POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. Objetivo 3
2. Alcance 3
3. Referencias 4
4. Definiciones 4
5. Políticas de seguridad Informática 5
5.1 Políticas de contraseñas 5
5.1.1 Confidencialidad 5
5.1.2 Características de la contraseña 5
5.1.3 Almacenamiento de las contraseñas 5
5.1.4 Sospecha de compromiso de la contraseña 6
5.1.5 Revelación de contraseñas 6
5.2 Política de escritorio limpio y pantalla 6
5.2.1 Bloqueo estación de trabajo 6
5.2.2 Control criptográfico 6
5.3 Política de administración de los recursos informáticos 7
5.3.1 Asignación y uso de los recursos informáticos 7
5.3.2 Prohibición instalación de software y hardware en los computadores. 7
5.3.3 Bloqueo de puertos 7
5.3.4 Control de recursos informáticos entregados a los funcionarios 7
5.3.5 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados. 8
5.3.6 Software de identificación de vulnerabilidades 8
5.3.7 Límite de intentos consecutivos de ingreso al sistema. 8
5.3.8 Respaldo de la información 8
5.3.9 Clasificación de la información 8
5.4 Políticas de internet y correo electrónico 9

5.4.1 Prohibición de uso de internet para propósitos personales. 9
5.4.2 Intercambio de información a través de internet 9
5.4.3 Preferencia por el uso del correo electrónico 9
5.4.4 Chequeo de virus en archivos recibidos en correo electrónico. 9
5.5 Políticas de administración de la red 10
5.5.1 Servicios de red 10
5.5.2 Protección de vulnerabilidades 10
5.5.3 Sincronización de reloj 10
5.5.4 Control de recurso móvil entregados 10
5.6 Políticas de cumplimiento 10
5.6.1 Cumplimiento de la norma 10
5.6.2 Medidas disciplinarias por incumplimiento de la política de seguridad 11
5.6.3 Cumplimiento con la seguridad de la información 11
5.6.4 Declaración de reserva de derechos de la notaría 11
5.7 Políticas de acceso físico 11
5.7.1 Carné del funcionario de la notaría 11
5.7.2 Acceso a zonas restringidas 11
5.7.3 Robo o perdida de identificación 12
5.7.4 Los privilegios de acceso a los recursos informáticos cuando termina el de la notaria 12
5.7.5 Orden de salida de activos 12

Notaria Quinta de Barranquilla	**POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN**

1. OBJETIVO

Establecer políticas o normas en la seguridad de la información que se maneja a través de la notaría, teniendo en cuenta los requisitos legales, operativos, tecnológicos, para los servicios Notariales.

2. ALCANCE

La política de seguridad reglamenta la protección y uso de los activos dispuestos por la notaría para el funcionamiento y está dirigido a todos aquellos funcionarios o usuarios que posean algún tipo de contacto con estos. Los funcionarios de la notaría que ingresan deberán diligenciar un acuerdo de confidencialidad y reserva. El cual refiere el cumplimiento de las políticas de seguridad descritas con el propósito de garantizar la protección de la información que se obtiene a través de los tramites o procesos realizados en la notaría. Los usuarios de la notaría se clasifican así:

A. **Notario**: sea titular, encargado o interino, el Notario es el actor principal por cuanto es el directamente responsable la custodia, resguardo de la seguridad de la información que se desarrolla dentro de las instalaciones de la notaría así, como por la delegación que haga de éste, a algún funcionario de su notaria.

B. **Funcionarios de Notarías**: empleados o colaboradores de planta de la notaría que han suscrito un contrato laboral.

C. Contratistas: Se definen como contratistas, a las personas que han suscrito un contrato con la Notaría y que pueden ser:

- Empleados en Misión.
- Asociados a Entidades Cooperativas.
- Empleados por Outsourcing: Son aquellas personas que laboran en la Entidad y tienen contrato con empresas de suministro de servicios y que dependen de ellos.

D. Entidades de Control

- Procuraduría General de la Nación
- Fiscalía General de la Nación
- Contraloría General de la República.
- Registraduría Nacional del Estado Civil.
- Superintendencia de Notariado y Registro.

- Revisoría Fiscal.
- Firmas Auditoras Externas.

3. REFERENCIAS

Para la implementación de la estrategia de seguridad de la información, la notaría debe regirse por lo dispuesto en el marco jurídico y normativo aplicable a las Notarías o entidades que las regulan y aglutinan.

Decreto-Ley 960 de 1970, Ley 527 de 1999, Decreto-Ley 019 de 201, Resolución 5633 de 2016 de la Registraduría Nacional del Estado Civil, Resolución 14681 de 2015, instrucción Administrativa 03 de 2017 de la Superintendencia de Notariado y Registro y demás reglamentaciones concordantes en el marco jurídico y normativo aplicable a las Notarías o entidades que las regulan.

4. DEFINICIONES

- **Activo**: Cualquier bien que tenga valor para la organización.
- **Acuerdo de Confidencialidad:** Es un documento que debe suscribir todo usuario con el objeto de lograr el acceso a recursos informáticos de la notaría.
- **Contraseña:** Clave de acceso a un recurso informático.
- **Control**: Medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.
- **Seguridad de la Información**: Preservación de la confidencialidad, integridad y disponibilidad de la información, además, otras propiedades tales como autenticidad, responsabilidad, no-repudio y confiabilidad pueden estar involucradas.
- **Política**: Toda intención y directriz expresada formalmente por la notaría.
- **Protector de pantalla**: Programa que se activa a voluntad del usuario, automáticamente después de un tiempo en el que no ha habido actividad.
- **Recursos informáticos:** Son aquellos elementos de tecnología de Información tales como: computadores, servidores de aplicaciones y de datos, computadores de escritorio, computadores portátiles, tableta Biométrica, elementos de comunicaciones, elementos de los sistemas de imágenes, elementos de almacenamiento de información, programas y datos y demás dispositivos que conforman el kit Biométrico tales como: Scanner, captores Biométricos, Impresora, Webcam, Pantalla de Firma Wacom.

5. POLÍTICAS DE SEGURIDAD INFORMÁTICA

Las normas son de obligatoriedad por parte de todos los funcionarios, que se encuentran dentro de la notaría y se han clasificado así:

- Políticas de contraseñas.
- Política de escritorio limpio y pantalla.
- Política de administración de los recursos informáticos.
- Políticas de internet y correo electrónico.
- Políticas de administración de la red.
- Políticas de cumplimiento
- Políticas de acceso físico

5.1 Políticas de contraseñas

5.1.1 Confidencialidad

La contraseña que tendrá el funcionario de la notaría para el acceso a la utilización de los servicios tecnológicos es personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas o aprendidas por otras personas.

5.1.2 Características de la contraseña

Las contraseñas deben contener o cumplir con las siguientes características: incluir mayúsculas, minúsculas y caracteres especiales. El tamaño será validado por el sistema en el momento de generar la contraseña para impedir que sea un tamaño menor. La contraseña no debe contener nombres propios, ni palabras del diccionario, deben ser una mezcla de número, letras y caracteres especiales.

Todos los funcionarios crearan la contraseña al ingresar a la notaría y cada mes realizaran el cambio correspondiente .

5.1.3 Almacenamiento de las contraseñas

Ninguna contraseña debe ser guardada de forma legible en archivos “batch”, scripts, macros, teclas de función de terminal, archivos de texto, en computadores o en otras ubicaciones en donde personas no autorizadas puedan descubrirlas o usarlas. Ningún usuario está autorizado para tener su contraseña en cualquier medio impreso.

5.1.4 Sospecha de compromiso de la contraseña

Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad, se debe informar al funcionario de la notaría encargado de la seguridad de la información indicando en incidente.

5.1.5 Revelación de contraseñas

En ninguna circunstancia está permitido que el funcionario de la notaría revele su contraseña a empleados o terceras personas. La contraseña es personal no beben ser digitada en presencia de terceras personas, así sean funcionarios. Todos los computadores y demás recursos tecnológicos que se encuentran dentro de la Notaria contaran con un sistema de control de acceso.

5.2 Política de escritorio limpio y pantalla

El escritorio del equipo de trabajo asignado a los funcionarios de la notaría deberá estar despejados y ordenados, de tal forma que la información sensible o privada se encuentre resguarda y bajo llave evitando mantenerla a la vista de terceras personas. Es responsabilidad de cada funcionario de la notaría mantener y resguardar la confidencialidad de la información que maneja.

Se debe aplicar un solo fondo de pantalla para las estaciones de trabajo ubicadas dentro de la Notaria este no debe ser alterado o cambiado.

5.2.1 Bloqueo estación de trabajo

Las estaciones o equipos de trabajo de los funcionarios de la notaría tendrán activado un bloqueo automático de estación el cual se activará luego de un periodo de ausencia o inactividad de 5 minutos.

5.2.2 Control criptográfico

Cada notario se encargará o funcionario designado de la administración de la administración de su firma digital (token) el cual es de uso exclusivo, personal e intransferible y deberá realizar todos los procesos correspondientes a las plataformas durante todo su ciclo de vida en la notaría.

El funcionario o administrador del token debe proteger la confidencialidad, integridad e inviolabilidad de la contraseña suministrada por el ente emisor del certificado.

En caso de robo o pérdida informar inmediatamente al área certificadora para efectuar el bloqueo

5.3 Política de administración de los recursos informáticos

5.3.1 Asignación y uso de los recursos informáticos

El uso del computador personal y demás recursos informáticos por parte del empleado, trabajadores o usuarios de la información de la notaría, debe someterse a todas las instrucciones técnicas, que imparta el encargado de la seguridad de la información o técnico por indicación del notario.

El funcionario de la notaría realizara una vez al mes una limpieza de los archivos, temporales, cookies, datos en cache, etc.

5.3.2 Prohibición instalación de software y hardware en los computadores.

La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de cómputo o demás recursos informáticos solo puede ser realizada por el funcionario delegado por el notario.

5.3.3 Bloqueo de puertos

Los equipos asignados a la notaría tendrán el bloqueo de puertos, brindando seguridad y resguardo a la información que se encuentra alojada en los computadores.

5.3.4 Control de recursos informáticos entregados a los funcionarios

Según contrato laboral firmado por el funcionario al momento de vincularse a la Notaria diligenciara el acuerdo de confidencialidad (funcionario).

5.3.5 El usuario es responsable por toda actividad que involucre su identificación personal o recursos informáticos asignados.

Todo funcionario es responsable por todas las actividades relacionadas con su identificación. La identificación no puede ser usada por otro individuo diferente a quien fue otorgada. Los usuarios no deben permitir que otros interesados realicen labores bajo su identidad. De forma similar, los funcionarios no deben realizar actividades bajo la identidad de alguien más.

La utilización de los recursos informáticos por parte de terceras personas con conocimiento o consentimiento del funcionario, o por su descuido o negligencia, lo hace responsable de los posibles daños que estas personas ocasionen a los equipos o a la propiedad de la notaría.

5.3.6 Software de identificación de vulnerabilidades

Los equipos de cómputo tendrán antivirus activo siempre.

5.3.7 Límite de intentos consecutivos de ingreso al sistema.

Todas las contraseñas por defecto que incluyen equipos deberán ser cambiadas siguiendo los lineamientos de la política “Contraseñas fuertes”.

5.3.8 Respaldo de la información

Para salvaguardar la integridad y seguridad de los tramites e información que se maneja dentro de la notaría, estos reposarán en un área establecida bajo las medidas adoptadas por la notaría. Adicional se realizará la digitalización de la información y podrán ser consultados o validados desde la plataforma o recurso designado por la notaría.

5.3.9 Clasificación de la información

Todos los activos de la notaría estarán claramente identificados y se realizara un inventario actualizado. El cual será administrado por el funcionario de la notaría.

Los funcionarios de la notaría recogerán la información que se imprima inmediatamente para evitar la divulgación confidencial.

La información que se manejará dentro de este recinto será directamente de los tramites que genera la notaría.

El funcionario no deberá realizar la divulgación de ninguno de los tramites que se generan la notaría, a terceros. Como persona encargada proporcionara el resguardo, confidencialidad e integridad de la información privada o sensible que se maneja.

5.4 Políticas de internet y correo electrónico

5.4.1 Prohibición de uso de internet para propósitos personales.

El uso del internet está limitado exclusivamente para propósitos laborales. Los usuarios serán notificados.

5.4.2 Intercambio de información a través de internet

La información sensible o privada que los funcionarios de la notaría, necesite ser enviada por internet debe transmitirse con la mayor seguridad posible entre las dos partes.

5.4.3 Preferencia por el uso del correo electrónico

Toda comunicación a través del correo electrónico de los funcionarios se realizará desde los correos corporativos de la notaría correspondiente.

5.4.4 Chequeo de virus en archivos recibidos en correo electrónico.

Cada funcionario de la notaría debe asegurar que todos los archivos descargados de Internet sean chequeados por un software de detección de virus informático, antes de ser transferidos a los computadores.

5.5 Políticas de administración de la red

5.5.1 Servicios de red

Se garantizará que el servicio de red utilizado dentro de la notaría se encuentra disponible y operando adecuadamente según los parámetros establecidos por el notario o encargado.

5.5.2 Protección de vulnerabilidades

Los equipos establecidos dentro de la notaría tendrán activo un antivirus de protección.

5.5.3 Sincronización de reloj

Todos los equipos de la notaría deben ser sincronizados según la zona horaria establecida para Colombia-Bogotá, los cuales no deben ser alterados, ni modificados en caso de presentarse alguna alteración con el sistema inmediatamente informar al funcionario encargado de la notaría.

5.5.4 Control de recurso móvil entregados

Al generar la entrega del móvil al funcionario de la notaría firmará el formato de entrega, este será para usos exclusivo de la notaría, en caso de robo o perdida informar al funcionario encargado o técnico.

5.6 Políticas de cumplimiento

5.6.1 Cumplimiento de la norma

Todos los funcionarios que se encuentren dentro de la notaría deben cumplir con los estándares de normas y controles vigentes, antes de realizar el ingreso al área establecida.

5.6.2 Medidas disciplinarias por incumplimiento de la política de seguridad

Cualquier incumplimiento de una política de seguridad de la información, estándar, o procedimiento es un argumento válido para que sea tomada cualquier acción disciplinaria.

5.6.3 Cumplimiento con la seguridad de la información

Todos los colaboradores o funcionarios de la notaría deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información.

5.6.4 Declaración de reserva de derechos de la notaría

La notaría usa controles de acceso y otras medidas de seguridad para proteger la confidencialidad, integridad y disponibilidad de la información manejada en computadores y sistemas de información. Para mantener estos objetivos la notaría se reserva el derecho y la autoridad de: 1. Restringir o revocar los privilegios de cualquier funcionario; 2. Inspeccionar, copiar, remover cualquier dato, programa u otro recurso que vaya en contra de los objetivos antes planteados; y, 3. Tomar cualquier medida necesaria para manejar y proteger los sistemas de información de la notaría. Esta autoridad se puede ejercer con o sin conocimiento de los funcionarios, bajo la responsabilidad del funcionario o técnico designado y el notario.

5.7 Políticas de acceso físico

5.7.1 Carné del funcionario de la notaría

Los funcionarios de la notaría durante la permanencia en la Notaria deben portar el carné de esta y el de la ARL en un sitio visible desde el momento de ingreso.

5.7.2 Acceso a zonas restringidas

Los funcionarios que se encuentra dentro de la notaría no podrán dejar ingresar a personal externo a zonas restringidas.

5.7.3 Robo o perdida de identificación

En caso de robo o pérdida del carné de la notaría se debe informar inmediatamente tanto al notario o persona encargada de la notaría.

5.7.4 Los privilegios de acceso a los recursos informáticos cuando termina el de la notaria

Todos los privilegios sobre los recursos informáticos de la notaría otorgados a los funcionarios serán eliminados en el momento de la culminación de este.

5.7.5 Orden de salida de activos

Todos los activos que afecten la seguridad de la información de la notaría como medios de almacenamiento, CD, DVD., entre otros, y que necesiten ser retirados de la entidad, deben ser autorizados por el notario o funcionario encargado para su salida.