SNR SUPERINTENDENCIA DE NOTARIADO & REGISTRO La guarda de la fe pública

PROYECTO DIGITALIZACIÓN NOTARIAL

ANEXO TÉCNICO

DOCUMENTO FINAL

VERSIÓN V1.0

BOGOTA D.C, ENERO DE 2021

TABLA DE CONTENIDO

1. GLOSARIO

- **ACTO NOTARIAL ELECTRÓNICO:** Es la actuación que lleva a cabo el notario a través de medios electrónicos, garantizando las condiciones de seguridad, interoperabilidad, integridad y accesibilidad necesarias.

- **AUTENTICIDAD:** Es el atributo generado en un mensaje de datos cuando existe certeza sobre la persona que lo ha elaborado, emitido, firmado o cuando existe certeza respecto de la persona a quien se atribuye el mensaje de datos.

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

- **INTEGRIDAD**: Es la condición que garantiza que la información consignada en un mensaje de datos ha permanecido completa e inalterada, salvo la adición autorizada de algún endoso o de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

- **DIGITALIZACIÓN:**
  El término "digitalización" se asocia con el de desmaterialización, entendida ésta como "el proceso por medio del cual un documento de papel o en cualquier otro formato análogo es transformado a un formato digital'. Podemos entender en sentido lato la desmaterialización, como un método por el cual la información contenida en un medio físico de lectura analógica es convertida por medios electrónicos o similares (particularmente a través del uso del lenguaje binario) a un formato electrónico, de manera que la información así reproducida sólo puede ser accesible por intermedio de un dispositivo computacional o similar. [1]

- **ESCRITURA PÚBLICA ELECTRÓNICA:** Es la escritura pública que nace como mensaje de datos garantizando la autenticidad, disponibilidad e integridad del documento, de conformidad con la ley 527 de 1999, además debe cumplir las normas sustanciales relativas a las diferentes actuaciones notariales que ella contiene y de los preceptos de derecho notarial, conforme al Decreto-ley 960 de 1970 y demás normas concordantes.

  Los documentos reproducidos por los citados medios gozarán de la validez y eficacia del documento original, siempre que se cumplan los requisitos exigidos por las leyes

[1] Circular Externa 005 de 2012 – Archivo General de la Nación

procesales y se garantice la autenticidad, integridad e inalterabilidad de la información. Los documentos originales que posean valores históricos no podrán ser destruidos, aun cuando hayan sido reproducidos y/o almacenados mediante cualquier medio

- **FIRMANTE:** Persona que utiliza directamente su firma electrónica para otorgar actos o instrumentos notariales

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

- **FIRMA DIGITAL:** Se entenderá como un valor numérico que se adhiere a un mensaje de datos y que, utilizando un procedimiento matemático conocido, vinculado a la clave del iniciador y al texto del mensaje permite determinar que este valor se ha obtenido exclusivamente con la clave del iniciador y que el mensaje inicial no ha sido modificado después de efectuada la transformación[2]. Esta firma cuenta con el respaldo de una Entidad de Certificación digital[3]

- **MARCO DE INTEROPERABILIDAD**: Es la estructura de trabajo común, definida por el Ministerio de las TIC, donde se alinean los conceptos y criterios que guían el intercambio de información. Define el conjunto de principios. recomendaciones y directrices que orientan los esfuerzos políticos, legales, organizacionales, semánticos y técnicos de las entidades, con el fin de facilitar el intercambio seguro y eficiente de información.

- **REGISTRO DE USUARIO:** Es el proceso que adelanta la notaría de forma presencial o virtual, mediante el cual las personas naturales o jurídicas se incorporan a los servicios que prestan esos despachos.

- **MEDIO ELECTRONICO:** Mecanismo, instalación, equipo o sistema que permite producir, almacenar o transmitir documentos, datos e informaciones, incluyendo cualesquiera redes de comunicación abiertas o restringidas como internet, telefonía y móvil u otras.

- **ACCESIBILIDAD Y USABILIDAD:** De acuerdo con la caracterización de usuarios, ciudadanos y grupos de interés de la entidad, éstas deben garantizar que las páginas web, portales web y sistemas de información web con sus respectivos contenidos, cuenten con características técnicas y funcionales que permitan al usuario percibir,

[2] Ley 527 de 1999, Artículo 2 – Literal C
[3] Ley 527 de 1999, Artículo 2 – Literal D Entidad de Certificación: Es aquella persona que, autorizada conforme a la presente ley, está facultada para emitir certificados en relación con las firmas digitales de las personas, ofrecer o facilitar los servicios de registro y estampado cronológico de la transmisión y recepción de mensajes de datos, así como cumplir otras funciones relativas a las comunicaciones basadas en las firmas digitales;

entender, navegar e interactuar adecuadamente. A su vez que las personas con discapacidad sensorial puedan acceder de manera autónoma e independiente a dichas páginas, portales y sistemas de información web. Para tal efecto se deben implementar pruebas de accesibilidad y usabilidad con los usuarios, para determinar ajustes a realizar y atributos a incorporar. Así mismo, la notaría debe garantizar que los contenidos audiovisuales cuenten con audio descripción, subtitulado, closed caption y lengua de señas. En ese orden, priorice los contenidos más relevantes, más usados o más demandados por los usuarios. Para ello, aplique: - Norma Técnica de Accesibilidad 5854 disponible en el sitio web del ICONTEC (INCONTEC, s.f.)20 - La Guía interactiva de implementación de la NTC 5854 (MinTIC, s.f.)21 - La guía de usabilidad disponible en el sitio web de Gobierno Digital (MinTIC, s.f.)

- **OPERADOR DIGITAL:** Los operadores digitales son las personas naturales o jurídicas, de derecho **público** o privado, que a elección del notario adelantarán el trámite de transferencia de los actos notariales digitales a la nube pública de la SNR, así como los procedimientos para la celebración de los mismos a través de medios digitales de cara al usuario del servicio público notarial, conforme a los términos contenidos en los anexos técnicos expedidos por la SNR y la RNEC. Cabe aclarar que las notarías podrán actuar de forma directa en calidad de operadores digitales, siempre que acrediten el cumplimiento de las condiciones contenidas en los anexos técnicos.

  Todas las notarías deberán contar con la correspondiente validación realizada por la Superintendencia Delegada para el Notariado que permita la prestación del servicio público notarial a través de medios electrónicos, previo concepto favorable expedido por la OTI de la SNR.

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

2. INTRODUCCIÓN

El parágrafo del artículo 3 del Decreto–Ley 960 de 1970, adicionado por el artículo 59 del Decreto–Ley 2106 de 2019, estableció que "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", asignando a la Superintendencia de Notariado y Registro la competencia para que ésta expida las directrices necesarias, para la correcta prestación del servicio público notarial a través de medios electrónicos.

El artículo 113 del Decreto – Ley 960 de 1970, modificado por el artículo 63 del Decreto–Ley 2106 de 2019, en consonancia con el artículo 9 de la Ley 588 de 2000, consagró que el archivo deberá llevarse en formato físico, no obstante, lo cual, cuando el trámite se surta por este medio, se deberá guardar copia en medio electrónico que permita su conservación segura, íntegra y accesible. Así mismo, estableció que cuando los documentos se originen y gestionen en forma electrónica, se archivarán por el mismo medio, garantizando su seguridad, autenticidad, integridad, inalterabilidad, disponibilidad y actualización de la información, que a su vez se integrará con la copia electrónica del archivo generado en formato físico.

El inciso final del artículo 113 del Decreto – Ley 960 de 1970, modificado por el artículo 63 del Decreto–Ley 2106 de 2019, indicó que, una vez 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 la reglamentación que sobre el particular expida.

Por consiguiente, la Superintendencia de Notariado y Registro – SNR, con el apoyo del Departamento de Tecnologías y Gestión de la Información en Justicia del Ministerio de Justicia, a la cual es adscrita y, siguiendo los lineamientos y estándares del Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC, entidad encargada de promover y definir el establecimiento de las Tecnologías de la Información y las Comunicaciones en el país, a través de este documento expide el anexo técnico que fija las condiciones, estándares, lineamientos y directrices técnicas que deben desarrollar e implementar los sistemas y aplicativos tecnológicos utilizados en las sedes electrónicas y despachos notariales, para que se puedan adelantar las actuaciones del servicio público notarial por medios electrónicos.

El Gobierno Nacional a través de diversas Directivas Presidenciales, CONPES y Planes Nacionales de Desarrollo, teniendo como fin esencial del Estado garantizar el acceso eficaz de los usuarios a la administración pública, ha fomentado la transformación digital e inteligencia artificial, de tal forma que permita la automatización y digitalización de los trámites, la eficiente gestión de la información y ha incorporado como objetivo su promoción a través de la implementación e integración de los servicios ciudadanos digitales, carpeta ciudadana, autenticación electrónica e interoperabilidad de los sistemas del Estado. En concordancia con esto, el Decreto Ley 019 de 2012 establece la obligatoriedad de identificar plenamente al ciudadano por medios electrónicos; más exactamente, cotejando la huella en tiempo real contra la base de datos biométrica de la Registraduría Nacional del Estado Civil.

Adicionalmente, Ley 1581 de 2012, "Por la cual se dictan disposiciones generales para la protección de datos personales", consagra las condiciones para el tratamiento de los datos personales en ejercicio de las funciones legales y el derecho que tienen las personas de conocer, rectificar y actualizar la información personal que figure en archivos o bases de datos.

Por otro lado, con la política de "Cero Papel" se promueven las buenas prácticas tanto en el sector público como privado para que se reduzca su consumo y se sustituyan por soportes en medios electrónicos gestados en la utilización de Tecnologías de la Información y las Telecomunicaciones. Por otra parte, con las disposiciones estipuladas en el Decreto 1078 de 2015, Decreto Único Reglamentario del Sector de las Tecnologías y las Comunicaciones, adicionado por el Decreto 1413 de 2017 y subrogado por el Decreto 620 de 2020, además de la reciente expedición de la Ley 2106 de 2019 y Ley 2052 de 2020 se configura el marco jurídico requerido para que la Superintendencia de Notariado y Registro – SNR fije los estándares y lineamientos técnicos que garanticen la implantación de los mecanismos electrónicos en los procedimientos y trámites de la función notarial.

3. CONTEXTO DEL PROYECTO

3.1. ALCANCE

El presente anexo relaciona las características técnicas, normativas y funcionales, que deben cumplir las notarías y sus sistemas de información, como solución para la prestación de servicios notariales no presenciales, a través de la utilización de medios electrónicos, estableciendo las condiciones, lineamientos, estándares, directrices técnicas de seguridad, interoperabilidad, integridad, disponibilidad, confidencialidad y accesibilidad necesarias para que las notarías puedan integrar sus sistemas tecnológicos, gestionar la información y garantizar la correcta prestación de los servicios públicos notariales a los usuarios de manera no presencial. No obstante, debe manifestarse que el usuario puede escoger la presencialidad de forma concomitante con la prestación del servicio público notarial a través de los medios digitales.

Las notarías interactúan con múltiples actores en el ámbito notarial: Las personas (naturales y jurídicas), El notario y los funcionarios; pero además se relacionan y/o requieren información de otros actores que participan indirectamente en los trámites, como los que se relacionan a continuación, entre otras:

- **Superintendencia de Notariado y Registros - SNR:** reporte de la información estadística notarial.
- **DIAN:** Información de recaudo y pago de impuestos, y reportes relacionados con la enajenación de bienes y facturación electrónica.
- **ICBF:** Reportes de actos notariales donde están involucrados menores de edad.
- **Registraduría Nacional del Estado Civil - RNEC:** Información relacionada con el registro civil de las personas, tales como inscripciones y anotaciones entre otros.
- **Unidad de Información y Análisis Financiero - UIAF:** Información general de las operaciones notariales que realizan las personas y de aquellas consideradas sospechosas.
- **Secretarías Municipales y Distritales de Hacienda:** Información sobre las transacciones del impuesto de industria y comercio donde la notaría hace parte.
- **Tesorerías Departamentales:** Escrituras públicas que deben pagar el impuesto de beneficencia.
- **Estrados Judiciales**: Recibo de comisiones para los remates y solicitud de actuaciones puntuales de los particulares en notarías.
- **Migración Colombia:** Autenticación de los permisos de salida de menores del país y cargue del repositorio de la SNR y consulta en línea por parte de los oficiales de migración.
- **Ministerio de Salud y Protección Social:** Acceso modulo RUAF
- **Dirección Nacional de Inteligencia – DNI:** Aplicación de políticas que se dicten de cara a la seguridad nacional.
- **Ministerio de Justicia:** Reporte de Conciliaciones y proceso de insolvencia de persona natural no comerciante.
- **Oficinas de Catastro:** Certificados catastrales y paz y salvos, entre otras…

La lógica de negocio y los procesos notariales seguirán estando en las notarías y sus proveedores tecnológicos. La solución tecnológica deberá permitir la comunicación con los actores en los flujos de los procesos de cada trámite digital.

La siguiente gráfica muestra la evolución normativa en materia tecnológica:

Ilustración 1. Normatividad

4. REQUISITOS TÉCNICOS

A continuación, se establecen los requerimientos técnicos que deben cumplir las notarías y sus sistemas de información. Estos deberán ser de estricto cumplimiento para lograr la autorización de operar por parte de la Superintendencia de Notariado y Registro.

La prueba técnica, establecerá los procedimientos necesarios para evaluar la plataforma tecnológica presentada por cada uno de los notarios, en términos de funcionalidad, seguridad, desempeño, auditoría, concurrencia, integridad, interoperabilidad y demás requerimientos expuestos por parte de la SNR.

Dentro de la ejecución de las diferentes fases de la prueba, el grupo técnico de la SNR documentará cada actividad adelantada dentro de la verificación, para lo cual, se contará con una lista de chequeo para registrar las diferentes pruebas y tareas adelantadas dentro del proceso.

Los requisitos establecidos por el grupo técnico de la SNR deben ser presentados por los interesados en prestar el servicio público notarial a treves de medios digitales, garantizando la seguridad, buen uso y reserva de la información y cumpliendo con los requerimientos exigidos por la normatividad vigente.

5. LINEAMIENTOS GENERALES

1. Los trámites adelantados en las notarías a través de las plataformas digitales deben obedecer a los procedimientos definidos en el Decreto ley 960 de 1970 y demás normas concordantes, garantizando su validez jurídica, blindándolos principalmente ante fraudes de suplantación de identidad y buscando la expresión de voluntad de adelantarlo.

2. Todos los trámites notariales no presenciales deberán tener trazabilidad en la plataforma buscando que el usuario del servicio público notarial tenga claro sus puntos de interacción, permitiendo la identificación del trámite en cada uno de sus estados o etapas dentro del proceso de generación del acto notarial digital.

3. La solución tecnológica debe generar y administrar los soportes del proceso, con el fin de garantizar la trazabilidad integral de los trámites.

4. La solución tecnológica debe garantizar los principios de interoperabilidad, seguridad, oportunidad, disponibilidad e integridad para los sistemas de información.

5. La solución tecnológica debe estar implementada para entornos web y móvil.

6. La solución tecnológica debe contar con un módulo para el agendamiento de citas virtuales para el desarrollo de los actos notariales digitales.

7. La solución tecnológica debe ser modular, de forma tal que permita la fácil agrupación de componentes según el trámite a realizar y de acuerdo con las necesidades de cada notaría.

8. La interfaz de trámites debe presentar al ciudadano la descripción de los mismos, los requisitos para su realización, pasos a seguir, la tarifa por trámite y los medios de pago electrónicos.

9. La solución tecnológica debe implementar los lineamientos detallados en el presente anexo, estableciendo un código CUANDI (cuyas especificaciones serán detalladas en párrafos subsiguientes), para cada acto electrónico que se realice, garantizando la autenticidad, inalterabilidad y singularidad del documento. Para el caso de las escrituras públicas, cada folio deberá estar numerado. Esta numeración podrá ser una combinación alfanumérica de 10 dígitos, que deberá establecer el notario para lograr la trazabilidad del documento.

10. Como mecanismo complementario para la verificación de rogación del trámite notarial, se podrá utilizar el recurso de video llamada siempre y cuando se cumplan con las siguientes características:

    - Debe realizarse de manera síncrona entre las partes.
    - Estampado cronológico
    - Garantizar comunicación estable entre las partes.
    - Garantizar la trazabilidad del acto notarial mediante grabación y descarga.

- Permitir la identificación permanente de las personas que intervienen en el acto notarial.

11. La solución tecnológica debe permitir el pago de servicios a través de canales electrónicos que garantice al notario el cobro de los derechos notariales. La pasarela de pago utilizada deberá dar cumplimiento de controles de seguridad y protección de datos, así como las normas y requisitos establecidas por las autoridades competentes.

12. La solución tecnológica debe permitir que el usuario envíe y cargue a la Notaría los documentos necesarios para la ejecución del trámite.

13. Autorización de operación a través de medios electrónicos: Aquellas notarías que acrediten el cumplimiento de los lineamientos establecidos en los anexos técnicos y actos administrativos, serán autorizadas por la Superintendencia de Notariado y Registro a través de la Superintendencia Delegada para el Notariado, para la prestación del servicio público notarial por medios electrónicos. Para tal efecto se expedirá el acto administrativo correspondiente.

6. INTEROPERABILIDAD

El Ministerio de las TIC definió la interoperabilidad como la "**Capacidad de las organizaciones para intercambiar información y conocimiento en el marco de sus procesos de negocio para interactuar hacia objetivos mutuamente beneficiosos, con el propósito de facilitar la entrega de servicios en línea a ciudadanos, empresas y a otras entidades, mediante el intercambio de datos entre sus sistemas".**

Y es por ello que surge el **Marco de Interoperabilidad para Gobierno Digital** cuyo propósito es contribuir en la entrega de servicios digitales, de manera completa, adecuada, minimizando los pasos y evitando el desplazamiento del ciudadano a diversas entidades para obtener la información necesaria de una entidad y acceder así a los derechos, obligaciones con el Estado. La interoperabilidad permite fortalecer la visión de unidad del Estado, al tener una mayor capacidad de comunicación, entrega y uso de servicios digitales de valor para mejorar la calidad de vida de los ciudadanos.

El Marco de Interoperabilidad de Gobierno Digital es la herramienta que acompaña a las entidades en el desarrollo de sus capacidades de intercambio de información, sin importar sus restricciones o su tamaño.

Los actores del proceso Notarial en Colombia deben adoptar e implementar los lineamientos establecidos en el Marco de Interoperabilidad de la política Gobierno Digital del Ministerio de las TIC[4]

Los objetivos del marco de interoperabilidad son:

- Apoyar a las entidades públicas en sus esfuerzos por diseñar y ofrecer trámites y servicios en línea sin interrupciones a otras entidades públicas, ciudadanos y empresas que, en la medida de lo posible, sean digitales por defecto, es decir, que proporcionen servicios y datos preferentemente a través de medios digitales, siendo accesibles para todas las entidades, los ciudadanos y que permitan la reutilización, participación, acceso y transparencia.

- Proporcionar orientación a las entidades públicas sobre el diseño y la actualización de los mecanismos de interoperabilidad sus políticas, estrategias y directrices, así como la visión nacional que se promueven en interoperabilidad;

- Contribuir al establecimiento de fuertes mecanismos de interoperabilidad en las entidades públicas para la prestación de trámites y servicios en línea.

6.1. PRINCIPIOS DE INTEROPERABILIDAD QUE DEBEN CUMPLIR LOS ACTORES DEL PROCESO NOTARIAL

- Enfoque en el ciudadano

4 Marco de Interoperabilidad: https://www.mintic.gov.co/arquitecturati/630/w3-propertyvalue-8117.html

- Cobertura y proporcionalidad
- Seguridad, protección y preservación de la Información
- Colaboración y participación
- Simplicidad
- Neutralidad, tecnológica y adaptabilidad
- Reutilización
- Confianza
- Costo-efectividad

6.2. CARACTERÍSTICAS TÉCNICAS DE LOS DESARROLLOS EN LOS PROCESOS DE INTEROPERABILIDAD

Los servicios de intercambio de información deben cumplir con los lineamientos del marco de interoperabilidad y el lenguaje común de intercambio de información de la política de Gobierno Digital descrita anteriormente. Esto permitirá la solicitud, gestión, resolución y entrega del resultado del trámite y/o de los sistemas de información de la entidad. De esta manera la entidad tendrá la responsabilidad por la información asegurando su calidad, disponibilidad, seguridad y privacidad.

Y para ello, la construcción o habilitación del (de los) servicios de exposición o consumo para el intercambio de información requerirá tener en cuenta las siguientes recomendaciones técnicas o las que establezca el Ministerio de las TIC de acuerdo al Marco de Interoperabilidad vigente:

- Utilizar estándares como RESTful o SOAP y formatos JSON o XML preferiblemente y bajo los criterios del marco de Interoperabilidad.
- Distribuir el desarrollo de los trámites en capas (presentación, servicios, datos)
- Aplicar los criterios de Seguridad JSON: Token o SOAP: WSSec
- Validar las buenas prácticas de seguridad (p.e: Denial of Service DoS, bloqueo de IP diferentes a las de NMF, etc.)
- Enviar los resultados en DTOs simples, por ejemplo, con atributos de tipo string, float, para transformación de los objetos y no usar hash, maps o algún tipo de estructuras que hagan que se pueda ralentizar el consumo de los servicios.
- Generación de alertas en tiempo real desde los sistemas de información y aplicativos de la entidad, asociados a los trámites y servicios que se integran, con relación al cambio de estado de una solicitud, de tal manera que se haga equivalente a los estados que se publicarán al usuario del servicio público notarial
- Los estados estandarizados de los trámites son: solicitud registrada – solicitud recibida a satisfacción – solicitud en trámite – solicitud resuelta
- Aseguramiento de la disponibilidad y calidad de la operación de los servicios implementados para esta integración.
- Administración y notificación oportuna de los cambios y novedades sobre el(los) web service(s) o API(s) implementados para esta integración. El reporte de la novedad frente a los servicios web que puedan afectar la disponibilidad del servicio a los ciudadanos, deberá efectuarse oportunamente a través de los canales establecidos entre las entidades.
- Utilización de vocabularios comunes y/o controlados que faciliten el entendimiento de

los términos utilizados en los flujos de intercambio de información entre los actores.

6.3. INTEROPERABILIDAD CON X-ROAD

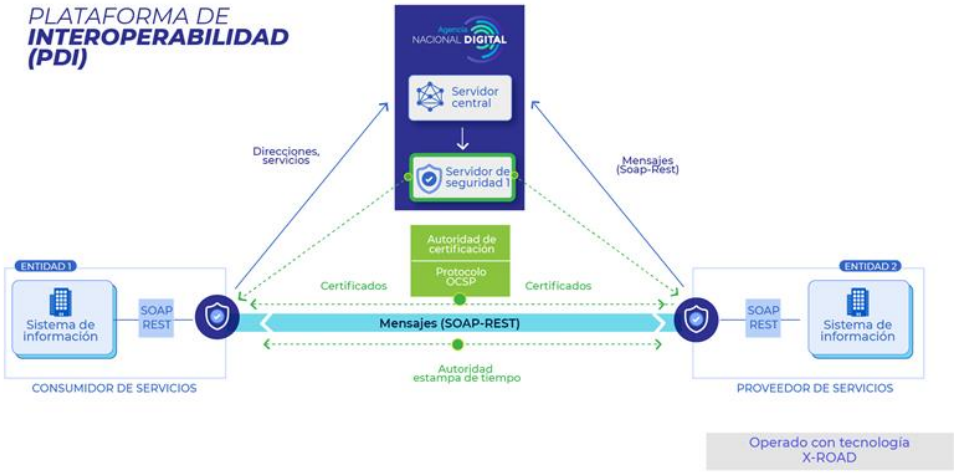
El Ministerio de las TIC como parte de la estrategia de implementación del Servicio Ciudadano Digital de Interoperabilidad, definió la utilización de **X-ROAD** (https://X-ROAD.global/) como la herramienta tecnológica que sustenta la Plataforma de Interoperabilidad del estado – PDI y es usada como el componente tecnológico de intercambio de datos. **X-ROAD** fue seleccionada luego de un análisis detallado de diferentes herramientas tecnológicas en los frentes técnicos y funcionales, así como de una revisión de las mejores prácticas y lecciones aprendidas de diferentes gobiernos en términos de Interoperabilidad.

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

X-ROAD le aporta a la Plataforma de Interoperabilidad del estado las siguientes características:

1. El intercambio de datos se produce directamente entre las entidades sin intermediarios.
2. Las entidades son las que autorizan el acceso a los servicios de intercambio de información expuestos.
3. La propiedad de los datos no cambia, la autoridad propietaria de los datos controla quién puede acceder al servicio de intercambio de información.
4. Cada miembro es autenticado a través de certificados digitales para el acceso a la plataforma.
5. El intercambio de datos se realiza con protocolos criptográficos seguros a través HTTPS con TLS y los mensajes cifrados aplicando el algoritmo RSA con la función Hash SHA512.
6. Todos los mensajes intercambiados a través de X-ROAD son estampados cronológicamente, el cual se utiliza para estampar todas las solicitudes salientes, solicitudes entrantes, respuestas salientes y respuestas entrantes entre los servidores de seguridad X-Road
7. Los mensajes intercambiados en la PDI tienen valor jurídico y pueden ser usados como evidencia digital de envío y recepción del mensaje intercambiado.
8. No hay roles predeterminados, una vez que una entidad se ha unido al ecosistema de X-ROAD, puede actuar como cliente y proveedor de servicios web sin tener que realizar ningún registro adicional.
9. Log y auditoria sobre los mensajes intercambiados

La siguiente figura ilustra el modelo conceptual de la plataforma de interoperabilidad.



La Agencia Nacional Digital -AND-, entidad adscrita al Ministerio de las TIC será la encargada de administrar los componentes centrales de la plataforma de interoperabilidad, prestará a través de las Entidades de Certificación Digital acreditadas ante la ONAC, los **servicios de confianza (Certificados Digitales, Estampa Cronológica de tiempo y validación del estado de un certificado).**

Las entidades actuarán dentro del ecosistema como proveedores y consumidores de servicios de intercambio de datos a través de los componentes de **X-ROAD** y las conexiones que realice al interior con los sistemas de información de cada entidad. El intercambio de datos se realiza entre cada entidad a través de internet estableciendo canales seguros y usando mecanismos de cifrado. Los componentes de X-ROAD dentro del ecosistema se comunican a través de servicios de gestión para la sincronización de la configuración y auditoría.

Cada uno de los miembros, servidores de seguridad **X-ROAD** y servicios dentro del ecosistema de **X-ROAD** serán identificado de acuerdo con la siguiente estructura:

- **Instancia:** Es un entorno organizativo que agrupa a todos los participantes del ecosistema X-ROAD, permitiendo el intercambio seguro de datos entre ellos y administrados por una autoridad de gobierno. Existirán 3 instancias relacionadas al ambiente de QA, Preproducción y Producción para Colombia
- **Clase Miembro:** Es un identificador dado por la autoridad de gobierno de X-ROAD para clasificar a los miembros que poseen características similares dentro del ecosistema. Las clases de miembro serán GOB para identificar a entidades públicas y PRIV para identificar a entidades privadas.
- **Nombre del Miembro**: Nombre que se le dará a cada miembro dentro del ecosistema, este será el nombre legal de cada entidad.
- **Código de Miembro**: Es el identificador único de cada miembro dentro de su Clase Miembro, este código permanece sin modificarse durante todo el tiempo de permanencia

dentro del ecosistema. Este código será generado de acuerdo con el código definido en la base de datos del SIGEP para las entidades.

- **Código del servidor de seguridad:** Código que identifica un servidor de seguridad de los demás servidores dentro del ecosistema. Este consta del código del miembro y el código del servidor de seguridad.
- **Código del subsistema:** Código que identifica de forma exclusiva el subsistema en todos los subsistemas del miembro. Se establecerá de acuerdo con los nombres de los sistemas de información de la entidad.
- **Código del servicio:** Código que identifica de forma exclusiva el servicio expuesto por un miembro en el ecosistema X-ROAD. El código es el nombre que haya establecido la entidad al servicio en estilo CamelCase.

En una primera fase se realizará la verificación de que la solución tecnológica de las notarías tenga Interoperabilidad con el repositorio de la SNR a través de X-ROAD.

La solución tecnológica de las Notarías en una segunda fase, debe permitir la interoperabilidad a través de X-ROAD con los demás actores requeridos en los tramites notariales.

Los actores del proceso notarial en Colombia deberán atender los lineamientos de la "Guía para la vinculación y uso de los servicios ciudadanos digitales" [5] del Ministerio TIC.

[5] Guías para la vinculación y uso de los servicios ciudadanos digitales; y Guía de lineamientos de los servicios ciudadanos digitales - https://www.gov.co/biblioteca/

6.4. INTEGRACIÓN CON EL REPOSITORIO PARA EL PROTOCOLO NOTARIAL

La SNR dispuso la adquisición de una nube pública para gestionar el almacenamiento y preservación de todos y cada uno de los actos notariales y/o repositorio notarial digital.

Para acceder al sistema de repositorio el usuario puede acceder mediante dos opciones, una interfaz web o un servicio web, donde el usuario queda validado para enviar los datos al repositorio documental del protocolo Notarial dispuesto en la nube publica adquirida por la SNR para tal fin. Este repositorio contendrá los datos meta-descriptivos de los documentos y los archivos digitalizados que hacen parte del protocolo notarial.

Una vez se tienen los datos y los archivos en el almacén de la nube, dicha información podrá ser consultada, analizada y aprovechada mediante técnicas de interoperabilidad según los lineamientos jurídicos de la SNR. El intercambio de la información con otras entidades se realiza aplicando el marco de interoperabilidad y su herramienta X-ROAD.

En todo caso, las notarías deberán consultar y acoger los lineamientos expuestos en el **Anexo Técnico - REPOSITORIO NOTARIAL VF – 20210104.**

7. CARPETA CIUDADANA

La Carpeta Ciudadana Digital de los Servicios Ciudadanos Digitales del Ministerio de las TIC, es el servicio que le permite a los usuarios acceder digitalmente y de manera segura, confiable y actualizada al conjunto de sus datos que tienen o custodian las entidades públicas, por ejemplo, para el caso de procesos de Digitalización Notarial las entidades que conforman el sistema notarial en Colombia.

La Carpeta Ciudadana Digital no es un repositorio de información para las entidades públicas; no se copia o se duplica la información, siempre estará bajo la custodia de las entidades, en este caso Notarias, y su acceso se hará solo por los mecanismos de interoperabilidad.

Una vez la Agencia Nacional Digital – AND habilite el servicio, las notarías deberán identificar y disponer en la Carpeta Ciudadana Digital toda la información relevante y de interés para los usuarios de tal forma que pueda ser consultada a través de este Servicio Ciudadano Digital.

Los actores del proceso notarial en Colombia deberán atender los lineamientos de la "Guía para la vinculación y uso de los servicios ciudadanos digitales"[6] del Ministerio TIC.

8. CÓDIGO UNICO DE ACTO NOTARIAL DIGITAL (CUANDI)

Se establecerá el nuevo código único de acto notarial Digital denominado CUANDI, el cual garantizará una codificación exclusivamente para los actos notariales que se generen digital o electrónicamente a fin de salvaguardar la seguridad y trazabilidad de los documentos, de la siguiente manera:

CODIGO DEPARTAMENTO (2) + CODIGO MUNICIPIO (3) + N° NOTARIA (4) + CODIGO ACTO NOTARIAL (8) + AÑO ACTO (4) + CONSECUTIVO ACTO NOTARIAL (6)

En donde:

Los códigos de departamento y municipio deben obedecer a lo establecido por el DANE en la DIVIPOLA.
El código de notaría, el cual será de 4 dígitos, y hace referencia al número del despacho.
El código del acto notarial corresponde a los incluidos en la Resolución No. 826 de 2018.
Y el consecutivo es un valor numérico de seis (6) dígitos que será asignado por el sistema de la notaría de manera automática.

[6] Guías para la vinculación y uso de los servicios ciudadanos digitales; y Guía de lineamientos de los servicios ciudadanos digitales - https://www.gov.co/biblioteca/

Ejemplo de codificación:

11 (Cundinamarca) + 001 (Bogotá) + 0016 (No. Notaría) + 00000001 (código referido de la resolución 826 de 2018) + 2020 (año del Acto) + 000001 (Código consecutivo Acto Notarial)

Ejemplo de numero de consecutivo:

11001001600001420202000001

En atención a lo anterior cada acto notarial deberá identificarse bajo los siguientes parámetros digitales, conservando su especial configuración numérica:

a. Código CUANDI
b. Firma digital por parte del notario
c. Sello electrónico (Imagen que corresponde al sello físico del notario)
d. Código QR
e. Firma electrónica usuario
f. Mecanismo opcional de identificación del operador

El código CUANDI, será utilizado con varios propósitos, entre ellos:

- Identificador universal de los actos notariales que se generen digitalmente.
- Mecanismo del sistema técnico de control para validar la integridad y autenticidad de informaciones claves del ejemplar del acto notarial electrónico.

El CUANDI tal como se relaciona en esta especificación técnica, está indicado y referenciado para las instancias o ejemplares que contienen datos con la sintaxis y la semántica de operaciones notariales y que se producen para dejar registro electrónico de la ocurrencia de estas.

9. REGISTRO, AUTENTICACIÓN E IDENTIFICACIÓN:

9.1. AUTENTICACIÓN DE LOS ACTORES

En el caso del trámite de actos notariales por medios electrónicos, se deberá tener un sistema-mecanismo de autenticación. La autenticación es un elemento esencial de los sistemas digitales, ya que permite la identificación y reconocimiento de la persona que intervendrá en el acto notarial.

Para la prestación del servicio de autenticación digital se deberán atender las disposiciones sobre firma electrónica y digital contenidas en el Decreto 2364 de 2012 y la Ley 527 de 1999, sus normas reglamentarias y aquellas que las modifiquen, deroguen o subroguen.

Para ello podrá utilizar como guía las recomendaciones de **ISO29155/ITUX1254**.

La autenticación debe distinguirse conjuntamente con la etapa de Registro, que se relaciona a continuación:

9.1.1. REGISTRO – ENROLAMIENTO

1. Los usuarios del servicio público notarial, se deberán registrar en la herramienta ingresando sus datos personales y de identificación, donde se validará la información con el Archivo Nacional de Identificación (ANI) de la Registraduría Nacional del Estado Civil, con el fin de asegurar que los atributos de la persona a registrar sean confiables, o en su defecto aportar en su registro documentación que permita validar su rol en el sistema.

2. En el caso de usuarios internos, tales como notarios titulares, secretarios delegados, notarios encargados, interinos y demás funcionarios que desarrollen actividades delegadas por el notario, se podrán registrar en la herramienta ingresando sus datos personales y de identificación, validando la información con el Archivo Nacional de Identificación (ANI) de la Registraduría Nacional del Estado Civil a excepción de ciudadanos extranjeros, los cuales serán validados mediante el enrolamiento con la presentación del pasaporte, cédula de extranjería, PEP o cualquier otro avalado por las autoridades correspondientes del Gobierno Nacional.

   Adicionalmente los administradores de la solución deberán darle de alta en el sistema **según su respectivo rol**. Los administradores de la herramienta podrán registrar todo tipo de usuarios directamente en el sistema.

3. La información mínima requerida de obligatorio diligenciamiento al usuario del servicio público notarial será: tipo de documento, número de documento, nombres, primer apellido, segundo apellido, fecha de nacimiento, sexo, estado civil, correo electrónico, teléfono fijo o móvil, departamento y municipio de domicilio según la DIVIPOLA diseñada por el DANE, dirección domicilio teniendo en cuenta los lineamientos de los catastros respectivos.

   Adicionalmente, se recomienda que el formulario tenga campos para solicitar datos que permitan posteriormente hacer análisis para decisiones de política pública (p. ej. condiciones sociodemográficas, género, sujetos de especial protección, entre otros), estos campos adicionales no deben ser de obligatorio diligenciamiento y deberán seguir lo estipulado en la ley de protección de datos personales.

4. La solución tecnológica utilizada por el despacho notarial debe verificar el número de teléfono móvil enviando un mensaje de verificación o llamando al usuario para que este lo confirme. También debe verificar el correo electrónico enviando un mensaje de verificación al usuario para que también lo confirme.

5. La solución tecnológica utilizada por el despacho notarial debe almacenar la fecha de registro y actualización del usuario.

6. La Solución tecnológica utilizada deben generar reglas de creación y almacenamiento de

contraseñas seguras incluyendo doble factor de autenticación.

7. En el procedimiento de registro se le debe solicitar al usuario la aceptación expresa de los términos y condiciones de uso y operación del servicio, la cual debe quedar almacenada para su posterior consulta.

8. En el procedimiento de registro se le debe solicitar al usuario la aceptación expresa del tratamiento de datos y habeas data de acuerdo a lo establecido en el Decreto 1377 de 2013, Ley 1581 de 2012 y demás concordantes.

9. La aceptación de términos y condiciones y la de tratamiento de datos personales, deberá ser firmada electrónicamente, y deberá tener una estampa cronológica y número único de transacción.

10. En el caso específico de los usuarios del servicio público notarial, que deban firmar documentos o mensajes de datos, se les exigirá por parte de la notaría, el uso de firmas electrónicas, y el administrador de la herramienta deberá registrarlas en el sistema, previo enrolamiento y/o registro del usuario ante el despacho notarial de su elección.

11. Los administradores de la solución deberán actualizar el respectivo rol de los usuarios internos y externos, de acuerdo con las funciones de este, y darle de baja en caso de que su vinculación con la notaría, finalice.

9.1.2. AUTENTICACIÓN DEL USUARIO PÚBLICO NOTARIAL EN EL SISTEMA

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

Con base en lo anterior, la autenticación en el sistema se debe realizar por los mecanismos emitidos en el registro: contraseña segura para los usuarios en general y firmas electrónicas a usuarios del servicio público notarial, que deban firmar documentos o mensajes de datos.

Una vez esté disponible el servicio de Autenticación Digital de los Servicios Ciudadanos Digitales del Ministerio TIC, se podrá hacer uso del mismo, el cual ofrece a los ciudadanos y empresas un único servicio de autenticación, que les permite acceder de un modo seguro y confiable a los servicios que ofrece el Estado de acuerdo con el nivel de riesgo del servicio, y les permitirá a las entidades delegarles esta actividad a prestadores de servicio especializados y validados en ello sin perjuicio de la autenticación notarial.

Para lograr integrarse a la autenticación digital de los servicios ciudadanos digitales, las notarías deberán crear sistemas que permitan el desacople de la autenticación de usuarios, y delegarla a prestadores de servicio habilitados por el Min TIC mediante uso de protocolo OpenID Connect 1.0 y de acuerdo con la GUÍA PARA LA VINCULACIÓN Y USO DE LOS

SERVICIOS CIUDADANOS DIGITALES[7].

Nota 1: Previa autorización, la entidad almacenará los registros básicos de usuarios que hacen uso de sus sistemas de información.

9.2. IDENTIFICACIÓN DE USUARIOS

1. Para evitar la suplantación y fraude, la ley 527 de 1999 establece que la forma en la que se identifique al iniciador de un mensaje de datos será criterio para establecer la confiabilidad y valor probatorio.

2. Como requisito para la expedición de los mecanismos digitales los usuarios deberán identificarse a través de la cédula de ciudadanía digital o por biometría contra la base de datos de la RNEC, siguiendo las disposiciones que para tal efecto esta expida.

3. Si la identificación biométrica contra la base de datos de la RNEC es imposible de realizar debido a la falta o baja calidad de los datos biométricos o por otras razones de tipo tecnológico, la verificación de la identidad del usuario del servicio público notarial, se hará dando aplicación al artículo 24 del Decreto Ley 960 de 1970.

4. La solución tecnológica utilizada por el despacho notarial debe insertar en logs los intentos de identificación con mínimo los siguientes campos: tipo de documento, número de documento, fecha y hora identificación, id método identificación, calidad datos biométricos, resultado identificación.

5. La solución tecnológica de la notaría, debe acreditar el cumplimiento de los requerimientos establecidos por la RNEC, demostrando que cuenta con el respaldo de un operador biométrico homologado, a través del siguiente enlace: https://wsp.registraduria.gov.co/biometria/operadores/listar/. Además, deberá tener Infraestructura Tecnológica aprobada, desplegada y auditada por la RNEC en producción, realizando consultas permanentes del servicio de validación contra las bases de datos de identificación ciudadana (Biometría), manejando el estándar ISO 197942, conforme a lo dispuesto en la Resolución 3341 del 2013 de la RNEC, (5633 RNEC) su anexo y la normatividad vigente.

   A su vez las Superintendencia de Notariado y Registro convalida y autoriza el procedimiento de acceso, consulta y utilización de la base de datos de la información que produce y administra la RNEC, para la autenticación e identificación biométrica en línea y se autoriza su prestación en algunas Notarías del país, conforme lo dispuesto en el Decreto Ley 019 de 2012.

   La solución tecnológica podrá validar la identidad del usuario del servicio público notarial mediante la utilización de sistemas de verificación de documentos, llamada telefónica y video llamada, con el objetivo de demostrar plenamente la identidad, siempre que se

[7] Guías para la vinculación y uso de los servicios ciudadanos digitales; y Guía de lineamientos de los servicios ciudadanos digitales - https://www.gov.co/biblioteca/

genere la certeza de la identificación y autenticación del usuario, previa acreditación de los requisitos establecidos en el presente anexo al momento de su registro y/o enrolamiento.

9.3. VERIFICACIÓN DE DOCUMENTOS DE IDENTIFICACIÓN

- La solución tecnológica deberá tener la capacidad de identificar documentos de identidad a través de un sistema de procesamiento de documentos por medio de cámara del computador de escritorio, equipo portátil o dispositivo móvil del usuario del servicio público notarial, disponiendo de una calidad óptima de imagen a través de una cámara digital HD o superior, así como el dispositivo de audio de alta fidelidad con disminución de ruidos externos en la llamada en curso. Así mismo las condiciones ambientales y calidad de luz deben garantizar la identificación plena de los factores biométricos del usuario de acuerdo con los lineamientos de la RNEC.
- La solución tecnológica deberá contar con la verificación de los siguientes tipos de documento de identificación como: Cédula de ciudadanía, Cédula de extranjería o Tarjeta de identidad, pasaporte, PEP y demás avalados por las entidades gubernamentales.
- La solución tecnológica debe capturar la imagen del documento por anverso y reverso, utilizando el dispositivo de hardware y el sistema de procesamiento de documentos definido por el operador tecnológico. Deberá leer y almacenar al menos los siguientes datos: Nombres y apellidos, foto, firma, huella, retrato sombra y código de barras y cualquier otro documento de identificación que se habilite por parte de las autoridades competentes.
- La lectura de información del documento puede realizarse con el código de barras que se encuentra en la parte posterior del documento utilizando el estándar PDF417.
- La integración con Archivo Nacional de Identificación - ANI para la validación de datos biográficos debe relacionar la siguiente información:

    - Departamento de expedición
    - Municipio de expedición
    - Estado de la cédula
    - Fecha de expedición
    - Número del documento
    - Primer nombre
    - Segundo nombre
    - Primer apellido
    - Segundo apellido

9.4. CORROBORACIÓN DE IDENTIDAD

La validación de captura desde el documento de identidad físico se debe realizar a través de las siguientes fuentes:

- Validación de identidad biográfica básica para ciudadanos colombianos mayores de 18 años: la lectura realizada vía OCR, barcode o MRZ, debe validarse contra

la base de datos de la ANI.

- Validación de identidad biométrica para ciudadanos colombianos mayores de 18 años: la lectura realizada vía OCR, barcode o MRZ, debe validarse contra la base de datos de la RNEC.
- Para el caso de cédula de ciudadanía, pasaporte y cédula de extranjería, el sistema de procesamiento de documentos debe comparar los datos del MRZ con la zona visual, cuyo resultado deberá ser coherente.

9.5. AUTENTICACIÓN BIOMÉTRICA

Si la autenticación se realiza utilizando medios biométricos se deberá contar con una plataforma que incluya un motor multibiométrico, cuyo fin será permitir identificar de múltiples maneras los usuarios utilizando las diferentes posibilidades de reconocimiento biométrico (multidáctilar, rostro, huella, voz), conforme a los lineamientos que para tal efecto expida la RNEC.

Para efectos del enrolamiento al usuario por parte de la notaría, se deberá contar con la autenticación biométrica a través de equipos o mecanismos que se podrán usar de forma presencial o a través de la figura del domicilio notarial, de forma tal que se garantice el cotejo biométrico de los usuarios del sistema mediante captura de las huellas, rostro y voz conforme los lineamientos que para tal efecto expida la RNEC, y con ello dar inicio a la elaboración de la base de datos de los usuarios de forma digital en la notaría. El sistema deberá garantizar búsquedas 1 a 1 o en su defecto 1 a N (con la toma de la huella, rostro y voz). Para tal efecto, el sistema deberá estar en capacidad de poder hacer una búsqueda en toda la base de datos e identificar el usuario o actor del sistema con toda su información, con el fin de validar la identidad de un usuario registrado en los módulos del sistema dispuestos para la seguridad.

Todo el proceso de inscripción biométrica se deberá llevar a cabo con todos los actores que intervienen en el proceso y los solicitantes, los cuales deberán leer del código de la cédula y cargar los datos demográficos. Esta misma funcionalidad se deberá poder tener en una aplicación para smartphones o dispositivos móviles.

Los datos mínimos que se deben capturar en la base de datos se requieren en dos partes:

- **Datos demográficos:** Nombre, Apellidos, Fecha de nacimiento, Número de identificación, Género, Foto del documento de identificación.
- **Datos biométricos:** huellas dactilares (índice derecho e izquierdo), Imagen multidactilar, imagen facial, registro de la voz.

9.5.1. DISPOSITIVOS Y TECNOLOGÍA PARA LA GESTIÓN DE IDENTIFICACIÓN CONTRA LA BASE DE DATOS DE LA RNEC.

Se recomienda contar con los siguientes dispositivos, suministros y periféricos en las Notarías, los cuales además deben contar con las características tecnológicas, y/o que homologuen las siguientes funcionalidades mencionadas a continuación, de conformidad con las especificaciones de la RNEC:

a. Un lector Biométrico de huellas dactilares con las siguientes especificaciones:
   - Tipo de Sensor Óptico, Resolución del Sensor: 500 dpi, Área de captura de la Imagen: 16 x 24 mm o superior.
   - Detección Dedo vivo y falso.
   - El dispositivo debe estar homologado en la RNEC soportado en la última resolución, se verificará cumplimiento en el siguiente link: https://wsp.registraduria.gov.co/biometria/dispositivos/listar/
   - El equipo deberá estar homologado de acuerdo con el protocolo descrito y establecidos por las SNR de control como lo determina la CRC (Comisión de Regulación de Comunicaciones) para ser comercializados y distribuidos en Colombia, se verificará cumplimiento en el siguiente link: http://www.siust.gov.co/siic/publico/terminal-homologada.
   - En los casos de detectar con evidencias el intento de manipulación o traslado de los dispositivos y suministros, el Operador homologado impedirá a que continúen las validaciones de idSNR desde la Notaria, informando de manera inmediata a la SNR y RNEC.
   - A su vez se exigirá que el equipo de biometría cuente con una de las siguientes certificaciones CE (conformidad europea) y/o FCC (Comisión federal de comunicaciones.
b. Se deberá contar con Pistola o Lector de Código de Barras Bidimensional.
c. Cámara con sensor digital de alta definición y que genere imágenes nítidas, la cual deberá soportar el esquema de reconocimiento facial ISO/IEC 197945 a través de software.
d. Pad de Firmas.
e. Dispositivo de Identificación de Geolocalización. Hardware interno que deberá cumplir la función de identificar la Geoposición del Centro de Control y/o monitoreo y PC mediante el uso de tecnología GPS:
   - Sincronización. GPS Mínimo 30 canales, Cobertura Nacional. El sistema de posicionamiento debe garantizar la permanente geolocalización de la máquina en todo el territorio Nacional.
   - Precisión de ubicación. Radio máximo de veinte (20) metros de margen de error en la posición geográfica donde esté ubicada la antena en área urbana y (treinta) 30 metros en área rural en cobertura satelital.
   - Actualización máxima de la geolocalización, comunicación celular y/o satelital. Marcación del posicionamiento interno cada 60 minutos.
   - Envío de la información de la ubicación al centro de control y/o plataforma de monitoreo cada 60 minutos enviará una (1) posición con la identificación del PC, dirección MAC y número de serie de la tarjeta madre.
   - Compatibilidad con los prestadores de servicios móviles de comunicación en cuanto a tecnología, cobertura y disponibilidad requerida, existentes en el mercado.
   - Este dispositivo debe permitir dar cumplimiento a lo establecido en el numeral 11. GEOLOCALIZACIÓN.

9.5.2. VALIDACIÓN CON BIOMETRÍA FACIAL

1. El procedimiento deberá contemplar la reglamentación que para tal efecto expida la

RNEC en la materia, pero en todo caso, a continuación, se describen los controles mínimos para asegurar la verificación de identidad usando métodos faciales, entre tanto se regula la materia:

2. El sistema podrá permitir la utilización de técnicas de rostro vivo.

3. Con el objetivo de garantizar que el rostro que se capture es vivo, el sistema deberá exigir la realización de pruebas de vida al ciudadano, a través del uso de verificación de movimientos y expresiones faciales.

4. El sistema debe exigir movimientos de faciales con los cuales se garantiza que la fotografía que se capture sea de una persona mirando al frente, y con ello cotejarla con la foto de la cédula del usuario.

5. Para aquellos actos notariales que exigen el requisito de la verificación de huella dactilar por medios electrónicos, los mismos se adelantaran a través del enrolamiento que debe hacer el notario de la firma electrónica del usuario en el repositorio que para tal efecto disponga, así como la captura de huella y el registro fotográfico por una única vez. Aunado a lo anterior, y previo a la suscripción del acto notarial, el notario generará al usuario del servicio público, las credenciales de acceso a la plataforma (usuario y contraseña), y el proceso debe generar las condiciones de validación y seguridad para identificar al usuario de la plataforma, ya sea a través del correo electrónico y/o mensaje de texto al dispositivo móvil.

6. El procedimiento de biometría facial debe seguir los siguientes pasos, conforme los lineamientos que para tal efecto dicte la RNEC:

   - El sistema debe solicitar los permisos de utilización de la cámara.
   - El sistema debe permitir capturar el rostro.
   - El sistema debe permitir aplicar técnicas de rostro vivo, utilizando las diferentes pruebas.
   - El sistema debe facilitar el envío de mensajes de texto al dispositivo móvil del usuario.
   - El sistema debe permitir el envío automático de correo electrónico al usuario.

10. FIRMA DIGITAL – FIRMA ELECTRÓNICA

La firma electrónica y la digital son medios de identificación personal y se asemejan a la clásica firma manuscrita. La manuscrita se plasma en cualquier documento en papel y se vincula a un soporte físico, en tanto que la electrónica y digital son un medio de identificación respecto de un mensaje de datos.

Los notarios, adicionalmente al registro físico de firmas de usuarios que conservan en su despacho; para efectos de las actuaciones notariales por medios electrónicos, previo a la rogación de éstas, deberán contar con un registro electrónico con base en el cual se creará la firma electrónica del usuario firmante, de conformidad con el Decreto 2364 de 2012, y tendrá una vigencia de un (1) año, contado a partir de la autorización del registro hecha por el notario.

Para este registro electrónico se requiere la plena identificación del usuario, la autorización para el tratamiento de sus datos personales, la manifestación de sus generales de ley, incluyendo su estado civil y demás datos personales, lo mismo que la captura de firmas y huellas para que se pueda otorgar virtualmente y en forma segura un acto o instrumento notarial.

La plataforma tecnológica deberá crear de forma automática los circuitos de firmado para cada uno de los trámites solicitados por los usuarios del servicio, de tal forma que la circularización esté completamente automatizada e integrada a los procesos regulares de la prestación del servicio. Los usuarios que otorgan o firman los instrumentos notariales deben estar vinculados al trámite desde su inicio o solicitud y la vinculación al proceso de firmado debe estar regido por el trámite notarial que se está llevando a cabo.

Los usuarios y sus derechos en la plataforma tecnológica autorizada son gestionados desde el módulo de usuarios en un proceso completamente integrado, en caso de hacer uso de plataformas externas para el firmado, el proceso se dispara de forma automática y el consumo de los servicios se realizan mediante web services con protocolos seguros.

La plataforma deberá permitir al usuario administrador:

- Crear o modificar configuraciones de usuarios firmantes o elaboradores.
- Gestionar grupos de firmantes que puedan suscribir el (los) documento(s), para los casos en los que deban ser firmados por varias personas.
- Crear roles de elaboradores de documentos en la notaría y asignarles usuarios en el sistema.
- Configurar las políticas de firma.
- Mostrar los campos de los tipos documentales asociados con los procesos de firma.
- Debe tener la opción de acceder a una sección de informes para monitorear el proceso de firma.

Parágrafo. Cuando una persona deje de ser apoderado, poderdante, representado y/o representante legal de una persona natural o jurídica, y tenga inscrita la firma en el registro

electrónico, deberá informar sobre esta situación al Notario para que éste lo cancele una vez pierda esa condición, sin perjuicio de hacerlo oficiosamente si tuviere conocimiento de esta circunstancia, con base en los documentos que la sustenten. La misma cancelación oficiosa procederá cuando el notario tenga conocimiento del fallecimiento de un inscrito, con base en el registro civil de defunción o su consulta en el Registro Único de Afiliados a la Protección Social –RUAF-.

10.1. FIRMA DEL NOTARIO

- La firma digital del Notario deberá contar con el respaldo de una entidad de certificación digital acreditada por el Organismo Nacional de Acreditación de Colombia (ONAC), permitiéndole identificar el grafo de su firma, su identificación y datos complementarios de la notaría.
- La firma incorporará un sello gráfico que identifique plenamente a la notaría y que permita acceder a los detalles del certificado digital y el resumen de su validez.
- La ubicación de la firma notarial se podrá parametrizar por cada notaría.

10.1.1. FORMATOS DE FIRMA

La plataforma debe tener habilitados los componentes de firma PAdES, CAdES y XAdES.

10.1.1.1. FIRMA ESTÁNDAR PADES (PDF)

En este nivel de confianza los documentos requieren una firma digital, que cumpla la acreditación como Entidad de Certificación digital abierta y tener valor legal completo de acuerdo con la normatividad vigente. Los documentos firmados deberán estar en formato PDF y la firma debe cumplir con el estándar PAdES. Debe evitar la modificación de los documentos PDF, como la adición de textos, imágenes u otros elementos durante el proceso de firma. La firma también puede tener una representación visual como un campo de formulario, tal como podría tenerla en un documento impreso.

En la siguiente lista se definen brevemente los perfiles definidos por PAdES (ETSI TS 102 778):

- **PAdES Basic:** Perfil básico que cumple con los requisitos especificados en la norma ISO 32000-1.
- **PAdES-BES Profile (Enhaced):** Este perfil especifica una firma PDF avanzada basada en CAdES-bes e incorpora opción de incluir en la firma un sello de tiempo (CADES-T).
- **EPES Profile (Enhaced):** Este perfil especifica una firma PDF avanzada basada en CAdES-EPES. Es el PAdES-BES Profile añadiendole un identificador de política de firma y, opcionalmente, una referencia al tipo de compromiso adquirido.
- **PAdES-LTV Profile (Long Term):** Es el formato de firma longeva. Este perfil permite prorrogar por tiempo indefinido la validez de las firmas en formato PDF. Puede ser usado en conjunción con el PAdES-CMS, PAdES-BES o perfiles PADES-EPES. Este perfil es utilizado para garantizar la validación tras muchos años después de la realización de la firma. Es decir, garantiza la validación a largo plazo.

10.1.1.2. FIRMA ESTÁNDAR CADES (TODOS LOS MENSAJES ELECTRÓNICOS).

En este nivel de confianza los documentos requieren una firma digital, que cumpla la acreditación como Entidad de Certificación digital abierta y tener valor legal completo de acuerdo con la normatividad vigente. Los documentos firmados deberán estar en formato cades y firmar cualquier mensaje de datos.

El formato CAdES tiene definidos 6 perfiles diferentes, según el nivel de protección ofrecido. Cada perfil incluye y mejora al anterior.

- **CAdES:** Forma básica que simplemente cumple los requisitos legales de la Directiva para firma electrónica avanzada
- **CAdES-T (timestamp):** Se le incorpora información el campo con sello de tiempos para proteger los datos de un posible repudio.
- **CAdES-C (complete):** Es un CAdES-T al que se le añade referencias sobre los certificados y listas de revocación utilizadas para permitir la validación off-line y su verificación en el futuro (sin almacenar los datos actuales de verificación).
- **CAdES-X (extended):** Es un CAdES-C al que se le añade información sobre la fecha y hora de los datos introducidos para la extensión C.
- **CAdES-X-L (extended long-term):** Es un CAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. Garantiza la validación off-line a largo plazo incluso si la fuente original no estuviera disponible.
- **CAdES-A (archivado):** Este formato incluye toda la información anterior, pero incluye meta-información asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. *El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.*

10.1.1.3. FIRMA ESTÁNDAR XADES (XML)

Es una familia de firmas basadas en formatos XML. A diferencia que un formato embebido como pudiera ser el PDF-Signature, es un lenguaje pensado para «conversar entre máquinas»; es decir, el intercambio de información entre sistemas automatizados es el propósito de usar un formato basado en XML. Dentro de este formato de firmas, se han ido evolucionando distintas extensiones que dan respuesta a distintas necesidades y escenarios; las extensiones descritas a continuación no tienen que considerarse de menos a más en el grado de robustez, fiabilidad o seguridad, sino que deben considerarse como evoluciones del formato que dan respuesta a escenarios distintos, y no por ello compiten entre sí.

- **XAdES-BES:** Firma básica
- **XAdES-EPES:** XAdES-BES al que se le incorpora información sobre la política de firma, como pudiera ser aquella información sobre el certificado empleado y la entidad certificadora que lo emitió.

- **XAdES-T (timestamp):** Es un XAdES-EPES al que se le añade una segunda firma, pero en esta ocasión, una firma realizada por una TSA (Time Stamp Authority). Esta segunda firma aporta información específica sobre la fecha y hora exacta de la firma.
- **XAdES-C (complete):** Es un XAdES-T al que se le añaden referencias sobre los certificados y listas de revocación utilizadas para la validación del propio certificado utilizado para la firma. Por ejemplo: fue firmado por Certificado CCC emitidos por CA AAA y cuya CRL RRRR fue consultada en el momento de la validación.
- **XAdES-X (extended):** Es un XAdES-C al que se le añade información sobre la fecha y hora de los datos introducido para la extensión C.
- **XAdES-XL (extended long-term):** Es un XAdES-X al que se le incorporan los certificados (sólo clave pública) y las fuentes de validación que se usaron. A diferencia del -C, donde sólo se incluía una referencia (un apuntador), en este formato se embebe toda esa información. Por ejemplo, en el caso de una CRL, se incorpora la lista firmada de certificados revocados que fue consultada en ese momento. Esto se utiliza para garantizar la validación muchos años después de la firma incluso en el caso que la CA que emitió el certificado, o la fuente de validación (CRL) que se consultó, ya no esté disponibles (publicadas, por ejemplo). Es decir, garantiza la validación off-line a largo plazo.
- **XAdES-A (archivado):** Este formato incluye toda la información anterior, pero incluye metainformación asociada a políticas de refirmado. Una política de refirmado establece un período de caducidad de la firma digital, y superado este tiempo, se procede a un refirmado. El escenario ideal para este formato de firma son aquellos documentos cuya validez sea muy elevada: *hipotecas, títulos universitarios, escrituras, etc. 15, 20, 50 años, etc.*

10.3. FIRMA ELECTRÓNICA DEL USUARIO DEL SERVICIO PUBLICO NOTARIAL

Se entiende como firma electrónica, métodos tales como, códigos, contraseñas, datos biométricos, o claves criptográficas privadas, que permite identificar a una persona, en relación con un mensaje de datos, siempre y cuando el mismo sea confiable y apropiado respecto de los fines para los que se utiliza la firma, atendidas todas las circunstancias del caso, así como cualquier acuerdo pertinente. Para tal efecto, el notario deberá realizar las labores de verificación del cumplimiento de los requisitos establecidos en el Decreto 2364 de 2012, respecto de la firma electrónica del usuario del servicio público notarial.

11. GEOLOCALIZACIÓN

La actividad notarial se ejerce en círculos geográficos definidos, y aunque tecnológicamente no existen barreras respecto a la ubicación para numerosos trámites, las disposiciones legales, condicionan la prestación del servicio a la ubicación tanto del Notario y sus funcionarios como de las personas naturales y jurídicas.

Es necesario en el ejercicio de la actividad notarial digital, validar la ubicación de los intervinientes en el acto, permitiendo que solo puedan adelantarlos aquellos notarios pertenecientes al círculo respectivo de rogación del servicio. Se debe validar para cada acto notarial el alcance y limitaciones de ubicación.

De acuerdo con las anteriores apreciaciones, se debe tener en cuenta:

- El sistema debe validar durante la actividad de registro los datos básicos del usuario, como son: nombre, número de identificación, dirección de residencia, correo electrónico y número de teléfono.

- La verificación del círculo notarial se hará al otorgamiento del acto, mediante la validación de la geolocalización del usuario del servicio público notarial.

- Para validar la ubicación de los actores, el sistema debe acogerse a la geolocalización dispuesta para América Latina, mediante la captura de las coordenadas GPS utilizando el Sistema de Coordenadas MAGNA-SIRGAS Datum Bogotá SIRGAS: Sistema de Referencia Geocéntrico para las Américas, el cual es el Establecido Oficialmente por parte del IGAC - Instituto Geográfico Agustín Codazzi, mediante la cual se garantiza la compatibilidad de las coordenadas colombianas con las técnicas espaciales de posicionamiento. Dicha métrica deberá garantizar la ubicación en tiempo real de los actores en el momento del acto público notarial.

12. SEGURIDAD DIGITAL

Las Notarías del país, al establecer la realización de actos o trámites notariales a través de medios digitales o presenciales, deberán contar con sistemas que permitan realizar los procesos y su interacción de manera segura para evitar las intrusiones, el desvío y/o pérdida de información.

Después de la correcta autenticación el componente de autorización debe permitir que los distintos usuarios solo tengan acceso a la información y funcionalidades acordes a su rol y llevar un registro de auditoría donde se pueda establecer la trazabilidad de las funcionalidades utilizadas en cada sesión de trabajo y sus modificaciones.

En el caso de la autenticación de ciudadanos, sin perjuicio de la notarial, se debe contemplar la utilización del sistema de autenticación electrónica de los servicios ciudadanos digitales como se referencia en la sección.

12.1. AUTENTICACION

Por la dinámica del negocio en servicios de trámites notariales, como ya se menciono es importante establecer de forma fidedigna la ubicación de los actores para que sea acorde a las limitaciones establecidas en cada trámite notarial, así que, según sea el caso se deberán implementar modelos que permitan establecer la ubicación de Notario, funcionarios notariales y personas, como se relacionó en el acápite geolocalización.

Se deben establecer políticas de seguridad, siguiendo los lineamientos del Modelo de Seguridad y Privacidad de la información - MSPI de la política de Gobierno digital, que garanticen la continuidad de operación y la recuperación en el caso de siniestros, con sistemas redundantes, copias de seguridad y hacking ético. El Sistema Integrado de Servicios y Gestión de la SNR -SISG- tendrá la capacidad de intercambiar información con el Repositorio administrado por la SNR, el cual contiene las políticas de seguridad necesarias que garanticen la fidelidad de la información con su original que reposa en cabeza del notario.

En el tema de riesgos también se deben contemplar aspectos del MSPI, el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI, el Modelo Integrado de Planeación y Gestión (MIPG) y La Guía para la Administración del Riesgo y el Diseño Controles en entidades Públicas, este modelo pertenece al habilitador transversal de Seguridad y Privacidad, de la Política de Gobierno Digital.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información.

12.2. SELLO DIGITAL NOTARIAL

Es el sello que de forma digital y personalizada debe elegir el notario, y que podrá imponer a los actos notariales que genere bajo condiciones de seguridad.

12.3. ESTAMPADO CRONOLÓGICO

El servicio de estampado cronológico o marca de tiempo, permite asociar los documentos electrónicos con una referencia temporal que certifica técnicamente que la serie de datos ha existido y no ha sido modificada tomando la hora legal colombiana del Instituto Nacional de Metrología, o quien haga sus veces, adhiriendo una firma digital certificada por una Autoridad de Sellado de Tiempo (Time Stamp Authority), según los lineamientos de la RFC3161.

Para que el solicitante pueda hacer uso del servicio de estampado cronológico deberá adquirir y asociar un certificado digital emitido por el operador digital de cada notaria, podrá adquirirlo mediante certificados digitales en token físico o por el servicio de firma centralizada y pagar acorde con la estimación de consumo.

Procesos del servicio de Sellado de Tiempo Digital confiable:

Solicitud del Sellado: Se debe generar una petición TimeStampRequest.

Los parámetros que se enviarán serán los siguientes:

- Función de resumen - Hash del documento a estampar.
- Nombre del algoritmo de hash a usar.
- Identificador de objetos - OID de política bajo la cual se proporciona la estampa.
- Versión: Número de versión de la sintaxis utilizada.
- MessageImprint: Contiene el hash de los datos que se quiere estampar. La longitud del hash tiene que coincidir con la longitud de hash del algoritmo utilizado.
- El algoritmo Hash criptográfico de 256 bits.
- Deberá tener el parámetro reqPolicy: que indique a la TSA la política bajo la cual quiere que se proporcione la estampa. Este parámetro será indicado por la Entidad de Certificación Digital.

Proceso:

En el proceso de sellado, el sistema deberá realizar diferentes acciones:

- 1) Realizar la revisión de la petición, verificando la correcta estructuración del objeto TimeStampRequest y el origen de la misma. Durante esta verificación se deberá comprobar que se han introducido los parámetros esperados como el algoritmo de hash y la política de sellado, y que son correctos.
- 2) Se debe obtener la fuente segura de tiempo del Instituto Nacional de Metrología y generar el token de tiempo que debe ser firmado digitalmente con las claves privadas del servicio de estampa cronológica de tiempo de la entidad de certificación digital.

- 3) Generar la respuesta TimeStamp Response, acorde con RFC3161.

En el instante de tiempo en el que se cree la estampa. de acuerdo las normas ISO como el IETF se expresará el instante de tiempo referido a la escala UTC.

12.4. SEGURIDAD INTEGRAL DEL SISTEMA

En el marco de los lineamientos de ISO 27001-2013, se requerirá al notario, el Plan Estratégico de Seguridad de la Información, el cual se debe alinear e implementar dentro de los doce (12) meses siguientes a la autorización para la prestación del servicio público notarial a través de medios electrónicos expedida por la SNR, atendiendo la Legislación Colombiana, el alineamiento con Gobierno en Línea y las demás normas aplicables en la materia.

El notario validará que el operador tecnológico a la implementación y una vez al año, realice una consultoría de detección y análisis de riesgos basada en Ethical Hacking, ejecutada por un profesional Ethical Hacking Certified por el EC-Council. Como resultado de las pruebas la notaria u operador deberá presentar el certificado de la actividad realizada de Ethical Hacking. A los 6 meses de realizada dicha prueba se realizará un retest para verificar que se hallan mitigado las vulnerabilidades detectadas.

La notaria deberá que entregar a la Superintendencia de Notariado y Registro – OTI- Oficina de tecnologías de la Información- un informe con capturas de pantalla que describan resultados de pruebas de carga y estrés. Para este fin tendrá que utilizar el software JMETER que permite hacer dicha identificación. Los resultados no deben superar el tiempo de 4 segundos para 20 conexiones simultaneas.

Dicha consultoría debe especificar un plan de remediación de los hallazgos y de mitigación de los riesgos encontrados.

Igualmente, se deberán definir las políticas de seguridad apegados al estándar ISO 27001.

Se recomienda que el notario cuente para su plataforma tecnológica con un BCP (Business Continuity Plan) y de un DRP (Disaster Recovery Plan) como parte de sus procesos de seguridad.

El notario debe cumplir las políticas, los controles de seguridad y directrices que la SNR defina, tales como:

El sistema de información notarial debe permitir asociar múltiples servicios a un rol.
El sistema de información notarial debe permitir asociar múltiples roles a un usuario.
El intercambio de datos entre cliente y servidor debe hacerse a través de un protocolo seguro como TLS v1.2 o SSL v3 y usar un cifrado mínimo de 256 bits.
Basar su sistema de control de acceso en una metodología reconocida de autenticación por doble factor.

12.5. SEGURIDAD DOCUMENTAL

a. Atributos de certificación digital (Autenticación e Integridad)
b. Confidencialidad
c. Custodia & Disponibilidad
d. Gestión de Notas & Aclaraciones

12.6. SEGURIDAD DE LA INFORMACIÓN

- Los servicios en la arquitectura deben contemplar las políticas y protocolos de seguridad de la información en los atributos de: Autenticidad, Integridad y No Repudio.
- Establecer un acuerdo de confidencialidad sobre la información manejada y sobre las actividades desarrolladas.
- Dar estricto cumplimiento los procedimientos del Sistema de Seguridad de la Información y a las políticas de Seguridad Informática definidas por la SNR.
- Definición de procedimientos y controles para la entrega de la información manejada al notario, a su vez el notario debe verificar la destrucción la información en custodia por parte del operador al finalizar su operación.
- El notario debe garantizar como parte del componente de seguridad control de acceso al sistema de información mediante privilegios de seguridad a través de configuración de roles acordes con el punto anterior.

12.6.1. GUARDA DIGITAL DEL TESTAMENTO:

De conformidad con el artículo 59 del Estatuto Notarial y D.U.R. 1069 de 2015 del sector justicia, para ejercer la custodia del testamento cerrado de forma digital, el notario deberá garantizar la encriptación del mismo, en el momento de su envío por medios digitales o electrónicos por parte del usuario del servicio, para que sólo sea abierto y publicado bajo las condiciones establecidas en la norma. A su vez de deben ejercer las mejores prácticas de seguridad y hacking ético, que garantice que no puede ser abierto ni visualizado y se garantice su conservación, a través de un algoritmo de encriptación avalado por la empresa que practique el hacking ético.

12.7. ASEGURAMIENTO DE LA SEGURIDAD DEL SOFTWARE

De forma complementaria se pueden utilizar modelos ampliamente utilizados para la identificación y mitigación de riesgos de seguridad como el de los 10 Principales Riesgos de Seguridad para las aplicaciones WEB según OWASP[8], que identifica las vulnerabilidades más críticas que se encuentran comúnmente las aplicaciones WEB, y sus recomendaciones para solucionarlas, estas son:

Inyección

Es una vulnerabilidad de las aplicaciones WEB, que afecta directamente a las bases de datos

[8] OWASP, Open Web Application Security Project. https://owasp.org/www-project-top-ten/

de la aplicación. Una inyección SQL, LDAP o CRLF consiste en insertar o en inyectar código SQL malicioso dentro de código SQL para alterar el funcionamiento normal y hacer que se ejecute el código "malicioso" dentro del sistema.

Pérdida de autenticación

Las vulnerabilidades relacionadas con la pérdida de autenticación son críticas en la seguridad de las aplicaciones y en especial de las aplicaciones WEB, ya que permiten a un usuario suplantar la personalidad de otro. Existen muchas situaciones en la que nos encontramos ante una aplicación WEB vulnerable a este tipo de ataque, pero la mayor parte de las veces se encuentran en la gestión de las contraseñas, la expiración de sesiones o el proceso de cierre de sesión.

Exposición a datos sensibles

Las aplicaciones WEB que no protegen adecuadamente los datos confidenciales, como datos financieros, nombres de usuario y contraseñas, o información de salud, podrían permitir a los atacantes acceder a dicha información para cometer fraudes o robar identidades.

Entradas XML

Este es un ataque contra una aplicación web que analiza la entrada XML *. Esta entrada puede hacer referencia a una entidad externa, intentando explotar una vulnerabilidad en el analizador. Una "entidad externa" en este contexto se refiere a una unidad de almacenamiento, como un disco duro. Se puede engañar a un analizador XML para que envíe datos a una entidad externa no autorizada, que puede pasar datos confidenciales directamente a un atacante.

Control de acceso

El control de acceso se refiere a un sistema que controla el acceso a la información o la funcionalidad. Los controles de acceso defectuosos permiten a los atacantes eludir la autorización y realizar tareas como si fueran usuarios privilegiados, como los administradores. Por ejemplo, una aplicación web podría permitir a un usuario cambiar la cuenta en la que inició sesión simplemente cambiando parte de una URL, sin ninguna otra verificación.

Mala configuración de la seguridad

Este riesgo se refiere a la implementación incorrecta de los controles destinados a mantener seguros los datos de la aplicación, como la mala configuración de los encabezados de seguridad, los mensajes de error que contienen información confidencial (fuga de información) y no los parches o los sistemas de actualización, los marcos y los componentes.

Secuencia de comandos en sitios cruzados (XSS)

Los ataques XSS tienen como objetivo el código (también llamado secuencia de comandos)

de una página web que se ejecuta en el navegador del usuario, no en el servidor del sitio web. Cuando el usuario es atacado, se introducen secuencias de comandos maliciosas en su navegador que intentarán dañar su equipo. La variedad de ataques XSS es prácticamente ilimitada, pero los más comunes suelen ser la recopilación de datos personales, el redireccionamiento de las víctimas a sitios controlados por hackers o el control del equipo por parte de estos.

Deserialización insegura.

La deserialización insegura es una nueva vulnerabilidad propuesta por la comunidad de OWASP que aparece por primera vez en OWASP Top 10. Se trata de una vulnerabilidad que podría permitir la ejecución remota de código en servicios web.

Uso de componentes con vulnerabilidades conocidas

Con frecuencia, los desarrolladores no saben qué componentes de código abierto y de terceros están en sus aplicaciones, lo que dificulta la actualización de los componentes cuando se descubren nuevas vulnerabilidades. Los atacantes pueden explotar un componente inseguro para hacerse cargo del servidor o robar datos confidenciales.
El análisis de la composición del software realizado al mismo tiempo que el análisis estático puede identificar versiones inseguras de componentes.
Está vulnerabilidad está motivada en parte por el uso extendido de múltiples componentes en aplicaciones web así como el crecimiento que está teniendo IoT y las dificultades que presenta dicho modelo en cuanto a gestión de actualizaciones.

Insuficiente registro y monitoreo

El tiempo para detectar una violación se mide con frecuencia en semanas o meses. El registro insuficiente y la integración ineficaz con los sistemas de respuesta a incidentes de seguridad permiten a los atacantes girar a otros sistemas y mantener amenazas persistentes.

13.CONFIDENCIALIDAD

Para las notarías los documentos son su activo más valioso y por ello se invierten considerables recursos en la creación, administración, distribución y consulta. Por otra parte, la diversidad de sistemas tecnológicos, medios de comunicación y formatos digitales permiten el acceso de forma remota de prácticamente cualquier fuente, el reto es entonces realizar los servicios notariales usando los medios tecnológicos asegurando la validez y autenticidad de los documentos presentados en el acto.

Entendiendo que el resultado de los actos y trámites notariales son principalmente documentos, es de vital importancia no solo la custodia sino la certeza de la inalterabilidad de estos. La Superintendencia de Notariado y Registro y las Notarías, deberán establecer la realización de actos o trámites notariales a través de medios digitales o presencialmente.

En el caso del trámite por medios digitales se deberá contar con sistemas que garanticen la autenticidad, el acceso o restricción de los documentos y archivos anexos.

En principio la definición de las políticas de seguridad que deben establecer la forma de interacción de los Sistemas de Información Notarial, las personas – naturales o jurídicas y los demás actores de cada proceso.

Todos los participantes de los procesos notariales, serán responsables de la seguridad de la información.

Los documentos electrónicos deberán seguir los lineamientos establecidos por el Archivo General de la Nación de Colombia implementando un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA), donde se establece el ciclo de vida de los documentos electrónicos, así mismo se puede referenciar la NTC-ISO/IEC 27001 Tecnología de la Información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).

Los documentos electrónicos tienen asociados niveles distintos de accesibilidad y restricción de modificaciones, por tanto, los sistemas de información notarial deben garantizar que el usuario cuente con la autorización necesaria para la funcionalidad realizada y contemplar la trazabilidad del acceso, copia, descarga, impresión y otras actividades que redunden en el acceso del documento por fuera del sistema. En los documentos de mayor confidencialidad se deben considerar sistemas de encriptación para limitar su acceso y de validación de autenticidad con la adición de firmas digitales, electrónicas y/o metadatos para establecer la autenticidad del documento.

Es posible que existan documentos que incluso solo puedan accederse en condiciones determinadas y que ni siquiera los funcionarios tengan acceso a él salvo que se cumplan los requisitos establecidos como una fecha o el deceso de una persona en el caso de un testamento.

En un escenario ideal, cada actor en el trámite notarial genera o avala información y certifica

su autenticidad, sin embargo, no todos los actores tienen en la actualidad la capacidad o recursos para hacerlo, por ello se debe considerar una implementación que permita la interacción con la situación actual y a disponer de un componente de intercambio para realizar la conexión a futuro. Por ejemplo, los sistemas de información deben permitir mediante gov.co, la interacción con Servicios Ciudadanos Digitales como son: el servicio de autenticación electrónica para el acceso de las personas, Carpeta ciudadana para el registro de los trámites notariales y el servicio de interoperabilidad para la interacción con otros actores que participan en el proceso, como la Registraduría General de la Nación. El acceso por usuarios y/o sistemas externos deben ceñirse a las políticas establecidas en SGDEA.

Toda vez que no existen sistemas invulnerables, es importante el monitoreo de incidentes de seguridad y pruebas aleatorias de los documentos para validar su integridad. Se deben disponer de procedimientos que realicen una detección oportuna de incidentes, así como los procedimientos de respuesta a contingencias; además se debe garantizar la evolución de las plataformas para adaptarse a los diversos cambios de mejora de procesos, experiencia y seguridad, así como su mantenimiento periódico.

14. BLOCKCHAIN

Se debe evaluar la aplicabilidad presente y futura del uso de nuevas tecnologías de autenticación distribuidas, como las cadenas de bloques -blockchain-.

El notariado es un escenario natural de blockchain. Algunos registros se mantienen en forma impresa y son susceptibles a cambios y manipulación por parte de un tercero o partes maliciosas internas. El almacenamiento en el Repositorio Notarial digital permite centralizarlo como una copia de respaldo y de validación con respecto a la que reposa digitalmente en la notaría. Si además se utilizan cadenas de bloques cada acto notarial y/o cambio asociado al documento, quedará marcado, lo que facilitará la inalterabilidad y validación del documento. El esquema sugerido para consideración es del de blockchain privado, en donde solo los que tienen permiso pueden acceder a las cadenas y la modificación de las mismas está determinada por la administración.

Asi pues, se puede comprobar la existencia de un documento desde el momento de su creación y la verificación es 100% precisa, teniendo en cuenta que los datos una vez escritos dentro de la blockchain no pueden modificarse por su esquema distribuido. Si alguien intenta cambiar los datos, el hash ya no coincidirá, evidenciando que datos han sido modificados y declarando al documento como no confiable.

15. COMUNICACIONES Y NOTIFICACIONES ELECTRÓNICAS

Las Notarías deben proveer el mecanismo de comunicaciones y notificaciones electrónicas, para que el ciudadano conozca o refrende su participación en todo acto o trámite notarial del cual haga parte, actuando en concordancia con la Ley 1437 de 2011 "Por la cual se expide el Código de Procedimiento Administrativo y de lo Contencioso Administrativo", el cual entró en vigencia el 2 de julio de 2012, según lo establecido en el artículo 56. "NOTIFICACIÓN ELECTRÓNICA. Las autoridades podrán notificar sus actos a través de medios electrónicos, siempre que el administrado haya aceptado este medio de notificación".

Los mecanismos de comunicaciones y notificaciones electrónicas mínimos requeridos son: correo electrónico, mensaje de texto (SMS), red social de WhatsApp y mediante el acceso a la plataforma con el usuario y contraseña como doble factor de autenticación. De acuerdo con la criticidad del evento del acto notarial, la notificación debe ser certificada electrónicamente, con mínimo las siguientes evidencias:

a. Prueba de envío y entrega: será aplicable lo dispuesto en los artículos 20 y 21 de la ley 527 de 1999 en la República de Colombia.

b. Prueba del contenido: tendrá pleno valor probatorio, de conformidad con lo dispuesto en el artículo 10 de la ley 527 de 1999.

c. Sello de hora oficial: Para ello se incorpora el servicio de estampado cronológico emitido por un proveedor de servicios de certificación digital, dando fe de la fecha y hora de envío y recibo, el cual se halla sincronizado con la hora legal colombiana que mantiene, coordina y difunde el Instituto Nacional de Metrología, según sus patrones de referencia del Laboratorio de Tiempo y Frecuencia (Articulo 6, Decreto 4175 de 2011).

d. Evidencia admisible: Los acuses de recibo generados son admisibles respecto del hecho de envío y entrega, así como sobre la autenticidad de su contenido, cumpliendo con las disposiciones legales sobre la materia, de conformidad con lo establecido por los artículos 12 y 20 de la Ley 527 de 1999.

16. GESTIÓN DE DOCUMENTOS Y EXPEDIENTES ELECTRÓNICOS

La gestión y el tratamiento de los documentos y expedientes electrónicos presentes en el ámbito notarial requiere el cumplimiento de las políticas y lineamientos técnicos dictados conjuntamente por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones.

La producción, gestión y tratamiento de los documentos y expedientes electrónicos deberán cumplir esas políticas, características y fases durante todo su ciclo de vida.

16.1. DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Las características son aplicables al documento electrónico de archivo y hace referencia a las políticas, mecanismos, técnicas y procedimientos que garantizan su autenticidad, fiabilidad, integridad y disponibilidad.

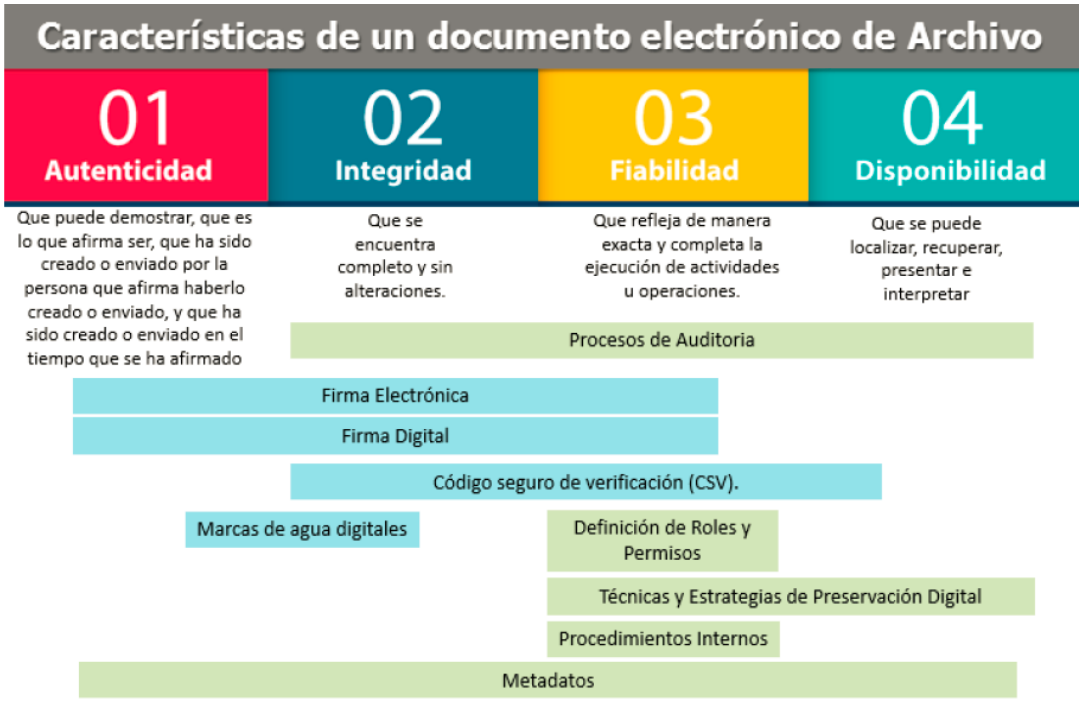


Ilustración 3. Características Genéricas de un documento electrónico de archivo. Fuente: Guía para la gestión de documentos y expedientes electrónicos (G.INF.07) MinTIC-AGN.

Para llevar a cabo una adecuada gestión del documento electrónico se deberá tener en cuenta unas etapas[9] y actividades dentro de cada una de ellas como se ilustra a continuación:

9 Artículo 2.8.2.5.7 del Decreto 1080 de 2015

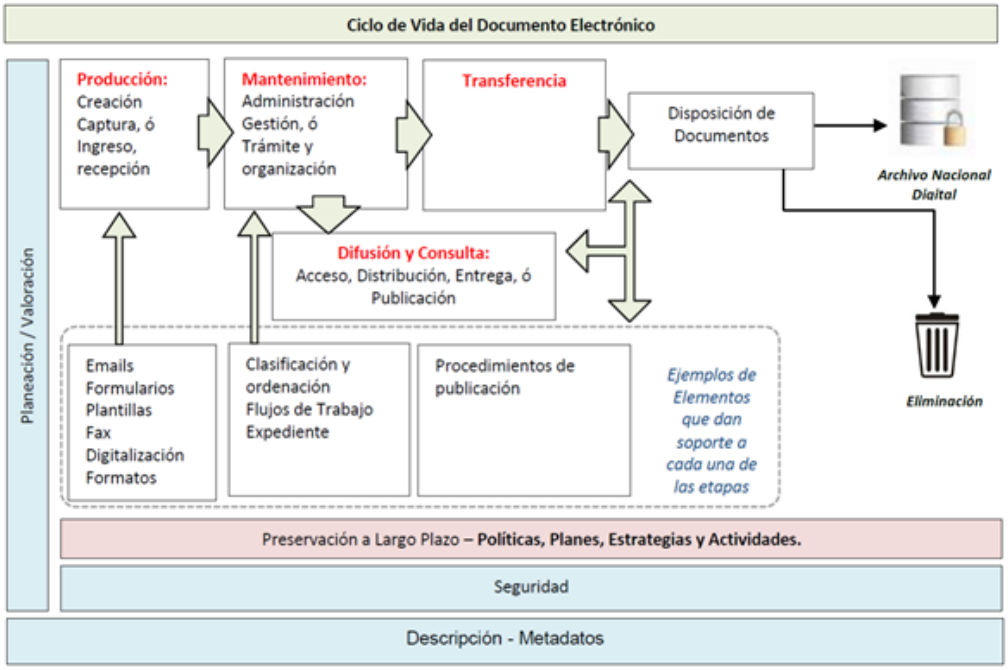


Ilustración 4. Etapas del ciclo de vida del documento electrónico y los procesos. Fuente: Guía para la gestión de documentos y expedientes electrónicos (G.INF.07) MinTIC-AGN.

16.2. EXPEDIENTES ELECTRÓNICOS

Por su parte, la Superintendencia de Notariado y Registro y la Notarías deberán tener en cuenta que los expedientes electrónicos que sean implementados en las herramientas y soluciones tecnológicas, cumplan con los siguientes elementos mínimos:

- Documentos electrónicos de archivo.
- Foliado electrónico.
- Índice electrónico.
- Firma del índice electrónico.
- Metadatos o información virtual contenida en ellos.
- Establecer de conformidad con los lineamientos del AGN y demás normas de archivo aplicables, las tablas de retención documental en la generación de los actos notariales.

Así mismo, el ciclo del expediente electrónico estará determinado por fases, las cuales abarcaran la conformación de los documentos electrónicos de archivo que lo integran, así como su disposición final, para garantizar su preservación.

Ilustración 5. Ciclo vital del expediente electrónico. Fuente: Guía para la gestión de documentos y expedientes electrónicos (G.INF.07) MinTIC-AGN.

Para un adecuado cumplimiento en la gestión de documentos y expedientes electrónicos, debe remitirse a la Guía para la gestión de documentos y expedientes electrónicos[10] elaborada por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones.

16.3. SISTEMAS DE GESTIÓN DE DOCUMENTOS ELECTRÓNICOS DE ARCHIVO

Para la implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo SGDEA se deben tener en cuenta las políticas y lineamientos que ha emitido el Archivo General de la Nación en la Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA)[11]

Para la unificación en el Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) de la entidad, se podrá hacer uso de servicios de integración e interoperabilidad, en el que los documentos creados en los diferentes aplicativos por parte de las notarías conformen el expediente electrónico para facilitar su tratamiento, conservación y acceso. Para este propósito se deberá tener en cuenta el documento técnico denominado: Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos[12]

10 G.INF.07 Guía para la gestión de documentos y expedientes electrónicos, consultar en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/DocumentoOficial_V1GuiaDocumentoYExpedienteElectronico_Nov2017.pdf
11 Guía de Implementación de un Sistema de Gestión de Documentos Electrónicos de Archivo (SGDEA) disponible en: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ImplementacionSGDEA.pdf
12 Modelo de requisitos para la implementación de un sistema de gestión de documentos electrónicos: https://www.archivogeneral.gov.co/sites/default/files/Estructura_Web/5_Consulte/Recursos/Publicacionees/ModeloDeRequisitosSistemaDeGestionElectronicos.pdf

17. PROCEDIMIENTO PARA EVALUACION TÉCNICA Y CRONOGRAMA

17.1. PRESENTACIÓN

Este capítulo muestra los diferentes aspectos que la SNR, evaluará para cada uno de los interesados con miras a las actividades de desarrollo del proyecto de Digitalización Notarial dispuesto por la SNR para las Notarías del país.

El objetivo principal de la prueba es validar y verificar que el interesado, cumple con los requisitos exigidos por las notarías a través del anexo técnico dispuesto por la SNR, en cuanto a términos de funcionalidad, seguridad, desempeño, auditoría, concurrencia, integridad, interoperabilidad, entre otros aspectos, para lo cual es necesario efectuar una evaluación y verificación por etapas, comprobando y documentando los procesos adelantados en la realización de los trámites notariales digitales.

Cada uno de los interesados, deberá proporcionar e implementar la infraestructura tecnológica para llevar a cabo la prueba técnica (hardware, software y plataforma de comunicaciones a nivel local), con los cuales se presente para la evaluación de los ítems requeridos.

La prueba medirá el cumplimiento de los diferentes aspectos exigidos por la SNR en concordancia con los estándares internacionales y normatividad existente y vigentes.

17.2. DESCRIPCIÓN DE LA PRUEBA TÉCNICA

La prueba técnica, establece los procedimientos necesarios para evaluar la plataforma tecnológica presentada por cado uno de los interesados, en términos de funcionalidad, seguridad, desempeño, auditoría, concurrencia, integridad y demás requerimientos expuestos por parte de la SNR.

La operación de los equipos estará a cargo de los funcionarios de la entidad interesada, además todo el hardware y software propios, deberán encontrarse instalados y configurados para iniciar la prueba.

Dentro de las diferentes fases de la prueba, el grupo técnico y funcional de la SNR, documentará cada actividad adelantada dentro de la verificación, para lo cual, se contará la lista de chequeo, mencionada en la sección 17.9, para registrar las diferentes pruebas y tareas adelantadas dentro del proceso.

Con el objeto de posibilitar el acceso a esta información los interesados deberán cumplir:

- Presentación de máximo veinte (20) minutos al grupo designado por parte de la SNR, para la verificación de las pruebas en la cual se muestre una síntesis de la solución propuesta para la prueba técnica y la infraestructura que se implementará en ambiente de producción, de acuerdo a los lineamientos definidos en este documento.

- Con la infraestructura tecnológica para llevar a cabo las pruebas necesarias, tanto a nivel de hardware, software y plataforma de comunicaciones propias de la notaría, La infraestructura tecnológica evaluada, debe corresponder con los ítems requeridos para producción.

- Para la ejecución de las pruebas, la SNR evaluara con los siguientes actos notariales:

    - CELEBRACION DE MATRIMONIO CIVIL
    - TESTAMENTO
    - DILIGENCIA DE AUTENTICACION AUTENTICACIÓN
    - ESCRITURA DE COMPRAVENTA

17.3. ORGANIZACIÓN DE LAS PRUEBAS

La secuencia de las pruebas o fases de aceptación se detallan en este documento a continuación; la organización y ejecución de todas las fases o pruebas estarán a cargo de la SNR, previo requerimiento del notario, así como la verificación de estas.

Las pruebas de aceptación serán organizadas de la siguiente manera:

17.3.1. ALISTAMIENTO

- ✓ Para el desarrollo de la prueba, el notario debe elevar solicitud a la SNR, previa verificación de cumplimiento de requisitos del presente anexo.
- ✓ La SNR fijará fecha y hora para la práctica de la prueba, para lo cual el notario deberá disponer de un dispositivo electrónico con capacidad de establecer comunicación vía internet entre las partes o de forma presencial si a ello hubiere lugar, dependiendo de las condiciones de bioseguridad por la presencia del Coronavirus Covid 19.
- ✓ Se deberá adelantar la debida sincronización de todos los equipos con la hora legal colombiana.
- ✓ Durante la práctica de la prueba, se verificará por parte de la SNR el cumplimiento de los lineamientos descritos en el presente anexo por parte del notario, para la prestación del servicio público a través de medios digitales.

17.4. DESARROLLO DE LA PRUEBA

La prueba se desarrollará de manera presencial en las instalaciones de la notaría y/o de forma remota con presencia del personal de la SNR a cargo de la verificación del cumplimiento de los requisitos del presente anexo en el desarrollo de la prueba, previa fijación de fecha y hora conforme requerimiento de la notaría, que deberá ser enviado al mail: proyectodigitalnotarial@supernotariado.gov.co una vez considere que está lista para acreditar el cumplimiento de los lineamientos del presente anexo.

El tiempo estimado para el desarrollo de la prueba será de mínimo (4) horas.

17.5. CALIFICACIÓN CUALITATIVA DE LA PRUEBA

Para la Evaluación Cualitativa de la solución propuesta y de las pruebas a ejecutarse, serán empleados los siguientes términos:

CUMPLE: La solución presentada cumple con los requerimientos.
NO CUMPLE: La solución propuesta no cumple con requerimientos.

17.6. OBSERVACIONES A LA CALIFICACION

Se harán las observaciones técnicas y jurídicas al desarrollo tecnológico presentado, si es el caso, las cuales deberán acreditarse previo a la autorización que deba expedir la SNR.

17.7. COMUNICACIÓN DE LOS RESULTADOS

El resultado de la Evaluación será comunicado por parte de la SNR, al interesado en un término de quince (15) días hábiles después de ejecutada la prueba técnica.

17.8. ACTA DE EJECUCIÓN PRUEBA TÉCNICA

LUGAR: _____	FECHA: _____
ENTIDAD SOLICITANTE:	
REPRESENTANTE DE LA ENTIDAD SOLICITANTE:	
REPRESENTANTE ALIADO TECNOLOGICO:	
ALIADO TECNOLOGICO QUE PRESENTA LA PRUEBA:	
FUNCIONARIOS SNR:	

OBSERVACIONES:

17.9. LISTA DE CHEQUEO EN LA EJECUCION DE PRUEBAS

LISTA DE CHEQUEO	Cumple	No Cumple	Observación
Verificar que la solución tecnológica de la notaría cuente con LOG de auditoria.			
Verificar que la solución tecnológica de la notaría se encuentre en ambiente web y móvil.			
Verificar que la solución tecnológica de la notaría presente la descripción de los trámites y requisitos para su realización, pasos a seguir, la tarifa por trámite y los medios de pago electrónicos.			
Verificar que la solución tecnológica de la notaría establezca un Código Único Acto Notarial Digital (CUANDI) para cada acto electrónico que se realice.			
Si se utiliza el recurso de video llamada como medio de verificación en la rogación de un trámite notarial, su grabación y descarga. Se verificará el cumplimiento del numeral 9 del capítulo 5. Lineamientos Generales.			
Verificar que la solución tecnológica de la notaría permita el uso de medios electrónicos para el pago de los derechos notariales.			
Verificar que la solución tecnológica de la notaría permita que el usuario notarial envíe y cargue a la notaria los documentos necesarios para la ejecución del trámite notarial.			
Verificar que la solución tecnológica de la notaría permita la Interoperabilidad con el repositorio de la SNR a través de X-ROAD.			

Verificar que la solución tecnológica de la notaría permita el acceso al repositorio notarial dispuesto por la SNR para el protocolo notarial.			
Verificar que la solución tecnológica de la notaría permita el enrolamiento del Usuario del Servicio Digital Notarial, verificando la información contra el ANI de la RNEC.			
Verificar que la solución tecnológica de la notaría permita en la autenticación de usuarios la verificación mediante el uso de doble factor.			
Verificar que la solución tecnológica de la notaría permita en el enrolamiento el cargue de la información mínima requerida de obligatorio cumplimiento. Se verificará el cumplimiento del numeral 3 del capítulo 9.1.1.Registro - Enrolamiento.			
Verificar que la solución tecnológica de la notaría permita en el enrolamiento el cargue de la información del departamento y municipio de domicilio según la DIVIPOLA diseñada por DANE. Se verificará el cumplimiento del numeral 3 del capítulo 9.1.1.Registro - Enrolamiento.			
Verificar que la solución tecnológica de la notaría permita en el enrolamiento la verificación del número del celular mediante mensaje de texto o llamada para confirmación.			
Verificar que la solución tecnológica de la notaría permita en el enrolamiento la verificación del correo electrónico mediante mensaje de correo para confirmación.			
Verificar que la solución tecnológica de la notaría permita en el enrolamiento el almacenamiento de la fecha de registro del usuario y de la fecha de actualización del registro del usuario.			
Verificar que la solución tecnológica de la notaría permita la creación y almacenamiento de contraseñas seguras y el doble factor.			
Verificar que la solución tecnológica de la notaría permita durante el procedimiento de registro del usuario la aceptación expresa de los términos y condiciones de uso y operación del servicio, la cual debe quedar almacenada para su posterior consulta.			
Verificar que la solución tecnológica de la notaría permita que en el procedimiento de registro se le solicite al usuario la aceptación expresa del tratamiento de datos y habeas.			
Verificar que la solución tecnológica de la notaría permita insertar en logs los intentos de identificación con mínimo los siguientes campos: tipo de documento, número de documento, fecha y hora identificación, id método identificación, calidad datos biométricos, resultado identificación.			

Verificar que la solución tecnológica de la notaría permita la aceptación de términos y condiciones y la de tratamiento de datos personales, que debe ser firmada electrónicamente, junto con una estampa cronológica y número único de transacción.			
Verificar que la solución tecnológica de la notaría de cumplimiento al capítulo 9.3 Verificación del Documento de Identificación.			
Verificar que la solución tecnológica de la notaría permita la autenticación biométrica permitiendo la identificación del usuario del acto digital notarial. Se verificará el cumplimiento del capítulo 9.5. Autenticación Biométrica.			
Verificar que la solución tecnológica de la notaría permita el uso de la Firma Electrónica por parte de Usuario del Servicio Digital Notarial.			
Verificar que la solución tecnológica de la notaría permita el uso de la Firma Digital por Parte del Notario.			
Verificar que la solución tecnológica de la notaría permita la Validación de la Geolocalización del notario al otorgamiento del acto notarial.			
Verificar que la solución tecnológica de la notaría permita la Validación de la Geolocalización del usuario al otorgamiento del acto notarial.			
Verificar que la solución tecnológica de la notaría permita la Validación de la Geolocalización del circulo notarial.			
Verificar que la solución tecnológica de la notaría permita que los distintos usuarios solo tengan acceso a la información y funcionalidades acordes a su rol y llevar un registro de auditoría donde se pueda establecer la trazabilidad de las funcionalidades utilizadas en cada sesión de trabajo y sus modificaciones. Se realizará la prueba según la definición de perfiles establecida por la notaria.			
Verificar que la solución tecnológica de la notaría permita el uso Sello Digital Notarial.			
Verificar que la solución tecnológica de la notaría utilice Estampado cronológico en la generación de documentos electrónicos.			
Verificar la existencia de la certificación de la actividad de Ethical Hacking realizada sobre la solución tecnológica de la notaria.			
Verificar la existencia del informe de pruebas de carga y estrés realizada sobre la solución tecnológica de la notaria.			
Verificar que la solución tecnológica de la notaría permita la custodia del testamento cerrado de forma digital.			

Verificar que la solución tecnológica de la notaría en el caso de generar comunicaciones o notificaciones electrónicas guarde la trazabilidad de las mismas, mediante la prueba de envío y entrega, y el sello de hora oficial.			
Verificar que la solución tecnológica de la notaría acredita el cumplimiento de los requerimientos establecidos por la RNEC, demostrando que cuenta con el respaldo de un operador biométrico homologado.			
Preguntar al notario sobre el cumplimiento de las políticas y lineamientos técnicos dictados conjuntamente por el Archivo General de la Nación y el Ministerio de Tecnologías de la Información y las Comunicaciones en la gestión de documentos y expedientes electrónicos en la solución tecnológica de la notaría implementada.	NA	NA	Si ___ No ___
Verificar que la solución tecnológica de la notaría en el documento generado del trámite notarial digital, contenga como Los siguientes parámetros digitales: • Código CUANDI • Firma digital por parte del notario • Sello electrónico (Imagen que corresponde al sello físico del notario) • Código QR • Firma electrónica usuario • Mecanismo opcional de identificación del operador			
Verificar que la solución tecnológica de la notaría cuente con un módulo para el agendamiento de citas virtuales.			

Nota aclaratoria:

INTEROPERABILIDAD X-ROAD:

En una primera fase se realizará la verificación de que la solución tecnológica de las notarías tenga Interoperabilidad con el repositorio de la SNR a través de X-ROAD,

La solución tecnológica de las Notarias en una segunda fase, deben permitir la interoperabilidad a través de X-ROAD con los demás actores requeridos en los tramites notariales.

INTEGRACIÓN CON CARPETA CIUDADANA:

Una vez la Agencia Nacional Digital – AND habilite el servicio de carpeta ciudadana, las notarías deberán hacer uso de ella; por lo tanto, la SNR realizará la verificación de dicho cumplimiento.

17.10. CRONOGRAMA

A continuación, se relacionan las fechas establecidas para el presente proyecto:

DICIEMBRE 2020

LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
	1	2	3	4	5	6
7	8	9	10	11	12	13
14	15	16	17	18	19	20
21	22	23 SNR Publicación Actos Administrativos Para comentarios	24	25	26	27
28 SNR Finalización publicación Actos Administrativos	29	30	31			

ENERO 2021

LUNES	MARTES	MIERCOLES	JUEVES	VIERNES	SABADO	DOMINGO
				1 SNR Inicio de tramites para publicación de Actos, Anexos definitivos e invitación a Pruebas Piloto (*)	2	3
4	5	6	7	8	9	10
11	12	13	14	15	16	17
18	19	20	21	22	23	24
25	26	27	28	29	30	31

(*) FASE 1 – NOTARÍAS DE 1ª CATEGORIA
(*) FASE 2 – NOTARÍAS DE 2ª CATEGORIA (Se establecerá en el 1er trimestre de 2021)