ESCUELA POLITÉCNICA NACIONAL

FACULTAD DE INGENIERÍA ELÉCTRICA Y ELECTRÓNICA

ANÁLISIS, DISEÑO E IMPLEMENTACIÓN DE UN PROTOTIPO DE NOTARÍAS DIGITALES

PROYECTO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE INFORMACIÓN

AGUIRRE PONCE ARSENIO ANTONIO
a_aguirre117@hotmail.com

CARCHI ALVEAR PABLO RODRIGO
myself_pc_zizou@yahoo.com

DIRECTOR: PhD ENRIQUE MAFLA
mafla@epn.edu.ec

Quito, junio de 2011

DECLARACIÓN

Nosotros, Arsenio Antonio Aguirre Ponce y Pablo Rodrigo Carchi Alvear, declaramos bajo juramento que el trabajo aquí descrito es de nuestra autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que hemos consultado las referencias bibliográficas que se incluyen en este documento.

A través de la presente declaración cedemos nuestros derechos de propiedad intelectual correspondientes a este trabajo, a la Escuela Politécnica Nacional, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____ _____

Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear

CERTIFICACIÓN

Certifico que el presente trabajo fue desarrollado por Aguirre Ponce Arsenio Antonio y Carchi Alvear Pablo Rodrigo, bajo mi supervisión.

_____

PhD Enrique Mafla

Director del Proyecto

AGRADECIMIENTO

Agradecemos a todas las personas que aportaron al desarrollo de este proyecto de titulación, pero en particular a las mencionadas a continuación.

Agradecimiento especial al PhD Enrique Mafla, quien con sus conocimientos y experiencia supo trazarnos el camino y darnos las pautas necesarias para el desarrollo de este proyecto de titulación.

A los funcionarios de la Notaría Octava del Cantón Quito, Dr. Jaime Espinoza y Ab. Cecilia Vargas, quienes con toda amabilidad nos ofrecieron su asesoría referente al proceso notarial.

Al personal del Directorio de la Entidad de Certificación de Información del Banco Central del Ecuador, los cuales nos impulsaron en el campo de la firma electrónica en el Ecuador.

Al grupo de desarrolladores de la Subsecretaría de Informática, quienes nos ayudaron con su Sistema de Gestión Documental Quipux, en especial al Ing. Mauricio Haro.

A David Loor, estudiante de la Facultad de Ingeniería en Sistemas, impulsador del software libre, quien aportó en la ejecución de este proyecto, muchas gracias por su apoyo y solidaridad.

Mil disculpas a quienes no hemos mencionado, pero por su valiosa ayuda les quedamos eternamente agradecidos.

Finalmente, lo más importante: agradecer profundamente a nuestras familias por su eterno apoyo, comprensión y amor.

_____ _____

Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear

DEDICATORIA

Dedico este proyecto de titulación primeramente a Dios, por haberme permitido llegar hasta este punto importante en mi vida y haberme dado buena salud para lograr este objetivo, acompañado de paz espiritual para hacer y pensar bien las cosas en los momentos difíciles.

A mis mamás Betty y Antonia por el amor que siempre me dan durante toda su vida, y ser las personas más maravillosas del mundo. Les dedico a ellas por el apoyo que me brindan en todos los momentos de mi vida para salir adelante y por transmitirse consejos, principios y valores que me han llevado a ser una persona de bien.

A mis tíos Juan y Adolfo y sus familias que me brindan lo mejor de ellos desde el primer día que comenzó este largo camino para ser un buen profesional, por confiar en mí y darme la oportunidad de no defraudarlos.

A toda mi familia que siempre me han demostrado todo su afecto a lo largo de mi vida porque este triunfo no es solo mío sino también de todos ustedes.

_____

Arsenio Antonio Aguirre Ponce

DEDICATORIA

Le dedico este trabajo al Padre Todopoderoso, como una simple respuesta a las pruebas que me presenta y por regalarme la dicha de despertar cada día y admirar su maravillosa creación. Por todas las lecciones que me ha presentado, proponerme ser feliz todos los días y prometerme una vida eterna de gracia a su lado.

A mis papis por inculcarme valores de responsabilidad, lealtad, solidaridad y estar en los momentos más difíciles y felices de mi vida. Se los dedico este trabajo para demostrarles el profesional que con amor, esfuerzo y paciencia han formado.

Dedicado a mis hermanos por ser mi compañía y valor a diario. A Danny por ser mi ejemplo y confiar en mis aptitudes y cualidades. Y Gabriel por ofrecerme su cariño y demostrarme la verdadera inteligencia, oculta para humanos pero perfecta para Dios.

Este proyecto no me habría sido posible hacerlo sin la ayuda de mi tío Manuel. Le dedico este trabajo por su aporte y apertura conmigo. También quiero dedicárselo a toda mi familia, porque siempre han creído en mi inteligencia y habilidades.

Dedico este trabajo a mis amigos, a quienes me acompañaron en la dura travesía de la EPN. Dedicado para quienes creyeron en mi desde el colegio y a quienes siempre apreciaré. A los nuevos amigos, que aún con sus errores, los recordaré por su agradable personalidad. A quienes valoran mis capacidades e incluso a quienes juzgan mis debilidades. Les dedico un trabajo bien realizado, una propuesta innovadora que demuestra que el verdadero ingenio está en la mente más humilde.

Finalmente quiero dedicar este trabajo a mi nenita porque ha sido mi mayor soporte en este tramo de mi vida. Sin su cariño, tiempo y compañía, este trabajo no tendría el mismo sentido que alcanzó. Soy dichoso de ser el ejemplo para la persona más valiosa en el mundo.

_____

Pablo Rodrigo Carchi Alvear

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Este proyecto de titulación propone la implementación de un prototipo de sistema distribuido para Notarías Digitales. El proyecto analiza los requerimientos de la Notaría. Posteriormente se diseña la infraestructura de hardware y software para la Notaría Digital. Finalmente se procede con la implementación del prototipo de Notaría Digital.

La documentación del proyecto de titulación se encuentra dividida en cinco capítulos. En el primer capítulo se describen temas relacionados a la definición del problema y el propósito que tiene una Notaría Digital según el presente proyecto de titulación. Se plantea una alternativa con base en los objetivos y los alcances que propone el proyecto de titulación. Además se realiza un análisis al marco legal que ampara la creación de Notarías Digitales en el Ecuador. Al finalizar este capítulo se describen las herramientas tecnológicas que aportan con un alto nivel de seguridad al funcionamiento de Notarías Digitales a través de Internet.

En el segundo capítulo se analiza la situación actual y de requerimientos de seguridad a los trámites y de gestión documental de la Notaría. Se detallan los usuarios que participan en los trámites notariales, sus funciones y obligaciones, así como los permisos para acceder al archivo. Luego, los flujos de trabajo que requieren los trámites notariales se describen mediante diagramas UML. Los mecanismos de seguridad que practica el Notario para brindar confianza al trámite notarial se consideran en este capítulo. Se finaliza con el análisis de requerimientos de gestión documental que se aplican al archivo.

En el tercer capítulo se diseña la Notaría Digital. Se inicia con el estudio de Gestión de Identidades sobre la base de la Infraestructura de la Entidad de Certificación de Información del Banco Central del Ecuador. Los trámites notariales digitales se diseñan mediante casos de uso sobre la base del levantamiento de los requerimientos del segundo capítulo. Se diseña el Sistema de Gestión Documental que cumpla con los requerimientos de seguridad del archivo digital y las opciones

que lo deberán componer para el almacenamiento de los trámites notariales digitales. Finalmente se diseña la infraestructura de la red de datos de la Notaría Digital mediante las recomendaciones de la Arquitectura SAFE de CISCO.

En el cuarto capítulo se describe la implementación del prototipo de Notaría Digital. El objetivo de este capítulo es implementar un prototipo que se aproxime al diseño de la Notaría Digital desarrollado en el capítulo 3. Este capítulo inicia con la configuración de los servidores del prototipo de Notaría Digital: Sistema de Gestión Documental, DNS y Firewall. Se define la parametrización inicial del Sistema de Gestión Documental sobre el cual se realizarán los trámites notariales digitales. A continuación se define la gestión de certificados de firma electrónica para el prototipo de Notaría Digital. La configuración de la red de datos del prototipo de Notaría Digital se incluye en este capítulo. Por último se realizan las pruebas del prototipo de Notaría Digital con los requerimientos para cada trámite notarial digital y los resultados respectivos. Las pruebas incluyen el análisis de resultados obtenidos.

En el último capítulo se desarrollan las conclusiones y recomendaciones derivadas de la realización del presente proyecto de titulación.

PRESENTACIÓN

El principal objetivo de este proyecto de titulación es analizar, diseñar e implementar un prototipo de sistema distribuido seguro para automatizar los trámites notariales acorde a las leyes vigentes. Se propone una alternativa a la realización de cinco trámites notariales a través de Internet.

El proyecto de Notarías Digitales propone adoptar herramientas tecnológicas para realizar los trámites notariales con base en los principios de la seguridad: autenticidad, confidencialidad, integridad y disponibilidad. El presente proyecto de titulación aprovecha que la normativa en el Ecuador no restringe el uso de nuevas tecnologías para la implementación de Notarías Digitales.

El problema que plantea resolver el proyecto de Notarías Digitales no apunta a alterar el fondo de cómo se realizan los trámites notariales convencionales, sino más bien aportar con las herramientas informáticas seguras para cambiar la forma en que éstos se realizan. Los trámites notariales convencionales manejados de manera presencial y física se plantea realizarlos de forma digital y distribuida.

El Ecuador cuenta con una Entidad de Certificación de Información que actúa como autoridad de confianza entre los participantes de un contrato electrónico. Una de sus aplicaciones potenciales es el uso en Notarías Digitales. El uso de los certificados de firma electrónica emitidos por la Entidad de Certificación de Información garantiza la autenticidad de los participantes en los trámites notariales digitales.

El proyecto de titulación propuesto cumple una metodología sistemática para detallar el procedimiento que se siguió para elaborar la investigación. Esta metodología brinda al lector una mejor comprensión del documento y para este proyecto de titulación se encuentra divida en tres fases. La primera fase consta del análisis de la situación actual y de los requerimientos de la Notaría. Esta primera fase fue realizada con base en entrevistas a usuarios de la Notaría Octava del cantón Quito. En la segunda fase se realizará el diseño de la infraestructura tecnológica. Por último se implementará el prototipo de Notaría Digital al cual se le realizarán pruebas.

CAPÍTULO 1

NOTARÍAS DIGITALES

El presente proyecto tiene como meta implementar un prototipo de sistema distribuido para Notarías Digitales mediante la aplicación de herramientas informáticas seguras. Los trámites notariales digitales cumplen con los parámetros de seguridad para brindar un servicio confiable a través de Internet. La aplicación de certificados de firma electrónica y marcas de tiempo, el diseño de una infraestructura física y lógica segura y el uso de un sistema de gestión documental son herramientas que permiten la implementación de Notarías Digitales en el país.

La definición del problema se plantea en el subcapítulo 1.1 con base en los objetivos y alcances que propone el proyecto de titulación. Además se plantea una definición de Notarías Digitales para este proyecto de titulación en el subcapítulo 1.1.1. El análisis legal que ampara la creación de Notarías Digitales en el Ecuador se realiza en el subcapítulo 1.2. Las herramientas tecnológicas que aportan con un alto nivel de seguridad al funcionamiento de las Notarías Digitales a través de Internet se mencionan en el subcapítulo 1.3.

1.1 DEFINICIÓN DEL PROBLEMA

La normativa en el Ecuador permite la implementación de Notarías Digitales. Sin embargo no ha habido una apertura o un interés por incursionar en este ámbito. Por esta razón el presente proyecto de titulación propone adoptar herramientas tecnológicas seguras para automatizar los trámites notariales regidos siempre por el marco legal.

El Ecuador cuenta con una Entidad de Certificación de Información que actúa como una autoridad de confianza entre los participantes de un contrato electrónico. Una de

sus aplicaciones potenciales es el uso en Notarías Digitales.[1] El uso de los certificados de firma electrónica emitidos por la Entidad de Certificación de Información garantiza la autenticidad de los participantes en los trámites notariales digitales. La firma electrónica además asegura la autenticidad e integridad del documento electrónico que utilizan los participantes.

1.1.1 DEFINICIÓN DE NOTARÍAS DIGITALES

El proyecto de titulación de Notarías Digitales brinda una alternativa a los trámites notariales convencionales. Los trámites notariales manejados de manera presencial y física se plantea realizarlos de forma digital y distribuida. El problema que plantea resolver el proyecto de Notarías Digitales no apunta a alterar el fondo de cómo se realizan los trámites notariales, sino más bien aportar con las herramientas informáticas para cambiar la forma en que éstos se realizan y llevar los mismos al mundo digital a través de Internet. La Ley Notarial, a la cual se rigen las Notarías en el Ecuador, será respetada por este proyecto de titulación.

El documento digital representa, para este proyecto de titulación, un archivo electrónico en lugar de un documento físico que ha sido digitalizado. Los trámites notariales digitales usarán este tipo de documentos de naturaleza electrónica. Las firmas digitales a utilizarse no se tratan de firmas digitalizadas sino de certificados de firma electrónica. Los documentos digitales y certificados de firmas electrónicas tienen todo el sustento legal, como lo señala la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos analizada en el subcapítulo 1.2.2.

1.1.2 OBJETIVOS

El principal objetivo de este proyecto de titulación es analizar, diseñar e implementar un prototipo de sistema distribuido seguro para automatizar los trámites notariales acorde a las leyes vigentes. Se propone una alternativa a la realización de trámites notariales a través de Internet, con los requerimientos que presente cada uno. El diseño de la Notaría Digital garantizará a los participantes del acto notarial la

[1] "Firma Electrónica en el Ecuador y su beneficio en la gestión comercial de las empresas", página 25.

confidencialidad e integridad del acto, la autenticidad de los involucrados en los trámites notariales y la validez jurídica de la Escritura Pública o Diligencia obtenida.

Para complementar el objetivo general se plantean los siguientes objetivos específicos:

- Analizar la normativa vigente en el Ecuador relacionada a la implementación de servicios notariales digitales.
- Desarrollar un sistema distribuido seguro en ambiente Web que implante cinco trámites notariales digitales.
- Aplicar certificados de firma electrónica y el servicio de marcas de tiempo para garantizar la autenticidad de los servicios notariales.
- Usar un Sistema de Gestión Documental para archivar los documentos digitales emitidos por la Notaría.

1.1.3 ALCANCE

El proyecto de titulación analiza la normativa en el Ecuador para sustentar la legalidad que permite implantar Notarías Digitales. Este proyecto incluye el análisis de las siguientes leyes: Ley Notarial, Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y, Ley del Sistema Nacional de Registro de Datos Públicos. Estas leyes constan en el Registro Oficial a la fecha de la redacción de este documento de proyecto de titulación.

El análisis, diseño e implementación de la aplicación distribuida segura se enfocará sobre cinco trámites notariales. Los trámites notariales fueron escogidos con base en recomendaciones de la Notaría Octava del Cantón Quito[2] enfocándose en el objetivo de trasladar el funcionamiento notarial al mundo digital. El Notario Dr. Jaime Espinoza facilitó a los autores de este proyecto de titulación la información de los

[2] Av. Amazonas 239 y Jorge Washington. Edificio Álvarez Burbano. Primer Piso Of.110

trámites notariales. El protocolo descrito para cada uno de estos trámites es el utilizado en esta Notaría.

El Notario y los usuarios harán uso de certificados de firma electrónica y marcas de tiempo. El diseño propone el uso de certificados de firma electrónica emitidos por la ECIBCE[3] porque es la única entidad pública acreditada por el CONATEL[4]. La Ley de Comercio Electrónico, firmas electrónicas y mensajes de datos acreditó al CONATEL como Organismo de Regulación y Control de las Entidades de Certificación. Además en este proyecto de titulación se sugiere la implementación de una Autoridad de marcas de tiempo en el Ecuador que asegure la fidelidad de una hora digital única en los trámites notariales digitales. Los mecanismos que aseguren una hora digital única dependerán de la infraestructura que implemente la Autoridad de Marcas de Tiempo acreditada en el Ecuador. Sin embargo, el prototipo utiliza certificados de firma electrónica de prueba que serán emitidas por una autoridad de certificación creada localmente. El diseño del proyecto incluye la manera en que intervienen las marcas de tiempo emitidas por una autoridad acreditada en el desarrollo de los trámites notariales digitales. El prototipo de Notaría Digital no utilizará el servicio de marcas de tiempo debido a que no existe una Autoridad de Marcas de Tiempo en el Ecuador.

El funcionamiento de los trámites notariales digitales ofrecidos por el prototipo de Notaría Digital será probado en un segmento de red. Los clientes accederán al servicio y del otro lado de la aplicación los usuarios de la Notaría actuarán de acuerdo al protocolo de los trámites notariales digitales. Los documentos digitales serán del tipo PDF y se firmarán electrónicamente mediante la herramienta JSignPdf. El prototipo no será accesible a través de Internet pero en este documento se especifican los requerimientos para que el diseño de Notaría Digital sea aplicable.

Se considera fuera del alcance de este proyecto de titulación la facturación electrónica para Notarías Digitales. El diseño de la Notaría Digital no solicitará el

[3] ECIBCE.- Entidad de Certificación de Información del Banco Central del Ecuador.
[4] CONATEL.- Consejo Nacional de Telecomunicaciones

pago que requieren los trámites notariales. El proyecto se limita a cumplir el protocolo notarial sin tomar en cuenta el costo que implica el mismo.

Las Políticas de Seguridad Informática para las Notarías Digitales no serán desarrolladas en este documento. El objetivo de este proyecto de titulación apunta a ofrecer una alternativa a la realización de trámites notariales más no a definir reglas de comportamiento del usuario final frente a la Notaría Digital. Sin embargo las Notarías Digitales pueden gestionar las Políticas de Seguridad Informática con base en la norma ISO/IEC 27001[5] y las Políticas establecidas por la ECIBCE para el uso de los certificados de firma electrónica.

1.2 ANÁLISIS LEGAL

En este subcapítulo se cubren los aspectos legales sobre los cuales debe enmarcarse el proyecto de titulación de Notaría Digital. En primer lugar se menciona la Ley Notarial donde se detallan los requisitos que debe cumplir la Notaría Digital para que su funcionamiento se considere válido bajo el ámbito jurídico. Posteriormente la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos describe el aporte y legalidad que brinda a la existencia y manejo de Firmas Electrónicas. Finalmente se procede con el análisis de la Ley del Sistema Nacional de Registro de Datos Públicos, que aporta a validar la información de los Clientes en los trámites requeridos por la Notaría Digital para su funcionamiento.

1.2.1 LEY NOTARIAL[6]

La Ley Notarial no considera la prohibición al uso de nuevas tecnologías como menciona el Artículo 2. El presente proyecto plantea una alternativa al funcionamiento de la Notaría sin alterar el marco legal, es decir, la Notaría mantiene las mismas funciones pero haciendo uso de la tecnología. El Notario conserva las

[5] ISO/IEC 27001.- Sistema de Gestión de Seguridad de la Información (Fuente: http://www.iso27000.es/iso27000.html)

[6] Ley Notarial del Ecuador. Decreto Supremo 1404, Registro Oficial 158, 11 de Noviembre de 1966.

mismas atribuciones, deberes y prohibiciones que se mencionan en los Artículos 18, 19 y 20 de la Ley Notarial respectivamente.

La Ley Notarial establece en el Título II: De los documentos notariales, la manera de administrar y organizar la documentación que se genera en los trámites notariales. El archivo notarial requiere mecanismos de almacenamiento y seguridad para ofrecer acceso y distribución confiable. La Ley Notarial también menciona en el Capítulo II del Título II: De las Escrituras Públicas, la manera de generar documentos que sean jurídicamente legales. La redacción de documentos notariales legales no será abarcada por este proyecto de titulación.

Mediante el análisis realizado a la Ley Notarial se determina que no existe prohibición para la implementación de Notarías Digitales en el Ecuador a través del uso de nuevas tecnologías y brindar accesibilidad al servicio notarial de una manera distribuida.

1.2.2 LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS[7]

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos garantiza en sus Artículos 2 y 3 la validez jurídica para el uso de los mensajes de datos, entre ellos, correo electrónico, mensajes de texto o documentos electrónicos. Para el caso de Notarías se tiene el mismo amparo legal para documentos digitales que para físicos. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos además atribuye validez a la firma electrónica sobre documentos digitales al mismo nivel que la firma manuscrita en los documentos físicos de acuerdo al Artículo 14.

La firma electrónica identifica al titular o propietario de la misma, registrado ante una Entidad de Certificación de Información según el Artículo 13. Se la puede implementar, entre otros, en mensajes de datos, en correos electrónicos o en documentos digitales. Como consecuencia de la firma electrónica se asegura la autenticidad e integridad del documento digital de acuerdo al Artículo 21.

[7] Ley No. 2002-67, publicada en el Registro Oficial Suplemento No. 577 del 17 de abril del 2002.

Según el literal b del Artículo 15, los documentos digitales firmados electrónicamente admiten mecanismos para verificar su validez, con el fin de evitar falsificaciones, el no repudio y ofrecer auditoría al documento. La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos establece sanciones para el uso irresponsable de la firma electrónica, la adulteración de información y distribución no autorizada de documentación electrónica de acuerdo al Título V: De las Infracciones Informáticas.

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos permite el uso de documentos digitales firmados electrónicamente con el mismo valor jurídico que los documentos físicos. Por lo tanto, no existe inconveniente en la implementación de Notarías Digitales en el Ecuador, debido a la legalidad que se consigue al utilizar documentación digital y firmas electrónicas.

1.2.3 LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS[8]

La Ley del Sistema Nacional de Registro de Datos Públicos garantiza el acceso y transparencia de la información completa de las personas naturales o jurídicas de acuerdo a su Capítulo I: Finalidad, Objeto y Ámbito de Aplicación. Esta información puede ser usada por instituciones del sector público o privado con el objeto de coordinar el intercambio de información. Por ende, las Notarías están aptas para el uso del Sistema Nacional de Registro de Datos Públicos y acceder a información confiable.

La Ley del Sistema Nacional de Registro de Datos Públicos, en su Artículo 13: De los Registros de Datos Públicos, clasifica como datos públicos a la información que hace referencia a: el Registro Civil, de la Propiedad, Mercantil, Societario, Vehicular, de naves y aeronaves, patentes y de propiedad intelectual. Estos datos serán de utilidad para la verificación de la información de los usuarios al momento de realizar trámites en la Notaría Digital.

El Sistema Nacional de Registro de Datos Públicos garantizará la confidencialidad e integridad de la información, según el Artículo 4: Responsabilidad de la Información.

[8] Ley Publicada en el Registro Oficial No. 162 del 31 de Marzo de 2010.

La Ley del Sistema Nacional de Registro de Datos Públicos aporta al funcionamiento de Notarías Digitales al proveer información completa, confiable y segura que servirá como sustento para que el Notario pueda dar fe de los datos que se le presenten en el acto.

1.3 HERRAMIENTAS TECNOLÓGICAS SEGURAS

Las herramientas tecnológicas que utilizará el proyecto de Notarías Digitales serán a través de hardware, software o conjunto de ellas. La finalidad es asegurar el trámite notarial distribuido y resguardar la documentación que almacena la Notaría Digital contra cualquier incidente que amenace la confidencialidad, integridad, disponibilidad de la información y permita autenticar a los participantes en el acto notarial.

Las herramientas tecnológicas seguras usadas para el proyecto de Notarías Digitales serán: certificados de firma electrónica y una arquitectura que permita asegurar la información dentro de la red de datos de la Notaría Digital. La herramienta tecnológica para diseñar la red de datos de la Notaría Digital es la arquitectura SAFE de CISCO. Esta arquitectura se caracteriza por su fácil comprensión y aplicación en pequeñas, medianas y grandes empresas. En los subcapítulos 1.3.1 y 1.3.2 se mencionan los certificados de firma electrónica y la arquitectura SAFE de CISCO respectivamente.

1.3.1 CERTIFICADO DE FIRMA ELECTRÓNICA

La Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos define en su Artículo 20 al Certificado de Firma Electrónica como “el mensaje de datos que certifica la vinculación de una firma electrónica con una persona determinada, a través de un proceso de comprobación que confirma su identidad” en el mundo electrónico.

El Banco Central del Ecuador según Resolución del CONATEL N° 481-20-2008 del 8 de octubre de 2008, se acreditó como Entidad de Certificación de Información. A

través de su infraestructura tecnológica de PKI[9] emite certificados de firma electrónica para cualquier ciudadano y se almacena en un dispositivo denominado Token[10], es portable, fácil de usar y brinda el más alto nivel de seguridad.[11]

El certificado de firma electrónica es un documento digital mediante el cual un tercero confiable, que actúa como autoridad de certificación, garantiza la vinculación entre la identidad de un sujeto y su clave pública.

1.3.2 ARQUITECTURA SAFE [12]

SAFE es una arquitectura recomendada por CISCO, que proporciona información acerca de las mejores prácticas para el diseño e implementación de redes de datos seguras. SAFE propone un enfoque de defensa hacia los datos más valiosos de la institución. En el caso de Notarías Digitales, la información crítica es la documentación generada por los trámites notariales digitales que se almacena en el Sistema de Gestión Documental.

SAFE establece una estructura modular, con el objetivo de facilitar su implementación acorde a las necesidades, las amenazas esperadas y los mecanismos para combatirlas. El enfoque modular facilita al diseñador ajustar las recomendaciones de seguridad a su entorno. Se recomienda la implementación módulo a módulo en lugar de todo el esquema en una sola fase. La arquitectura permite el diseño de una infraestructura de datos segura que prevé riesgos y brinda protección ante fallos físicos y ataques lógicos.

El proyecto de Notarías Digitales en el Ecuador requiere utilizar la arquitectura SAFE para ofrecer una infraestructura de red de datos confiable, de alta disponibilidad, resistente a fallas y de implementación modular acorde a las necesidades de protección sobre los recursos notariales críticos.

---

[9] PKI (*Public Key Infraestructure*).- Infraestructura de Llave Pública es el ambiente de administración de información de llave pública en un sistema criptográfico. Una Autoridad de Certificación (CA) tiene la finalidad de ofrecer confianza al usuario mediante una PKI. (Fuente: http://csrc.nist.gov)

[10] Token.- Elemento físico donde se almacena en forma segura el certificado de firma electrónica que será emitido por la ECIBCE. (Fuente: Declaración de Prácticas de Certificación de la ECIBCE)

[11] Documento “Certificados de Firma Electrónica" de la ECIBCE, página 2.

[12] Cisco SAFE: A Security Blueprint for Enterprise Networks.

CAPÍTULO 2

ANÁLISIS DE LA SITUACIÓN ACTUAL Y DE REQUERIMIENTOS

En el presente capítulo se analiza la situación actual y de requerimientos de la Notaría en el Ecuador. El análisis de la situación actual se realiza en el subcapítulo 2.1 con base en los actores que intervienen en la Notaría y al protocolo que se usa para efectuar los trámites notariales. El análisis de requerimientos de la Notaría se menciona en el subcapítulo 2.2. Los requerimientos de seguridad para garantizar autenticidad, no repudio, confidencialidad, integridad y disponibilidad de los trámites notariales se analizan en el subcapítulo 2.2.1. Los requerimientos de gestión documental que realiza la Notaría se analizan en el subcapítulo 2.2.2. El análisis del archivo notarial considera los parámetros de control de acceso, organización, almacenamiento, distribución y seguridad del archivo.

Los requerimientos presentados en este documento fueron estudiados en la Notaría Octava del Cantón Quito. El plan de trabajo se definió con base en entrevistas con el Dr. Jaime Espinoza Cabrera y la Ab. Cecilia Vargas que tienen los cargos de Notario y Verificador respectivamente. La información solicitada se centró en conocer la forma en que se realizan los trámites notariales y la organización que tiene el archivo. Las entrevistas incluyeron una revisión para certificar el protocolo de los trámites notariales.

2.1 ANÁLISIS DE LA SITUACIÓN ACTUAL

En este subcapítulo se analizan los requerimientos de organización, funcionalidad y de procedimiento de la Notaría. El análisis de la situación actual se realiza en base a dos componentes: Análisis de la Notaría y Análisis de los Trámites Notariales. El Análisis de la Notaría se realiza con base en los usuarios que conforman la Notaría,

sus funciones y su interacción con el archivo notarial. El Análisis de los Trámites Notariales se realiza con base en los requerimientos del flujo de trabajo. El Análisis de la Notaría se describe en el subcapítulo 2.1.1. El Análisis de los Trámites Notariales y la metodología a utilizarse para describir sus requerimientos funcionales se muestra en el subcapítulo 2.1.2.

2.1.1 ANÁLISIS DE LA NOTARÍA

En la tabla 2.1 se menciona el papel que cumple cada usuario de la Notaría. La primera columna muestra los usuarios que intervienen en los trámites notariales. La segunda columna denominada Funciones y Obligaciones indica las actividades que desempeñan los usuarios. Y la tercera columna menciona los permisos que tienen los usuarios para acceder al archivo.

Usuario	Funciones y Obligaciones	Acceso al archivo
Notario	• Dar fe de los actos que se le presenten. • Controlar la organización y custodia del archivo.	• Es responsabilidad del Notario custodiar el archivo encargado. • Acceso total mediante llave al lugar que almacena el archivo.
Verificador	• Revisar la legalidad de los requerimientos. • Verificar la validez de la documentación presentada	• No tiene acceso al archivo.
Matrizador	• Realizar las matrices[13] de los trámites notariales.	• No tiene acceso al archivo.

Tabla 2.1: Análisis de participantes en la Notaría y sus funciones

[13] Matriz.- Documento notarial que contiene la información que el cliente presenta en el trámite notarial para obtener su Escritura Pública.

Usuario	Funciones y Obligaciones	Acceso al archivo
Administrador del Archivo	• Añadir las escrituras y diligencias al archivo. • Organizar documentación del archivo. • Mantener un registro del número de copias de escrituras entregadas.	• Tiene entera confianza por parte del Notario para administrar el archivo. • Acceso total mediante llave al lugar que almacena el archivo.
Clientes	• Requerir los servicios de la Notaría. • Presentar documentación y requerimientos en regla.	• No tiene acceso al archivo. • Solicita copias de escrituras al Notario.

Tabla 2.1: Análisis de participantes en la Notaría y sus funciones (Continuación)

Existen otros usuarios que colaboran en la Notaría. El Notario Suplente tiene iguales atribuciones que el Notario Principal cuando lo reemplaza. No se menciona el personal encargado de la facturación por el alcance del presente proyecto de titulación. Los empleados encargados de recepción tampoco se mencionan debido a que no cumplen una función importante en el flujo de trabajo notarial. Los testigos del trámite notarial no intervienen en los procesos propuestos a continuación.

2.1.2 ANÁLISIS DE TRÁMITES NOTARIALES

En este subcapítulo se analiza el protocolo de cinco trámites notariales. Los cinco trámites notariales escogidos fueron: Declaración Patrimonial Jurada, Declaración Juramentada, Poder Especial, Fiel Copia del Original y Compraventa Vehicular. La elección de los trámites notariales se realizó con base en la demanda que presenta la Notaría Octava del Cantón Quito y la fácil comprensión del flujo de trabajo que presentan estos trámites notariales. El protocolo de cada trámite notarial muestra los

requerimientos funcionales de la Notaría. La finalidad es describir el flujo de trabajo que realizan los usuarios de los trámites notariales. El flujo de trabajo de los trámites notariales escogidos incluyen: los usuarios que intervienen, las precondiciones documentales o de identidad, el flujo de trabajo o secuencia normal, la postcondición como resultado del proceso realizado, las excepciones cuando no se cumple la secuencia normal y la frecuencia esperada. El valor asignado en la frecuencia esperada resulta de un estimado del número de trámites notariales realizados en la Notaría Octava del Cantón Quito durante los meses de Febrero y Marzo de 2010.

La herramienta utilizada para detallar los trámites de la Notaría es UML. UML posee las siguientes herramientas de modelado: Diagramas de casos de uso, de clases, de estados, de secuencias, de actividades, de colaboraciones, de componentes y de distribución[14]. De estas opciones disponibles se optó por diagramas de casos de uso, debido a que este método captura todos los requisitos de comunicación y de comportamiento en un sistema. Analiza los escenarios de interacción entre los diferentes usuarios para solucionar un problema. Además los casos de uso usan un lenguaje comprensible para el usuario final.[15]

La figura 2.1 recrea la interacción entre los participantes de los trámites notariales. La interacción entre los usuarios de la Notaría y los clientes a través del caso de uso se muestran mediante un color distintivo. Los cinco procedimientos se describen a continuación mediante su caso de uso.

[14] UML: Diagramas UML. ¿Qué es UML? Análisis y Diseño. Ingeniería del software (Fuente: http://www.ingenierosoftware.com /analisisydiseno/uml.php)
[15] Diagrama de casos de uso (Fuente: http://es.wikipedia.org/wiki/Diagrama_de_casos_de_uso)

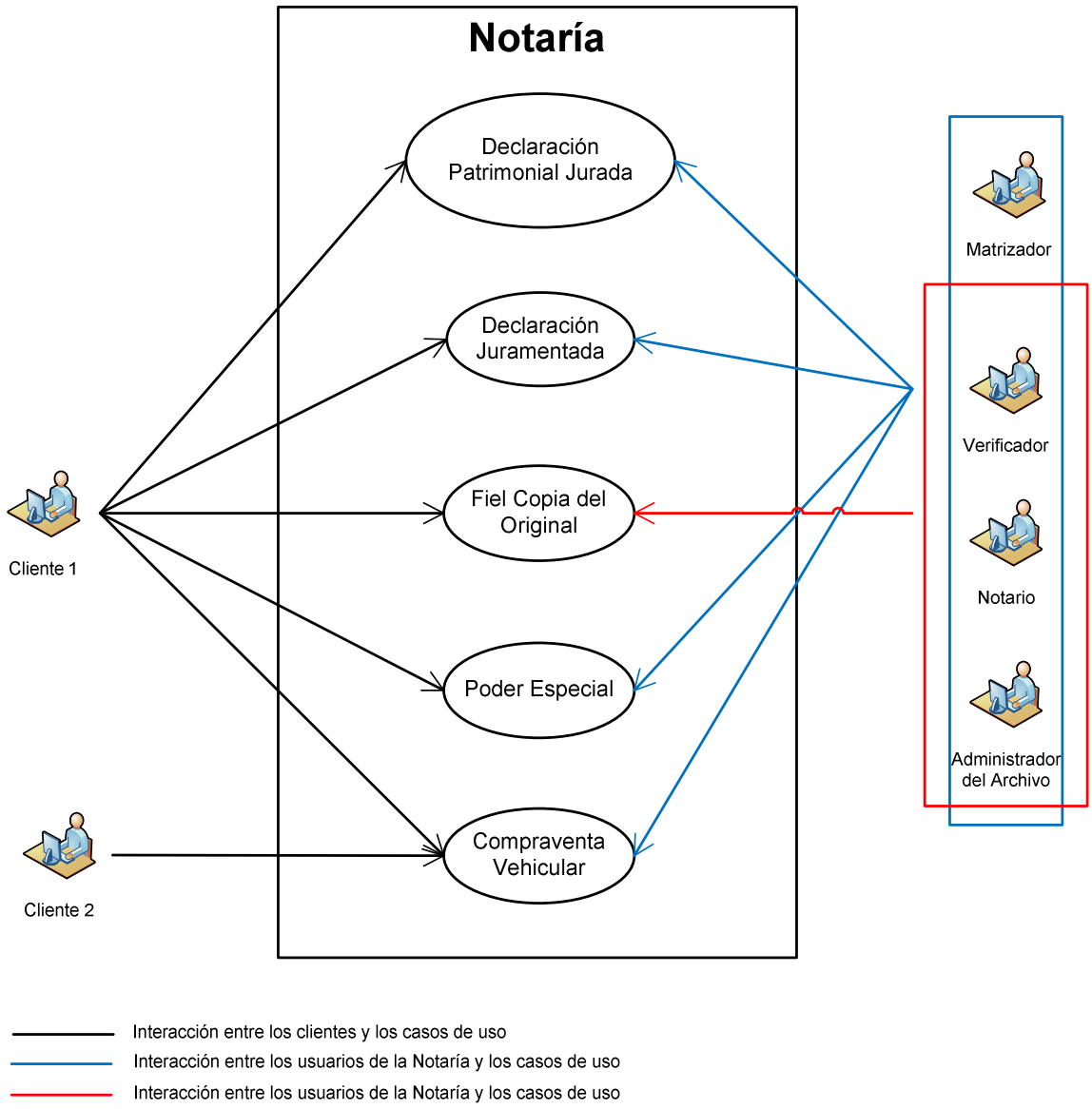

Figura 2.1: Casos de Uso de la Notaría

2.1.2.1 Trámite Declaración Patrimonial Jurada

La Declaración Patrimonial Jurada es un acto jurídico mediante el cual una persona declara ante el Notario información correspondiente al patrimonio que mantenga tanto en el país como en el exterior. El declarante autorizará expresamente para que se levante el sigilo de sus cuentas bancarias, de ser necesario. La tabla 2.2 describe el caso de uso del trámite notarial Declaración Patrimonial Jurada.

Caso de Uso

UC-0001	**Declaración Patrimonial Jurada**
Versión	1.0 (15/05/2010)
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear
Descripción	El trámite notarial Declaración Patrimonial Jurada se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría.
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente
Precondición	El Cliente posee el Formulario para la Declaración Patrimonial Jurada de la Contraloría General del Estado lleno a computadora, la cédula de ciudadanía y la papeleta de votación, y una copia a color de estos documentos de identidad.

Tabla 2.2: Caso de Uso Declaración Patrimonial Jurada

UC-0001	Declaración Patrimonial Jurada	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente presenta al Verificador su Formulario de la Declaración Patrimonial Jurada, la cédula de ciudadanía, la papeleta de votación y una copia a color de estos documentos de identidad.
	2	El Verificador revisa la validez de la cédula de ciudadanía y la papeleta de votación presentada por el Cliente.
	3	El Verificador revisa la validez del Formulario de Declaración Patrimonial Jurada presentada por el Cliente.
	4	El Verificador envía el Formulario de la Declaración Patrimonial Jurada al Matrizador.
	5	El Matrizador redacta la matriz de la Declaración Patrimonial Jurada sobre la base de la información del Formulario presentado por el Cliente.
	6	El Matrizador imprime la matriz de la Declaración Patrimonial Jurada, la revisa y la envía al Verificador.
	7	El Verificador da lectura de la matriz de la Declaración Patrimonial Jurada al Cliente.
	8	El Cliente firma la matriz de Declaración Patrimonial Jurada.
	9	El Notario firma la matriz de Declaración Patrimonial Jurada.
	10	El Verificador cierra la Escritura Pública de la Declaración Patrimonial Jurada que contiene las firmas del Notario y del Cliente. El Formulario de la Contraloría General del Estado, la copia a color de la cédula de ciudadanía y papeleta de votación se adjuntan como documentos habilitantes.

Tabla 2.2: Caso de Uso Declaración Patrimonial Jurada (Continuación)

UC-0001	Declaración Patrimonial Jurada	
Secuencia normal	**Paso**	**Acción**
	11	El Verificador saca dos copias de la Escritura Pública de la Declaración Patrimonial Jurada, del Formulario y de la documentación de identidad del Cliente.
	12	El Matrizador imprime dos concuerdos[16].
	13	El Verificador adjunta las copias generadas en el paso 11 con los concuerdos.
	14	El Notario firma los concuerdos para certificar que son copias de la documentación original de la Declaración Patrimonial Jurada y sumilla las copias.
	15	El Verificador entrega al Cliente las dos copias certificadas de la documentación de la Declaración Patrimonial Jurada.
	16	El Notario entrega al Administrador del Archivo la Escritura Pública de la Declaración Patrimonial Jurada junto con los documentos habilitantes.
	17	El Administrador del Archivo almacena la Escritura Pública de la Declaración Patrimonial Jurada junto con los documentos habilitantes en el tomo anual del Protocolo de Escrituras Públicas del archivo notarial.
Postcondición	El cliente ha obtenido dos copias de la Escritura Pública de su Declaración Patrimonial Jurada junto con sus documentos habilitantes.	

Tabla 2.2: Caso de Uso Declaración Patrimonial Jurada (Continuación)

[16] Concuerdo.- Redacción en que se ratifica la entrega de una copia de la Escritura Pública original.

UC-0001	Declaración Patrimonial Jurada	
Excepciones	**Paso**	**Acción**
	1	Si el Formulario de la Declaración Patrimonial Jurada no está lleno a computadora, el Verificador envía a corregir al Cliente y se termina el trámite notarial.
	2	Si la cédula de ciudadanía o la papeleta de votación no están en buen estado o se encuentran caducadas, el Verificador devuelve al Cliente notificando los inconvenientes y se termina el trámite notarial.
	3	Si existen errores en el Formulario de la Declaración Patrimonial Jurada, el Verificador envía a corregir al Cliente y se termina el trámite notarial.
	6	Si la matriz está incorrecta, el Matrizador realiza e imprime una nueva matriz de la Declaración Patrimonial Jurada.
	7	Si el Cliente encuentra inconvenientes con la matriz de la Declaración Patrimonial Jurada, notifica al Verificador las observaciones.
	7.a	El Verificador reporta las observaciones del Cliente al Matrizador para que realice una nueva matriz de la Declaración Patrimonial Jurada.
	7.b	El Matrizador redacta, imprime la nueva matriz de la Declaración Patrimonial Jurada y la envía al Verificador.
	7.c	El Verificador da lectura de la nueva matriz de la Declaración Patrimonial Jurada al Cliente.
Frecuencia esperada	200 veces por mes.	

Tabla 2.2: Caso de Uso Declaración Patrimonial Jurada (Continuación)

2.1.2.2 Trámite Declaración Juramentada

La Declaración Juramentada es un acto jurídico mediante el cual una persona declara ante el Notario cualquier hecho o información asumiendo la responsabilidad legal de lo declarado. La tabla 2.3 describe el caso de uso del trámite notarial Declaración Juramentada.

Caso de Uso

UC-0002	**Declaración Juramentada**	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial Declaración Juramentada se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría.	
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente	
Precondición	El Cliente posee el documento con el texto a declarar, la cédula de ciudadanía y la papeleta de votación, y una copia a color de estos documentos de identidad.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente presenta al Verificador el documento con el texto a declarar, la cédula de ciudadanía, la papeleta de votación y una copia a color de estos documentos de identidad.

Tabla 2.3: Caso de Uso Declaración Juramentada

UC-0002	Declaración Juramentada	
Secuencia normal	**Paso**	**Acción**
	2	El Verificador revisa la legalidad del documento con el texto a declarar. (La legalidad está basada según las atribuciones que se citan en el Art.18 de la Ley Notarial.)
	3	El Verificador revisa la ortografía del documento con el texto a declarar presentado por el Cliente.
	4	El Verificador revisa la validez de la cédula de ciudadanía y la papeleta de votación presentadas por el Cliente.
	5	El Verificador envía el documento con el texto a declarar al Matrizador.
	6	El Matrizador redacta la matriz sobre la base del documento con el texto a declarar presentado por el Cliente.
	7	El Matrizador imprime la matriz de la Declaración Juramentada, la revisa y la envía al Verificador.
	8	El Verificador da lectura de la matriz de la Declaración Juramentada al Cliente.
	9	El Cliente firma la matriz de la Declaración Juramentada.
	10	El Notario firma la matriz de la Declaración Juramentada.
	11	El Verificador cierra la Escritura Pública de la Declaración Juramentada que contiene las firmas del Notario y del Cliente. La copia a color de la cédula de ciudadanía y papeleta de votación se adjuntan como documentos habilitantes.
	12	El Verificador saca dos copias de la Escritura Pública de la Declaración Juramentada y de la documentación de identidad del Cliente.

Tabla 2.3: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Secuencia normal	**Paso**	**Acción**
	13	El Matrizador imprime dos concuerdos.
	14	El Verificador adjunta las copias generadas en el paso 12 con los concuerdos.
	15	El Notario firma los concuerdos para certificar que son copias de la documentación original de la Declaración Juramentada y sumilla las copias.
	16	El Verificador entrega al Cliente las dos copias certificadas de la documentación de la Declaración Juramentada.
	17	El Notario entrega al Administrador del Archivo la Escritura Pública de la Declaración Juramentada junto con los documentos habilitantes.
	18	El Administrador del Archivo almacena la Escritura Pública de la Declaración Juramentada junto con los documentos habilitantes en el tomo anual del Protocolo de Escrituras Públicas del archivo notarial.
Postcondición	El Cliente ha obtenido dos copias de la Escritura Pública de su Declaración Juramentada con sus documentos habilitantes.	
Excepciones	**Paso**	**Acción**
	2	Si el documento con el texto a declarar es ilegal, el Verificador notifica al Cliente y se termina el trámite notarial.
	3	Si existen errores ortográficos en el documento con el texto a declarar, el Verificador envía a corregir al Cliente y se termina el trámite notarial.

Tabla 2.3: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Excepciones	**Paso**	**Acción**
	4	Si la cédula de ciudadanía o la papeleta de votación no están en buen estado o se encuentran caducadas, el Verificador devuelve al Cliente notificando los inconvenientes y se termina el trámite notarial.
	7	Si la matriz de la Declaración Juramentada está incorrecta, el Matrizador realiza e imprime una nueva matriz.
	8	Si el Cliente encuentra inconvenientes con la matriz de la Declaración Juramentada, notifica al Verificador las observaciones.
	8.a	El Verificador reporta las observaciones del Cliente al Matrizador para que realice una nueva matriz de la Declaración Juramentada.
	8.b	El Matrizador redacta, imprime la nueva matriz de la Declaración Juramentada y la envía al Verificador.
	8.c	El Verificador da lectura de la nueva matriz de la Declaración Juramentada al Cliente.
Frecuencia esperada	50 veces por mes.	

Tabla 2.3: Caso de Uso Declaración Juramentada (Continuación)

2.1.2.3 Trámite Poder Especial

Poder Especial es la autorización que da una persona, a favor de otra, con la finalidad que pueda actuar en su nombre y representación. La tabla 2.4 describe el caso de uso del trámite notarial Poder Especial.

UC-0003	Poder Especial	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial Poder Especial se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría.	
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente	
Precondición	El Cliente posee la Minuta de Poder Especial elaborada y firmada por un Abogado, la cédula de ciudadanía y la papeleta de votación, y una copia a color de estos documentos de identidad.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente presenta al Verificador la Minuta de Poder Especial, la cédula de ciudadanía, la papeleta de votación y una copia a color de estos documentos de identidad.
	2	El Verificador revisa la validez de la cédula de ciudadanía y la papeleta de votación presentada por el Cliente.
	3	El Verificador envía la Minuta de Poder Especial al Matrizador.
	4	El Matrizador redacta la matriz de Poder Especial sobre la base de la información de la Minuta de Poder Especial presentada por el Cliente.

Tabla 2.4: Caso de Uso Poder Especial

UC-0003	Poder Especial	
Secuencia normal	**Paso**	**Acción**
	5	El Matrizador imprime la matriz de Poder Especial, la revisa y la envía al Verificador.
	6	El Verificador da lectura de la matriz de Poder Especial al Cliente.
	7	El Cliente firma la matriz de Poder Especial.
	8	El Notario firma la matriz de Poder Especial.
	9	El Verificador cierra la Escritura Pública de Poder Especial que contiene las firmas del Notario y del Cliente. La copia a color de la cédula de ciudadanía y papeleta de votación se adjuntan como documentos habilitantes.
	10	El Verificador saca dos copias de la Escritura Pública de Poder Especial y de la documentación de identidad del Cliente.
	11	El Matrizador imprime dos concuerdos.
	12	El Verificador adjunta las copias generadas en el paso 10 con los concuerdos.
	13	El Notario firma los concuerdos para certificar que son copias de la documentación original de Poder Especial y sumilla las copias.
	14	El Verificador entrega al Cliente las dos copias certificadas de la documentación de Poder Especial.
	16	El Notario entrega al Administrador del Archivo la minuta y la Escritura Pública de Poder Especial junto con los documentos habilitantes.

Tabla 2.4: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Secuencia normal	**Paso**	**Acción**
	17	El Administrador del Archivo almacena la Escritura Pública de Poder Especial junto con los documentos habilitantes en el tomo anual del Protocolo de Escrituras Públicas del archivo notarial.
	18	El Administrador del Archivo almacena la minuta de Poder Especial en el archivo notarial de Minutas.
Postcondición	El Cliente ha obtenido dos copias de la Escritura Pública de Poder Especial junto con sus documentos habilitantes.	
Excepciones	**Paso**	**Acción**
	2	Si la cédula de ciudadanía o la papeleta de votación no están en buen estado o se encuentran caducadas, el Verificador devuelve al Cliente notificando los inconvenientes y se termina el trámite notarial.
	5	Si la matriz de Poder Especial está incorrecta, el Matrizador realiza e imprime una nueva matriz.
	6	Si el Cliente encuentra inconvenientes con la matriz de Poder Especial, notifica al Verificador las observaciones.
	6.a	El Verificador reporta las observaciones del Cliente al Matrizador para que realice otra matriz de Poder Especial.
	6.b	El Matrizador redacta, imprime la nueva matriz de Poder Especial y la envía al Verificador.
	6.c	El Verificador da lectura de la nueva matriz de Poder Especial al Cliente.
Frecuencia	50 veces por mes.	

Tabla 2.4: Caso de Uso Poder Especial (Continuación)

2.1.2.4 Trámite Fiel Copia del Original

Fiel Copia del Original es un proceso mediante el cual se certifica una o varias copias por parte del Notario ante la presentación del documento original. La tabla 2.5 describe el caso de uso del trámite notarial Fiel Copia del Original.

Caso de Uso

UC-0004	**Fiel Copia del Original**	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial Fiel Copia del Original se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría.	
Actores	Notario Verificador Administrador del Archivo Cliente	
Precondición	El Cliente posee el documento original.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente presenta el documento original a certificar y especifica el número de copias necesarias.
	2	El Verificador revisa la validez del documento original.
	3	El Verificador saca el número de copias requeridas del documento original y una copia adicional para el Libro de Diligencias.
	4	El Notario firma todas las copias del documento original.

Tabla 2.5: Caso de Uso Fiel Copia del Original

UC-0004	Fiel Copia del Original	
Secuencia normal	**Paso**	**Acción**
	5	El Verificador entrega al Cliente el número de copias notarizadas solicitadas.
	6	El Notario entrega al Administrador del Archivo la copia adicional notarizada obtenida del documento original.
	7	El Administrador del Archivo almacena la copia adicional notarizada obtenida del documento original en el tomo anual del Libro de Diligencias del archivo notarial.
Postcondición	El Cliente ha obtenido el número de copias notarizadas requeridas del documento original.	
Excepciones	**Paso**	**Acción**
	2	Si el documento original presenta algún inconveniente, el Verificador devuelve al Cliente notificando el problema y se termina el trámite notarial.
Frecuencia esperada	100 veces por mes.	

Tabla 2.5: Caso de Uso Fiel Copia del Original (Continuación)

2.1.2.5 Trámite Compraventa Vehicular

Según el Código Civil, la Compraventa es el contrato mediante el cual el vendedor se obliga a transferir la propiedad de un bien al comprador, y este a su vez, se obliga a pagar su precio en dinero. Para este caso de uso se utilizará el trámite notarial de Compraventa Vehicular. El trámite notarial de Compraventa Vehicular se analiza con solo un Comprador y un Vendedor. El trámite notarial se considera un reconocimiento de firmas del Contrato de Compraventa Vehicular presentado por los participantes. La tabla 2.6 describe el caso de uso del trámite notarial Compraventa Vehicular.

Caso de Uso

UC-0005	**Compraventa Vehicular**	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial Compraventa Vehicular se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría.	
Actores	Notario Verificador Matrizador Administrador del Archivo Comprador del vehículo Vendedor del vehículo	
Precondición	El Comprador y Vendedor del vehículo poseen en total dos Contratos idénticos de Compraventa Vehicular firmados, sus cédulas de ciudadanía y papeletas de votación.	
Secuencia normal	**Paso**	**Acción**
	1	El Comprador o Vendedor del vehículo presentan al Verificador los dos Contratos idénticos de Compraventa Vehicular firmados, sus cédulas de ciudadanía y papeletas de votación.
	2	El Verificador revisa la validez de las cédulas de ciudadanía y papeletas de votación presentadas por el Comprador y Vendedor del vehículo.

Tabla 2.6: Caso de Uso Compraventa Vehicular

UC-0005	Compraventa Vehicular	
Secuencia normal	**Paso**	**Acción**
	3	El Verificador realiza el reconocimiento de firmas de los Contratos de Compraventa Vehicular presentados por los Clientes con sus cédulas de ciudadanía.
	4	El Verificador envía los Contratos de Compraventa Vehicular al Matrizador.
	5	El Matrizador redacta el Acta digital de Compraventa Vehicular sobre la base de los Contratos presentados por el Comprador o Vendedor del vehículo.
	6	El Matrizador imprime dos Actas de Compraventa Vehicular, las revisa y las envía al Verificador.
	7	El Verificador da lectura del Acta de Compraventa Vehicular al Comprador y Vendedor del vehículo.
	8	El Comprador del vehículo firma las dos Actas de Compraventa Vehicular.
	9	El Vendedor del vehículo firma las dos Actas de Compraventa Vehicular.
	10	El Notario firma las dos Actas de Compraventa Vehicular.
	11	El Verificador saca una copia del Contrato y del Acta notarizada de Compraventa Vehicular para el Libro de Diligencias.
	12	El Verificador entrega un Acta notarizada junto con un Contrato de Compraventa Vehicular al Comprador y otro par al Vendedor del vehículo.

Tabla 2.6: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Secuencia normal	**Paso**	**Acción**
	13	El Notario entrega al Administrador del Archivo la copia del Acta notarizada y del Contrato de Compraventa Vehicular.
	14	El Administrador del Archivo almacena la copia del Acta notarizada y del Contrato de Compraventa Vehicular en el tomo anual del Libro de Diligencias del archivo notarial.
Postcondición	El Comprador y Vendedor del vehículo han obtenido cada uno un Acta notarizada y su Contrato de Compraventa Vehicular.	
Excepciones	**Paso**	**Acción**
	1	Si los Clientes no presentan dos Contratos idénticos de Compraventa Vehicular firmados, el Verificador notifica el inconveniente y se termina el trámite notarial.
	2	Si las cédulas de ciudadanía o las papeletas de votación no están en buen estado o se encuentran caducadas, el Verificador devuelve al Comprador o Vendedor del vehículo notificando los inconvenientes y se termina el trámite.
	3	Si las firmas de los dos Contratos de Compraventa Vehicular no coinciden con las de sus cédulas de ciudadanía, el Verificador notifica el inconveniente y se termina el trámite.
	6	Si el Acta de Compraventa Vehicular está incorrecta, el Matrizador realiza e imprime una nueva acta.
	7	Si el Comprador o Vendedor del vehículo encuentra inconvenientes con las Actas de Compraventa Vehicular, notifica al Verificador las observaciones.

Tabla 2.6: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Excepciones	**Paso**	**Acción**
	7.a	El Verificador reporta las observaciones del Comprador o Vendedor del vehículo al Matrizador para que realice una nueva Acta de Compraventa Vehicular.
	7.b	El Matrizador redacta, imprime la nueva Acta de Compraventa Vehicular y la envía al Verificador.
	7.c	El Verificador da lectura de la nueva Acta de Compraventa Vehicular al Comprador y Vendedor del vehículo.
Frecuencia esperada	100 veces por mes.	

Tabla 2.6: Caso de Uso Compraventa Vehicular (Continuación)

2.2 ANÁLISIS DE REQUERIMIENTOS

En este subcapítulo se analizan los requerimientos de seguridad y de gestión documental. Los criterios de seguridad se analizan sobre el flujo de trabajo de los trámites notariales en el subcapítulo 2.2.1. Los parámetros de gestión documental se enfocan en el archivo notarial y se describen en el subcapítulo 2.2.2.

2.2.1 ANÁLISIS DE REQUERIMIENTOS DE SEGURIDAD

En este subcapítulo se describen los requerimientos de seguridad que demandan los protocolos de los trámites notariales desarrollados en el subcapítulo 2.1.2. El análisis se realiza sobre la base de los objetivos de la seguridad para garantizar el acto notarial: autenticidad, no repudio, confidencialidad, integridad y disponibilidad.

- **Autenticidad**

  El Notario se autentica frente al Presidente de la Corte Superior de Justicia. En su nombramiento registra su firma, rúbrica, sello y ubicación de su oficina.

  El cliente identifica al Notario mediante la dirección de su oficina y la firma que utilice en el acto notarial. La autenticación del cliente se realiza mediante cédula de ciudadanía y papeleta de votación actualizadas.

  El trámite notarial es presencial para cumplir con la unidad de acto. El Notario es el encargado de dar fe de la autenticidad del cliente.

- **No Repudio**

  La firma de los participantes del trámite notarial está bajo la responsabilidad de los mismos. El contenido del documento que resulte del trámite notarial tiene efectos legales cuando los participantes implantan su firma. Los participantes no pueden retractarse si se comprueba que su firma es original.

- **Confidencialidad**

  El trámite notarial es de carácter público. Los clientes comparten espacio físico en la oficina de la Notaría. El cliente puede solicitar al Notario la privacidad de su acto notarial. El trámite notarial se vuelve confidencial mediante el requerimiento de unidad de acto[17]. La fe pública de la que goza el Notario garantiza la confiabilidad del trámite notarial.

- **Integridad**

  El Notario actúa como persona de confianza para asegurar la integridad del trámite notarial. La unidad de acto impide la adulteración de documentación presentada en el trámite notarial. La matriz definitiva se lee al cliente para ratificar

[17] Unidad de Acto.- Procedimiento notarial mediante el cual se lee el contenido de la matriz directamente al cliente.

que la redacción concuerda con su requerimiento. Si los participantes firman la matriz aceptan que su requerimiento no ha sido alterado.

- **Disponibilidad**

  La Ley Notarial reglamenta que todos los días del año son hábiles para la realización de trámites notariales. Sin embargo la Notaría establece un horario laboral para atención al público. La disponibilidad para realizar trámites notariales está sujeta a este horario. Al tratarse de una oficina pública, se excluyen días festivos y fines de semana. El Notario Suplente toma el lugar del Principal, con las mismas atribuciones, cuando éste se ausente a fin de mantener disponible el servicio de la Notaría.

2.2.2 ANÁLISIS DE REQUERIMIENTOS DE GESTIÓN DOCUMENTAL

En este subcapítulo se analizan los requerimientos de almacenamiento y seguridad que requiere el archivo notarial. El análisis se realiza mediante parámetros de gestión documental: Organización y Distribución. Además se incluyen parámetros para resguardar la documentación con base en los objetivos de seguridad: Control de Acceso, No Repudio, Confidencialidad, Integridad y Disponibilidad.

- **Organización**

  La organización del archivo notarial comprende toda la documentación generada en los trámites notariales. El archivo notarial se divide en Protocolo y Libro de Diligencias según la Ley Notarial.

  - ***Protocolo***

    El protocolo está compuesto por todas las Escrituras Públicas y Privadas generadas anualmente. Para organización se lo divide en libros o tomos mensuales de 500 hojas. Las hojas están numeradas acorde a la fecha de creación de la Escritura. El protocolo incluye un índice alfabético de los otorgantes de la Escritura Pública. Las minutas forman un archivo similar mantenido por dos años. Para el presente proyecto de titulación el

Protocolo almacenará las Escrituras Públicas de los trámites notariales: Declaración Patrimonial Jurada, Declaración Juramentada y Poder Especial.

- ***Libro de Diligencias***

  El Libro de Diligencias almacena los actos notariales que no requieren las solemnidades de una Escritura Pública. En este archivo estarán las Actas que no formen parte del Protocolo. Su organización es semejante a la del Protocolo de Escrituras Públicas. En este proyecto de titulación, los trámites notariales Fiel Copia del Original y Compraventa Vehicular se almacenan en este Libro de Diligencias.

- **Distribución**

  La documentación del archivo notarial es de carácter público. La Notaría está obligada a entregar fotocopias de la documentación del archivo a los ciudadanos que la soliciten. El control de la cantidad de copias entregadas se realiza mediante numeración y registro en la Escritura Pública original archivada.

- **Control de Acceso**

  El Notario tiene control total sobre el archivo notarial porque está bajo su responsabilidad. El Notario autoriza el acceso al archivo notarial al Administrador del Archivo. Ningún otro usuario está autorizado a acceder al archivo notarial. Los clientes solo se limitan a solicitar documentación del archivo notarial.

  El Administrador del Archivo accede para la organización y almacenamiento de la documentación diaria que se genere. Además se encarga de gestionar la distribución de copias de documentación del archivo notarial. El Notario accede para controlar que el archivo notarial se encuentre bien organizado.

- **No Repudio**

  La Escritura Pública que forme parte del archivo notarial es la original para discrepancias de no repudio. Es válida si posee la firma de todos los participantes. Los integrantes que constan en la Escritura Pública no podrán rechazar sus acciones si su firma está estampada en el documento.

  La copia entregada a los clientes es válida si consta el concuerdo con la firma del Notario. El concuerdo incluye además el sello y firma del Notario. El Notario con su firma asegura que la fotocopia es fiel copia de la Escritura Pública original que mantiene en su archivo notarial.

- **Confidencialidad**

  Las Escrituras Públicas del archivo notarial son de naturaleza pública según la Ley Notarial. Los ciudadanos pueden solicitar copias de cualquier Escritura Pública. La confidencialidad del archivo notarial radica en que es propiedad del Estado. La información entregada a la Notaría está protegida por la Ley Notarial. La custodia del archivo notarial es responsabilidad del Notario.

- **Integridad**

  La integridad del archivo notarial se asegura mediante el control de acceso que maneja el Notario. La adulteración a los documentos notariales se evita mediante la numeración de hojas y sumillado del Notario. Entre la documentación del archivo notarial y la copia entregada al cliente se considera íntegra la primera.

- **Disponibilidad**

  El archivo notarial está disponible en la oficina del Notario. El acceso está sujeto al horario establecido por la Notaría. El Notario entregará el archivo notarial a quien lo reemplace al cesar sus funciones. La Ley Notarial no especifica un límite de años para desechar la documentación.

CAPÍTULO 3

DISEÑO DE LA NOTARÍA DIGITAL

En este capítulo se documenta el diseño de la infraestructura de Notaría Digital. El diseño de la infraestructura física y lógica abarca todos los requerimientos de organización, funcionalidad, protocolo, seguridad y gestión documental analizados en el capítulo anterior. La infraestructura de la red de datos de la Notaría Digital se compone de dispositivos de interconexión, servidores y estaciones de trabajo que sirven para intercomunicar y compartir información entre los usuarios. La infraestructura lógica se compone de directorio de identidades, sistema de gestión documental, certificados de firma electrónica y marcas de tiempo para ofrecer los trámites notariales digitales a través de Internet de manera segura.

La infraestructura de la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE) como opción para Gestionar Identidades en la Notaría Digital, se analiza en el subcapítulo 3.1. Los protocolos para realizar los cinco trámites en la Notaría Digital se modelan usando casos de uso en el subcapítulo 3.2. El diseño de un Sistema de Gestión Documental que cumpla los requerimientos de almacenamiento y seguridad del archivo notarial digital se explica en el subcapítulo 3.3. Para finalizar el capítulo se diseña la Infraestructura de la Red de Datos para las instalaciones de la Notaría con base en la arquitectura SAFE de CISCO.

3.1 GESTIÓN DE IDENTIDADES

En este subcapítulo se analiza los beneficios que presenta la infraestructura de la ECIBCE como Gestor de Identidades en la Notaría Digital. El análisis se realiza sobre dos parámetros: Directorio de Identidades y Seguridad de la ECIBCE, como se muestra en la figura 3.1. El primero se enfoca en la distinción entre cuentas de usuario y la distribución de llaves públicas. El segundo parámetro se subdivide en: Autenticación para certificar que un usuario es quien dice ser, Autorización para

identificar si un certificado de firma electrónica tiene validez para usarlo y, Auditoría para conocer quién y cuándo usó el certificado de firma electrónica y si estuvo habilitado para hacerlo. Para complementar la Auditoría se analiza la necesidad de una Autoridad de Tiempo en el Ecuador. Al finalizar este subcapítulo se analiza la factibilidad de tercerizar la Gestión de Identidades en la Notaría Digital a la ECIBCE frente a la implementación de una propia PKI.

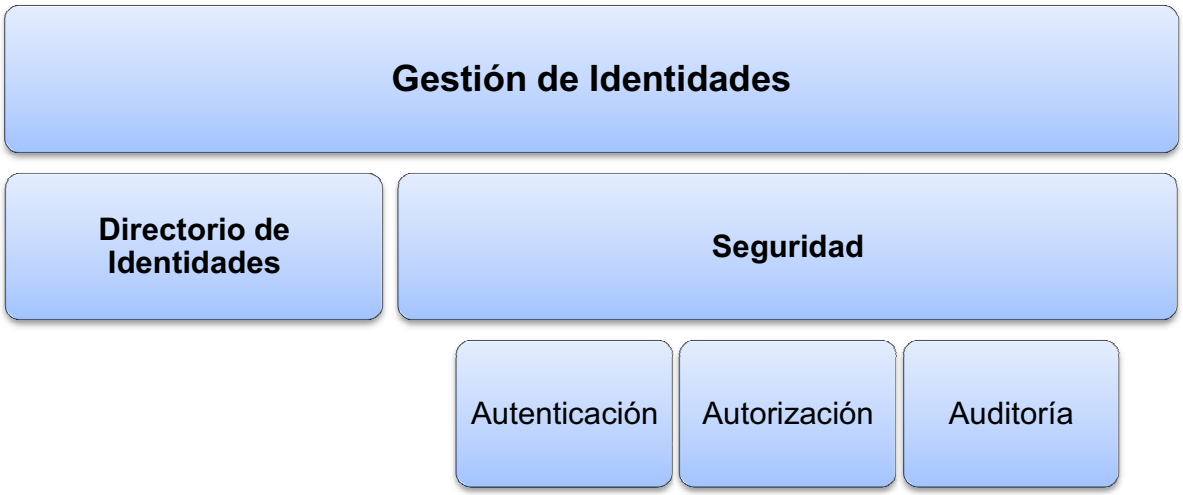

Figura 3.1: Criterios de análisis para Gestión de Identidades en la Notaría Digital

La información utilizada en este subcapítulo para el análisis se obtuvo de los documentos "Declaración de Prácticas de Certificación" (junio del 2010), "Declaración de Políticas de Seguridad" (junio del 2010) y "Certificados de Firma Electrónica" publicados en el sitio web de la ECIBCE: http://www.eci.bce.ec.

3.1.1 DIRECTORIO DE IDENTIDADES DE LA ECIBCE [18]

El objetivo de este parámetro es distinguir la cuenta de un usuario de otra. Se analiza si los atributos de los certificados de firma electrónica emitidos por la ECIBCE permiten diferenciar entre cuentas de usuarios finales. Los datos incluidos en el

[18] El Directorio de Identidades de la ECIBCE almacena todos los usuarios que han solicitado un certificado digital de firma electrónica. El Directorio posee información de personas naturales, jurídicas y funcionarios públicos.

certificado de firma electrónica son resultado del registro personal que hace la ECIBCE al usuario final que requiere un certificado de firma electrónica.

Todos los tipos de certificados de firma electrónica que emite la ECIBCE incluyen campos comunes que se muestran en la tabla 3.1. Estos campos no permiten diferenciar si un certificado de firma electrónica es de persona natural, funcionario público o persona jurídica, que son los tres tipos de certificados que emite la ECIBCE

Campos del certificado	Descripción
Versión	Muestra la versión dentro del estándar X.509
Número de serie	Número de serie del certificado
SHA1 RSA	Algoritmos de firma electrónica
countryName (c)	(ec) país de autoridad de certificación: Ecuador
organizationName (o)	(bce) nombre de organización de certificación: Banco Central del Ecuador
organizationalUnitName (ou)	(eci) entidad de certificación de Información
Válido desde	Fecha de emisión del certificado
Válido hasta	Fecha de caducidad del certificado
commonName (cn) / Emisor	Nombre completo del suscriptor
X509v3 Subject Alternative Name	nombre alternativo/correo electrónico del suscriptor
X509v3 CRL Distribution Points	Puntos de distribución de CRL. Dirección donde se publica la lista de revocación de Certificados
Clave Pública	Clave Pública del Suscriptor
Uso de clave	Identifica el uso que será aplicable
Período de uso clave privada	Tiempo en que estará vigente la clave privada

Tabla 3.1: Campos Comunes de los Certificado de Firma Electrónica de la ECIBCE para un Usuario Final[19]

[19] Políticas de Certificado de Firma Electrónica de Persona Natural. Junio del 2010. Fuente: http://www.eci.bce.ec/documents/10155/17777/politicasCertificadoFirmaElectronicaPersonaNatural.pdf

Campos del certificado	Descripción
Identificador de clave de entidad emisora	Extensión del estándar X.509
Identificador clave de asunto	Extensión del estándar X.509
Restricciones Básicas	Determina a que está destinada la AC, la ruta de certificación como entidad final de ECI
Algoritmo de identificación	Algoritmo de firma utilizado por la AC
Huella digital	Id de huella asociado al certificado

Tabla 3.1: Campos Comunes de los Certificado de Firma Electrónica de la ECIBCE para un Usuario Final (Continuación)

Las tablas 3.2, 3.3 y 3.4 detallan los campos propios de los certificados de firma electrónica emitidos por la ECIBCE para persona natural, persona jurídica y funcionario público respectivamente. La columna izquierda representa el campo y la derecha muestra el valor correspondiente a ese campo. Estos campos constan en el detalle del certificado de firma electrónica como lo muestra la figura 3.3.

Detalles propios de certificado de firma electrónica de Persona Natural	
1.2.3.4.1	CÉDULA DE CIUDADANIA
1.2.3.4.2	Nombre(s)
1.2.3.4.3	APELLIDO1
1.2.3.4.4	APELLIDO2
1.2.3.4.7	DIRECCIÓN
1.2.3.4.8	TELÉFONO
1.2.3.4.9	CIUDAD

Tabla 3.2: Campos Propios de los Certificado de Firma Electrónica de la ECIBCE para Persona Natural[20]

[20] Políticas de Certificado de Firma Electrónica de Persona Natural. Junio del 2010. Fuente: http://www.eci.bce.ec/documents/10155/17777/politicasCertificadoFirmaElectronicaPersonaNatural.pdf

Detalles propios de certificado de firma electrónica de Persona Jurídica	
1.2.3.4.10	RAZÓN SOCIAL
1.2.3.4.11	RUC
1.2.3.4.2	Nombre(s)
1.2.3.4.3	APELLIDO1
1.2.3.4.4	APELLIDO2
1.2.3.4.1	CÉDULA DE CIUDADANÍA
1.2.3.4.5	CARGO
1.2.3.4.7	DIRECCIÓN
1.2.3.4.8	TELÉFONO

Tabla 3.3: Campos Propios de los Certificado de Firma Electrónica de la ECIBCE para Persona Jurídica[21]

Detalles propios de certificado de firma electrónica de Funcionario Público	
1.2.3.4.1	CÉDULA DE CIUDADANÍA
1.2.3.4.2	Nombre(s)
1.2.3.4.3	APELLIDO1
1.2.3.4.4	APELLIDO2
1.2.3.4.5	CARGO
1.2.3.4.6	INSTITUCIÓN
1.2.3.4.7	DIRECCIÓN
1.2.3.4.8	TELÉFONO

Tabla 3.4: Campos Propios de los Certificado de Firma Electrónica de la ECIBCE para Funcionario Público[22]

[21] Políticas de Certificado de Firma Electrónica de Persona Jurídica**.** Junio del 2010. http://www.eci.bce.ec/documents/10155/17777/politicasCertificadoFirmaElectronicaPersonaJuridica.pf
[22] Políticas de Certificado de Firma Electrónica de Funcionario Público. Junio del 2010. http://www.eci.bce.ec/documents/10155/17777/politicasCertificadoFirmaElectronicaFuncionarioPublico.pdf

Beneficios del Directorio de la ECIBCE

- La ECIBCE dispone de un repositorio LDAP[23] publicado en Internet a través de la URL ldap://ldap.bce.ec. Este directorio almacena los usuarios de certificados de firma electrónica y provee información como: datos del titular, llave pública, período de validez, entre los más importantes. La búsqueda se realiza mediante nombre o correo electrónico del titular del certificado de firma electrónica como se muestra en la figura 3.2.

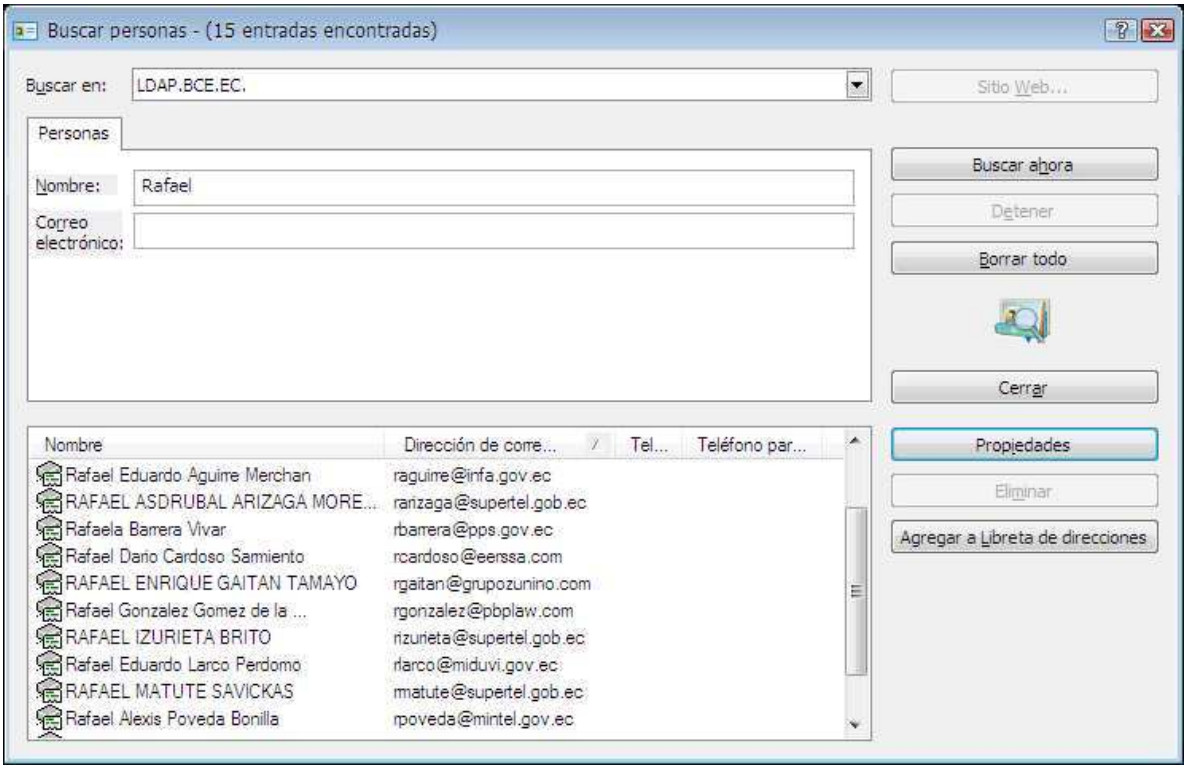

Figura 3.2: Usuarios Finales del LDAP de la ECIBCE de Nombre "Rafael"

- El Nombre Distinguido ó Distinguished Name (DN) del certificado de Usuario Final es el parámetro que permite diferenciar un usuario de otro. El DN consta de los campos c=ec, o=bce, ou=eci que aseguran que la ECIBCE es la Autoridad de

[23] LDAP (*Lightweight Directory Access Protocol*). Protocolo de Acceso Ligero a Directorio basado en el estándar X.500. Permite acceder a información almacenada en un directorio de información. (Fuente: http://www.ldapman.org/articles/sp_intro.html)

Certificación y cn=nombres completos del suscriptor para diferenciarlo del resto de usuarios. La figura 3.3 muestra el DN de un usuario del LDAP de la ECIBCE.

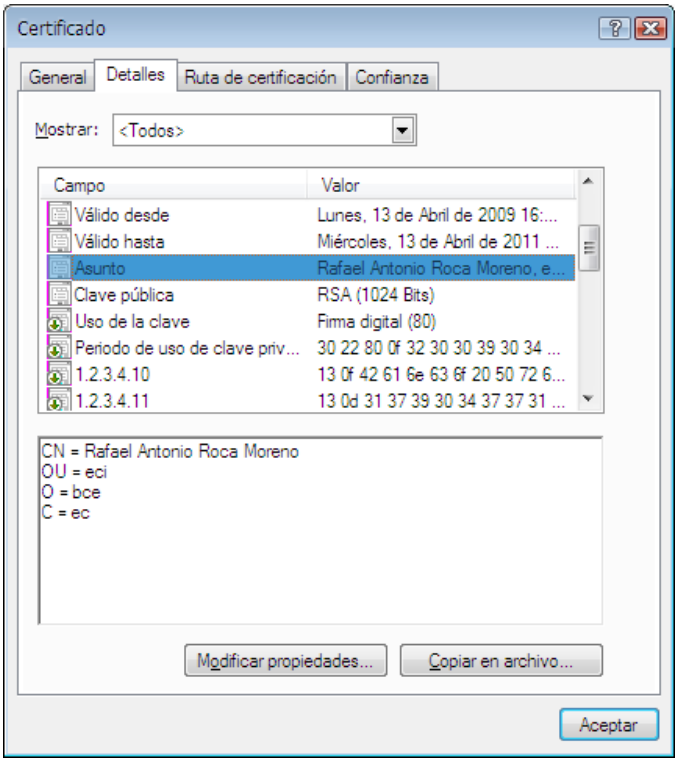

Figura 3.3: DN de un usuario del LDAP de la ECIBCE

- La ECIBCE aplica el algoritmo estandarizado RSA[24]. RSA es criptográficamente fuerte para la creación de llaves pública y privada del certificado de firma electrónica. Este algoritmo de seguridad evita la falsificación o adulteración del certificado de firma electrónica de un usuario final. Así se impide que se intente suplantar la identidad de un usuario auténtico por uno falso. Además aporta a la confianza en la PKI de la ECIBCE, porque sus llaves pública y privada son únicas y auténticas.

- La existencia de una Autoridad de Certificación acreditada en el Ecuador como entidad de confianza para procedimientos digitales es una ventaja para el manejo

[24] RSA. Algoritmo de cifrado de llave pública desarrollado por Rivest-Shamir-Adleman del MIT cuyo esquema usa expresiones exponenciales para generar llaves pública y privada.

de usuarios. Las personas que deseen hacer uso de la firma electrónica deberán obligatoriamente formar parte de la infraestructura del directorio de identidades de la ECIBCE.

3.1.2 SEGURIDAD DE LA ECIBCE

El objetivo de este parámetro es analizar la confiabilidad en la Gestión de Identidades que ofrecen los componentes de seguridad de la ECIBCE. Se toma como referencia las ventajas que presenta la ECIBCE en parámetros de autenticación, autorización y auditoría. El análisis se lo realiza sobre la base de los procesos de registro y emisión de certificados, mecanismos de seguridad y control de los tipos de usuarios que admite la ECIBCE.

3.1.2.1 Autenticación

El objetivo de este parámetro es confirmar que el usuario que va a registrar su cuenta frente a la ECIBCE es quien dice ser. La autenticación se obtiene con el proceso personal de registro que realiza un usuario para identificarse ante la ECIBCE presentando los requisitos solicitados para adquirir un certificado de firma electrónica de acuerdo a su procedimiento de registro.

Beneficios

- Añade un nivel de seguridad al requerir una contraseña para el uso del *token*. En este dispositivo se almacena el certificado de firma electrónica. Es una ventaja en términos de autenticidad, pues un atacante debió haber obtenido el *token*, acertar en la contraseña y esperar que el usuario auténtico no haya revocado el certificado para poder suplantar la identidad del titular. La figura 3.4 muestra el *token* que emite la ECIBCE y el *password* de autenticación que requiere para el uso del certificado de firma electrónica.
- La ECIBCE es reconocida como autoridad de confianza a través del certificado raíz que se instala en los ordenadores. Los certificados de firma electrónica que emita la ECIBCE se validan mediante la clave pública del certificado raíz y la clave pública que posee el certificado de firma electrónica.

Figura 3.4: Token donde se almacena el certificado digital emitido por la ECIBCE

(Fuente: Documento "Firma Electrónica en el Ecuador y su beneficio en la gestión comercial de las empresas" de la ECIBCE)

- La adquisición del certificado de firma electrónica es un proceso personal. Esto garantiza la identificación del usuario ante la ECIBCE. A su vez la ECIBCE verifica que los datos que se encuentren en la documentación presentada por el usuario sean correctos y no se encuentre novedades para la emisión del certificado de firma electrónica.

3.1.2.2 Autorización

El objetivo de este parámetro es analizar cuando un usuario de certificado de firma electrónica emitido por la ECIBCE está autorizado a utilizarlo. La ECIBCE avala la legalidad para el uso del certificado de firma electrónica mientras no esté revocado. El análisis se enfoca en el período de validez de un certificado de firma electrónica.

Beneficios

- La ECIBCE autoriza el uso de todos sus certificados de firma electrónica emitidos para un período de validez de 2 años. Todo usuario que posee un certificado de firma electrónica que no haya sobrepasado ese tiempo está autorizado a utilizarlo. Si el período de validez concluye, el certificado se considera caducado.

- La ECIBCE maneja una lista de certificados revocados (CRL) que sirve para identificar los certificados de firma electrónica que no tienen validez. Todas las acciones realizadas con un certificado de firma electrónica revocado no tendrán sustento legal. Esta CRL es actualizada diariamente por la ECIBCE.

3.1.2.3 Auditoría

El objetivo de este parámetro es analizar el ciclo de vida del certificado de firma electrónica de un usuario final. El análisis se realiza en el proceso de creación y en el proceso de revocatoria del certificado de firma electrónica realizado por la ECIBCE.

Beneficios

- La ECIBCE posee procedimientos bien definidos para la creación de certificados de firma electrónica[25]. La ECIBCE requiere que el trámite sea presencial con la presentación de documentos de identificación personal. El proceso personal de registro garantiza que no haya fraude en la generación de certificados. La ECIBCE mantiene asegurada esta información como lo establece la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos en su Art. 9.

- La ECIBCE posee procedimientos para la revocatoria de certificados de firma electrónica. La ECIBCE define razones para revocar un certificado de firma electrónica. Entre los motivos están: muerte del titular, olvido de la clave del token, cese de funciones del titular, por orden de autoridad competente, entre otras[26]. El formulario de solicitud de revocatoria requiere datos personales obligatorios para autenticar al solicitante. La ECIBCE comunica la resolución de revocatoria al usuario final vía telefónica o mediante correo electrónico.

- La ECIBCE proporciona una lista de certificados revocados mediante la siguiente URL http://www.eci.bce.ec/CRL/eci_bce_ec_crlfile.crl. Esta URL permite importar la lista de certificados revocados por la ECIBCE con la siguiente información:

[25] Solicitud Certificado de Firma Electrónica. (Fuente: http://www.eci.bce.ec/web/guest/solicitud-de-certificado1)
[26] Razones por la que un certificado puede ser revocado. (Fuente: http://www.bce.fin.ec/documentos/ElBancoCentral/EntidadCert/razonescertificadoRevocado.pdf)

número de serie, fecha y motivo de la revocación de los certificados de firma electrónica. La figura 3.5 muestra la lista de certificados revocados de la ECIBCE.

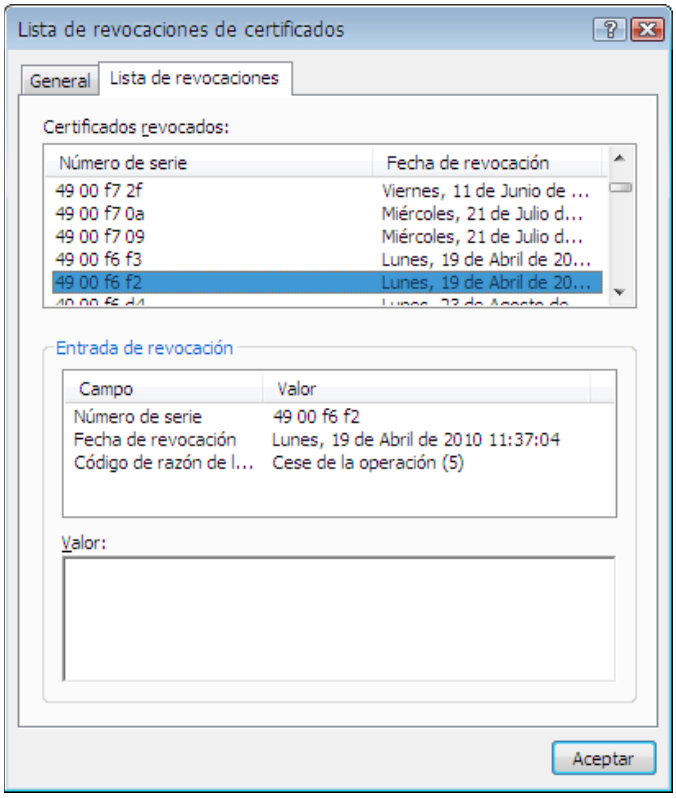

Figura 3.5: Lista de certificados revocados (CRL) de la ECIBCE

3.1.2.3.1 Autoridad de Tiempo

La fecha y hora en que se firmó un documento son de extrema importancia para procesos de auditoría en la Gestión de Identidades de la ECIBCE. Por esta razón se realiza un análisis acerca de la necesidad de una autoridad de tiempo en el Ecuador, de utilidad para la auditoría sobre el uso que den los usuarios finales al certificado de firma electrónica emitido por la ECIBCE.

- Las fechas de emisión y caducidad del certificado de firma electrónica asignadas por la ECIBCE permiten conocer desde y hasta cuando está habilitado para utilizarlo. El proceso personal de registro permite confiar en las fechas otorgadas. Al no cumplir la ECIBCE las funciones de Autoridad de Tiempo pierde el control

sobre la manipulación del tiempo al cual está expuesto el certificado de firma electrónica.

- El usuario está en capacidad de manipular la fecha y hora que se estampa en un documento digital. Dicha acción la puede realizar en la configuración de hora y fecha del ordenador donde vaya a utilizar el certificado de firma electrónica. Esto debido a que la firma electrónica utiliza la fecha y hora de la estación de trabajo donde se firma si no existe una Autoridad de Tiempo. Al modificar la fecha y hora de la estación de trabajo se puede hacer uso de un certificado de firma electrónica revocado.

- La falta de una Autoridad de Tiempo digital en Ecuador impide determinar si es real la fecha y hora que presenta un documento firmado con un certificado de firma electrónica. Cada usuario puede aplicar su propia fecha y hora si no se le provee de una infraestructura única de tiempo digital.

Luego de este análisis se recomienda la implementación de una Autoridad de Tiempo en el Ecuador. Con este servicio aumenta la confianza en el uso de certificados de firma electrónica emitidos por la ECIBCE. La finalidad es aportar a la fidelidad de la fecha y hora en que se firmó un documento digital. El proceso de Auditoría dentro de la Gestión de Identidades se fortalece con la existencia de una Autoridad de Tiempo digital en el Ecuador que propone este proyecto de titulación.

Adicionalmente, todos los servicios y registros que ofrece el diseño de la Notaría Digital se regirán a la Autoridad de Tiempo digital que propone este proyecto. Esta Autoridad de Tiempo asegurará una fecha y hora única para la auditoría de la Notaría Digital.

3.1.3 GESTIÓN DE IDENTIDADES PARA LA NOTARÍA DIGITAL

Luego del análisis de los parámetros de Gestión de Identidades se concluye que el diseño utilizará la PKI de la ECIBCE para gestionar identidades en la Notaría Digital. La decisión se toma con base en los beneficios que presenta la PKI de la ECIBCE

frente al estudio que implica implementar una propia PKI que brinde iguales beneficios de directorio de identidades y de seguridad analizados en 3.1.1 y 3.1.2.

El uso de la ECIBCE como gestor de identidades para el presente proyecto de titulación garantiza el manejo de un único directorio de identidades en el Ecuador. Un usuario de la Notaría Digital requiere ser usuario de la ECIBCE previamente. El usuario no necesita registrarse ante la Notaría Digital si ya está registrado ante la ECIBCE. Los certificados de firma electrónica de la ECIBCE admitidos por el diseño de Notaría Digital son: de persona natural, persona jurídica y funcionario público.

La Notaría Digital interactuará con el directorio de identidades de la ECIBCE para obtener información de los usuarios. Esta información permitirá crear cuentas de usuario para la Notaría Digital automáticamente. Las cuentas de usuario creadas por defecto tendrán permisos básicos de Cliente como se menciona en la sección Autorización del diseño del Sistema de Gestión Documental en el subcapítulo 3.3.1.

3.2 DISEÑO DE LOS CINCO TRÁMITES NOTARIALES DIGITALES

En este subcapítulo se diseñan los protocolos para los cinco trámites notariales digitales sobre la base del análisis realizado en el subcapítulo 2.1.2. Este subcapítulo incluye información técnica referente a la firma electrónica y marcas de tiempo en documentación de los trámites notariales digitales. El mecanismo de firmado electrónico en documentos digitales y su validación se explica en el subcapítulo 3.2.1. El mecanismo de marcado de tiempo en documentos digitales se explica en el subcapítulo 3.2.2. El diseño de los cinco trámites notariales digitales mediante casos de uso se desarrolla en el subcapítulo 3.2.3.

3.2.1 FIRMA ELECTRÓNICA EN DOCUMENTOS DIGITALES

En este subcapítulo se explica el procedimiento técnico que se realiza en el lado del Emisor de un documento digital para firmarlo electrónicamente. También se incluye el procedimiento técnico de validación de la firma electrónica en el lado del Receptor

del documento digital firmado electrónicamente. Estos procedimientos identifican a la persona que firmó electrónicamente el documento.

- **Procedimiento de Firma Electrónica**

El procedimiento de firma electrónica en documentos digitales para los trámites de la Notaría Digital funciona de la siguiente manera:

En el lado del Emisor se extrae un resumen único del contenido del documento digital a firmarse. A este resumen único se lo denomina función Hash. El Emisor del documento digital cifra la función Hash con su llave privada. El documento digital más la función Hash cifrada forman el documento digital firmado electrónicamente.

La figura 3.6 muestra el procedimiento de firmado electrónico de documentos digitales.

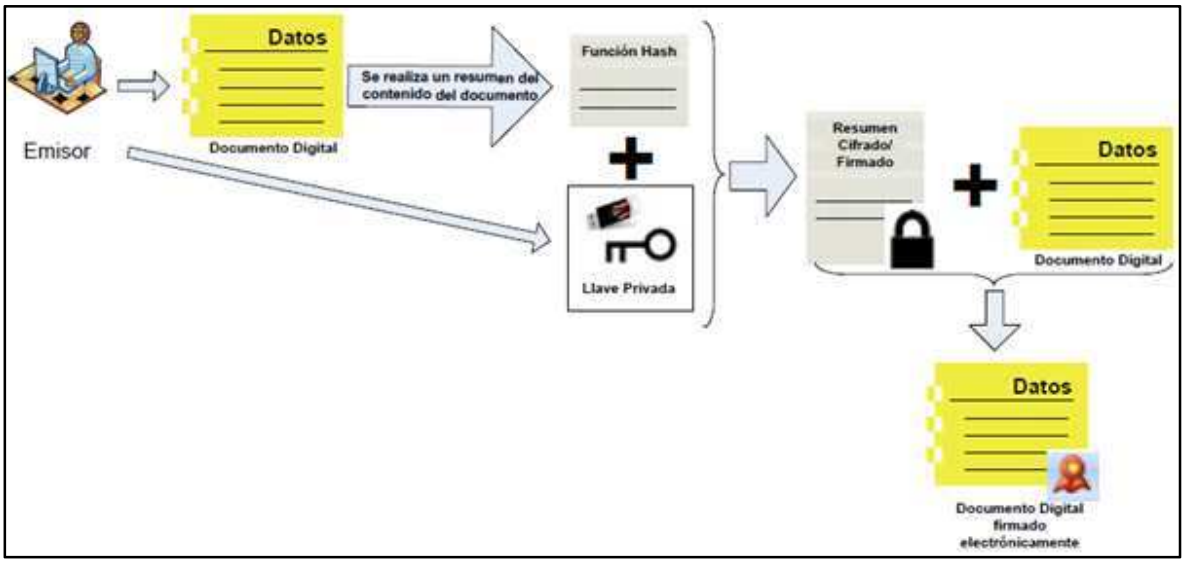

Figura 3.6: Proceso de Firmado Electrónico de Documentos (Fuente: "Uso y Aplicación de la Firma Electrónica en el Ecuador". http://www.eci.bce.ec)

- **Verificación de Firmado Electrónico**

El procedimiento de verificación de firmado electrónico en documentos digitales para los trámites de la Notaría Digital funciona de la siguiente manera:

En el lado del Receptor se separan la función Hash cifrada y el documento digital en texto plano. La función Hash cifrada se descifra con la llave pública del Emisor del documento digital. Se compara la función Hash descifrada con la función Hash del documento digital en texto plano calculada en el lado del Receptor. La firma electrónica se valida solo si coinciden ambas funciones Hash.

La figura 3.7 muestra el procedimiento de verificación de firmado electrónico de documentos digitales.

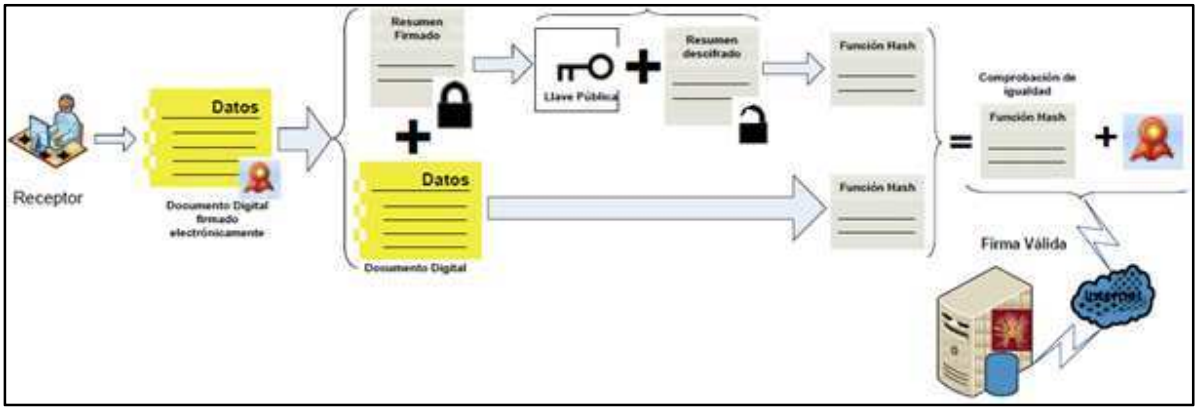

Figura 3.7: Proceso de Verificación de Firmado Electrónico de Documentos (Fuente: "Uso y Aplicación de la Firma Electrónica en el Ecuador". http://www.eci.bce.ec)

3.2.2 MARCAS DE TIEMPO EN DOCUMENTOS DIGITALES

El proceso de marcado de tiempo en documentos digitales para los trámites de la Notaría Digital cuando exista una Autoridad de Marcas de Tiempo (TSA)[27] acreditada en el Ecuador funcionará de la siguiente manera:

En el lado del Emisor se extrae un resumen único del contenido del documento digital. A este resumen único se lo denomina función Hash. La función Hash se envía a la TSA. La TSA añade la marca de tiempo a la función Hash. La marca de tiempo consiste en una operación entre la función Hash y la fecha/hora otorgada por la TSA.

[27] TSA (Time - Stamping Authority). Autoridad de Marcas de Tiempo.- Autoridad de Confianza que ofrece el servicio de Marcado de Tiempo especificado en el RFC 3161. (Fuente: http://www.ietf.org/rfc/rfc3161.txt, http://www.opentsa.org/)

La autenticidad de la TSA se consigue con el cifrado de la marca de tiempo con la llave privada de la TSA. Esta marca de tiempo firmada por la TSA se retorna al Emisor para que se adjunte al documento digital. La figura 3.9 muestra el proceso de generación de marcas de tiempo por una TSA.

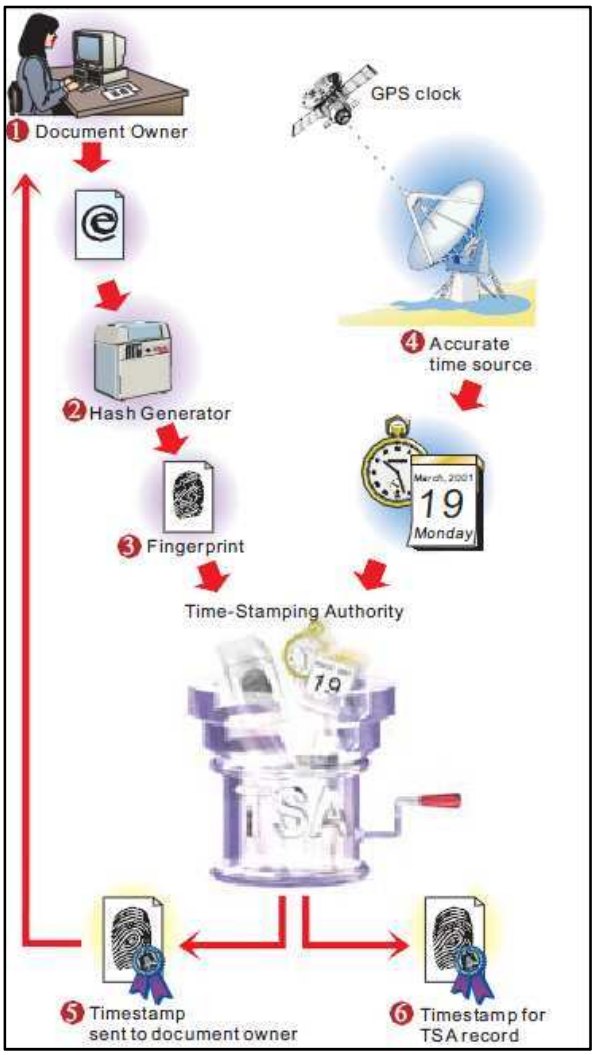

Figura 3.8: Pasos de la generación de marcas de tiempo (Fuente: "Open Secure Time-Stamping Platform". http://www.e-timestamping.com/itf_eng.pdf)

3.2.3 PROTOCOLOS PARA LOS CINCO TRÁMITES NOTARIALES DIGITALES

En este subcapítulo se muestra el diseño de los protocolos para la realización de cinco trámites notariales de manera distribuida en la Notaría Digital. Los requisitos

previos para todos los trámites notariales digitales se definen en el subcapítulo 3.2.3.1. Los casos de uso de los protocolos para los cinco trámites notariales se diseñan desde el subcapítulo 3.2.3.2. Los casos de uso toman en cuenta la gestión de identidades que se definió en el subcapítulo 3.1.3.

3.2.3.1 Requisitos para todos los trámites notariales digitales

Los trámites notariales digitales diseñados desde el subcapítulo 3.2.3.2 requieren precondiciones comunes para todos los protocolos. A fin de evitar la repetición de estos requisitos en cada protocolo se optó por describirlos en esta sección. El diseño de los protocolos para los cinco trámites notariales digitales toma en cuenta las siguientes precondiciones:

- El registro ante la ECIBCE es requisito indispensable para la realización de los trámites notariales digitales.
- Todos los usuarios se autentican ante el sitio Web seguro de la Notaría Digital mediante su certificado de firma electrónica adquirido en la ECIBCE.
- Los funcionarios de la Notaría Digital acceden al sitio Web seguro desde el inicio de sus labores diarias para cumplir con las funciones en las solicitudes de los trámites notariales digitales de los Clientes.
- Los usuarios disponen de un ordenador individual para interactuar con el protocolo de los trámites notariales digitales.
- La firma electrónica en documentos notariales digitales reemplaza el sumillado descrito en el análisis de requerimientos. El asunto en la firma electrónica sustituye la impresión y firma de concuerdos.
- El procedimiento de firmado electrónico en los documentos de los trámites notariales digitales incluye el marcado de tiempo acorde al procedimiento descrito en 3.2.2. Los documentos digitales mencionados en los casos de uso de la figura 3.9 estarán con la marca de tiempo si se hallan firmados electrónicamente.

La figura 3.9 de casos de uso recrea la interacción entre los participantes de los trámites notariales en el mundo digital. El usuario Administrador del Sistema no interacciona con ningún caso de uso. La explicación de sus funciones se mencionará en la sección Autorización del subcapítulo 3.3.1.

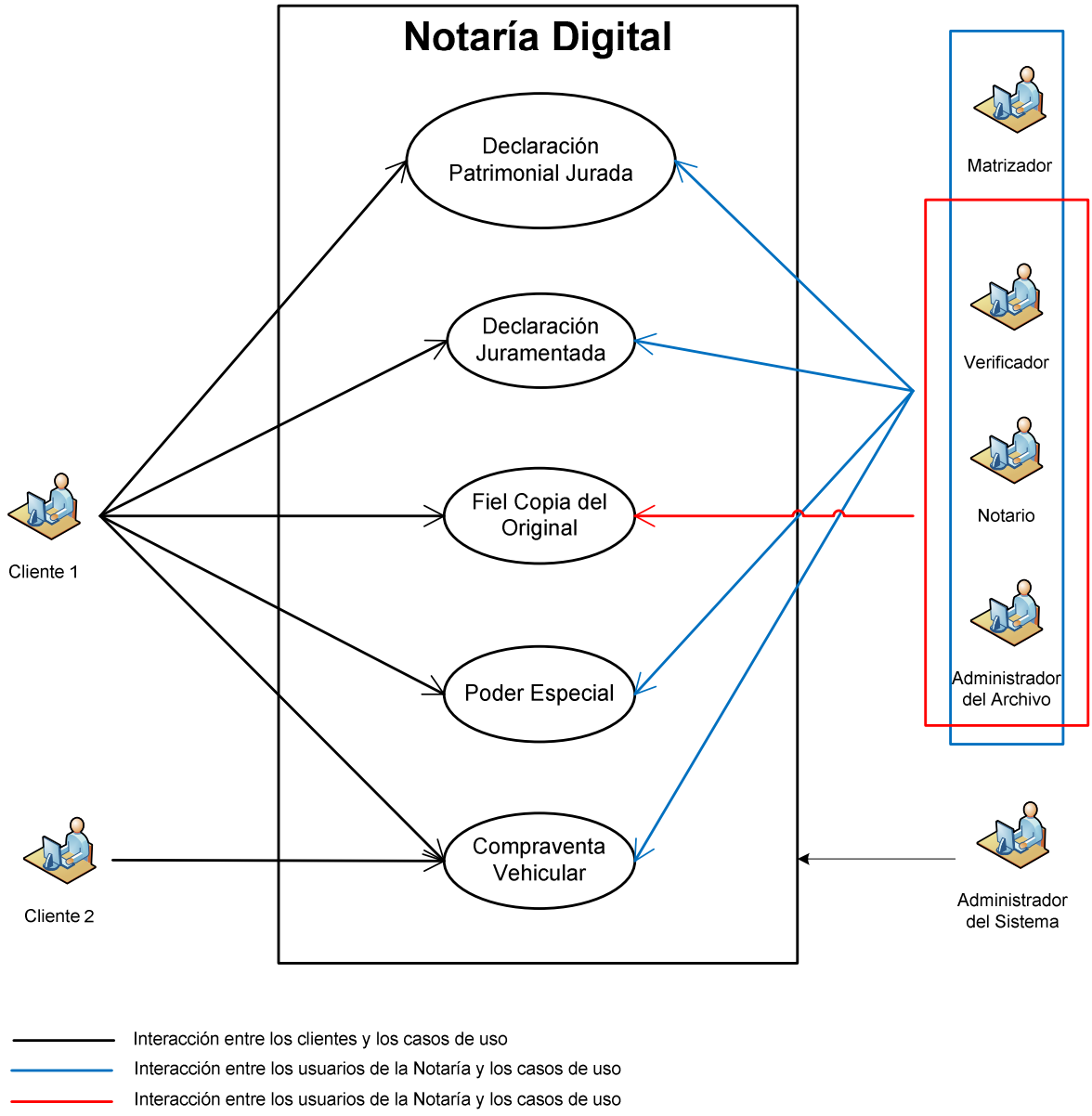

Figura 3.9: Casos de Uso de la Notaría Digital

3.2.3.2 Trámite Declaración Patrimonial Jurada

UC-0001	**Declaración Patrimonial Jurada**	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial digital Declaración Patrimonial Jurada se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría Digital.	
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente	
Precondición	El Cliente posee lleno y firmado electrónicamente el Formulario digital de la Contraloría General del Estado para la Declaración Patrimonial Jurada.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente se autentica en la Notaría Digital con su certificado de firma electrónica emitido por la ECIBCE.
	2	El Cliente selecciona el trámite “Declaración Patrimonial Jurada” en la Notaría Digital.
	3	El Cliente redacta un mensaje con la solicitud del trámite notarial digital de Declaración Patrimonial Jurada y adjunta el Formulario digital en la solicitud.

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada

UC-0001	Declaración Patrimonial Jurada	
Secuencia normal	**Paso**	**Acción**
	4	El Cliente envía el mensaje con su solicitud del trámite notarial digital de Declaración Patrimonial Jurada a la cuenta del Verificador.
	5	El Verificador lee la solicitud del Cliente y descarga el Formulario digital de Declaración Patrimonial Jurada para revisar la validez.
	6	El Verificador constata la identidad del Cliente mediante la comparación entre la cuenta del Emisor del trámite y el titular de la firma electrónica incluida en el Formulario digital de Declaración Patrimonial Jurada.
	7	El Verificador reasigna el Formulario digital de Declaración Patrimonial Jurada a la cuenta del Matrizador.
	8	El Matrizador descarga el Formulario digital de Declaración Patrimonial Jurada, sobre la base del cual redacta la matriz y la revisa.
	9	El Matrizador adjunta la matriz digital de Declaración Patrimonial Jurada y redacta el mensaje para informar al Cliente que firme la matriz adjunta si está de acuerdo con su contenido.
	10	El Matrizador envía a la cuenta del Cliente el mensaje con la matriz digital adjunta de Declaración Patrimonial Jurada.
	11	El Cliente lee el mensaje del Matrizador, descarga la matriz digital de Declaración Patrimonial Jurada, la revisa y la firma electrónicamente.

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada (Continuación)

UC-0001	Declaración Patrimonial Jurada	
Secuencia normal	**Paso**	**Acción**
	12	El Cliente adjunta la matriz digital de Declaración Patrimonial Jurada firmada electrónicamente y redacta el mensaje para informar que ha firmado la matriz.
	13	El Cliente envía el mensaje a la cuenta del Verificador con la matriz digital adjunta de Declaración Patrimonial Jurada firmada electrónicamente.
	14	El Verificador lee el mensaje, descarga la matriz digital de Declaración Patrimonial Jurada firmada por el Cliente y la revisa.
	15	El Verificador reasigna el mensaje del Cliente a la cuenta del Notario. Adicionalmente adjunta el Formulario de Declaración Patrimonial Jurada del Cliente descargado en el paso 5.
	16	El Notario lee el mensaje, descarga el Formulario y la matriz digital de Declaración Patrimonial Jurada. Firma electrónicamente la matriz. Esta matriz firmada por el Notario se convierte en la Escritura Pública digital de Declaración Patrimonial Jurada del Cliente.
	17	El Notario firma nuevamente dos Escrituras Públicas digitales de Declaración Patrimonial Jurada indicando en el asunto de la firma electrónica el concuerdo con el número de copia que genera.
	18	El Notario envía a la cuenta del Cliente las dos Escrituras Públicas digitales de Declaración Patrimonial Jurada que contienen la doble firma del Notario junto con un Formulario del Cliente que es el documento habilitante.

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada (Continuación)

UC-0001	Declaración Patrimonial Jurada	
Secuencia normal	**Paso**	**Acción**
	19	El Cliente descarga las dos Escrituras Públicas digitales de Declaración Patrimonial Jurada y el Formulario que se encuentran en la cuenta del Cliente.
	20	El Notario redacta un mensaje para el Administrador del Archivo y adjunta la Escritura Pública digital generada en el paso 16 junto con el Formulario digital de Declaración Patrimonial Jurada.
	21	El Notario envía el mensaje redactado a la cuenta del Administrador del Archivo con los documentos digitales adjuntos.
	22	El Administrador del Archivo lee el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital de acuerdo a la organización de los tomos anuales.
Postcondición	El Cliente ha obtenido dos copias notarizadas de la Escritura Pública digital de su Declaración Patrimonial Jurada junto con su Formulario digital de la Contraloría General del Estado que actúa como documento habilitante.	
Excepciones	**Paso**	**Acción**
	1	Si el certificado de firma electrónica no es válido en el Directorio de la ECIBCE, la Notaría Digital no autentica al Cliente y el trámite notarial digital se termina.

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada (Continuación)

UC-0001	Declaración Patrimonial Jurada	
Excepciones	**Paso**	**Acción**
	5	Si el Cliente no adjuntó el Formulario de Declaración Patrimonial Jurada o existen errores, el Verificador le responde indicando el inconveniente y se termina el trámite notarial digital.
	6	Si existen inconvenientes en la identidad del Cliente, el Verificador le responde indicando el problema y se termina el trámite notarial digital.
	11	Si el Cliente está inconforme con el contenido de la matriz digital, notifica al Matrizador las observaciones.
	11.a	El Matrizador corrige las observaciones requeridas por el Cliente, redacta una nueva matriz y se la envía al Cliente
	11.b	El Cliente descarga la nueva matriz digital de Declaración Patrimonial Jurada, la revisa y la firma electrónicamente.
	14	Si el contenido o la firma electrónica de la matriz digital de Declaración Patrimonial Jurada no coinciden con el Formulario descargado en el paso 5 de la secuencia normal, el Verificador informa al Cliente el inconveniente.
	14.a	El Cliente corrige el error y envía la documentación correcta.
	14.b	El Verificador revisa la nueva documentación enviada por el Cliente.

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada (Continuación)

UC-0001	Declaración Patrimonial Jurada	
Excepciones	**Paso**	**Acción**
	19	Si el Cliente detecta que el Notario no adjuntó el Formulario del Cliente, no envió dos Escrituras Públicas digitales de Declaración Patrimonial Jurada, no están doblemente firmadas o poseen el mismo concuerdo, informa al Notario el inconveniente.
	19.a	El Notario corrige los inconvenientes y envía a la cuenta del Cliente la documentación solicitada.
	19.b	El Cliente descarga el Formulario y las dos Escrituras Públicas digitales de Declaración Patrimonial Jurada con la doble firma del Notario.
	22	Si el Administrador del Archivo constata que el Notario no adjuntó la Escritura Pública o el Formulario digital de Declaración Patrimonial Jurada, le informa el inconveniente.
	22.a	El Notario corrige el error y adjunta la Escritura Pública y el Formulario digital de Declaración Patrimonial Jurada.
	22.b	El Administrador del Archivo revisa el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital.
Frecuencia esperada	100 veces por mes.	

Tabla 3.5: Caso de Uso Declaración Patrimonial Jurada (Continuación)

3.2.3.3 Trámite Declaración Juramentada

UC-0002	**Declaración Juramentada**	
Versión	1.0 (15/05/2010)	
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear	
Descripción	El trámite notarial digital Declaración Juramentada se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría Digital.	
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente	
Precondición	El Cliente posee el documento digital firmado electrónicamente con el texto a declarar.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente se autentica en la Notaría Digital con su certificado de firma electrónica emitido por la ECIBCE.
	2	El Cliente selecciona el trámite “Declaración Juramentada” en la Notaría Digital.
	3	El Cliente redacta un mensaje con la solicitud del trámite notarial digital de Declaración Juramentada y adjunta el documento digital en la solicitud.
	4	El Cliente envía el mensaje con su solicitud del trámite notarial digital de Declaración Patrimonial Jurada a la cuenta del Verificador.

Tabla 3.6: Caso de Uso Declaración Juramentada

UC-0002	Declaración Juramentada	
Secuencia normal	**Paso**	**Acción**
	5	El Verificador lee la solicitud del Cliente y descarga el documento digital de Declaración Juramentada para revisar la validez.
	6	El Verificador revisa la legalidad del documento digital con el texto a declarar. (La legalidad está basada según las atribuciones que se citan en el Art.18 de la Ley Notarial.)
	7	El Verificador revisa la ortografía del documento digital con el texto a declarar presentado por el Cliente.
	8	El Verificador constata la identidad del Cliente mediante la comparación entre la cuenta del Emisor del trámite y el titular de la firma electrónica incluida en el documento digital con el texto a declarar.
	9	El Verificador reasigna el documento digital con el texto a declarar a la cuenta del Matrizador.
	10	El Matrizador descarga el documento digital con el texto a declarar, sobre la base del cual redacta la matriz y la revisa.
	11	El Matrizador adjunta la matriz digital de Declaración Juramentada y redacta el mensaje para informar al Cliente que firme la matriz adjunta si está de acuerdo con su contenido.
	12	El Matrizador envía a la cuenta del Cliente el mensaje con la matriz digital adjunta de Declaración Juramentada.
	13	El Cliente lee el mensaje del Matrizador, descarga la matriz digital de Declaración Juramentada, la revisa y la firma electrónicamente.

Tabla 3.6: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Secuencia normal	**Paso**	**Acción**
	14	El Cliente adjunta la matriz digital de Declaración Juramentada firmada electrónicamente y redacta el mensaje para informar que ha firmado la matriz.
	15	El Cliente envía el mensaje a la cuenta del Verificador con la matriz digital adjunta de Declaración Juramentada firmada electrónicamente.
	16	El Verificador lee el mensaje, descarga la matriz digital de Declaración Juramentada firmada por el Cliente y la revisa.
	17	El Verificador reasigna el mensaje del Cliente a la cuenta del Notario.
	18	El Notario lee el mensaje, descarga la matriz digital de Declaración Juramentada. Firma electrónicamente la matriz. Esta matriz firmada por el Notario se convierte en la Escritura Pública digital de Declaración Juramentada del Cliente.
	19	El Notario firma nuevamente dos Escrituras Públicas digitales de Declaración Juramentada indicando en el asunto de la firma electrónica el concuerdo con el número de copia que genera.
	20	El Notario envía a la cuenta del Cliente las dos Escrituras Públicas digitales de Declaración Juramentada que contienen la doble firma del Notario.
	21	El Cliente descarga las dos Escrituras Públicas digitales de Declaración Juramentada que se encuentra en la cuenta del Cliente.

Tabla 3.6: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Secuencia normal	**Paso**	**Acción**
	22	El Notario redacta un mensaje para el Administrador del Archivo y adjunta la Escritura Pública digital de Declaración Juramentada del Cliente.
	23	El Notario envía el mensaje redactado a la cuenta del Administrador del Archivo con la Escritura Pública digital de Declaración Juramentada del Cliente
	24	El Administrador del Archivo lee el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital de acuerdo a la organización de los tomos anuales.
Postcondición	El Cliente ha obtenido dos copias notarizadas de la Escritura Pública digital de su Declaración Juramentada.	
Excepciones	**Paso**	**Acción**
	1	Si el certificado de firma electrónica no es válido en el Directorio de la ECIBCE, la Notaría Digital no autentica al Cliente y el trámite notarial digital se termina.
	5	Si el Cliente no adjuntó el documento digital con el texto a declarar o existen errores, el Verificador le responde indicando el inconveniente y se termina el trámite notarial digital.
	6	Si el documento digital con el texto a declarar es ilegal, el Verificador notifica al Cliente y se termina el trámite notarial digital.
	7	Si existen errores ortográficos en el documento digital con el texto a declarar, el Verificador envía a corregir al Cliente y se termina el trámite notarial digital.

Tabla 3.6: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Excepciones	**Paso**	**Acción**
	8	Si existen inconvenientes en la identidad del Cliente, el Verificador le responde indicando el problema y se termina el trámite notarial digital.
	13	Si el Cliente está inconforme con el contenido de la matriz digital, notifica al Matrizador las observaciones.
	13.a	El Matrizador corrige las observaciones requeridas por el Cliente, redacta una nueva matriz y se la envía al Cliente
	13.b	El Cliente descarga la nueva matriz digital de Declaración Juramentada, la revisa y la firma electrónicamente.
	16	Si el contenido o la firma electrónica de la matriz de Declaración Juramentada no coinciden con el documento digital con el texto a declarar descargado en el paso 5 de la secuencia normal, el Verificador informa al Cliente el inconveniente.
	16.a	El Cliente corrige el error y envía la documentación correcta.
	16.b	El Verificador revisa la nueva documentación enviada por el Cliente.
	21	Si el Cliente detecta que el Notario no adjuntó las dos Escrituras Públicas digitales de Declaración Juramentada, no están doblemente firmadas o poseen el mismo concuerdo, informa al Notario el inconveniente.
	21.a	El Notario corrige los inconvenientes y envía a la cuenta del Cliente la documentación solicitada.

Tabla 3.6: Caso de Uso Declaración Juramentada (Continuación)

UC-0002	Declaración Juramentada	
Excepciones	**Paso**	**Acción**
	21.b	El Cliente las dos Escrituras Públicas digitales de Declaración Juramentada con la doble firma del Notario.
	24	Si el Administrador del Archivo constata que el Notario no adjuntó la Escritura Pública le informa el inconveniente.
	24.a	El Notario corrige el error y adjunta la Escritura Pública de Declaración Juramentada.
	24.b	El Administrador del Archivo revisa el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital.
Frecuencia esperada	25 veces por mes.	

Tabla 3.6: Caso de Uso Declaración Juramentada (Continuación)

3.2.3.4 Trámite Poder Especial

UC-0003	Poder Especial
Versión	1.0 (15/05/2010)
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear
Descripción	El trámite notarial digital Poder Especial se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría Digital.

Tabla 3.7: Caso de Uso Poder Especial

UC-0003	Poder Especial	
Actores	Notario Verificador Matrizador Administrador del Archivo Cliente	
Precondición	El Cliente posee la Minuta digital de Poder Especial elaborada y firmada electrónicamente por un abogado.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente se autentica en la Notaría Digital con su certificado de firma electrónica emitido por la ECIBCE.
	2	El Cliente selecciona el trámite “Poder Especial” en la Notaría Digital.
	3	El Cliente redacta un mensaje con la solicitud del trámite notarial digital de Declaración Patrimonial Jurada y adjunta la Minuta digital del Poder Especial.
	4	El Cliente envía el mensaje con su solicitud del trámite notarial digital de Poder Especial a la cuenta del Verificador.
	5	El Verificador lee la solicitud del Cliente y descarga Minuta digital de Poder Especial para revisar la validez.
	6	El Verificador constata la identidad del Cliente mediante la comparación entre la cuenta del Emisor del trámite y los datos que se encuentran en la Minuta digital de Poder Especial.
	7	El Verificador reasigna la Minuta digital de Poder Especial a la cuenta del Matrizador.

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Secuencia normal	**Paso**	**Acción**
	8	El Matrizador descarga la Minuta digital de Poder Especial, sobre la base del cual redacta la matriz digital y la revisa.
	9	El Matrizador adjunta la matriz digital de Poder Especial y redacta el mensaje para informar al Cliente que firme la matriz adjunta si está de acuerdo con su contenido.
	10	El Matrizador envía a la cuenta del Cliente el mensaje con la matriz digital adjunta de Poder Especial.
	11	El Cliente lee el mensaje del Matrizador, descarga la matriz digital de Poder Especial, la revisa y la firma electrónicamente.
	12	El Cliente adjunta la matriz digital de Poder Especial firmada electrónicamente y redacta el mensaje para informar que ha firmado la matriz digital.
	13	El Cliente envía el mensaje a la cuenta del Verificador con la matriz digital adjunta de Poder Especial firmada electrónicamente.
	14	El Verificador lee el mensaje, descarga la matriz digital de Poder Especial firmada por el Cliente y la revisa.
	15	El Verificador reasigna el mensaje del Cliente a la cuenta del Notario. Adicionalmente adjunta la Minuta digital de Poder Especial descargada en el paso 5 de la secuencia normal.

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Secuencia normal	**Paso**	**Acción**
	16	El Notario lee el mensaje, descarga la Minuta digital y la matriz digital de Poder Especial. Firma electrónicamente la matriz. Esta matriz digital firmada por el Notario se convierte en la Escritura Pública digital de Poder Especial.
	17	El Notario firma nuevamente dos Escrituras Públicas digitales de Poder Especial indicando en el asunto de la firma electrónica el concuerdo con el número de copia que genera.
	18	El Notario envía a la cuenta del Cliente las dos Escrituras Públicas digitales de Poder Especial que contienen la doble firma del Notario.
	19	El Cliente descarga las dos Escrituras Públicas digitales de Poder Especial.
	20	El Notario redacta un mensaje para el Administrador del Archivo y adjunta la Escritura Pública digital generada en el paso 16 de la secuencia normal.
	21	El Notario envía el mensaje redactado a la cuenta del Administrador del Archivo con los documentos digitales adjuntos.
	22	El Administrador del Archivo lee el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital de acuerdo a la organización de los tomos anuales.
	23	El Notario redacta un mensaje para el Administrador del Archivo y adjunta la Minuta digital de Poder Especial.

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Secuencia normal	**Paso**	**Acción**
	24	El Notario envía el mensaje redactado a la cuenta del Administrador del Archivo con la Minuta digital de Poder Especial adjunta.
	25	El Administrador del Archivo lee el mensaje y lo almacena en el Protocolo de Minutas del archivo notarial digital de acuerdo a la organización de los tomos anuales.
Postcondición	El Cliente ha obtenido dos copias de la Escritura Pública digital de su Poder Especial.	
Excepciones	**Paso**	**Acción**
	1	Si el certificado de firma electrónica no es válido en el Directorio de la ECIBCE, la Notaría Digital no autentica al Cliente y el trámite notarial digital se termina.
	5	Si el Cliente no adjuntó la Minuta digital de Poder Especial, el Verificador le responde indicando el inconveniente y se termina el trámite notarial digital.
	6	Si existen inconvenientes en la identidad del Cliente, el Verificador le responde indicando el problema y se termina el trámite notarial digital.
	11	Si el Cliente está inconforme con el contenido de la matriz digital, notifica al Matrizador las observaciones.
	11.a	El Matrizador corrige las observaciones requeridas por el Cliente, redacta una nueva matriz digital y se la envía al Cliente

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Excepciones	**Paso**	**Acción**
	11.b	El Cliente descarga la nueva matriz digital de Poder Especial, la revisa y la firma electrónicamente.
	14	Si el contenido o la firma electrónica de la matriz digital de Poder Especial no coinciden con la Minuta digital descargada en el paso 5 de la secuencia normal, el Verificador informa al Cliente el inconveniente.
	14.a	El Cliente corrige el error y envía la documentación correcta.
	14.b	El Verificador revisa la nueva documentación enviada por el Cliente.
	19	Si el Cliente detecta que el Notario no adjuntó las dos Escrituras Públicas digitales de Poder Especial, no están doblemente firmadas o poseen el mismo concuerdo, informa al Notario el inconveniente.
	19.a	El Notario corrige los inconvenientes y envía a la cuenta del Cliente la documentación solicitada.
	19.b	El Cliente descarga las dos Escrituras Públicas digitales de Poder Especial con la doble firma del Notario.
	22	Si el Administrador del Archivo constata que el Notario no adjuntó la Escritura Pública de Poder Especial, le informa el inconveniente.
	22.a	El Notario corrige el error y adjunta la Escritura Pública digital de Poder Especial.

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

UC-0003	Poder Especial	
Excepciones	**Paso**	**Acción**
	22.b	El Administrador del Archivo revisa el mensaje y lo almacena en el Protocolo de Escrituras Públicas del archivo notarial digital.
	23	Si el Administrador del Archivo constata que el Notario no adjuntó la Minuta digital de Poder Especial, le informa el inconveniente.
	23.a	El Notario corrige el error y adjunta la Minuta digital de Poder Especial.
	23.b	El Administrador del Archivo revisa el mensaje y lo almacena en el Protocolo de Minutas del archivo notarial digital.
Frecuencia esperada	50 veces por mes.	

Tabla 3.7: Caso de Uso Poder Especial (Continuación)

3.2.3.5 Trámite Fiel Copia del Original

UC-0004	Fiel Copia del Original
Versión	1.0 (15/05/2010)
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear
Descripción	El trámite notarial digital Fiel copia del Original se comporta tal como se describe en el siguiente caso de uso cuando un Cliente solicite el trámite en la Notaría Digital.

Tabla 3.8: Caso de Uso Fiel Copia del Original

UC-0004	Fiel Copia del Original	
Actores	Notario Verificador Administrador del Archivo Cliente	
Precondición	El Cliente posee el documento digital original firmado electrónicamente.	
Secuencia normal	**Paso**	**Acción**
	1	El Cliente se autentica en la Notaría Digital con su certificado de firma electrónica emitido por la ECIBCE.
	2	El Cliente selecciona el trámite “Fiel Copia del Original” en la Notaría Digital.
	3	El Cliente redacta un mensaje con la solicitud del trámite notarial digital de Fiel Copia del Original y adjunta el documento digital original en la solicitud.
	4	El Cliente envía el mensaje con su solicitud del trámite notarial digital de Fiel Copia del Original a la cuenta del Verificador.
	5	El Verificador lee la solicitud del Cliente y descarga el documento digital original para revisar su validez.
	6	El Verificador reasigna el mensaje de Fiel Copia del Original del Cliente a la cuenta del Notario.

Tabla 3.8: Caso de Uso Fiel Copia del Original (Continuación)

UC-0004	Fiel Copia del Original	
Secuencia normal	**Paso**	**Acción**
	7	El Notario lee el mensaje y descarga el documento digital original. Firma electrónicamente el documento digital original el número de veces que el Cliente solicitó e indica en el asunto de la firma electrónica el concuerdo. Estos documentos firmados por el Notario se convierten en las copias notarizadas del documento digital original.
	8	El Notario genera una copia notarizada adicional del documento digital original destinada al Libro de Diligencias del archivo notarial digital.
	9	El Notario envía un mensaje a la cuenta del Cliente, con la cantidad requerida de copias notarizadas del documento digital original adjuntas.
	10	El Cliente lee el mensaje del Notario y descarga el número de copias notarizadas solicitadas del documento digital original que se encuentran en las cuentas de ambos Clientes.
	11	El Notario envía un mensaje a la cuenta del Administrador del Archivo con la copia notarizada adicional del documento digital original adjunta.
	12	El Administrador del Archivo lee el mensaje y lo almacena en el Libro de Diligencias del archivo notarial digital de acuerdo a la organización de los tomos anuales.
Postcondición	El Cliente ha obtenido el número de copias notarizadas requeridas del documento digital original.	

Tabla 3.8: Caso de Uso Fiel Copia del Original (Continuación)

UC-0004	Fiel Copia del Original	
Excepciones	**Paso**	**Acción**
	1	Si los certificados de firma electrónica no son válidos en el Directorio de la ECIBCE, la Notaría Digital no autentica al Cliente y el trámite notarial digital se termina.
	5	Si el Cliente no adjuntó el documento digital original o existen errores en el documento, el Verificador le responde indicando el inconveniente y se termina el trámite notarial digital.
	10	Si el Cliente detecta que el Notario no adjuntó el número de copias notarizadas solicitadas del documento digital original, informa al Notario el inconveniente.
	10.a	El Notario corrige los inconvenientes y envía a la cuenta del Cliente el número correcto de copias notarizadas.
	10.b	El Cliente descarga el número correcto de copias notarizadas del documento digital original.
	12	Si el Administrador del Archivo constata que el Notario no adjuntó la copia notarizada adicional del documento digital original, le informa el inconveniente.
	12.a	El Notario corrige el error y adjunta la copia notarizada adicional del documento digital original.
	12.b	El Administrador del Archivo revisa el nuevo mensaje y lo almacena en el Libro de Diligencias del archivo notarial digital de acuerdo a la organización de los tomos anuales
Frecuencia esperada	100 veces por mes.	

Tabla 3.8: Caso de Uso Fiel Copia del Original (Continuación)

3.2.3.6 Trámite Compraventa Vehicular

La Notaría podrá confirmar la veracidad de la información presentada por el Vendedor para realizar el trámite notarial digital de Compraventa Vehicular. La comprobación se realizará mediante el Sistema Nacional de Registro de Datos Públicos. La Notaría podrá acceder a información de los registros de la propiedad y vehicular del cliente que actúe como Vendedor. El trámite notarial digital de Compraventa Vehicular se analiza con solo con un Comprador y un Vendedor. El trámite notarial digital se considera un reconocimiento de firmas del Contrato de Compraventa Vehicular.

UC-0005	**Compraventa Vehicular**
Versión	1.0 (15/05/2010)
Autores	Arsenio Antonio Aguirre Ponce Pablo Rodrigo Carchi Alvear
Descripción	El trámite notarial digital Compraventa Vehicular se comporta tal como se describe en el siguiente caso de uso cuando un Comprador o Vendedor de un vehículo solicite el trámite en la Notaría Digital.
Actores	Notario Verificador Matrizador Administrador del Archivo Comprador del vehículo Vendedor del vehículo
Precondición	El Comprador o Vendedor del vehículo poseen un Contrato digital de Compraventa Vehicular firmado electrónicamente por ambos Clientes.

Tabla 3.9: Caso de Uso Compraventa Vehicular

UC-0005	Compraventa Vehicular	
Secuencia normal	**Paso**	**Acción**
	1	El Comprador y Vendedor se autentican en la Notaría Digital con su certificado de firma electrónica emitido por la ECIBCE.
	2	El Comprador selecciona el trámite “Compraventa Vehicular” en la Notaría Digital.
	3	El Comprador redacta un mensaje con la solicitud del trámite notarial digital de Compraventa Vehicular y adjunta el Contrato digital en la solicitud.
	4	El Comprador envía el mensaje con su solicitud del trámite notarial digital de Compraventa Vehicular a la cuenta del Verificador.
	5	El Verificador lee la solicitud del Comprador y descarga el Contrato digital de Compraventa Vehicular para constatar las identidades del Comprador y Vendedor. La identidad del Comprador se verifica mediante la comparación entre la cuenta del Emisor del trámite, el nombre y el titular de la firma electrónica del Comprador que consta en el Contrato digital. La identidad del Vendedor se verifica mediante la comparación entre el nombre y el titular de la firma electrónica del Vendedor que consta en el Contrato digital.
	6	El Verificador reasigna el Contrato digital de Compraventa Vehicular a la cuenta del Matrizador.
	7	El Matrizador descarga el Contrato digital de Compraventa Vehicular, sobre la base del cual redacta el Acta y la revisa.

Tabla 3.9: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Secuencia normal	**Paso**	**Acción**
	8	El Matrizador adjunta el Acta digital de Compraventa Vehicular y redacta el mensaje para informar al Comprador que firme el Acta adjunta si está de acuerdo con su contenido.
	9	El Matrizador envía a la cuenta del Comprador el mensaje con el Acta digital adjunta de Compraventa Vehicular.
	10	El Comprador lee el mensaje del Matrizador, descarga el Acta digital de Compraventa Vehicular, la revisa y la firma electrónicamente.
	11	El Comprador adjunta el Acta digital de Compraventa Vehicular firmada electrónicamente y redacta el mensaje para informar que ha firmado el Acta.
	12	El Comprador envía el mensaje a la cuenta del Vendedor del Vehículo con el Acta digital adjunta de Compraventa Vehicular firmada electrónicamente.
	13	El Vendedor lee el mensaje del Comprador, descarga el Acta digital de Compraventa Vehicular firmada por el Comprador, la revisa y la firma electrónicamente.
	14	El Vendedor adjunta el Acta digital de Compraventa Vehicular firmada electrónicamente por ambos Clientes y redacta el mensaje para informar que ha firmado el Acta.
	15	El Vendedor envía el mensaje a la cuenta del Verificador con el Acta digital adjunta de Compraventa Vehicular firmada electrónicamente por ambos Clientes.

Tabla 3.9: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Secuencia normal	**Paso**	**Acción**
	16	El Verificador lee el mensaje del Vendedor, descarga el Acta digital de Compraventa Vehicular firmada por ambos Clientes y la revisa.
	17	El Verificador reasigna el mensaje del Vendedor a la cuenta del Notario. Adicionalmente adjunta el Contrato digital de Compraventa Vehicular descargado en el paso 5.
	18	El Notario lee el mensaje, descarga el Contrato y el Acta digital de Compraventa Vehicular. Firma electrónicamente el Acta e incluye el concuerdo. Esta Acta firmada por el Notario se convierte en el Acta digital notarizada de Compraventa Vehicular.
	19	El Notario envía un mensaje a las cuentas del Comprador y Vendedor, con el Contrato y el Acta digital notarizada de Compraventa Vehicular adjuntos.
	20	El Comprador y el Vendedor leen el mensaje y descargan el Contrato y el Acta digital notarizada de Compraventa Vehicular que se encuentran en las cuentas de ambos Clientes.
	21	El Notario envía un mensaje a la cuenta del Administrador del Archivo con el Contrato y el Acta digital notarizada de Compraventa Vehicular adjuntos.
	22	El Administrador del Archivo lee el mensaje y lo almacena en el Libro de Diligencias del archivo notarial digital de acuerdo a la organización de los tomos anuales.

Tabla 3.9: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Postcondición	El Comprador y Vendedor han obtenido un Contrato y un Acta digital notarizada de Compraventa Vehicular.	
Excepciones	**Paso**	**Acción**
	1	Si los certificados de firma electrónica no son válidos en el Directorio de la ECIBCE, la Notaría Digital no autentica a los Clientes y el trámite notarial digital se termina.
	5	Si el Comprador no adjuntó el Contrato de Compraventa Vehicular o existen errores en la validación de las identidades, el Verificador le responde indicando el inconveniente y se termina el trámite notarial digital.
	10	Si el Comprador está inconforme con el contenido del Acta, notifica al Matrizador las observaciones.
	10.a	El Matrizador corrige las observaciones requeridas por el Cliente, redacta una nueva Acta y se la envía al Comprador.
	10.b	El Comprador descarga la nueva Acta digital de Compraventa Vehicular, la revisa y la firma electrónicamente.
	13	Si el Vendedor está inconforme con el contenido del Acta, notifica al Matrizador las observaciones.
	13.a	El Matrizador corrige las observaciones requeridas por el Vendedor, redacta una nueva Acta y se la envía al Comprador.
	13.b	El caso de uso continúa en el paso 10 de la secuencia normal.

Tabla 3.9: Caso de Uso Compraventa Vehicular (Continuación)

UC-0005	Compraventa Vehicular	
Excepciones	**Paso**	**Acción**
	16	Si el contenido o las firmas electrónicas del Acta de Compraventa Vehicular no coinciden con el Contrato descargado en el paso 5, el Verificador informa al Comprador el inconveniente.
	16.a	El caso de uso continúa en el paso 10 de la secuencia normal.
	20	Si el Comprador o el Vendedor detectan que el Notario no adjuntó el Contrato o el Acta digital notarizada de Compraventa, informa al Notario el inconveniente.
	20.a	El Notario corrige los inconvenientes y envía la documentación solicitada a la cuenta del Cliente que presentó el problema.
	20.b	El Comprador o Vendedor descarga el Contrato o el Acta digital notarizada de Compraventa.
	22	Si el Administrador del Archivo constata que el Notario no adjuntó el Contrato o el Acta digital notarizada de Compraventa, le informa el inconveniente.
	22.a	El Notario corrige el error y adjunta el Contrato o el Acta digital notarizada de Compraventa.
	22.b	El Administrador del Archivo revisa el mensaje y lo almacena en el Libro de Diligencias del archivo notarial digital de acuerdo a la organización de los tomos anuales
Frecuencia esperada	100 veces por mes.	

Tabla 3.9: Caso de Uso Compraventa Vehicular (Continuación)

3.3 SISTEMA DE GESTIÓN DOCUMENTAL

En este subcapítulo se describe el diseño del Sistema de Gestión Documental para la Notaría Digital. El Sistema de Gestión Documental se basa en las especificaciones que cumplan los requerimientos del análisis realizado en el subcapítulo 2.2.2. El diseño del Sistema de Gestión Documental se enfoca en ofrecer organización, control de acceso y seguridad a los documentos electrónicos generados por los trámites notariales digitales y almacenados en el archivo notarial digital. En este subcapítulo la redacción se realiza desde una perspectiva operativa, es decir, qué parámetros deberá garantizar el Sistema de Gestión Documental hacia el usuario desde que se autentica hasta que se archiva la documentación generada por los trámites notariales digitales. Estos parámetros de seguridad se definen en el subcapítulo 3.3.1. El Sistema de Gestión Documental incluye el diseño de las opciones mínimas requeridas para su desarrollo en el subcapítulo 3.3.2.

3.3.1 SEGURIDAD

En este subcapítulo se diseña la seguridad que requiere el documento notarial electrónico y el archivo notarial digital del Sistema de Gestión Documental de la Notaría Digital. La seguridad del Sistema de Gestión Documental se consigue mediante ciertos parámetros. Estos parámetros formarán parte íntegra del documento notarial digital. El diseño adopta la recomendación de Adobe[28] que propone incluir los siguientes seis criterios mostrados en la Figura 3.10 para proteger documentación electrónica.

[28] A primer on electronic document security. (Fuente: http://www.adobe.com/security/pdfs/acrobat_livecycle_security_wp.pdf)

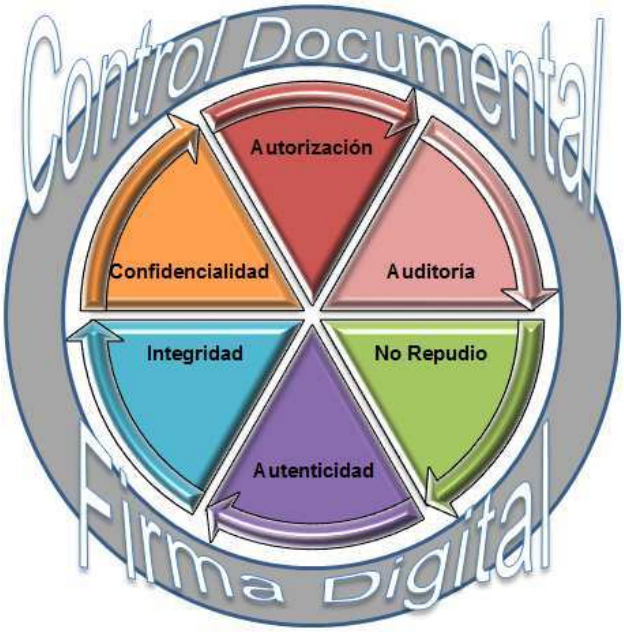

Figura 3.10: Seis criterios clave para proveer seguridad documental según Adobe

- **Confidencialidad**

  El documento notarial digital es de carácter público. No se dispondrá de cifrado para permitir que el documento digital pueda ser leído por quien lo requiera. El control de acceso al archivo notarial digital se consigue mediante los permisos sobre las cuentas de usuario descritas en el ítem de Autorización. El Sistema de Gestión Documental admitirá el acceso al archivo notarial digital solo al Notario y al Administrador del Archivo. El control de acceso físico se logra mediante la restricción de ingreso a las instalaciones de la Notaría donde se almacene el servidor del Sistema de Gestión Documental.

- **Autorización**

  Los documentos notariales digitales solo tendrán permisos de lectura para todos los usuarios. No se permitirá su edición. No habrá permisos para copiar el contenido del documento digital. No se podrá imprimir el documento a fin de mantener su naturaleza digital y perder su validez legal. El documento notarial digital permitirá la firma electrónica de varios actores para cumplir los requerimientos de los protocolos de los trámites notariales digitales.

  El usuario cuyo certificado de firma electrónica no se encuentre en la lista de certificados revocados (CRL) de la ECIBCE está autorizado para firmar los documentos que intervengan en el proceso notarial que desee realizar. El diseño del Sistema de Gestión Documental deberá incluir los siguientes permisos para definir responsabilidades a los usuarios en el Sistema de Gestión Documental de la Notaría Digital. Los permisos también limitan las acciones que se puedan realizar sobre la documentación electrónica en los trámites notariales digitales.

  - *Notario*

    El Notario tendrá acceso total al archivo notarial digital para controlar la consistencia de la documentación digital. Podrá recibir y enviar mensajes electrónicos según el protocolo de los trámites notariales digitales. Podrá reasignar mensajes con documentación firmada electrónicamente al Archivador para que la incluya en el Protocolo.

  - *Administrador del Archivo*

    El Archivador tendrá control total sobre el Protocolo de Escrituras Públicas digitales y el Libro de Diligencias digitales. Recibirá del Notario los mensajes con la documentación firmada electrónicamente para almacenarla en el archivo notarial digital. Se encargará de registrar las acciones realizadas sobre este archivo notarial digital. El Administrador del Archivo creará la estructura del archivo notarial digital en libros, protocolos anuales y tomos mensuales.

- *Verificador y Matrizador*

  El Verificador tendrá permisos para recibir mensajes electrónicos del cliente. Podrá reasignar los mensajes al matrizador o al cliente. El Matrizador podrá recibir solicitudes revisadas por el Verificador y enviar mensajes digitales con las matrices redactadas al cliente. Estos dos usuarios no tendrán acceso al archivo de la Notaría Digital.

- *Administrador del Sistema*

  La función del Administrador será configurar el Sistema de Gestión Documental para habilitar cuentas de usuarios y establecer los permisos a los demás usuarios para que puedan intervenir en el protocolo de los trámites notariales digitales. El Administrador del Sistema tiene la responsabilidad de mantener consistente la información del Sistema de Gestión Documental. Esta cuenta no participa en el protocolo de los trámites notariales digitales.

- *Cliente*

  El Cliente tendrá permisos para enviar y recibir mensajes digitales con la documentación notarial según el protocolo de los trámites notariales digitales. No tendrá acceso al archivo digital de la Notaría.

- **Auditoría**

  El Sistema de Gestión Documental almacenará registros del acceso a la documentación y de las acciones realizadas por los usuarios. Esta auditoría consigue evitar el no repudio ante el uso incorrecto del Sistema de Gestión Documental. El Sistema de Gestión Documental no ofrece control al documento digital luego de ser descargado por el cliente. El objetivo del proyecto no es conocer el uso que se dé al documento digital luego de ser descargado por el usuario. El Sistema de Gestión Documental solo deberá limitarse a ofrecer auditoría al documento notarial digital dentro del archivo de la Notaría Digital.

- **Integridad**

  La integridad del documento notarial digital se consigue mediante la implantación de la firma electrónica. Con esto se evitará que se pueda alterar el contenido del documento notarial digital. Los permisos para el uso del documento digital se describieron en el ítem de Autorización y aportan al mantenimiento de la integridad del documento notarial digital.

  El Sistema de Gestión Documental contará con una base de archivos digitales almacenados en un servidor dedicado. Este servidor de archivos estará localizado en las oficinas de la Notaría. El resguardo del servidor y el control de acceso a las instalaciones estarán bajo responsabilidad del Notario.

- **Autenticidad**

  La autenticidad del documento notarial digital se logra al implantar la firma electrónica. Solo el titular del certificado de firma electrónica podrá implantar su firma electrónica en el documento digital. El receptor podrá identificar a los actores de los documentos de los trámites notariales digitales mediante la firma electrónica incluida en el documento. El usuario autentica al Sistema de Gestión Documental mediante su certificado digital que el browser deberá reconocerlo como válido. El Sistema de Gestión Documental autenticará al usuario mediante su certificado de firma electrónica. El Sistema de Gestión Documental autenticará únicamente los certificados de firma electrónica emitidos por la ECIBCE y validados según la Autorización analizada en el subcapítulo 3.1.2.2.

- **No Repudio**

  La firma electrónica implantada en el documento notarial digital asegura que el firmante no podrá negar las acciones legales que conlleve su firma electrónica. La marca de tiempo impide el no repudio sobre la fecha/hora en que un documento digital fue firmado electrónicamente. El Notario será la autoridad en problemas de no repudio. El diseño considerará original al documento notarial digital que repose en el Sistema de Gestión Documental para inconvenientes de no repudio.

3.3.2 DISEÑO DEL SISTEMA DE GESTIÓN DOCUMENTAL

En este subcapítulo se diseña del Sistema de Gestión Documental para la Notaría Digital. El Sistema de Gestión Documental de la Notaría Digital deberá estar formado por un servicio Web seguro y un servicio de Base de Datos. El servicio Web seguro del Sistema de Gestión Documental facilita la interacción de los usuarios con la Notaría Digital a través de Internet. El diseño propone la implementación del Sistema de Gestión Documental en un entorno seguro, a través del protocolo HTTPS[29] que utiliza el puerto TCP/443. El servicio de Base de Datos deberá contener la estructura del modelo relacional del Sistema de Gestión Documental. La Base de Datos almacenará información referente a: cuentas de usuarios, documentos de trámites notariales digitales, registros de auditoría, entre otra información. Se deberán establecer mecanismos de seguridad para proteger los datos sensibles de esta Base de Datos.

El Sistema de Gestión Documental será la plataforma sobre la cual se realicen los trámites notariales digitales diseñados en el subcapítulo 3.2.3. El Sistema de Gestión Documental además organizará la documentación digital que sea producto de los trámites notariales digitales. Los trámites notariales generarán documentos digitales del tipo PDF. El diseño opta por este formato por considerarse el estándar internacional para documentación digital[30]. Además las herramientas para firmar electrónicamente aceptan este formato. El Sistema de Gestión Documental se conformará de las siguientes opciones para cumplir con los requerimientos de gestión documental analizados en el subcapítulo 2.2.2:

---

[29] HTTPS (HyperText Transfer Protocol Secure).- Es una combinación del protocolo HTTP y protocolos criptográficos. Se emplea para lograr conexiones más seguras en la WWW, (Fuente: http://www.alegsa.com.ar/Dic/https.php)

[30] ISO 32000-1:2008. Document management – Portable document format – Part 1: PDF 1.7 http://www.adobe.com/content/dam/Adobe/en/devnet/acrobat/pdfs/PDF32000_2008.pdf

- **Administración del Sistema de Gestión Documental**

  El Administrador del Sistema será el único autorizado a acceder a esta opción. Esta opción deberá permitirle al Administrador del Sistema importar la información del Directorio de Identidades de la ECIBCE para crear cuentas de usuarios. La opción Administración del Sistema deberá permitir crear roles para asignar a las cuentas de los usuarios de la Notaría Digital. Los roles deberán tener permisos acorde a las funciones que cumplan los usuarios en el Sistema de Gestión Documental. Los roles que defina el Administrador del Sistema no deberán tener permisos para modificar la información del Sistema de Gestión Documental.

- **Reportes del Sistema de Gestión Documental**

  El Sistema de Gestión Documental deberá tener la opción de consultar reportes de acuerdo a los trámites notariales digitales realizados por los clientes y a las necesidades que requiera la Notaría Digital. Los reportes deberán ser activados para el Administrador del Archivo y el Notario.

- **Archivo Notarial Digital**

  La opción Archivo Notarial Digital del Sistema de Gestión Documental almacenará las Escrituras Públicas y Diligencias de la Notaría Digital. Solo el Notario y el Administrador del Archivo deberán tener permisos en su cuenta para gestionar esta opción. El Archivo Notarial Digital deberá estar organizado en Protocolo de Escrituras Públicas digitales y Libro de Diligencias digitales. Estos archivos notariales además se dividirán en tomos anuales para cumplir con la Ley Notarial.

  - ***Protocolo de Escrituras Públicas digitales***

    En este archivo notarial se almacenarán los mensajes que contienen los documentos digitales de Escrituras Públicas como resultados de los trámites notariales digitales. La organización se realizará anualmente mediante tomos mensuales. El índice del Protocolo de Escrituras Públicas digitales se

reemplazará por una opción de búsqueda. Las minutas formarán un archivo especial que el Administrador del Archivo deberá organizar de manera similar.

- ***Libro de Diligencias digitales***

  En este archivo notarial se almacenarán los mensajes que contienen los documentos digitales de Diligencias como resultados de los trámites notariales digitales. La organización se realizará anualmente mediante tomos mensuales. El índice del Libro de Diligencias se reemplazará por una opción de búsqueda.

Para distinguir entre mensajes almacenados en ambos Archivos Digitales del Sistema de Gestión Documental mínimo se debe contar con los parámetros descritos en la tabla 3.10.

Parámetro	Descripción
Usuario	El nombre distintivo de la cuenta del cliente que realizó el trámite.
Asunto	El título del mensaje digital que permitirá distinguir fácilmente el contenido del mensaje.
Fecha	Se refiere al día en que se envió el mensaje digital según la Autoridad de Tiempo. Estará acorde al año de organización al que pertenezca el mensaje digital.

Tabla 3.10: Parámetros de la opción Archivo Digital

- **Búsqueda**

La opción de Búsqueda del Sistema de Gestión Documental realizará las funciones del índice del archivo digital que menciona la Ley Notarial. El Administrador del Archivo realizará la búsqueda en el Archivo Digital de la Notaría acorde al tipo de trámite notarial en el Protocolo de Escrituras Públicas digitales o en el Libro de Diligencias digitales.

La opción Búsqueda del Sistema de Gestión Documental deberá disponer mínimo de los parámetros descritos en la tabla 3.11 para obtener una búsqueda eficiente.

Parámetro	Descripción
Asunto	El título del mensaje digital que permitirá distinguir fácilmente su contenido.
Fecha de Creación	Se referirá a la fecha en que se guardó el mensaje digital en el Sistema de Gestión Documental.
Remitente	Contendrá el nombre distintivo del usuario creador del mensaje digital.
Destinatario	Nombre distintivo del usuario a quien se envió el mensaje digital.
Tipo de Trámite	Elemento que permitirá distinguir qué tipo de trámite se desea buscar.

Tabla 3.11: Parámetros de la opción Búsqueda

- **Nuevo**

La opción Nuevo permitirá crear los mensajes digitales para los trámites notariales. Esta opción del Sistema de Gestión Documental permitirá adjuntar el documento firmado electrónicamente al Nuevo mensaje digital generado.

La opción Nuevo deberá contar como mínimo con los parámetros descritos en la tabla 3.12 para crear un mensaje digital en el Sistema de Gestión Documental.

Parámetro	Descripción
De	Representará el nombre distintivo de la persona que redacta el nuevo mensaje digital.
Para	Contendrá el nombre distintivo del usuario destinatario del mensaje digital.
Tipo de Trámite	Permitirá elegir el tipo de trámite notarial digital a realizar.
Anexos	Adjuntará el o los documentos firmados electrónicamente.
Cuerpo del Mensaje	Se refiere a una explicación del mensaje digital generado.

Tabla 3.12: Parámetros para crear un Nuevo Mensaje

- **Bandeja de Entrada**

  La Bandeja de Entrada almacenará los mensajes digitales que reciba el usuario. El mensaje digital contiene la documentación adjunta referente a Escrituras Públicas, Diligencias finales y documentos habilitantes. Para organizar los mensajes digitales en la Bandeja de Entrada del Sistema de Gestión Documental mínimo deberá contar con los parámetros descritos en la tabla 3.13.

Parámetro	Descripción
Remitente	Contendrá el nombre distintivo de la cuenta del emisor del mensaje digital.
Asunto	El título del mensaje digital que permitirá distinguir fácilmente el contenido del mensaje.
Fecha	Se refiere al día en que se recibió el mensaje digital según la Autoridad de Tiempo.

Tabla 3.13: Parámetros de la Bandeja de Entrada

- **Elementos Enviados**

  La opción Elementos Enviados deberá almacenar los mensajes digitales enviados a otros usuarios del Sistema de Gestión Documental. Los parámetros mínimos que permitirán distinguir mensajes digitales en los Elementos Enviados en el Sistema de Gestión Documental son descritos en la tabla 3.14.

Parámetro	Descripción
Destinatario	Contendrá el nombre distintivo de la cuenta del receptor del mensaje digital.
Asunto	El título del mensaje digital que permitirá distinguir fácilmente el contenido del mensaje digital enviado.
Fecha	Se refiere al día en que se envió el mensaje digital según la Autoridad de Tiempo.

Tabla 3.14: Parámetros de la opción Elementos Enviados

- **Reasignación de Mensajes**

  La opción Reasignación almacenará los mensajes digitales que se transfieren a otro usuario para cumplir con el protocolo de los trámites notariales digitales. Esta opción del Sistema de Gestión Documental estará activa solo para las cuentas del Verificador y Matrizador que deben reasignar los mensajes digitales del Cliente acorde al protocolo del trámite notarial digital.

  La opción Reasignación de Mensajes del Sistema de Gestión Documental deberá poseer como mínimo los siguientes parámetros descritos en la tabla 3.15:

Parámetro	Descripción
Destinatario	El nombre distintivo de la cuenta a quien se reasignó el mensaje digital.
Asunto	El título del mensaje digital que permitirá conocer el contenido del mensaje digital reasignado.
Fecha	Se refiere al día en que se reasignó el mensaje digital según la Autoridad de Tiempo.

Tabla 3.15: Parámetros de la opción Reasignación de Mensajes

3.4 INFRAESTRUCTURA SEGURA

En este subcapítulo se utiliza la arquitectura modular SAFE de CISCO para el diseño de la red de datos para la Notaría Digital. SAFE toma las consideraciones de seguridad, rendimiento, escalabilidad y disponibilidad que serán aplicadas para el diseño de la infraestructura segura de la Notaría Digital. El diseño de la infraestructura segura de la Notaría Digital se basa en los requerimientos de seguridad analizados en el capítulo 2.2.

La arquitectura SAFE se encuentra dividida en dos capas. La primera capa de modularidad de SAFE representa una vista general de la red de datos de la Notaría Digital y está compuesta por las siguientes áreas funcionales: Notaría, Borde de la Notaría y Proveedor de Servicios de Internet (ISP)[31] como se muestra en la figura 3.11. La segunda capa de modularidad de SAFE representa una vista detallada de todos los módulos de cada área funcional de la Notaría Digital como se muestra en la figura 3.12. Cada módulo realiza funciones específicas dentro de la red de datos y cumplen con requerimientos de seguridad. El diseño descarta el módulo del ISP

[31] ISP (Proveedor de Servicios de Internet) - Es una compañía que ofrece acceso a Internet, normalmente por una cuota. (Fuente: http://windows.microsoft.com/es-ES/windows-vista/What-is-an-Internet-Service-Provider-ISP)

porque la seguridad de este módulo se garantiza mediante Acuerdos de Nivel de Servicio (SLA)[32].

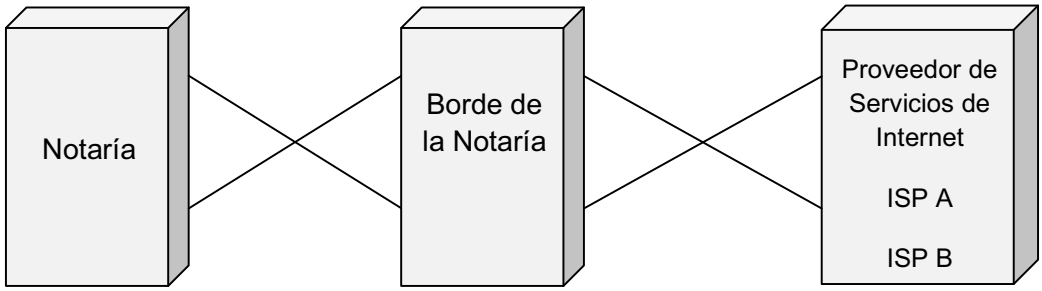

Figura 3.11: Primera capa de modularidad de la red de datos de la Notaría Digital

[32] SLA (Acuerdos de Nivel de Servicios) - Es un contrato que existe entre el cliente y su proveedor de servicio o entre proveedores para definir el nivel de servicio. (Fuente: http://www.gestiopolis.com/delta/term/TER450.html)

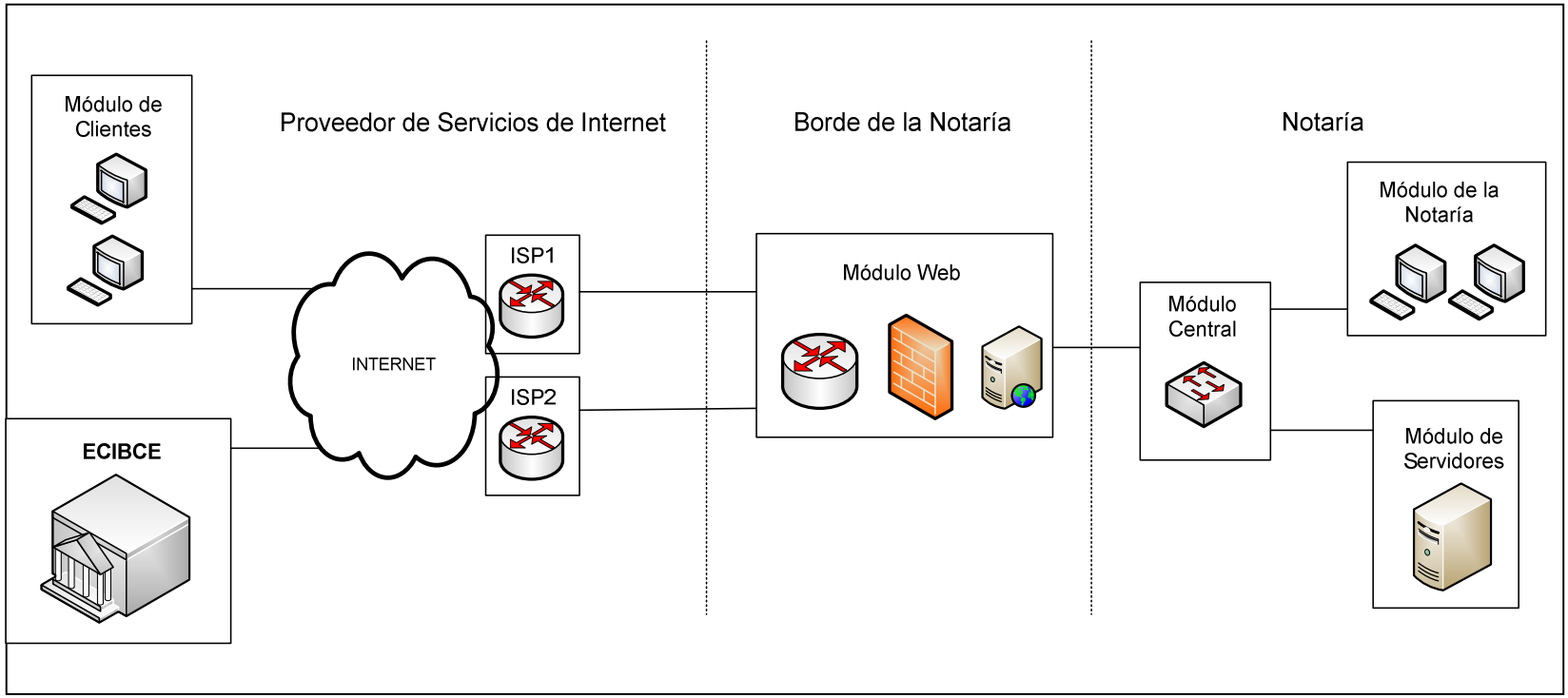

Figura 3.12: Arquitectura Modular de la Infraestructura de Notaría Digital

3.4.1 ARQUITECTURA DE LA RED DE DATOS

La arquitectura de la red de datos de la Notaría Digital está basada en SAFE. El diseño de la infraestructura segura de la Notaría Digital analiza dos áreas funcionales: Notaría y Borde de la Notaría. Los módulos que forman estas áreas funcionales se describen de acuerdo a las actividades que cumplen en la infraestructura de la red de datos. Algunos módulos de la arquitectura SAFE se han omitido porque la red de datos de la Notaría Digital no se ha considerado como un entorno complejo.

3.4.1.1 Área Funcional Notaría

El área funcional denominada Notaría describe los módulos necesarios para interconectar a los usuarios internos con los servicios de la Notaría Digital. El área funcional Notaría se compone de tres módulos: el módulo Central, el módulo de la Notaría y el módulo de Servidores. El área funcional Notaría con sus tres módulos se muestra en la figura 3.13.

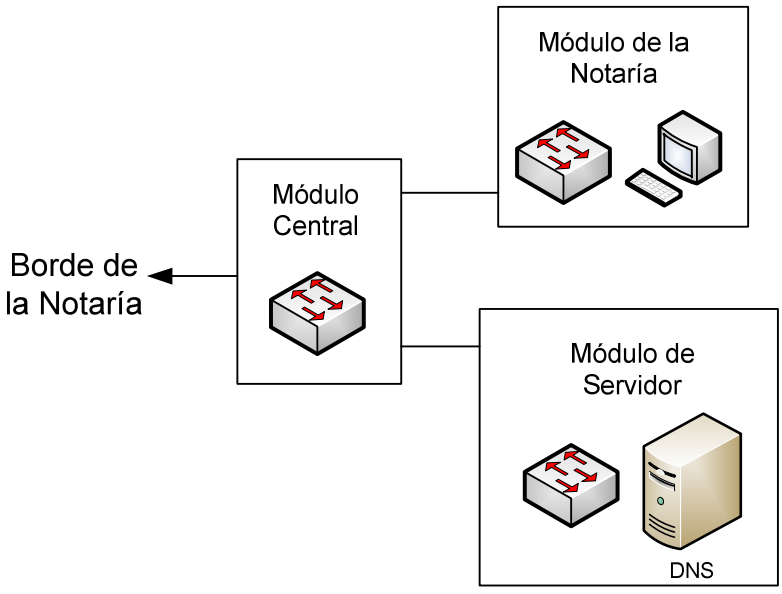

Figura 3.13: Área funcional Notaría

3.4.1.1.1 Módulo Central

El módulo Central de la red de datos de la Notaría Digital está formado por un switch capa 2. En este módulo el diseño propone la configuración de tres Redes de Área Local Virtuales (VLAN)[33]. La VLAN aumenta la seguridad porque la información se encapsula en un nivel adicional y disminuye la transmisión de tráfico en la red de datos de la Notaría Digital[34]. La primera VLAN agrupa los usuarios internos de la Notaría Digital. La segunda VLAN contiene al servidor interno. Y la tercera VLAN consta del servidor expuesto hacia Internet situado en la zona DMZ[35] del Firewall. El módulo Central de la Notaría se muestra en la figura 3.14.

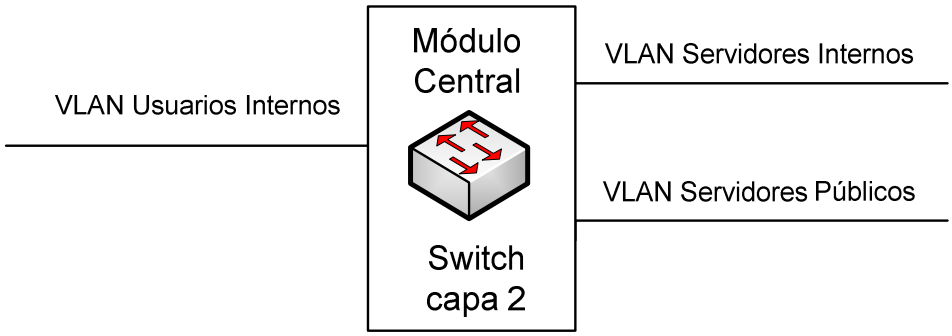

Figura 3.14: Diagrama del módulo Central

3.4.1.1.2 Módulo de la Notaría

El módulo de la Notaría de la red de datos contiene todas las estaciones de trabajo de los usuarios internos de la Notaría Digital. Las estaciones de este módulo pertenecen a la VLAN de usuarios internos. Se conectan al switch capa 2 del módulo Central para acceder a los servicios de la Notaría Digital. Las estaciones de trabajo usan direcciones IP privadas configuradas manualmente. El módulo de la Notaría se muestra en la figura 3.15. Los usuarios que forman el módulo de la Notaría son:

[33] VLAN (Red de Área Local Virtual). "Virtual Bridged Local Area Networks" Estándar IEEE 802.1Q (Fuente: http://standards.ieee.org/getieee802/download/802.1Q-2005.pdf)
[34] Fuente: http://es.kioskea.net/contents/internet/vlan.php3
[35] DMZ (Zona Desmilitarizada).- Es una red local que se ubica entre la red interna de una organización y una red externa, generalmente Internet. (Fuente: http://www.solusan.com/que-es-una-dmz.html)

Notario, Verificador, Matrizador, Administrador del Archivo y Administrador del Sistema, los cuales se ilustran en la figura 3.16.

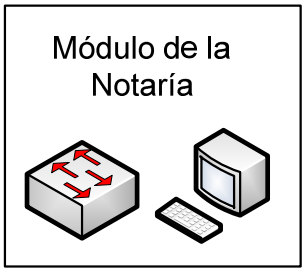

Figura 3.15: Diagrama del módulo de Notaría

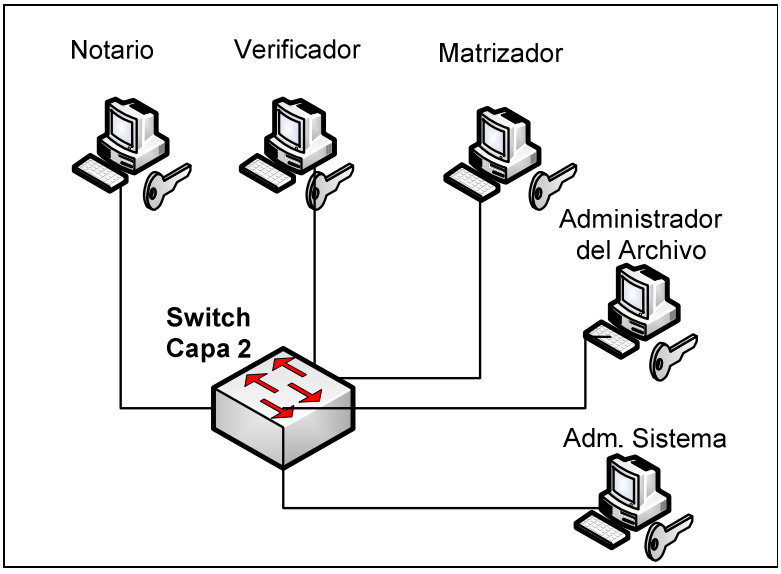

Figura 3.16: Diagrama esquemático del módulo de Notaría

3.4.1.1.3 Módulo de Servidor

El módulo de Servidor de la red de datos de la Notaría Digital está formado por el servidor DNS[36]. El servidor DNS de este módulo pertenece a la VLAN de servidores internos. Se conecta al switch capa 2 usando una dirección IP privada configurada manualmente. El módulo de Servidor se muestra en la figura 3.17.

[36] DNS (Servicio de Nombres de Dominio).- Es el sistema utilizado en TCP/IP para mantener una correspondencia de los nombres de las máquinas con sus direcciones IP y viceversa. (Fuente: http://www.fi.upm.es/?pagina=237)

El servidor DNS traducirá el nombre de los servicios de la Notaría Digital a las direcciones IP asignadas. La finalidad es evitar la conexión a Internet para acceder al Servidor Web seguro ahorrando tiempos de respuesta..

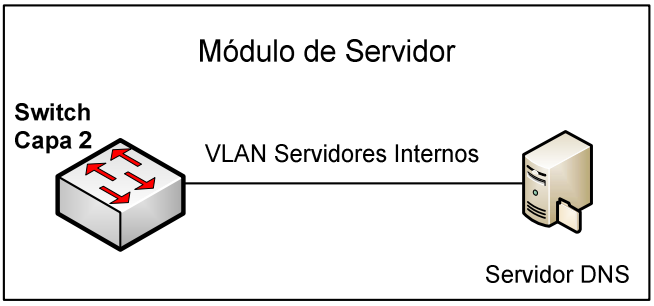

Figura 3.17: Diagrama del módulo de Servidor

El diseño de la red de datos de la Notaría Digital no considera un servidor que configure automáticamente las direcciones IP de los equipos debido al reducido número de equipos finales.

3.4.1.2 Área Funcional Borde de la Notaría

El área funcional denominada Borde de la Notaría describe el módulo requerido para ofrecer servicios seguros de la Notaría Digital en Internet. El área funcional Borde de la Notaría se compone del módulo Web. El área funcional Borde de la Notaría se muestra en la figura 3.18.

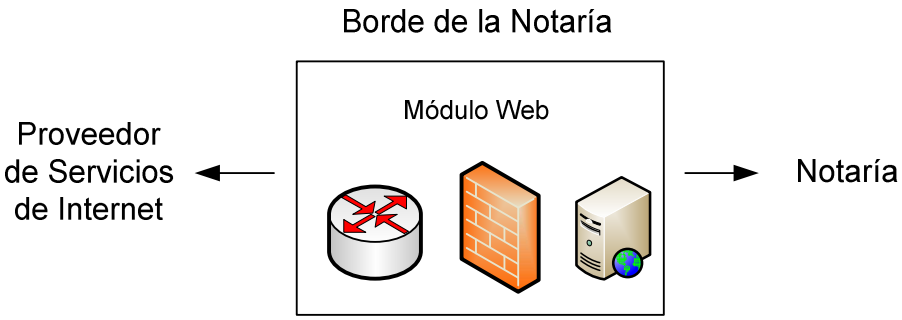

Figura 3.18: Área funcional Borde de la Notaría

3.4.1.2.1 Módulo Web

El Módulo Web de la red de datos de la Notaria Digital está formado por un Router Firewall y servidor Web seguro. Este módulo proporciona los servicios de la Notaría Digital a todos los usuarios. El modulo Web de la Notaria Digital se muestra en la figura 3.19.

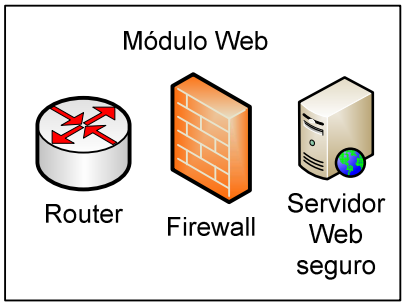

Figura 3.19: Diagrama del módulo de Web

En el servidor Web seguro de este módulo corre el Sistema de Gestión Documental para realizar los trámites notariales bajo el protocolo HTTPS. El servidor Web seguro pertenece a la VLAN de servidores públicos. Se configura en la zona DMZ del Firewall. Se conecta al switch capa 2 del módulo Central de la Notaría usando una dirección IP privada configurada manualmente. El servidor Web seguro permitirá ser administrado remotamente sólo por el Administrador del Sistema mediante la configuración de políticas en el Firewall.

El módulo Web de la Notaria Digital permite la creación de una VPN[37] a través de Internet entre la red de datos de la Notaria Digital y la red de datos de la ECIBCE. La creación de la VPN tiene por objetivo la transferencia segura de la información del Directorio de Identidades de la ECIBCE. El servidor del Directorio de Identidades de la ECIBCE actúa como servidor VPN, mientras que el servidor Web seguro de la Notaría Digital actúa como cliente VPN. La configuración de la VPN en este módulo

[37] VPN (Virtual Private Network).- Es una red privada construida dentro de una infraestructura de red pública, tal como la red mundial de Internet. Las redes privadas virtuales proporcionan el mayor nivel posible de seguridad mediante seguridad IP (IPsec) cifrada o túneles VPN de Secure Sockets Layer (SSL) y tecnologías de autenticación.
(Fuente: http://www.cisco.com/web/LA/soluciones/la/vpn/index.html)

garantiza una conexión confiable a través de protocolos de comunicación seguros. El transporte de la información se protege con la configuración del protocolo IPSec[38]. La VPN para la conexión de la ECIBCE y la Notaría Digital se muestra en la figura 3.20.

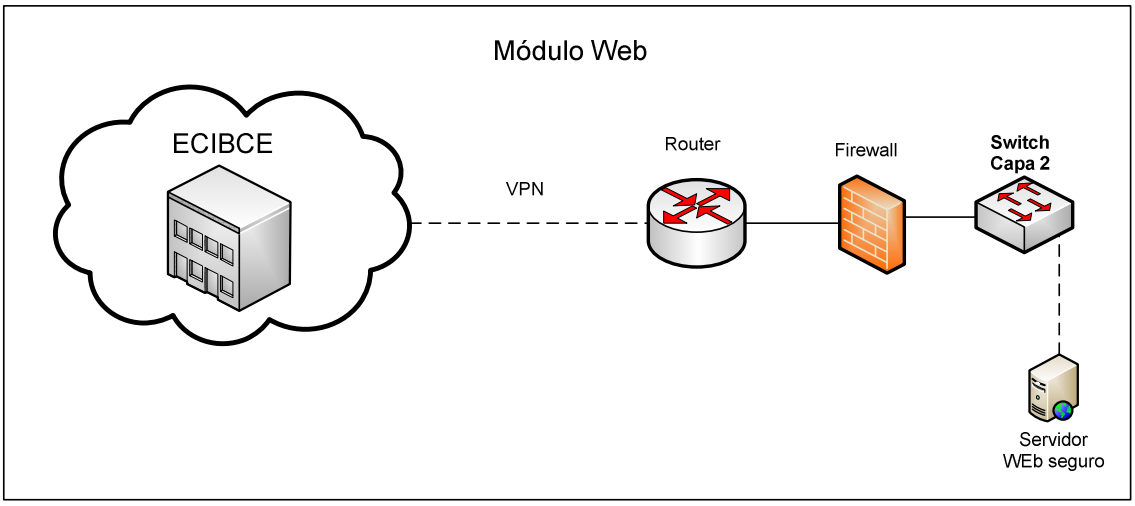

Figura 3.20: Diagrama de la conexión VPN

El módulo Web permite controlar la seguridad perimetral de la Notaría Digital mediante el Firewall. La configuración de este módulo permitirá que los usuarios internos puedan hacer uso de Internet. La finalidad es monitorear el tráfico que atraviese la red de datos para bloquear intrusos que pongan en riesgo la seguridad de la información.

- **Firewall**

  El Firewall del módulo Web de la red de datos de la Notaría Digital es el equipo de seguridad perimetral. La función del Firewall es permitir o negar el tráfico que atraviesa la red de datos. Estas acciones se configuran mediante políticas y responden a necesidades de interconexión de la Notaría Digital. La infraestructura

[38] IPSec (Security IP).- Es un marco de estándares abiertos para lograr comunicaciones privadas seguras a través de redes con el Protocolo de Internet (IP) mediante el uso de servicios de seguridad criptográfica. (Fuente: http://technet.microsoft.com/es-es/library/cc779754%28WS.10%29.aspx)

segura de la Notaría Digital define la configuración de tres zonas[39] para el intercambio de información que se mencionan en la tabla 3.16.

La primera fila de la tabla 3.16 muestra las tres zonas que requiere el Firewall de la red de datos de la Notaría Digital. La segunda fila describe los equipos que conforman cada zona. La tercera fila caracteriza el tipo de tráfico que genera cada zona según el Firewall. Y la cuarta fila detalla la configuración de las políticas de seguridad para el intercambio de información entre las zonas.

	Zona Trust	**Zona Untrust**	**DMZ**
Conformada por:	Servidor DNS y estaciones de trabajo de la red interna	Usuarios externos a la red de la Notaría	Servidor Web seguro publicado en Internet
Característica según el Firewall	Tráfico de confianza	Tráfico de desconfianza	Tráfico DMZ
Políticas de Configuración	Permitir tráfico hacia las zonas Untrust y DMZ	Permitir tráfico hacia la DMZ usando HTTPS	Permitir tráfico hacia servidores de la zona Trust

Tabla 3.16: Zonas del Firewall de la red de datos de la Notaría Digital

3.4.2 DIAGRAMA ESQUEMÁTICO DE LA RED DE DATOS DE LA NOTARÍA DIGITAL

En este subcapítulo se muestra el diagrama esquemático del diseño de la red de datos de la Notaría Digital. El resultado del diagrama esquemático obedece al análisis realizado a la arquitectura modular SAFE de CISCO para aplicarlo al diseño de la red de datos de la Notaría Digital.

[39] Zonas del Firewall. Identifican el origen y destino de un paquete de datos y agrupan a ciertos equipos de la red de datos.

Los autores del presente proyecto optaron por el diseño de la red de datos que junte en un solo dispositivo los equipos de los módulos descritos en el subcapítulo 3.4.1. Los routers y firewalls de los módulos de Comercio Electrónico, VPN e Internet de la Notaría integran sus funciones en un solo Router y Firewall. Los switches de los módulos Central, Notaría y Servidor se concentran en un switch capa 2. El diseño considera la conexión a dos ISPs para garantizar la disponibilidad de los servicios de la Notaría Digital. Sin embargo la disponibilidad para realizar los trámites notariales digitales depende del horario laboral de atención que impone la Notaría.

El diagrama esquemático de la infraestructura de la red de datos de la Notaría Digital se muestra en la figura 3.21. Las llaves junto a las estaciones de trabajo de los usuarios representan los certificados de firma electrónica que requieren para realizar los trámites notariales digitales.

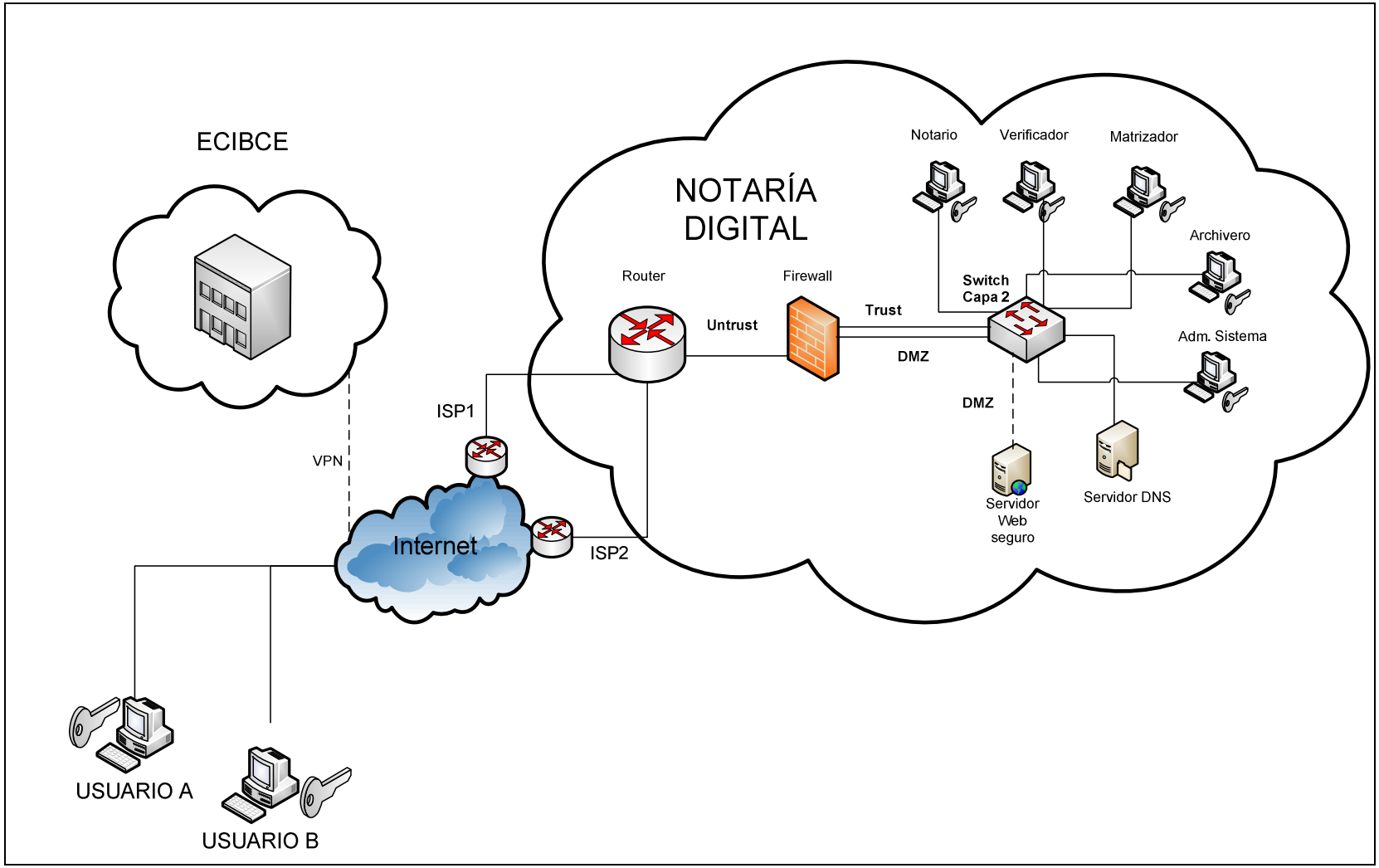

Figura 3.21: Diagrama esquemático del diseño de la red de datos de la Notaría Digital

3.4.2.1 Requisitos mínimos de equipos

En este subcapítulo se describe el dimensionamiento de los siguientes equipos que se encuentran en la figura 3.22. La tabla 3.17 se compone de los requisitos mínimos que deben tener los equipos para funcionar en la Notaría Digital.

Equipos	Requisitos mínimos
Firewall	Administración remota Configuración vía web 3 Interfaces 100/1000 MBPS Monitoreo de tráfico para detectar y prevenir intrusos VPN sobre el protocolo IPSec Filtrado de contenido Protección de virus para páginas web Control de ancho de banda Reportes de acceso a Internet y tráfico que cruza por la red de datos.
Router	Administración remota Configuración vía web 3 Interfaces 10/100 MBPS Enrutamiento entre VLAN's con protocolos abiertos Configuración de ACL's
Switch Capa 2	Administración remota Configuración vía web Switch administrable 9 Interfaces 100/1000 Mbps Full Dúplex Método de acceso CSMA/CD Protocolo IEEE 802.1Q Backplane de 1.8Gbps (9PC*100Mbps*2(FullDuplex)) Control de flujo para transmisiones seguras Actualización automática de direcciones MAC

	Store and forward Puertos auto MDI/MDIX
Servidor DNS	Memoria RAM 2 GB Disco Duro 40 GB Procesador Core 2 Duo de 1,83 GHZ
Servidor Web Seguro	Memoria RAM 6 GB Procesador Core Quad de 2 GHZ Disco Duro de 500 GB Cada trámite notarial digital tiene como promedio un tamaño de 1 MB. Mensualmente la frecuencia esperada de todos los trámites de la Notaría Digital suma 375, lo que genera 375 MB de almacenamiento mensual en el servidor. Tomando en cuenta que este servidor almacena logs de los servicios instalados, base de datos del Sistema de Gestión Documental se estima un almacenamiento mínimo de 500 GB.

Tabla 3.17: Requisitos mínimos de equipos

3.4.2.2 Capacidad del acceso a Internet

Para dimensionar la capacidad del canal de subida del acceso a Internet de la Notaria Digital, se consideró que, de acuerdo a los requerimientos de los trámites notariales estos ocupan un promedio de 1 MB. Además se consideró el valor de 375 trámites notariales digitales tomando en cuenta la frecuencia esperada, lo que resulta el valor aproximado de 3 trámites por hora. Aplicando estas consideraciones se tiene el siguiente análisis:

$$V_{Upstream} = \frac{1024Kbytes}{trámite} * \frac{8bits}{1byte} * \frac{3trámites}{h} * \frac{1h}{3600seg} = 6{,}82Kbps$$

Esta capacidad se considera la mínima para contratar el enlace de acceso a Internet en el canal de subida.

CAPÍTULO 4

IMPLEMENTACIÓN DEL PROTOTIPO DE NOTARÍA DIGITAL

En este capítulo se describe la implementación del prototipo de Notaría Digital. El prototipo de Notaría Digital se implementó en un segmento de red. El prototipo de Notaría Digital utilizó un Sistema de Gestión Documental, certificados de firma electrónica emitidos por una autoridad de certificación de prueba, un servidor DNS y un servidor Firewall. El objetivo fue conseguir una similitud al diseño de la Notaría Digital descrito en el capítulo 3. El Sistema de Gestión Documental utilizado por el prototipo de Notaría Digital fue Quipux[40].

La configuración de los servidores del prototipo de Notaría Digital se explica en el subcapítulo 4.1. La parametrización del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital se explica en el subcapítulo 4.2. La gestión de certificados de firma electrónica utilizados en el prototipo de Notaría Digital se explica en el subcapítulo 4.3. La configuración de la red de datos del prototipo de Notaría Digital se explica en el subcapítulo 4.4. Y por último se realizan las pruebas del prototipo de Notaría Digital en el subcapítulo 4.5 sobre la base de la configuración descrita en los subcapítulos anteriores.

4.1 CONFIGURACIÓN DE SERVIDORES

En este subcapítulo se describe la configuración de los servidores que forman parten del prototipo de Notaría Digital. El sistema de Gestión Documental Quipux para el prototipo de Notaría Digital se explica en el subcapítulo 4.1.1. Como complemento se configuraron los servidores DNS y Firewall en el prototipo de Notaría Digital. El servidor DNS para el prototipo de Notaría Digital se define en el subcapítulo 4.1.2. El

[40] Sistema de Gestión Documental Quipux (Fuente: http:// www.quipux.org/)

servidor Firewall para el prototipo de Notaría Digital se describe en el subcapítulo 4.1.3.

El prototipo de Notaría Digital se configuró en una máquina virtual usando el software VMWare Workstation[41] 7.1.2 debido al conocimiento de esta herramienta de los autores de este proyecto de titulación. El Sistema Operativo escogido para el prototipo de Notaría Digital fue Linux CentOS[42] 5.4. Esta distribución de Linux fue escogida por recomendación del Manual de Instalación Quipux desarrollado por la Subsecretaria de Informática[43]. Todos los servidores para el prototipo de Notaría Digital descritos en este subcapítulo fueron configurados en la misma máquina virtual corriendo bajo Linux CentOS 5.4.

4.1.1 SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX

En este subcapítulo se muestra la configuración de los servidores que requiere el Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital. El Sistema de Gestión Documental Quipux consta de los servidores Web y Base de Datos. La configuración del servidor Web seguro del Sistema de Documental Quipux se explica en el subcapítulo 4.1.1.1. El servidor de Base de Datos del Sistema de Documental Quipux se define en el subcapítulo 4.1.1.2.

Quipux fue desarrollado por la Subsecretaria de Informática del Ecuador con base en el Sistema de Gestión Documental Orfeo desarrollado en Colombia y que utiliza tecnologías y estándares abiertos. Quipux es utilizado en la actualidad por alrededor de 100 empresas del Estado[44] debido a la política del Gobierno del Ecuador que promueve el uso de software libre[45]. Quipux ofrece para el prototipo de Notaría Digital: creación de mensajes digitales con documentación adjunta para cumplir con

---

[41] VMWare Workstation.- Permite ejecutar múltiples sistemas operativos al mismo tiempo. (Fuente: http://www.vmware.com/products/workstation/)
[42] CentOS (Community ENTerprise Operating System).- CentOS es una distribución Linux Enterprise basado en las fuentes disponibles de forma gratuita de Red Hat Enterprise Linux. (Fuente: http://wiki.centos.org/FrontPage)
[43] http://redmine.quipux.org/attachments/download/10/Manual-Instalacion-Quipux-v1.1-1.sxw
[44] http://www.informatica.gov.ec/index.php?option=com_reporte_usuarios_quipux
[45] Ec. Rafael Correa promueve Software Libre (Fuente: http://www.youtube.com/watch?v=Hy5yAk4dYOk)

el protocolo de trámites notariales digitales, archivado digital, administración de cuentas de usuarios y búsqueda, recuperación y presentación de mensajes digitales. Por las razones descritas anteriormente se opto por Quipux como el Sistema de Gestión Documental para el prototipo de Notaría Digital.

4.1.1.1 Servidor Web seguro

En este subcapítulo se define la configuración del servidor Web seguro para el prototipo de Notaría Digital. El Manual de Instalación Quipux desarrollado por la Subsecretaria de Informática configura Apache para el servidor Web pero el prototipo de Notaría Digital implementa un nivel de seguridad utilizando un servidor Web seguro. El servidor Web seguro instalado en el prototipo de Notaría Digital fue Apache – SSL[46], a fin de respetar la recomendación del manual de instalación.

- **Apache-SSL**

Apache – SSL permite establecer una comunicación Web segura usando el protocolo HTTPS. La configuración de Apache – SSL se realizó en el archivo: /etc/httpd/conf.d/ssl.conf. El archivo de configuración ssl.conf permite al servidor Web interactuar con certificados digitales para implementar un servidor Web seguro. En la figura 4.1 se muestra el archivo ssl.conf para la configuración del servidor Web seguro del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital.

Adicionalmente, el servidor Web seguro requiere la configuración del archivo del lenguaje de programación PHP[47] y del archivo config.php del Sistema de Gestión Documental Quipux de acuerdo al Manual de Instalación.

[46] Apache – SSL.- Es un servidor web seguro, basado en Apache y OpenSSL SSLeay /. Es licenciado bajo BSD. (Fuente: http://www.apache-ssl.org/)
[47] PHP (Hypertext Pre-processor).- Lenguaje de programación usado generalmente en la creación de contenidos para sitios web. (Fuente: http://www.alegsa.com.ar/Dic/php.php)

- **PHP 5.2**

El Sistema de Gestión Documental Quipux es desarrollado sobre la base del lenguaje de programación PHP y soporta solo la versión 5.2. El archivo de configuración de PHP modificado se encuentra en la dirección: /etc/php.ini. En la figura 4.2 se muestra el archivo php.ini con la configuración de las variables para el buen funcionamiento del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital.

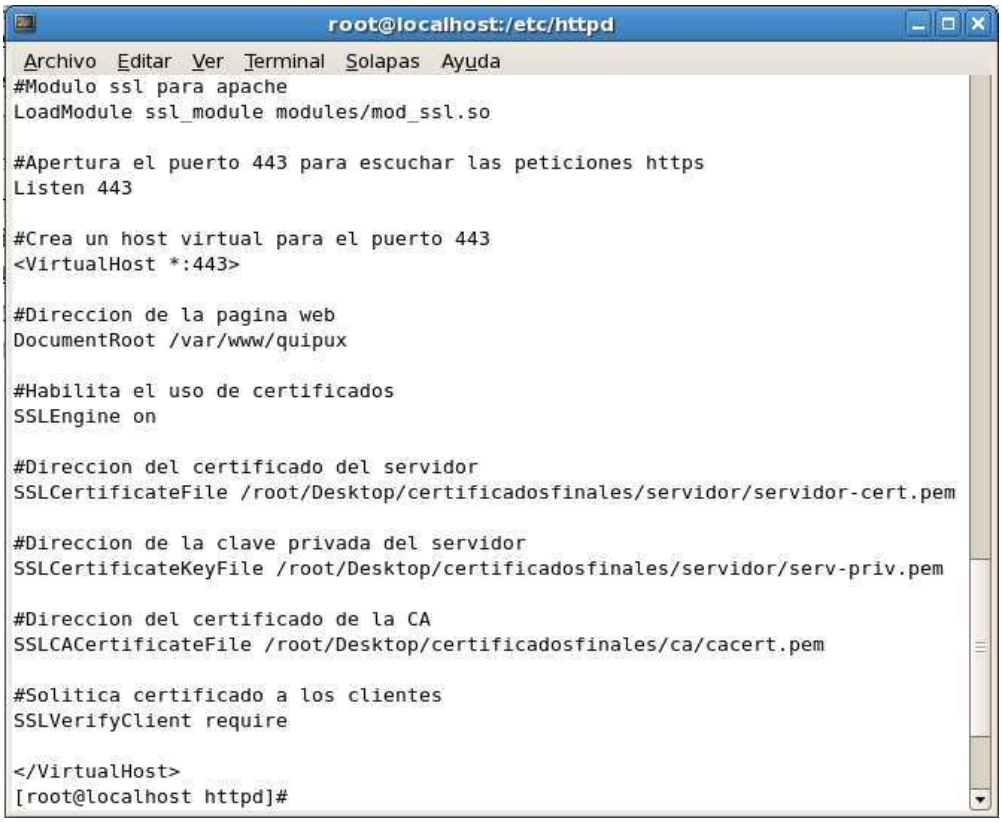

Figura 4.1: Archivo de configuración de Apache-SSL

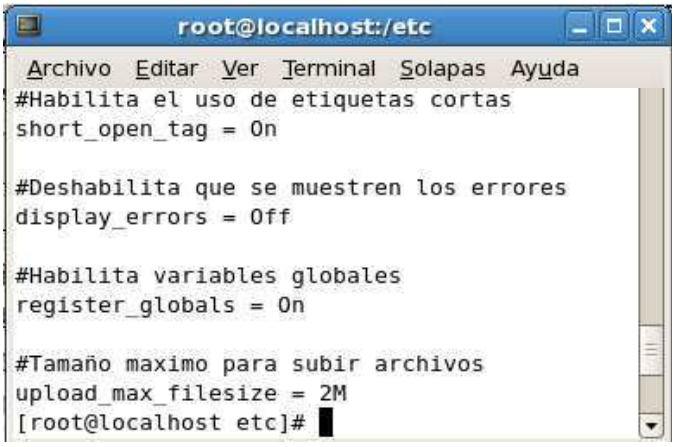

Figura 4.2: Archivo de configuración php.ini

- **Quipux**

La programación del Sistema de Gestión Documental Quipux requirió la configuración del archivo /var/www/quipux/config.php. Este archivo define los parámetros de conexión entre la interfaz Web programada en PHP y la base de datos desarrollada en Postgresql[48]. La figura 4.3 muestra el archivo config.php con la configuración del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital.

Figura 4.3: Archivo de configuración del servidor Quipux

[48] Postgresql.- Es un potente sistema de base de datos objeto-relacional de código abierto. (Fuente: http://www.postgresql.org/about/)

4.1.1.2 Servidor Base de Datos

En este subcapítulo se muestra la configuración del servidor de Base de Datos del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital. El Sistema de Gestión Documental Quipux utiliza la Base de Datos Postgresql. El servidor de Base de Datos almacena la información ingresada por los usuarios del Sistema de Gestión Documental Quipux. En este subcapítulo se abarca la configuración de Postgresql y PgAdmin[49] III.

- **Postgresql**

El motor de base de datos Postgresql se configura en los archivos de las direcciones: /var/lib/pgsql/data/postgresql.conf y /var/lib/pgsql/data/pg_hba.conf. El archivo posrgresql.conf permite especificar la dirección en que el servidor escucha las peticiones de clientes. El archivo pg_hba.conf permite especificar las redes de datos o direcciones IP que pueden acceder al servidor de Base de Datos. En la figura 4.4 se muestra el archivo postgresql.conf para que el servidor escuche peticiones de los clientes a través de todas sus interfaces de red. En la figura 4.5 se muestra el archivo pg_hba.conf para que el servidor sea accedido localmente o desde cualquier host que se encuentre en la red 192.168.1.0/24.

Figura 4.4: Archivo de configuración postgresql.conf

[49] PgAdmin.- Permite la administración y desarrollo sobre la plataforma de base de datos Postgresql. (Fuente: http://www.pgadmin.org/)

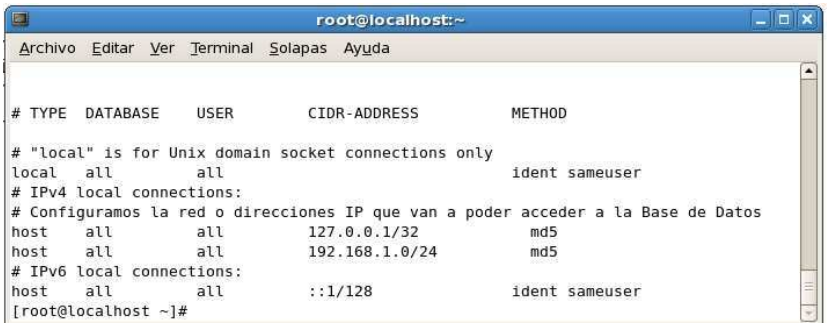

Figura 4.5: Archivo de configuración pg_hba.conf

- **PgAdmin III**

PgAdmin III es un programa que permite administrar la base de datos del Sistema de Gestión Documental Quipux mediante un interfaz gráfico. En la figura 4.6 se muestra la Base de Datos de nombre quipux creada para el prototipo de Notaría Digital. La Base de Datos quipux es administrada con una cuenta de usuario llamada quipux.

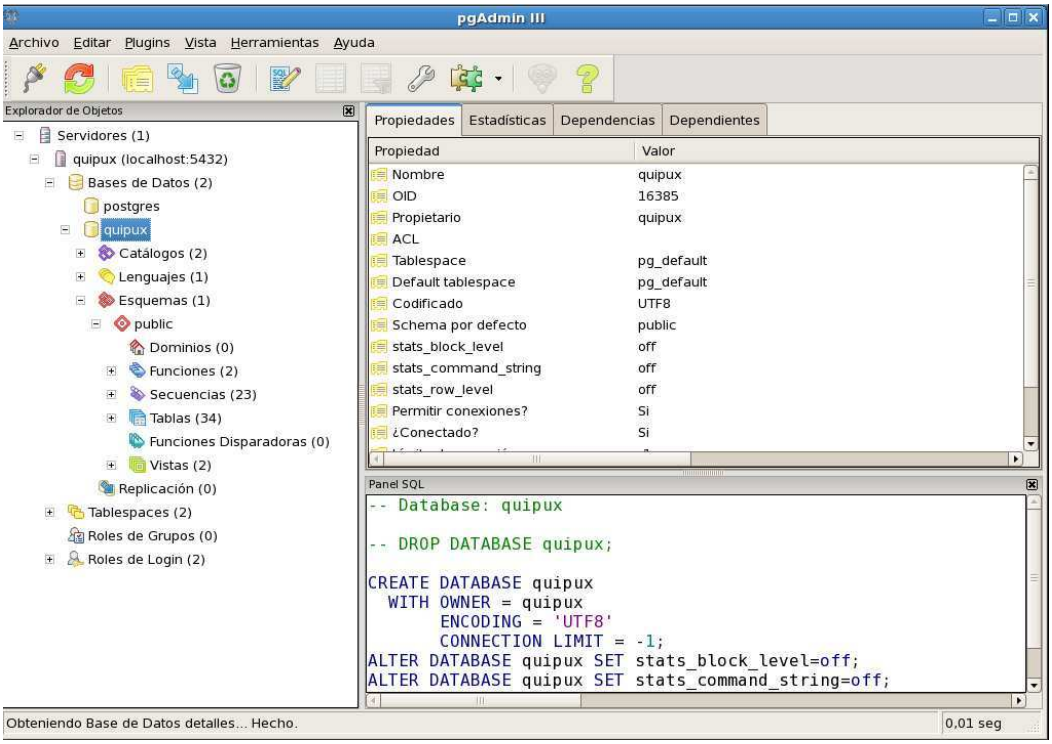

Figura 4.6: Interfaz principal del programa PgAdmin III

4.1.2 SERVIDOR DNS

En este subcapítulo se define la configuración del servidor DNS para el prototipo de Notaría Digital. El servidor DNS instalado en el prototipo de Notaría Digital fue bind[50], debido al conocimiento de este programa por los autores de este proyecto de titulación. El prototipo de Notaría Digital utilizó el dominio www.notaria-n.com para el Sistema de Gestión Documental Quipux instalado en el servidor con la dirección IP 192.168.1.4/24. Los usuarios del prototipo de Notaría Digital deberán configurar esta dirección IP en el campo Servidor DNS en las propiedades de las conexiones de red para resolver el dominio www.notaria-n.com.

La figura 4.7 muestra en la parte derecha el archivo de configuración de la zona de búsqueda directa del servidor DNS. El archivo de configuración se ubica en /var/named/chroot/var/named/directa. La parte izquierda de la figura muestra la prueba del servidor DNS del prototipo con el comando nslookup[51]. El dominio www.notaria-n.com se tradujo a la dirección IP del servidor con el Sistema de Gestión Documental Quipux: 192.168.1.4.

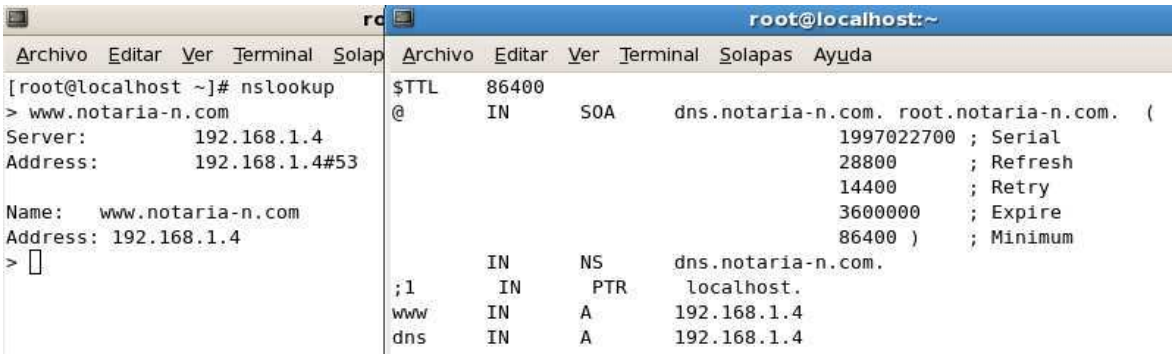

Figura 4.7: Archivo de configuración del servidor DNS

[50] Bind (Berkeley Internet Name Domain). - Es una implementación del protocolo DNS y proporciona una referencia abiertamente redistribuible de los principales componentes del sistema de nombres de dominio. (Fuente: http://www.bind9.net/)

[51] NSLOOKUP.- Es una herramienta administrativa de la línea de comandos para probar y solucionar problemas de los servidores DNS. (Fuente: http://support.microsoft.com/kb/200525/es)

4.1.3 SERVIDOR FIREWALL USANDO IPTABLES[52]

En este subcapítulo se define la configuración del servidor Firewall para permitir el tráfico deseado por el prototipo de Notaría Digital. El servidor Firewall instalado en el prototipo de Notaría Digital fue iptables, ya que el prototipo utilizó un firewall a nivel de software en lugar de hardware. En el archivo /etc/sysconfig/iptables se configuraron las reglas para permitir el tráfico hacia el prototipo de Notaría Digital. Los puertos habilitados en el servidor Firewall se muestran en la figura 4.8.

```
Archivo  Editar  Ver  Terminal  Solapas  Ayuda
# Generated by iptables-save v1.3.5 on Tue Feb  1 14:12:21 2011
*filter
:INPUT ACCEPT [0:0]
:FORWARD ACCEPT [0:0]
:OUTPUT ACCEPT [42:4488]
:RH-Firewall-1-INPUT - [0:0]
-A INPUT -j RH-Firewall-1-INPUT
-A FORWARD -j RH-Firewall-1-INPUT
#Permite las conexiones desde localhost
-A RH-Firewall-1-INPUT -i lo -j ACCEPT

#Solo el equipo con IP (192.168.1.20) accede remotamente via ssh. --Adm del sist
ema
-A RH-Firewall-1-INPUT -s 192.168.1.20 -p tcp -m tcp --dport 22 -j ACCEPT

#Niega el acceso para los demas usuarios via puerto 5432
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 22 -j DROP

#Acceso HTTPS al servidor web
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 443 -j ACCEPT

#Solicitudes DNS al servidor DNS
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 53 -j ACCEPT
-A RH-Firewall-1-INPUT -p udp -m udp --dport 53 -j ACCEPT

#Solo el equipo con IP (192.168.1.20) accede a la BDD. --Adm del sistema
-A RH-Firewall-1-INPUT -s 192.168.1.20 -p tcp -m tcp --dport 5432 -j ACCEPT

#Niega el acceso para los demas usuarios via puerto 5432
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 5432 -j DROP
-A RH-Firewall-1-INPUT -p tcp -m tcp --dport 23 -j DROP

COMMIT
# Completed on Tue Feb  1 14:12:21 2011
```

Figura 4.8: Archivo de configuración del servidor iptables

[52] IPTABLES.- Es un sistema de firewall vinculado al kernel de Linux. (Fuente: http://www.pello.info/filez/firewall/iptables.html)

4.2 PARAMETRIZACIÓN DEL SISTEMA DE GESTIÓN DOCUMENTAL QUIPUX

En este subcapítulo se define la parametrización del Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital. La parametrización consiste en la configuración inicial de Quipux requerida por una institución. La Estructura Organizacional de la Notaría Digital se describe en el subcapítulo 4.3.1.1. La Estructura Organizacional se compone de áreas para clientes y funcionarios de la Notaría Digital. La creación de cuentas de usuarios en el Sistema de Gestión Documental para el prototipo de Notaría Digital se detalla en el subcapítulo 4.3.1.2. Las Carpetas Virtuales creadas para administrar el Archivo de la Notaría Digital se definen en el subcapítulo 4.3.1.3.

4.2.1 ESTRUCTURA ORGANIZACIONAL

La estructura organizacional del Sistema de Gestión Documental Quipux que utilizó el prototipo de Notaría Digital consiste en una institución que posee dos áreas. El prototipo utilizó la institución: *Notaría N del Cantón Quito*. Las áreas creadas en la institución *Notaría N del Cantón Quito* fueron: *Área Usuarios Internos* para los funcionarios que laboran en la Notaría Digital y *Área Usuarios Externos* para los clientes que requieren los servicios notariales digitales. La cuenta del Administrador del Sistema fue la cuenta encargada de crear la estructura organizacional de la Notaría Digital.

La figura 4.9 muestra los campos asignados a la nueva institución *Notaría N del Cantón Quito*. La figura 4.10 muestra los campos asignados en la creación del *Área Usuarios Internos*. La figura 4.11 muestra los campos asignados en la creación del *Área Usuarios Externos*.

Figura 4.9: Campos de la institución Notaría N del Cantón Quito

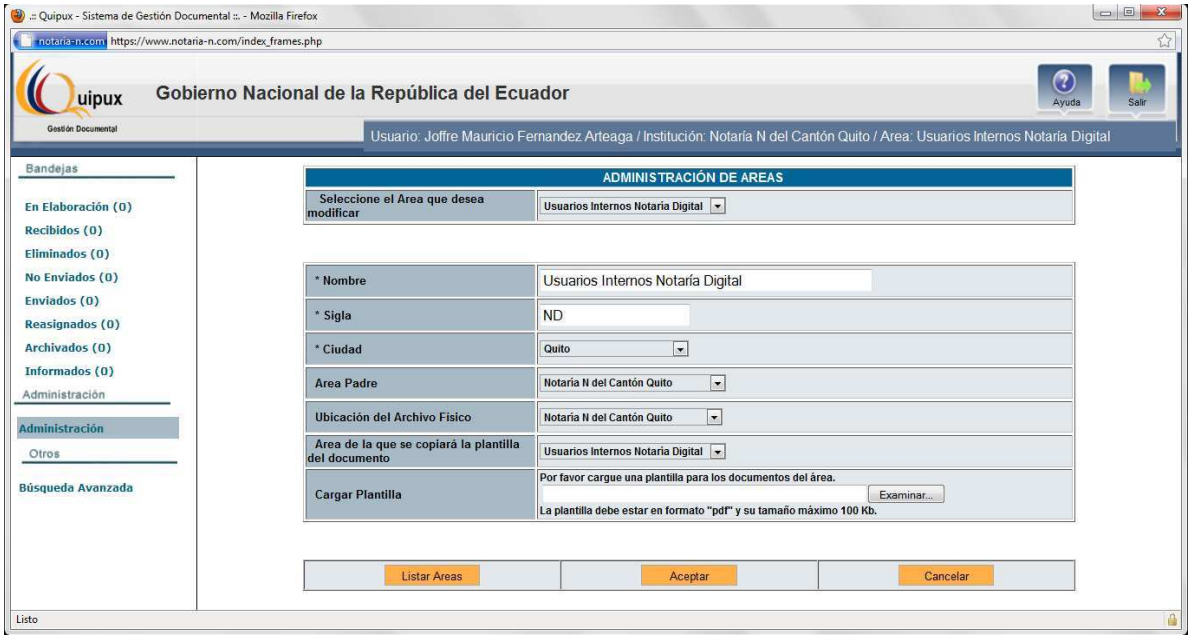

Figura 4.10: Campos del Área Usuarios Internos de la Notaría N del Cantón Quito

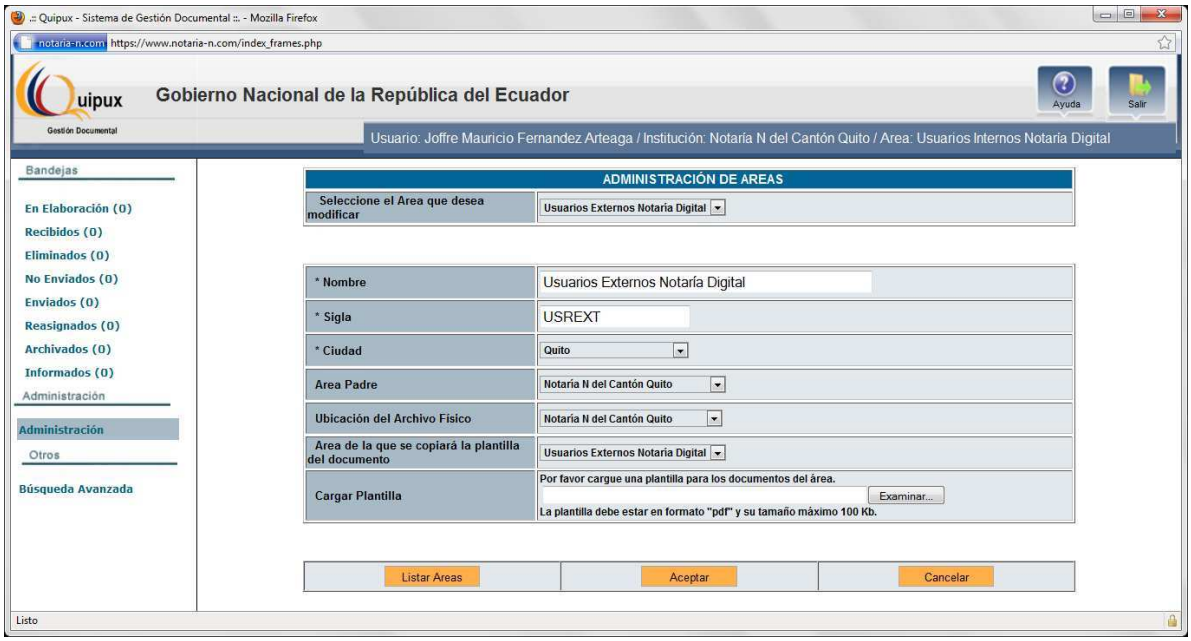

Figura 4.11: Campos del Área Usuarios Externos de la Notaría N del Cantón Quito

4.2.2 CREACIÓN DE CUENTAS DE USUARIOS

En este subcapítulo se mencionan las cuentas de usuarios del Sistema de Gestión Documental que participan en el prototipo de Notaría Digital. El prototipo de Notaría Digital no cumple con la Gestión de Identidades analizada en 3.1. La cuenta del Administrador del Sistema fue la encargada de crear todas las cuentas de usuarios para el prototipo de Notaría Digital. Las cuentas fueron creadas localmente en el Sistema de Gestión Documental Quipux. Estas cuentas no se importaron desde un Directorio de Identidades como se diseñó en el capítulo 3. En este subcapítulo se muestra la creación de la cuenta de usuario *Notaria*. El resto de cuentas de usuarios que interactúan en el prototipo de Notaría Digital se crearon de la misma manera.

Los usuarios que participarán en el Sistema de Gestión Documental Quipux para el prototipo de Notaría Digital son los descritos en la tabla 4.1. La figura 4.12 muestra los datos personales incluidos para la cuenta de usuario *Notaria* en el Sistema de Gestión Documental Quipux.

Usuario	Nombre
Notaria	Carmen Inés Suasnavas Mesa
Verificador	Arsenio Antonio Aguirre Ponce
Matrizador	Ricardo Paúl Gómez Salcedo
Administrador del Archivo	Pablo Rodrigo Carchi Alvear
Clientes	• Lorena Nathaly Polo Soria • Mérida Alexandra Rodríguez Mera
Administrador del Sistema	Joffre Mauricio Fernández Arteaga

Tabla 4.1: Usuarios de la Notaría Digital creados en Quipux

Figura 4.12: Datos personales para la cuenta del usuario "Notaria" en Quipux

La figura 4.13 señala los permisos que admite el Sistema de Gestión Documental Quipux y aquellos que se habilitaron para la cuenta del usuario Notaria. Estos permisos definen responsabilidades para cada usuario y son autorizados por el Administrador del Sistema.

Figura 4.13: Permisos para la cuenta del usuario "Notaria" en Quipux

4.2.3 CREACIÓN DE CARPETAS VIRTUALES

En este subcapítulo se describe la organización del archivo notarial digital. El Sistema de Gestión Documental Quipux ofrece la opción Archivos Digitales. Los Archivos Digitales constan de carpetas virtuales que simulan la organización anual dividida en tomos mensuales que requieren los archivos de la Notaría Digital. La cuenta del Administrador del Archivo fue la cuenta permitida para la estructuración del archivo notarial digital.

El prototipo de Notaría Digital utilizó el Sistema de Gestión Documental Quipux para crear tres archivos: *Libro de Diligencias digitales, Protocolo de Escrituras Públicas digitales* y *Minutas digitales.* Los archivos poseen una carpeta virtual para el *Año 2011*. Las carpetas virtuales anuales de cada archivo fueron divididas en tomos mensuales para: *Enero, Febrero* y *Marzo*. La figura 4.14 muestra la estructura del archivo del prototipo de Notaría Digital creado por la cuenta del Administrador del Archivo al utilizar el Sistema de Gestión Documental Quipux.

Figura 4.14: Estructura del archivo de la Notaría Digital en Quipux

4.3 CERTIFICADOS DE FIRMA ELECTRÓNICA

En este subcapítulo se define la gestión de los certificados de firma electrónica para el prototipo de Notaría Digital. El objetivo de este subcapítulo fue asimilar la creación de los certificados de firma electrónica de la ECIBCE analizada en 3.1. Los certificados de firma electrónica utilizados tendrán validez únicamente en las estaciones de trabajo que configuren a la Autoridad de Certificación de prueba como válida. El prototipo de Notaría Digital utiliza doble autenticación del usuario. Además de autenticarse con el número de cédula y password que ofrece el Quipux, se añade un nivel de seguridad al utilizar los certificados de firma electrónica detallados en este subcapítulo como método de autenticación. El prototipo de Notaría Digital no asocia las cuentas de usuarios creadas en 4.2.2 con los certificados de firma electrónica creados en 4.3.1.

La creación de los certificados de firma electrónica se define en el subcapítulo 4.3.1. La instalación de los certificados de firma electrónica se menciona en el subcapítulo 4.3.2. Y por último la firma electrónica con los certificados digitales creados en 4.3.1 se explica en el subcapítulo 4.3.3.

4.3.1 CREACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA[53]

En este subcapítulo se define la creación de los certificados de firma electrónica para el prototipo de Notaría Digital. El programa para crear certificados de firma electrónica fue OpenSSL[54], porque es un programa de software libre que genera certificados digitales. Primero se creó una Autoridad de Certificación de prueba para emitir los certificados de firma electrónica requeridos por el prototipo. Segundo se emitieron los certificados digitales para el servidor Web seguro. Y por último se emitieron los certificados de firma electrónica para todos los usuarios del prototipo de Notaría Digital. Dado que la Autoridad de Certificación es una entidad de prueba, los certificados que emita esta Autoridad también serán de prueba.

[53] Certificados digitales con OpenSSL (Fuente: http://bulma.net/body.phtml?nIdNoticia=2280)
[54] OpenSSL.- Es un proyecto de software desarrollado por los miembros de la comunidad Open Source. Permite crear certificados digitales que pueden aplicarse a un servidor, por ejemplo Apache. (Fuente: http://es.wikipedia.org/wiki/OpenSSL)

- **Creación de una Autoridad de Certificación de prueba**

Para emitir certificados de firma electrónica primero se creó una Autoridad de Certificación de prueba. La Autoridad de Certificación de prueba creada fue: *Autoridad de Confianza Electrónica*. La tabla 4.2 muestra la información solicitada por el programa OpenSSL para la creación de la Autoridad de Certificación.

Detalles propios de certificado de la Autoridad de Certificación de prueba	
Country Name	EC
State or Province Name	Pichincha
Locality Name	Quito
Organization Name (o)	Autoridad de Confianza Electrónica
Organizational Unit Name (ou)	Aplicaciones SSL
Common Name (cn)	http://www.ace-ec.com
Email Addres	soporte@ace-ec.com

Tabla 4.2: Información de la Autoridad de Certificación de prueba

- **Creación de certificados digitales para el servidor Web seguro**

La Autoridad de Certificación emitió certificados digitales para el servidor Web seguro del prototipo de Notaría Digital. El servidor Web seguro usó los certificados digitales para implementar el protocolo HTTPS, transmitir la información de manera segura y autenticarse hacia el cliente. La tabla 4.3 muestra la información solicitada por OpenSSL para la creación de los certificados digitales del servidor Web seguro.

Campos incluidos en el certificado	**Descripción**
Common Name (cn)	www.notaria-n.com
organizationName (o)	Notaria Digital N
organizationalUnitName (ou)	Servidor de Notaría Digital

Tabla 4.3: Información del certificado digital del servidor Web seguro

- **Creación de certificados de firma electrónica para los usuarios**

Los certificados de firma electrónica para los usuarios del prototipo de Notaría Digital emitidos por la Autoridad de Certificación de prueba se crearon con base en la tabla 4.2. Los usuarios usaron el certificado de firma electrónica para autenticarse ante el prototipo de Notaría Digital y firmar la documentación para realizar los trámites notariales digitales. La tabla 4.4 muestra la información solicitada por el programa OpenSSL para la creación de los certificados de firma electrónica para los usuarios.

Detalles propios de certificado de firma electrónica para el Usuario	
Common Name (cn)	Polo Soria Lorena Nathaly
organizationName (o)	Notaria Digital N
organizationalUnitName (ou)	Usuario Notaria Digital N

Tabla 4.4: Información del certificado de firma electrónica para el usuario

4.3.2 INSTALACIÓN DE CERTIFICADOS DE FIRMA ELECTRÓNICA

En este subcapítulo se muestran los certificados de firma electrónica de los usuarios instalados para usar en el prototipo de Notaría Digital. La estructura MMC[55] a través de la herramienta Certificados del Sistema Operativo Windows se utilizó para instalar los certificados de firma electrónica de los usuarios. En la figura 4.15 se muestran los certificados de firma electrónica de los usuarios instalados en la misma estación de trabajo. Adicionalmente se observa que todos los usuarios pertenecen a la Autoridad de Certificación creada en 4.3.1. Los certificados digitales de la Autoridad de Certificación, del Servidor Web seguro y de los usuarios se instalan en diferentes carpetas. Para visualizar la información de los certificados se usó el programa Mozilla

[55] MMC (Microsoft Managment Console).- Es una estructura que aloja herramientas administrativas llamadas complementos, en los sistemas operativos Windows. (Fuente: http://msdn.microsoft.com/en-us/library/bb756943.aspx)

Firefox[56], ya que es un programa de software libre y además viene instalado con el Sistema Operativo Linux CentOS 5.4.

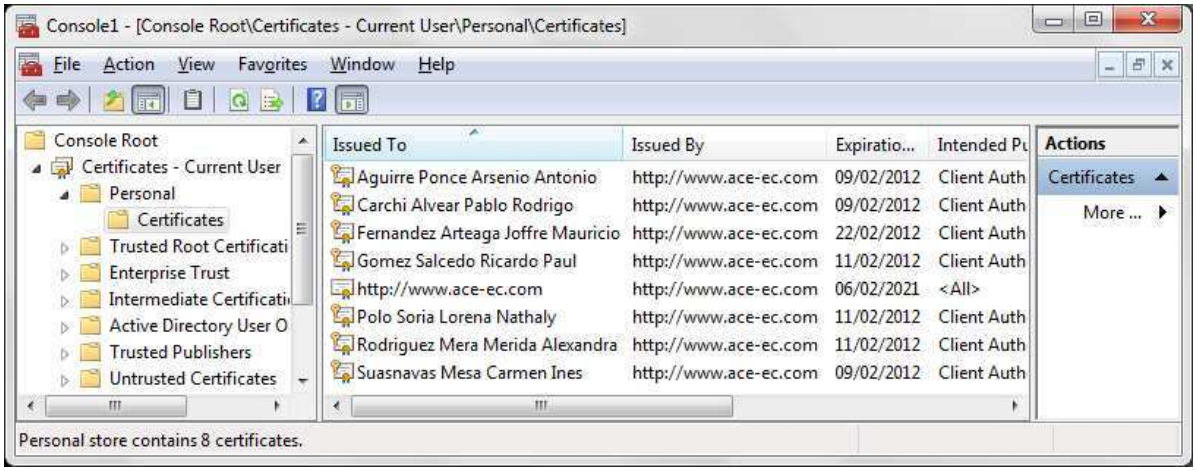

Figura 4.15: Certificados de firma electrónica instalados

- **Certificado de la Autoridad de Certificación**

La figura 4.16 muestra el certificado de la Autoridad de Certificación instalado en el programa Mozilla Firefox con la información de la tabla 4.3. La validez del certificado de la Autoridad de Confianza Electrónica es 10 años.

- **Certificado digital del servidor Web seguro**

La figura 4.17 muestra el certificado del servidor Web seguro instalado en el programa Mozilla Firefox con la información de la tabla 4.4. La validez del certificado digital del servidor Web seguro www.notaria-n.com es 10 años.

- **Certificado de firma electrónica del usuario**

La figura 4.18 muestra el certificado de firma electrónica para el usuario instalado en el programa Mozilla Firefox con la información de la tabla 4.5. La validez del certificado de firma electrónica del usuario es 1 año.

[56] Mozilla Firefox.- Es un programa para navegar por la web. (Fuente: http://www.mozilla.com/es-ES/firefox/)

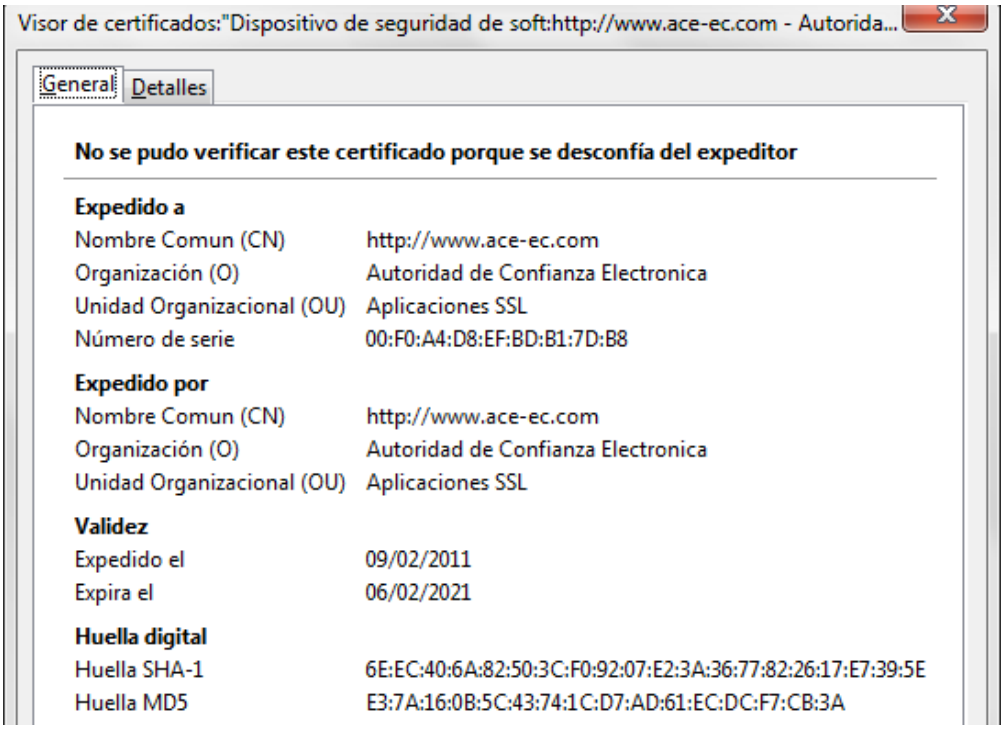

Figura 4.16: Certificado de la Autoridad de Certificación

Figura 4.17: Certificado digital del servidor Web seguro

Figura 4.18: Certificado de firma electrónica para los usuarios

4.3.3 FIRMA ELECTRÓNICA CON EL PROGRAMA JSIGNPDF

En este subcapítulo se muestra la aplicación del programa JSignPdf para firmar electrónicamente documentos notariales digitales. El prototipo de Notaría Digital utiliza este programa para firmar electrónicamente por recomendación de la ECIBCE[57]. El instalador del programa se descargó de la página http://jsignpdf.sourceforge.net/. El documento JSignPdf Quick Start Guide ofrece información detallada sobre cómo utilizar el programa JsignPdf. Este documento está incluido en el directorio donde se instala el programa JsignPdf.

El prototipo de Notaría Digital utilizó los siguientes campos del programa JSignPdf. En el campo *Key Alias* se escoge el certificado de firma electrónica del usuario que vaya a firmar el documento digital PDF. En el campo *Input PDF file* se selecciona el documento digital que se desee firmar electrónicamente. En el campo *Output PDF file* se elige el nombre y la ubicación donde se almacenará el documento digital firmado electrónicamente. En el campo *Reason* se redacta el mensaje que sustituye

[57] Taller de Firma Electrónica de la ECIBCE. Página 10.

al concuerdo de la documentación notarial. El cuadro de *Visible Signature* debe estar marcado para que la firma electrónicamente aparezca en el documento notarial. La opción *Settings* permite ubicar la firma electrónica en un lugar específico del documento digital PDF. El cuadro *Append Signature* debe estar marcado para incluir varias firmas electrónicas en el documento notarial. El botón *Sign It* realiza el procedimiento de firmado electrónico en el documento digital.

El programa JSignPdf admite el marcado de tiempo. La opción TSA/OCSP/CRL permite incluir la URL de una TSA. El prototipo de Notaría Digital implementado en este proyecto de titulación no usó el servicio de marcado de tiempo debido a que en el Ecuador no existe una TSA en la actualidad. La fecha y hora implantadas en el documento digital proceden del equipo en que se realizó el firmado electrónico.

La figura 4.19 muestra la ventana con los campos del programa JSignPdf. La figura 4.20 muestra el documento digital PDF firmado electrónicamente en la parte izquierda y las propiedades de la firma electrónica en la parte derecha. El programa Adobe Reader requiere la configuración manual de la Autoridad de Certificación descrita en 4.3.1 para validar las firmas electrónicas emitidas.

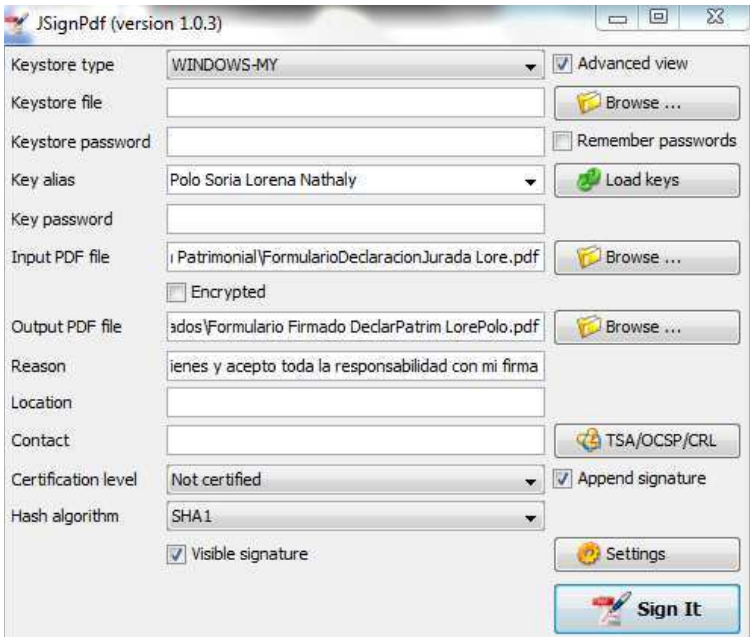

Figura 4.19: Programa JSignPdf para firma electrónica de un documento notarial

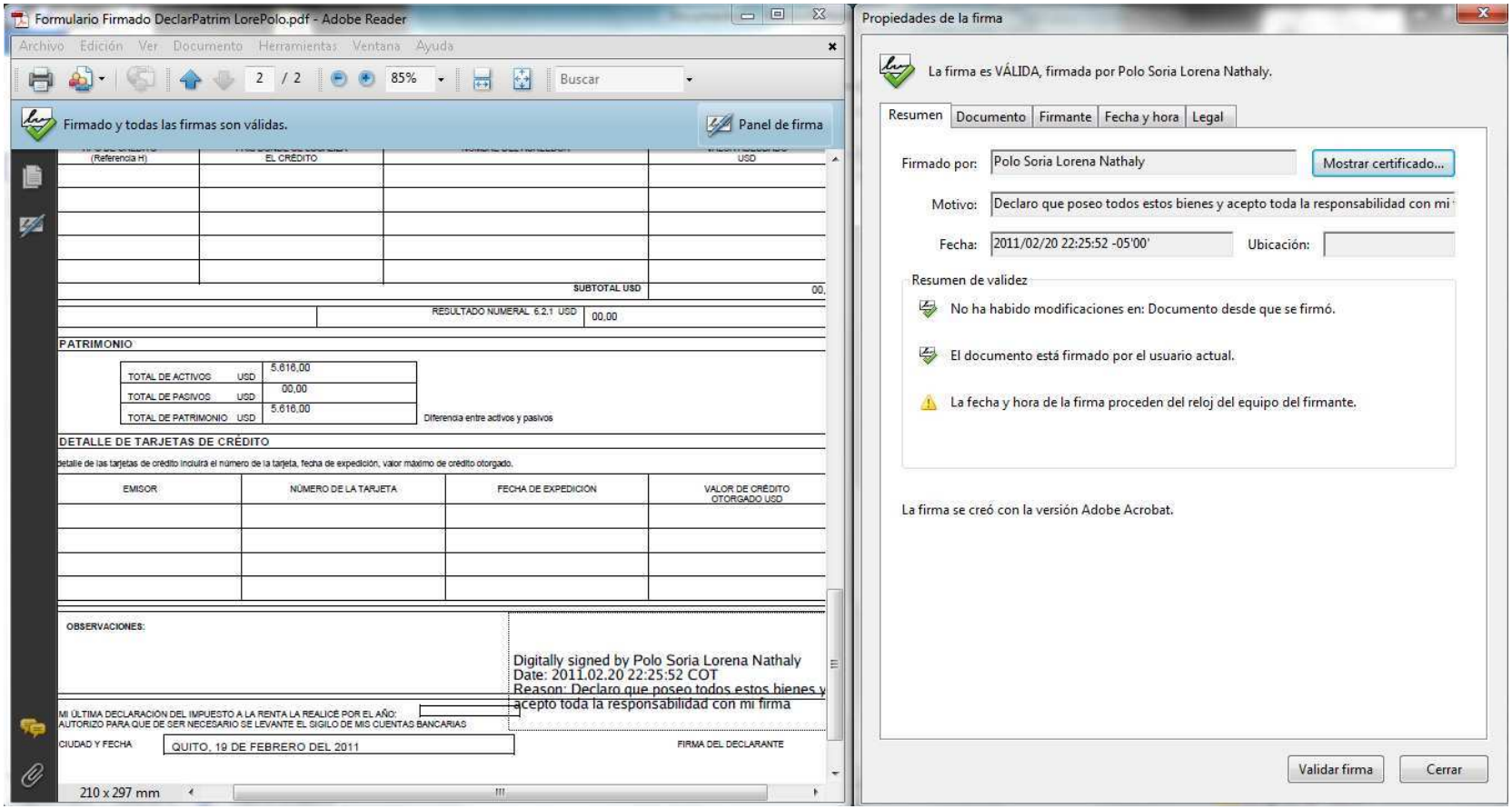

Figura 4.20: Formulario digital de Declaración Patrimonial firmado electrónicamente y validado

4.4 CONFIGURACIÓN DE LA RED FÍSICA DEL PROTOTIPO DE NOTARÍA DIGITAL

En este subcapítulo se configura la red de datos del prototipo de Notaría Digital. El diseño de la red de datos de la Notaría Digital de la figura 3.22 se resume para el prototipo de Notaría Digital en dos estaciones de trabajo conectadas en red mediante un cable UTP CAT 6[58] a través de un switch de laboratorio, como se muestra en la figura 4.21. El prototipo de Notaría Digital se define sobre un segmento de red con una estación de trabajo que realiza la función de servidor y otra desde donde acceden los usuarios que intervienen en los trámites notariales digitales. El servidor consiste del Sistema de Gestión Documental Quipux configurado en 4.1.1 y parametrizado en 4.2. Los usuarios mencionados en la tabla 4.2 acceden al servicio del Sistema de Gestión Documental Quipux.

La red de datos utilizada en el prototipo de Notaría Digital es la red privada 192.168.1.0/24. El Servidor que contiene el Sistema de Gestión Documental Quipux instalado en el Sistema Operativo Linux CentOS 5.4 posee la dirección IP 192.168.1.4/24. Los funcionarios de la Notaría Digital acceden con dirección IP 192.168.1.20/24. Los clientes de la Notaría Digital acceden con la dirección IP 192.168.1.100/24. Ambas direcciones IP están dentro del rango de la red privada.

El prototipo aprovechó el mismo Servidor con Sistema Operativo Linux CentOS 5.4 para la configuración de la Autoridad de Certificación local descrita en 4.3.1. El prototipo además utilizó el mismo Servidor para configurar el servicio DNS desarrollado en 4.1.2. El servidor Firewall con base en *iptables* explicado en 4.1.3 también se configuró en el mismo servidor Linux CentOS 5.4. Esta integración de servicios se realizó debido a que se trató de un prototipo y no de un ambiente de producción. La figura 4.21 muestra el diagrama esquemático de la red física del prototipo de Notaría Digital.

[58] Cable UTP CAT 6 (ANSI/TIA/EIA-568-B.2-1).- Estándar de cables para Gigabit Ethernet. El cable posee 4 pares de cable de cobre trenzado. Alcanza frecuencias de hasta 250 MHz por cada par y capacidad de hasta 1 Gbps. (Fuente: http://es.wikipedia.org/wiki/Cable_de_categor%C3%ADa_6)

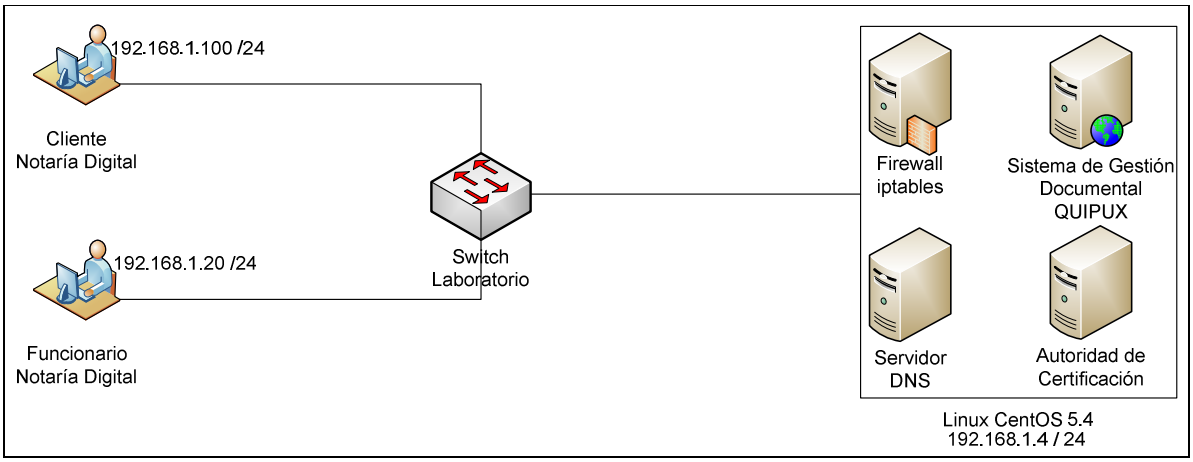

Figura 4.21: Diagrama esquemático de la red física del prototipo de Notaría Digital

4.5 PRUEBAS DEL PROTOTIPO DE NOTARÍA DIGITAL

En este subcapítulo se realizan las pruebas del prototipo de Notaría Digital con base en los trámites notariales digitales. El objetivo de este proyecto de titulación fue implantar cinco trámites notariales digitales. Las pruebas del prototipo de Notaría Digital determinan la validez de la realización de trámites notariales digitales en el Ecuador. Las pruebas utilizaron las herramientas tecnológicas disponibles mencionadas en este capítulo. Este subcapítulo concluye con el análisis de los resultados de las pruebas del prototipo de Notaría Digital en la sección 4.5.6 con base en los protocolos de los cinco trámites notariales digitales.

Las pruebas del prototipo de Notaría Digital presenta una limitación para cumplir un flujo de trabajo automatizado. El Sistema de Gestión Documental Quipux no ofrece Workflow, razón por la cual en el prototipo de Notaría Digital se realizaron manualmente los protocolos de los trámites notariales digitales. El Workflow de Notarías Digitales es necesario para obtener un sistema distribuido seguro y automatizado. Sin embargo el prototipo utilizó la herramienta Quipux, aún con esta limitación. El browser utilizado fue Mozilla Firefox por ser compatible con Quipux.

Las pruebas del prototipo de Notaría Digital muestran de manera resumida los protocolos de los cinco trámites notariales digitales propuestos en el subcapítulo 3.2.3. Las pruebas del prototipo de Notaría Digital muestran en un principio el requisito del protocolo para iniciar el trámite notarial digital. Las pruebas además muestran el resultado obtenido en el protocolo de los trámites del prototipo de Notaría Digital.

La tabla 4.5 muestra los parámetros de las pruebas del prototipo de Notaría Digital. La primera columna detalla los cinco trámites notariales digitales. La segunda columna describe el requisito de entrada al trámite notarial digital. Y la tercera columna señala el resultado del trámite notarial digital.

Trámite notarial	**Requisito de entrada**	**Resultado del trámite notarial**
Declaración Patrimonial Jurada	Formulario digital de la Contraloría General del Estado firmado electrónicamente.	Escritura Pública digital de Declaración Patrimonial Jurada.
Declaración Juramentada	Documento digital con el texto a declarar firmado.	Escritura Pública digital de Declaración Juramentada.
Poder Especial	Minuta digital de Poder Especial firmada electrónicamente por un Abogado.	Escritura Pública digital de Poder Especial.
Fiel Copia del Original	Documento digital original.	Número de copias solicitadas del documento digital original certificadas.
Compraventa Vehicular	Contrato digital de Compraventa Vehicular firmado.	Acta digital de Compraventa Vehicular.

Tabla 4.5: Parámetros de las pruebas del prototipo de Notaría Digital

4.5.1 TRÁMITE DIGITAL DECLARACIÓN PATRIMONIAL JURADA

La entrada de la prueba del trámite notarial digital Declaración Patrimonial Jurada consiste en el inicio del requerimiento notarial por parte del cliente. El cliente redactó su *Nuevo* mensaje e incluyó como *Anexo* su Formulario digital de Declaración Patrimonial Jurada firmado electrónicamente por el cliente.

La figura 4.22 indica la captura de la entrada a la prueba del trámite digital Declaración Patrimonial Jurada. El cliente autenticado en el Sistema de Gestión Documental Quipux fue *Lorena Nathaly Polo Soria*. La parte derecha de la figura indica el Formulario digital de Declaración Patrimonial Jurada en formato PDF firmado electrónicamente por el cliente. La parte izquierda de la figura muestra el anexado del formulario digital en un *Nuevo* mensaje en Quipux.

El resultado de la prueba del trámite notarial digital Declaración Patrimonial Jurada se señala en el lado del cliente y en la Notaría Digital. El resultado en el lado del cliente consta de las dos copias de su Escritura Pública de Declaración Patrimonial Jurada. El resultado en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo consiste en el almacenamiento del mensaje que contiene la Escritura de Declaración Patrimonial Jurada en el Protocolo de Escrituras Públicas del archivo notarial digital.

La figura 4.23 indica la captura del resultado de la prueba del trámite notarial digital Declaración Patrimonial Jurada en el lado del cliente. En la parte izquierda de la figura se muestran las dos copias de la Escritura Pública de Declaración Patrimonial Jurada adjuntas en un mensaje *Recibido*. En la parte derecha de la figura se indica la segunda copia en formato PDF de la Escritura Pública de Declaración Patrimonial Jurada de *Lorena Nathaly Polo Soria* certificada por la Notaría.

La figura 4.24 muestra la captura del resultado de la prueba del trámite notarial digital Declaración Patrimonial Jurada en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo. El usuario autenticado como Administrador del Archivo en el Sistema de Gestión Documental Quipux fue *Pablo Rodrigo Carchi Alvear*. En la

parte izquierda de la figura se muestra el archivado del mensaje *Recibido* en el tomo mensual de *Febrero* del año *2011* de la carpeta virtual *Protocolo de Escrituras Públicas digitales*. En la parte derecha de la figura se indica la Escritura Pública digital en formato PDF de la Declaración Patrimonial Jurada de *Lorena Nathaly Polo Soria* que consta como anexo en el mensaje archivado.

4.5.2 TRÁMITE DIGITAL DECLARACIÓN JURAMENTADA

La entrada de la prueba del trámite notarial digital Declaración Juramentada consiste en el inicio del requerimiento notarial por parte del cliente. El cliente redactó su *Nuevo* mensaje e incluyó como *Anexo* su documento digital con el texto a declarar firmado electrónicamente por el cliente.

La figura 4.25 indica la captura de la entrada a la prueba del trámite digital Declaración Juramentada. El cliente autenticado en el Sistema de Gestión Documental Quipux fue *Lorena Nathaly Polo Soria*. La parte derecha de la figura indica el documento digital con el texto a declarar en formato PDF firmado electrónicamente por el cliente. La parte izquierda de la figura muestra el anexado del documento digital en un *Nuevo* mensaje en el Sistema de Gestión Documental.

El resultado de la prueba del trámite notarial digital Declaración Juramentada se señala en el lado del cliente y en la Notaría Digital. El resultado en el lado del cliente consta de dos copias de su Escritura Pública de Declaración Juramentada. El resultado en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo consiste en el almacenamiento del mensaje que contiene la Escritura de Declaración Juramentada en el Protocolo de Escrituras Públicas del archivo notarial.

La figura 4.26 indica la captura del resultado de la prueba del trámite notarial digital Declaración Juramentada en el lado del cliente. En la parte izquierda de la figura se muestran las dos copias de la Escritura Pública de Declaración Juramentada adjuntas en un mensaje *Recibido*. En la parte derecha de la figura se indica la primera copia en formato PDF de la Escritura Pública de Declaración Juramentada de *Lorena Nathaly Polo Soria* certificada por la Notaría.

La figura 4.27 muestra la captura del resultado de la prueba del trámite notarial digital Declaración Juramentada en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo. El usuario autenticado como Administrador del Archivo en el Sistema de Gestión Documental Quipux fue *Pablo Rodrigo Carchi Alvear*. En la parte izquierda de la figura se muestra el archivado del mensaje *Recibido* en el tomo mensual de *Febrero* del año *2011* de la carpeta virtual *Protocolo de Escrituras Públicas digitales*. En la parte derecha de la figura se indica la Escritura Pública digital en formato PDF de la Declaración Juramentada de *Lorena Nathaly Polo Soria* que consta como anexo en el mensaje archivado.

4.5.3 TRÁMITE DIGITAL PODER ESPECIAL

La entrada de la prueba del trámite notarial digital Poder Especial consiste en el inicio del requerimiento notarial por parte del cliente. El cliente redactó su *Nuevo* mensaje e incluyó como *Anexo* la minuta digital de Poder Especial firmada electrónicamente por un Abogado.

La figura 4.28 indica la captura de la entrada a la prueba del trámite digital Poder Especial. El cliente autenticado en el Sistema de Gestión Documental Quipux fue *Mérida Alexandra Rodríguez Mera*. La parte derecha de la figura indica la minuta digital de Poder Especial en formato PDF firmado electrónicamente por el Abogado. La parte izquierda de la figura muestra el anexado de la minuta digital en un *Nuevo* mensaje en el Sistema de Gestión Documental Quipux.

El resultado de la prueba del trámite notarial digital Poder Especial se señala en el lado del cliente y en la Notaría Digital. El resultado en el lado del cliente consta de las dos copias de su Escritura Pública de Poder Especial. El resultado en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo consiste en el almacenamiento del mensaje que contiene la Escritura de Poder Especial en el Protocolo de Escrituras Públicas del archivo notarial digital.

La figura 4.29 indica la captura del resultado de la prueba del trámite notarial digital Poder Especial en el lado del cliente. En la parte izquierda de la figura se muestran

las dos copias de la Escritura Pública de Poder Especial adjuntas en un mensaje *Recibido*. En la parte derecha de la figura se indica la primera copia en formato PDF de la Escritura Pública de Poder Especial de *Mérida Alexandra Rodríguez Mera*.

La figura 4.30 muestra la captura del resultado de la prueba del trámite notarial digital Poder Especial en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo. El usuario autenticado como Administrador del Archivo en el Sistema de Gestión Documental Quipux fue *Pablo Rodrigo Carchi Alvear*. En la parte izquierda de la figura se muestra el archivado del mensaje *Recibido* en el tomo mensual de *Febrero* del año *2011* de la carpeta virtual *Protocolo de Escrituras Públicas digitales*. En la parte derecha de la figura se indica la Escritura Pública digital en formato PDF del Poder Especial de *Mérida Alexandra Rodríguez Mera* que consta como anexo en el mensaje archivado.

4.5.4 TRÁMITE DIGITAL FIEL COPIA DEL ORIGINAL

La entrada de la prueba del trámite notarial digital Fiel Copia del Original consiste en el inicio del requerimiento notarial por parte del cliente. El cliente redactó su *Nuevo* mensaje e incluyó como *Anexo* el documento digital original a certificar.

La figura 4.31 indica la captura de la entrada a la prueba del trámite digital Fiel Copia del Original. El cliente autenticado en el Sistema de Gestión Documental Quipux fue *Mérida Alexandra Rodríguez Mera*. La parte derecha de la figura indica el documento digital original en formato PDF. Para esta prueba del trámite digital Fiel Copia del Original se utilizó un título digital de tercer nivel de la Escuela Politécnica Nacional. La parte izquierda de la figura muestra el anexado del documento digital original en un *Nuevo* mensaje en el Sistema de Gestión Documental Quipux.

El resultado de la prueba del trámite notarial digital Poder Especial se señala en el lado del cliente y en la Notaría Digital. El resultado en el lado del cliente consta de las copias solicitadas certificadas de su documento digital original. Para esta prueba el cliente requirió tres copias certificadas del documento digital original. El resultado en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo

consiste en el almacenamiento del mensaje que contiene una copia certificada en el Libro de Diligencias del archivo notarial digital.

La figura 4.32 indica la captura del resultado de la prueba del trámite notarial digital Fiel Copia del Original en el lado del cliente. En la parte izquierda de la figura se muestran las tres copias certificadas adjuntas en un mensaje *Recibido*. En la parte derecha de la figura se indica una copia en formato PDF del documento digital original de *Mérida Alexandra Rodríguez Mera* certificada por la Notaría.

La figura 4.33 muestra la captura del resultado de la prueba del trámite notarial digital Fiel Copia del Original en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo. El usuario autenticado como Administrador del Archivo en el Sistema de Gestión Documental Quipux fue *Pablo Rodrigo Carchi Alvear*. En la parte izquierda de la figura se muestra el archivado del mensaje *Recibido* en el tomo mensual de *Marzo* del año *2011* de la carpeta virtual *Libro de Diligencias digitales*. En la parte derecha de la figura se indica la copia del documento original de *Mérida Alexandra Rodríguez Mera* que consta como anexo en el mensaje archivado.

4.5.5 TRÁMITE DIGITAL COMPRAVENTA VEHICULAR

La entrada de la prueba del trámite notarial digital Compraventa Vehicular consiste en el inicio del requerimiento notarial por parte del comprador. El comprador redactó su *Nuevo* mensaje e incluyó como *Anexo* el contrato de Compraventa Vehicular digital firmado electrónicamente por comprador y vendedor.

La figura 4.34 indica la captura de la entrada a la prueba del trámite digital Compraventa Vehicular. El cliente autenticado en el Sistema de Gestión Documental Quipux fue *Lorena Nathaly Polo Soria*. La parte derecha de la figura indica el contrato de Compraventa Vehicular digital en formato PDF firmado electrónicamente por el comprador y vendedor del vehículo. La parte izquierda de la figura muestra el anexado del Contrato Vehicular digital en un *Nuevo* mensaje en el Sistema de Gestión Documental Quipux.

El resultado de la prueba del trámite notarial digital Compraventa Vehicular se señala en el lado del comprador, vendedor y en la Notaría Digital. El resultado en el lado del comprador y vendedor consta del Acta digital de Compraventa Vehicular certificado y del Contrato Vehicular digital. El resultado en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo consiste en el almacenamiento del mensaje que contiene una copia del Acta digital de Compraventa Vehicular y del Contrato Vehicular digital en el Libro de Diligencias del archivo notarial digital.

La figura 4.35 indica la captura del resultado de la prueba del trámite notarial digital Compraventa Vehicular en el lado del comprador. En la parte izquierda de la figura se muestran el Acta digital de Compraventa Vehicular y el Contrato digital de Compraventa Vehicular adjuntos en un mensaje *Recibido* en la cuenta del comprador. En la parte derecha de la figura se indica el Acta digital de Compraventa Vehicular de *Lorena Nathaly Polo Soria* certificada por la Notaría.

La figura 4.36 indica la captura del resultado de la prueba del trámite notarial digital Compraventa Vehicular en el lado del vendedor. En la parte izquierda de la figura se muestran el Acta digital de Compraventa Vehicular y el Contrato digital de Compraventa Vehicular adjuntos en un mensaje *Recibido* en la cuenta del vendedor. En la parte derecha de la figura se indica el Acta digital de Compraventa Vehicular de *Mérida Alexandra Rodríguez Mera* certificada por la Notaría.

La figura 4.37 muestra la captura del resultado de la prueba del trámite notarial digital Compraventa Vehicular en el lado de la Notaría Digital a través de la cuenta del Administrador del Archivo. El usuario autenticado como Administrador del Archivo en el Sistema de Gestión Documental Quipux fue *Pablo Rodrigo Carchi Alvear*. En la parte izquierda de la figura se muestra el archivado del mensaje *Recibido* en el tomo mensual de *Febrero* del año *2011* de la carpeta virtual *Libro de Diligencias digitales*. En la parte derecha de la figura se indica el Acta digital de Compraventa Vehicular en formato PDF entre *Lorena Nathaly Polo Soria* y *Mérida Alexandra Rodríguez Mera* que consta como anexo en el mensaje archivado.

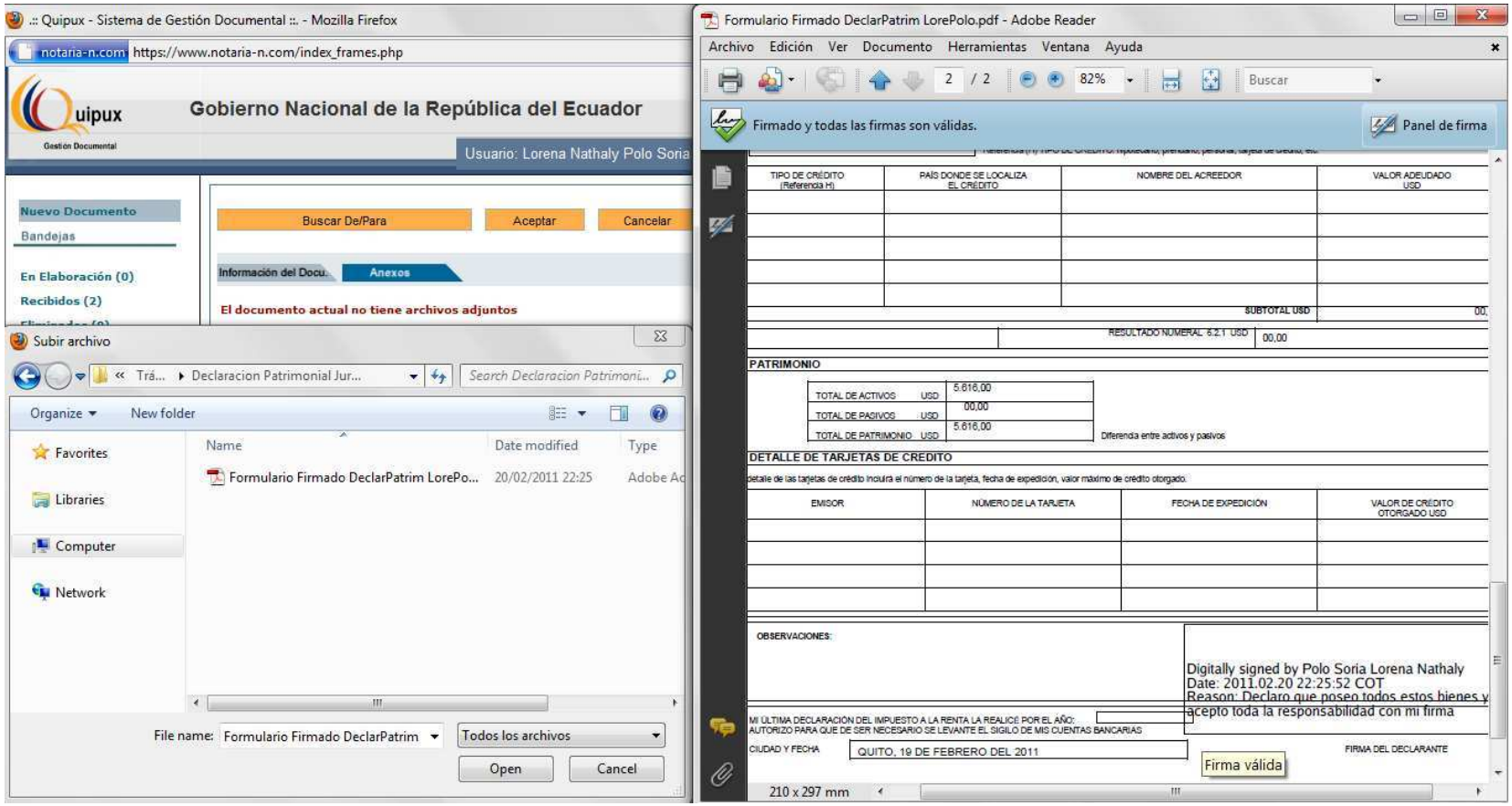

Figura 4.22: Entrada en el trámite digital Declaración Patrimonial Jurada

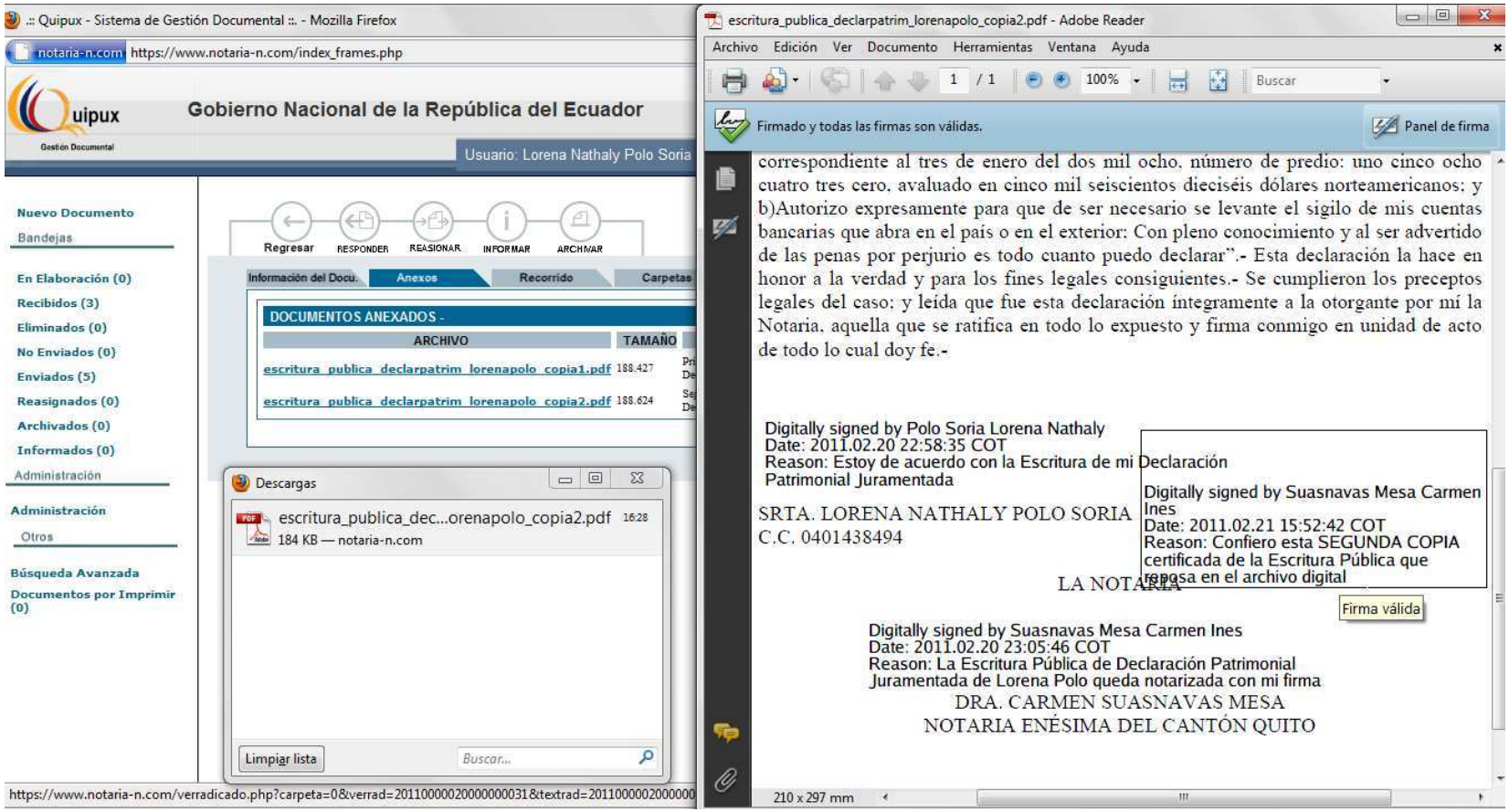

Figura 4.23: Resultado del trámite digital Declaración Patrimonial Jurada en la cuenta del Cliente

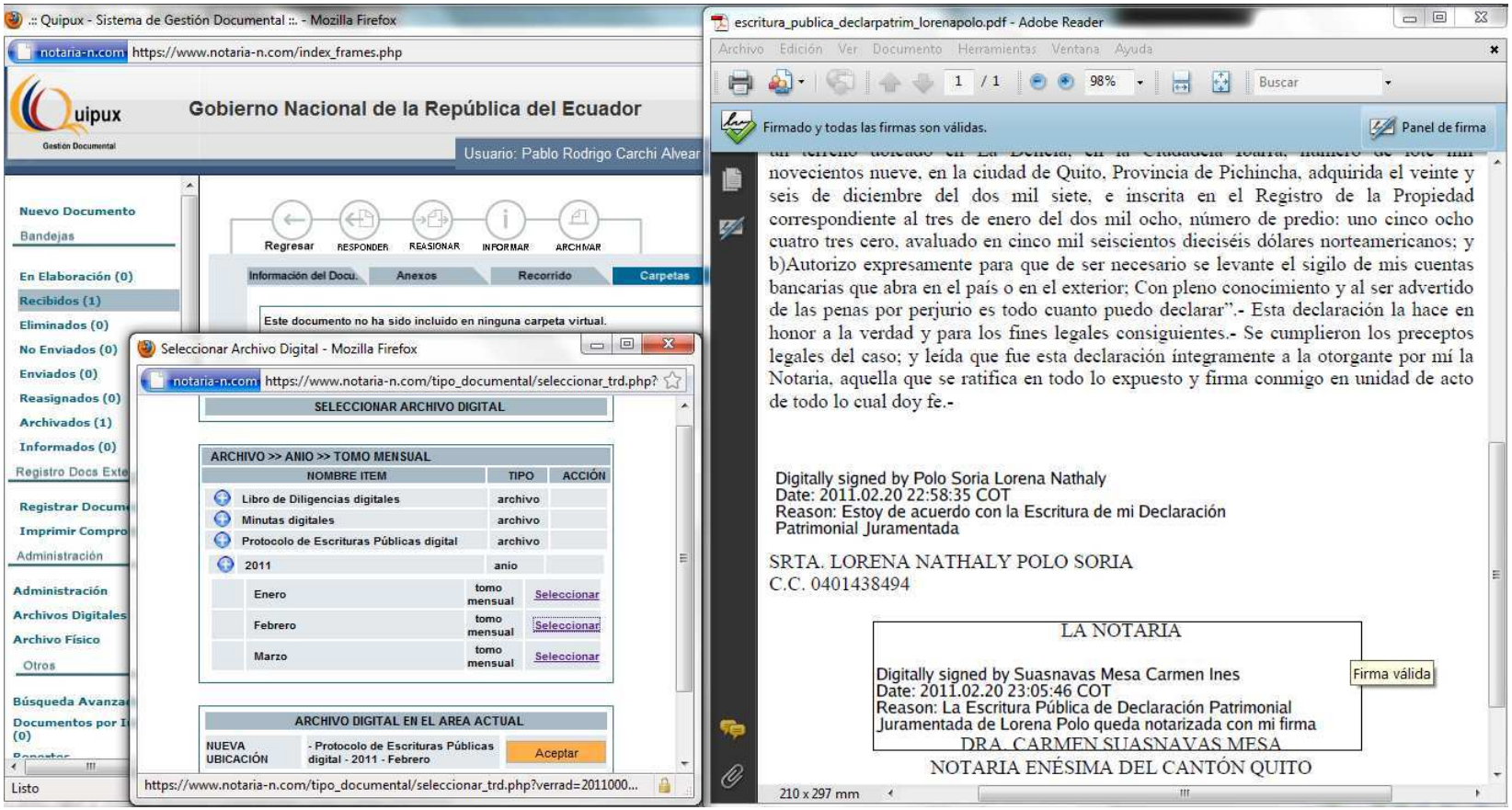

Figura 4.24: Almacenamiento de la Declaración Patrimonial Jurada en el Protocolo de Escrituras Públicas digitales

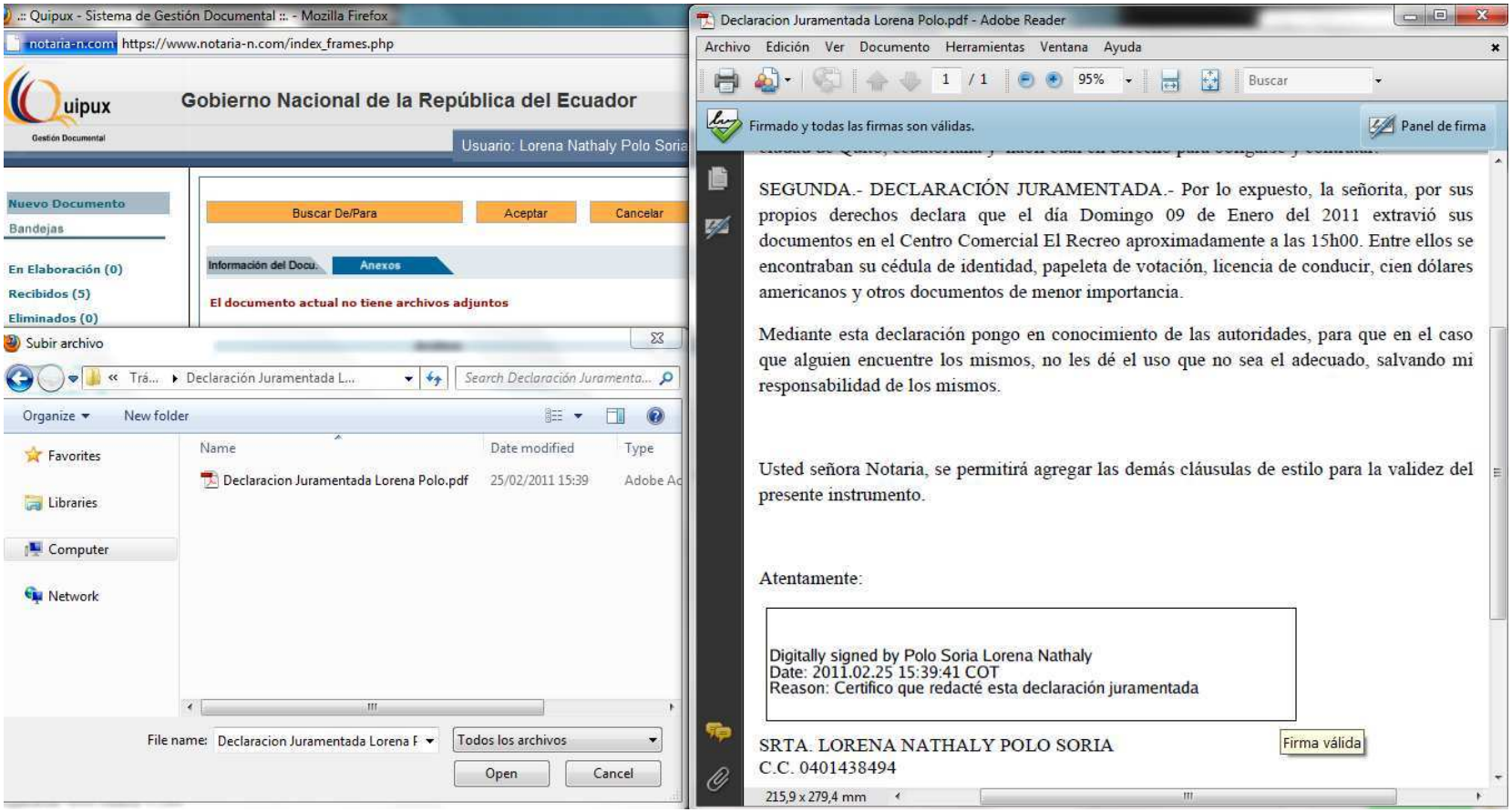

Figura 4.25: Entrada en el trámite digital Declaración Juramentada

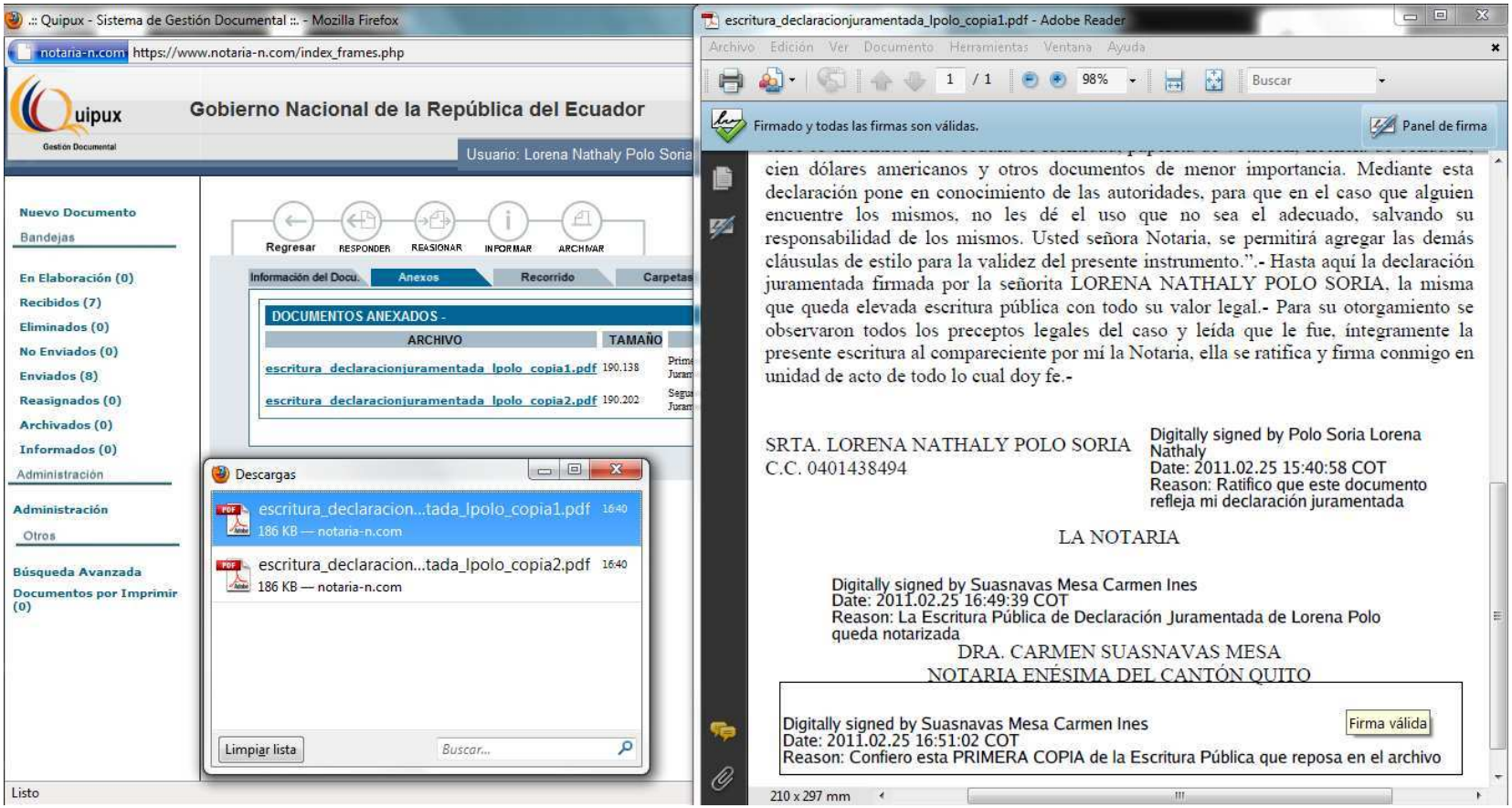

Figura 4.26: Resultado del trámite digital Declaración Juramentada en la cuenta del Cliente

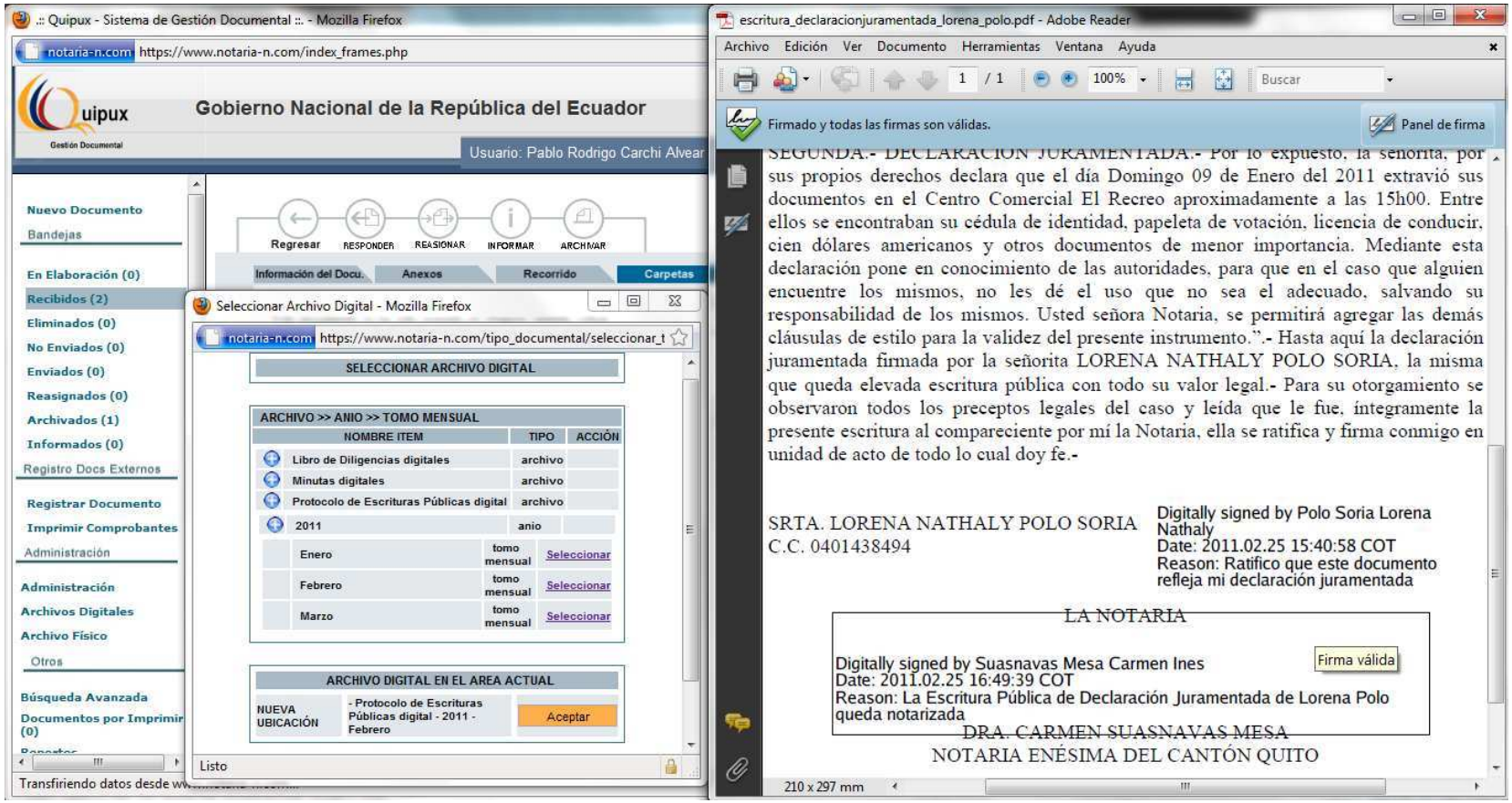

Figura 4.27: Almacenamiento de la Declaración Juramentada en el Protocolo de Escrituras Públicas digitales

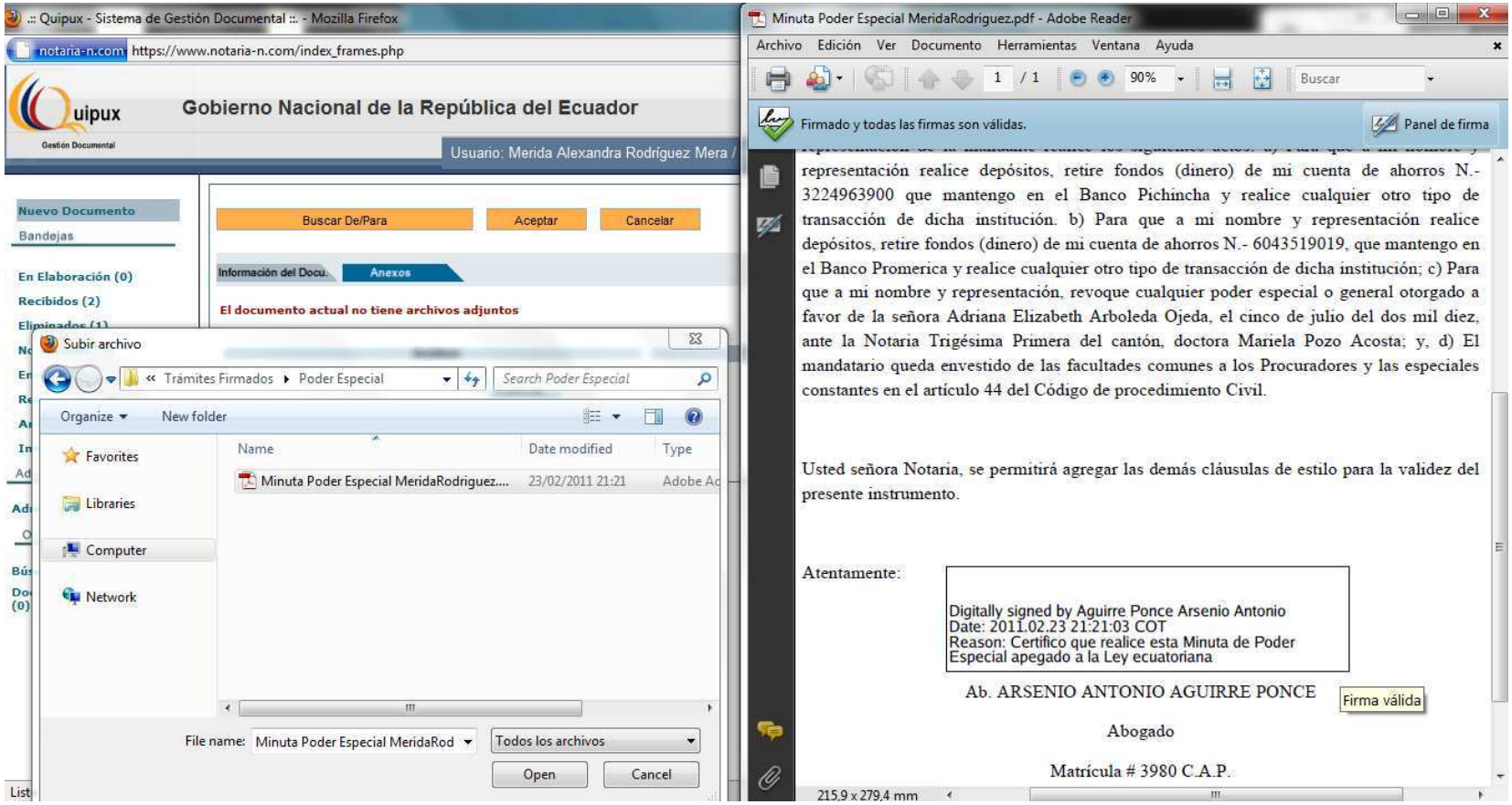

Figura 4.28: Entrada en el trámite digital Poder Especial

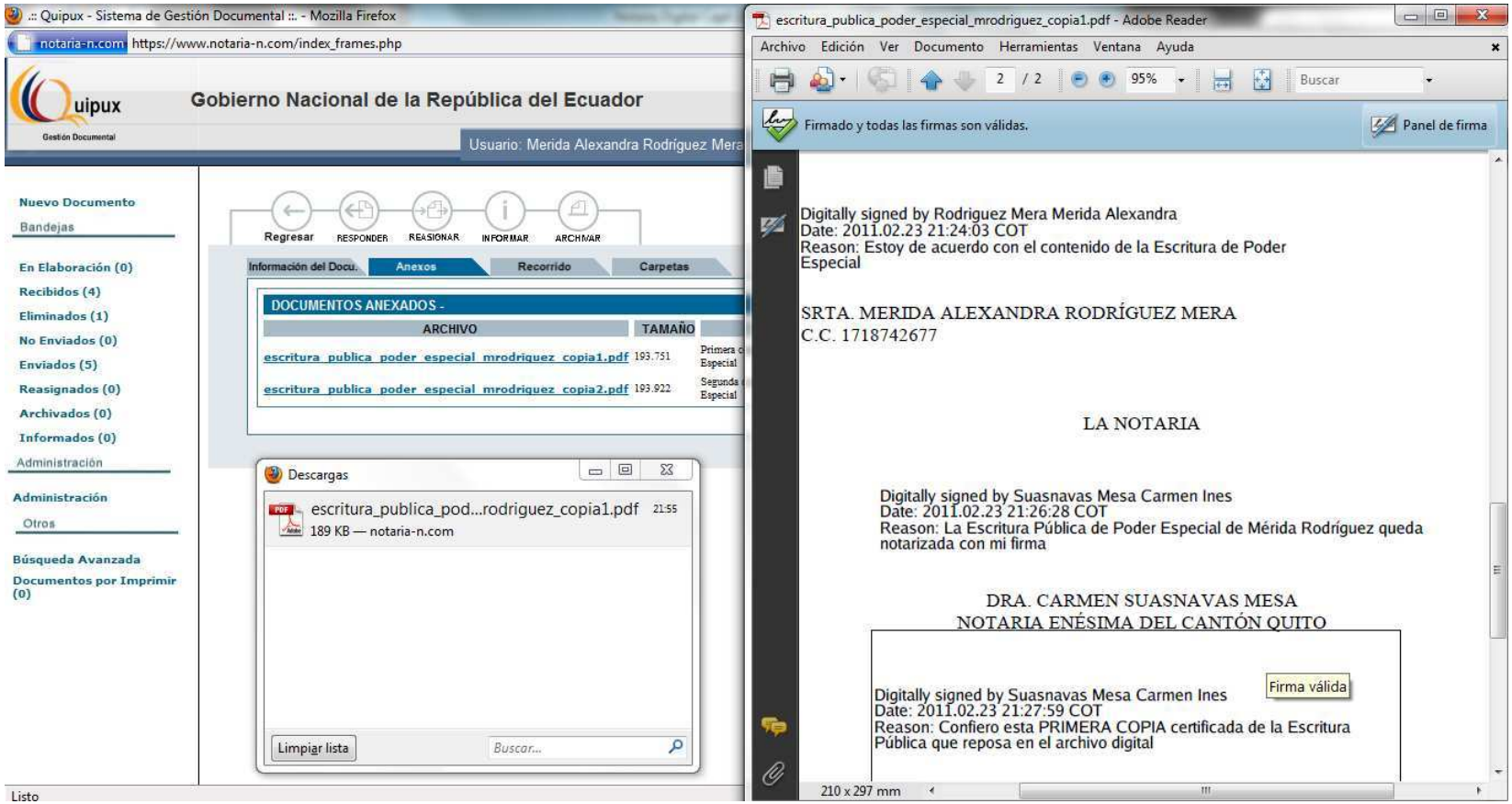

Figura 4.29: Resultado del trámite digital Poder Especial en la cuenta del Cliente

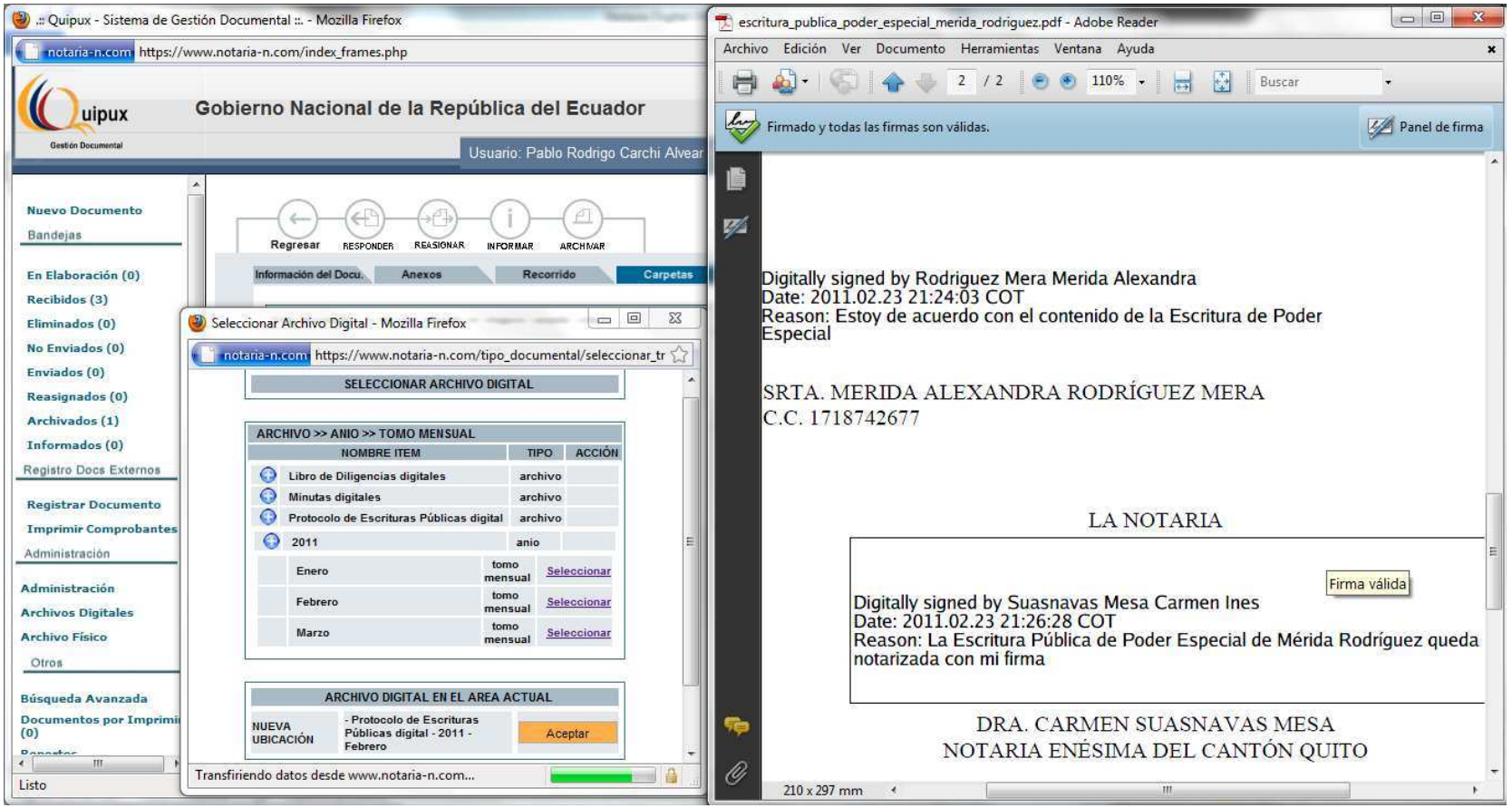

Figura 4.30: Almacenamiento del Poder Especial en el Protocolo de Escrituras Públicas digitales

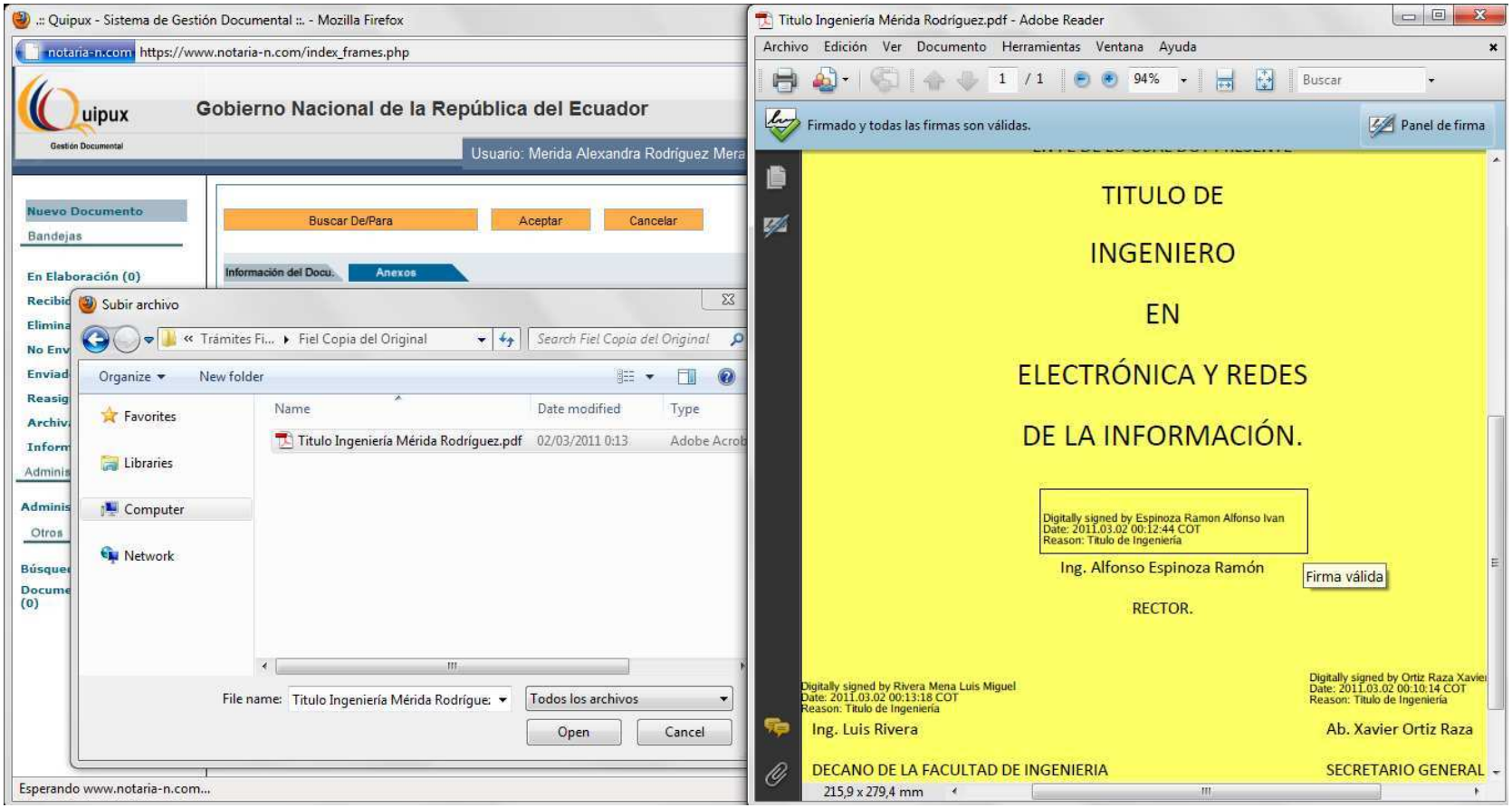

Figura 4.31: Entrada en el trámite digital Fiel Copia del Original

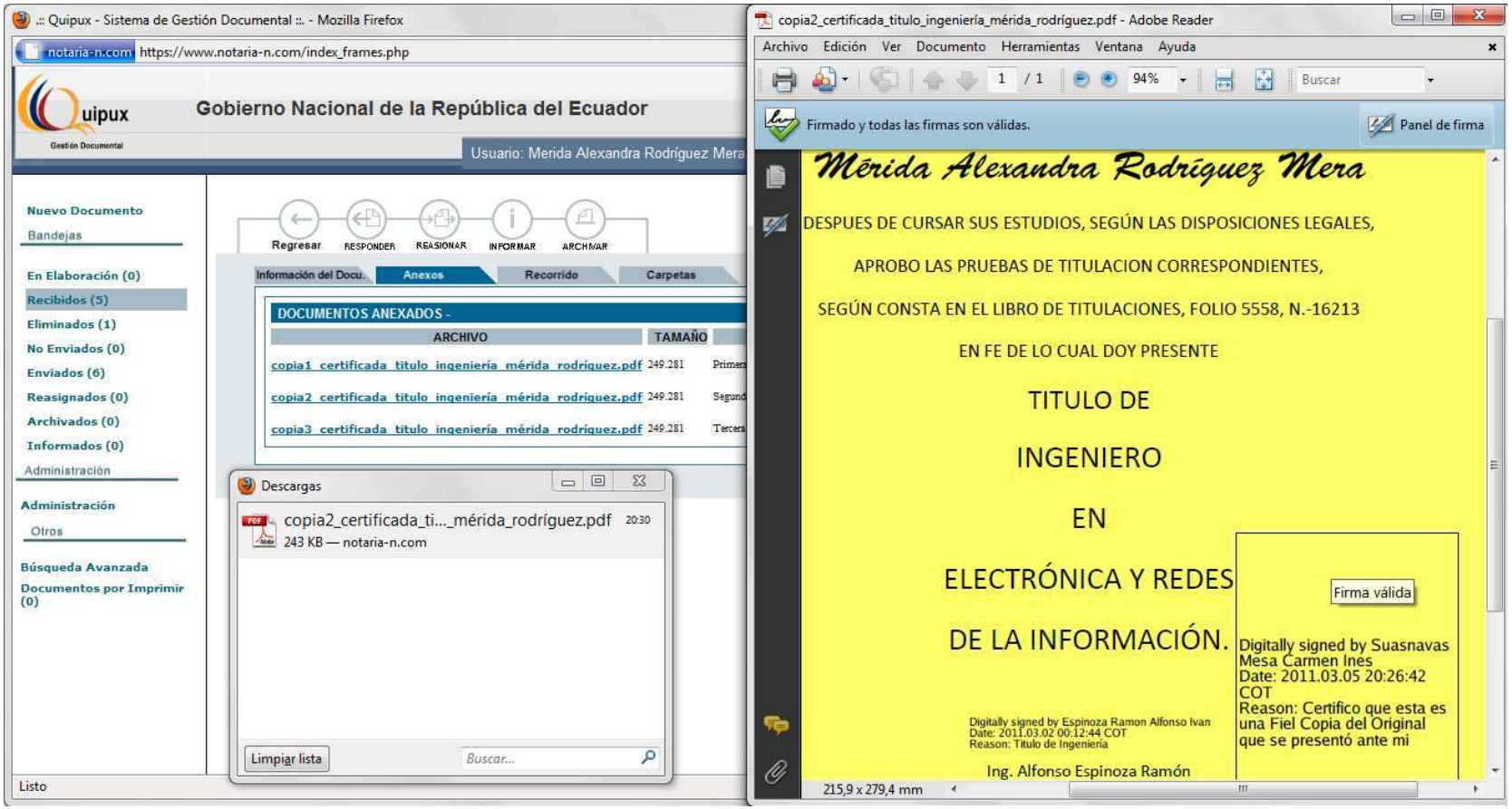

Figura 4.32: Resultado del trámite digital Fiel Copia del Original en la cuenta del Cliente

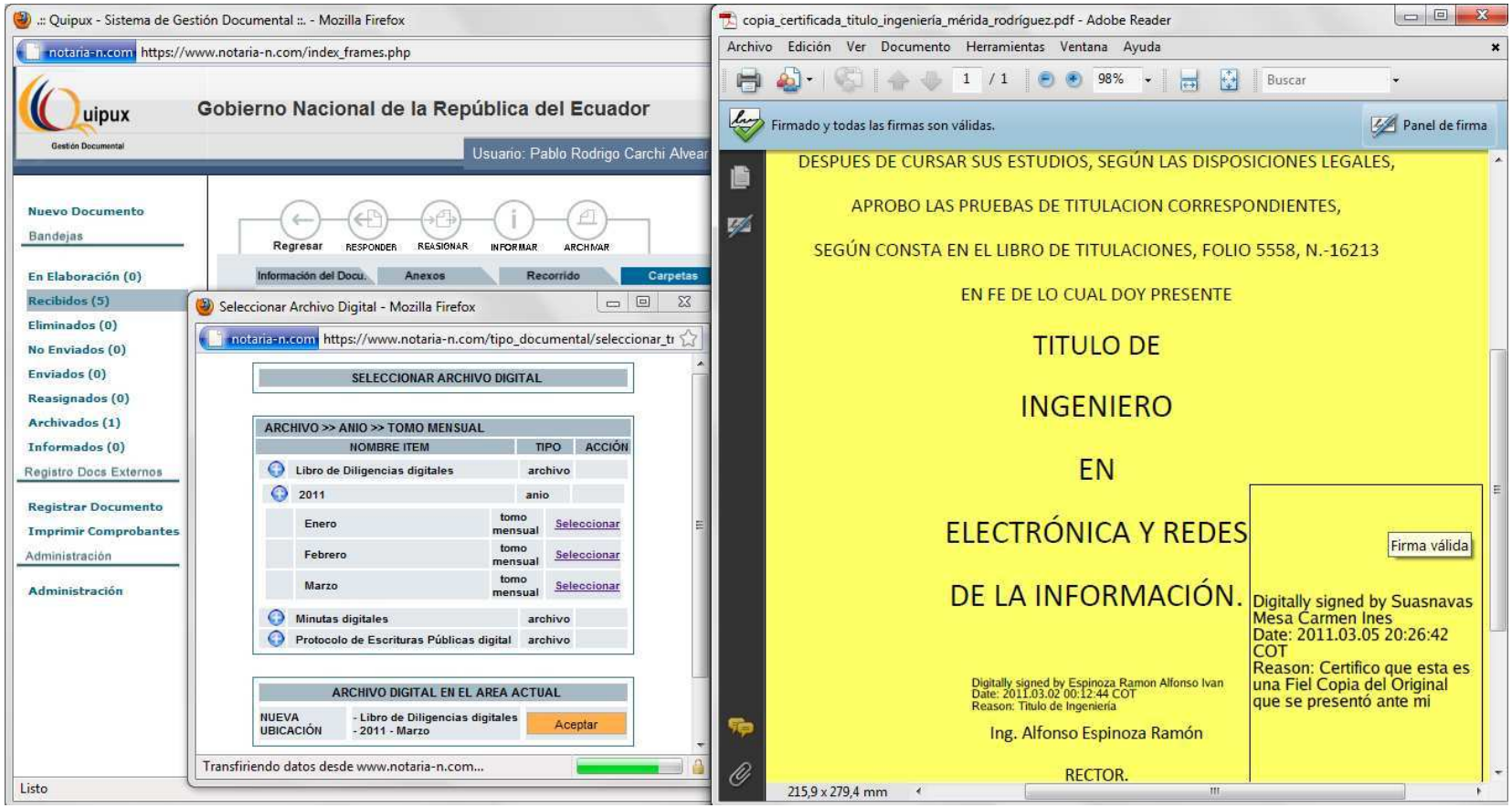

Figura 4.33: Almacenamiento del trámite digital Fiel Copia del Original en el Libro de Diligencias digitales

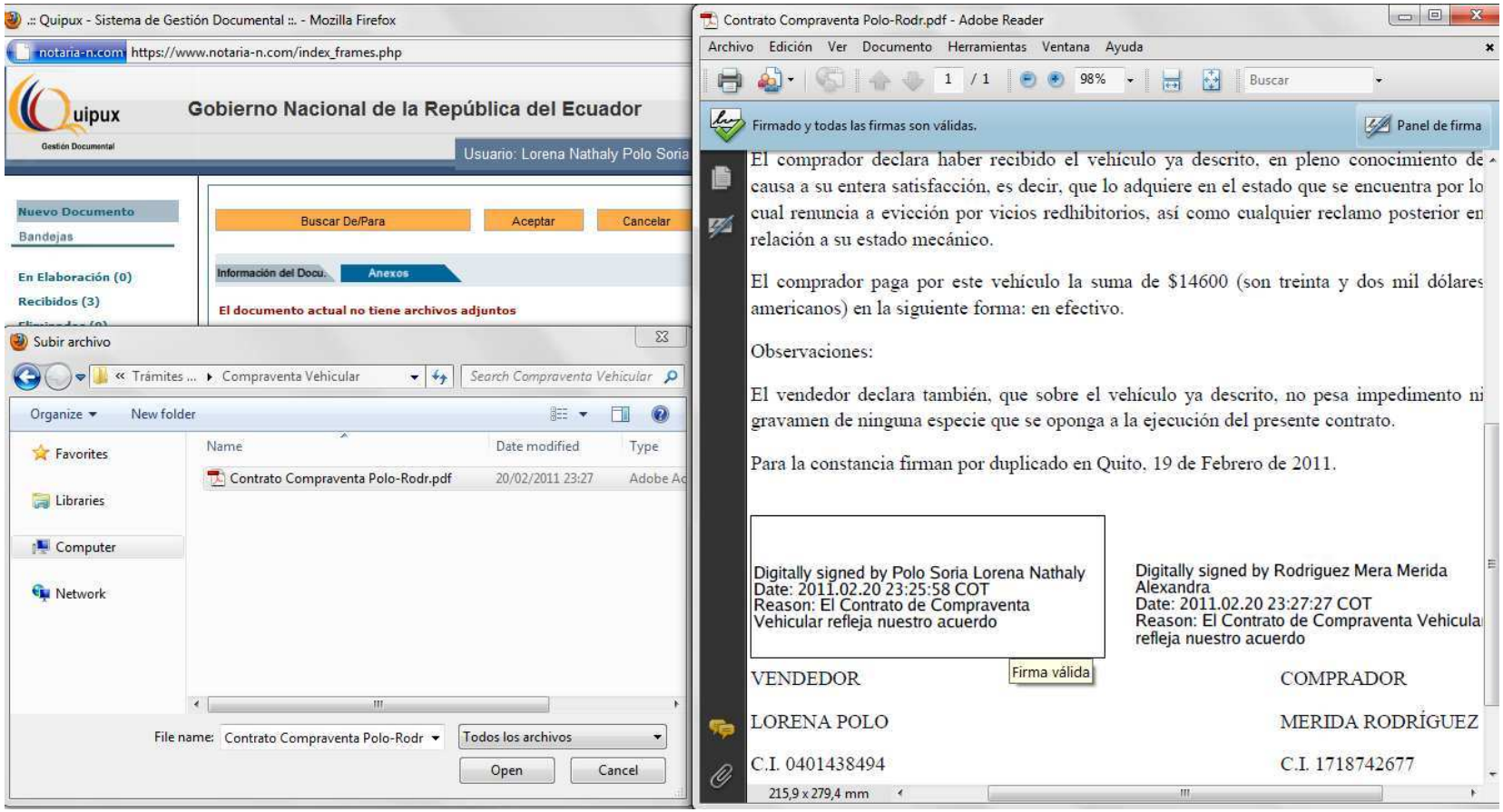

Figura 4.34: Entrada en el trámite digital Compraventa Vehicular

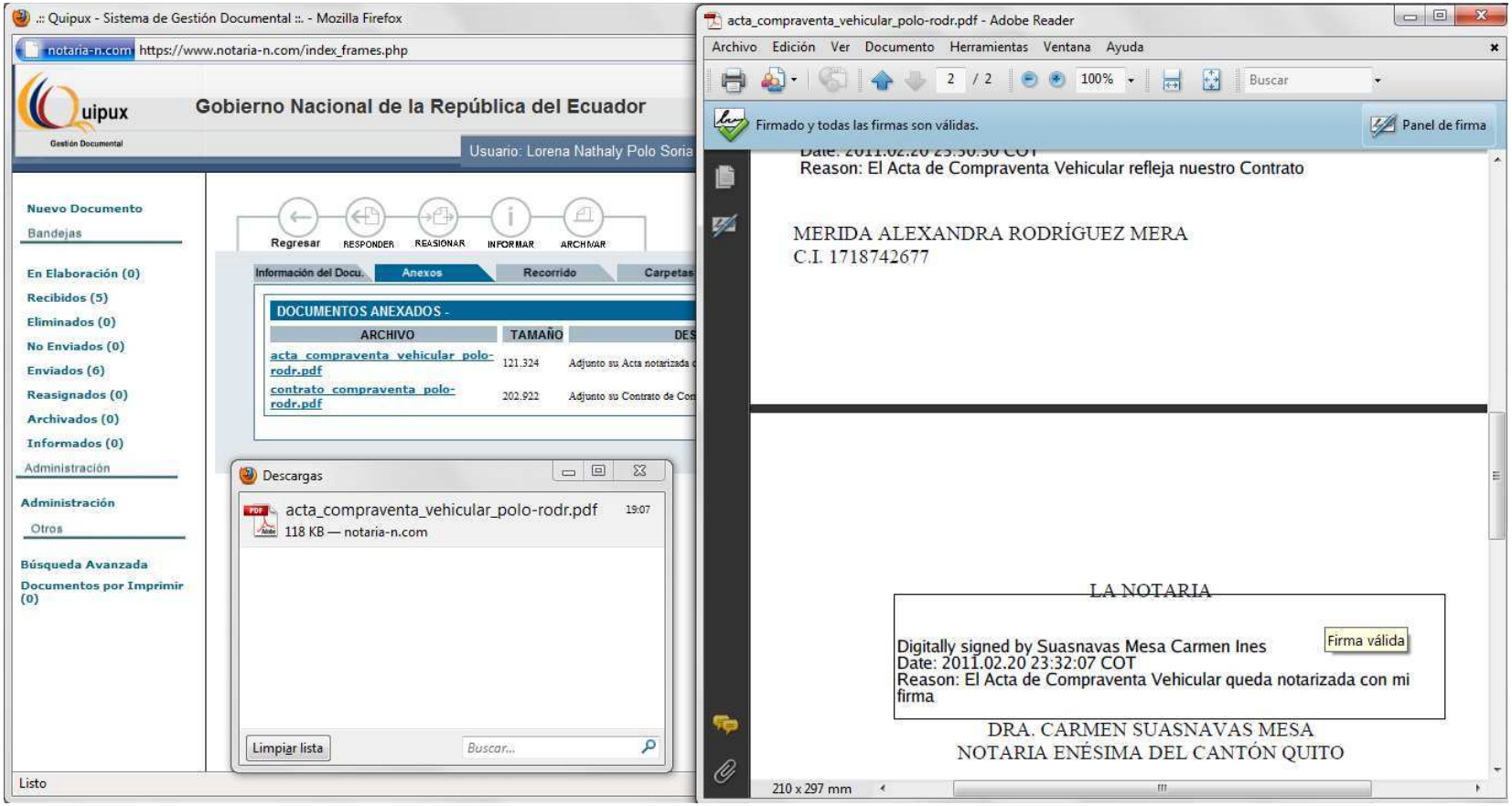

Figura 4.35: Resultado del trámite digital Compraventa Vehicular en la cuenta del Comprador

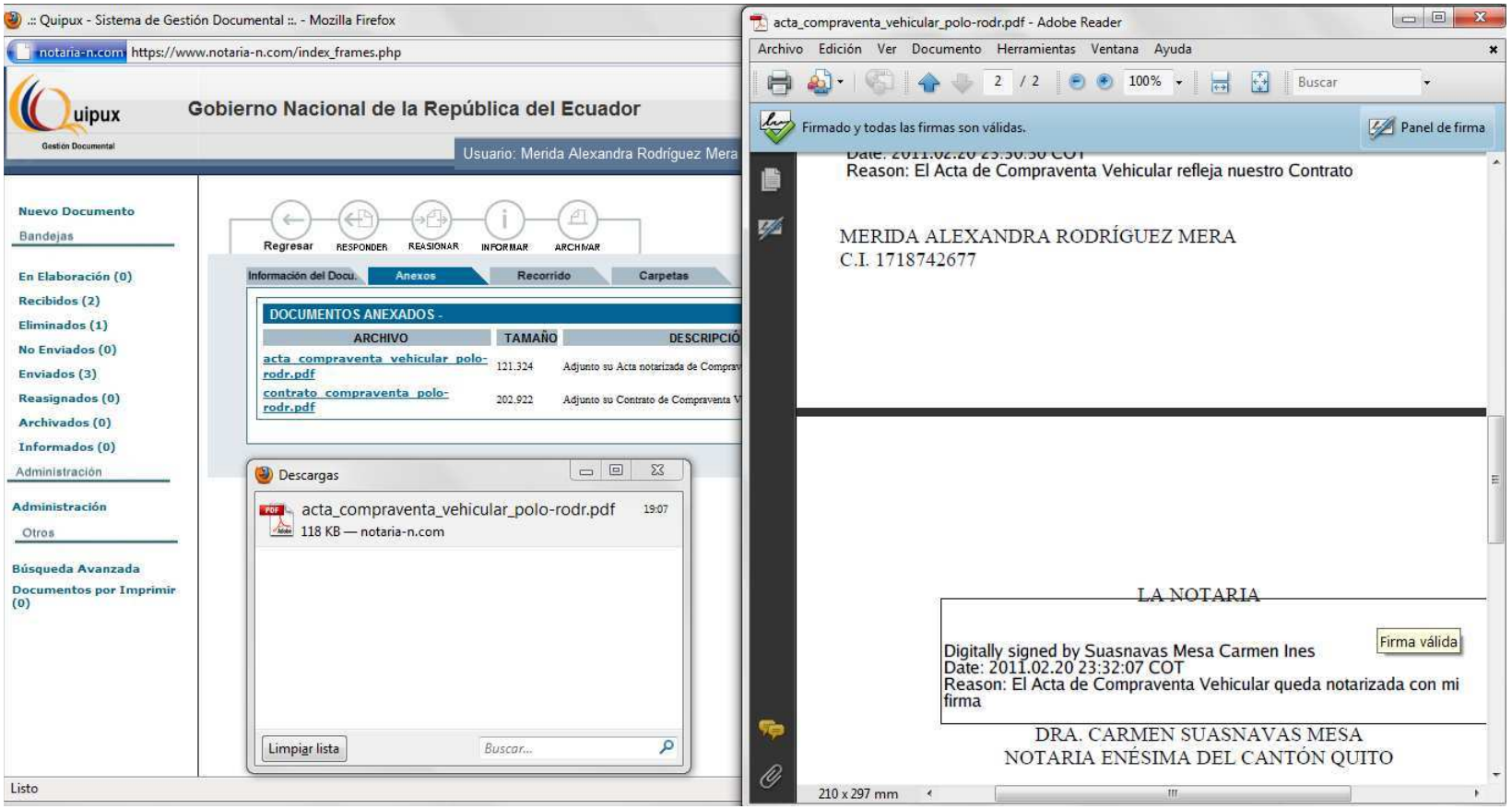

Figura 4.36: Resultado del trámite digital Compraventa Vehicular en la cuenta del Vendedor

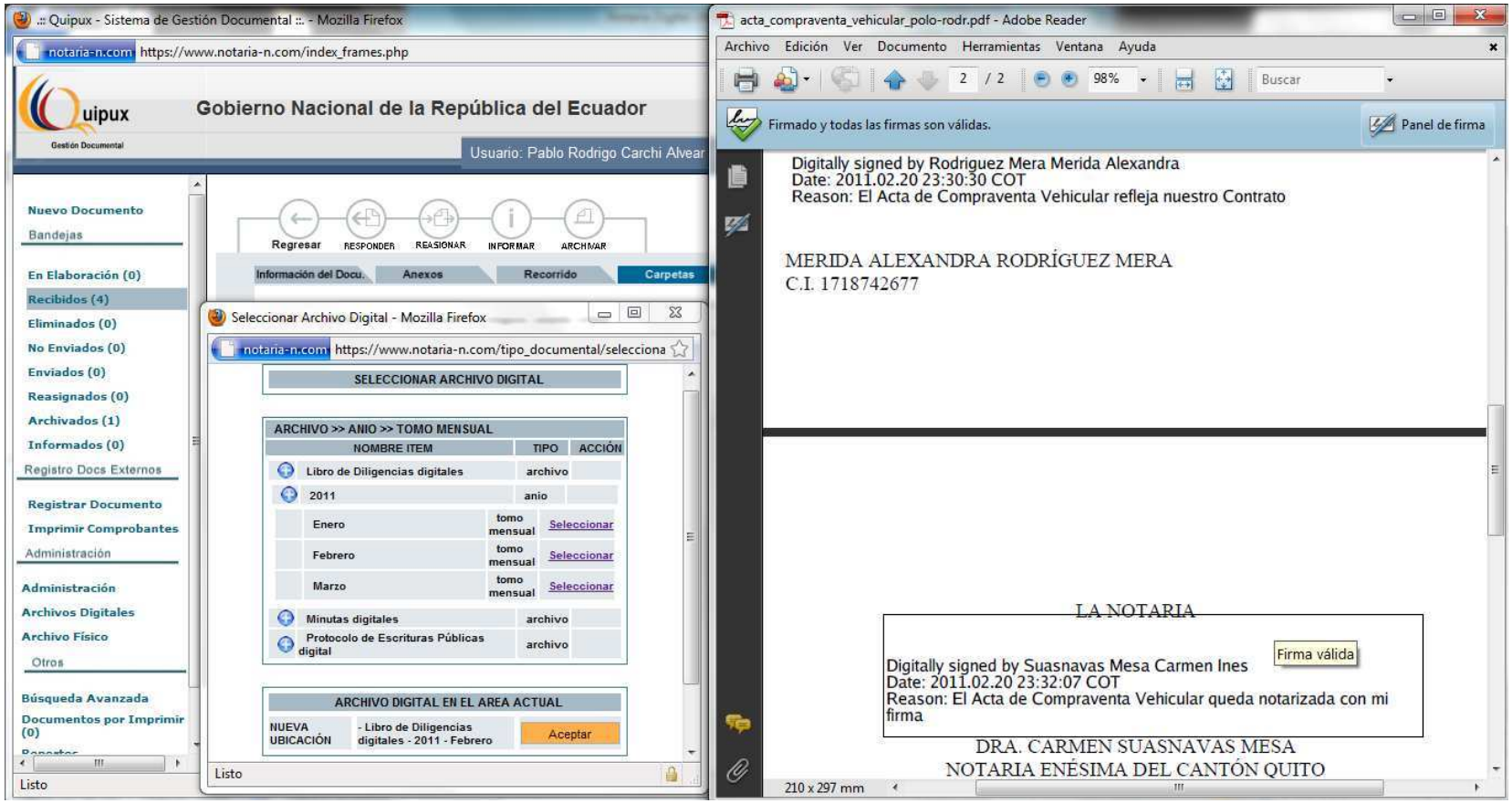

Figura 4.37: Almacenamiento del Acta de Compraventa Vehicular en el Libro de Diligencias digitales

4.5.6 ANÁLISIS DE RESULTADOS DE LAS PRUEBAS

En este subcapítulo se realiza el análisis de resultados obtenido con las pruebas del prototipo de Notaría Digital. El análisis se enmarca en definir si el prototipo ofreció una alternativa a los trámites notariales convencionales para realizarlos de forma digital y distribuida. El análisis se basa en la comparación entre los objetivos planteados en el subcapítulo 1.1.2 y los resultados obtenidos en las pruebas.

- Las pruebas demostraron que el prototipo funcionó en un ambiente Web distribuido seguro. Las pruebas muestran que el prototipo utilizó el protocolo HTTPS para establecer una comunicación segura entre el Sistema de Gestión Documental y los usuarios. Los protocolos de los cinco trámites notariales escogidos se cumplieron en el prototipo de Notaría Digital.

- El prototipo de Notaría Digital aplicó certificados de firma electrónica emitidos por una Autoridad de Certificación de prueba. El firmado electrónico con estos certificados sobre documentos notariales digitales se realizó mediante el programa JSignPdf. Los resultados de las pruebas muestran que el programa Adobe Reader validó las firmas implantadas en los documentos notariales digitales autenticando así a los participantes de los trámites notariales.

- El servicio de marcas de tiempo no se implementó en el prototipo de Notaría Digital. La ausencia del servicio de marcado de tiempo en el prototipo no influyó en el resultado de los protocolos de los trámites notariales digitales del prototipo. Sin embargo las firmas electrónicas utilizan la fecha y hora del equipo en que se realizó el firmado electrónico.

- Las pruebas demostraron que el Sistema de Gestión Documental Quipux almacenó los documentos notariales digitales. Se constató que Quipux organiza la documentación tanto en la cuenta del Cliente como en la Notaría Digital. Los protocolos de los trámites notariales se realizaron mediante Quipux.

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

En este capítulo se describen las conclusiones y recomendaciones derivadas del desarrollo de los capítulos: Análisis de la Situación Actual y de Requerimientos, Diseño de la Notaría Digital e Implementación del Prototipo. Las conclusiones se desarrollan en el subcapítulo 5.1 y las recomendaciones se encuentran en el subcapítulo 5.2.

5.1 CONCLUSIONES

- El proyecto de titulación demostró mediante las pruebas del prototipo de Notaría Digital realizadas en el subcapítulo 4.5 que los trámites notariales convencionales escogidos en la sección 2.1.2 se pueden realizar de forma digital y distribuida sin prescindir de alguno de los participantes en el protocolo notarial descritos en la sección 2.1.1. Se concluye entonces que al seguir la metodología: análisis de requerimientos y diseño mediante casos de uso, se pueden desarrollar otros trámites notariales que no fueron elegidos para este proyecto de titulación.

- Las pruebas del prototipo de Notaría Digital realizados en el subcapítulo 4.5 necesitaron la implementación de una Autoridad de Marcas de Tiempo como la expuesta en la sección 3.2.2. La procedencia de la fecha y hora de la firma electrónica desde el ordenador en que se firmó el documento notarial digital impidió garantizar que se trate de un tiempo digital auténtico como se analizó en la sección 3.1.2.3.1. El prototipo de Notaría Digital funcionó y ofreció una alternativa digital y distribuida a los cinco trámites notariales convencionales analizados en la sección 2.1.2 pero sin marcado de tiempo.

- El proyecto de Notaría Digital diseñó una infraestructura física flexible en el subcapítulo 3.4. La red de datos de la Notaría Digital mostrado en la figura 3.22 permite la interconexión con otras redes de datos para intercambiar información. El diseño de la infraestructura segura con base en la Arquitectura Modular SAFE de Cisco garantiza la escalabilidad de la red de datos de la Notaría Digital.

- Se constató que la automatización total de los trámites notariales escogidos en la sección 2.1.2 es inviable. El principal inconveniente es la Ley Notarial analizada en la sección 1.2.1 que obliga a la unidad de acto. Además la automatización de los trámites notariales conlleva un gran desarrollo para que las funciones de los involucrados en los trámites notariales analizadas en la sección 2.1.1 sean realizadas a través del sistema distribuido.

- El Sistema de Gestión Documental Quipux instalado en la sección 4.1.1 y configurado en el subcapítulo 4.2 del prototipo de Notaría Digital ofreció beneficios para los protocolos de los trámites notariales diseñados en la sección 3.2.3 y almacenamiento de documentación según el diseño de la sección 3.3. Las pruebas del prototipo realizadas con Quipux en el subcapítulo 4.5 mostraron las limitaciones de este Sistema de Gestión Documental referentes a Workflow y autenticación según el diseño de la sección 3.3.1.

- La tercerización de la gestión de identidades en Notarías Digitales hacia la Infraestructura de Llave Pública de la ECIBCE, como se propone en el subcapítulo 3.1, aprovecha el manejo de un directorio de identidades único en el Ecuador. Los usuarios de Notarías Digitales deberán pertenecer previamente al directorio de la ECIBCE. Aprovechar la existencia de la Infraestructura de Llave Pública de la ECIBCE permitió no realizar un estudio para implementar una PKI exclusiva para Notarías Digitales.

- La integración de herramientas tecnológicas permitió implementar el prototipo de Notaría Digital. Usar los certificados de firma electrónica de prueba definidos en el subcapítulo 4.3 y los programas con base en software libre descritos en las

secciones 4.1 y 4.3.3 (Quipux, JSignPdf, Linux CentOS) permitieron implementar el prototipo de Notaría Digital sin demandar gasto alguno.

5.2 RECOMENDACIONES

- La Ley Notarial establece un pago por parte del cliente previo a la realización del trámite notarial. Con este antecedente es obligatorio complementar este proyecto de titulación con el desarrollo de un sistema de facturación electrónica para Notarías Digitales. Los protocolos diseñados en la sección 3.2.3 no contemplan la facturación electrónica porque así se estableció en el alcance de este proyecto de titulación. Sin embargo el pago electrónico debería realizarse después del paso 2 de cada caso de uso.

- Es recomendable establecer políticas de seguridad informática para Notarías Digitales previa a su implementación. Esta recomendación es necesaria para una adecuada gestión de tecnología en Notarías Digitales. La norma ISO/IEC 27001 ofrece un enfoque para establecer la gestión de estas políticas de seguridad. El establecimiento de políticas de seguridad informática no formaron parte del alcance de este proyecto de titulación.

- La Notaría Digital sin una Autoridad de Marcas de Tiempo no puede funcionar. Es necesario la implementación de una Autoridad de Marcas de Tiempo en el Ecuador para complementar el proyecto de Notarías Digitales. El beneficio del marcado de tiempo de una TSA acreditada en el Ecuador genera confianza al establecer una hora digital única para los trámites notariales digitales propuestos. Esta recomendación surge del análisis realizado en la sección 3.1.2.3.1.

- Se recomienda establecer Acuerdos de Nivel de Servicios con los Proveedores de Servicio de Internet que aseguren una continuidad 24x7x365 de la Notaría Digital a fin de garantizar la disponibilidad del servicio notarial en el horario de atención que establece la Notaría. Los SLA no se establecieron en este proyecto

de titulación porque la Arquitectura SAFE que siguió el diseño de la red de datos de la Notaría Digital en el subcapítulo 3.4 no abarca el módulo del ISP.

- Es indispensable contar con un plan de capacitación a los usuarios para mostrar los beneficios de las herramientas tecnológicas que permiten realizar los trámites notariales de manera digital y distribuida. Con la capacitación se pretende que los usuarios se adapten al uso de nuevas tecnologías y no se opongan a los cambios.

- Se recomienda aplicar en el servidor Web del Sistema de Gestión Documental diseñado en el subcapítulo 3.3, certificados digitales emitidos por una Autoridad de Certificación reconocida a nivel mundial. Con esto se garantiza al usuario la autenticidad del servidor Web de la Notaría Digital y la confidencialidad de la sesión SSL para el trámite notarial digital.

- Se recomienda realizar un análisis más exhaustivo para escoger las herramientas tecnológicas más apropiadas para implementar una Notaría Digital. Las limitaciones de Workflow y autenticación que tuvo el prototipo de Notaría Digital pueden ser superadas mediante la aplicación de otras herramientas que ofrezcan mejores características y permitan obtener un mejor funcionamiento. Aún con estas limitaciones, para este proyecto de titulación se escogieron las herramientas definidas en el capítulo 4 por su naturaleza de prototipo.

- Es importante respaldar la información del Sistema de Gestión Documental diseñado en el subcapítulo 3.3, a fin de preservar el archivo notarial digital. Esta recomendación surge por lo crítico que es para la Notaría perder documentación del archivo según el análisis de la sección 2.2.2. Adicionalmente se recomienda analizar requerimientos de dimensionamiento de servidores para la Notaría Digital. Mediante estas recomendaciones se garantiza la disponibilidad que requiere la Notaría de acuerdo al análisis del subcapítulo 2.2.

REFERENCIAS BIBLIOGRÁFICAS

Libro

Stallings, W., 1999, “Cryptography and Network Security”, Segunda Edición, Prentice Hall, New Jersey, EE.UU.

Comer, D. 2001, “Internetworking with TCP/IP Vol III: Client-Server Programming and Applications*”,* Prentice Hall.

White Papers

Adobe Systems Incorporated, 2004, “A primer on electronic document security”, San José, California, EE.UU.

Corvery, S. y Trudel B., 2000, “Cisco SAFE: A Security Blueprint for Enterprise Networks”, Cisco Systems, San José, California, EE.UU.

Sitios Web

Registro Oficial del Ecuador: http://www.derechoecuador.com/

Entidad de Certificación de Información del Banco Central del Ecuador: http://www.eci.bce.ec/

LDAP (Lightweight Directory Access Protocol): http://www.ldapman.org

Time-Stamping: http://www.e-timestamping.com/itf_eng.pdf

Sistema de Gestión Documental Quipux: http://www.quipux.org/

Creación de Certificados Digitales: http://bulma.net/body.phtml?nIdNoticia=2280