Política General y políticas específicas del Sistema de Seguridad de la Información

SUPERINTENDENCIA
DE NOTARIADO Y REGISTRO

Código:	Versión:	Fecha:

EQUIPO DIRECTIVO:

GOETNHY FERNANDA GARCÍA FLÓREZ
SUPERINTENDENTE DE NOTARIADO Y REGISTRO.
SANDRA VIVIANA CADENA MARTÍNEZ
SECRETARIA GENERAL.
ÁLVARO MOZO GALLARDO
SUPERINTENDENTE DELEGADO PARA EL REGISTRO.
DANIELA ANDRADE VALENCIA
SUPERINTENDENTE DELEGADA PARA EL NOTARIADO.
KARINA ISABEL CABRERA DONADO
SUPERINTENDENTE DELEGADA PARA PROTECCIÓN, RESTITUCIÓN Y FORMALIZACIÓN DE TIERRAS.
MAURICIO RIVERA GARCÍA
DIRECTOR TÉCNICO DE REGISTRO (E).
SOL MILENA GUERRA ZAPATA
DIRECTORA DE VIGILANCIA Y CONTROL NOTARIAL.
NANCY CRISTINA MESA ARANGO
DIRECTORA DE ADMINISTRACIÓN NOTARIAL.
BEATRIZ HELENA GALINDO LUGO
DIRECTORA DE TALENTO HUMANO.
CAMILA LUCIA MONTES BALLESTAS
DIRECTORA DE CONTRATACIÓN.
ÁLVARO DE FÁTIMA GÓMEZ TRUJILLO
DIRECTOR ADMINISTRATIVO Y FINANCIERO
JULIA BEATRIZ GUTIÉRREZ RODRÍGUEZ
JEFE OFICINA DE ATENCIÓN AL CIUDADANO (E)
JUAN CARLOS TORRES RODRÍGUEZ
JEFE OFICINA ASESORA DE PLANEACIÓN (E)
SHIRLEY PAOLA VILLAREJO PULIDO
JEFE OFICINA ASESORA JURÍDICA.
LUIS GERARDO CUBIDES SILVA
JEFE OFICINA DE TECNOLOGIAS DE LA INFORMACIÓN
JOSE DANIEL JUTINICO RODRIGUEZ
JEFE OFICINA CONTROL INTERNO DE GESTIÓN. (E)
EDUARD JESUS DÍAZ ARCHILA
JEFE OFICINA DE CONTROL DISCIPLINARIO INTERNO.

República de Colombia

Ministerio de Justicia y del Derecho

Superintendencia de Notariado y Registro

CONTENIDO

INTRODUCCIÓN

La Superintendencia de Notariado y Registro, determina la información como un activo de alto grado de importancia, que genera aporte en el desarrollo continuo de su misión y los objetivos estratégicos descritos en ellos, generando la necesidad de implementar reglas y medidas de control que permitan proteger la confidencialidad, integridad, disponibilidad y trazabilidad de la información durante todo su ciclo de vida.

El presente documento establece la Política General, así como las políticas específicas, que integran el Sistema de Gestión de Seguridad de la Información -SGSI-, las cuales deben ser adoptadas por los funcionarios, servidores públicos, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Superintendencia de Notariado y Registro; estas se encuentran enfocadas en el cumplimiento de la normatividad legal Colombiana vigente, a buenas prácticas gestión y al modelo de seguridad y privacidad de la información que hace parte de la estrategia de Gobierno Digital del Estado Colombiano.

OBJETIVOS GENERALES

Establecer las directrices para fortalecer la seguridad de la información en los procesos de La Superintendencia de Notariado y Registro, estableciendo dentro del plan estratégico de seguridad su liderazgo y desarrollo.

Informar al mayor nivel de detalle a los usuarios, directivos, servidores públicos, funcionarios y contratistas, las normas y mecanismos de obligatorio cumplimiento en las interacciones con los activos de información de la Superintendencia de Notariado y Registro, definiendo el alcance de las responsabilidades de cada uno de ellos.

Promover la cultura frente a la Seguridad de la Información a nivel interno y externo, con la finalidad de aplicar controles de seguridad de la información, y así disminuir el índice de eventos en los riegos tecnológicos y fortalecer la labor del Estado Colombiano para contar con entidades con servicios más eficientes y seguros.

DIRECTRICES

Todos los usuarios de los sistemas de información y telecomunicaciones de La Superintendencia de Notariado y Registro tienen la responsabilidad y obligación de cumplir con la Política General y Políticas Específicas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente documento y los demás afines.

Los jefes de área o dependencia deben asegurarse de que todos los procedimientos de seguridad de la información dentro de su área de responsabilidad se realicen correctamente para lograr el cumplimiento de la Política General, Políticas Específicas y estándares de seguridad de la información de la Superintendencia de Notariado y Registro, con el fin de alcanzar un adecuado nivel de protección en cuanto a confidencialidad, integridad y disponibilidad de la información.

Este documento debe ser de conocimiento de todos los servidores públicos, contratistas y proveedores de la Superintendencia de Notariado y Registro. Así mismo, se exigirá su cumplimiento en los procesos de contratación de la Superintendencia de Notariado y Registro, y su lectura debe ser requisito necesario antes de realizar cualquier proceso de esta índole.

REFERENCIAS NORMATIVAS Y REGLAMENTARIAS

Con el objeto de mitigar los riesgos relacionados con la autenticidad, la integridad, la disponibilidad, el no repudio, la confidencialidad y la trazabilidad de la información, se tiene que cualquier incidente que viole el marco normativo legal vigente en Colombia en materia de Política de Seguridad de la Información, estará sujeto, entre otras, a lo establecido en las siguientes disposiciones legales:

I. Marco normativo de buenas prácticas para el tratamiento de la información: Ley 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales, Decreto Reglamentario 1377 de 2013 y 1081 de 2015, Ley 1712 de 2014, por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones, Decreto Reglamentario 103 de 2015, Ley 527 de 1999, por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se dictan otras disposiciones. Las recomendaciones y buenas prácticas de los estándares.

II. Marco Normativo Sancionatorio: Ley 734 de 2002, por la cual se expide el Código Disciplinario único. Ley 1273 de enero 5 de 2009, por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información.

III. Adopción: El artículo 2.2.22.2.1 del Decreto 1083 de 2015, establece las políticas de Gestión y Desempeño Institucional, entre las que se encuentran las de “11. Gobierno Digital, antes Gobierno en Línea" y “12. Seguridad Digital”.

El Documento CONPES 3854 establece la Política Nacional de Seguridad Digital en la República de Colombia, fortaleciendo las capacidades de las múltiples partes interesadas, para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital y se generarán mecanismos permanentes para impulsar la cooperación, colaboración y asistencia en materia de seguridad digital, a nivel nacional e internacional, con un enfoque estratégico.

El Documento CONPES 3995 formula la Política Nacional de Confianza y Seguridad Digital en la República de Colombia, estableciendo medidas para ampliar la confianza digital y mejorar la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital, fortaleciendo las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado del país; actualizando el marco de gobernanza en materia de seguridad digital para aumentar su grado de desarrollo y finalmente, se analizará la adopción de modelos, estándares y marcos de trabajo en materia de seguridad digital, con énfasis en nuevas tecnologías.

A su vez, el parágrafo del artículo 16 del Decreto 2106 de 2019, establece que las autoridades que realicen trámites, procesos y procedimientos por medios digitales, deberán disponer de una estrategia de seguridad digital siguiendo los lineamientos que emita el Ministerio de Tecnologías de la Información y las Comunicaciones.

GLOSARIO

Acción correctiva: Remediación de los requisitos o acciones que dieron origen al establecimiento de una no conformidad, de tal forma que no se vuelva a presentar.

Acción preventiva: Disposición de operaciones que buscan de forma preliminar, que no se presente en su ejecución, desarrollo e implementación una no conformidad.

Aceptación del Riesgo: Después de revisar las consecuencias que puede acarrear el riesgo, se toma la decisión de afrontarlo.

Activo: Recurso del sistema de información o cualquier elemento que tenga valor para la organización, hacen parte de los activos de información los siguientes:

a) **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen en la Superintendencia de Notariado y Registro. Ejemplo: archivo de Word ¨listado de personal.docx¨.
b) **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información. Ejemplo: VUR.
c) **Personal:** Es todo el recurso humano de la Superintendencia de Notariado y Registro, el subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Superintendencia de Notariado y Registro. Ejemplo: Julián García.
d) **Servicios:** Utilidad o función que presta la Superintendencia de Notariado y Registro, los hay tanto internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.
e) **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones.
f) **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información. Ejemplo: Nivel Central.

Activo de Información: Todo aquel elemento lógico o físico que conforme cualquiera de los sistemas de información y que tiene un valor para la institución. Ej. Bases de datos, sistemas operacionales, redes, sistemas de información y comunicaciones, documentos impresos, fichas, formularios y recursos humanos.

Administrador del Sistema: Persona responsable de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas. Dicha administración está dirigida por la Oficina de Tecnologías de la Información - OTI y se realizará por conducto de las Coordinaciones de esta.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la Superintendencia de Notariado y Registro. Su enfoque se basa en tres pilares fundamentales que son: Detectar cualquier alteración en los servicios TI, registrar y clasificar estas alteraciones, asignar el personal encargado de restaurar el servicio.

Administrador de Correo: Persona responsable de solucionar problemas en el correo electrónico, responder preguntas a los usuarios y otros asuntos en un servidor.

Análisis de riesgos: Proceso sistemático que permite identificar y determinar el impacto o grado de vulnerabilidad de los activos de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Almacenamiento en la Nube: Del inglés Cloud Storage, es un modelo de almacenamiento de datos basado en redes de computadoras que consiste en guardar archivos en un lugar de Internet por medio de aplicaciones o servicios.

Amenaza: Causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

APT (*Advance Persistent Threat*) Amenaza Avanzada: Persistente Especie de ciberataque que es responsable del lanzamiento de ataques de precisión y tienen como objetivo comprometer una máquina en donde haya algún tipo de información valiosa.

Ataque Cibernético: Intento de penetración de un sistema informático por parte de un usuario no deseado ni autorizado, por lo general con intenciones insanas y perjudiciales.

Brecha de Seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Autenticidad: Es el mecanismo mediante la cual la Superintendencia de Notariado y Registro busca garantizar que los activos de información provienen de una fuente fidedigna, es decir, que el origen sea realmente de quien envía la información ya sea un usuario, una entidad o un sistema de información.

Buzón: También conocido como cuenta de correo, es un espacio exclusivo, asignado en el servidor de correo, para almacenar los mensajes y archivos adjuntos enviados por otros usuarios internos o externos a La Superintendencia de Notariado y Registro.

Características de la Información: Las principales características desde enfoque de seguridad de información son: *Confidencialidad, disponibilidad e integridad.*

Checklist: Lista de apoyo para el auditor con los puntos a auditar, que ayuda a mantener claros los objetivos de la auditoría, sirve de evidencia del plan de auditoría, asegura su continuidad y profundidad y reduce los prejuicios del auditor y su carga de trabajo, este tipo de listas también se pueden utilizar durante la implantación del SGSI para facilitar su desarrollo.

Centro de Cómputo: También conocido como Centro de Procesamiento de Datos o Data Center, es una instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea.

Chat: Comunicación simultánea y sincronizada entre dos o más personas a través de Internet.

Confidencialidad: Característica de la información por medio de la cual no se revela ni se encuentra a disposición de individuos, organizaciones o procesos no autorizados. La información debe ser vista o estar disponible solo a las personas autorizadas.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Control: Mecanismo para manejar el riesgo, incluyendo políticas, procedimientos, guías, estructuras organizacionales, buenas prácticas, y que pueden ser de carácter administrativo, técnico o legal.

Control correctivo: Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

Control detectivo: Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado, pero por sí mismo no la corrige.

Control disuasorio: Control que reduce la posibilidad de materialización de una amenaza, p.ej., por medio de avisos disuasorios.

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Correo electrónico: También conocido como E-mail, es un servicio de red que permite a los usuarios enviar y recibir textos, imágenes, videos, audio, programas, a través de internet.

Computo forense: Llamado informática forense, computación forense, análisis forense digital o examinación forense digital, es la aplicación de técnicas científicas y analíticas especializadas a

infraestructura tecnológica que permiten identificar, preservar, analizar y presentar datos que sean válidos dentro de un proceso legal.

Cuentas de Correo: Son espacios de buzones para la recepción, envío y almacenamiento de mensajes de correo electrónico en internet.

Contraseña o Password: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al usuario tener acceso a un computador, a un archivo y/o a un programa.

Criptografía: Conjunto de herramientas matemáticas, técnicas y algoritmos, que con el uso de una o más claves permiten cifrar la información y, por tanto, protegerla y dotarle al menos de confidencialidad e integridad.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo. La mayoría de las ocasiones se busca dejar fuera de servicio los servidores informáticos de una compañía o en su defecto en situaciones más complejas ocasionar graves daños, para que no puedan utilizarse ni consultarse servicios importantes. Un aspecto para resaltar es el gran daño a la imagen y reputación de las Superintendencia de Notariado y Registro es que estas acciones dejan en el ambiente público.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Disponibilidad: Característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad o proceso autorizada al interior de la Superintendencia de Notariado y Registro.

Evaluación de riesgos: Proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento de Seguridad de La información: Ocurrencia identificada de una situación de sistema, servicio o red que indica una posible violación de la política de seguridad de la información o falla de salvaguardas, o una situación previamente desconocida que puede ser relevante para la seguridad de un activo de información.

Evidencia objetiva: Información, registro o declaración de hechos, cualitativa o cuantitativa, verificable y basada en observación, medida o test, sobre aspectos relacionados con la confidencialidad, integridad o disponibilidad de un proceso o servicio o con la existencia e implementación de un elemento del sistema de seguridad de la información.

Gusano (Worm): Es un programa malicioso de computador que tiene la capacidad de duplicarse a sí mismo. A diferencia del virus, no altera información, aunque casi siempre causan problemas de red debido al consumo de ancho de banda y su gran facilidad para mutar.

Firma Digital: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la Superintendencia de Notariado y Registro de una persona o de un equipo informático al mensaje o documento.

Firewall: Dispositivo que permite bloquear o filtrar el acceso en redes de comunicación.

Hacker: Persona dedicada a realizar entradas no autorizadas a los sistemas, por medio de redes de comunicación como Internet, con el objeto de encontrar vulnerabilidades en los sistemas.

Host: Termino usado en informática para referirse a los computadores conectados a la red, que proveen y/o utilizan servicios de ella. Los usuarios deben utilizar hosts para tener acceso a la red.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Ingeniería Social: Es la manipulación de las personas para conseguir que hagan que algo debilite la seguridad de la red o faciliten información con clasificación confidencial o superior.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Infraestructura de Procesamiento de Información: Es cualquier sistema de procesamiento de información, servicio, plataforma tecnológica, o instalación física que los contenga.

Integridad: La propiedad de salvaguardar la exactitud y completitud de los activos de información.

Internet: Conjunto de redes conectadas entre sí, que utilizan el protocolo TCP/IP para comunicarse entre sí.

Intranet: Red privada dentro de una empresa, que utiliza el mismo software y protocolos empleados en la Internet global, pero que es de uso interno.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

IPS: Sistema de prevención de intrusos. Es un dispositivo que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

Incidente de Seguridad de la información: Es la identificación de la ocurrencia de un hecho que está relacionado con los activos de información, que indica una posible brecha en las Políticas de Seguridad o falla en los controles y/o protecciones establecidas.

Keyloggers: Son software o aplicaciones que almacenan información digitada mediante el teclado de un computador por un usuario; es común relacionar este término con malware del tipo Daemon (demonio), es decir, actúa como un proceso informático que no interactúa con el usuario, ya que se ejecuta en segundo plano. Usualmente puede ser un tipo de software o un dispositivo hardware que se encarga de registrar las pulsaciones que se hacen con el teclado, para posteriormente memorizarlas en un archivo o enviarlas a través de internet.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

LAN: (*Local Area Network*). (*Red de Área Local*). Red de computadoras ubicadas en el mismo ambiente, piso o edificio.

Malware: Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema informático.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

No repudio: Los activos de información deben tener la capacidad para probar que una acción o un evento han tenido lugar, de modo que tal evento o acción no pueda ser negado posteriormente.

PDCA Plan-Do-Check-Act: Modelo de proceso basado en un ciclo continuo de las actividades de planificar (establecer el SGSI), realizar (implementar y operar el SGSI), verificar (monitorizar y revisar el SGSI) y actuar (mantener y mejorar el SGSI). PHVA.

Phishing: Tipo de delito encuadrado dentro del ámbito de las estafas, que se comete mediante el uso de un tipo de ingeniería social caracterizado por intentar adquirir información confidencial de forma

fraudulenta (como puede ser una contraseña o información detallada sobre tarjetas de crédito u otra información bancaria), mediante una aparente comunicación oficial electrónica.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Superintendencia de Notariado y Registro en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Plan de recuperación de desastres: proceso de recuperación que cubre los datos, el hardware y el software crítico, para que la entidad pueda comenzar de nuevo sus operaciones en caso de un desastre natural o una causa externa.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

Política de escritorio despejado: Se define como la política que establece e indica a los funcionarios, contratista y demás colaboradores de la Superintendencia de Notariado y Registro a asegurar la información pública reservada o información pública clasificada (privada o semiprivada) en lugares que ofrezca la protección necesaria, así mismo los escritorios deben permanecer libres de documentos o informaciones susceptibles de ser afectados en su integridad, confidencialidad y/o disponibilidad.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información. La protección de copia es a menudo tema de discusión y se piensa que en ocasiones puede violar los derechos de copia de los usuarios, por ejemplo, el derecho a hacer copias de seguridad de una videocinta que el usuario ha comprado de manera legal, el instalar un software de computadora en varias computadoras, o el subir la música a reproductores de audio digital para facilitar el acceso y escucharla.

Ransomware: Código malicioso para secuestrar datos, una forma de explotación en la cual el atacante cifra los datos de la víctima y exige un pago por la clave de descifrado.

Red: Se tiene una red, cada vez que se conectan dos o más computadoras de manera que pueden compartir recursos.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Riesgo residual: Es el riesgo remanente, después de la implantación de las medidas de seguridad determinadas en el plan de seguridad de la información.

Segregación de tareas: Separar tareas sensibles entre distintos funcionarios o contratistas para reducir el riesgo de un mal uso de los sistemas e informaciones deliberado o por negligencia.

Sistema de Gestión de Seguridad de la información: SGSI La parte del sistema total de gestión, basada en un enfoque de riesgo de negocios, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información.

Seguridad: Mecanismos de control que evitan el uso no autorizado de recursos, no es un producto sino un proceso, en el que intervienen todos los aspectos de la tecnología y también las personas, siendo estas últimas por lo general el eslabón más débil de toda la cadena.

Seguridad de la Información: Son medidas preventivas que incluyen factores de confidencialidad, integridad, disponibilidad, autenticidad, responsabilidad, aceptabilidad y confiabilidad de la información e incluye aquellos aspectos sistémicos de la gestión de la seguridad, como podrían ser: Gestión de la seguridad de la información, asesoría y auditoría de la seguridad, análisis y gestión de riesgos, continuidad de negocio, gobierno, comercio electrónico y legislación relacionada con seguridad.

Definido también en el artículo 2.2.9.1.1.3 del Decreto 1078 de 2015 como el principio que busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.

Seguridad informática: Aspectos de seguridad que inciden o tienen que ver directamente con la informática; es decir, en los medios informáticos en los que se genera, gestiona, almacena o destruye esta información, pero sin profundizar en aspectos sistémicos de la gestión de esa seguridad.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red.

Servidor de Correo: Dispositivo y/o aplicación informática, cuya función es gestionar el tráfico de ficheros a través del correo electrónico, su misión es la de almacenar, en su disco duro, los mensajes que envía y que reciben los usuarios.

Sistema Operativo: Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil.

Spamming: Se llama spam, correo basura o SMS basura a los mensajes no solicitados, habitualmente de tipo publicitario, enviados en grandes cantidades (incluso masivas) que perjudican de alguna o varias maneras al receptor. La acción de enviar dichos mensajes se denomina Spamming. La vía más usada es el correo electrónico.

Sniffers: Programa de captura de las tramas de red. Generalmente se usa para gestionar la red con una finalidad docente o de control, aunque también puede ser utilizado con fines maliciosos.

Spoofing: Falsificación de la Superintendencia de Notariado y Registro origen en una sesión: la Superintendencia de Notariado y Registro es por una dirección IP o Mac Address.

Tratamiento de riesgos: a partir del riesgo definido, se aplican los controles con los cuales se busca que el riesgo no se materialice.

Trazabilidad: Propiedad que garantiza que las acciones de la Superintendencia de Notariado y Registro se pueden rastrear únicamente hasta dicha Superintendencia.

Troyano: Aplicación que aparenta tener un uso legítimo pero que tiene funciones ocultas diseñadas para sobrepasar los sistemas de seguridad. Así mismo, es considerado como un programa con una determinada función o utilidad, pero que contiene código oculto para ejecutar acciones no esperadas por el usuario.

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena a la Superintendencia de Notariado y Registro, como proveedores, contratistas o consultores, que provean servicios o productos a esta Superintendencia.

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así programas ejecutables, sin la autorización ni el conocimiento del usuario.

VPN (Virtual Private Network): es una tecnología de red que permite una extensión segura de la red privada de área local (LAN) sobre una red pública o no controlada como Internet.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.

CAPITULO I. POLÍTICA GENERAL DE SEGURIDAD DE LA INFORMACIÓN.

Justificación.

La Superintendencia de Notariado y Registro consciente de que su principal activo es la información, se compromete fehacientemente con la protección de la misma y por tal motivo adopta como parte de sus estrategias institucionales la realización e implementación de un sistema de gestión de seguridad de la información con el fin de lograr generar confianza mediante la vigilancia y control del servicio registral y notarial supervisando la Guarda de la Fe Pública, la seguridad jurídica de los bienes inmuebles y las estrategias para restituir, formalizar y proteger las tierras en Colombia, a partir de la modernización y optimización de los procesos administrativos, tecnológicos y humanos y trámites más ágiles y confiables en las Oficinas de Registro de Instrumentos Públicos a lo largo de todo el país.

Dado lo anterior, se establece un esquema conformado por la Política General, políticas específicas, parámetros, guías y descripción de roles y responsabilidades que involucran las actividades de operación, gestión, administración de riesgos, preservación de la confidencialidad, integridad, disponibilidad, trazabilidad, continuidad de las operaciones, gobernabilidad de las TICS, gestión de riesgos y adopción de una cultura de la seguridad de la información aplicable a toda la Superintendencia

de Notariado y Registro, todo ello bajo el cumplimiento del marco legal y regulatorio establecido por el Estado colombiano.

Alcance de la política: El alcance de esta política cubre todas las fuentes en las que se genera, almacena o destruye información en la SNR, así como establecer derechos y deberes para los actores de la seguridad de la información como servidores públicos, contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Superintendencia de Notariado y Registro.

Objetivos específicos: La política general de seguridad de la información tendrá como ejes centrales u objetivos generar acciones para:

- Disminuir el riesgo de pérdida de confidencialidad, integridad, disponibilidad de la información durante la ejecución de los procesos institucionales.
- Definir los lineamientos de estricto cumplimiento para fortalecer la seguridad de la información en toda la superintendencia.
- Caracterizar el sistema de gestión de seguridad de la información.
- Definir los mecanismos de protección de los activos de información de la Superintendencia de Notariado y Registro.
- Generar confianza digital en las partes interesadas internas y externas respecto a los servicios prestados por la Superintendencia de Notariado y Registro.
- Construir políticas, procesos, procedimientos, guías e instructivos que permitan la adopción de la seguridad de la información en la Superintendencia de Notariado y Registro.
- Crear una cultura enfocada en la seguridad de la información que facilite la adopción de nuevas tecnologías.
- Dotar a la Superintendencia de Notariado y Registro de mecanismos que permitan garantizar la continuidad del negocio, la recuperación de desastres y el análisis de impacto frente a las amenazas, incidentes y problemas asociados con seguridad de la información.
- Articular el sistema de gestión de seguridad de la información con el sistema integrado de gestión de la SNR para permitir su implementación, operación y mejora continua.
- Diseñar, programar y realizar los programas y planes de auditoría del sistema de gestión de seguridad de la información -SGSI.
- Definir los presupuestos que permitan contar con dispositivos y sistemas de seguridad perimetral, para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
- Mantener alineado el SGSI con los planes estratégicos de la entidad.
- Cumplir con los criterios y requisitos de seguridad atendiendo el marco normativo y legal de la SNR

Para fortalecer el cumplimiento estricto de la política general y soportar la implementación del sistema de seguridad de la información la Superintendencia de Notariado y Registro adopta como obligaciones los siguientes:

a) Los roles, responsabilidades y tareas serán comunicados de manera oportuna a todos los funcionarios, servidores públicos contratistas, personal en comisión administrativa, visitantes y terceros que presten sus servicios o tengan algún tipo de relación con la Superintendencia de Notariado y Registro.
b) Proteger la información en los lugares de creación, procesamiento y distribución de la misma (infraestructura tecnológica de la SNR), así como en aquellos escenarios donde se involucren activos de información de la Superintendencia de Notariado y Registro, de acceso a terceros o proveedores.
c) Proteger la información involucrada en los procesos de negocio de la Superintendencia.
d) Proteger la información de las amenazas que puedan originar funcionarios, terceros o partes ajenas a la entidad.
e) Implementar controles, en el acceso, la operación y las comunicaciones para salvaguardar los activos de información de la entidad.
f) Garantizar la continuidad de los procesos misionales de la entidad, mediante un análisis de impacto, planes de continuidad del negocio y planes de recuperación de desastres.
g) Garantizar el cumplimiento de las leyes y regulaciones en materia de seguridad de la información.

El incumplimiento a la política de Seguridad de la Información, traerá consigo las consecuencias legales que apliquen al interior de la Superintendencia y las que para ello se encuentran definidas por la legislación Colombiana.

Por último, la política general del sistema de gestión de seguridad de la información se fortalece con las políticas específicas, definidas en los capítulos siguientes de este documento.

CAPITULO II. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DE LA INFORMACIÓN

Las políticas específicas de seguridad de la información de la Superintendencia de Notariado y Registro establecen los siguientes aspectos a tener en cuenta:

Política estructura organizacional de seguridad de la información

La Superintendencia de Notariado y Registro establece roles y responsabilidades que involucran las actividades de operación, gestión y administración de la seguridad de la información, por ello se establece el comité de seguridad de la información y perfiles para el sistema.

Conformación Comité de Seguridad de la Información:

El comité de seguridad de la información estará conformado por:

- El Secretario General.
- El Director Administrativo y Financiero, acompañado del coordinador de gestión documental.
- El Jefe de la Oficina Asesora de Planeación o su representante.
- El Jefe de la Oficina Tecnologías de la Información, quien será el Secretario Técnico del Comité.
- El funcionario que sea designado como especialista en seguridad de la información

- El Jefe de la Oficina de Control Interno.

Funciones del Comité de Seguridad de la Información:

Además de las funciones aquí señaladas, el Comité de Gestión, como instancia orientadora de la implementación de la estrategia de Gobierno Digital, de acuerdo con lo señalado en el artículo 2.2.9.1.1.1. del Decreto 1078 de 2015, debe:

- Proponer y revisar el cumplimiento de normas y políticas de seguridad, que garanticen acciones preventivas y correctivas para la salvaguarda de equipos e instalaciones de cómputo, así como las bases de datos e información en general.
- Revisar el estado general de la seguridad de la información.
- Revisar y analizar los incidentes de seguridad de la información existentes.
- Revisar y aprobar los proyectos de seguridad de la información.
- Formular las modificaciones o nuevas políticas de seguridad de la información.
- Participar en la formulación y evaluación de planes de acción para mitigar y/o eliminar riesgos.
- Identificar necesidades de evaluación de los procesos soportados por los recursos informáticos y su plataforma tecnológica.
- Realizar otras actividades inherentes a la naturaleza del comité relacionadas con la seguridad de la información.
- Promover la mejora continua del Sistema de Gestión de Seguridad de la Información.

Las funciones del Comité de Seguridad de la Información irán de la mano a las del Comité de Gestión, quien tiene a su cargo la aprobación de las modificaciones o nuevas políticas de seguridad de la información; como instancia orientadora de la implementación de la estrategia de Gobierno Digital.

Funciones del Secretario Técnico:

- Realizar convocatoria a los integrantes del Comité a las sesiones ordinarias y extraordinarias.
- Remitir la agenda a los miembros del Comité con tres días de antelación.
- Verificar el quórum al inicio de las sesiones.
- Recibir y preparar la respuesta a los documentos que sean de competencia del Comité.
- Firmar las actas que hayan sido aprobadas.
- Realizar seguimiento a los compromisos y tareas pendientes del Comité.
- Elaborar las actas de reunión del Comité oportunamente.
- Llevar y custodiar el archivo de las actas y demás documentos soporte del Comité.
- Las demás que le sean asignadas por el Comité.

Responsabilidades del Comité de Seguridad de la Información.

- Los miembros del Comité de Seguridad de la Información son responsables de:

- Del análisis, revisión y centralización de todas las acciones referidas a la gestión de Seguridad de la Información de la organización y de mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos de la Superintendencia de Notariado y Registro.
- Asegurar que exista una dirección y apoyo gerencial sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestión de la seguridad de los activos de la información, a través de compromisos apropiados y de recursos adecuados, como la formulación y mantenimiento de las políticas de seguridad de la información a través de todos los funcionarios de la organización.
- Validar las políticas de seguridad de la información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los servidores públicos y contratistas de la organización, asegurando que la información se encuentre protegida.
- Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smartphones), tabletas), entre otros, suministrados por la Superintendencia de Notariado y Registro y que hagan uso de los servicios de información de la Superintendencia de Notariado y Registro.
- Definir la estrategia informática que permita lograr los objetivos y minimizar de los riesgos de la institución.
- Monitorear el estado del proyecto en términos de calidad de los productos, tiempo y los costos.
- Realizar el seguimiento y/o verificación de la implementación de los requisitos, controles e indicadores del Sistema de Gestión de Seguridad de la Información
- Velar por la aprobación de presupuestos para las actividades del SGSI.

Equipo de respuesta a incidentes: Con el fin de facilitar la implementación, seguimiento y mejora continua, se define el equipo de respuesta a incidentes o CSIRT (Computer Security Incident Response) de la Superintendencia de Notariado y Registro, el cual estará conformado por:

- Profesionales especializados y universitarios de la oficina de Tecnologías de información OTI.
- Consultores especialistas en seguridad de la información.
- Profesional de la oficina Asesora de Planeación.
- Profesionales de gestión documental.

La definición de roles y responsabilidades específicas se definen en documento independiente, ajustados a las condiciones del manual de funciones de la SNR y aprobación del Comité.

Funciones del equipo de respuesta de incidentes o CSIRT (computer security incident response)

- Realizar el registro detallado y comunicar por escrito de manera oportuna la ocurrencia de eventos e incidentes de seguridad de la información, con el fin que la OTI y en casos mayores el Comité de S.I, generen las acciones pertinentes.
- Coordinar con la Oficina de Tecnologías de la Información OTI, la definición de proyectos y medidas de seguridad de la Información.
- Presentar propuestas sobre información relacionada e indicadores para que el Comité de Seguridad de la Información determine si deben considerarse de interés de la SNR.

- Suministrar conceptos sobre condiciones que permitan garantizar la seguridad de la Información en la SNR.
- Asesorar y formular acciones para orientar, capacitar y mejorar la Seguridad de la Información de la SNR.

Política de seguridad para los recursos humanos

La Superintendencia de Notariado y Registro establece acciones para asegurar que los funcionarios, servidores públicos, contratistas, proveedores y demás colaboradores, entiendan sus responsabilidades frente al cumplimiento de las políticas como usuarios y las responsabilidades que las mismas conllevan.

La Superintendencia establece capacitar y sensibilizar a los funcionarios en temas de seguridad de la información mínimo una vez al año, con el fin de asegurar que los funcionarios, contratistas y demás colaboradores, acaten sus responsabilidades en relación con las políticas de seguridad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información.

Los servidores públicos, candidatos, aspirantes, contratistas y proveedores, deben dar aprobación a la Superintendencia de Notariado y Registro, para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012 y, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales, lo que se deberá ver reflejado en las cláusulas de los contratos y en el aplicativo aspirante.

Proceso Disciplinario

En situaciones de incumplimiento y/o violaciones a las políticas de seguridad de la información se deberá tramitar el cumplimiento de la Ley 734 de 2002 y demás normas que reglamenten los procesos disciplinarios, para los empleados del Estado.
Las actuaciones que conllevan a la violación de la seguridad de la información establecidas por la Superintendencia de Notariado y Registro son, entre otras:

1. No firmar los acuerdos de confidencialidad o de entrega de información o de activos de información.
2. No reportar los incidentes de seguridad o las violaciones a las políticas de seguridad, cuando se tenga conocimiento de ello, para lo cual se debe seguir el procedimiento establecido por la Superintendencia de Notariado y Registro.
3. No actualizar la información de los activos de información a su cargo.
4. Clasificar y registrar de manera inadecuada la información en caso de que su cargo o responsabilidad ameriten clasificarla, desconociendo los estándares establecidos por la Superintendencia de notariado y registro para tal fin.
5. No guardar de forma segura la información cuando se ausenta de su puesto de trabajo o al terminar la jornada laboral (documentos impresos que contengan información pública reservada, información pública clasificada -privada o semiprivada).
6. No guardar la información digital, producto del procesamiento de la información perteneciente a la Superintendencia de Notariado y Registro.

7. Dejar información pública reservada en carpetas compartidas o en lugares distintos al servidor de archivos, obviando las medidas de seguridad.
8. Dejar las gavetas abiertas o con las llaves puestas en los escritorios.
9. Dejar los computadores encendidos en horas no laborables.
10. Permitir que personas ajenas a la Superintendencia de Notariado y Registro deambulen sin acompañamiento al interior de las instalaciones, en áreas no destinadas al público.
11. Almacenar en los discos duros de los computadores personales de los usuarios la información de la Superintendencia de Notariado y Registro.
12. Solicitar cambio de contraseña de otro usuario, sin la debida autorización del titular o su jefe inmediato (Esta autorización debe ser por escrito).
13. Hacer uso de la red de datos de la institución para obtener, mantener o difundir en los equipos de sistemas, material pornográfico (penalizado por la ley) u ofensivo, mensajes con contenido religioso, político, racista, sexista, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros.
14. Hacer uso de la red de datos de la institución para obtener, mantener o difundir mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales. Igualmente, cadenas de correos y correos masivos que contengan alguna de las conductas descritas en el presente numeral.
15. Utilización de software no relacionados con la actividad laboral y que pueda degradar el desempeño de la plataforma tecnológica institucional.
16. Recibir o enviar información institucional a través de correos electrónicos personales, diferentes a los asignados por la institución.
17. Enviar información pública reservada o información pública clasificada (privada o semiprivada) por correo, copia impresa o electrónica sin la debida autorización y sin la utilización de los protocolos establecidos para la divulgación.
18. Utilizar equipos electrónicos o tecnológicos desatendidos o a través de sistemas de interconexión inalámbrica, sirvan para transmitir, recibir y almacenar datos.
19. Usar dispositivos de almacenamiento externo en los computadores, cuya autorización no haya sido otorgada de manera escrita por la Oficina de Tecnologías de la Información de la Superintendencia de Notariado y Registro.
20. Permitir el acceso de funcionarios a la red corporativa sin la autorización de la Oficina de Tecnologías de la Información de la Superintendencia de Notariado y Registro.
21. Descuidar documentación con información pública reservada o clasificada de la Superintendencia de Notariado y Registro sin las medidas apropiadas de seguridad que garanticen su protección.
22. Registrar información pública reservada o clasificada en pos-it, apuntes, agendas, libretas, etc., sin el debido cuidado.
23. Almacenar información pública reservada o clasificada en cualquier dispositivo de almacenamiento que no permanezca a la Superintendencia de Notariado y Registro o conectar computadores portátiles u otros sistemas eléctricos o electrónicos personales a la red de datos de la Superintendencia de Notariado y Registro, sin la debida autorización.
24. Archivar información pública reservada o clasificada, sin claves de seguridad o cifrado de datos.
25. Promoción o mantenimiento de negocios personales o utilización de los recursos tecnológicos de la Superintendencia de Notariado y Registro para beneficio personal.

26. El que sin autorización acceda en todo o parte del sistema informático o se mantenga dentro del mismo en contra de la voluntad de la Superintendencia de Notariado y Registro.
27. El que impida u obstaculice el funcionamiento o el acceso normal al sistema informático, los datos informáticos o las redes de telecomunicaciones de La Superintendencia de Notariado y Registro, sin estar autorizado.
28. El que destruya, dañe, borre, deteriore o suprima datos informáticos o un sistema de tratamiento de información de La Superintendencia de Notariado y Registro.
29. El que distribuya, envíe, introduzca software malicioso u otros programas de computación de efectos dañinos en la plataforma tecnológica de la Superintendencia de Notariado y Registro.
30. El que viole datos personales de las bases de datos de la Superintendencia de Notariado y Registro.
31. Utilización de servicios disponibles a través de internet, como FTP y Telnet, no permitidos por La Superintendencia de Notariado y Registro o de protocolos y servicios que no se requieran y que puedan generar riesgo para la seguridad.
32. Negligencia en el cuidado de los equipos, dispositivos portátiles o móviles entregados para actividades propias de la Superintendencia de Notariado y Registro.
33. No cumplir con las políticas o directrices para la protección de los activos de información de la Superintendencia de Notariado y Registro
34. Destruir o desechar de forma incorrecta la documentación institucional.
35. Descuidar documentación con información pública reservada o clasificada de la Superintendencia de Notariado y Registro sin las medidas apropiadas de seguridad que garanticen su protección.
36. El que superando las medidas de seguridad informática suplante un usuario ante los sistemas de autenticación y autorización establecidos por la Superintendencia de Notariado y Registro.
37. No mantener la confidencialidad de las contraseñas de acceso a la red de datos, los recursos tecnológicos o los sistemas de información de la Superintendencia de Notariado y Registro o permitir que otras personas accedan con el usuario y clave del titular a éstos.
38. Permitir el acceso u otorgar privilegios de acceso a las redes de datos de la Superintendencia de Notariado y Registro a personas no autorizadas.
39. Llevar a cabo actividades fraudulentas o ilegales, o intentar acceso no autorizado a cualquier computador de La Superintendencia de Notariado y Registro o de terceros.
40. Ejecutar acciones tendientes a eludir o variar los controles establecidos por la Superintendencia de Notariado y Registro.
41. Retirar de las instalaciones de la institución, estaciones de trabajo o computadores portátiles que contengan información institucional sin la autorización pertinente.
42. Sustraer de las instalaciones de la Superintendencia de Notariado y Registro, documentos con información institucional calificada como información pública reservada o clasificada, o abandonarlos en lugares públicos o de fácil acceso.
43. Entregar, enseñar y divulgar información institucional, calificada como información pública reservada y clasificada a personas no autorizadas por la Superintendencia de Notariado y Registro.
44. No realizar el borrado seguro de la información en equipos o dispositivos de almacenamiento de la Superintendencia de Notariado y Registro, para traslado, reasignación o para disposición final.
45. Ejecución de cualquier acción que pretenda difamar, abusar, afectar la reputación o presentar una mala imagen de la Superintendencia de Notariado y Registro o de alguno de sus funcionarios.
46. Realizar cambios no autorizados en la plataforma tecnológica de la Superintendencia de Notariado y Registro.
47. Acceder, almacenar o distribuir pornografía infantil.

48. Instalar programas o software no autorizados en las estaciones de trabajo o equipos portátiles institucionales, cuyo uso no esté autorizado por la OTI de la Superintendencia de Notariado y Registro.
49. Copiar sin autorización los programas de la Superintendencia de Notariado y Registro o violar los derechos de autor o acuerdos de licenciamiento.
50. Detectar el ingreso a carpetas de otros procesos, unidades, grupos o áreas reservadas, sin autorización y no reportarlo al SSNR (Grupo de incidentes de seguridad de la información de la SNR) o al CSIRT local (Computer Security Incident Response) -Equipo de respuesta a incidentes de la SNR.

Política de gestión - uso de activos de información.

La Superintendencia de Notariado y Registro implementa directrices para lograr y mantener la protección adecuada y uso de los activos de información para que los usuarios finales los administren de acuerdo con sus roles y funciones; por lo tanto, los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música, y fotos y cualquier tipo de archivo que no sean de carácter institucional.

La Superintendencia de Notariado y Registro es propietaria de los activos de información y los administradores de estos son los funcionarios, contratistas o demás colaboradores de la entidad (denominados “usuarios”) que estén autorizados y son los responsables por la información de los procesos a su cargo, la seguridad de los sistemas de información o aplicaciones informáticas, el hardware o la infraestructura de Tecnología y Sistemas de Información, por tal razón los usuarios deben cumplir con lo estipulado en el aparte proceso disciplinario de este documento, con el fin de evitar ser objeto de sanciones.

Propiedad intelectual.

La Superintendencia de Notariado y Registro es el dueño de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato conforme a lo establecido en las leyes generales de protección de datos, por lo tanto, los terceros no tienen derecho a reclamar sobre estas invenciones.

Política de uso de estaciones cliente.

Los usuarios no podrán realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, papel tapiz y protector de pantalla corporativo.

La información almacenada en los equipos de cómputo de la Superintendencia de Notariado y Registro es de su propiedad y cada usuario es responsable por proteger su integridad, confidencialidad y disponibilidad.

Política de uso de internet.

La Superintendencia de Notariado y Registro permite el acceso al servicio de internet exclusivamente para el facilitar el desempeño de las labores de los trabajadores, a su vez implementa mecanismos para evitar, errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones web.

La OTI implementa herramientas para evitar la descarga de software no autorizado y/o código malicioso en los equipos institucionales desde internet, así mismo, controla el acceso a la información contenida en portales de almacenamiento en internet para prevenir la fuga de información.

Se limitará el acceso a los usuarios de los activos de información de la entidad, por tal motivo tienen restringido el acceso a redes sociales, sistemas de mensajería instantánea, acceso a sistemas de almacenamiento en la nube (diferentes a los suministrados por la Superintendencia de Notariado y Registro) y cuentas de correo no institucional. En caso de ser requerido por las funciones del cargo, el jefe inmediato debe remitir la solicitud a Jefe de área de la OTI, para que sea autorizado por el Comité de Seguridad de la Información y será objeto de auditorías de seguridad mediante el módulo de seguridad web que tiene la entidad.

Se prohíbe el acceso a páginas relacionadas con pornografía, nueva era, música, videos, concursos o sitios de violencia específica.

Se prohíbe la descarga, uso, intercambio y/o instalación de programas, juegos, música, videos, películas, imágenes, protectores, fondos de pantalla y software de libre distribución.

Política de clasificación de la información.

La Superintendencia de Notariado y Registro consiente de la necesidad de asegurar que la información reciba el nivel de protección apropiado de acuerdo con el tipo de clasificación establecido por la Ley 1581 de 2012 y su Decreto reglamentario 1377 de 2013 define reglas de como clasificar la información.

Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Superintendencia de Notariado y Registro, por ejemplo:

- Formularios / comprobantes propios o de terceros.
- Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
- Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
- Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.

Política de manejo, disposición de información, medios y equipos.

La Superintendencia de Notariado y Registro establece directrices para evitar la divulgación, la modificación, el retiro o la destrucción no autorizada de información almacenada en los medios proporcionados, velando por la disponibilidad y confidencialidad de la información.

Los medios y equipos donde se almacena procesan o comunica la información deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos cada vez que se requiera, para lo cual se le avisará al usuario sobre la realización de estas actividades con anterioridad.

El servicio de acceso a Internet, Intranet, sistemas de información, medio de almacenamiento, aplicaciones (Software), cuentas de red, navegadores y equipos de cómputo (que son propiedad de la Superintendencia de Notariado y Registro) deben ser usados únicamente para el cumplimiento de la misión y visión de la Superintendencia de Notariado y Registro.

La superintendencia adopta como control el borrado seguro en los equipos de cómputo y demás dispositivos una vez el funcionario haya sido retirado de la institución, de acuerdo con los procedimientos que para tal fin tenga contemplada la entidad.

Política de control de acceso.

El acceso a los activos de información de la Superintendencia de Notariado y Registro está permitido únicamente a los usuarios autorizados.

La conexión remota a la red de área local de la Superintendencia de Notariado y Registro solo se realiza a través de una conexión VPN segura, la cual es suministrada aprobada, registrada y auditada únicamente por la OTI.

El funcionario que disponga de claves de acceso a los activos de información será responsable de su uso, esta clave es personal e intransferible y la debe usar durante el proceso de autenticación.

Todo activo informático debe ser adquirido por la OTI conforme a las necesidades de la SNR y su acceso gestionado por la misma.

Política de establecimiento, uso y protección de claves de acceso.

Ningún usuario debe acceder a la red o a los servicios TIC de la Superintendencia de Notariado y Registro, utilizando una cuenta de usuario o clave de otro usuario.

La Superintendencia de Notariado y Registro suministra a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.

El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta, comunicándose a Mesa de Ayuda, en donde se llevará a cabo la validación de los datos personales; en caso de ser solicitado el cambio de contraseña para otra persona, debe ser realizada por su jefe inmediato (previa autorización por parte del jefe de la OTI).

Las claves o contraseñas de los usuarios deben:

Tener mínimo ocho (8) caracteres alfanuméricos.

Cada vez que se cambien estas deben ser distintas por lo menos de las últimas 4 anteriores.

La contraseña debe cumplir con “tres” de los cuatro requisitos:

- Caracteres en mayúsculas
- Caracteres en minúsculas
- Base de 10 dígitos (0 a 9)
- Caracteres no alfabéticos (Ejemplo: ¡,$,%,&)

Se debe garantizar en las plataformas de tecnología que el ingreso se realice con la vinculación directamente de las credenciales de los usuarios de directorio activo.

Manejo de contraseñas para administradores de tecnología.

Los usuarios administradores y sus correspondientes contraseñas a las consolas administrables se dejan en custodia en sobre sellado en el área segura donde designe la Superintendencia de Notariado y Registro, las credenciales allí contenidas deben ser modificadas de manera mensual o cuando amerite.

Las contraseñas referentes a las cuentas “predefinidas” incluidas en los sistemas o aplicaciones adquiridas deben ser desactivadas. Al no ser posible su desactivación, las contraseñas deben ser cambiadas después de la instalación del producto.

El personal de la OTI no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del jefe de OTI.

Los usuarios y claves de los administradores de sistemas y del personal de la OTI son de uso personal e intransferible.

El personal de la OTI debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la Superintendencia de Notariado y Registro de acuerdo con el rol asignado.

Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el jefe de la OTI o el asesor asignado por el Comité de Seguridad de la Información de la SNR para asumir este rol.

Política de uso de discos de red o carpetas virtuales.

Asegurar la operación correcta y segura de los discos de red o carpetas virtuales.

Las Directrices de uso de discos de red o carpetas virtuales se encuentran definidas en el documento de lineamiento de uso de servicios de la OTI.

Política de uso de puntos de red de datos (red de área local –LAN).

Las direcciones internas, configuraciones e información relacionada con la topología y diseño de los sistemas de comunicación y redes de la Superintendencia de Notariado y Registro serán restringidas, de tal forma que no sean conocidas por usuarios internos, clientes o personas ajenas sin la previa autorización escrita de la OTI.

Todas las conexiones a redes externas, que accedan a la red interna de la Superintendencia de Notariado y Registro pasarán a través de un punto adicional de control como: firewall, Gateway, o servidor de acceso.

Los usuarios que tengan acceso a direcciones IP públicas, no pueden establecer conexiones a redes de acceso a información privadas, a menos que hayan sido aprobadas de manera escrita por la OTI.

Segregación en redes.

La infraestructura tecnológica de La Superintendencia de Notariado y Registro que soporta aplicaciones debe estar separada en segmentos de red físicos y lógicos e independientes de los segmentos de red de usuarios, de conexiones con redes con terceros y del servicio de acceso a Internet. La separación de estos segmentos debe ser realizada por medio de elementos de conectividad perimetrales e internos de enrutamiento y de seguridad.

Control de Acceso Remoto.

La administración remota de equipos o de la infraestructura de cómputo debe dejar evidencia escrita de la justificación por las que se asigna, al igual que de la responsabilidad que tiene el funcionario a quien se otorga este permiso, la solicitud debe ser realizada por el jefe del área correspondiente y debe ser avalada por la OTI.

Política de controles criptográficos

Implementar directrices para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

Cualquier usuario interno o externo que requiera acceso remoto a la red y a la infraestructura de cómputo de la Superintendencia de Notariado y Registro, sea por cualquier medio tecnológico existente, siempre debe estar autenticado y sus conexiones deberán estar cifradas.

Toda información que se extraiga de los aplicativos misionales debe estar cifrada para evitar que la misma pierda su confidencialidad.

Política de Seguridad Física

La OTI debe tener implementadas, alarmas de detección de intrusos en los centros de datos y centros de cableado de la Superintendencia de Notariado y Registro.

La SNR a través de la OTI, debe mantener actualizado el programa de seguridad física de las instalaciones, así como el programa de mantenimiento de las barreras de seguridad (Perimetrales e internas) de las instalaciones pertenecientes a la Superintendencia de Notariado y Registro.

Todas las áreas destinadas al procesamiento, almacenamiento de documentos o información, así como aquellas en las que se encuentren los equipos de cómputo y demás infraestructura de los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Por tanto, contarán con medidas de control de *acceso físico* en el perímetro, de tal forma que puedan ser auditadas con procedimientos de seguridad operacionales, que permitan proteger la información.

Políticas de seguridad del centro de datos y centros de cableado.

Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

En las instalaciones del centro de datos o de los centros de cableado, no está permitido:

- Fumar dentro del Data Center.
- Introducir alimentos o bebidas al Data Center
- El porte de armas de fuego, corto punzantes o similares.
- Mover, desconectar y/o conectar equipo de cómputo sin autorización.
- Modificar la configuración del equipo o intentarlo sin autorización.
- Alterar software instalado en los equipos sin autorización.
- Alterar o dañar las *etiquetas de identificación* de los sistemas de información o sus conexiones físicas.

- Extraer información de los equipos en dispositivos externos.
- Abuso y/o mal uso de los sistemas de información.
- Toda persona debe hacer uso únicamente de los equipos y accesorios que les sean asignados y para los fines que se les autorice.
- Los centros de cómputo deben mantener las condiciones físicas y ambientales óptimas recomendadas, así como controles automáticos para incendio, temperatura y cuando sea posible, monitoreo por Circuito Cerrado de Televisión.

Políticas de seguridad de los equipos informáticos.

Con el fin de actuar contra eventos que pongan en riesgo la integridad y confidencialidad de la información, los equipos de cómputo de la Superintendencia de Notariado y Registro deben permanecer conectados a las instalaciones eléctricas apropiadas de corriente regulada, fase, neutro y polo a tierra, para evitar pérdidas o daños de la información.

No se permite el ingreso sin autorización a los equipos en donde se encuentren alojados los Sistemas de Información de Superintendencia de Notariado y Registro, que estén protegidos con medidas de seguridad y políticas de restricción de acceso o que no me haya sido asignada su utilización.

En caso de que el equipo de cómputo deba ser retirado de las instalaciones de la Superintendencia de Notariado y Registro, el usuario solicitará autorización previa a la Grupo de sistemas, con el visto bueno del jefe o encargado del área que tenga a cargo el equipo, entregando debidamente diligenciados los formatos respectivos que para ello disponga la OTI.

Se debe informar oportunamente a la OTI de la Superintendencia cualquier falla en los equipos de cómputo que se detecte, para ello se hará uso del aplicativo de la mesa de servicio, sin embargo, en caso de ser un daño que impida el acceso a la misma, se podrá informar de manera presencial el daño a esta o realizar una llamada telefónica reportando la novedad.

Política de escritorio y pantalla limpia.

Los funcionarios, servidores públicos, contratistas, personas en comisión, pasantes y terceros que tienen algún vínculo con la Superintendencia de Notariado y Registro, deben conservar su escritorio libre de información, propia de la entidad que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.

Los usuarios de la entidad deben bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo y cerrar las aplicaciones y servicios de red cuando ya no los necesiten.

No se debe utilizar fotocopiadoras, escáneres, equipos de fax, cámaras digitales y en general equipos tecnológicos que se encuentren desatendidos.

Al imprimir documentos con información pública reservada y/o pública clasificada (semiprivada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

Política de Seguridad de las Operaciones de TIC.

Con el fin de asegurar las operaciones la Superintendencia estableció un plan para la implementación de procedimientos y políticas, los cuales se encuentran especificados en la caracterización del sistema de gestión de seguridad de la información de la entidad que se encuentra en el repositorio:

Macroproceso SIG/ SGSI/ Caracterización

Paulatinamente se definirán e implementarán o ajustarán procedimientos, registros e instructivos de trabajo debidamente documentados, con el fin de asegurar el mantenimiento y operación adecuada de la infraestructura tecnológica, en los cuales cada procedimiento tendrá un responsable para su definición, mantenimiento e implementación.

Para la gestión de las operaciones de la infraestructura de procesamiento de información, la OTI con el apoyo de las áreas, establecerá mecanismos que permitan segregar las funciones de administración (sistemas operativos, bases de datos y aplicaciones), monitoreo y operación, separando entre estos los diferentes ambientes de desarrollo, pruebas y producción.

No deberán realizarse pruebas, instalaciones o desarrollos de software, directamente sobre el entorno de producción, con el fin de evitar problemas de disponibilidad o confidencialidad de la información.

Si se llegaran a utilizar datos reales en el ambiente de producción, se debe definir el protocolo de seguridad que permita salvaguardar la integridad de la información de estos.

Política de respaldo y restauración de información.

La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información y solicitadas a través de la herramienta de gestión de requerimientos establecida por la Superintendencia de Notariado y Registro.

Semanalmente, los administradores de la plataforma de backup de la Superintendencia de Notariado y Registro, verificarán la correcta ejecución de los procesos de backup, suministrarán las cintas requeridas para cada trabajo y controlarán la vida útil de cada cinta o medio empleado.

Los medios que vayan a ser eliminados o que cumplan el periodo de retención deben surtir un proceso de borrado seguro y posteriormente serán eliminados o destruidos de forma adecuada.

El administrador de la plataforma de backup de la Superintendencia de Notariado y Registro, debe generar tareas de restauración aleatorias de la información y deben ser documentadas.

La información previamente definida y contenida en los servidores de la Superintendencia de Notariado y Registro se respaldará de forma periódica, determinada según el procedimiento "Gestión de copias de respaldo y Backup de Información" y los medios que se consideren necesarios, se almacenarán en una custodia externa que cuente con mecanismos de protección ambiental como detección de humo incendio, humedad, y mecanismos de control de acceso físico. Adicionalmente, se realizarán pruebas periódicas de recuperación y verificación de la información almacenada en los medios con el fin de verificar su integridad y disponibilidad.

Política para realización de copias en estaciones de trabajo de usuario final

Todos los usuarios son responsables de realizar una copia de respaldo del original de la información de valor, confidencial o crítica a su cargo, si el usuario no está seguro de cómo realizar esta operación debe comunicarse con la mesa de ayuda tecnológica para que se le indiquen los procedimientos. Estas copias separadas deben ser efectuadas con la periodicidad requerida de acuerdo con los cambios que se presenten en la información.

El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.), pueden ocasionalmente generar riesgos para la Superintendencia de Notariado y Registro al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada. Para utilizar dispositivos de almacenamiento externo se debe obtener aprobación formal.

Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información, excepto aquellos que se encuentren habilitados los privilegios de escritura por puertos USB y el agente del cliente fuga de información DLP instalado, el cual mantendrá el cliente DLP instalado el cual mantendrá un registro de los archivos copiados.

Todos los mensajes son sujetos a análisis frente a amenazas y ataques dirigidos, y pueden ser conservados, puestos en cuarentena y/o eliminados permanentemente por parte de la Superintendencia de Notariado y Registro.

Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

Los servidores públicos y contratistas de la Superintendencia de Notariado y Registro deberán informar inmediatamente al Comité de Seguridad de la Información mediante la mesa de ayuda, cualquier

situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.

El Comité de Seguridad de la Información será el encargado de realizar la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

Política de control de software operacional de la Superintendencia de Notariado y Registro.

Los responsables de la administración de las plataformas de producción están obligados a controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en ellas, así como a la programación de las actualizaciones necesarias a realizar.

No se permitirá la instalación de herramientas de desarrollo ni programas fuente en los sistemas de producción, a menos que sea autorizado por el Comité de Seguridad de la información y la OTI.

No se permitirá el uso de versiones de software en los sistemas de producción que no sean soportadas por los fabricantes, ni versiones de prueba que no hayan sido liberadas al mercado (Beta), a menos que sea autorizado por el Comité de Seguridad de la Información y la OTI.

Los usuarios no están autorizados a cambiar la configuración, a desinstalar software, formatear o restaurar de fábrica los equipos móviles institucionales, cuando se encuentran a su cargo, únicamente se deben aceptar y aplicar las actualizaciones.

Política de gestión de vulnerabilidades.

La Superintendencia de Notariado y Registro efectúa gestión de vulnerabilidades, detección, clasificación y plan de mitigación.

Una vez identificadas las vulnerabilidades técnicas potenciales, la Superintendencia de Notariado y Registro identificará los riesgos asociados y los controles de seguridad a ser tenidos en cuenta (esta acción puede implicar la actualización de sistemas vulnerables y/o aplicación de las medidas de acción necesarias).

El Comité de Seguridad de la información realizará el seguimiento y verificación de que se hayan corregido las vulnerabilidades identificadas, apoyándose para ello en el grupo de atención de incidentes de seguridad de la Superintendencia de Notariado y Registro (SSNR).

Política de seguridad de las comunicaciones.

La Superintendencia de Notariado y Registro a través del Comité de Seguridad de la información y soportado por el equipo de respuesta a incidentes, identificará los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión sobre los servicios de red, incluyendo los mismos en los contratos establecidos con sus contratistas.

Política para la transferencia de información.

La OTI realiza el control del uso de sistemas de transferencia de archivos vía FTP a terceros.

Las directrices para transferencia de información se encuentran definidas en el documento de lineamientos para acuerdos de transferencia de información que hace parte del sistema integrado de gestión.

Política de uso de correo electrónico

Se prohíbe enviar o reenviar cadenas de correo, mensajes con contenido religioso, político, racista, sexista, pornográfico, publicitario no corporativo o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y/o que inciten a realizar prácticas ilícitas o promuevan actividades ilegales incluido el lavado de activos.

La cuenta de correo electrónico deberá ser usada para el desempeño de las funciones asignadas dentro de la Superintendencia de Notariado y Registro y únicamente se podrán enviar correos electrónicos relacionados con asuntos de la Entidad.

Los mensajes y la información contenida en los buzones de correo son de propiedad de la Superintendencia de Notariado y Registro. El usuario podrá crear un histórico de su correo siempre y cuando sea almacenado en el disco duro del usuario y bajo su propia responsabilidad.

Política de uso de mensajería instantánea y redes sociales

La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Superintendencia de Notariado y Registro que sea creado a nombre personal en redes sociales como: Twitter®, Facebook®, YouTube® LinkedIn®, blogs, Instagram, etc., se considera fuera del alcance de las políticas establecidas y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Toda información distribuida en las redes sociales que sea originada por la Superintendencia de Notariado y Registro debe ser autorizada por los jefes de área para ser socializadas y con un vocabulario institucional.

Política adquisición, desarrollo y mantenimiento de sistemas de información

La supervisión y seguimiento a proyectos de infraestructura informática deben incorporar como un elemento básico de la supervisión, el cumplimiento de la aplicación de políticas de seguridad, tanto en el

desarrollo de la solución como en el producto final que será entregado a la Superintendencia de Notariado y Registro.

Todos los desarrollos de software deben surtir una fase de pruebas de funcionalidad, en la cual se evidencien los controles establecidos, en relación con la integridad de la información que será ingresada una vez se lleve a cabo su implementación.

Los desarrollos de software deben involucrar la correspondiente documentación interna y externa que permitan identificar su seguimiento hasta el nivel de rutinas y procedimientos.

Se debe contemplar en el desarrollo de aplicaciones para la Superintendencia de Notariado y registro los requisitos de seguridad en aplicaciones como arquitectura:

- Verificar que todos los componentes de la aplicación, bibliotecas, módulos, frameworks, plataformas y sistemas operativos se encuentran libres de vulnerabilidades conocidas.

- Requisitos de verificación de autenticación, gestión de sesiones, control de acceso, manejo de entrada de datos maliciosos, criptografía, gestión de registro y errores, seguridad de las comunicaciones, y protección de datos entre otros.

Política de Tercerización u Outsourcing.

Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la Superintendencia de Notariado y Registro.

Se debe establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad de la información de la Superintendencia de Notariado y Registro, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios. En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad de la información.

Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la Superintendencia de Notariado y Registro.

La OTI deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a sus sistemas de información. Se debe identificar y monitorear los riesgos relacionados con

los contratistas o proveedores en relación con los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.

Se deben identificar los riesgos para la información y los servicios de procesamiento de información que involucren partes externas a la Superintendencia de Notariado y Registro.

El resultado del análisis de riesgos será la base para el establecimiento de los controles y debe ser presentado al Comité de seguridad de la Información antes iniciar el estudio de mercado y publicación del proyecto de pliegos del contrato de outsourcing en el portal de contratación.

Los funcionarios de la Superintendencia de Notariado y Registro que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas, conformes al manual de contratación de la SNR.

Se deben establecer mecanismos o condiciones con los contratistas o proveedores que permitan realizar la gestión de cambios en los servicios suministrados.

Política de Gestión de los Incidentes de la Seguridad de la Información.

El Comité de Seguridad de la Información a través del equipo de respuesta de atención de incidentes de seguridad de la información, será el encargado de gestionar mediante la ejecución del procedimiento de gestión de incidentes, realizar el tratamiento, la investigación y seguimiento a los eventos e incidentes de seguridad reportados.

Todos los incidentes de seguridad reportados serán investigados y se les hará seguimiento por parte del Comité de Seguridad de la Información.

Los resultados de las investigaciones serán informados a la Superintendencia de Notariado y Registro, especificando las causas, consecuencias, responsabilidades, solución y acciones para evitar que se presenten nuevamente.

La Superintendencia de Notariado y Registro, como mecanismo para la gestión de incidentes. Ejecutará las etapas de prevención, protección, detección, respuesta, comunicación, recuperación y aprendizaje. De conformidad a lo establecido en la Resolución No.500 de marzo 10 de 2021 del Ministerio de Tecnologías de la Información y las Comunicaciones en su artículo 9, para lo cual la SNR:

1. Gestionará los incidentes de seguridad digital, para lo cual se creará una bitácora que contenga la descripción de cada una de las actividades desarrolladas.

2. Designará dentro de la Entidad los responsables de gestionar y dar respuesta a los incidentes de Seguridad digital, el cual será liderado por el responsable de seguridad digital.

3. Una vez identificado el incidente de seguridad digital se reportará a la instancia correspondiente según el caso.

4. Los incidentes catalogados como menos graves y menores, serán comunicados al CSIRT Gobierno en el formulario establecido, una vez sea gestionado.

5. Una vez analizada la causa raíz de los incidentes presentados se realizaran los planes de mejoramiento a que haya lugar, y se efectuará el respectivo seguimiento, para lo cual el responsable de seguridad digital de la entidad supervisará y hará seguimiento a su cumplimiento.

Política de cumplimiento de requisitos legales y contractuales.

La Superintendencia de Notariado y Registro respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la Superintendencia de Notariado y Registro, relacionada con la seguridad de la información.

La Superintendencia de Notariado y Registro, establecerá el procedimiento para protección de derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los recursos de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

La OTI realizará el procedimiento de copias de respaldo (backups) de los registros alojados en los sistemas de información.

Las dependencias de la Superintendencia de Notariado y Registro que tratan con datos personales de funcionarios, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Superintendencia de Notariado y Registro, así mismo los Jefes de las dependencias deben asegurar que tendrán acceso a los datos personales únicamente los funcionarios que tengan una necesidad laboral legitima.

Se respetarán los requisitos legales y reglamentarios relacionados con las políticas de privacidad y protección de datos (Ley 1273 de 2009 y Ley 1581 de 2012).

El uso indebido de la información proporcionada a los contratistas por la Superintendencia de Notariado y registro en el desarrollo de sus actividades, o su divulgación a terceros sin previa autorización, dará lugar a que se inicie las acciones civiles y/o penales que se originen por violación al derecho de autor (ley 23 de 1982).

La información manipulada por el contratista en desarrollo de sus actividades será de tipo confidencial, los informes, productos, desarrollos y en general los resultados de la ejecución del contrato, serán de propiedad intelectual de la Superintendencia de notariado y registro, los contratistas y funcionarios ceden a la Superintendencia los derechos patrimoniales e intelectuales que pueda tener sobre los mismos.

Política de Teletrabajo.

La Superintendencia de Notariado y Registro garantizará la seguridad de la información cuando se haga uso de los activos tecnológicos y recursos de la institución para actividades relacionadas con teletrabajo según lo estipulado en el artículo 2 de la Ley 1221 de 2008.

Antes de realizar actividades relacionadas con teletrabajo, se debe definir el alcance de las actividades a desarrollar, teniendo en cuenta los activos de información requeridos para realizar el trabajo, el horario, los servicios que se van a utilizar y la información a la que el funcionario o contratista tendrá derecho a acceder.

Para situaciones extraordinarias relacionadas a estados de emergencia como terremotos, atentados, pandemias se aplicará la Ley 1221 con excepciones como la verificación del puesto de trabajo por parte de la Asesora de Riesgos Laborales o la verificación física de las condiciones de trabajo del teletrabajador, estas excepciones están contempladas por el sistema de gestión de seguridad en el trabajo de la Superintendencia de Notariado y Registro.

Política de Trabajo de Casa

La Superintendencia de Notariado y Registro garantizará la seguridad de la información cuando se haga uso de los activos tecnológicos y recursos de la institución para actividades relacionadas con trabajo en casa, según lo estipulado en el artículo 8 de la Ley 2088 de 2021.

Antes de realizar actividades relacionadas con trabajo en casa, se definirá el alcance de las actividades a desarrollar, teniendo en cuenta los activos de información requeridos para realizar el trabajo, el horario, los servicios que se van a utilizar y la información a la que el funcionario o contratista tendrá derecho a acceder a los equipos, sistemas de información, software o materiales necesarios para el desarrollo de la función.

De conformidad a lo establecido en el artículo 2 de la Ley 2088 de 2021, el Trabajo en casa está dado para que el servidor público desempeñe transitoriamente sus funciones, cuando se presenten circunstancias ocasionales, excepcionales o especiales que impidan que el trabajador pueda realizar sus

funciones en su lugar de trabajo. En este caso, la Superintendencia de Notariado y Registro definirá los criterios y responsabilidades en cuanto al acceso y cuidado de los equipos, así como respecto a la custodia y reserva de la información de conformidad con la normativa vigente sobre la materia.

Política de Revisiones de Seguridad de la Información

La Superintendencia de Notariado y Registro realiza auditorias con personal externo e interno a la Superintendencia de Notariado y Registro al sistema de gestión de seguridad de la información, para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la información. Los altos directivos, altos consejeros, consejeros, directores, secretarios, Jefes de Oficina, Jefes de Área deben verificar y supervisar el cumplimiento de las políticas de seguridad de la información en su área de responsabilidad.

La Superintendencia de Notariado y Registro asignará un funcionario para realizar revisiones esporádicas no programadas con el fin verificar el cumplimiento de las políticas de seguridad de la información en las instalaciones.

La OTI debe establecer el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.

Política de retención y archivo de datos.

La política de retención de archivos establece cuánto tiempo se deben mantener almacenados los archivos en la Superintendencia de Notariado y Registro de acuerdo con las tablas de retención documental.

Las reglas y los principios generales que regulan la función archivística del Estado se encuentran definidos por la ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.

La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

Política de tratamiento de datos personales.

Para el tratamiento de datos personales se tendrán en cuenta las siguientes definiciones, las cuales han sido tomadas textualmente de la Ley 1581 de 2012

a) Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

b) Base de Datos: Conjunto organizado de datos personales que sea objeto de Tratamiento.

c) Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

d) Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del responsable del tratamiento.

e) Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

f) Titular: Persona natural cuyos datos personales sean objeto de Tratamiento.

g) Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

El objetivo de esta política es establecer los lineamientos para administración y tratamiento de datos personales en la Superintendencia de Notariado y Registro.

La Superintendencia adoptará como lineamiento para la protección de datos personales los preceptos establecidos en la Ley 1581 de 2012, para ello propenderá por el cumplimiento de los siguientes deberes:

La SNR pedirá de manera explícita, solicitud para el tratamiento de datos personales con el fin de lograr el consentimiento del titular de estos para poder almacenar, recolectar, usar, transferir compartir, suprimir y actualizar su información.

Garantizar al Titular de los datos el pleno y efectivo ejercicio del derecho de hábeas data.

Implementar las medidas necesarias para garantizar que los datos solicitados para tratamiento al titular de estos sean pertinentes y no excesivos conforme a la finalidad para la cual han sido recogidos.

Informar al titular de los datos en caso de que este lo solicite, el lugar en donde van a estar almacenados, quien es el responsable de su tratamiento y como se va a gestionar esa administración.

La Superintendencia tomará las medidas necesarias para mantener seguros datos especialmente sensibles como Fichas de memoria, hojas de vida, datos de ideología, afiliación sindical, creencias, salud, vida social, o partido político.

No se podrán ceder datos personales a un tercero sin consentimiento del titular de estos.

Se garantizará el derecho a los titulares de los datos para el acceso, rectificación, cancelación, oposición y supresión de datos.

La Superintendencia podrá solicitar información adicional cuando se dude de la titularidad de la persona que Solicita datos personales.

La Superintendencia exigirá políticas de tratamiento de datos personales a los proveedores que por su naturaleza tengan acceso a la información de la entidad.

La Superintendencia se compromete a mejorar las condiciones de conservación de la información con el fin de reducir el riesgo de pérdida, modificación no autorizada, o acceso de carácter fraudulento.

Cuando se presenten violaciones a la seguridad de la información y en particular a las directrices contenidas en este se deberá Informar de manera inmediata a la autoridad de protección de datos.

Esta Superintendencia se abstendrá de realizar transferencias de datos personales a países que no tengan niveles adecuados de protección de datos personales.

El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor, en concordancia con lo establecido por la Ley 1098 de 2006 “Código de Infancia y Adolescencia”.

La Política General de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

Se restringirá el acceso a Datos Personales de terceros y únicamente lo podrán hacer aquellos funcionarios que para la realización de sus labores les sea estrictamente necesarios.

En caso de que la Superintendencia de Notariado y Registro decida seleccionar a un tercero para el tratamiento de sus datos personales la selección se hará bajo parámetros de idoneidad como experiencia y códigos de conducta.

Procedimientos que apoyan la política de seguridad.

Procedimiento de control de documentos.

Garantiza que la entidad cuenta con los documentos estrictamente necesarios a partir de su perfil de actuación en cada momento y maneja la dinámica del mejoramiento, mostrando la realidad que atraviesa la Superintendencia de Notariado y Registro en cada momento, porque incorpora la eficacia de las diferentes acciones, a través de la revisión documental y del cumplimiento de los requisitos idénticos en los diferentes modelos de gestión sobre el control de documentos. Así mismo, busca garantizar que los documentos en uso sean confiables y se mantengan actualizados, una vez se evidencie la eficacia de las acciones correctivas, preventivas y de mejora que hacen que los procesos se ajusten y evolucionen; de

igual manera que los documentos existentes en el momento de la evaluación y comprobación del cambio que se implementó como solución a un problema, riesgo o a una oportunidad se conserven.

Procedimiento de control de registros

Está definido para evidenciar las acciones realizadas y los resultados obtenidos en la ejecución de las actividades, con el fin de analizar los datos, y lo que es más importante, para la toma de decisiones, de tal forma que registro que no aporta valor o no lleva a una decisión de mejora o de acción, no se debe tener en el sistema, ya que lo único que haría es desgastar a la organización y generar residuos sólidos como papel mal utilizado.

Procedimiento de auditoría interna

La auditoría interna es una herramienta para la alta dirección, en el momento de determinar la eficacia y la eficiencia del sistema de gestión, a través de la identificación de las fortalezas y debilidades. Esta es la razón por la cual se recomienda siempre realizar auditorías internas antes de llevar a cabo la revisión gerencial, ya que para esta última se requiere información sobre el sistema y los procesos, de tal manera que se pueda evaluar la adecuación, la conveniencia y la eficacia del sistema de gestión. Se hacen auditorias para evaluar la conformidad con las políticas de la organización, para evaluar el nivel de implementación del sistema de gestión, para evaluar el estado de mantenimiento y la capacidad de mejoramiento del sistema de gestión.

Procedimiento de acción correctiva

El objetivo de este procedimiento es definir los lineamientos para eliminar la causa de no conformidades asociadas con los requisitos de la política de seguridad de la Superintendencia de Notariado y Registro, así como: definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones correctivas necesarias para evitar que se repita la no conformidad.

Procedimiento de acción preventiva

El objetivo de este procedimiento es definir los lineamientos para identificar, registrar, controlar, desarrollar, implantar y dar seguimiento a las acciones preventivas generadas por la detección de una no conformidad real o potencial en el sistema de gestión de seguridad de la información y eliminar sus causas.

Procedimiento de revisión de la Política de Seguridad de la Información

El objetivo de este procedimiento es revisar, por parte de la dirección o su representante las Políticas de Seguridad de la Información de la Superintendencia de Notariado y Registro, al menos una vez al año, y/o cuando ocurran cambios significativos en la Entidad., para asegurar su conveniencia, eficiencia y eficacia continúa.

Los usuarios de la Superintendencia de Notariado y Registro pueden consultar las descripciones detalladas de cada procedimiento a través del sistema integrado de gestión o la OTI.

Gestión de la continuidad del negocio.

Se debe desarrollar e implantar un plan de gestión de la continuidad del negocio para asegurar que la Superintendencia de Notariado y Registro restaure, dentro de escalas de tiempo razonables y aceptadas por la entidad, sus servicios de información.

La Superintendencia de Notariado y Registro deberá tener definido un plan de acción el cual estará definido en el DRP (Disaster Recovery Plan) que permita mantener la continuidad de sus funciones teniendo en cuenta los siguientes aspectos:

- Identificación y asignación de prioridades a los procesos críticos de TI, establecimiento de tiempos de recuperación identificación de recursos, disposición de los RTO/RPO (Recovery Time Objective / Recovery Point Objective), Evaluación de Impactos Operacionales, identificación de procesos alternos y generación de un informe de impacto del negocio sobre la Superintendencia de Notariado y Registro de acuerdo con la misión de la entidad.

- El plan de recuperación del negocio de acuerdo con la estrategia definida anteriormente deberá documentarse.

- Plan de pruebas de la estrategia de continuidad del negocio.

La alta dirección de la Superintendencia de Notariado y Registro se encargará de la definición y actualización de las normas, políticas, procedimientos y estándares relacionados con la continuidad de la prestación del servicio, igualmente velará por la implantación y cumplimiento de estas.

Cumplimiento

Los diferentes aspectos contemplados en esta Política son de obligatorio cumplimiento para todos los funcionarios, personal en comisión permanente, contratistas y otros colaboradores de la Superintendencia de Notariado y Registro.

En caso de que se violen las políticas de seguridad ya sea de forma intencional o por negligencia, la Superintendencia de Notariado y Registro, tomará las acciones disciplinarias y legales correspondientes.

La Política de Seguridad de la Información debe prevenir el incumplimiento de las leyes, estatutos, regulaciones u obligaciones contractuales que se relacionen con los controles de seguridad.

Controles

La implementación de la Política de Seguridad de la Información de la Superintendencia de Notariado y Registro esta soportada sobre la reingeniería de procesos que actualmente adelanta la Entidad y se documentará paulatinamente. Los usuarios de los servicios y recursos de tecnología de la Superintendencia de Notariado y Registro pueden consultar los procedimientos a través del Portal Institucional de la Superintendencia de Notariado y Registro.

RESPONSABLE DEL DOCUMENTO

Jefe Oficina Tecnologías de la Información / Jefe Oficina Asesora de Planeación.

VERSIÓN DE CAMBIOS			
Código:	**Versión:**	**Fecha:**	**Motivo de la actualización:**
N.A. N.A.	1.1 1.2	Abril -2020 Mayo 27 - 2021	Creación de Política de seguridad corporativa Actualización según observaciones comité.

ELABORACIÓN Y APROBACIÓN					
ELABORÓ		**APROBÓ**		**Vo.Bo Oficina Asesora de Planeación**	
Ing. Dario David Peña Ing. Miguel Felizzola Figueredo Ing. Leyla Guzmán Rodríguez	Contratista líder Seguridad SNR Contratista Asesor Seguridad Profesional Oficina de Tecnologías de la Información.	Ing. Luis Gerardo Cubides Silva. Comité de Gestión Institucional de Gestión y Desempeño No.002 del 2021.	Jefe Oficina Tecnologías de la Información. Comité de Gestión Institucional de Gestión y Desempeño No.002 del 2021.	Dr. Juan Carlos Torres R. Dra. Ceidy Ortiz E. Dra. Laura Marcela Rengifo Rodríguez	Jefe Oficina Asesora de Planeación. (e) Profesional especializado OAP Asesora del Despacho.
Fecha: 20-05 -2021		**Fecha:**		**Fecha: 20-05-2021**	