POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

INDICE

1. INTRODUCCIÓN.

La Política de Seguridad de la Información física o electrónica de la notaría es la agrupación de procedimientos y normas que orientan y soportan la gestión de la seguridad de la información. La información es un activo de gran valor, razón por la que se debe tener conciencia de la importancia que representa y las consecuencias que pueden traer la pérdida, alteración, acceso no autorizado o mal intencionado. Como la información de la notaría no se escapa de amenazas, como: desastres naturales, incendio, inundación, sabotaje, vandalismo, robo, posibilidad de daños y pérdidas por causa de códigos maliciosos, ataques de denegación de servicios o simplemente mal uso; a través de este documento se establecen y proporcionan directrices para que todos los que hagan uso de ella, conozcan, respeten y cumplan la Política de Seguridad de la Información.

La notaría protege los datos y la información con estrategias que permitan su administración y control para garantizar la seguridad, autenticidad, confidencialidad, disponibilidad e integridad. La notaría implementa, hace seguimiento, aplica y mejora continuamente la Política de Seguridad de la Información, asegurando y protegiendo los datos y la información frente a las diversas amenazas, lo cual contribuye a minimizar riesgos asociados de daño y a garantizar el cumplimiento de los objetivos de la notaría, el de su clientela, personas usuarias y terceras personas.

La notaría toma como base fundamental para la elaboración del Sistema de Gestión de Seguridad de la Información, las leyes y demás regulaciones legales aplicables vigentes en Colombia, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

2. OBJETIVO.

La notaría implementa, mantiene vigente y actualizada la Política de Seguridad de la Información, asegurando su eficacia para preservar, proteger y administrar efectivamente la Información y las tecnologías que se utilizan para sus procesamientos, frente a todas las amenazas accidentales o deliberadas que se puedan presentar, de tal forma que se garantice la integridad, disponibilidad, legalidad, actualización, no repudio, confidencialidad y seguridad de dicha información en la ejecución de trámites y prestación de servicios notariales presenciales o digitales.

3. ALCANCE.

La Política de Seguridad de la Información, como parte de Sistema de Gestión de Seguridad de la Información-SGSI, está dirigida, tiene alcance y se aplica a todas las personas, recursos y procesos internos o externos que componen o tienen que ver con la información y los datos que la notaría recopila, produce, procesa, administra o transfiere, mediante la ejecución de trámites y prestación de servicios notariales presenciales o digitales. La Política de Seguridad de la Información debe ser cumplida por la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que hagan uso de la información y los datos, asegurando su calidad,

protección y seguridad y generando las medidas preventivas y correctivas necesarias para conseguir el logro del objetivo de esta Política.

4. APLICABILIDAD DE LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN.

Las políticas del SGSI estipuladas en este manual aplican y son de obligatorio cumplimiento para la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de la notaría.

5. TÉRMINOS Y DEFINICIONES.

Accesos autorizados: autorizaciones concedidas a una persona usuaria y/o empleados/empleadas para la utilización de los diversos recursos, sin que pueda utilizarlos para fines propios.

Acción correctiva: remediación de los requisitos o acciones que dieron origen al establecimiento de no una 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 de información: son aquellos recursos (hardware y software) con los que cuenta la notaría. Es decir, todo elemento que compone el proceso completo de comunicación, partiendo desde la información, el emisor, el medio de transmisión y receptor. Estos pueden ser:

- **Datos:** son todos aquellos elementos básicos de la información, en cualquier formato, que se generan, recogen, gestionan, transmiten y destruyen.
- **Aplicaciones:** es todo el software que utiliza la notaría para la gestión de la información.
- **Personal:** es toda persona de la notaría, la gerencia o dirección, la coordinación, empleados/empleadas, subcontratada, clientela, personas usuarias y en general todas aquellas personas que tengan acceso de una manera u otra a los activos de información de la notaría.
- **Trámites y Servicios:** son aquellas acciones tanto internas -que se suministran dentro de la notaría- como las externas -que la misma suministra a la clientela y a personas usuarias.
- **Tecnología:** refiere al uso de equipos de herramientas, sistemas, plataformas, infraestructura, telecomunicaciones y computadoras (ordenadores) para la

transmisión, el procesamiento y el almacenamiento de datos. La noción abarca cuestiones propias de la informática, la electrónica y las telecomunicaciones.

Acto notarial electrónico: es la actuación que lleva a cabo notario/notaria a través de medios electrónicos, garantizando las condiciones de seguridad, interoperabilidad, integridad y accesibilidad necesarias.

Acuerdo de Confidencialidad: documento en los que la gerencia o dirección, la coordinación, empleados/empleadas, personas usuarias, personas proveedoras o terceras personas manifiestan su voluntad de mantener la privacidad de la información, comprometiéndose a no divulgar, usar o explotarla al tener acceso, en virtud de la labor que desarrollan.

Administración de riesgos: gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

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 notaría y cuyo objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que se prestan, de manera rápida y eficaz. No se limita a la solución de problemas específicos sino a buscar las causas que determinaron el incidente limitando el marco de acción de futuras ocurrencias.

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.

Amenaza: situación que puede desencadenar incidentes que comprometen los activos de información de la notaría.

Análisis de riesgos: a partir del riesgo definido, se define las causas del uso sistemático de la información para identificar fuentes y estimar el riesgo.

Autenticación: es el proceso que da la confianza o asegura que un recurso humano, sistema u objeto es realmente quien o lo que dice ser.

Autenticación digital notarial: es el procedimiento que, utilizando mecanismos de autenticación, permite a notario/notaria verificar los atributos digitales de una persona cuando adelanten actos notariales a través de medios digitales. Además, en caso de requerirse, permite tener certeza sobre la persona que ha firmado un mensaje de datos, o la persona a la que se atribuya el mismo en los términos de la Ley 527 de 1999 y sus normas reglamentarias, o las normas que la modifiquen, deroguen o subroguen.

Comité de Seguridad de la Información: grupo integrado por personas delegadas por la notaría con el propósito de garantizar la seguridad de los datos y la información. Su labor principal es estructurar, definir, implementar, hacer seguimiento y verificar la correcta aplicación de la Política de Seguridad de la Información.

Confiabilidad: se puede definir como la capacidad que tiene un producto para 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

Confidencialidad: hace referencia a la necesidad de ocultar o mantener secreta determinada información o recursos.

Control: son las prácticas, procedimientos, políticas, y estructuras organizativas que permiten mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Control de acceso: es el mecanismo o uso de sistemas automatizados de autenticación de la notaría, que solo permiten el acceso a los recursos de las tecnologías de la información a quienes tienen autorización.

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

Datos abiertos: son los datos sin procesar que se encuentran en formatos estándar y que facilitan su acceso, reutilización y están bajo la custodia de entidades públicas o privadas que ejercen con funciones públicas y son puestos a disposición de cualquier persona, de forma libre y sin restricciones, con el objeto de que terceras personas puedan reutilizarlos y crear servicios derivados de los mismos.

Dato personal: es la información vinculada o asociada a una o varias personas naturales determinadas o determinables.

Dato público: son datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Pueden estar contenidos, entre otros, en documentos públicos, registros públicos, boletines oficiales y gacetas o en sentencias judiciales que no estén sometidas a reserva.

Datos sensibles: son todos los datos que afectan la intimidad del Titular, entre otros, los relativos a sus datos biométricos, su salud, su vida sexual, los que revelen su orientación política, su origen étnico o racial, sus creencias religiosas, sus convicciones filosóficas, la pertenencia a organizaciones sociales, sindicatos, o de derechos humanos.

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.

Digitalización: el término “digitalización” se asocia con el de desmaterialización, entendida ésta como “el proceso por medio del cual un documento de papel o en cualquier otro formato análogo es transformado a un formato digital’. Podemos entender en sentido lato la desmaterialización, como un método por el cual la información contenida en un medio físico de lectura analógica es convertida por medios electrónicos o similares (particularmente a través del uso del lenguaje binario) a un formato electrónico, de manera que la información así reproducida sólo puede ser accesible por intermedio de un dispositivo computacional o similar.

Disponibilidad: garantía de poder usar la información cuando es requerida por un sujeto u objeto autorizado.

Escritura pública electrónica: es la escritura pública que nace como mensaje de datos garantizando la autenticidad, disponibilidad e integridad del documento, de conformidad con la ley 527 de 1999, además debe cumplir las normas sustanciales relativas a las diferentes actuaciones notariales que ella contiene y de los preceptos de derecho notarial, conforme al Decreto-ley 960 de 1970 y demás normas concordantes. procesales y se garantice la autenticidad, integridad e inalterabilidad de la información. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio

Evento: suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Firmante: persona que utiliza directamente su firma electrónica para otorgar actos o instrumentos notariales

Firma electrónica: métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente.

Firma digital: se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación2. Esta firma cuenta con el respaldo de una Entidad de Certificación digital.

Gestión de claves: controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos.

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: conjunto organizado de datos procesados, que constituyen un mensaje que cambia de estado el conocimiento del sujeto o sistema que recibe dicho mensaje. Toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que se genere en desarrollo de una actividad.

Información pública. es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal.

Información pública clasificada. es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en la ley.

Información confidencial es la información privada, generalmente en poder del Estado, cuyo acceso público se prohíbe por mandato constitucional o legal debido a un interés personal que está jurídicamente protegido. Es decir, la información referente a la intimidad personal y familiar, al honor y propia imagen, así como archivos médicos cuya divulgación constituye una invasión a la privacidad de la persona. A esta información sólo tendrán acceso las personas dueñas de ella.

Integridad: fidelidad de la información. Su objetivo es prevenir modificaciones impropias o no autorizadas de la información.

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.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 27001: estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ISO 27002: código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de Julio de 2007.

La coordinación del Comité de Seguridad de la Información: es la persona responsable del cumplimiento de la Política de Seguridad de la Información.

La gerencia o dirección: persona encargada de administrar la notaría o una de sus dependencias. Estas pueden ser: La gerencia, jefatura jurídica, o la jefatura de alguna de las dependencias de la notaría.

Legalidad: el principio de legalidad o primacía de la ley es un principio fundamental del derecho público 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. Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, seguridad de información, seguridad informática y garantía de la información.

Medida correctiva: acción de tipo reactivo orientada a eliminar la causa de no conformidad asociada a la implementación y operación del sistema de gestión de la seguridad de la información con el fin de prevenir su repetición.

Medida preventiva: acción de tipo proactivo orientada a prevenir potenciales no conformidades asociadas a la implementación y operación del SGSI.

Medio electrónico: mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía y móvil u otras.

Medio de procesamiento: mecanismo o recurso utilizado para implementar o aplicar técnicas eléctricas, electrónicas o mecánicas para manipular datos e información para el empleo humano o de máquinas.

No-repudio: capacidad de aprobar un evento o una acción, de manera que este evento o acción no sea negado posteriormente.

Política de seguridad: documento por el cual se establece un compromiso de dirección y enfoque para la notaría. Documento que establece los procesos y procedimientos más relevantes para manejar el riesgo y mejorar la seguridad de la información de la notaría.

Recursos: todas aquellas fuentes que consultamos. Fuentes o suministros del cual se produce un beneficio.

Recursos de la información: medios y bienes que permiten adquirir, ampliar o precisar conocimientos con el fin de resolver la necesidad de una organización.

Registro de las personas usuarias: es el proceso que adelanta la notaría de forma presencial o virtual, mediante el cual las personas naturales o jurídicas se incorporan a los servicios que prestan esos despachos.

Riesgo: posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la Información: preservación de la confidencialidad, integridad y disponibilidad de la información, además también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no repudio, confiabilidad.

Sistema de Información: según la ISO/IEC 27002:20005 es la preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas. Es el conjunto de elementos ordenados cuyas propiedades se relacionan permitiendo el procesamiento, mantenimiento, recopilación, difusión y transmisión de información usando mecanismos manuales o automatizados.

Software malicioso: es un tipo de software que tiene como objetivo infiltrarse o dañar una computadora o sistema de información sin el consentimiento de su propietario.

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

Terceras personas: todas las personas, jurídicas o naturales, como las personas proveedoras, contratistas o consultoría, que provean servicios o productos a la notaría.

Virus: programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente a la persona usuaria y éste tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidad: puntos débiles de aplicaciones, equipos, personal, procesos y mecanismos de control que facilitan la concreción de una amenaza potencial o posibilidad de que se materialice una amenaza.

X-ROAD es una capa de intercambio de datos distribuidos que proporciona una forma estandarizada y segura de producir y consumir servicios. Adicionalmente, garantiza la confidencialidad, integridad e interoperabilidad entre las partes de intercambio de datos. Funciona como una capa intermedia entre los sistemas de información que intercambian información.

6. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La notaría garantiza la seguridad, confidencialidad, integridad y disponibilidad de los activos de la información y permite establecer mecanismos y procedimientos para asegurar el eficiente cumplimiento de las funciones y la labor de la gerencia o dirección, la coordinación, empleados/empleadas, personas usuarias y terceras personas, minimizando los riesgos y amenazas a los datos y a la información con la implementación, mantenimiento, control, divulgación y mejoramiento continuo de la Política de Seguridad de la Información.

6.1. POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

Para minimizar riesgos y garantizar la seguridad, confidencialidad, integridad y disponibilidad de los activos, la notaría establece reglas con las que se deben operar los recursos y procesos de la información mediante la implementación de la Política de Seguridad de la Información, con el objeto de asegurar una apropiada protección a la información que produce, procesa o administra la notaría.
Control 1: esta Política debe ser conocida y aplicada por la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas y en general por todas las personas usuarias de la información según las funciones o actuaciones que realicen y la relación que tengan con la notaría. La no aplicación de la Política de Seguridad de la información implica sanciones según el caso que se presente.

Control 2: la gerencia o dirección de la notaría deben crear un Comité de Seguridad de la Información, responsable de determinar, establecer, controlar, mantener, mejorar y asegurar la Política, para el correcto uso de los activos de información.

Control 3: este Comité debe estar conformado por una persona de la alta gerencia, una directiva y una de la coordinación del Comité que será nombrado por la gerencia, cuando exista el recurso humano; en caso contrario, se conformará por lo dispuesto por notario/notaria.

Control 4: la notaría definirá las políticas de seguridad de la información de acuerdo con lo que se identifique en el análisis de riesgos y sea aprobado por el Comité de Seguridad de la Información, para luego publicar y comunicar a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

6.1.1. RESPONSABLES DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

La gerencia o dirección de la notaría deben garantizar y apoyar el proceso de implementación, mantenimiento y actualización de la Política de Seguridad de la información de la Notaría.

Control 1: el Comité de Seguridad de la Información, la gerencia o dirección, la coordinación, y empleados/empleadas de la notaría son los responsables de la Política de Seguridad de Información y con el fin de minimizar y eliminar los riesgos a que se expone la información deben identificar dichos riesgos, para evitar que los activos de la información que produce, procesan o administra la notaría puede ser modificada, copiada, divulgada o destruida.

Control 2: la gerencia o dirección de la notaría y su Comité de Seguridad de la Información son responsables de las autorizaciones para las modificaciones, revisiones y actualizaciones que se hagan a los activos de la información y/o a la Política de Seguridad de la Información.

6.1.2. DOCUMENTAR LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN

La notaría debe documentar, actualizar e implementar periódicamente la Política de Seguridad de la Información para asegurar la confidencialidad, integridad, seguridad y disponibilidad de la información.

Control 1: el Comité de Seguridad de la Información es el responsable de crear el documento o manual de la Política de Seguridad de Información y velar por su obligatorio cumplimiento, el cual debe ser aprobado, publicado y comunicado a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tengan relación con los datos y la información, de acuerdo con su correspondencia.

Control 2: se debe garantizar que el Comité de Seguridad de la Información de la Notaría cuente con los documentos rigurosamente necesarios dependiendo el perfil de actuación de cada empleado/empleada y la dependencia en que se desempeña. Los documentos deben ser manejados y controlados asegurando su confidencialidad, integridad, seguridad y disponibilidad.

6.1.3. REVISIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN.

El Comité de Seguridad de la Información de la Notaría revisará, auditará, verificará que se cumpla y actualizará la Política de Seguridad de la Información para garantizar su idoneidad, eficiencia y efectividad.

Control: la notaría verificará que se definan, implementen, revisen y actualicen las Políticas de Seguridad de la Información conforme con la necesidad de la notaría y/o de las normas legales vigentes.

7. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN.

El Comité de Seguridad de la Información debe revisar y actualizar, periódicamente, la Política de Seguridad de la Información de la Notaría y presentarla a la gerencia para su correspondiente aprobación. Dicha actualización debe seguir las directrices y procedimientos estipulados en esta política y en los estándares y normas legales vigentes. También debe asegurar el debido proceso para el tratamiento, archivo y protección adecuada de la información que produce, procesa, administra o transfiere la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría crearán esquemas de seguridad de la información definiendo y estableciendo roles y responsabilidades de acuerdo con las actividades de gestión, operación o administración para garantizar y apoyar el proceso de implementación, operación, control, mantenimiento, revisión y mejora de la Política de Seguridad de la Información de la Notaría.

Control 2: el Comité de Seguridad de la Información debe definir las actividades y los resultados que espera obtener al aplicar estas políticas en cumplimiento de cada labor y conforme con las funciones, roles, responsabilidades y actuaciones asignadas en la notaría

a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

Control 3: el Comité de Seguridad de la Información debe garantizar el desarrollo, implementación, operación, control, mantenimiento, revisión, actualización y mejora de la Seguridad de la Información de la Notaría.

7.1. ORGANIZACIÓN INTERNA.

El Comité de Seguridad de la Información se encarga de manejar la seguridad de la información dentro de la notaría.

Control: El Comité de Seguridad de la Información de la Notaría definirá y asignará roles y responsabilidades a los empleados/empleadas de acuerdo con sus tareas.

7.1.1. COMPROMISO DE LA GERENCIA O DIRECCIÓN CON LA SEGURIDAD DE LA INFORMACIÓN.

La gerencia o dirección de la notaría deben apoyar activamente la seguridad de la información y al Comité de Seguridad de la Información de la Notaría, exponiendo claramente las instrucciones y asignando responsabilidades que contribuyan al buen manejo de la seguridad de la información.

Control: La gerencia o dirección de la notaría proveerá al Comité de Seguridad de la Información de la Notaría las herramientas necesarias para asegurar que sus empleados/empleadas cumplan con sus roles y responsabilidades como garantía de la seguridad de la información desde el ingreso de cada empleado/empleada hasta su retiro.

7.1.2. ASIGNACIÓN DE RESPONSABILIDADES DE LA SEGURIDAD DE LA INFORMACIÓN.

Toda información debe ser apropiadamente identificada, clasificada y documentada, para de esta forma definir los responsables, responsabilidades, custodia y permisos de acceso a la información de la notaría. La información debe clasificarse conforme a las guías de clasificación establecidas por el Comité de Seguridad de la Información y por las normas y estándares legales vigentes para el funcionamiento de la notaría.

Control: la notaría mantendrá un esquema de seguridad donde los roles y responsabilidades establecidos sean definidas y asignadas a empleados/empleadas o personas colaboradoras.

7.1.3. PROCESO DE AUTORIZACIÓN PARA LOS MEDIOS DE PROCESAMIENTO DE LA INFORMACIÓN.

El Comité de Seguridad de la Información de la notaría debe definir e implementar un protocolo de autorizaciones para el uso de los medios de procesamiento de la información y, en ningún caso, está permitido a empleados/empleadas, personas proveedoras, clientela,

personas usuarias y terceras personas, el acceso a estos sin previa autorización de la gerencia o dirección y/o la Coordinación de la respectiva dependencia de la notaría.

Control 1: la notaría a través de su Comité de Seguridad de la Información se reserva el derecho de negar o restringir el acceso a cualquier información a empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

Control 2: el Comité de Seguridad de la Información de la notaría será el único responsable de autorizar la conexión a los activos o red de la notaría de computadores, equipos portátiles, dispositivos móviles, notebooks o cualquier otro dispositivo de uso personal de los empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

7.1.4. TELETRABAJO.

Control: la notaría protegerá la información a la que se tiene acceso, que sea consultada o procesada en lugares en los que se realice teletrabajo. Se tendrá acceso a esta información haciendo uso de sistemas que protejan los datos y a través de canales o protocolos de comunicación seguros. En ninguno de los casos se podrá almacenar información sensible o privada en los sitios remotos de teletrabajo.

7.1.5. ACUERDOS DE CONFIDENCIALIDAD.

La gerencia o dirección, la coordinación, empleados/empleadas y personas proveedoras que tenga acceso a la información de la notaría deberán garantizar la completa confidencialidad mediante estipulaciones contenidas en los respectivos contratos, compromisos de confidencialidad y/o términos y condiciones de uso de las herramientas tecnológicas.

Control: la notaría al momento de hacer contrataciones, ejecutar trámites o prestar servicios establecerá cláusulas de confidencialidad y/o términos y condiciones con todos y cada una de las personas de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tenga acceso a la información, con el fin de garantizar la seguridad de la información de la notaría.

7.2. INTERCAMBIO DE INFORMACIÓN CON ORGANIZACIONES EXTERNAS Y CON LA FINALIDAD DE REALIZAR TRÁMITES Y PRESTAR SERVICIOS POR MEDIOS ELECTRÓNICOS.

Las peticiones de intercambio de información por parte de entes externos deben ser aprobadas por el Comité de Seguridad de la Información de la notaría y dirigidas de acuerdo con la Política de Seguridad de la Información de la notaría, con la continua y estricta supervisión del Comité de Seguridad de la Información. Para la ejecución de trámites y prestación de servicios por medios electrónicos, la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas son responsables de cumplir la Política de Seguridad de la Información de la

Notaría y los Términos y condiciones estipulados para el uso de las herramientas tecnológicas.

Control 1: el Comité de Seguridad de la Información de la Notaría debe mantener la seguridad y los servicios de procesamiento de información, a los cuales acceden personas proveedoras, clientela, personas usuarias, terceras personas, empresas o entidades externas; o los que son comunicados, procesados o dirigidos por estas.
Control 2: el Comité de Seguridad de la Información debe seguir los estándares de gestión de calidad y seguridad de la información, identificando los riesgos que se pueden presentar con el intercambio de información con personas u organizaciones externas y estableciendo controles de seguridad de acuerdo con los criterios establecidos por el Comité de Seguridad de la Información de la Notaría y los Términos y condiciones estipulados para el uso de las herramientas tecnológicas.

Control 3: el Comité de Seguridad de la Información de la Notaría debe velar porque el personal provisto por terceras personas, tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y para que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

Control 4: la información sensible debe ser encriptada de forma que solo las personas autorizadas puedan acceder a ella. Cualquier información intercambiada por medios electrónicos (USB, correo electrónico, descarga) debe ser analizada con antivirus previo al contacto con el sistema de información.

Control 5: el Comité de Seguridad de la Información de la Notaría será el encargado de autorizar y en tal caso, proveer herramientas necesarias para el acceso o intercambio de información a entes externos, teniendo en cuenta la clasificación de la información y con el fin de asegurarla.

7.2.1. IDENTIFICACIÓN DE LOS RIESGOS Y TRATAMIENTO DE LA SEGURIDAD.

El Comité de Seguridad de la Información de la Notaría debe contar con un documento de identificación y valoración de riesgos de la información. Se debe evitar desarrollar procesos que se asocian a riesgos altos no mitigados.

Control 1: el Comité de Seguridad de la Información de la Notaría debe evaluar periódicamente las amenazas y vulnerabilidades hacia la información o instalaciones de procesamiento de esta, la ocurrencia, su impacto y el desarrollo de estrategias para manejarlas y mitigarlas.

Control 2: el Comité de Seguridad de la Información de la Notaría debe generar las recomendaciones conforme con la evaluación y valoración de riesgos y tratamiento de seguridad de la información.

7.2.2. TRATAMIENTO DE LA SEGURIDAD PARA PERSONAS USUARIAS.

Las personas usuarias de la notaría solo pueden acceder a los datos o recursos de la información catalogados como públicos y a los permitidos conforme a la constitución y las

leyes. el Comité de Seguridad de la Información de la Notaría es el responsable de controlar, vigilar y autorizar el acceso a información confidencial y velar por el uso adecuado de la información y los recursos de la notaría por parte de los empleados.

Control: el Comité de Seguridad de la Información de la Notaría será el encargado de autorizar y definir el acceso a la información y el tratamiento a esta de la gerencia o dirección. la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de acuerdo con la clasificación de la información y las normas legales vigentes.

7.2.3. TRATAMIENTO DE LA SEGURIDAD EN CONTRATOS CON TERCERAS PERSONAS O PERSONAS PROVEEDORAS.

De acuerdo con la información intercambiada y la clasificación, los contratos entre terceras personas o personas proveedoras y la notaría, deben contener cláusulas de confidencialidad y compromisos de servicio que permitan cumplir con los objetivos y la Política de Seguridad de la Información de la Notaría.

Control: la notaría incluirá en todos los contratos con la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas, cláusulas de confidencialidad y tratamiento de datos para garantizar la seguridad de la información.

8. GESTIÓN DE ACTIVOS.

El Comité de Seguridad de la Información de la Notaría debe establecer los parámetros para la implementación de la política de seguridad de la información, de tal forma que se logre la protección adecuada de los activos de la información de la notaría. Esta política se aplica a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que hagan uso de los datos y la información de la notaría.

Control: la notaría dará a conocer a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas la Política de Seguridad de la Información de la Notaría, con el fin de que se respete y garantice la protección y seguridad de los activos de la notaría.

8.1. RESPONSABILIDAD POR LOS ACTIVOS.

El Comité de Seguridad de la Información de la Notaría es el responsable de los activos de la información; por lo tanto, debe practicar periódicamente auditorías sobre los procesos, actividades y sistemas vinculados con la gestión de activos de la información de la notaría. También es el responsable del cumplimiento de las medidas y especificaciones establecidas en esta Política de Seguridad de la Información.

Control: el Comité de Seguridad de la Información de la Notaría deberá practicar periódicamente auditorías sobre los procesos, actividades y sistemas vinculados con la gestión de activos de la información de la notaría.

8.1.1. INVENTARIOS DE ACTIVOS.

El Comité de Seguridad de la Información de la Notaría debe determinar y mantener un inventario actualizado de todos los activos de la información de la notaría, los cuales deben estar claramente identificados de acuerdo con las especificaciones de software y hardware, funciones, roles y responsabilidades correspondientes a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

Control 1: todos los activos de información de la notaría deben tener un responsable de su seguridad. El Comité de Seguridad de la Información de la Notaría asignará el o los activos a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas y mantendrá un inventario actualizado de cada uno de ellos.

Control 2: el Comité de Seguridad de la Información de la Notaría implementará las medidas y controles necesarios para cumplir con lo dispuesto en la Ley 594 de 2000 en concordancia con el Decreto 960 de 1970 y demás normas reglamentarias con relación al protocolo o archivos, de tal forma que se cuente con su gestión, mecanismos de seguridad, tablas de retención documental y aquellas que garanticen la conservación, integridad, disponibilidad, confidencialidad y seguridad de la información de la notaría.

8.1.2. PROPIEDAD DE LOS ACTIVOS DE LA INFORMACIÓN.

La notaría es la propietaria de todos los activos de la información y el Comité de Seguridad de la Información de la Notaría es el responsable y administrador de ellos.

Control: el Comité de Seguridad de la Información de la Notaría está encargado del inventario, mantenimiento, administración y auditoría de los activos de la información de la notaría.

8.1.3. USO ACEPTABLE DE LOS ACTIVOS DE LA INFORMACIÓN.

El Comité de Seguridad de la Información de la Notaría debe identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la misma, logrando mantener una adecuada protección de estos y aplicación de la política de seguridad de la información por parte de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tengan relación con dichos activos, aquellos que tenga bajo su responsabilidad o para el cumplimiento de los propósitos generales de la notaría. El Comité de Seguridad de la Información de la Notaría, para el uso adecuado de los activos de la información, debe tener en cuenta y hacer cumplir las siguientes directrices:

Control 1: los activos de la información pertenecen o son responsabilidad de la notaría y su uso debe ser única y exclusivamente para el cumplimiento de los propósitos de la notaría.

Control 2: la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas deben usar únicamente los activos de la información autorizados por el Comité de Seguridad de la Información de la Notaría.

Control 3: la posibilidad de acceso a los activos de la información de la notaría o los que están bajo su responsa08bilidad, por parte de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas, no implica el permiso de uso libre, por consiguiente, no deben leer, modificar copiar, transmitir o borrar información sin la debida autorización del Comité de Seguridad de la Información de la Notaría.

Control 4: cuando empleados/empleadas de la notaría impriman, saquen copias, escaneen, envíen faxes, ejecuten trámites o presten servicios electrónicos deben verificar los lugares adyacentes a las herramientas y equipos utilizados, para asegurar que no se queden documentos relacionados con la actividad y así evitar el acceso o divulgación no autorizada de los activos de la información de la notaría o aquellos que estén bajo su responsabilidad.

Control 5: la gerencia o dirección, la coordinación y empleados/empleadas al momento de ausentarse de sus escritorios o puestos de trabajo, deben asegurarse de cerrar la sesión de los aplicativos o sistemas de información y verificar que sus escritorios se encuentren libres de documentos y medios de almacenamiento utilizados para el desempeño de sus labores en la notaría.

Control 6: la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas no deben explotar las vulnerabilidades o deficiencias de seguridad de los medios (software, páginas web, sistemas, aplicaciones, servidores, archivadores, plataformas, infraestructura física o tecnológica) que almacena o facilita la información de la notaría.

Control 7: en caso de que la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas encuentren vulnerabilidades o riesgos que comprometan la seguridad de la información de la notaría, estas deben ser reportadas de inmediato al Comité de Seguridad de la Información de la Notaría.

Control 8: la información que se encuentre bajo custodia en la notaría debe ser protegida bajo controles de acceso físico y/o electrónico eficientes, seguros y buenas condiciones de almacenamiento y resguardo.

Control 9: está prohibida la ingestión de bebidas u otro tipo de alimentos sobre o en las proximidades de cualquiera de los documentos, archivadores, computadoras, aparatos electrónicos o demás activos de la información con que cuenta la notaría en sus puestos de trabajo, así como el manejo de sustancias o elementos que puedan ocasionar daños a los mismos.

Control 10: los usuarios de la notaría solo pueden acceder a los datos o recursos de la información catalogados como públicos y a los permitidos por la gerencia o dirección, la coordinación de la notaria y conforme con la constitución y las leyes.

Control 11: el Comité de Seguridad de la Información de la Notaría es el encargado de suministrar a cada empleado los equipos, programas y recursos informáticos; los datos e información creados, procesados, almacenados y recibidos, serán propiedad de la notaría.

Control 12: el Comité de Seguridad de la Información de la Notaría asignará a la persona encargada de realizar las copias de seguridad o backup de la información de la notaría, de manera periódica y frecuente, la cual debe ser almacenada en sitios apropiados para garantizar la seguridad de esta y que se pueda recuperar en caso de desastres o incidentes con los equipos de procesamiento.

Control 13: la gerencia o dirección, la coordinación o la persona encargada solo podrán realizar backup de la información de la notaría conforme lo establezca el Comité de Seguridad de la Información de la Notaría. Cualquier otro tipo de copia o backup debe ser con autorización de dicho comité y de acuerdo con la clasificación de la información.

Control 14: la modificación, copia, sustracción, daño intencional o utilización para fines distintos a los propósitos de la notaría, son sancionadas de acuerdo con lo establecido en la Política de Seguridad de Información de la Notaría y en las normas y legislación vigentes.

Control 15: el Comité de Seguridad de la Información de la Notaría debe inventariar, revisar y auditar los activos de la información utilizados en cada dependencia de la notaría.

Control 16: la descarga, instalación o uso de aplicativos o programas informáticos no autorizados por el Comité de Seguridad de la Información de la Notaría son sancionadas conforme con la Política de Seguridad de la Información de la Notaría.

Control 17: el Comité de Seguridad de la Información de la Notaría es la encargada de tener bajo custodia los medios magnéticos y electrónicos, como: disquetes, cd’s, manuales, licencias de uso, claves para descargar el software de fabricantes de sus páginas web o sitios en internet, las contraseñas de administración de los equipos informáticos, sistemas de información o aplicativos, etc.

Control 18: los activos de la información de la notaría no pueden ser utilizados, sin previa autorización escrita del Comité de Seguridad de la Información la Notaría para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o para otro uso que no esté autorizado.

Control 19: la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de la notaría que intenten actos que atenten contra el buen uso de los activos de la información de la notaría, como: envió de correo electrónico masivo con fines diferentes a los propósitos de la notaría y práctica de juegos en línea, deben ser sancionados conforme con lo estipulado en la Política de Seguridad de la Información de la Notaría.

Control 20: el Comité de Seguridad de la Información de la Notaría es el encargado de la aprobación y autorización de: instalación de software en equipos de la notaría o equipos que estén bajo la responsabilidad de la notaría; descarga de software de internet u otro servicio, modificación, revisión, transformación o adaptación de software en línea en cualquier equipo de la notaría; copiar o distribuir software de propiedad de la notaría; realizar registro conforme a las normas legales vigentes de la gerencia o dirección, la coordinación, empleados/empleadas o terceras personas autorizadas para ejecutar trámites y prestar servicios por medios electrónicos en la notaría.

Control 21: la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de la notaría son responsables de todas las transacciones o actuaciones realizadas bajo su cuenta de usuario.

Control 22: la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de la notaría no pueden acceder a la red o a otros servicios utilizando una cuenta de usuario o clave de otra persona usuaria.

Control 23: las peticiones de intercambio de información por parte de entes externos deben ser aprobadas por el Comité de Seguridad de la Información de la Notaría y dirigidas de acuerdo con la Política de Seguridad de la Información de la Notaría.

Control 24: el Comité de Seguridad de la Información de la Notaría es el responsable de asegurar el acceso a los activos de la información de la notaría, así como los accesos a internet, a redes sociales o demás herramientas tecnológicas; prevenir el acceso no autorizado de cuentas de usuarios u otros; controlar la introducción o propagación de programas destructivos o virus.

Control 25: el Comité de Seguridad de la Información de la Notaría debe revisar todos los materiales, archivos o descargas de redes externas para detectar programas destructivos y virus.

Control 26: el Comité de Seguridad de la Información de la Notaría es el encargado de aprobar, autorizar y controlar los cambios en la infraestructura informática de la notaría.

8.2. CLASIFICACIÓN DE LA INFORMACIÓN.

El Comité de Seguridad de la Información de la Notaría debe asegurar que los activos de información reciban una adecuada clasificación, etiquetado, manejo y protección de acuerdo con la Política de Seguridad de la Información de la notaría y de los estándares y normas legales vigentes garantizando la integridad, confidencialidad, disponibilidad y seguridad de la información.

El Comité de Seguridad de la Información de la Notaría puede almacenar la información en medios de información como: servidores, protocolo, bases de datos, medios magnéticos y

electrónicos, servicios en la nube, archivadores con carpetas que contienen actas, documentos, contratos, etc.
Control: el Comité de Seguridad de la Información de la Notaría clasificará la información y autorizará su uso y tratamiento de acuerdo con Política de Seguridad de la Información y los estándares y normas legales vigentes de tal forma que se garantice su integridad, confidencialidad, disponibilidad y seguridad.

8.2.1. LINEAMIENTOS DE CLASIFICACIÓN.

La gerencia o dirección, la coordinación y empleados de la notaría deben identificar y valorar los activos de información y tratarlos responsablemente con la finalidad de seguir los lineamientos de clasificación establecidos por el Comité de Seguridad de la Información de la Notaría, conforme a la Política de Seguridad de la Información y de los estándares y normas legales vigentes para garantizar la integridad, confidencialidad, disponibilidad y seguridad de la información.

Conforme a la normatividad legal vigente la información se clasifica en:

- **Información clasificada:** Es la información que por su naturaleza no debe ser divulgada ya que puede atentar contra la intimidad de la persona propietaria y solo es relevante para la persona titular. En esta categoría se encuentra la información de carácter privado y semiprivado.

- **Información disponible:** Información que puede ser solicitada o consultada por la ciudadanía, pero que no se encuentra publicada.

- **Información privada:** Es aquella que por versar sobre información personal o no, y que, por encontrarse en un ámbito privado, sólo puede ser obtenida y ofrecida por la persona titular o por orden de autoridad judicial en el cumplimiento de sus funciones. Es el caso de los libros de los comerciantes, de los documentos privados, de las historias clínicas o de la información extraída a partir de la inspección del domicilio.

- **Información Pública:** Es toda información que una autoridad genere, obtenga, adquiera o controle en su calidad de tal. Esta información es creada en el curso normal de la función misional y tiene poca probabilidad de causar daño.

- **Información Pública Clasificada:** Es aquella información que estando en poder o custodia de una autoridad en su calidad de tal, pertenece al ámbito propio, particular y privado o semiprivado de una persona natural o jurídica por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de esta ley. En caso de la divulgación de esta información, puede existir afectación a los derechos de privacidad de personas naturales o jurídicas.

- **Información pública reservada:** Es aquella información que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada de acceso a la ciudadanía por daño a bienes o intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en la ley.

- **Información semiprivada:** Es el que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.

El Comité de Seguridad de la Información para asegurar los activos de la notaría debe identificar la información y clasificarla conforme a la que se puede divulgar, así: según limitaciones de uso y según el valor de la información. Esto con el fin de que se pueda dar a conocer esta clasificación a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas y se garanticen buenas prácticas para proteger la información, su integridad, confidencialidad y disponibilidad.

Información de acuerdo con limitaciones de uso:

- **Información de uso general.** Es información que se puede compartir fuera y dentro de la notaría.
- **Información restrictiva.** Es información sensible que su divulgación puede perjudicar a una persona natural o jurídica.
- **Información confidencial.** Su uso o divulgación no autorizada puede ocasionar grandes perjuicios a los intereses económicos y comerciales de una persona natural o jurídica.

Según el valor de la información:

- **Información clave.** Su pérdida puede perjudicar la continuidad de un proyecto o proceso en la notaría.
- **Información no vital.** Su no disponibilidad no afecta la actividad de la notaría.

Control: el Comité de Seguridad de la Información de la Notaría tendrá en cuenta los anteriores lineamientos de clasificación de la información al momento de definir y autorizar el uso y tratamiento de la información.

9. SEGURIDAD DE LOS RECURSOS HUMANOS.

El Comité de Seguridad de la Información de la Notaría debe garantizar que la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tienen relación con los activos de información de la Notaría acaten con responsabilidad la Política de Seguridad de la Información y hagan un adecuado uso de los activos de información de la notaría, de acuerdo con roles, tareas

que desempeñen, responsabilidades y situación contractual para reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones de la notaría.

Control: el Comité de Seguridad de la Información de la Notaría debe definir un perfil para todo el personal que tiene relación con los activos de información de la notaría y debe conservar un directorio completo y actualizado de tales perfiles.

9.1. ROLES, RESPONSABILIDADES Y FUNCIONES.

la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tienen relación con los activos de la notaría, deben asegurar y entender sus responsabilidades en relación con la Política para la Seguridad de la Información de la Notaría y actuar de manera consecuente frente a ella, con el objetivo de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado o mal intencionado de los activos de la información de la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría debe elaborar, mantener, actualizar, mejorar y difundir el manual de Responsabilidades Personales para garantizar la seguridad de la información en la notaría.

Control 2: el Comité de Seguridad de la Información de la Notaría es el encargado de definir los perfiles para el personal que tiene que ver con los activos de la información.

Control 3: el Comité de Seguridad de la Información de la Notaría es responsable de revisar y proponer el texto de la Política de Seguridad de la Información de la Notaría y asignar las funciones generales que deben cumplir la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tienen relación con la información de la notaría.

Control 4: el Coordinador del Comité de Seguridad de la Información de la Notaría es el responsable de organizar las acciones del Comité y de impulsar la implementación y cumplimiento de la Política de Seguridad de la Información por parte de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas de la notaría.

Control 5: todos empleados/empleadas de la notaría son responsables de proteger la información que está contenida en documentos, formatos, listados, equipos, sistemas etc., derivado de sus funciones y que son el resultado de los procesos informáticos.

Control 6: cada dependencia de la notaría debe mantener depurada la información de las carpetas virtuales para la optimización del uso de los recursos de almacenamiento y debe velar por la seguridad de los medios de la información de los que son responsables.

Control 7: las terceras personas son responsables de asegurar y mantener la Política de Seguridad de la Información y los activos de la información que suministran a la notaría.

Control 8: la gerencia o dirección y la coordinación son responsables de definir los permisos de acceso a la información que autoriza a empleados/empleadas de acuerdo con sus

funciones y competencia para que se mantenga y asegure la integridad., confidencialidad y disponibilidad de la información en la notaría.

Control 9: la gerencia o dirección responsable de la notaría debe cumplir la función de notificar al personal que se vincule contractualmente con la notaría, de las obligaciones respecto del cumplimiento de la Política de Seguridad de la Información de la Notaría, de todos los estándares, procesos, prácticas y guías que surjan del sistema de la Seguridad de la información. También es el responsable de informar los cambios que en ella se produzcan y suscribir compromisos de confidencialidad.

9.2. PROCESO DISCIPLINARIO.

Sin perjuicio de las demás disposiciones legales aplicables que la conducta pueda ocasionar, es necesaria la clasificación de las violaciones a la Políticas de Seguridad de la Notaría, con el fin de aplicar medidas correctivas conforme a la clasificación definida y mitigar la afectación a la seguridad de los activos de la información de la notaría.

Se considerarán entre las medidas correctivas: llamados de atención y acciones administrativas de orden disciplinario o penal, de acuerdo con las circunstancias que así lo ameriten.

Control: el Comité de Seguridad de la Información es el encargado de imponer los procesos y medidas disciplinarias para los casos que se presenten por usos indebidos o malintencionados de los activos de la información y que violan la Política de Seguridad de la Información de la Notaría.

9.3. TERMINACIÓN O CAMBIO DE FUNCIÓN Y ELIMINACIÓN DE DERECHOS DE ACCESO.

A la terminación del contrato o cambio de labor de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas, se deben, inmediatamente, ser revocados los mecanismos de autenticación y controles de acceso y devuelto todos los activos de la información de la notaría, otorgados con ocasión del contrato o acuerdo.

Control: el Comité de Seguridad de la Información de la Notaría es el encargado de establecer los mecanismos y controles para garantizar el cambio o entrega de los activos de la información de la notaría e impedir el acceso, una vez haya cambio de labor o terminación del contrato entre la notaría y la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

9.4. DEVOLUCIÓN DE ACTIVOS.

A la terminación del contrato de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras

personas deben ser devueltos al Comité de Seguridad de la Información todos los activos de la información de la notaría que le fueron puestos a disposición con ocasión del desempeño de la labor.

Control: el Comité de Seguridad de la Información de la Notaría es el encargado de establecer los mecanismos y controles para garantizar la devolución de los activos de la información de la notaría una vez terminado el contrato entre la compañía y la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

10. SEGURIDAD FÍSICA Y AMBIENTAL.

El objetivo de la Política de Seguridad de la Información física y ambiental de la notaría es impedir acceso no autorizado a las áreas donde se encuentran los activos de información, instalaciones, centros de datos y centros de cableado, evitando así posibles daños o perjuicios en la prestación de los servicios y garantizando la integridad, disponibilidad e integridad de la información.

Control: la notaría garantizará la seguridad física y ambiental de la información mediante controles de acceso a instalaciones, centros de datos, centros de cableado y demás de la compañía.

10.1. ÁREAS SEGURAS.

Los lugares físicos donde se encuentran los medios que contienen servidores, almacenes principales de datos, equipos, cableado estructurado, conexiones de red, documentos o cualquier activo de información de uso reservado de la notaría deben estar en áreas seguras y con un sistema de seguridad que no permita el acceso de terceros a dichas áreas.

Control: la seguridad física de las instalaciones, centros de datos, centros de cableado y demás de la notaría se basará en áreas seguras, las cuales serán protegidas por medio de controles de acceso apropiados.

10.1.1. CONTROLES DE ENTRADA FÍSICOS.

El Comité de Seguridad de la Información de la Notaría debe controlar y restringir el acceso de personas no autorizadas a las áreas seguras. Se debe dejar registro, de fecha y hora, de los terceros o usuarios autorizados que ingresan a las áreas seguras de la notaría.

Control: las entradas a las áreas físicas de la notaría tendrán niveles de seguridad conforme con la clasificación de la información que se utiliza y administra. La información confidencial o sensitiva cuando no sea utilizada se mantendrá en lugares con acceso restringido.

10.1.2. PERÍMETROS DE SEGURIDAD FÍSICA.

Control: la notaría debe contar la seguridad física necesaria para evitar el ingreso a las áreas que contienen documentos, información o medios de procesamiento de la información.

10.1.3. PROTECCIÓN CONTRA AMENAZAS EXTERNAS Y AMBIENTALES.

En la Notaría se debe aplicar la protección contra incendios, inundación, explosión, robo u otras catástrofes que puedan afectar, modificar o acabar con los activos de la información de la notaría.

Control: la notaría tomará todas las medidas necesarias para proteger los activos de la información y no almacenará materiales peligrosos o combustibles que puedan afectar los activos de la información de la compañía.

10.2. SEGURIDAD DEL EQUIPO.

Todo equipo debe ser revisado, registrado y aprobado por el Comité de Seguridad de la Información de la notaría cumpliendo con todos los requisitos y controles establecidos. Únicamente podrán realizar las tareas para las que fueron autorizados.

Control: los servidores y equipos que contengan información de la notaría deben estar ubicados en áreas seguras con controles de acceso, seguridad física y ambiental y respaldados con UPS.

10.2.1. MANTENIMIENTO DE EQUIPO.

La notaría mantendrá las herramientas y equipos donde se almacena, procesa o comunica la información de la compañía con las medidas de protección lógicas y físicas, de tal forma que permitan su correcto estado de funcionamiento, monitoreo y control.

Control 1: los equipos de la notaría deben recibir mantenimiento y soporte de hardware y software constante con el fin de asegurar la disponibilidad de los servicios.

Control 2: los puestos de trabajo deben tener bien asegurados los equipos y deben ser operados únicamente por los directivos, empleados o terceros autorizados por el Comité de Seguridad de la Información de la Notaría.

Control 3: el Comité de Seguridad de la Información debe informar de la Política de Seguridad de la Información de la Notaría a la gerencia o dirección, la coordinación, empleados/empleadas y terceras personas para el uso responsable de los equipos y recursos de la información.

Control 4: las copias de seguridad deben ser conservadas de acuerdo con la Política de Seguridad de la Información de la Notaría y a los estándares vigentes.

10.2.2. SEGURIDAD DEL EQUIPO FUERA DE LAS INSTALACIONES DE LA COMPAÑÍA.

Control 1: el Comité de Seguridad de la Información debe implementar la Política de Seguridad para proteger los medios de la información que se requieran sacar de las instalaciones de la notaría.
Control 2: las Política de Seguridad de la Información implementada en los equipos que se requieren sacar de las instalaciones de la notaría deben tener en cuenta los riesgos a que se expone y la forma de mitigarlos.

10.2.3. ELIMINACIÓN SEGURA O RE-USO DEL EQUIPO.

Control 1: el Comité de Seguridad de la Información es el encargado de determinar re-usar o eliminar equipos o medios de información de la notaría.

Control 2: los equipos o medios de información de la notaría que vayan a ser re-usados o eliminados deben surtir un proceso de borrado seguro y posteriormente serán re-usados, eliminados o destruidos de forma adecuada. Se debe realizar la destrucción de información cuando se ha cumplido su ciclo de almacenamiento.

11. GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES.

El Comité de Seguridad de la Información de la Notaría debe fortalecer las comunicaciones y operaciones seguras y correctas de los medios de procesamiento de la información, con el fin de garantizar la continuidad de las tecnologías de la información y las comunicaciones. El Comité de Seguridad de la Información de la Notaría debe aplicar estas políticas a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tienen relación con la información de la compañía.

Control: el Comité de Seguridad de la Información de la notaría debe realizar guías de operación de los activos de información de la notaría, ponerlas a disposición de los usuarios que los requiera, generando programas de seguimiento a las operaciones y comunicaciones para asegurar la disponibilidad de los servicios.

11.1. PROCEDIMIENTOS Y RESPONSABILIDADES OPERACIONALES.

Un procedimiento describe de forma más detallada lo que se hace en las actividades de un proceso de la notaría, en él se especifica cómo se deben desarrollar las actividades, cuáles son los recursos, el método y el objetivo que se pretende lograr o el valor agregado que genera y caracteriza los procesos en la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría elabora y aprueba la Política de Seguridad de la Información, de acuerdo con las necesidades y el compromiso de diseño e implementación de estrategias eficientes que garanticen la correcta y segura operación de los medios de procesamiento, recursos y activos de la información en la notaría.

Control 2: el Comité de Seguridad de la Información debe elaborar los instructivos para detallar aún más las tareas y acciones puntuales que se deben desarrollar dentro de un procedimiento, como son: los instructivos de trabajo y de operación; los primeros para la ejecución de la tarea por la persona y los segundos para la manipulación o la operación de un equipo y que tengan que ver con los datos y la información de la notaría.

11.1.1. PROCEDIMIENTO DE OPERACIÓN DOCUMENTADOS.

Control 1: el Comité de Seguridad de la Información de la Notaría se encargará de elaborar y mantener actualizados los manuales de los procedimientos de operación implementados en la notaría y los divulgará a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tengan relación con los datos y la información de la notaría.

11.1.2. GESTIÓN DE CAMBIO.

Control: el Comité de Seguridad de la Información de la Notaría será el encargado de aprobar y controlar los cambios en los medios y en los sistemas de procesamiento de la información de la notaría.

11.1.3. SEGREGACIÓN DE DEBERES.

Control: el Comité de Seguridad de la Información debe definir los roles y responsabilidades, así como la persona encargada y autorizada para el control de los medios y sistemas, para evitar el mal uso o las modificaciones no autorizadas o mal intencionadas a los activos de la notaría.

11.2. GESTIÓN DE LA ENTREGA DEL SERVICIO A TERCERAS PERSONAS.

El Comité de Seguridad de la Información de la Notaría debe implementar y mantener una apropiada seguridad de los activos de la información de la notaría y de los trámites y servicios de información ejecutados a personas proveedoras, clientela, personas usuarias y terceras personas.

Control: la notaría incluirá la prohibición de divulgar la información entregada por la notaría a personas proveedoras, clientela, personas usuarias y terceras personas, con quienes se establecerán acuerdos y/o entrega y/o destrucción de dicha información una vez cumpla su cometido.

11.2.1. ENTREGA DEL SERVICIO.

Control: el Comité de Seguridad de la Información de la Notaría debe asegurar que se implementen, operen y mantengan los controles de seguridad, definiciones de servicio y de entrega, al momento de la contratación, ejecución de trámites y prestación de servicios de información con terceras personas.

11.2.2. MONITOREO Y REVISIÓN DE LOS SERVICIOS DE TERCERAS PERSONAS.

Control: los reportes y servicios suministrados por terceras personas a la notaría, deben ser monitoreados, revisados y auditados regularmente de conformidad a lo establecido por el Comité de Seguridad de la Información de la Notaría y conforme a la Política de Seguridad de la Información y de las normas legales vigentes.

11.2.3. MANEJO DE LOS CAMBIOS EN LOS SERVICIOS DE TERCERAS PERSONAS.

Control: el Comité de Seguridad de la Información de la Notaría debe estar atento a los cambios en el suministro de los servicios informáticos. Debe mantener y mejorar la Política de Seguridad de la Información, los procedimientos y controles de seguridad teniendo en cuenta los procesos comerciales, el grado crítico y reevaluando de riesgos.

11.3. PROTECCIÓN CONTRA SOFTWARE MALICIOSO.

Se debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información de la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría debe elaborar, mantener y controlar la Política de Seguridad de la Información, procedimientos, estándares y normas para proteger los sistemas informáticos, teniendo un enfoque que involucre controles físicos, humanos y técnicos que garanticen la mitigación de riesgos asociados a software malicioso y técnicas de hacking.

Control 2: el Comité de Seguridad de la Información debe garantizar que las estaciones de trabajo se encuentren protegidas con antivirus con capacidad de actualización automática.

11.4. RESPALDO O BACK-UP.

Toda información que sea fundamental para el funcionamiento de la notaría se debe respaldar por una copia de seguridad, tomada conforme lo disponga el Comité de Seguridad de la Información de la Notaría y deben incluir lo referente al almacenamiento de dichas copias.

Control: el Comité de Seguridad de la Información de la Notaría es el encargado de elaborar las directrices para el manejo, control, administración y protección de las copias de seguridad de la información de la notaría. Empleados/empleadas deben entregar periódicamente las copias de seguridad correspondientes a la información de sus dependencias conforme lo establezca dicho Comité.

11.5. GESTIÓN DE SEGURIDAD EN LA RED.

El acceso a la red de la notaría debe ser permitido sólo a personas usuarias autorizadas, una vez definidos, verificados y controlados los perfiles y roles para el acceso a los activos de información, conforme lo establezca El Comité de Seguridad de la Información de la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría es el encargado de definir autorizar y definir las condiciones y los perfiles de acceso a la red.

Control 2: está prohibido el uso de los recursos o acceso a internet para tareas diferentes a las asignadas y la instalación de software o hardware, sin previa autorización del Comité de Seguridad de la Información de la Notaría.

Control 3 se debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información.

Control 4: se deben actualizar y parchear todo software (sistemas operativos, servidor de base de datos, servidor web) para prevenir el acceso a estos por medio de cualquier vulnerabilidad conocida.

11.6. GESTIÓN DE MEDIOS.

Ninguna persona de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas puede divulgar, modificar, eliminar o destruir los activos de la información de la notaría sin autorización expresa del Comité de Seguridad de la Información de la Notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría debe establecer los procedimientos y el control de la eliminación de los medios de una manera segura cuando ya no se requieran, lo mismo que el procedimiento para almacenar y proteger la información de la notaría, su divulgación no autorizada o mal uso.

Control 2: el acceso a la documentación de la notaría debe ser conforme a la Política de Seguridad de la Información, a los estándares y disposiciones legales vigentes.

11.7. INTERCAMBIO DE INFORMACIÓN.

Las peticiones de información por parte de entes externos de control deben ser aprobadas por el Comité de Seguridad de la Información de la Notaría y deben ser dirigidos por estos ante los responsables de la custodia.

Control 1: la notaría deberá encriptar la información sensible de forma que solo las personas autorizadas puedan acceder a ella.

Control 2: cualquier información intercambiada con la notaría por medios electrónicos (USB, correo electrónico, descarga, mensajes de texto, sistemas en línea, etc.) debe ser analizada con antivirus previo contacto con el sistema de información de la notaría.

11.8. SERVICIOS DE COMERCIO ELECTRÓNICO.

Control: el Comité de Seguridad de la Información de la Notaría es el encargado de autorizar, controlar y auditar el uso responsable de internet y de los servicios de correo electrónico, conforme a la Política de Seguridad de la Información y las normas legales y vigentes.

11.9. MONITOREO.

El Comité de Seguridad de la Información de la Notaría debe establecer mecanismos y procedimientos que garanticen la integridad, disponibilidad, legalidad, actualización, no repudio, confidencialidad y seguridad de la información.

Control 1: el Comité de Seguridad de la Información de la Notaría debe establecer mecanismos y procedimientos para que pueda producir registros de actividades de auditoría y mantenerlos durante un periodo estipulado para contribuir con investigaciones futuras y monitoreo de control de acceso.

Control 2: el Comité de Seguridad de la Información de la Notaría debe monitorear el uso de los medios de procesamiento de la información.

Control 3: el Comité de Seguridad de la Información de la Notaría debe proteger los medios de registro y la información del registro contra alteraciones y acceso no autorizado.

Control 4: el Comité de Seguridad de la Información de la Notaría debe registrar, analizar y corregir las fallas.

12. CONTROL DE ACCESO.

Se proveerán mecanismos de autenticación y control de acceso con el fin de salvaguardar los activos de la información de la Notaría y para que la gerencia o dirección, la coordinación y empleados/empleadas hagan uso responsable de la información a la cual se les autoriza el acceso.

Control 1: el Comité de Seguridad de la Información de la Notaría debe definir la política del control de acceso para las personas usuarias, sistemas de seguridad, sistemas de información, sistema de redes y otros.

Control 2: la gerencia o dirección, la coordinación y empleados/empleadas son responsables de toda actividad que derive del uso de su usuario o contraseña o mecanismo de autenticación, por ende, no deben ser divulgados o cedidos a otros, para evitar que esta sea revelada o robada.

Control 3: empleados/empleadas no deben permitir que otras personas usuarias realicen labores bajo sus mecanismos de autenticación. De igual forma, no se deben realizar actividades bajo los de alguien más.

12.1. REQUERIMIENTO PARA EL CONTROL DE ACCESO.

El Comité de Seguridad de la información de la Notaría debe controlar los accesos y recursos de los tratamientos y procesos de la información estableciendo regulaciones y autorizaciones que garanticen la seguridad de la información.

Control: El Comité de Seguridad de la información de la Notaría debe definir los requerimientos de seguridad de las aplicaciones y asegurar que se imponen responsabilidades conforme a incumplimientos, no conformidades y otros incidentes.

12.2. GESTIÓN DE ACCESO DE LA PERSONA USUARIA.

Empleadas/empleados del área de la información y sistemas harán parte del Comité de Seguridad de la Información de la Notaría y serán encargadas de controlar los privilegios especiales de los demás empleados/empleadas en sus estaciones de trabajo.

Control 1: el Comité de Seguridad de la Información de la Notaría debe mediante un proceso formal, realizar la inscripción y anular la misma a los accesos de las personas usuarias de los sistemas de información.

Control 2: el Comité de Seguridad de la Información de la Notaría es encargado de controlar y auditar que las personas usuarias cumplan la Política de Seguridad de la Información, respecto del acceso de la persona usuaria.

12.3. RESPONSABILIDADES DE LA PERSONA USUARIA.

La notaría debe garantizar el acceso a las personas usuarias autorizadas e impedir los accesos no autorizados a los sistemas de información. La responsabilidad de cada persona usuaria es proteger los activos de la información de la notaría, que se encuentra en medio físico y magnético, los cuales son producto de los procesos informáticos realizados en la notaría.

Control 1: el Comité de Seguridad de la Información de la Notaría prohibirá el uso de los recursos o acceso a internet para tareas diferentes a las asignadas.

Control 2: el Comité de Seguridad de la Información de la Notaría debe establecer los procedimientos para cubrir todas las etapas del ciclo de vida del acceso de las personas usuarias, a partir del registro inicial hasta su baja a los sistemas y servicios de información.

12.4. CONTROL DE ACCESO A LA RED.

Los equipos de cómputo de la persona usuaria final que se conecten o deseen conectar a las redes de datos de las dependencias de la notaría, deben cumplir con la totalidad de los

requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizadas. Todas las redes con salida a redes públicas deben ser aseguradas con los mecanismos de seguridad pertinentes (Firewalls, mecanismos de autenticación y protocolos de comunicación seguros).

Control 1: el Comité de Seguridad de la Información de la Notaría debe asegurar que las redes inalámbricas de la organización cuenten con métodos de autenticación que evite accesos no autorizados.

Control 2: el Comité de Seguridad de la Información de la Notaría debe verificar periódicamente los controles de acceso, mecanismo de autenticación, privilegios de empleados/empleadas y personas usuarias provistos por terceras partes, con el fin de revisar que dichas personas usuarias tengan únicamente el acceso permitido a aquellos recursos y servicios para los que fueron autorizados.

Control 3: el Comité de Seguridad de la Información de la Notaría debe proteger las redes de datos, lugares de almacenamiento, y demás recursos de la notaría contra accesos no autorizados a través de mecanismos de autenticación, o control de acceso.

Control 4: el Comité de Seguridad de la Información de la Notaría debe contar con el formato de creación de mecanismos de autenticación debidamente autorizado y Acuerdo de Confidencialidad firmado previamente.

Control 5: el Comité de Seguridad de la información de la Notaría establecerá privilegios para el control de acceso lógico de cada persona usuaria o grupo de personas usuarias a las redes de datos, los recursos físicos, tecnológicos y los sistemas de información.

12.5. CONTROL DE ACCESO AL SISTEMA OPERATIVO.

La notaría establecerá procedimientos para controlar la instalación de software operativo, contará con el soporte de sus proveedores y garantizará funcionalidad y operatividad de los sistemas de información en las plataformas tecnológicas cuando el sistema operativo es actualizado.

Control: el Comité de Seguridad de la Información de la Notaría debe proteger los sistemas operativos en todas las estaciones de trabajo deben estar protegidos mediante un usuario y una contraseña la cual debe ser cambiada cada 6 meses.

12.6. CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN.

La notaría debe monitorear regularmente el software instalado, como también analizar el equipo con herramientas que aseguren la no presencia de software malicioso, que comprometan la seguridad de la información. Queda prohibida la instalación de software o hardware sin la debida autorización del Comité de Seguridad de la Información de la Notaría o sin la licencia pertinente.

Control 1: el Comité de Seguridad de la Información de la Notaría debe actualizar, parchear todo software (sistemas operativos, servidor de base de datos, servidor web) para prevenir el acceso a estos, por medio cualquier vulnerabilidad conocida.

Control 2: al asignar contraseñas se debe tener en cuenta que sean mayores a 8 caracteres, hacer combinaciones entre minúsculas y mayúsculas, números y caracteres especiales como “& @ # -“

Control 3: al asignar contraseñas no se deben usar datos de personas usuarias que sean fácilmente deducibles ejemplo, fechas de nacimiento, nombres de personas cercanas o cualquier dato que guarde relación con la persona usuaria o de la notaría.

Control 4: al asignar contraseñas se debe evitar utilizar secuencias básicas de teclado (por ejemplo: ”qwerty”, “asdf” o las típicas en numeración: “1234” ó “98765”)

Control 5: al asignar contraseñas no repetir los mismos caracteres en la misma contraseña. (ej.: “111222”).

Control 6: al asignar contraseñas no se deben digitar las contraseñas en presencia de personas que puedan observarlas.

Control 7: se recomienda el cambio de las contraseñas como mínimo cada 3 meses y no deben ser reutilizadas.

Control 8: la gerencia o dirección, la coordinación y empleadas/empleados cuando se requiera deben autenticarse por medios biométricos como la huella dactilar y deben abstenerse de utilizar los mecanismos de autenticación en equipos que no pertenezcan a la notaría o que no estén autorizados para realizar las tareas encomendadas.

Control 9: la gerencia o dirección, la coordinación y empleadas/empleados deben utilizar las herramientas tecnológicas bajo su método de autenticación. No está permitido por ninguna circunstancia utilizar dichas herramientas tecnológicas bajo el método de autenticación de otra persona usuaria. La gerencia o dirección, la coordinación y empleadas/empleados son responsables por cualquier actividad que se realice bajo su método de autenticación.

Control 9: en caso de sospecha, pérdida, o uso indebido de los mecanismos de autenticación se debe notificar por escrito de inmediato al Comité de Seguridad de la Información de la Notaría.

12.7. REQUERIMIENTOS DE SEGURIDAD DE LOS SISTEMAS DE INFORMACIÓN.

General. Los recursos designados por la notaría deben ser de uso exclusivo para las actividades aprobadas por el Comité de Seguridad de la Notaría y cada empleado/empleada será responsable de cumplir los requisitos de seguridad de las herramientas tecnológicas y/ activos de información. Además, empleados/empleadas deben permitir a la persona designada por el Comité de Seguridad de la Información de la

Notaría realizar inspecciones de seguridad periódicas las cuales serán informadas con anterioridad. De igual manera, en el momento que empleado/empleada sea desvinculado o se retire por voluntad propia debe entregar todos los accesos y contraseñas que tiene en su poder al Comité de Seguridad de la Notaría para que estos sean revocados.

Control 1: **virus y código dañino de computadores.** Todos los equipos entregados al empleado deben mantenerse libre de virus y otros códigos dañinos de computadores, para lo cual la gerencia o dirección, la coordinación y empleados/empleadas deberán tomar las medidas necesarias para su cumplimiento. Igualmente, cualquier equipo externo que sea conectado a la red de la Notaría, previa autorización del Comité de Seguridad de la Información debe contar con un antivirus vigente y debidamente licenciado.

Control 2: **restricciones del uso de software.** Todo software que sea necesario para el cumplimiento de los deberes de la gerencia o dirección, la coordinación y empleadas/empleados y que requiera de su uso y/o instalación debe ser aprobado por el Comité de Seguridad de la Notaría, de igual manera, está restringido todo tipo de software de uso personal por parte de la gerencia o dirección, la coordinación y empleadas/empleados, el cual no debe estar instalado en ninguno de los equipos de la notaría.

Control 3: **gestión de cambios.** Cualquier cambio relacionado al ambiente de producción o de pruebas en las plataformas instaladas, accedidas y manejadas local o remotamente, deben seguir las normas que se estipulan en el proceso de gestión de cambios de la notaría.

Control 4: **respaldo de información.** Cada una de las personas de la gerencia o dirección, la coordinación y empleadas/empleados deben cumplir las normas de respaldo de la información realizando los backups de la información que se tiene en cada uno de los equipos o conforme a las directrices del Comité de Seguridad de la Información de la Notaría.

Control 5: **información clasificada.** Toda información clasificada como reservada, restringida o interna, según estipulado en los acuerdos de confidencialidad de la notaría u otra información de carácter sensitivo, debe ser protegida de acuerdo con la Política de Seguridad de la Información y todas las personas usuarias, la gerencia o dirección, la coordinación y empleadas/empleados, deben firmar un acuerdo de confidencialidad a la notaría.

Control 6: **propiedad intelectual.** El conocimiento que la gerencia o dirección, la coordinación y empleadas/empleados obtengan acerca de la notaría, sus servicios, equipo, instalaciones, redes, sistemas de computación, planes, procedimientos, etc., no podrán ser utilizado con el fin de ventaja personal o el provecho de otras personas, notarías, entidades, organizaciones o gobiernos. De igual manera, los derechos de uso y patrimoniales derivados de la actividad de manera absoluta, junto con los programas, soportes lógicos, códigos fuentes, algoritmos, modelos, circuitos, artes y los documentos que estas contienen, así como las invenciones, mejoras y procedimientos que a estas se apliquen como resultado de las actividades contratadas son propiedad de la Notaría o de sus aliados tecnológicos y, por lo tanto, estas tienen derecho a patentarlas o registrarlas a nombre

propio o de terceras personas y en ningún tiempo el empleado/empleada podrá reclamar derechos de uso o patrimoniales.

Control 7: **autenticación.** Para el proceso de autenticación se establecen normas que serán de obligatorio cumplimiento para la gerencia o dirección, la coordinación y empleado/empleada cuando este se encuentre en el ejercicio de sus labores contractuales, entre las cuales se contempla el ingreso de las contraseñas de manera manual, no guardar las contraseñas de manera automatizada, la longitud, inclusión de caracteres especiales de la misma y la divulgación de esta a cualquier otra persona de la notaría a excepción del momento de su retiro.

12.8. CONTROLES CRIPTOGRÁFICOS.

La gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas deben usar herramientas de encriptación para transferencias de archivos de la información clasificada como pública reservada o información pública clasificada, por medio de los sistemas de información y comunicaciones y siguiendo las pautas establecidas por el Comité de Seguridad de la información de la Notaría.

Control 1: el Comité de Seguridad de la información de la Notaría debe Implementar herramientas criptográficas para proteger los activos de información clasificada y fortalecer la disponibilidad, confidencialidad, e integridad de la información. El Comité de Seguridad de la información de la Notaría debe aplicar estas políticas a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que hagan uso de la información de la notaría.

Control 2: el Comité de Seguridad de la información de la Notaría debe controlar que las aplicaciones y sistemas que permitan y/o realicen transmisión de información pública reservada o pública clasificada se realice utilizando cifrado de datos, para lo cual debe proveer herramientas de encriptación de datos, cuya clave debe establecerla cada persona usuaria que administre la información. El Comité de Seguridad de la información de la Notaría o sus aliados tecnológicos indicarán la política que se debe seguir para configurar dichas contraseñas.

12.9. SEGURIDAD EN LOS PROCESOS DE DESARROLLO Y SOPORTE.

Desarrollo. Se le entregará a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas toda la información, herramientas y datos necesarios para la ejecución de proyectos.

Control 1: La gerencia o dirección, la coordinación, empleados/empleadas serán responsables de resguardar la información en su equipo teniendo en cuenta las Políticas de Seguridad de la Información, extracción de código, documentos o datos, actualización de versiones del repositorio, almacenamiento de archivos, acceso a servidores de desarrollo y demás, según haya sido autorizado por el Comité de Seguridad de la Información de la Notaría.

Soporte. Empleada/empleado que desempeñe algún cargo en el área de soporte debe cumplir con los estándares requeridos por la notaría para el uso de las herramientas adecuadas para el correcto almacenamiento de los datos, soporte remoto, registro y estado de los casos, tipo de caso y solución de este.

Control 1: los datos suministrados al personal de soporte deben almacenarse conforme con lo que estipule el Coordinador del Comité de Seguridad de la Información de la Notaría.

Control 2: empleados/empleadas deben tener contraseña de acceso o autenticación biométrica a las herramientas tecnológicas a las cuales le dará soporte, las contraseñas deberán ser manualmente ingresadas, sin opción a recordar en ningún navegador o software. La contraseña debe ser conocida solamente por empleada/empleado quien la crea. Nadie deberá compartir una contraseña. Si en una situación dada se debe revelar una contraseña a una segunda persona, el dueño/a de la contraseña deberá cambiar la contraseña apenas la situación emergente haya terminado. No está permitido realizar actividades bajo mecanismo de autenticación de otra persona.

12.10. GESTIÓN DE LA VULNERABILIDAD TÉCNICA.

El Comité de Seguridad de la información de la Notaría debe aplicar estas políticas de gestión de la vulnerabilidad técnica a la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que hagan uso de la información de la notaría.

Control 1: el Comité de Seguridad de la información de la Notaría debe controlar y evitar el uso de vulnerabilidades técnicas en las herramientas y sistemas de información y comunicaciones, para lo cual debe implementar los indicadores para gestión de vulnerabilidades.

Control 2: el Comité de Seguridad de la información de la Notaría debe implementar programas de gestión de vulnerabilidades técnicas, realizar pruebas técnicas de vulnerabilidad e incluir planes de tratamiento de vulnerabilidades en las herramientas y sistemas de información y comunicaciones de la notaría.

12.11. CONTROL DE ACCESO Y MECANISMOS DE AUTENTICACIÓN.

Las redes de datos, lugares de almacenamiento, y demás recursos de la notaría deben ser debidamente protegidas contra accesos no autorizados a través de mecanismos de autenticación, o control de acceso.

Control 1: se debe asegurar que las redes inalámbricas de la organización cuenten con métodos de autenticación que evite accesos no autorizados.

Control 2: se tienen que verificar periódicamente los controles de acceso, mecanismo de autenticación y privilegios para empleadas/empleados y personas usuarias provistos por terceras partes, con el fin de revisar que estos tengan únicamente el acceso permitido a aquellos recursos y servicios para los que fueron autorizados.

Control 3: es obligatorio contar con el formato de creación de mecanismos de autenticación debidamente autorizado y Acuerdo de Confidencialidad, firmado previamente. Los equipos de cómputo de persona usuaria final que se conecten a las redes de datos de las dependencias de la notaría deben cumplir con todos los requisitos o controles para autenticarse en ellas y únicamente podrán realizar las tareas para las que fueron autorizados.

Control 4: todas las redes con salida a redes públicas deben ser aseguradas con los mecanismos de seguridad pertinentes como firewalls, mecanismos de autenticación y protocolos de comunicación seguros.

Control 5: el Comité de Seguridad de la Información de la Notaría establecerá privilegios para el control de acceso lógico de cada persona usuaria o grupo de personas usuarias a las redes de datos, los recursos físicos, tecnológicos y los sistemas de información de la notaría.

Control 6: se velará porque empleadas/empleados y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus labores y para que la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

13. DEL TRATAMIENTO Y ALMACENAMIENTO DE INFORMACIÓN SENSIBLE Y CONFIDENCIAL.

Si la información sensible y confidencial es almacenada, se debe incluir con metadatos y funciones hash para garantizar la integridad y no repudio de la información y debe ser conforme con la Política de Seguridad de la Información de la Notaría y los estándares y disposiciones legales vigentes.

Control: el Comité de Seguridad de la Información de la Notaría debe garantizar y controlar el tratamiento de la información sensible y confidencial, por parte de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas conforme con lo que exigen las normas legales vigentes.

14. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.

De acuerdo con la ley y la Política de Seguridad de la Información de la Notaría el Comité de Seguridad de la Información de la Notaría está autorizado para realizar seguimiento o interceptación a los mecanismos o recursos que permitan determinar incidentes en la seguridad de la información.

Control 1: todo el personal que tenga relación con los activos de la información de la notaría está obligado a reportar, con responsabilidad, presuntas violaciones a la seguridad de la información de la notaría.

Control 2: El Comité de Seguridad de la Información de la Notaría es el encargado de preparar, mantener y difundir los procesos y normas para el reporte de investigación de incidentes de seguridad de la información.

15. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE HERRAMIENTAS, SISTEMAS O SOFTWARE.

Los procesos operativos y estratégicos de la notaría son apoyados con el uso de las tecnologías de la información y las comunicaciones. El software utilizado por la notaría es producido e implementado por Notaria/Notario y por tal razón la notaría realiza el mantenimiento preventivo y correctivo de las herramientas tecnológicas y sistemas.

El Comité de Seguridad de la Información de la Notaría es el encargado de elegir, autorizar y comprar el hardware y las aplicaciones informáticas a utilizar en la notaría, además de evitar autorizar la implementación de software que tenga asociado riesgo no mitigado, asegurar que los aplicativos o sistemas informáticos implementados incluyan los controles de seguridad, difundir procesos, lineamientos, estrategias, buenas prácticas, identificando los riesgos y la forma de mitigarlos, para asegurar la calidad en la implementación de la solución siendo el único que autoriza copias de seguridad del software original, siempre que esté estipulado en la licencia, para ser utilizada en caso de que el medio presente algún daño. El hardware o software adquirido debe especificar los requerimientos de los controles de seguridad y el software adquirido por la notaría no puede ser copiado o suministrado a terceras partes.

Control 1: el Comité de Seguridad de la información debe asegurar y controlar que el hardware o software, adquirido por la notaría, y sus correspondientes mantenimientos se realicen respetando la Política de Seguridad de la Información de la Notaría.

Control 2: el Comité de Seguridad de la Información de la Notaría debe asegurar y controlar el procesamiento correcto de las aplicaciones adquiridas por la notaría para evitar errores, pérdida, modificaciones no-autorizadas o mal uso de la información en las aplicaciones.

Control 3: el Comité de Seguridad de la Información de la Notaría debe chequear y validar las aplicaciones adquiridas, para evitar y controlar los errores de procesamiento o mal uso de estas. También debe identificar los requerimientos de dichas aplicaciones para asegurar, controlar y proteger la autenticidad, integridad y disponibilidad del mensaje.

16. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.

16.1. CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

Control: la notaría mantendrá la seguridad de la información integrada en los sistemas de gestión de continuidad del negocio de la notaría, para lo cual implementará herramientas y actuaciones que le permitan responder rápidamente ante cualquier contingencia.

16.1.1. PLANIFICACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

Control: la notaría desarrollará, documentará, implementará y probará continuamente procedimientos para garantizar recuperación razonable y a tiempo de la información crítica de la notaría, sin disminuir los niveles de seguridad establecidos.

16.1.2. IMPLANTACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

Control 1: la notaría proporcionará recursos necesarios para proporcionar una respuesta efectiva en caso de contingencia o eventos catastróficos que se puedan presentar y que puedan afectar la continuidad de las operaciones de la notaría.

Control 2: la notaría responderá de forma efectiva ante eventos catastróficos según la magnitud y grado de afectación de estos; las operaciones se restablecerán con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos.

Control 3: la notaría mantendrá adecuados canales de comunicación con la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas.

16.1.3. VERIFICACIÓN, REVISIÓN Y EVALUACIÓN DE LA CONTINUIDAD DE LA SEGURIDAD DE LA INFORMACIÓN.

Control: el Comité de Seguridad de la Información de la Notaría realizará pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad de la información durante su realización.

16.2. REDUNDANCIAS.

Control: la Notaría dispondrá de mecanismos y herramientas de procesamiento de información para garantizar la continuidad de negocio de la notaría.

16.2.1. DISPONIBILIDAD DE INSTALACIONES PARA EL PROCESAMIENTO DE LA INFORMACIÓN.

Control 1: la Notaría dispondrá de sistemas redundantes que satisfagan los requerimientos de disponibilidad aceptables para garantizar la continuidad del negocio de la Notaría.

Control 2: el Comité de Seguridad de la Información de la Notaría debe analizar y establecer los requerimientos de redundancia para los sistemas de información críticos de la notaría; además, evaluar y probar soluciones de redundancia tecnológica y seleccionar la herramienta que mejor cumple dichos requerimientos.

Control 3: el Comité de Seguridad de la Información de la Notaría debe realizar pruebas periódicas sobre dichas soluciones, para asegurar el cumplimiento de los requerimientos de disponibilidad para garantizar la continuidad del negocio de la notaría.

17. CUMPLIMIENTO.

La Política de la Seguridad de la Información de la Notaría y los estándares de seguridad de las informaciones legales vigentes son de obligatorio cumplimiento para la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas. Este cumplimiento se debe tener como condición al momento de realizar contrataciones, compromisos o acuerdos con personal que tenga relación con los activos de la información de la notaría.

La Política de la Seguridad de la Información de la Notaría se empieza a implementar con la aprobación del texto de este documento y se debe establecer un plazo máximo para la implementación total de la Política de Seguridad de la Información en las instalaciones, medios y recursos de la notaría.

17.1. REQUISITOS LEGALES Y/O REGLAMENTARIOS.

Control: la notaría debe respetar y velar por el cabal cumplimiento de los requisitos y las normas legales aplicables y vigentes de acuerdo con la constitución y a la ley por parte de la gerencia o dirección, la coordinación, empleados/empleadas, personas proveedoras, clientela, personas usuarias y terceras personas que tienen relación con la seguridad de la información.

17.1.1. MARCO LEGAL

- Constitución Política de Colombia 1991.
- Decreto 960 de 1970 - Estatuto del Notariado.
- Decreto 1260 de 1970.
- Ley 29 de 1973.
- Ley 23 de 1982 de Propiedad Intelectual - Derechos de Autor.
- Decreto 2148 de 1983.
- Decreto 902 de 1988.
- Decreto 999 de 1988.
- Decreto 2668 de 1988.
- Decreto 1555 de 1989.
- Decreto 1556 de 1989.
- Decreto 1557 de 1989.
- Ley 446 de 1998.

- Ley 588 de 2000.
- Ley 527 de 1999, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000 - Ley General de Archivos.
- Código Penal Colombiano - Decreto 599 de 2000.
- Ley 640 de 2001.
- Ley 906 de 2004, Código de Procedimiento Penal.
- Ley 962 de 2005.
- Ley 1098 de 2006 - Código de la Infancia y la Adolescencia.
- Ley 1150 de 2007.
- Ley 1266 de 2008 o Ley del Habeas • Data que regula el manejo de la información contenida en base de datos personales.
- Ley 1273 de 2009, Delitos Informáticos protección de la información y los datos.
- Ley 1341 de 2009
- Decreto 2952 de 2010
- Ley 1437 de 2011 - Código de Procedimiento Administrativo y de lo Contencioso Administrativo.
- Decreto 0019 de 2012 - Ley Anti-Trámites.
- Ley 1581 de 2012 para la Protección de Datos Personales.
- Ley 1564 de 2012 - Código General del Proceso.
- Decreto 2364 de 2012 - Decreto Reglamentario del Artículo 7° de la Ley 527 de 1999.
- Decreto 2609 de 2012, por la cual se reglamenta la Ley 594 de 2000 y Ley 1437 de 2011.
- Decreto 188 de 2013 - Derechos por concepto del ejercicio de la función notarial.
- Decreto 1377 de 2013, por la cual se reglamenta la ley 1581 de 2012.
- Ley 1712 de 2014. Ley de Transparencia y derecho de acceso a la información.
- Decreto 886 de 2014.
- Decreto 1000 de 2015 – Decreto Modifica el artículo 6° del Decreto 188 de 2013.
- Ley 1753 de 2015 - Plan Nacional de Desarrollo 2014-2018.
- Decreto 1083 de 2015.
- CONPES 3854 de 2016.
- Decreto 1413 de 2017.
- Ley 1878 de 2018 – Modifica Ley 1098 de 2006.
- Ley 1943 de 2018 - Ley de Financiamiento.
- Ley 1952 de 2019 - Código General Disciplinario.
- Ley 1955 de 2019 - Plan Nacional de Desarrollo 2018-2022.
- Ley 1996 de 2019 - Ley para el ejercicio de la capacidad legal de las personas.
- Decreto Ley 2106 de 2019.
- Decreto 620 de 2020.
- Decreto 1429 de 2020.

17.1.2. REQUISITOS TÉCNICOS Y REFERENCIAS.

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información.
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO 27001:2005. Sistemas de gestión de Seguridad en la Información– Requerimientos.

Esta Política de Seguridad de la información fue actualizada el 26 de mayo de 2021.

LA NOTARÍA