notaría 3
MEDELLÍN
LUIS DAVID ECHEVERRI DUQUE

POLITICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Dirección: Carrera 48 No. 20-114

PBX: 604 3228221

Celular: 3116480202

Correo electrónico: info@notaria3medellin.com

INTRODUCCIÓN

Los avances tecnológicos en la prestación de los servicios públicos, entre ellos, los notariales, generan la necesidad de implementar un Sistema de Gestión de Seguridad de la Información (SGSI), con el fin de establecer la política y los controles necesarios para mantener la seguridad de esta, adaptados a nuestra planeación estratégica 2020-2029.

Para ello, hemos consultado y estudiado la Guía No 2 del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que contiene los lineamientos para elaborar la política general de seguridad y privacidad de la información, el Modelo de Seguridad y Privacidad de la Información del citado Ministerio y los Lineamientos de Controles Criptográficos de la Presidencia de la de la República.

De igual importancia será la revisión de la normatividad como el Decreto- Ley 960 de 1970 modificado por el Decreto 1769 de 2015, la ley 527 de 1999, Ley 594 de 2000 (Ley General de Archivos y de Gestión Documental), Ley 962 de 2005, Ley 1341 de 2009, Decreto 2364 de 2012, Decreto 019 de 2012, Ley 1581 de 2012, Decreto 1377 de 2013, Ley 1712 de 2014 (Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional), Decreto 103 de 2015, Decreto 1078 de 2015 adicionado por el Decreto 1413 de 2017 y subrogado por el Decreto 620 de 2020 y el Decreto-Ley 2106 de 2019, Decreto 2052 de 2020, entre otros, con e fin que el Sistema de Seguridad de la Información integré toda la normatividad existente, teniendo como fundamento la función fedataria

El Decreto Ley 2106 de 2019, consagra en su artículo 59: "**COMPETE A LOS NOTARIOS.** Se adiciona un parágrafo al artículo 3o del Decreto Ley 960 de 1970, así: "Parágrafo. Para el desarrollo y ejecución de las competencias relacionadas en este artículo, el notario podrá adelantar las actuaciones notariales a través de medios

electrónicos, garantizando las condiciones de seguridad, interoperabilidad, integridad y accesibilidad necesarias.

La Superintendencia de Notariado y Registro expedirá las directrices necesarias para la correcta prestación del servicio público notarial a través de medios electrónicos".

Igualmente, el artículo 63 de la mima ley, consagra la custodia y conservación de los archivos, señalando: "…Cuando los documentos se originen y se gestionen de forma electrónica, se archivarán por el mismo medio, garantizando su seguridad, autenticidad, integridad, accesibilidad, inalterabilidad, disponibilidad y actualización de la información, que a su vez se integrará con la copia electrónica del archivo generado en formato físico, en los términos establecidos por la ley.

Consolidado el archivo digital de los libros, el notario deberá remitir copia del archivo al repositorio que disponga la Superintendencia de Notariado y Registro, conforme a la reglamentación que sobre el particular expida".

Los avances tecnológicos en la producción, conservación y entrega de la información generan la necesidad de crear un sistema que tenga como objetivo principal la seguridad de la misma.

GLOSARIO

(Guía No. 2 para la elaboración de la Política General de Seguridad y Privacidad de la Información de MinTIC)

Acceso a la Información Pública:

Derecho fundamental consistente en la facultad que tienen todas las personas de conocer sobre la existencia y acceder a la información pública en posesión o bajo control de sujetos obligados. (Ley 1712 de 2014, art 4)

Activo:

En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la Organización. (ISO/IEC 27000).

Activo de Información:

En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

Archivo:

Conjunto de documentos, sea cual fuere su fecha, forma y soporte material, acumulados en un proceso natural por una persona o entidad pública o privada, en el transcurso de su gestión, conservados respetando aquel orden para servir como testimonio e información a la persona o institución que los produce y a los ciudadanos, o como fuentes de la historia. También se puede entender como la institución que está al servicio de la gestión administrativa, la información, la investigación y la cultura. (Ley 594 de 2000, art 3)

Amenazas

Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la organización. (ISO/IEC 27000).

Análisis de Riesgo

Proceso para comprender la naturaleza del riesgo y determinar el nivel de riesgo. (ISO/IEC 27000).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencias de auditoría y obviamente para determinar el grado en el que se cumplen los criterios de auditoría. (ISO/IEC 27000).

Autorización:

Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales (Ley 1581 de 2012, art 3)

Bases de Datos Personales:

Conjunto organizado de datos personales que sea objeto de Tratamiento (Ley 1581 de 2012, art 3)

Ciberseguridad

Capacidad del Estado para minimizar el nivel de riesgo al que están expuestos los ciudadanos, ante amenazas o incidentes de naturaleza cibernética. (CONPES 3701).

Ciberespacio

Es el ambiente tanto físico como virtual compuesto por computadores, sistemas computacionales, programas computacionales (software), redes de telecomunicaciones, datos e información que es utilizado para la interacción entre usuarios. (Resolución CRC 2258 de 2009).

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo

asumido. Control es también utilizado como sinónimo de salvaguarda o contramedida. En una definición más simple, es una medida que modifica el riesgo.

Datos Abiertos:

Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos (Ley 1712 de 2014, art 6)

Datos Personales:

Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art 3).

Datos Personales Públicos:

Es el dato que no sea semiprivado, privado o sensible. Son considerados 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. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva. (Decreto 1377 de 2013, art 3)

Datos Personales Privados:

Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular. (Ley 1581 de 2012, art 3 literal h)

Datos Personales Mixtos:

Para efectos de esta guía es la información que contiene datos personales públicos junto con datos privados o sensibles.

Datos Personales Sensibles:

Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos. (Decreto 1377 de 2013, art 3)

Declaración de aplicabilidad

Documento que enumera los controles aplicados por el Sistema de Gestión de Seguridad de la Información – SGSI, de la organización tras el resultado de los procesos de evaluación y tratamiento de riesgos y su justificación, así como la justificación de las exclusiones de controles del anexo A de ISO 27001. (ISO/IEC 27000).

Derecho a la Intimidad:

Derecho fundamental cuyo núcleo esencial lo constituye la existencia y goce de una órbita reservada en cada persona, exenta de la intervención del poder del Estado o de las intromisiones arbitrarias de la sociedad, que le permite a dicho individuo el pleno desarrollo de su vida personal, espiritual y cultural (Jurisprudencia Corte Constitucional).

Encargado del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento. (Ley 1581 de 2012, art 3)

Gestión de incidentes de seguridad de la información

Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información. (ISO/IEC 27000).

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 el artículo 18 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

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 intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo 19 de la Ley 1712 de 2014. (Ley 1712 de 2014, art 6)

Ley de Habeas Data:

Se refiere a la Ley Estatutaria 1266 de 2008.

Ley de Transparencia y Acceso a la Información Pública:

Se refiere a la Ley Estatutaria 1712 de 2014.

Mecanismos de protección de datos personales:

Lo constituyen las distintas alternativas con que cuentan las entidades destinatarias para ofrecer protección a los datos personales de los titulares tales como acceso controlado, anonimización o cifrado.

Plan de continuidad del negocio

Plan orientado a permitir la continuación de las principales funciones misionales o del negocio en el caso de un evento imprevisto que las ponga en peligro. (ISO/IEC 27000).

Plan de tratamiento de riesgos

Documento que define las acciones para gestionar los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma. (ISO/IEC 27000).

Registro Nacional de Bases de Datos:

Directorio público de las bases de datos sujetas a Tratamiento que operan en el país. (Ley 1581 de 2012, art 25)

Responsabilidad Demostrada:

Conducta desplegada por los Responsables o Encargados del tratamiento de datos personales bajo la cual a petición de la Superintendencia de Industria y Comercio deben estar en capacidad de demostrarle a dicho organismo de control que han implementado medidas apropiadas y efectivas para cumplir lo establecido en la Ley 1581 de 2012 y sus normas reglamentarias.

- **Privacidad:**

En el contexto de este documento, por privacidad se entiende el derecho que tienen todos

los titulares de la información en relación con la información que involucre datos personales y la información clasificada que estos hayan entregado o esté en poder de la entidad en el marco de las funciones que a ella le compete realizar y que generan en las entidades destinatarias del Manual de GEL la correlativa obligación de proteger dicha información en observancia del marco legal vigente.

Responsable del Tratamiento de Datos:

Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos. (Ley 1581 de 2012, art 3).

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Suele considerarse como una combinación de la probabilidad de un evento y sus consecuencias. (ISO/IEC 27000).

Seguridad de la información

Preservación de la confidencialidad, integridad, y disponibilidad de la información. (ISO/IEC 27000).

Sistema de Gestión de Seguridad de la Información SGSI

Conjunto de elementos interrelacionados o interactuantes (estructura organizativa, políticas, planificación de actividades, responsabilidades, procesos, procedimientos y recursos) que utiliza una organización para establecer una política y unos objetivos de seguridad de la información y alcanzar dichos objetivos, basándose en un enfoque de gestión y de mejora continua. (ISO/IEC 27000).

Titulares de la información:

Personas naturales cuyos datos personales sean objeto de Tratamiento. (Ley 1581 de 2012, art 3)

Tratamiento de Datos Personales:

Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, art 3).

Trazabilidad

Cualidad que permite que todas las acciones realizadas sobre la información o un sistema de tratamiento de la información sean asociadas de modo inequívoco a un individuo o entidad. (ISO/IEC 27000).

Vulnerabilidad

Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000).

Partes Interesadas (Stakeholder)

Persona u organización que puede afectar a, ser afectada por o percibirse a sí misma como afectada por una decisión o actividad.

POLÌTICA SEGURIDAD DE LA INFORMACIÓN

La Dirección General, con fundamento en los lineamientos establecidos por el Notario Tercero de Medellín, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un Sistema de Gestión de Seguridad de la Información buscando que el ejercicio de la función fedataria delegada

por el Estado Colombiano, se realice enmarcada dentro de nuestros principios institucionales de servicio, legalidad y confianza, de manera que aporte al cumplimiento de nuestros objetivos estratégicos, con fundamento en los lineamientos establecidos por nuestra Misión y Visión, buscando liderar la prestación del servicio público notarial de manera ágil, eficiente y soportada en tecnología de vanguardia.

Para la Notaría Tercera de Medellín, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos que cada día presentan los avances tecnológicos, con el objetivo de mantener un nivel de exposición que permita responder por la integridad, confidencialidad de la misma, acorde con las necesidades de nuestras Partes Interesadas.

Con el fin de garantizar la disponibilidad, integridad y confidencialidad de la información, la Notaría Tercera de Medellín, empleará equipos con los controles criptográficos en toda la Organización, conforme lo establecerán los procedimientos.

Esta política aplica a la Notaría Tercera de Medellín, sus Colaboradores de todo nivel vinculados, contratistas y aprendices, todas las Partes Interesadas, y en general para toda la comunidad, teniendo en cuenta que los principios sobre los que se basa el desarrollo de acciones o la toma de decisiones alrededor del SGSI estarán determinadas por las siguientes premisas:

- Minimizar el riesgo en la información generada en nuestros procesos misionales y de apoyo.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función fedataria.
- Mantener la legalidad y la confianza de nuestros colaboradores, usuarios y de la comunidad en general.

- Apoyar la innovación tecnológica y la estrategia de Gobierno en Línea del Estado Colombiano.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los colaboradores, aprendices, terceros, clientes, aliados estratégicos y en general en todas las Partes Interesadas de la Notaría Tercera de Medellín.
- Garantizar la continuidad en la prestación del servicio público notarial frente a los incidentes.
- La Notaría Tercera de Medellín, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades de nuestra función fedataria, y a los requerimientos de nuestros entes regulatorios y de control.

El Sistema de Gestión de Seguridad de la Información deberá articularse con los Sistema de Gestión de Calidad y Gestión Documental, contribuyendo al incremento de la transparencia en la función pública fedataria.

PRINCIPIOS DE SEGURIDAD QUE SOPORTAN EL SISTEMA DE GESTIÓN Y SEGURIDAD DE LA INFORMACIÓN DE LA NOTARIA TERCERA DE MEDELLIN

1. La Notaría Tercera de Medellín, ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del servicio público notarial y a los requerimiento de los entes reguladores.

2. Las responsabilidades frente a la seguridad de la información serán definidas, publicadas y aceptadas por cada uno de los colaboradores, proveedores y en general por todas las Partes Interesadas.

3. La Notaría Tercera de Medellín, protegerá la información generada, procesada, transmitida o resguardada por los procesos misionales de escrituración, registro civil, autenticaciones, declaraciones extrajuicios y trámites no contenciosos, su infraestructura tecnológica y activos, del riesgo que se genera de los accesos otorgados a terceros (colaboradores, proveedores y usuarios en general).

4. Protegerá la información generada, procesada, trasmitida o resguardada de uso incorrecto, creando los controles necesarios.

5. Protegerá su información de las amenazas originadas por parte de los colaboradores.

6. Protegerá las instalaciones de procesamiento y la infraestructura tecnológica.

7. Controlará la operación de sus procesos misionales, garantizando la seguridad de los recursos tecnológicos y las redes de datos.

8. Implementará control de acceso a la información, sistemas y recursos de red.

9. Garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

10. Garantizará una mejora efectiva de su modelo de seguridad.

11. Garantizará la disponibilidad de sus procesos misionales de escrituración, registro civil, autenticaciones, declaraciones extrajuicio y trámites no contenciosos y la continuidad de su operación.

12. Garantizará el cumplimiento de las obligaciones legales.

13. Asegurará que la información clasificada como pública reservada o información pública clasificada (privada o semiprivada) sea protegida por el usuario generador de la información, con el uso de la herramienta de encripción para transferencias de archivos con esta clasificación, por medio de los sistemas de información y comunicaciones, con el fin de fortalecer la seguridad de la información.

14. El sistema de mensajería instantánea, cumplirá con los requerimientos criptográficos del estandar federal de procesamiento de información FIPS 140-2.

15. El Área de Tecnología y Sistemas deberá verificar que las aplicaciones que utilice, permitan la transmisión de información pública reservada o información pública clasificada (privada o semiprivada), mediante herramientas de cifrado de datos.

16. El Área de Tecnología y Sistemas proveerá la herramienta de encripción de datos a los usuarios, previa solicitud formal.

17. Se utilizarán controles criptográficos en los siguientes casos:

a. En la protección de claves de acceso a sistemas, datos y servicios.
b. Para la transmisión de información Reservada o Clasificada, fuera de la Notaría Tercera de Medellín.
c. En la protección de la información a resguardar cuando así se establezca por la Notaría Tercera de Medellín.

Será responsable del Sistema el Área de Tecnología y Sistemas de la Notaría Tercera de Medellín.

POLÍTICAS ESPECÍFICAS PARA LA IMPLEMENTACIÓN DE CONTROLES DE SEGURIDAD DE LA INFORMACIÓN

1. **ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN:**

Se creará el Comité Directivo de la Seguridad de la Información, conformado por un representante de las siguientes áreas: Dirección General, Tecnología, Sistemas e Infraestructura, Comunicación Organizacional y Administración Web, Gestión Documental, Gestión de la Calidad.

Esté Comité tendrá como Objetivo principal, la creación, actualización y mejoramiento continuo del Sistema de Seguridad de la Información, estableciendo las estrategias, programas, actividades y controles, revisando la política establecida y verificar su cumplimiento.

2. **GESTIÓN DE ACTIVOS:**

Se crearan directrices específicas para que todos los colaboradores tengan pleno conocimiento de los límites en el manejo de la información, señalando los procedimientos frente a la identificación, uso, administración y responsabilidad respecto de los activos de información.

- Identificación de Activos: Se determinaran los diferentes Activos de Información de la Notaría Tercera de Medellín.

- Clasificación de Activos: Cada trimestre se identificará y/o actualizará el inventario de Activos de Información por el líder del Área de Tecnología, Sistemas e Infraestructura en

coordinación con el Área de Gestión Documental con el fin de identificar el propietario del Activo, clasificarlos de acuerdo a la criticidad, sensibilidad y reserva de conformidad con lo normado por la Ley 1581 de 2012, Decreto 1377 de 2013 Ley 1712 de 2014 y Decreto 103 de 2015.

- Etiquetado de la Información: Igualmente debe etiquetarse la información o rotularse los Activos.

- Devolución de los Activos: Cada colaborador y contratista, al terminar la relación laboral deberá realizar la entrega de Activos físicos y de la información, mediante el mecanismo que genere el Área de Tecnología, Sistemas e Infraestructura.

- Gestión de medios removibles: El Comité Directivo, establecerá los usos y permisos que tienen los colaboradores y usuarios de la Notaría Tercera de Medellín frente a los medios removibles, entendiendo por estos, aquellos dispositivos electrónicos que almacenan información y pueden ser extraídos de los computadores. El uso de estos medios removibles debe ir alineado a las clasificaciones de Activos.

- Disposición de los Activos: Es obligatorio la construcción del flujograma del proceso y los procedimientos para realizar de forma segura y correcta la eliminación, retiro, traslado o re uso cuando ya no se requieran los Activos. Se deberá hacer cada 8 días el backup de los activos evitando el accedo o borrado no autorizado de la información. Estas decisiones serán tomadas por la Dirección General con el apoyo del líder del Área de Tecnología, Sistemas e Infraestructura. Esta decisión cobija los medios removibles, activos de procesamiento y/o almacenamiento de información.

- **Dispositivos Móviles**: Todos los Colaboradores, contratistas y en general todos los usuarios de la Notaría Tercera de Medellín que tengan acceso a las redes inalámbricas, deben cumplir con los lineamientos establecidos para la protección y seguridad de la

información; asimismo debe generarse el listado de personal que tiene instalado chat corporativos y/o correos electrónicos de la Notaría mediante el uso de los dispositivos móviles, estableciendo las responsabilidades que tienen en el uso de la información que se encuentra almacenada en los dispositivos móviles pertenezcan o no a la Notaría; estableciéndose claramente por el Área de Tecnología, Sistemas e Infraestructura los controles para proteger, mitigar, supervisar y monitorear los riesgos asociados al acceso y divulgación no autorizada de la información.

3. CONTROL DE ACCESO:

En la Notaría Tercera de Medellín, todos los colaboradores, contratistas y usuarios en general, deberán tener claves y/o contraseñas para el acceso a la información, siendo responsables del buen uso de la información sea física o electrónica.

- Control de acceso con usuario y contraseña: Las redes, aplicaciones y/o sistemas de información de la Notaría deben tener control de acceso y contraseña; estableciéndose por el Área de Tecnología, Sistemas e Infraestructura el procedimiento para la creación, modificación, suspensión o eliminación de usuarios (ID) y contraseñas y las responsabilidades en el uso, debiendo quedar estipulado que son personales e intransferibles y no deben prestarse ni compartirse. Cada uno tendrá su propio usuario.-

- Suministro del control de acceso: Se debe establecer el procedimiento y las directrices para la asignación, modificación, revisión o revocación de derechos y/o privilegios a cada uno de los usuarios (ID) creados. Igualmente describir quiénes tendrán un ID con privilegios superiores utilizados para la administración de infraestructura, aplicaciones y sistemas de información de la Notaría Tercera de Medellín, describiéndose las responsabilidades si violentan la seguridad de la información, la protección de datos personales o la confidencialidad de los procesos misionales poniendo en riesgo la Notaría.

- Gestión de contraseñas: Debe establecerse las exigencias para la creación de contraseñas para ser utilizadas como mecanismo de autenticación en los accesos de red, aplicaciones y/o sistemas de información de la Notaría Tercera de Medellín. Indicar los parámetros mínimos para que una contraseña sea identificada con fuerte, gestión de cambio de contraseña y acceso seguro a la información.

- Perímetros de seguridad: Se debe identificar al interior de las instalaciones de la Notaría Tercera de Medellín, los perímetros físicos de seguridad donde se encuentra información crítica, sensible o se realice almacenamiento y/o procesamiento de información, estableciendo el control de acceso del personal, describiendo el responsable de dar autorización para los accesos.