información establece controles para acceso lógico y de seguridad perimetral lógica para acceso y protección de las redes de la Superintendencia.

6.8. SEGURIDAD EN LA NUBE

La Oficina de Tecnologías de la información establece los controles necesarios tanto para el despliegue de la infraestructura tecnológica en la nube como para la protección de esta. Ninguna otra área está autorizada para gestionar recursos en la nube.

6.9. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

Toda actividad de adquisición, implementación o mantenimiento de software que requiera desarrollo, debe ser gestionada y autorizada formalmente con la Oficina de Tecnologías de la Información. Así mismo, se definen lineamientos específicos para la adquisición, desarrollo, despliegue y mantenimiento seguro de los sistemas de información.

6.10. CONCIENTIZACIÓN Y COMUNICACIÓN EN SEGURIDAD DE LA INFORMACIÓN

La Superintendencia debe contar con un programa o plan de cultura permanente en Seguridad de la Información y/o ciberseguridad que deberá ser actualizado mínimo una vez al año con el fin de mantener a todo su personal informado acerca de las políticas, las responsabilidades de seguridad de la información y las continuas amenazas que ponen en riesgo la información que administra y/o procesa.

6.11. SEGURIDAD EN LAS RELACIONES CON LOS PROVEEDORES

La superintendencia deberá contar con lineamientos de seguridad de la información para el aseguramiento de la cadena de suministro, Los responsables de los contratos y de la contratación, deben garantizar que las responsabilidades de seguridad de la información de los terceros que tengan acceso procesen, almacenen o distribuyan información de valor para la Superintendencia, se encuentren documentadas en los contratos u otros acuerdos de prestación de servicios y deben supervisar su cumplimiento durante toda la vigencia de la relación contractual.

6.12. GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

La Superintendencia gestiona los incidentes de seguridad de la información utilizando procedimientos establecidos y personal capacitado para proteger la confidencialidad, integridad y disponibilidad de los activos de información. Todo el personal de la Superintendencia, incluyendo contratistas y terceros, debe reportar de inmediato cualquier evento adverso, sospechoso o que pueda comprometer la seguridad de los activos de información a través de los canales establecidos. La Oficina de Tecnologías de la Información será responsable de la evaluación, respuesta y documentación de todos los incidentes reportados, asegurando la implementación de medidas correctivas y preventivas para minimizar futuros riesgos. Así mismo, se realizará el reporte de los incidentes de seguridad a los entes externos correspondientes cuando aplique.

6.13. GESTIÓN DE LA CONTINUIDAD TECNOLÓGICA

La Superintendencia a través de la Oficina de Tecnologías de la Información define un plan de continuidad tecnológica, en el cual se establezcan las estrategias para la restauración de los sistemas de información más críticos de la entidad, incorporando los controles de seguridad necesarios.

6.14. CUMPLIMIENTO

La Superintendencia vela por el cumplimiento de la legislación vigente aplicable en los requisitos establecidos para la seguridad de la información de acuerdo con lo establecido por el gobierno nacional, entre ellos los derechos de propiedad intelectual, protección de datos personales, transparencia y del derecho de acceso a la información pública, para lo anterior se define la matriz de requisitos legales que será encabezada por la Oficina Asesora Jurídica.

7. CAPÍTULO III - POLÍTICAS DE SEGURIDAD PARA EL BUEN USO DE LOS ACTIVOS DE INFORMACIÓN

La Superintendencia define los siguientes lineamientos para el buen uso de sistemas de información, los cuales van orientados a los funcionarios y contratistas de la entidad que accedan, utilicen, procesen o almacenen activos de información.

Todos los usuarios que tengan acceso a los activos de información de la Superintendencia deberán seguir las políticas establecidas para el uso aceptable de estos. Además, serán responsables del uso de dichos activos que por sus funciones y/u obligaciones contractuales tienen acceso.

7.1. PROPIEDAD DE LOS ACTIVOS

a. La información, los sistemas y aplicaciones, los servicios y los equipos (Desktops, laptops, impresoras, redes, internet, dispositivos móviles, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y faxes, entre otros), son activos de información propiedad de la Superintendencia de Notariado y Registro, que se proporcionan a los funcionarios, contratistas y/o terceros autorizados, para cumplir con actividades específicas de la entidad.
b. La Superintendencia se reserva el derecho de monitorear y supervisar su información, sistemas, servicios y equipos, en el marco de las investigaciones, eventos y/o incidentes de seguridad que así lo requieran.
c. El personal de la Superintendencia de Notariado y Registro al hacer uso de los recursos (incluyendo recursos TIC como correos electrónicos, usuarios en aplicaciones, cuentas de productividad y colaboración entre otros) proporcionados por la entidad, no podrá argumentar derechos de privacidad o propiedad sobre la información almacenada en estos, siendo esta siempre propiedad de la Superintendencia.
d. Todo activo de información que repose en los recursos de TIC asignados al personal de la Superintendencia es de propiedad de la entidad. Por tal razón, la Oficina de Tecnologías de la Información podrá acceder en cualquier momento que se requiera a dichos activos para auditoría, revisión o búsqueda de la información, previa autorización de la Alta Dirección cuando sea necesario.

7.2. USUARIOS Y CONTRASEÑAS:

La Oficina de Tecnologías de la Información asigna usuarios y contraseñas a todos los funcionarios o contratistas según sus roles y responsabilidades en los diferentes servicios tecnológicos. Por lo tanto, se establecen los siguientes lineamientos en cuando a su uso adecuado:

a. Las credenciales son personales e intransferibles, por lo tanto, no deben compartirse con otros funcionarios o contratistas.
b. Todos los funcionarios y contratistas son responsables de las acciones ejecutadas con sus usuarios en los sistemas de información de la Superintendencia.
c. Las actividades ejecutadas por los usuarios en los sistemas de información o aplicaciones quedan almacenadas para efectos de auditoría, es decir, que podrán ser revisadas por parte de la Oficina de Tecnologías de la Información en caso de ser necesario.
d. La creación y modificación de usuarios y contraseñas en la infraestructura tecnológica son responsabilidad de la persona designada por la Oficina de Tecnologías de la Información y debe seguir los procedimientos correspondientes.
e. Las contraseñas o credenciales de acceso no deben escribirse en memos o notas que puedan encontrarse a la vista de los demás usuarios.
f. La longitud mínima de las contraseñas será igual o superior a ocho caracteres y estarán constituidas por combinación de caracteres alfabéticos, numéricos y especiales.
g. Se debe cambiar la contraseña de acceso cada 120 días, o cuando considere que ha perdido la confidencialidad y se pueda comprometer la información.
h. Los funcionarios y/o contratistas y demás, no deben utilizar ninguna información personal (por ejemplo, el número de la cédula) o familiar (por ejemplo, nombres de familiares) o secuencias genéricas (por ejemplo 1234 o abcdef), para crear sus contraseñas, ya que pueden ser fácilmente deducibles.
i. Está prohibido facilitar o proporcionar acceso a las aplicaciones e información a usuarios o a terceros no autorizados.

7.3. USO ADECUADO DE LA INFORMACIÓN:

La Información es un elemento fundamental para el cumplimiento de los objetivos de la Superintendencia, de tal forma que puede ser entendida, compartida, protegida y utilizada cumpliendo con las siguientes políticas:

a. El personal de la Superintendencia deberá leer y conocer el índice de información clasificada y reservada y seguir los lineamientos que se dicten para su adecuado manejo.

b. Los activos de información almacenados en los recursos TIC o que se encuentren en medios físicos (Documentos) asignados al personal de la Superintendencia deberán ser tratados como información clasificada (a menos que el índice de información clasificada y reservada definan lo contrario) y usada solo para los fines que fue creada u obtenida.
c. Los activos de información clasificados como información reservada o clasificada no podrán ser enviados por correo electrónico ni guardados en dispositivos móviles (memorias USB, CD, DVD), a menos que se encuentren cifrados y protegidos por un factor de autenticación fuerte. En ninguno de los dos casos se podrá compartir la información para descifrar estos activos por el mismo medio en que fueren entregados.
d. Todo el personal de la Superintendencia deberá suscribir un acuerdo de confidencialidad donde se adquiera el compromiso respecto al cuidado de la información que cada uno tendrá bajo su responsabilidad.
e. La Oficina de Tecnologías de la Información definirá las políticas para ejecución de copia de respaldo de información en los equipos de cómputo. Los funcionarios y contratistas serán responsables de alojar la información en el repositorio correspondiente según las políticas definidas.
f. Todo activo de información que sufra daño, pérdida, contaminación por malware o ciberataque deberá ser reportado a la Oficina de Tecnologías de la Información como un incidente de seguridad de la información.

7.4. USO DE INTERNET:

El Internet es un recurso que la Superintendencia provee a sus funcionarios y contratistas para apoyar el desarrollo de sus funciones, por tal motivo, se definen las siguientes medidas para un uso y aprovechamiento adecuado:

a. La Oficina de Tecnologías de la Información implementará políticas de navegación basadas en categorías y niveles de usuario, con el objetivo de proteger la entidad de riesgos como infecciones por malware, fuga de información o navegación de contenido inapropiado.
b. La Oficina de Tecnologías de la Información, realiza monitoreo permanente de tiempos de navegación y páginas visitadas por parte de los funcionarios y/o terceros. Así mismo, se puede inspeccionar, registrar e informar las actividades realizadas durante la navegación.
c. Cada uno de los usuarios es responsable de dar uso adecuado a este recurso y en ningún momento puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros, la legislación vigente, las políticas de seguridad de la información, entre otros.
d. Para los dispositivos tecnológicos que no sean propiedad de la Superintendencia, se brindará acceso a internet a través de la red de invitados debidamente aislada de la red productiva de la entidad.

RESTRICCIONES GENERALES:

e. Las siguientes categorías se encontrarán restringidas salvo excepciones específicas de las áreas que requieren alguna categoría en particular para el desempeño de sus actividades:

CATEGORÍAS RESTRINGIDAS	
Pornografía	Redes Sociales y Mensajería
Drogas	Transmisión de Video (Excepto Youtube)
Terrorismo	DropBox/BOX/Wetransfer y/o Similares
Segregación Racial / Odio	Proxies/WebProxies
Hacking / Malware	Descarga de Software / Juegos / Juegos en línea
Descarga de Películas / Torrents	Deep Web / Dark Web

f. El uso de internet no considerado dentro de las restricciones anteriores es permitido siempre y cuando se realice de manera ética, razonable, responsable, no abusiva y sin afectar la productividad, ni la protección de la información de la Superintendencia.

7.5. CORREO ELECTRÓNICO:

La Oficina de Tecnologías de la Información que presta servicios a los procesos de la Superintendencia, asigna una cuenta de correo electrónico con dominio (*@supernotariado.gov.co*) a cada uno de los empleados, contratistas y/o terceros que lo requieren para el desempeño de sus funciones.

El uso de este recurso está sujeto a los siguientes lineamientos:

a. El único servicio de correo autorizado para el manejo o transmisión de la información institucional es el proporcionado por la Oficina de Tecnologías de la Información.
b. La cuenta de correo electrónico debe ser usada únicamente para el desempeño de las funciones y/u obligaciones asignadas dentro de la Superintendencia.
c. Los mensajes y la información contenida en los buzones de correo son de propiedad de la Superintendencia. Cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

d. Todo mensaje tipo SPAM o malicioso deberá reportarse a la Oficina de Tecnologías de la Información a través de los canales correspondientes. Está expresamente prohibido el reenvío de mensajes sospechosos a otros buzones, ya que se entenderá como propagación intencional de malware.
e. Todo mensaje de índole personal debe ser eliminado del buzón institucional.
f. El tamaño de los buzones de correo, de los mensajes enviados y recibidos, está determinado por la Oficina de Tecnologías de la Información, teniendo en cuenta las buenas prácticas de seguridad vigentes.
g. No debe registrarse la cuenta de correo institucional en servicios gratuitos en línea o de comercio electrónico.
h. El envío de correos masivos estará limitado solo para buzones específicos que así lo requieran.
i. No deben remitirse mensajes que contengan adjuntos archivos ejecutables y/o con extensiones (.mp3, wav, .exe, .com, .dll, .bat. entre otros).
j. No se debe distribuir, copiar o reenviar información de la Superintendencia a través de correos personales o sitios web diferentes a los autorizados en el marco de sus funciones u obligaciones contractuales.

7.6. RECURSOS TECNOLÓGICOS:

a. Solo se permite el uso de software autorizado por la Oficina de Tecnologías de la Información de la Superintendencia, sea software licenciado, abierto o gratuito.
b. La instalación y/o modificación de cualquier tipo de software y/o hardware en los equipos de cómputo de la Superintendencia es responsabilidad de la Oficina de Tecnologías de la Información y por tanto son los únicos autorizados para realizar o autorizar esta labor.
c. La asignación, retiro y/o reasignación de recursos de TIC deberá ser solicitada por medio de la mesa de ayuda conforme al procedimiento definido por la Oficina de Tecnologías de la Información.
d. La Oficina de Tecnologías de la Información será la única encargada del despliegue, mantenimiento y/o soporte de aplicaciones y/o servicios tecnológicos en la Superintendencia.
e. Los equipos de cómputo de la Superintendencia se deben emplear exclusivamente para las actividades misionales y el desarrollo de las funciones de cada funcionario o contratista que le sea asignado. Así mismo, el funcionario o contratista que tenga un equipo de cómputo asignado será el responsable del buen uso de este bien, lo que incluye no emplearlo para fines personales o en beneficio de terceros.
f. En caso de daño, perdida o mal uso de los recursos tecnológicos asignados, debe reportarse inmediatamente a la Oficina de Tecnologías de la Información para realizar las gestiones correspondientes.
g. Los usuarios no deben realizar cambios de hardware y/o de software, repotenciación, traslados de equipos, cambios de papel tapiz, protectores de pantalla, fechas y hora del sistema en los equipos de

cómputo, cualquier soporte deberá solicitarse a la mesa de ayuda de la Oficina de Tecnologías de la Información.

h. La Oficina de Tecnologías de la Información realizará el control y verificación de cumplimiento del licenciamiento del respectivo software y aplicaciones asociadas.
i. Actividades como escaneo o escucha en la red, ataques de autenticación y demás actividades relacionadas con Hacking solo podrán ser ejecutadas por la Oficina de Tecnologías de la Información o personal autorizado por esta.

7.7. DISPOSITIVOS EXTRAÍBLES:

a. Las unidades de CD, DVD, USB o unidades extraíbles estarán deshabilitadas en las estaciones de trabajo, no está permitido el uso de medios removibles en equipos que estén conectados a la red corporativa de la Superintendencia. Solamente el personal autorizado expresamente por la Alta Dirección tendrá unidades extraíbles habilitadas, con previo análisis del Oficial de Seguridad de la Información.
b. Las unidades USB de los equipos de cómputo únicamente podrán recibir dispositivos periféricos autorizados por la entidad (Tokens, Mouse, Diademas y Teclado).

7.8. ESCRITORIO LIMPIO:

a. Cada vez que los funcionarios se retiren del puesto de trabajo deben bloquear los equipos de cómputo.
b. Las estaciones de trabajo serán apagadas al final de la jornada, salvo excepciones particulares que lo requieran.
c. Los puestos de trabajo deben mantenerse limpios y sin información sensible a la vista, salvo cuando se esté utilizando. Al ausentarse, los usuarios deben guardar dicha información de forma segura en los cajones disponibles para evitar robos o pérdidas.
d. Los computadores portátiles deben bloquearse con un cable de seguridad o deben almacenarse dentro de los cajones del escritorio.

7.9. PANTALLA LIMPIA:

a. La información no debe dejarse en el “escritorio” del computador. Este espacio estará restringido por políticas de sistema. En su lugar la información debe guardarse en carpetas específicas en otras ubicaciones como “Mis Documentos”.
b. Está prohibido ubicar memos, post-it o similares que contengan información de acceso a los sistemas y/o información sensible de cualquier tipo sobre el puesto de trabajo o las pantallas de los equipos.

7.10. GESTIÓN DE PROYECTOS CON COMPONENTES TIC:

Todos los proyectos de la Entidad que involucren componentes de tecnologías de la información y comunicaciones (software, hardware y/o sistemas de información) deberán ser informados y socializados a la Oficina de Tecnologías de la Información a través de la mesa de ayuda, donde se evaluará el nivel de acompañamiento, liderazgo, apoyo y/o intervención requerida por parte de la oficina, así como los recursos disponibles para las actividades requeridas.

a. Los proyectos o iniciativas que no sean informados a la Oficina de Tecnologías de la Información no podrán ser implementados en la Entidad ni usar recursos TIC disponibles.
b. En caso de que suceda lo anterior, se informará a la Alta Dirección quien tomará las decisiones respectivas de implementación, las cuales en cualquier caso deberán cumplir con los lineamientos, lineamientos, tecnologías y otros recursos definidos por la Oficina de Tecnologías de la Información.
c. El área responsable del proyecto o iniciativa no informado deberá asumir los riesgos y los gastos que se puedan derivar de esta decisión.
d. Si se desea entregar un servicio a la Oficina de Tecnologías de la Información, deberá surtirse un proceso de alineación y entrega de recursos adicionales para su mantenimiento y soporte. Hasta tanto esta alineación no esté dada, el jefe de la Oficina de Tecnologías de la Información podrá posponer la recepción de este si las condiciones no se cumplen.

7.11. REPORTE DE INCIDENTES O INCUMPLIMIENTOS A LOS LINEAMIENTOS

Cualquier colaborador o tercero de la Superintendencia deberá reportar los incidentes o incumplimientos a los lineamientos que identifique.

Los reportes recibidos por parte de la Oficina de Tecnologías de la Información serán tratados como confidenciales y con absoluta reserva, cualquier falla en esta confidencialidad podrá ser sancionada.

8. SANCIONES

La falta de conocimiento de los presentes lineamientos no libera al personal de la Superintendencia de las responsabilidades establecidas en ellos por el mal uso que hagan de los recursos TIC, por lo tanto, las sanciones podrán ser las siguientes:

a. Sanciones de acuerdo con el Código Único Disciplinario o sanciones penales según la gravedad.
b. Ejecución de incumplimiento de contrato según aplique.

La Oficina de Tecnologías de la Información apoyará a la Oficina de Control Disciplinario Interno en recopilar las evidencias de incumplimiento de los lineamientos, informes de impactos y consecuencias y cualquier otro insumo requerido para la determinación de la sanción, así mismo será el encargado de gestionar el Incidente de seguridad correspondiente.

9. REVISIÓN Y ACTUALIZACIÓN DEL MANUAL

La revisión y actualización (cuando aplique) del manual deberá ser realizada anualmente por el Oficial de Seguridad de la Información en coordinación con el Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones, para posteriormente ser llevada al Comité Institucional de Gestión y Desempeño.

9.1. CONTROL DEL MANUAL

Este manual es desarrollado y actualizado por el Oficial de Seguridad de la Información, revisado por la Oficina de Tecnologías de la Información y es aprobado por el Comité Institucional de Gestión y Desempeño de la Superintendencia.

La actualización de este manual se realizará de acuerdo con los lineamientos establecidos por la Oficina Asesora de Planeación. Cualquier copia impresa de este manual es considerada copia no controlada.

BIBLIOGRAFÍA:

https://www.mintic.gov.co/portal/inicio/

Superintendencia de Notariado y Registro

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
SIG - SSI - PO - 04 - MN - 01	1	29/10/2024	Se crea el Manual el presente Manual de Políticas del Sistema de Gestión de Seguridad, que proporciona directrices generales, las cuales serán desplegadas de forma detallada en los diferentes procedimientos, manuales, guías y documentos que componen el SGSI. • Definición de política general de seguridad. • Ajuste de objetivos, • Ajuste de lineamientos del SGSI • Eliminación de procedimientos que estaban enunciados en el documento. • Establecimiento de Roles y Responsabilidades frente al SGSI. • Creación de capítulos para segregación de temáticas con mayor claridad.

<table>
<tr><th colspan="6">ELABORACIÓN Y APROBACIÓN</th></tr>
<tr><th>ELABORÓ</th><th>REVISIÓN METODOLOGICA</th><th colspan="2">APROBÓ</th><th colspan="2">Vo. Bo. Oficina Asesora de Planeación</th></tr>
<tr><td>Juan Carlos Valenzuela Buitrago

Hugo Alejandro Casallas Larrota</td><td>Sandra Milena Niño Camacho

Alirio Tovar Castellanos

Juan Camilo Guiran Sánchez</td><td rowspan="2">José Ricardo Acevedo Solarte

Comité de Gestión Institucional de Gestión y Desempeño ActaNo.006 del 2024.</td><td rowspan="2">Jefe Oficina de Tecnologías de la Información</td><td rowspan="2">Mónica Yaneth Galvis García</td><td rowspan="2">Coordinadora Grupo Arquitectura Organizacional y Mejoramiento Continuo de la Oficina Asesora De Planeación</td></tr>
<tr><td>Oficina de Tecnología de la Información y las Comunicaciones</td><td>Grupo Arquitectura Organizacional y Mejoramiento Continuo de la Oficina Asesora De Planeación</td></tr>
<tr><td>Fecha: 10 de Octubre de 2024</td><td>Fecha: 15 de Octubre de 2024</td><td colspan="2">Fecha: 29 de Octubre de 2024</td><td colspan="2">Fecha Aprobación: 29 de Octubre de 2024</td></tr>
</table>