# POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN DEL PROYECTO SISTEMA DE AUTENTICACIÓN BIOMÉTRICA EN LÍNEA NOTARIAL.

## PO-TEC-001

| | | | | | |
|---|---|---|---|---|---|
| **5** | 14/01/2025 | Coordinador de tecnologías de la información. | Coordinador Mesa de Soporte | Director de Proyectos | Actualización definiciones, cambio líneas soporte |
| **4** | 25/10/2022 | Coordinador de tecnologías de la información. | Coordinador Mesa de Soporte | Director de Proyectos | Cambio de entidades de control, líneas de soporte, cambio límite de intentos consecutivos |
| **3** | 22/04/2021 | Líder de Proyectos | Oficial de Seguridad de la Información | Director de Proyectos | Nuevo aplicativo – Portal web<br>Cambio de contraseñas<br>Ingreso al portal Web |
| **2** | 10/12/2020 | Líder de Proyectos | Oficial de Seguridad de la Información | Director de Proyectos | Nuevo aplicativo – Portal web<br>Cambio de contraseñas<br>Ingreso al portal Web |
| **1** | 12/06/2019 | Líder de Proyectos | Director de Proyectos | Director de Proyectos | Actualización de canales de comunicación<br>Eliminación de usuarios |
| **Inicial** | 27/05/2016 | Director de Proyectos | Gerente General | Presidencia | Primera edición |
| **Versión** | **Fecha** | **Elaboró** | **Revisó** | **Aprobó** | **Descripción de la Revisión** |

## CONTROL DEL DOCUMENTO

## TABLA DE CONTENIDO

## 1. INTRODUCCIÓN

Mejorar la estrategia de Seguridad de la Información del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, surge la necesidad de buscar un modelo base que permita alinear los procesos hacia un mismo objetivo de seguridad en el manejo de la información.
Para tal fin, se establece una Política de la Seguridad de la Información, como marco de trabajo de la organización, buscando niveles adecuados de protección y resguardo de la información, definiendo sus lineamientos, para garantizar el debido control y minimizar los riesgos asociados.

## 2. OBJETIVO

Este documento establece las normas para proteger de posibles riesgos de daño, pérdida y uso indebido de la información, los equipos y demás recursos informáticos que hacen parte del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, definir los lineamientos que debe seguir las Notarías con relación a la seguridad de la Información. Estos lineamientos están escritos en forma de políticas.

## 3. ALCANCE

El documento de Política de Seguridad de la información del Proyecto Sistema de Autenticación Biométrica en Línea Notarial reglamenta la protección y uso de los activos del proyecto. Por tanto, está dirigido a todos aquellos usuarios que posean algún tipo de contacto con estos activos. Los usuarios que tengan acceso al sistema se comprometen al cumplimiento de las políticas de seguridad aquí descritas. Los usuarios de los activos de información de la notaría se clasifican así:

**A. Notario:** Bien sea titular, encargado o interino, el Notario es el actor principal del Sistema de Identificación y Autenticación Biométrica en Línea por cuanto es el directamente responsable por el uso, mantenimiento y custodia del sistema, así, como por la delegación que haga de éste, a algún funcionario de su notaria.

**b. Funcionarios de Notarías:** empleados de notarías que acceden el Sistema de Autenticación Biométrica en Línea.

**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.

- Personas naturales que prestan servicios independientes a la Entidad.
- Proveedores de recursos informáticos.

**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.
- "U.C.N.C."
- Wireles and Mobile W&M
- GSE
-

## 4. REQUISITOS LEGALES Y/O REGLAMENTARIOS

La implementación de la estrategia de seguridad de la información contenida en el sistema de identificación y autenticación biométrica en línea, debe regirse por lo dispuesto en 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.

## 5. DEFINICIONES

Para los propósitos de este documento se aplican los siguientes términos y 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 **"U.C.N.C."**
- **Administradores:** Usuarios a quienes la **"U.C.N.C."** ha dado la tarea de administrar los recursos informáticos y poseen un identificador que les permite tener privilegios administrativos sobre los recursos informáticos de la **"U.C.N.C."**, quienes estarán bajo la dirección de la Presidencia de la Entidad.

- **Amenaza**: Causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.
- **Análisis de Riesgos**: Uso sistemático de la información para identificar las fuentes y estimar el riesgo.
- **Backup**: Copia de la información en un determinado momento, que puede ser recuperada con posterioridad.
- **Circulo Notarial**: Los círculos registrales o Notariales son donde corresponde efectuar el reparto notarial, según se trate de círculos notariales que cuentan con dos o más notarías. Es decir, deben realizar trámites Notariales dentro del mismo Municipio a ello hace referencia el circulo que pertenece la Notaria.
- **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.
- **Derecho moral**: Es la relación intangible que une al creador de una obra y su obra, es un derecho inalienable, nadie puede expropiar ese derecho.
- **Derechos patrimoniales**: Los derechos patrimoniales de una obra referencia a la forma en cómo se puede utilizar, o recibir algún tipo de beneficio de la obra. Es un derecho temporal, expropiable disponible, renunciable y embargable.
- **Directrices**: Descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.
- **Evaluación de Riesgos**: Todo proceso de análisis y valoración del riesgo.
- **Evento de seguridad de la información**: Un evento de seguridad de la información es la presencia identificada de un estado del sistema, del servicio o de la red que indica un posible incumplimiento de la política de seguridad de la información, una falla de controles, o una situación previamente desconocida que puede ser pertinente para la seguridad.
- **Firewall**: Conjunto de recursos de hardware y software que protegen recursos informáticos de accesos indebidos.
- **Freeware:** Software de computador que se distribuye sin ningún costo, pero su código fuente no es entregado.
- **Gestión del riesgo**: Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.
- **GPS**: Es un sistema que permite determinar en toda la Tierra la posición de un objeto (una persona, un vehículo) con una precisión de hasta centímetros (si se utiliza GPS diferencial), aunque lo habitual son unos pocos metros de precisión. El sistema fue desarrollado, instalado y empleado por el Departamento de Defensa de los Estados Unidos. Para determinar las posiciones en el globo, el sistema GPS se sirve de 24 satélites y utiliza la trilateración.

- **Incidente de seguridad de la información**: Está indicado por un solo evento o una serie de eventos inesperados o no deseados de seguridad de la información que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.
- **Información pública:** Es la información administrada por la **"U.C.N.C."**, que está a disposición del público en general; un ejemplo son los catálogos de productos y servicios.
- **LAN:** Grupo de computadores y dispositivos asociados que comparten un mismo esquema de comunicación y se encuentran dentro de una pequeña área geográfica (un edificio o una oficina).
- **Licencia de Software:** Es la autorización o permiso concedido por el dueño del programa al usuario para utilizar de una forma determinada y de conformidad con unas condiciones convenidas. La licencia precisa los derechos (de uso, modificación, o redistribución) concedidos a la persona autorizada y sus límites, además puede señalar el lapso de duración y el territorio de aplicación.[1]
- **Módem (Modulador - Demodulador de señales):** Elemento de comunicaciones que permite transferir información a través de líneas telefónicas.
- **Monitoreo**: Verificación de las actividades de un usuario con respecto a los recursos informáticos de la **"U.C.N.C."**
- **Open Source (Fuente Abierta)**: Es el término por el que se conoce al software que es distribuido y desarrollado de forma libre, en el cual la licencia específica el uso que se le puede dar al software.
- **OTP (One Time Password):** Contraseña entregada por el administrador de un recurso informático que permite el primer acceso a dicho recurso y obliga al usuario a cambiarla una vez ha hecho este acceso.
- **Plan de contingencia**: Plan que permite el restablecimiento ágil en el tiempo de los servicios asociados a los Sistemas de Información de la **"U.C.N.C."** en casos de desastres y otros casos que impidan el funcionamiento normal.
- **Política**: Toda intención y directriz expresada formalmente por la dirección.
- **Propiedad Intelectual**: Es una disciplina normativa que protege las creaciones intelectuales provenientes de un esfuerzo, trabajo o destreza humana, dignos de reconocimiento jurídico.[2]
- **Protector de pantalla**: Programa que se activa a voluntad del usuario, o automáticamente después de un tiempo en el que no ha habido actividad.
- **Proxy**: Servidor que actúa como puerta de entrada a la Red Internet.
- **Recursos informáticos**: Son aquellos elementos de tecnología de Información tales como: computadores, servidores de aplicaciones y de datos, computadores de escritorio,

[1] Tomado del diccionario Wikipedia. http://es.wikipedia.org/wiki/Licencia_de_software
[2] Tomado de http://www.derautor.gov.co/htm/preguntas.htm#01

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.

- **Riesgo**: Combinación de la probabilidad de un evento y sus consecuencias.
- **Router**: Equipo que permite la comunicación entre dos o más redes de computadores.
- **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.
- **Servicios de procesamiento de información**: Cualquier servicio, infraestructura o sistema de procesamiento de información o los sitios físicos que los albergan.
- **Sesión**: Conexión establecida por un usuario con un Sistema de Información.
- **Shareware:** Clase de software o programa, cuyo propósito es evaluar por un determinado lapso de tiempo, o con unas funciones básicas permitidas. para adquirir el software de manera completa es necesario un pago económico.
- **Sistema de control de acceso**: Elementos de hardware o software que autorizan o niegan el acceso a los recursos informáticos de acuerdo con políticas definidas.
- **Sistema de detección de intrusos (IDS)**: Es un conjunto de hardware y software que ayuda en la detección de accesos o intentos de acceso no autorizados a los recursos informáticos.
- **Sistema multiusuario**: Computador y su software asociado, que permiten atender múltiples usuarios a la vez a través de las redes de comunicación.
- **Sistema operativo**: Software que controla los recursos físicos de un computador.
- **Sistema sensible:** Es aquel que administra información confidencial o de uso interno que no debe ser conocida por el público en general.
- **Software de Dominio Público:** Tipo de software en que no se requiere ningún tipo de licencia y cuyos derechos de explotar, usar, y demás acciones son para toda la humanidad, sin que con esto afecte a su creador, dado que pertenece a todos por igual. En términos generales software de dominio público es aquel en el cual existe una libertad total de usufructo de la propiedad intelectual.
- **Software Libre**: Software que una vez obtenido puede ser usado, copiado, modificado, o redistribuido libremente, en el cual la licencia expresamente especifica dichas libertades.
- **Software pirata:** Es una copia ilegal de aplicativos o programas que son utilizados sin tener la licencia exigida por ley.
- **Tercera parte**: Persona u organismo reconocido por ser independiente de las partes involucradas, con relación al asunto en cuestión.
- **Usuario**: toda persona que pueda tener acceso a un recurso informático de la **"U.C.N.C."**
- **Usuarios de red y correo**: Usuarios con los cuales la **"U.C.N.C."** ha establecido un

contrato de al menos 30 días de duración y a quienes se les entrega un identificador de cliente para acceso a sus recursos informáticos.

- **Usuarios externos con contrato**: Usuarios externos con los cuales la Notaría establece un contrato y a quienes se da acceso limitado a recursos informáticos de uso interno.
- **Usuarios externos**: Son aquellos clientes externos que utilizan los recursos informáticos de la Notaría a través de Internet o de otros medios y tienen acceso únicamente a información clasificada como pública.
- **Valoración del riesgo**: Proceso de comparación del riesgo estimado frente a criterios de riesgo establecidos para determinar la importancia del riesgo.
- **Vulnerabilidad**: Debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

## 6. RESPONSABLES

### 6.1. COMPROMISO DEL NOTARIO

El Notario como responsable en el ejerció de sus funciones y por lo tanto del sistema de identificación y autenticación biométrica en línea, se compromete a:

Brindar evidencia de su compromiso con el establecimiento, implementación, operación, seguimiento, revisión, mantenimiento y mejora de los mecanismos para asegurar información:

- Mediante el seguimiento de la política de seguridad de la información;
- Asegurando el cumplimiento de los objetivos y planes de seguridad de la información;
- Cumpliendo las funciones y responsabilidades de la seguridad de la información;
- Comunicando a los funcionarios de la Notaría la importancia de cumplir los objetivos de seguridad de la información, las responsabilidades legales, y las necesidades de la mejora continua.

### 6.2. COMPROMISOS DE LOS FUNCIONARIOS QUE OPERAN EL SISTEMA.

El funcionario designado por el notario para responsabilizarse de la operación del sistema de identificación y autenticación biométrica en línea, se compromete a:

- Manejar de manera confidencial la información que le sea presentada y entregada, especialmente, la obtenida a través del sistema de identificación y autenticación biométrica en línea, esta es de orden restringido y su uso constituye reserva legal y solo puede ser revelada previa autorización del titular o por orden judicial o autoridad competente.

- Guardar confidencialidad sobre esa información y no emplearla ni revelarla en beneficio propio o de terceros bajo ninguna circunstancia, sin perjuicio de orden judicial o de autoridad competente.
- A dar cumplimiento a la Ley 1581 de 2012 de protección de datos personales (habeas data). El desconocimiento de los compromisos descritos, puede conllevar demandas civiles, penales y administrativas según lo señalan las leyes colombianas. (Artículo 308, Ley 599 de 2000; Ley 256 de 1996; Decisión 486 de la CAN, Tit. XVI).
- Atender, cuidar y responder por la estación del sistema de identificación y autenticación biométrica con el cuidado y diligencia del que habla el artículo 63 del Código Civil Colombiano Ins 2. "*Culpa leve, descuido leve, descuido ligero, es la falta de aquella diligencia y cuidado que los hombres emplean ordinariamente en sus negocios propios. Culpa o descuido, sin otra calificación, significa culpa o descuido leve. Esta especie de culpa se opone a la diligencia o cuidado ordinario o mediano. El que debe administrar un negocio como un buen padre de familia, es responsable de esta especie de culpa.*"
- Responder por el uso y cuidado del kit biométrico, así como de la conservación de las contraseñas derivadas del mismo, las que deben ser custodiadas en total confidencialidad, en un lugar seguro, fuera del acceso de terceros.

### 6.3. MEDIDAS DE SEGURIDAD SOBRE LOS RECURSOS TECNOLÓGICOS

- Asegurar que las políticas de seguridad de la información brinden apoyo a los requisitos de la Notaría.
- Identificar y atender los requisitos legales y reglamentarios, así como las obligaciones de seguridad contractuales.
- Mantener la seguridad suficiente mediante la aplicación correcta de todos los controles implementados.
- Asegurar que todo el personal tome conciencia de la importancia de la seguridad de la información.

## 7. POLITICAS DE SEGURIDAD

Las políticas de seguridad informática tienen como objetivo reducir el riesgo de incidentes de seguridad y minimizar su efecto. Establecen las reglas básicas con las cuales la organización debe operar sus recursos informáticos. El diseño de las políticas de seguridad informática está encaminado a disminuir y eliminar muchos factores de riesgo.

## 7.1. POLÍTICA DE SEGURIDAD PARA LAS NOTARÍAS

Se reconoce la importancia de la seguridad informática, así como la necesidad de su protección para constituir un activo estratégico de la Notaría, el no uso adecuado de los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial puede poner en peligro la continuidad de este o al menos suponer daños muy importantes que afecten el normal funcionamiento de los procesos.

El Notario, los funcionarios, terceros y en general deberán conocer el presente documento, normas, reglas, estándares y procedimientos que apliquen según las funciones que realicen para la organización, el desconocimiento que conlleve a la violación de lo anteriormente mencionado representará para la persona involucrada las sanciones disciplinarias que apliquen según el incidente presentado.

Igualmente se implementarán los controles de seguridad encaminados a garantizar la confidencialidad, integridad y disponibilidad de los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, con el objetivo de lograr un nivel de riesgo aceptable de acuerdo con la visión, misión, planeación y estrategia del proyecto, y dando cumplimiento al marco jurídico aplicable a los estándares nacionales.

## 7.2. POLÍTICAS GENERALES DE SEGURIDAD INFORMÁTICA.

Estas normas son de obligatorio cumplimiento por parte de todos los usuarios de recursos informáticos y se han clasificado en:

- ✓ Políticas de Cumplimiento y Sanciones
- ✓ Políticas de uso de recursos informáticos.
- ✓ Políticas de uso de las contraseñas.
- ✓ Políticas de uso de la información.
- ✓ Políticas del uso de Internet y correo electrónico.
- ✓ Políticas Generales para usuarios y personal de la Notaría.
- ✓ Políticas para Administradores de Sistemas.
- ✓ Políticas de Uso de Firewall.
- ✓ Políticas para Usuarios Externos.
- ✓ Políticas de Acceso Físico.

## 7.3. POLÍTICAS DE CUMPLIMIENTO Y SANCIONES

- **Cumplimiento con la seguridad de la información**
  Todos los colaboradores de la Notaría, deben cumplir y acatar el manual de políticas y los procedimientos en materia de protección y seguridad de la información. Corresponde velar por

su estricto cumplimiento al Notario en cada una de las Notarías.

- **Medidas disciplinarias por incumplimiento de políticas de seguridad**
  Cualquier incumplimiento de una política de seguridad de la información, estándar, o procedimiento es un argumento válido para la suspensión del permiso de uso del servicio de biometría, sin perjuicio a las sanciones de ley a que haya a lugar, o terminación del contrato laboral de los usuarios de los sistemas de información de la Notaría.

## 7.4. POLÍTICAS DE USO DE RECURSOS INFORMÁTICOS

- **Instrucciones para el uso de recursos informáticos.**
  El uso de los recursos informáticos por parte del empleado, trabajadores o usuarios del Proyecto Sistema de Autenticación Biométrica en Línea para las estaciones fijas y móviles debe considerar todas las instrucciones técnicas, que imparta la **"U.C.N.C."**.

- **Uso personal de los recursos informáticos.**
  Los activos del Proyecto Sistema de Autenticación Biométrica en Línea para las estaciones fijas y móviles solo deben ser usados para fines laborales y prestación del servicio de autenticación biométrica en línea a los usuarios finales de las Notarías. El producto del uso de dichos recursos tecnológicos está sometido a reserva legal y solo podrá ser entregado a autoridad judicial o administrativa competente.

  No se permite el almacenamiento de datos biográficos y biométricos en memorias externas SD, micro SD u otros medios.

- **Prohibición de instalación de software y hardware en los computadores de la organización.**
  La instalación de hardware o software, la reparación o retiro de cualquier parte o elemento en los equipos de computación o demás recursos informáticos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial a solo puede ser realizada con previa autorización por parte de la **"U.C.N.C."**

  Para los Dispositivos móviles o tabletas biométricas, la gestión de software será administrada por el componente MDM asignado al proyecto; por otra parte, no se permite hacer ningún tipo de modificación a la tableta a nivel de hardware.

- **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 dicha

identificación. Los funcionarios no deben permitir que otros usuarios 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 del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, para las estaciones fijas y móviles.

- **Acceso no autorizado a los sistemas de información de la notaría**
  Está totalmente prohibido obtener acceso a sistemas de información a los que no se tiene privilegios y de alguna forma dañar o alterar la operación de dichos sistemas. Esto implica la prohibición de capturar contraseñas, llaves de encriptación y otros mecanismos de control de acceso que le puedan permitir obtener ingreso no autorizados a los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

- **Posibilidad de acceso no implica permiso de uso.**
  Los usuarios no deben leer, modificar, copiar, borrar, compilar, sustraer, interceptar, modificar, recolectar, almacenar, replicar o complementar la base de datos, a partir de la información biométrica obtenida en el proceso.

- **Prohibición de Cambios de Software y Hardware de los recursos informáticos y explotación de vulnerabilidades.**
  A no ser que exista una aprobación por escrito para ello por parte de la **"U.C.N.C."**, los usuarios no deben explotar las deficiencias de seguridad, reemplazar, actualizar o reconfigurar ningún elemento de Hardware o Software de los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, obtener acceso a recursos a los cuales no se les ha dado acceso. En el caso de encontrar vulnerabilidades, estas deben ser reportadas de inmediato la **"U.C.N.C."**.

- **Dejar sistemas sensibles desatendidos.**
  Si el usuario está conectado a los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial, éste no debe dejar la sección de usuario del computador o tableta Biométrica desatendida.

- **Notificación de sospecha de pérdida, divulgación o uso indebido de información sensible.**
  Cualquier incidente de Seguridad debe reportarse inmediatamente a los canales de atención y soporte (Ver Numeral 8 Canales de comunicación)

- **Traslado de equipos estaciones fijas.**
  Ningún equipo de cómputo asignado por la "U.C.N.C.", o elemento de kit biométrico debe ser

reubicado o trasladado fuera de las instalaciones de la notaria a las cuales fue asignado, sin previa autorización de la “U.C.N.C.”. El traslado de los equipos se debe hacer con las medidas de seguridad necesarias, por el personal autorizado de la Notaría.

- **Traslado de equipos estaciones Móviles**
  La tableta Biométrica esta asignada a una única Notaría, por lo tanto, el uso de Identificación Biométrica en línea debe ser realizado dentro de su círculo Notarial.
  Por lo anterior, no puede ser utilizada en otro Circulo Notarial que no sea asignado, para realizar estos cambios la “U.C.N.C” la asignará a otro Círculo de ser el caso.

- **Precauciones para el uso de los recursos informáticos.**
  Está prohibida la ingestión de bebidas u otro tipo de alimentos sobre o en las proximidades de cualquiera de los recursos informáticos, así como el manejo de sustancias o elementos que puedan ocasionar daños a los mismos.

  Para dispositivos móviles o tableta biométrica, evitar los impactos o caídas.

  Evitar el uso de los recursos informáticos por personas ajenas a las autorizadas por la Notaría. Se prohíbe la manipulación de los sellos de seguridad, la apertura o procesos de reingeniería sobre la tableta.

- **Monitoreo de Software instalado estaciones fijas**
  Regularmente se deben realizar actividades de monitoreo sobre el software instalado en cada uno de los equipos de la organización, lo anterior para asegurar que los programas instalados correspondan correctamente con las licencias adquiridas por la Notaría.

- **Monitoreo de Software instalado estaciones Móviles**
  La función del Monitoreo, bloqueo y desbloqueo, se realizará a través de aplicación del MDM, implementado para esta arquitectura.

- **Custodia de Licencias de Software**
  Las licencias deben ser custodiadas y controladas. Se debe realizar auditorías de licencia de software como mínimo una vez al año generando las evidencias respectivas, lo anterior para garantizar que los funcionarios solo tienen instalado software legal en los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

- **Uso de GPS**

De acuerdo al numeral 7.13.1 de la Resolución 5633 de 2016, cada identificación Biométrica realizada deberá contar con su respectiva geolocalización, la cual será obtenida por la coordenada de latitud y longitud del GPS del dispositivo móvil al momento de realizar el cotejo. En caso de no ser obtenidas las coordenadas no podrá realizarse el cotejo Biométrico.

- **Apagado de equipos en la noche**
  Los equipos de cómputo de usuario deben quedar apagados durante la noche, esto es con fin de proteger la seguridad y distribuir bien los recursos de la Notaría.

## 7.5. POLÍTICAS DE USO DE LAS CONTRASEÑAS

- **Confidencialidad de las contraseñas.**
  Las credenciales de autenticación como lo son, certificado digital, tokens, contraseñas, usuario o patrón para el acceso o uso del sistema Identificación y Autenticación Biométrica en línea, debe ser personal, confidencial e intransferible. Cada usuario debe velar porque sus contraseñas no sean vistas y aprendidas por otras personas, en caso de olvido de la misma debe solicitar la asignación de una nueva clave al notario titular o encargado de la notaría. Así mismo en caso de pérdida del token, el notario debe solicitar la revocación del certificado digital a la **"U.C.N.C."**, asumiendo el costo que pueda tener este trámite.

- **Identificación única para cada usuario estación fija**
  Los notarios titulales, encargados y funcionarios contarán con el acceso de identificación única personal y su respectiva contraseña asignada por el Notario titular. Cada usuario tendrá una identificación única en cada sistema al que tenga acceso, acompañado de un elemento para su autenticación (contraseña) de carácter personal y confidencial para la utilización de los recursos tecnológicos necesarios para sus labores.

- **Identificación única para cada usuario estación móvil**
  Los notarios titulares y sus encargados contarán con acceso al sistema con contraseña, usuario y certificado digital, los funcionarios de la notaria contarán con una identificación única personal y su respectiva contraseña y como un segundo factor, por seguridad de acceso al sistema.

- **Cambios periódicos de contraseñas.**
  El mecanismo de ingreso al sistema de Identificación y Autenticación Biométrica en línea, para Notarios titulares o encargados se realiza mediante credenciales de acceso, usuario y contraseña, cada Notario deben garantizar la confidencialidad de las contraseñas, estas deben ser cambiadas periódicamente. La periodicidad dependerá de la criticidad de la información a la que dan acceso, se sugiere que se realice cada 3 meses. No deben utilizarse contraseñas que hayan sido usadas con anterioridad.

- **Longitud mínima de contraseñas.**
  Todas las contraseñas deben tener una longitud mínima de SEIS (6) caracteres que debe cumplir con algunas de las siguientes características: Incluir combinación de números, letras mayúsculas, minúsculas. Este tamaño debe ser validado por el sistema en el momento de generar la contraseña para impedir un tamaño menor.

- **Contraseñas fuertes.**
  Las contraseñas no deben ser nombres propios ni palabras del diccionario, debe ser una mezcla de números, letras y/o caracteres especiales.

- **Prohibición de contraseñas cíclicas.**
  No se debe generar contraseñas compuestas por una combinación fija de caracteres y una combinación variable pero predecible. Un ejemplo de este tipo de contraseñas prohibidas es "Enero-2004" que según la política "Contraseñas fuertes", es una contraseña válida, pero al mes siguiente pasa a ser "Febrero-2004" y así sucesivamente.

- **Las contraseñas creadas por usuarios no deben ser reutilizadas.**
  El usuario no debe generar una contraseña idéntica o sustancialmente similar a una que ya haya utilizado anteriormente. Esta política es complementada por la política "Prohibición de contraseñas cíclicas".

- **Sospechas de compromiso deben forzar cambios de contraseña.**
  Toda contraseña deberá ser cambiada de forma inmediata si se sospecha o se conoce que ha perdido su confidencialidad.

- **Revelación de contraseñas prohibida.**
  En ninguna circunstancia está permitido revelar la contraseña a empleados o a terceras personas.
  La contraseña personal no debe ser digitada en presencia de terceras personas, así sean funcionarios de la Notaría.
  Ningún usuario deberá intentar obtener contraseñas de otros usuarios. Las contraseñas no deben de compartirse con nadie.
  Todas las contraseñas deben ser tratadas como sensibles, como Información confidencial de la Notaría.
  Las contraseñas no se deben adjuntar en mensajes de correo electrónico u otras formas de comunicación electrónica.
  No escriba ni guarde contraseñas en post-its o papel en cualquier lugar de su oficina.
  No guarde las contraseñas en archivos en su computadora o dispositivos móviles (teléfonos, tablets) sin cifrado.

- **Bloqueo estación de trabajo.**
  Todas las estaciones de trabajo de los usuarios deben tener activado el bloqueo automático de estación, el cual debe activarse luego de un período de ausencia o inactividad de 5 minutos.
  Por otra parte, el escritorio del equipo de trabajo debe estar despejado y ordenado, de tal forma que la información que se encuentre en el puesto de trabajo o en la pantalla (escritorio) del equipo sea estrictamente la suficiente y necesaria para la labor desempeñada.

## 7.6. POLÍTICAS DE USO DE LA INFORMACIÓN

- **Divulgación de la información manejada por los Notarios y los funcionarios autorizados por estos.**
  La **"U.C.N.C."** podrá divulgar la información de un usuario almacenada en los sistemas de acuerdo con la autorización suscrita por él mismo, por disposición legal o salvo las excepciones indicadas en este documento.

- **Transferencia de datos solo a organizaciones con suficientes controles.**
  La Notaría puede transmitir información privada solamente a entidades públicas en el marco de sus funciones de control, inspección, vigilancia, investigación y en general cualquier competencia legal que legitime la solicitud, que por escrito se comprometan a mantener dicha información bajo controles adecuados de protección. Se da una excepción en casos en los que la divulgación de información es forzada por la ley.

- **Registro de las compañías que reciben información privada.**
  El personal de la Notaría que liberó información privada a entidades públicas en el marco de sus funciones de control, inspección, vigilancia, investigación y en general cualquier competencia legal que legitime la solicitud debe mantener un registro de toda divulgación y este debe contener qué información fue revelada, a quién fue revelada y la fecha de divulgación.

- **Transferencia de la custodia de información de un funcionario que deja la Notaría**
  Cuando un empleado se retira de la Notaría, El Notario debe revisar tanto los archivos magnéticos, correo electrónico como documentos impresos para determinar quién se encargará de dicha información, procesos y procedimientos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

- **Eliminación Segura de la Información en Medios Informáticos**
  Todo medio informático reutilizable de terceros como equipos rentados, discos externos, memorias USB, etc. utilizados por la Notaría, antes de su entrega se les realizara un proceso de borrado seguro en la información.

## 7.7. POLÍTICAS DEL USO DE INTERNET Y CORREO ELECTRÓNICO

- **Uso de Internet para propósitos personales.**
  En cuanto al uso de Internet debe ser para propósitos laborales. Los usuarios de Internet deben ser advertidos sobre las vulnerabilidades que conlleva el acceso a sitios no recomendados, la consulta de redes sociales o la descarga de Software de dudosa procedencia en los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

  Para las estaciones móviles el MDM, restringe acceso a enlaces, aplicativos, que no son permitidos para el uso del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

- **Formalidad del correo electrónico.**
  Toda comunicación a través del correo electrónico interno se considera una comunicación de tipo laboral y formal, por tanto, podrá ser supervisada por el Notario.

- **Preferencia por el uso del correo electrónico.**
  Debe preferirse el uso del correo electrónico al envío de documentos físicos siempre que las circunstancias lo permitan.

- **Revisión del correo electrónico Institucional.**
  Las Notarías que dispongan de correo electrónico institucional con la **"U.C.N.C."** están en la obligación de revisarlo al menos dos veces diarias. Así mismo, es su responsabilidad mantener espacio libre en el buzón.

- **Mensajes prohibidos.**
  Se prohíbe el uso del correo electrónico institucional de la **"U.C.N.C."** con fines religiosos, políticos, lúdicos o personales o en beneficio de terceros o que vulnere los derechos fundamentales de las personas. Por tanto, está prohibido el envío, reenvío o en general cualquier otra conducta tendiente a la transmisión de mensajes humorísticos, pornográficos, en cadena, publicitarios y en general cualquier otro mensaje ajeno a los fines laborales sin importar si son solo texto, audio, video o una combinación de los tres.

- **Acciones para frenar el SPAM.**
  En el caso de recibir un correo no deseado y no solicitado (también conocido como SPAM), el usuario debe abstenerse de abrirlo y avisar inmediatamente al área de sistemas de la Notaría sin embargo se recomienda utilizar filtros de correo electrónico y bloquea remitentes, activar las funciones de bloqueo de llamadas y mensajes en tu teléfono .

- **Todo buzón de correo debe tener un responsable.**
  Todo buzón de correo electrónico institucional de la **"U.C.N.C."** asignado debe tener una

persona responsable de su administración.

- **Intercambio de información a través de Internet.**
  La información interna puede ser intercambiada a través de Internet, pero exclusivamente para propósitos laborales, con la debida aprobación y usando los mecanismos de seguridad apropiados.

- **Uso de conexiones Inalámbricas para dispositivos Móviles**
  Está prohibida las conexiones, configuraciones de redes públicas con las siguientes características:

  - Configuración y/o acceso a redes inalámbricas WIFI públicas.
  - Configuración y/o acceso a redes inalámbricas WIFI que no cuenten con cifrado de seguridad WPA o superior
  - Configuración de dispositivos adicionales no autorizados a través de cualquier tipo de conexión.
  - Conexión mediante redes inalámbricas de área personal o WPAN (Wireless Personal área Network) o tecnología Bluetooth (estándar IEE 802.15).
  - Configuración y acceso a dispositivos Bluetooth.
  - Configurar la funcionalidad NFC

- **Redes de datos Permitidas**
  Solo se permite conexiones a redes de datos como son Telefonía Móvil 2G o GPRS; telefonía móvil 3G, Telefonía Móvil 4G o superior, WIFI privado.

## 7.8. POLÍTICAS GENERALES PARA USUARIOS Y PERSONAL DE LA NOTARÍA

- **Restricción por acceso telefónico e Internet sobre recursos tecnológicos de uso interno a clientes externos.**
  No se le deben otorgar privilegios de acceso telefónico o Internet a terceros a no ser que la necesidad de dicho acceso sea justificada y aprobada. En tal caso se deben habilitar privilegios específicos para ese usuario, con vigencia solamente del período de tiempo necesario para la actividad justificada y mediante el uso de los mecanismos de control de acceso aprobados por del Notario.

- **Los computadores multiusuario y sistemas de comunicación deben tener limitado el acceso físico.**
  Todos los computadores multiusuario, equipos de comunicaciones del Proyecto De Autenticación Biométrica que contengan información sensible y software licenciado de

propiedad de la notaria deben ubicarse en lugares que impidan el fácil acceso físico de personal ajeno a la misma.

- **Entrenamiento compartido para labores técnicas críticas.**
  Al menos dos personas deben tener la misma capacidad técnica para la adecuada administración y uso de los activos del Proyecto De Autenticación Biométrica.

- **Preparación y mantenimiento de planes para la recuperación de desastres y para respuesta a emergencias.**
  Todo sistema o recurso informático debe tener definido un plan de contingencia para la restauración de la operación. Se debe preparar, actualizar y probar periódicamente un plan para la recuperación de desastres que permita que sistemas y computadores críticos puedan estar operativos en la eventualidad de un desastre. De igual forma se deben crear planes de respuesta a emergencia con el fin de que se pueda dar una pronta notificación de problemas y solución a los mismos en la eventualidad de emergencias informáticas. Estos planes de respuesta a emergencias pueden llevar a la formación de un equipo dedicado a esta labor.

- **Personal competente en el Centro de Cómputo para dar pronta solución a problemas.**
  Con el fin de garantizar la continuidad de los procesos del Proyecto de Autenticación Biométrica, en la medida de lo posible la Notaría debe contar con personal técnico competente que pueda detectar problemas y buscar la solución de una forma eficiente.

- **Chequeo de virus en archivos recibidos en correo electrónico.**
  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 de los usuarios.

- **Personas autorizadas para leer los registros de auditoria.**
  Los registros de sistemas y aplicaciones no deben estar disponibles para personal no autorizado. Personal no autorizado es aquel que no pertenece a auditoría interna, personal de seguridad informática, personal de administración de sistemas o administradores de bases de datos.

## 7.9. POLÍTICAS PARA ADMINISTRADORES DE SISTEMAS

- **Soporte para usuarios con privilegios especiales.**
  Todos los sistemas y computadores multiusuarios deben soportar un usuario con privilegios superiores a un usuario normal con el fin de poder ejercer las correspondientes labores administrativas y por lo cual estos privilegios deben ser asignados únicamente a los administradores.

No se permite secciones simultaneas de un mismo usuario desde diferentes dispositivos.

- **Los privilegios de acceso a los sistemas de información otorgados a un usuario terminan cuando el usuario finaliza su vínculo contractual con la notaría.**
  Todos los privilegios sobre los recursos informáticos de la Notaría otorgados a un usuario deben eliminarse en el momento que éste abandone la notaria y la información almacenada queda en manos de su jefe inmediato para aplicar los procedimientos de retención o destrucción de información.

- **Límite de intentos consecutivos de ingreso al sistema.**
  El acceso al proyecto de autenticación biométrica limita el número de intentos consecutivos a tres (3) intentos fallidos el usuario, este queda bloqueado por 1 minuto. De no recordar la contraseña contara con la opción de olvide mi contraseña para realizar el cambio.

- **Brindar acceso a personal externo.**
  El área administrativa velará porque individuos que no sean empleados, contratistas o consultores de la Notaría no tengan privilegio alguno sobre los recursos tecnológicos de uso interno de la notaría a menos que exista una aprobación escrita.

- **Restricción de administración remota a través de Internet.**
  La administración remota desde Internet no es permitida a terceros, esta actividad debe ser exclusiva del personal técnico de la **"U.C.N.C"** o del operador del servicio para las tareas de soporte técnico sobre los recursos informáticos del Proyecto De Autenticación Biométrica.

- **Captura de Información cuando hay crimen informático o existe sospecha de abuso de intrusión.**
  Para suministrar evidencia para investigación, persecución y acciones disciplinarias, cierta información debe ser capturada inmediatamente cuando se sospecha un crimen informático o abuso. Esta información se deberá almacenar de forma segura en algún dispositivo fuera de línea. La información a recolectar incluye configuración actual del sistema, copias de backup y todos los archivos potencialmente involucrados.

- **Captura de Huellas Biométricas a Compareciente**
  Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El funcionario encargado de realizar el trámite de Autenticación Biométrica en Línea debe verificar las manos del compareciente, es decir que no tenga nada adherido a sus huellas (Colbón, silicona, papel etc.).
  Así mismo, de acuerdo con las políticas de seguridad de la Registraduría Nacional del Estado Civil – RNEC (anexo técnico # 2 V2 de la Resolución 5633 del 2016) solo se pueden utilizar

captores biométricos homologados por dicha entidad. Por otra parte, debe garantizarse la integridad física del captor biométrico.
Otros componentes que no son requisito indispensable para validar la identidad de un compareciente por medios electrónicos, según lo exponen los anexos técnicos de la Registraduría Nacional del Estado Civil – RNEC, pero que también fueron entregados en comodato por la UCNC: el lector de código de barras, escáner, cámara web y tableta digitalizadora.

- **Confidencialidad en la información relacionada con investigaciones internas.**
  Hasta que no se hayan presentado cargos o se haya tomado alguna acción disciplinaria, toda investigación relacionada con abusos de los recursos tecnológicos o actividad criminal debe ser confidencial para mantener la reputación del empleado.

- **Información con múltiples niveles de clasificación en un mismo sistema.**
  Si un sistema o computador maneja información con diferentes niveles de sensibilidad, los controles usados deben ser los adecuados para proteger la información más sensible.

- **Software de antivirus.**
  Para asegurar que el equipo técnico de la Notaría ha tomado las medidas preventivas adecuadas, a todos los sistemas conectados a Internet deben contar con un Antivirus que cuente con una consola de administración en la cual se visualizan los reportes de eventos relacionados con vulnerabilidades. Para la Biometría Móvil, las medidas preventivas de la Tablet, se aplica Windows defender y firewall de Windows.

- **Mantenimiento preventivo en computadores, sistemas de comunicación y sistemas de condiciones ambientales**
  Se debe realizar mantenimiento preventivo regularmente en todos los computadores y sistemas para que el riesgo de falla se mantenga en un nivel bajo.

- **Verificación física de equipos.**
  Se debe verificar periódicamente el estado físico de los equipos de cómputo.

- **Servicios de Red**
  Se debe garantizar que el servicio de red utilizado por la Notaría se encuentre disponible y operando adecuadamente, el administrador del sistema o una persona autorizada por la Notaría puede efectuar escaneos de la red con la finalidad de: resolver problemas de servicio, como parte de las operaciones normales del sistema y del mantenimiento, para mejorar la seguridad de los sistemas o para investigar incidentes de seguridad.

- **Revisión de accesos de usuarios**
  Las aplicaciones utilizadas deben actualizarse por lo menos dos veces por año, y eliminar los usuarios inmediatamente dejen de hacer uso de la Biometría, comunicándose con los canales de atención correspondientes.

## 7.10. POLÍTICAS DE USO DE FIREWALL

- **Toda conexión externa debe estar protegida por el firewall.**
  Toda conexión a los servidores de la Notaría proveniente del exterior, sea Internet, acceso telefónico o redes externas debe pasar primero por el Firewall. Esto con el fin de limitar y controlar las puertas de entrada a la organización.

- **Toda conexión hacia Internet debe pasar por el Firewall.**
  El firewall debe ser el único elemento conectado directamente a Internet por lo cual toda conexión desde la red interna hacia Internet debe pasar por el firewall.
  En las infraestructuras donde se cuente con un solo equipo conectado a internet, el firewall de este debe estar configurado de forma que no permita conexiones externas exceptuando las conexiones desde Certicámara o la “U.C.N.C.”.

- **Segmentación de la red.**
  Todos los servidores públicos deben ser ubicados en un segmento de red especial, protegidos por el Firewall, con el fin de proteger la red Interna y los servidores críticos. De igual forma los servidores críticos deben ser ubicados en un segmento de red especial con controles de acceso adecuados, siempre y cuando no se afecte la operación normal de la red y de sus servicios.

- **El sistema interno de direccionamiento de red no debe ser público.**
  Las direcciones internas de red y configuraciones internas deben estar restringidas de tal forma que sistemas y usuarios que no pertenezcan a la red interna no puedan acceder a esta información.

## 7.11. POLÍTICAS PARA USUARIOS EXTERNOS

- **Acuerdos con terceros que manejan información o cualquier recurso informático de la Notaría**
  Todos los acuerdos relacionados con el manejo de información o de recursos de informática de la Notaría por parte de terceros, deben incluir una cláusula especial que involucre confidencialidad y derechos reservados. Esta cláusula debe permitirle a la Notaría ejercer auditoría sobre los controles usados para el manejo de la información y específicamente de cómo será protegida la información de los activos del Proyecto Sistema de Autenticación Biométrica en Línea Notarial.

### 7.12. POLÍTICAS DE ACCESO FÍSICO

- **Permitir paso a través de puertas controladas.**
  Los funcionarios no deben permitir que personal desconocido o no autorizado entre a zonas restringidas.

- **Control de acceso físico para áreas que contienen información sensible.**
  El acceso a cada oficina, cuarto de computadores, cuarto de equipos de comunicaciones y puestos de trabajo que contengan información sensible, debe estar físicamente restringido.

- **Reporte de pérdida o robo de identificación.**
  Todo empleado debe reportar con la mayor brevedad, cualquier sospecha de pérdida o robo de carnés de identificación y tarjetas de acceso físico a las instalaciones, o perdida de certificados digitales.
  En caso de pérdida y /o rodo de dispositivos móviles, se debe comunicar inmediatamente a la "U.C.N.C"., a reportar la perdida.

- **Orden de salida de activos**
  Todos los activos del Proyecto de Autenticación Biométrica que afecten la seguridad de la información de la Notaría como medios de almacenamiento, CDs, DVDs., entre otros, y que necesiten ser retirados de la entidad, deben ser autorizados por la "U.C.N.C." para su salida.

- **Cuando se da una terminación laboral, los privilegios de acceso a activos del Proyecto De Autenticación Biométrica deben ser revocados.**
  Cuando se termine el vínculo laboral existente con el notario, el usuario deberá devolver los objetos de acceso a los activos del Proyecto De Autenticación Biométrica (carnets, tarjetas de acceso, etc, se deben devolver de ser el caso a la "U.C.N.C." todos los elementos utilizados para el proyecto biométrico) y a su vez todos sus privilegios de acceso deberán ser revocados enviando los datos de funcionarios autorizados vía correo electrónico al área de Sistemas de la "U.C.N.C.".

## 8. CANALES DE COMUNICACIÓN

Mesa de Ayuda de la "U.C.N.C": 6015145846
Celular: 3176857228
Chat: 3155851313
"U.C.N.C." 6017464040 opción 2