ESCUELA POLITÉCNICA DEL EJÉRCITO

DPTO. DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA

DESARROLLO DEL WEB SITE CORPORATIVO PARA LA GESTIÓN Y VALIDACIÓN DE LA DOCUMENTACIÓN LEGAL DE UNATEC; MEDIANTE EL USO DE LA FIRMA ELECTRÓNICA

Previa a la obtención del Título de:
Ingeniero en Sistemas e Informática

POR: JAVIER FERNANDO VILLALBA FIALLOS

SANGOLQUÍ, Julio del 2013

AUTORIZACIÓN

Yo, JAVIER FERNANDO VILLALBA FIALLOS, autorizo a la Escuela Politécnica del Ejército a que publique en el repositorio digital de la biblioteca Alejandro Segovia el presente proyecto de tesis, así como también los materiales y documentos relacionados a la misma.

Sangolquí, 31 de Julio del 2013

_____

JAVIER VILLALBA

DECLARACIÓN

Yo, Javier Fernando Villalba Fiallos, declaro que el trabajo aquí descrito es de mi autoría; que no ha sido previamente presentado para ningún grado o calificación profesional; y, que he consultado las referencias bibliográficas que se incluyen en este documento.

La Escuela Politécnica del Ejército (ESPE), puede hacer uso de los derechos correspondientes a este trabajo, según lo establecido por la Ley de Propiedad Intelectual, por su Reglamento y por la normatividad institucional vigente.

_____

JAVIER VILLALBA

CERTIFICACIÓN

Ing. José Sancho

Ing. Omar Baldeón

Que el trabajo titulado **"DESARROLLO DEL WEB SITE CORPORATIVO PARA LA GESTIÓN Y VALIDACIÓN DE LA DOCUMENTACIÓN LEGAL DE UNATEC; MEDIANTE EL USO DE LA FIRMA ELECTRÓNICA",** realizado por el Sr. Javier Fernando Villalba Fiallos ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas por la ESPE, en el reglamento de estudiantes de la Escuela Politécnica del Ejército.

El mencionado trabajo consta de documento empastado y disco compacto el cual contiene los archivos en formato portátil de Acrobat (PDF). Autorizan a que entregue al Ing. Mauricio Campaña en Calidad de Director de Carrera.

Ing. José Sancho	Ing. Omar Baldeón
DIRECTOR	CODIRECTOR

Dedicatoria

Dedico este proyecto de tesis a mis amados padres

Dolores y Carlos, a mis hermanos Sandra,

Juan Carlos y Andrea que siempre me han

demostrado su apoyo y preocupación, a mi mejor amiga

Valeria, que me ha entregado su

amistad sincera e incondicional, y a

mis mentores y profesores

que han compartido su conocimiento

y sus experiencias con mi persona.

Javier Villalba F.

Agradecimientos

Agradezco a Dios por permitirme disfrutar otro día de vida

y permitirme llegar al final de esta meta.

Agradezco a mis Padres Dolores y Carlos por

entregarme su amor y confianza incondicional,

por su paciencia, su preocupación, por enseñarme que se

puede lograr todo lo que uno se propone

y principalmente por darme la vida.

Agradezco a mis hermanos Sandra, Juan Carlos

y Andrea por haber sido un gran apoyo desde siempre.

Agradezco a Valeria, mi mejor amiga, por su paciencia

y por todos los momentos vividos y por vivir,

apoyándonos en todas las circunstancias.

Agradezco a mis Directores, Ing. Sancho e Ing. Baldeón por

su guía, ayuda y paciencia a lo largo de todo este proyecto.

Javier Villalba F.

ÍNDICE DE CONTENIDO

CAPÍTULO 1

INTRODUCCIÓN

CAPÍTULO 2

MARCO TEÓRICO

CAPÍTULO 4

IMPLEMENTACIÓN Y PRUEBAS

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

ANEXO A

ANEXO B

ANEXO C

ANEXO D

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto tiene por objetivo el desarrollo y la implementación de una solución que permita administrar y a su vez validar la documentación de la Unión Nacional de Taxi Ejecutivo Comercial (UNATEC) utilizando la metodología de desarrollo Web denominada UWE y aplicando el concepto de la Firma electrónica.

La base de la investigación, se centra en el concepto que comprende el uso, obligaciones y responsabilidades de los certificados digitales y con ello el desarrollo de un software que permita procesar documentos PDF y validar los certificados digitales con los que fueron firmados.

Para cumplir con el objetivo es necesario obtener un certificado digital de firma electrónica mediante una autoridad certificadora (AC) en el Ecuador, en este caso y para ejecución de este proyecto con la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE); en la parte técnica, se identificarán las herramientas que permitan procesar la información almacenada en el mencionado certificado.

Con la funcionalidad que nos brindan los certificados digitales que emiten la autoridades de certificación (AC), en base a las leyes, normativas y políticas de uso del mismo nos permitirá garantizar la integridad y el origen de los documentos PDF (formato PKSC#7) firmados electrónicamente con un certificado digital, el mismo que como herramienta criptográfica proporcionará un íntegro y seguro manejo de los documentos de importancia para la organización.

CAPÍTULO 1

INTRODUCCIÓN

1.1. Antecedentes

La Unión Nacional de Taxi Ejecutivo Comercial (UNATEC) es una organización que se orienta al servicio del usuario, brindándole la comodidad, garantía y seguridad que merece. En Unatec se ampara a los socios que pertenecen a las distintas compañías que se encuentran distribuidas a lo largo de la ciudad y que brindan el servicio de Taxi Ejecutivo a los clientes que lo soliciten, por lo que la organización se encuentra defendiendo los derechos de los socios que brindan este servicio de taxi ejecutivo mientras se culmina el proceso de la regularización de Taxis por parte del Distrito Metropolitano de Quito y de la Agencia Nacional de Tránsito, la misma que fue decretada por el Presidente de la República con los respectivos procesos para cada provincia del Ecuador.

Debido a que el crecimiento de la organización no está controlado, es de vital importancia planificar una mejor administración para aumentar la proyección de la organización, facilitar su acceso y control de la información.

Con la funcionalidad que nos brindan los certificados digitales que otorga la entidad competente en el país, como lo es el Banco Central del Ecuador, en base a las leyes, normativas y políticas de uso del mismo nos permitirá aprovechar sus beneficios, ya que como herramienta criptográfica nos brindará la seguridad y validación que la organización necesita para el manejo de su documentación.

1.2. Planteamiento del Problema

1.2.1. Contextualización del Problema

La Unatec (Unión Nacional de Taxi Ejecutivo Comercial) debido a que es una organización nueva y fundada hace apenas 5 años, no cuenta con las herramientas apropiadas para optimizar sus procesos, y debido a que se encuentra en crecimiento, necesita los medios necesarios para que el manejo de la información, la documentación y las consultas se lo deje de realizar de manera manual. Actualmente, toda la documentación la tienen en medios físicos mediante formularios o solamente por medio de documentos Excel o Word.

Con este método que utiliza el personal de la Unión Nacional de Taxi Ejecutivo Comercial se encuentran problemas de tiempo de atención a los socios, dificultad en las consultas, actualización de datos, veracidad e integridad de la información, tiempo de localización del documento, perdida de documentos e incluso se ha detectado casos de falsificación de la documentación de los socios.

1.3. Formulación del problema

En Unatec se ha detectado la falta de un aplicativo con un adecuado motor de base de datos para el almacenamiento y administración de su información.

Causas

- La información se encuentra en varios medios magnéticos (Excel, Word, etc) por lo cual no se garantiza la integridad de la información.
- Dificultad en la administración de la información.
- Elaboración de reportes manuales.
- Dificultad en el acceso a la información.
- Existe confusión por parte del usuario al momento de actualizar individualmente los archivos de su información (Excel, Word).

1.3.1. Definición Espacial

El sistema se lo realizará en la organización sin fines de lucro UNATEC bajo los requerimientos solicitados por la misma.

1.3.2. Delimitación Temporal

El sistema se lo realizará en base a la información y datos de la organización correspondiente al año 2012.

1.4. Objetivos

1.4.1. Objetivo General

Desarrollar el Web Site Corporativo para la gestión y validación de documentos de la organización UNATEC aplicando certificados de firma electrónica.

1.4.2. Objetivos Específicos

- Determinar el procedimiento para obtener el certificado digital de firma electrónica a través de una autoridad certificadora en el Ecuador (Banco Central del Ecuador).
- Aplicar la metodología de desarrollo web UWE[1] en el desarrollo del sistema propuesto.
- Utilizar los certificados digitales de firma electrónica para validar documentos en formato PDF[2].
- Implementar el Web Site Corporativo de UNATEC.

1.5. Justificación

UNATEC necesita garantizar la integridad y el origen de su documentación ya que no todos los documentos pueden ser emitidos por cualquier persona, debido a que se pueden presentar problemas de falsificación en los datos de los socios,

[1] **UWE:** UML Web Engineering (Metodología de desarrollo web)
[2] **PDF:** Formato de documento portátil

para esto se identificarán las deficiencias que existen actualmente en sus procesos y según ello realizar las mejoras necesarias para poder ofrecer la seguridad que merecen el personal y los socios de la organización.

Posteriormente, concluido el proceso de legalización de taxis Ejecutivos por parte del municipio, Unatec abarcará y respaldará a las pequeñas compañías de Taxi Ejecutivo del país convirtiéndose posiblemente a futuro en una federación, para lo cual necesitará las herramientas y la infraestructura de software necesaria para este crecimiento.

Debido a que el control de la documentación se lo realiza de manera manual, se dificulta la búsqueda y la conservación de la misma, por eso salta a relucir la necesidad de digitalizar e ingresar esta información para agilitar los trámites y mantener el control en la documentación de los socios (Licencias, Matrículas, etc), con esto se solventaría el problema de la perdida de documentos, el acceso a la información y la ágil elaboración de consultas y carpetas para los trámites de los socios.

1.6. Alcance

Desarrollar el Web Site Corporativo que permita manejar contenidos informativos y la administración de los datos de los socios con sus respectivos documentos, esto incluye a las compañías que laboran actualmente, y a los vehículos con los que prestan sus servicios de transporte, con el fin de que los dirigentes y el personal que forman parte de la organización tengan las soluciones ideales para optimizar sus procesos.

Las funcionalidades que abarca la propuesta se divide en los siguientes módulos:

Módulo de Usuarios

- Ingresar nuevo usuario
- Actualización de datos de usuario
- Asignar roles de acceso
- Consultar Usuarios

Módulo de Socios

- Ingresar nuevo socio a la organización
- Actualizar datos del Socio.
- Eliminar Socio de la Organización
- Asignar Fotografía a Socio
- Consultar Socios de la Organización
- Asignar Socio a una Compañía
- Asignar Licencia a Socio
- Ver Licencia de Socio
- Asignación /Retiro de Vehículo a Socio
- Ver Vehículo (Datos Básicos del Vehículo)
- Asignación /Retiro de Compañía
- Ver Compañía (Datos Básicos de la Compañía)
- Cargar Socios

Módulo de Compañías

- Ingresar nuevas Compañías a la organización
- Actualizar los datos de las Compañías
- Asignar Representante Legal a Compañía
- Actualizar Datos de Representante de Compañía
    - Eliminar Compañía (No debe tener Socios Asignados para realizar esta operación)
- Control de pago de cuotas mensuales
- Consulta Compañías

Módulo de Vehículos

- Ingreso Nuevos Vehículos
- Eliminar Vehículos
- Actualización de Vehículos
- Control de Caducidad de Matrículas
- Consultar Vehículos

Módulo de Perfiles

- Crear Nuevo perfil de Acceso
- Actualizar perfil de Acceso
- Eliminar Perfil de Acceso
- Actualizar Funciones del Perfil de Acceso

Módulo de Documentos

- Ingresar nuevo Oficio
    - Cargar documentos PDF
    - Verificar Firmas Electrónicas
- Ver Oficios Ingresados
- Descargar Oficios

Módulo de Mantenimiento

- Mantenimiento Módulo Socios
    - Administrar Estados de Socios
    - Administrar Categorías de Socios
    - Administrar Tipos de Licencia
- Mantenimiento Módulo Vehículos
    - Administrar Clases Vehículos
    - Administrar Colores
    - Administrar Combustibles
    - Administrar Marca y Modelo
    - Administrar Letreros
    - Administrar Tipo de Placa
    - Administrar Tipo de Vehículo
- Mantenimiento de Documentos
    - Administrar Tipos de Oficios

Módulo de Firma Electrónica

- Carga de nuevo Certificado de Firma Electrónica
- Activar / Desactivar Firma Electrónica Autorizada
- Consultar Certificados de Firma Electrónica.

Módulo de Consulta

- Consulta Dinámica de Socios
- Consulta Dinámica de Vehículos
- Consulta Dinámica de Compañías
- Consulta de Oficio
- Ver Estadísticas

Para efectos el uso de la firma electrónica se ejecutará los siguientes puntos:

- Obtención de Certificado de Firma Electrónica en token o archivo como persona natural en la Entidad de Certificación de Información del Banco Central del Ecuador (ECIBCE).
- Se utilizarán las herramientas proporcionadas por el Banco Central del Ecuador para firmar documentos PDF.
- El aplicativo web NO firmará digitalmente ningún tipo de documento.
- El aplicativo web verificará certificados de firma electrónica en documentos PDF.

1.7. Visión

Se describe el propósito, alcance y los objetivos que el Web Site Corporativo deberá cumplir para poder proporcionar una descripción general de lo que se va a desarrollar y las funciones que tendrá el aplicativo web.

1.7.1. Propósito

El Web Site presentará una vista general informativa de la organización y permitirá la navegabilidad de los usuarios a través del mismo, en el cual se mostrará la misión, visión y propósito de la empresa, lo que hace, y los servicios que ofrece y con ello poder fortalecer la organización que está proyectándose al crecimiento.

Adicionalmente deberá permitir la administración de compañías y a su vez a los socios que conforman las mismas, esto incluye su documentación e información personal.

El aplicativo contará con consultas a definir por los usuarios funcionales y permitirá que la documentación emitida por UNATEC pueda ser cargada en un servidor web para su posterior consulta y validación.

1.8. Herramientas

GlassFish.- Servidor de aplicaciones web accesible y compatible para las empresas de hoy en día, puede ser implementado en cualquier sistema operativo.

XolidoSign.- Herramienta gratuita que permite firmar electrónicamente documentos PDF, adicional, posee el servicio de TimeStamp o sello cronológico por el cual se certifica la hora en la que el documento fue firmado.[3]

SafeNet.- Herramienta de licencia gratuita facilitada por el Banco Central del Ecuador que contiene el driver del dispositivo "Token" otorgado por la entidad, adicional cuenta con una interfaz que permite extraer la información del contenido del certificado de firma electrónica almacenada en el dispositivo.[4]

[3] **Fuente:** http://www.xolido.com/lang/
[4] **Fuente:** http://www.eci.bce.ec/web/guest/paso-2

BouncyCastle.- Librerías Open Source para lectura y procesamiento de certificados digitales en formato x.509[5].[6]

MagicDraw UML: Herramienta Case compatible con el estándar UML 2.3 y orientado para el modelado de datos, es compatible con varios IDEs de desarrollo.[7]

Prime Faces.- Es una tecnología y framework para aplicaciones Java basada en web que simplifica el desarrollo de interfaces de usuario en aplicaciones Java EE. Usa JavaServer Faces (JSF) como la tecnología que permite hacer el despliegue de las páginas.[8]

PowerDesigner.- Herramienta que facilita el proceso de modelar datos usando UML[9], el mapeo de metadatos, características distintas en reportes, soportes para diferentes motores de bases de datos, etc. Y permite el diseño de la estructura del software de manera rápida y confiable.

Firma Electrónica (Token[10], Archivo).- Constituye el equivalente a la firma manuscrita de puño y letra de un individuo, garantiza la identidad del mismo (autenticación del origen y el no repudio) y la integridad de los datos, la fecha y hora de firma del documento y evita la manipulación de los documentos firmados.

IntiSign.- Herramienta de licencia gratuita facilitada por el Banco Central del Ecuador para la firma de Documentos PDF utilizando dispositivo Token o archivo de Firma Electrónica otorgado por la entidad.[11]

---

[5] **X.509:** Estándar criptográfico para infraestructuras de claves públicas
[6] **Fuente:** http://www.bouncycastle.org/documentation.html
[7] **Fuente**: http://es.wikipedia.org/wiki/MagicDraw_UML
[8] **Fuente:** http://es.wikipedia.org/wiki/MagicDraw_UML
[9] **UML:** Lenguaje de modelamiento unificado
[10] **Token:** Dispositivo Electrónico que contiene la información digital de una persona.
[11] **Fuente:** http://www.eci.bce.ec/web/guest/intisign-firma-archivos-v2

Itext.- Librería que permite procesar Documentos en formato PDF, y extraer los certificados de firma electrónica en caso de que aplique el caso, permite exportación de datos en formato Excel y PDF.[12]

MySql.- Base de datos Open Source con un motor confiable tanto para los usuarios como para los administradores, con capacidad de procesamiento multihilo.

Netbeans.- IDE de desarrollo que facilita la implementación del lenguaje de programación Java, proporcionando apertura para el desarrollo de aplicaciones en distintas plataformas.

[12]**Fuente:** http://itextpdf.com/book/chapter.php?id=1

CAPÍTULO 2

MARCO TEÓRICO

UNIÓN NACIONAL DE TAXI EJECUTIVO COMERCIAL

Figura 2.1: Organigrama de la Organización

Presidencia

Se encarga de la gestión y control de las compañías de Taxi Ejecutivo a nivel de Quito.

Adicional se encarga de las negociaciones sobre las normas a cumplir para la adecuada circulación de los Taxis en la ciudad de Quito.

La representación y la voz de la Unatec es un factor importante para el apoyo de estas compañías que buscan obtener, mediante el cumplimiento de las normas y resoluciones establecidas por las entidades gubernamentales su permiso de operación definitivo como Taxi Ejecutivo.

Gerencia

Se encarga de la gestión económica de la organización, en esencia, administra los bienes económicos de la Unatec, sus ingresos, egresos, inversiones y necesidades que requiere Unatec para su funcionamiento y operatividad.

Coordinadores

La coordinación para los eventos, reuniones y toma de decisiones es muy importante, por eso, existe este grupo excepcional por el cual los socios se encuentran informados de las últimas noticias, resoluciones y trámites que se deben realizar para poder mantenerse al margen de la ley, y así poder seguir prestando sus servicios de taxi ejecutivo a los clientes que lo requieran.

Asesoría Jurídica

Se encarga como su nombre lo indica, en asesorar a los socios que pertenecen a las distintas compañías con los temas de carácter legal, es decir, informar y guiar adecuadamente a los socios para que puedan cumplir con la documentación, trámites y procedimientos que ayudará a los socios a la obtención del permiso de operación que posteriormente se convertirá en un permiso de operación definitivo.

Definición de la Metodología

2.2.1. Metodología UWE

La Ingeniería Web basada en UML (UML-Based Web Enginering, UWE) brinda una importancia significativa al desarrollo web a lo largo del proyecto, la funcionalidad y la navegabilidad son un aspecto necesario para poder entregar un producto funcional, útil e intuitivo para el cliente.[13]

[13]**Fuente:** http://www.pst.ifi.lmu.de/personen/kochn/presentations/UWE_27042010_sevilla.pdf

La Metodología UWE es una propuesta basada en UML y en el proceso unificado para modelar aplicaciones web. Esta propuesta está formada por una notación para especificar el dominio y un modelo para llevar a cabo el desarrollo del proceso de modelado. Los sistemas adaptativos y la sistematización son dos aspectos sobre los que se enfoca UWE.

Mediante las siguientes actividades se obtiene una colección de modelos y diagramas que describen una aplicación Web de manera integral:

- Análisis de Requerimientos
- Modelo Lógico-Conceptual
- Modelo de Navegación
- Modelo de Presentación
- Visualización de Escenarios Web

Con estas actividades se representa de manera satisfactoria los elementos arquitectónicamente significativos de una aplicación Web.

Mediante UWE se logrará conseguir la adaptabilidad, mitigar errores, colaboración y aprendizaje, con estas características se puede realizar la estructuración de los requisitos, necesidades y funcionalidades que necesita la organización, se diseña una solución para posteriormente desarrollarla.

La aplicación de la metodología, comienza en la captura de los requisitos funcionales. Los mismos que se los especificará detallada y adecuadamente para llegar a un acuerdo con la parte técnica y funcional, se evaluarán los requisitos y las funcionalidades para conseguir el "ok" de quienes usarán el sistema, y de quienes forman parte del desarrollo, de ser necesario se analizarán nuevos cambios tanto en los requisitos como en las funcionalidades y corregir los errores que se puedan presentar. En lo que se denomina "entregables", se podrá analizar el estatus del proyecto y posteriormente tomar decisiones, todo esto de forma constante, hasta obtener el producto final con el máximo nivel de satisfacción del cliente.[14]

[14]**Fuente:** http://www.pst.ifi.lmu.de/personen/kochn/presentations/UWE_27042010_sevilla.pdf

Etapas del desarrollo

2.3.1. Análisis de Requerimientos

El resultado final de la captura de requisitos en UWE es un modelo de casos de uso acompañado de documentación que describe los usuarios del sistema, reglas de adaptación e interfaz. UWE clasifica los requisitos en dos grandes grupos: funcionales y no funcionales. Los requisitos funcionales tratados por UWE son relacionados con:

- El contenido
- La estructura
- La presentación
- La adaptación
- Los usuarios

Un caso de uso en UML es una unidad coherente de la funcionalidad proporcionada por la aplicación que obra recíprocamente con uno o más actores de la aplicación.[15]

Adicionalmente, describe una parte del comportamiento de la aplicación sin revelar la estructura interna, por lo cual se emplea el modelo de casos de uso, como se muestra en la figura 2.3.1.[16]

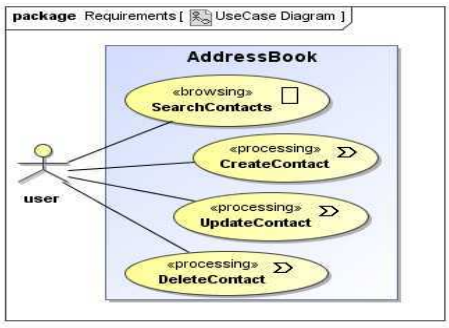


Figura 2.3.1: Ejemplo Diagrama de Casos de Uso[17]

[15]**Fuente:** http://www.slideshare.net/ktyk/uml-casos-de-uso
[16]**Fuente:**http://uwe.pst.ifi.lmu.de/teachingTutorialSpanish.html
[17]**Fuente:** http://uwe.pst.ifi.lmu.de/teachingTutorialRequirements.html

2.3.2. Modelo Conceptual

Un diagrama de clases en UML se utiliza para representar gráficamente un modelo conceptual como visión estática que demuestre una colección de los elementos estáticos del dominio. UWE apunta a construir un modelo conceptual de una aplicación web, la cual procura no hacer caso en la medida de lo posible de cuestiones relacionadas con la navegación, y de los aspectos de interacción de la aplicación web. Estos aspectos se posponen a los pasos navegacionales y de presentación del diseño.

La construcción de este modelo conceptual se debe llevar a cabo de acuerdo con los casos de uso que se definen en la especificación de requerimientos. El modelo conceptual incluye los objetos implicados en las actividades típicas que los usuarios realizarán en la aplicación web, es decir, los objetos que son relevantes para la realización de una actividad o que son el resultado de una de ellas.

Por lo tanto, utiliza elementos del modelo de la estructura UML como modelo de clases, asociaciones y paquetes. Además, puede hacer uso de los modelos de comportamiento como estado de máquinas y diagramas de secuencia.[18]

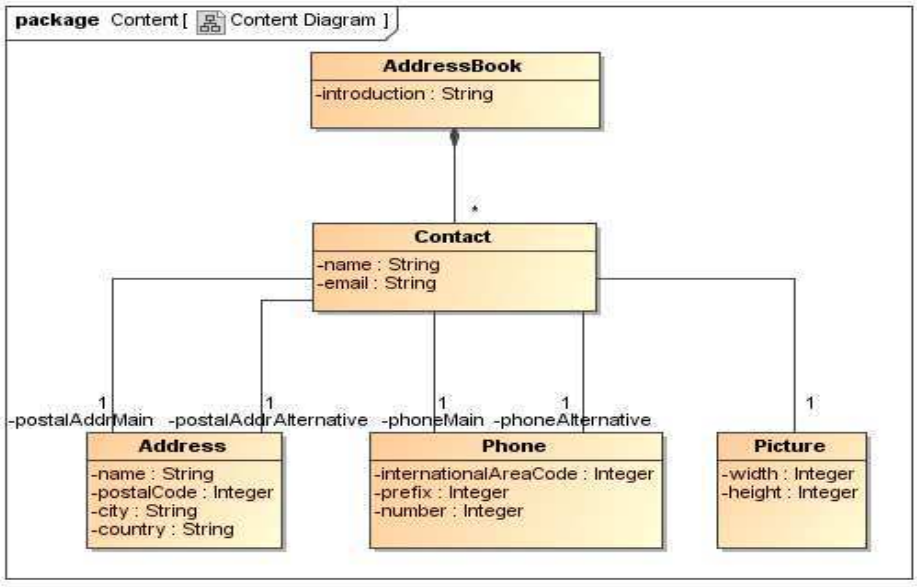


Figura 2.3.2: Modelo Conceptual[19]

[18] **Fuente:** http://uwe.pst.ifi.lmu.de/teachingTutorialSpanish.html

2.3.3. Modelo de Navegación

El modelo de navegación de una aplicación web comprende la especificación de que objetos pueden ser visitados mediante la navegación a través de la aplicación web y las asociaciones entre ellos. Los modelos de la navegación son representados por los diagramas de clases estereotipadas. Este modelo se destaca en el marco de UWE como el más importante, pues con él se pueden representar elementos estáticos, a la vez que se pueden incorporar lineamientos semánticos de referencia para las funcionalidades dinámicas de una aplicación web.[20]

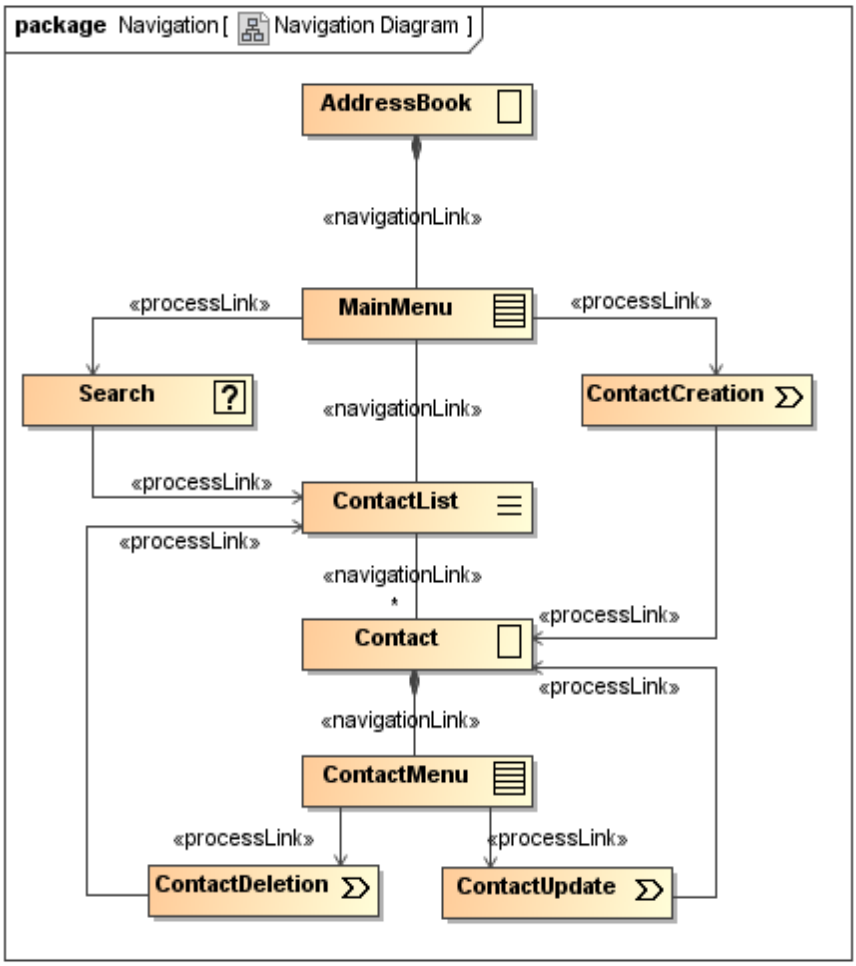


Figura 2.3.3 Ejemplo Modelo de Navegación[21]

[19] **Fuente:** http://uwe.pst.ifi.lmu.de/teachingTutorialContent.html
[20] **Fuente:** http://uwe.pst.ifi.lmu.de/teachingTutorialSpanish.html
[21] **Fuente:** http://uwe.pst.ifi.lmu.de/teachingTutorialNavigation.html

2.3.4. Modelo de Presentación

El modelo de presentación proporciona una vista abstracta sobre la interfaz de usuario (IU) de una aplicación web. Está basado en el modelo de navegación. El modelo de presentación extrae aspectos concretos de la IU, como el uso de colores, fuentes y donde los elementos de la IU son colocados en la página web y su lugar; describe la estructura básica de la interfaz de usuario (por ejemplo, texto, imágenes, anclas, las formas) son usadas para presentar los nodos de navegación. Además, los elementos IU no representan los componentes concretos de ninguna tecnología, sino describen lo que requiere la funcionalidad en ese punto en particular de la interfaz de usuario. Esto simplemente podría significar que un texto o imagen tienen que mostrarse o por ejemplo permitir al usuario provocar una transición en el modelo de navegación. En este último caso, es evidente que un ancla sería usada en el modelo de presentación de UWE, pero UWE no define la forma en que el ancla debería ser utilizada en la aplicación web final.

Las clases de presentación pueden contener otros elementos.En el caso de los elementos IU, como el texto o imagen, la propiedad de presentación está asociada con una propiedad de navegación que contiene el contenido para ser representada.

La inclusión de clases de presentación dentro de otras del mismo tipo o páginas conduce a un árbol de clases de presentación que se muestran juntas. Esto significa que los enlaces entre sus nodos correspondientes a la navegación son "automáticamente seguidos". Por otra parte, si dos clases de presentación no pertenecen al mismo árbol de inclusión, entonces el enlace entre sus nodos de navegación tiene que ser activado por una acción del usuario.[22]

[22]**Fuente:** http://www.pst.ifi.lmu.de/personen/kochn/presentations/UWE_27042010_sevilla.pdf

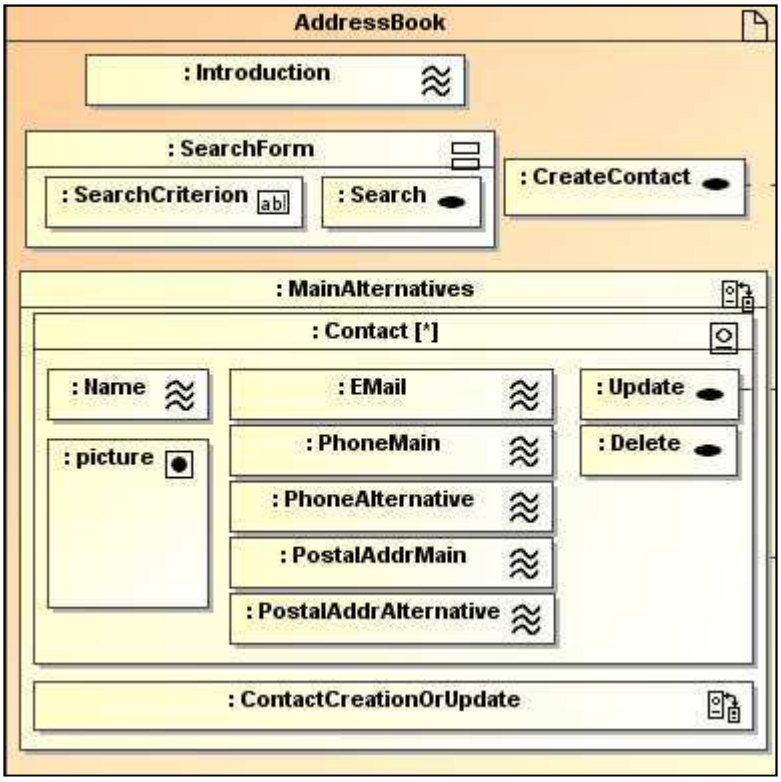


Figura 2.3.4: Ejemplo de Modelo de Presentación[23]

2.3.5. Modelo de Procesos.

El modelo de procesos proporciona un modelo de elementos para integrar procesos de negocios en un modelo de aplicación web de UWE. Se separa en tres procesos:

Integración de los procesos de negocio en el modelo de navegación.

Esto es permitido por dos metaclasesProcessClass y ProcessLink que amplían el nodo y el enlace respectivamente y esto permite definir como un proceso puede ser alcanzado por la navegación y como la navegación seguirá después del proceso.[24]

[23] http://uwe.pst.ifi.lmu.de/teachingTutorialNavigation.html
[24] http://uwe.pst.ifi.lmu.de/teachingTutorialProcess.html

Definición de interfaz de usuario.

Los procesos requieren una interfaz de usuario para los datos de entrada y presentación.

Esta interfaz de usuario puede ser definida como en el modelo de presentación UWE para cada clase de proceso justo como la IU de las clases de navegación. Sin embargo, la entrada del usuario puede requerir varios puntos en el flujo del proceso. Esto se resuelve creando una clase de proceso por cada paso y asociación con la clase de procesos principal que es integrada en el modelo de navegación. Por cada una de estas clases de procesos, una clase de presentación es creada definiendo la interfaz de usuario. Los elementos IU son conectados con las propiedades del proceso de la clase de proceso correspondiente.[25]

Definición del comportamiento.

El comportamiento de un proceso está definido por una actividad UML que es propiedad de la principal clase de proceso. Las siguientes restricciones y semánticas especiales son aplicadas:

Una acción especial del usuario (UserAction) es usado para marcar un punto en el control del flujo cuando se pide al usuario ingresar un dato. La acción del usuario es asociada con una clase de proceso para identificar que datos son editados y qué clase de presentación es mostrada. El control de flujo de la actividad continúa después que el usuario ha presentado los datos solicitados.

En muchos casos, un proceso necesita algunas entradas de su nodo predecesor en la gráfica de navegación. Esta situación puede ser modelada por un nodo de parámetro de actividad que es usado en vez de un nodo de acción inicial. El nodo de parámetro debe tener el mismo tipo que la clase de contenido de la clase de navegación que precede a la clase de proceso.[26]

---

[25] **Fuente:** http://www.pst.ifi.lmu.de/personen/kochn/presentations/UWE_27042010_sevilla.pdf
[26] **Fuente:** http://www.slideshare.net/techmi/curso-uml-24-diagramas-de-comportamiento

Las acciones en la actividad de proceso que no son acciones del usuario pueden llamarse operaciones del objeto de parámetro de entrada y cada instancia que es creada durante la actividad de proceso. Como el acceso a otros contextos es expresado mientras aumenta la modelación.

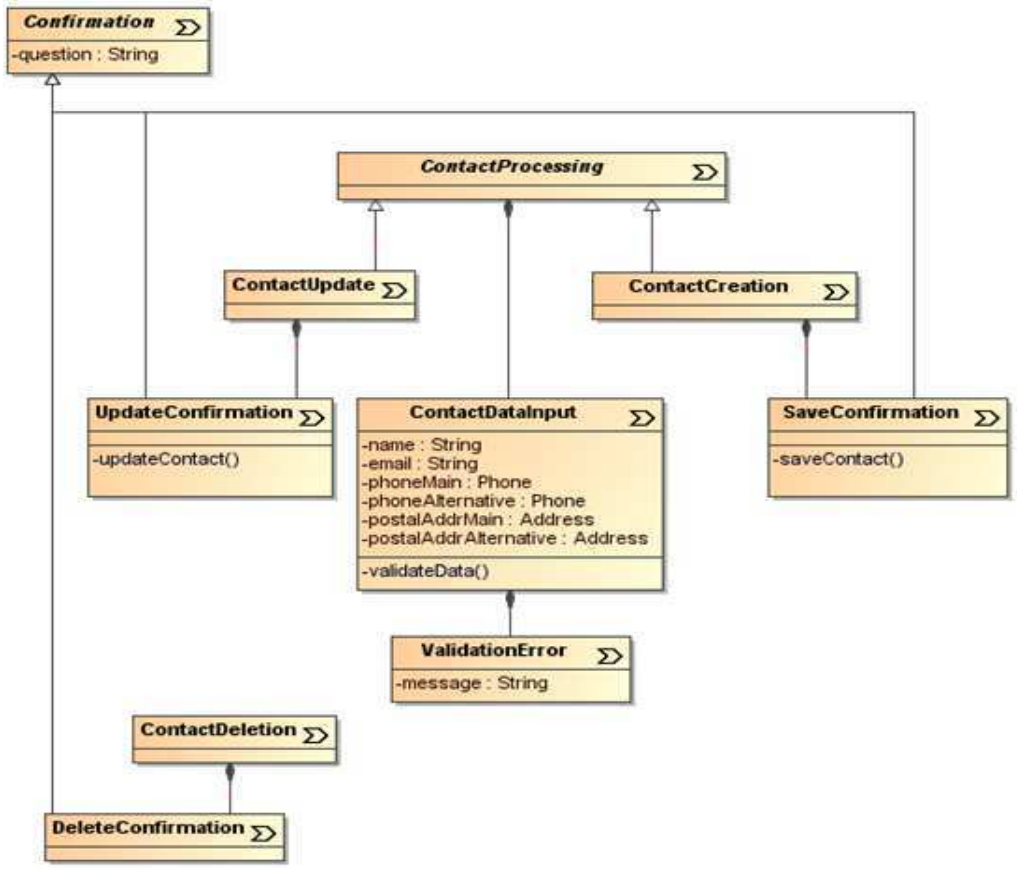


Figura 2.3.5: Modelo de Procesos[27]

Como se muestra en la figura 2.3.5 el proceso puede crear o seleccionar una clase de contenido instanciada que debería ser pasada a un nodo sucesivo (clase de navegación o clase de proceso). Esto puede ser modelado por un nodo de parámetro de actividad que es usado en vez de un nodo de actividad final.[28]

[27] Fuente: http://uwe.pst.ifi.lmu.de/teachingTutorialProcessSpanish.html
[28] Fuente: http://uwe.pst.ifi.lmu.de/teachingTutorialProcessSpanish.html

2.3.6. Iteración Temporal

Un diagrama de secuencia de UML demuestra la interacción de elementos dispuesta en orden temporal. Presenta los objetos que participan en la interacción y la secuencia de los mensajes enviados entre ellos. UWE propone el uso de los diagramas de secuencia para representar los aspectos dinámicos de la navegación, es decir, las secuencias describen la realización de los casos de uso. De esta manera, los diagramas de secuencia proveen una representación funcional centrada en el tiempo del modelo de navegación.[29]

2.3.7. Visualización de Escenarios Web

Un diagrama de estados de UML denota una secuencia de los estados que un objeto puede adquirir durante su actividad, junto con acciones fiables, ejecutando eventos y las condiciones asociadas para indicar estas transiciones. UWE da otro sentido a los diagrama de estados de UML puro ya que los utiliza para visualizar escenarios de navegación. Estos diagramas permiten detallar la parte dinámica del modelo de navegación, especificando los eventos que se ejecutan presentando uno o varios resultados, definen condiciones y explícitamente incluyen las acciones que son realizadas. [30]

2.4. Marco Legal

2.4.1. Firma Electrónica[31]

Es la equivalencia digital de la firma manuscrita, tiene la misma validez legal y se encuentra amparada por la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

---

[29]**Fuente:** http://www.pst.ifi.lmu.de/Lehre/fruhere-semester/sose-2007/web-engineering/materialien/WE_04_Modelling-v2.pdf
[30]**Fuente:** http://mlozanoavalos.blogspot.com/2009/06/articulo-ingenieria-web.html
[31]**Fuente:** http://www.informatica.gob.ec/sistemas/transversales/firma-electronica

Desde el punto de vista técnico, la firma es un conjunto de datos digitales que se añaden a un archivo digital y que se obtienen del cifrado del mismo mediante programas computacionales.

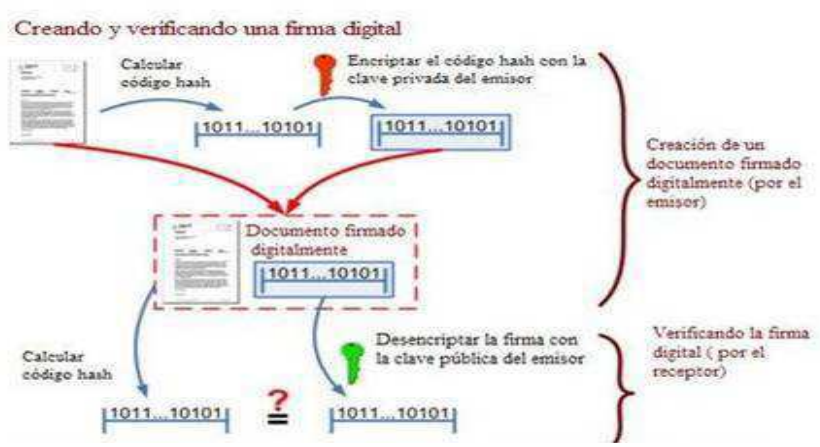


Figura 2.4.1: Verificación de una Firma Digital[32]

La firma digital permite garantizar la no alteración de documentos y operaciones en aplicaciones computacionales garantizando los siguientes aspectos:

- **Identidad**, reconoce unívocamente a un emisor como autor del mensaje.
- **Integridad**, el documento no puede ser alterado de forma alguna durante la transmisión.
- **No repudio**, el emisor no puede negar en ningún caso que un documento no fue firmado.
- **Confidencialidad**, solo las partes puedan leer el documento (si fuera el caso).

2.4.2. Formatos básicos para Firma[33]

Los formatos principales para firma electrónica son los siguientes:

- PKCS#7.
- Firma XML
- PDF (PKCS#7)

[32] **Fuente:** http://www.informatica.gob.ec/images/images_sti/firma.jpg
[33] **Fuente:** http://www.informatica.gob.ec/sistemas/transversales/firma-electronica

A. PKCS#7[34]

Es uno de los formatos tradicionales más extendidos, se trata de un formato de encapsulamiento codificado en ASN-1, aunque también puede ser codificado en Base64, habitualmente, una firma en PKCS#7 puede representarse en su modalidad Attached (habitual) o Dettached, en función de que incluya o no el propio documento.

La firma propiamente dicha es un compendio de datos formales referidos al tipo de firma así como de atributos firmados y no firmados bajo una estructura dada.

- **Contenido del Formato**

  Versión: Versión del formato.

  Tipo de Algoritmo hash: SHA2, SHA1, SHA0, MD5.

- **Información del contenido**

  Tipo de contenido: (normalmente Data).

- **Contenido: Documento a firmar**

  Certificados: Certificado del firmante y de toda la cadena.

  CRLs: Lista de Certificados Revocados donde verificar el estado de revocación.

  Información del firmante: Versión.

- **Identificación**

  Issuer del Certificado: Emisor del certificado.

  No de serie: No de serie del certificado.

  Tipo de algoritmo hash: SHA1.

  Tipo de contenido: Valor fijo = DATA.

[34] **PKCS:** Estándar Criptográfico para Claves Públicas

- **Certificado del firmante**

  Fecha y hora de firma: momento de firma en formato (YYMMDDHHMMSSZ).

  Hash del mensaje: Obtenida del documento al aplicarle el algoritmo hash.

- **Política de firma**

Atributos no firmados: (Num. de firmas, cargo del emisor, localización, etc.).

Tipo de algoritmo de firma: Generalmente RSA (también DSA).

B. XML DSIG[35]

Es el formato de mayor expansión usado frecuentemente en aplicaciones en lineaEl formato XML DSig funcionalmente y estructuralmente, es bastante similar al PKCS, pero la codificación original de firmas y certificados se realiza en B64 en toda firma XML, según el estándar XML DSig, existirían 3 modos de firma:

Enveloped: En el que la firma se añade al final del documento XML como un elemento más. Se firma todo lo inmediatamente anterior al documento.

Envoloping: En el que el documento se incluye dentro de la firma en la que se referencia lo firmado como objeto insertado en la firma. Ya que se referencian los objetos, este modelo permitiría distinguir lo que se firma, pudiendo firmar el objeto entero o partes de él (asignando un id diferenciador).

Detached:En el que la firma y el documento se separan en dos archivos, la URL donde se encuentra el documento puede aparecer en la propia firma.

C. Formato PDF[36]

Una de las principales ventajas del formato PDF es la capacidad de gestionar firmas. En realidad se trata de una implementación de PKCS#7, la creación y validación de firmas electrónicas se ha ido mejorando a lo largo de las

[35] **Fuente:** http://www.informatica.gob.ec/sistemas/transversales/firma-electronica
[36] **Fuente:** http://www.informatica.gob.ec/sistemas/transversales/firma-electronica

versiones hasta convertirse en la herramienta genérica que realiza un mejor tratamiento con PDF,y hace posible realizar las denominadas firmas longevas, de gran importancia.

Principales características:

- Firma y validación con Acrobat Reader
- Personalización de la razón de la firma y de una imagen personalizada
- Incorporación de CRL / OCSP, sello de tiempo y cadena de certificados
- Firmas visibles /invisibles
- Limitación de certificados a emplear
- Creación de políticas de firma
- Integración con el repositorio de confianza de Windows
- Firma sólo de campos seleccionados (sólo válido con versión 8)

2.5. Uso de la Firma Electrónica

Con la firma electrónica pueden realizarse diferentes tipos de transacciones a través de la Internet sin necesidad de desplazarse, ni hacer filas de forma que los trámites públicos se agilitan aumentando la transparencia, lo que se traduce en ahorros significativos de tiempo y dinero. Las aplicaciones de la firma digital son diversas. Se cita algunas de ejemplo a continuación:

- Compras públicas
- Trámites ciudadanos (Gobierno electrónico)
- Gestión documental
- Operaciones bancarias
- Dinero (pago) electrónico
- Balances electrónicos
- Trámites judiciales y notariales
- Comercio electrónico
- Facturación electrónica

2.6. Función Hash

Es una función hash H aquella que es computable mediante un algoritmo que tiene como entrada un conjunto de elementos, por ejemplo cadenas, y las mapea en un rango de salida finito, normalmente cadenas de longitud fija. Es decir, la función actúa como una proyección del conjunto **a** sobre el conjunto **b**.

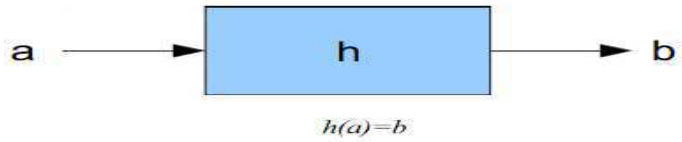


Figura 2.8.1 Función de un Algoritmo Hash

Observar que **b** puede ser un conjunto definido de enteros. En este caso se puede considerar que la longitud es fija si el conjunto es un rango de números enteros, tomando en cuenta que la longitud fija es la del número con mayor número de cifras. Todos los números se pueden convertir al número especificado de cifras simplemente anteponiendo ceros.

Normalmente el conjunto **b** tiene un número elevado de elementos y **a** es un conjunto de cadenas con un número más o menos pequeño de símbolos. Por esto se dice que estas funciones resumen datos del conjunto dominio.

La idea básica de un valor hash es que sirva como una representación compacta de la cadena de entrada. Por esta razón se dice que estas funciones **resumen** los datos del conjunto dominio.

```
SHA224("")
0x d14a028c2a3a2bc9476102bb288234c415a2b01f828ea62ac5b3e42f
SHA256("")
0x e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855
SHA384("")
0x 38b060a751ac96384cd9327eb1b1e36a21fdb71114be07434c0cc7bf63f6e1da274edebfe76f65fbd51ad2f14898b95b
SHA512("")
0x cf83e1357eefb8bdf1542850d66d8007d620e4050b5715dc83f4a921d36ce9ce47d0d13c5d85f2b0ff8318d2877eec2f63b931bd47417a81a538327af927da3e
SHA512/224("")
0x 6ed0dd02806fa89e25de060c19d3ac86cabb87d6a0ddd05c333b84f4
SHA512/256("")
0x c672b8d1ef56ed28ab87c3622c5114069bdd3ad7b8f9737498d0c01ecef0967a
```

Figura 2.8.2 Ejemplo de Mapeo de una cadena Vacía[37]

[37]**Fuente:**https://en.wikipedia.org/wiki/SHA-2

Existen varios tipos de algoritmos hash, entre ellos se encuentran algoritmos bajo la denominación de SHA, estos fueron creados por la Agencia de Seguridad Nacional de los Estados Unidos (NSA), existen varias versiones de estos algoritmos, empezando por Sha0, Sha1 y Sha2, los mismos que difieren en los bits de encriptación y el número de bytes de salida para su representación, por ejemplo utilizando una cadena los bytes de salida varía dependiendo del número de bits que emplee cada algoritmo.

Figura 2.8.3 Firma Digital de un Documento[38]

Para firmar un documento:

- El documento original pasa por un proceso para calcular un hash(una especie de resumen del documento; si el documento cambia aunque sea por un byte, el hash resulta completamente diferente).
- Se cifra el hash con la llave privada del firmante (a esto se le llama firma del documento).
- Se adjuntan al documento la firma y la llave pública del firmante (así todos pueden verificarla).

[38]**Fuente:** https://www.soportefirmadigital.com/sfd/fd.aspx

Para el caso de ficheros, se realiza el mapeo de todo su conjunto de datos y para efecto de la firma digital, se utiliza la clave privada para cifrar el código hash resulto proveniente del conjunto de datos, a este proceso se lo conoce como firmado digital, bajo este concepto se valida la integridad del conjunto de datos, ya que al ser modificado de alguna manera el código hash resultante será distinto del original.

Figura 2.8.4 Verificación de Firma Digital[39]

Para verificar la firma:

- Del documento firmado se extrae el documento original, y se aplica la función de hash para obtener el código hash resultante.
- También del documento firmado se obtiene la firma como tal y el certificado del firmante (que contiene su llave pública únicamente).
- Se descifra la firma del documento con la llave pública del firmante, obteniendo otro hash.
- Se compara el hash del paso 1 con el del paso 3. Si son idénticos, la firma es válida.

[39]**Fuente:** https://www.soportefirmadigital.com/sfd/fd.aspx

Para la verificación de un documento firmado digitalmente se descifra el código hash resultante del documento mediante el uso de la clave pública del certificado y se compara el hash resultante descifrado versus el código hash original del documento, si coinciden entonces la firma es válida y los conceptos de integridad y no repudio se aplican al documento, es decir, se aplican las normas jurídicas tipificadas en la ley.

2.7. Prestación de Servicios con la ECIBCE[40]

En el contrato de prestación de servicios se tiene cláusulas que aplican a los diferentes tipos de certificado, entre los individuos que pueden realizar solicitud de certificado digital de firma electrónica están los siguientes:

2.7.1. Persona Natural

Persona Natural es una persona humana que ejerce derechos y cumple obligaciones a título personal.

Lo que implica que la persona asume la responsabilidad y garantiza con todo el patrimonio que posea (los bienes que estén a su nombre), las deudas u obligaciones que pueda contraer la empresa.[41]

2.7.2. Persona Jurídica

Persona Jurídica es una empresa que ejerce derechos y cumple obligaciones a nombre de ésta.

Al constituir una empresa como Persona Jurídica, es la empresa (y no el dueño) quien asume todas las obligaciones de ésta.

Lo que implica que las deudas u obligaciones que pueda contraer la empresa, están garantizadas y se limitan solo a los bienes que pueda tener la empresa a su nombre (tanto capital como patrimonio).[42]

---

[40] **ECIBCE:** Entidad de Certificación de Información del Banco Central del Ecuador
[41] **Fuente:**http://www.slideshare.net/cabeto51748/persona-natural-y-juridica

2.7.3. Funcionario Público

Un funcionario público es aquel trabajador que desempeña funciones en un organismo, ya sea el legislativo, el ejecutivo o el judicial

Habitualmente estos organismos son el Gobierno, la Asamblea, el Parlamento, los tribunales, la Administración pública y, en general, todos aquellos organismos que no pertenezcan al sector privado.

Un funcionario del gobierno o un funcionario público es un servidor que participa en la administración pública o de gobierno, ya sea a través de elección, nombramiento o selección. [43]

2.7.4. Solicitud de Revocatoria

Este es el tipo de revocatoria que permite al usuario titular del certificado, subir una solicitud de revocatoria por los siguientes motivos:

- Traslado de Funciones
- Cambio de nivel de firma
- Cesación de funciones
- Uso no permitido del certificado
- Pérdida del dispositivo criptográfico o medio de almacenamiento
- Terminación de la representación o extinción de la persona jurídica representada
- Inexactitudes graves en los datos aportados por el suscriptor para la obtención del certificado
- Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas
- Cambio de datos en el certificado[44]

---

[42]**Fuente:**http://www.slideshare.net/cabeto51748/persona-natural-y-juridica
[43]**Fuente:** http://es.scribd.com/doc/36062542/Ley-Organica-del-Servicio-Publico-aprobada-en-la-Asamblea-Nacional
[44]**Fuente:** http://www.eci.bce.ec/c/document_library/get_file?uuid=b18038a0-9007-446a-b741-2de1e8c925c7&groupId=10155 (Normas Generales)

2.7.5. Recuperación de Certificado:

De igual manera la ECIBCE para recuperar el certificado de firma electrónica debe ser bajo las siguientes circunstancias:

- Olvido de clave.
- Inutilización de datos del soporte del certificado (problemas con el medio donde se encuentra almacenado el certificado).

Este tipo de revocatoria es la única que permite recuperar el certificado por el tiempo restante de vigencia del certificado.[45]

2.7.6. Solicitud de Revocatoria por Representante Legal[46]

Esta solicitud permite solicitar una revocatoria cuando el usuario final por algún motivo no puede realizar la solicitud de revocatoria por sí mismo. (Ej.: cese de funciones)

- Traslado de Funciones.
- Cambio de nivel de firma.
- Cesación de funciones.
- Uso no permitido del certificado.
- Pérdida del dispositivo criptográfico o medio de almacenamiento.
- Fallecimiento del suscriptor, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Terminación de la representación o extinción de la persona jurídica representada.
- Inexactitudes graves en los datos aportados por el suscriptor para la obtención del certificado.
- Que se detecte que las claves privadas del Suscriptor o de la AC han sido comprometidas.

---

[45]**Fuente:** http://www.eci.bce.ec/c/document_library/get_file?uuid=911072aa-6647-4a0b-b03e-447a13d00bab&groupId=10155 (Declaración de Practicas de Certificación)

[46]**Fuente:** http://www.eci.bce.ec/c/document_library/get_file?uuid=2ddaa2ce-b415-48e8-85d1-95151641dca9&groupId=10155 (Políticas de Certificado)

Esta revocatoria no permite recuperar certificados, por lo que se deberá realizar nuevamente una solicitud de certificado de firma electrónica y obtener un nuevo certificado.

- Por Olvido de clave.
- Por Inutilización de datos del soporte del certificado.

2.7.7. Definiciones Legales[47]

El ECIBCE informa en el contrato de prestación de servicios las definiciones técnicas y legales básicas para que el suscriptor tenga el conocimiento de lo que está utilizando, y de sus obligaciones ante la ECIBCE, de manera recíproca, entre las definiciones se enumeran las siguientes:

Clave privada: Es la clave confidencial que mantiene en privado el usuario. Usada generalmente para descifrar los mensajes codificados y también para generar la firma electrónica.

Clave pública: Es la clave del certificado digital que se utiliza para la verificación de la firma electrónica y el cifrado de datos.

Claves RSA: Es el sistema criptográfico con clave pública RSA llamado así por sus creadores Ron Rivest, Adi Shamir y Len Adleman, es un algoritmo asimétrico que utiliza una clave pública, la cual se distribuye (en forma autenticada preferentemente), y otra privada, la cual es guardada en secreto por su propietario.

Contrato de Prestación de Servicios de Certificación: Contrato que tiene por objeto regular los derechos y obligaciones derivados de la prestación por la ECIBCE, al suscriptor, de los servicios de certificación, y, en su caso, la revocación y renovación, del mencionado servicio de certificación.

Declaración de Prácticas de Certificación: Documento que reúne las reglas que la ECIBCE utiliza para gestión, administración, homologación, generación, uso y conservación de cada uno de los certificados de firma electrónica así como de los servicios relacionados que ofrece.

---

[47]**Fuente:** http://www.eci.bce.ec/c/document_library/get_file?uuid=2ddaa2ce-b415-48e8-85d1-95151641dca9&groupId=10155 (Políticas de Certificado)

Dispositivo criptográfico portable seguro-Token: Elemento físico donde se almacena en forma segura el certificado de firma electrónica y que será emitido por la ECIBCE.

Suscriptor: El suscriptor será la persona natural, jurídica, funcionario o servidor público a favor de la cual se ha emitido un certificado. Los suscriptores deberán ajustarse a lo señalado en la DPC, en la PC del certificado que han obtenido y, en su caso, en contrato de Prestación de Servicios suscrito con la ECIBCE Los suscriptores deberán ajustarse a los procedimientos establecidos para la petición de cada tipo de certificado, y cumplir los requisitos que se establezcan en esta DPC

Lista de Certificados Revocados (CRL): Es una lista de certificados que han sido revocados, que no son válidos y en los que no debe confiar ningún usuario del sistema.

OCSP: Online Certificate Status Protocol (OCSP) es un método para determinar el estado de revocación de un certificado digital X.509 en línea.

Persona física: (o persona natural) concepto jurídico. Es todo ser humano susceptible de adquirir derechos y contraer obligaciones.

Persona Jurídica: Son entidades a las que el Derecho atribuye y reconoce una personalidad jurídica propia y, en consecuencia, capacidad para actuar como sujetos de derecho, esto es, capacidad para adquirir y poseer bienes de todas clases, para contraer obligaciones y ejercitar acciones judiciales.

PKI: En criptografía, una infraestructura de clave pública (Public Key Infrastructure) es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas

Obligaciones del Suscriptor

- Cumplir en todo momento con las normas y regulaciones emitidas la ECIBCE.
- Comunicar a la ECIBCE cualquier modificación o variación de los datos que se aportaron para obtener el Certificado de Firma Electrónica.
- Verificar, a través de la Lista de Certificados Revocados, el estado de los Certificados de firma electrónica y la validez de las firmas electrónicas emitidas por la ECIBCE.
- Proteger y conservar el Dispositivo Portable Seguro-Token.
- Solicitar a la ECIBCE de forma personal y escrita, en caso de olvido, una nueva clave de protección del Certificado de Firma Electrónica.
- Responder por el uso del Certificado de Firma Electrónica y de las consecuencias que se deriven de su utilización.
- Las demás contempladas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y, su Reglamento.[48]

Obligaciones de la ECIBCE

- Garantizar la prestación permanente, inmediata, confidencial, oportuna y segura del servicio de certificación de información.
- Mantener sistemas de respaldo de la información relativa a los certificados.
- Proceder de forma inmediata a la suspensión o revocatoria de certificados electrónicos previo mandato del Superintendente de Telecomunicaciones, en los casos que se especifiquen en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.
- Mantener una publicación del estado de los certificados electrónicos emitidos.
- Las demás contempladas en la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos y, su Reglamento.

[48]**Fuente:**http://www.eci.bce.ec/c/document_library/get_file?uuid=b5bc29b1-d4e1-4fec-bc6e-edfd10d3d95f&groupId=10155 (Declaración de políticas de certificado, 2011) .

Terminación

Serán causales de terminación del contrato de prestación de servicios de Certificación de Información las siguientes:

- La terminación del plazo de vigencia del certificado de firma electrónica.
- La declaración unilateral de alguna de las partes contratantes con al menos 15 días de antelación, la cual deberá ser comunicada por escrito a la dirección informada por cada una de las partes en la Cláusula Vigésimo Primera de este instrumento legal.
- Fallecimiento, incapacidad, cesación o destitución del cargo del Suscriptor.
- Por causa judicialmente declarada.
- Por revocación del Certificado de firma electrónica.

Por seguridad El Suscriptor debe tener en cuenta estas recomendaciones:

- El Certificado de firma electrónica es personal e intransferible.
- No debe permitir el uso del certificado a ningún tercero.
- Debe memorizar la Clave.
- No debe permitir que otras personas conozcan la Clave.
- Si olvida o pierde el control de su Clave, se debe solicitar inmediatamente a la ECIBCE la revocación del certificado.
- Importante: No olvidar la Clave Privada, la ECIBCE no almacena ni asigna la Clave, por tanto su olvido implica la revocación del certificado de firma electrónica asociado y la emisión de un nuevo certificado de firma electrónica estará a cargo de El Suscriptor. [49]

Vigencia

El Certificado de Firma Electrónica tendrá una vigencia de 2 años, contados a partir de la fecha de emisión del mismo, y podrá ser renovado por igual período, previa solicitud de su titular con al menos treinta días de anticipación a su vencimiento y el respectivo pago. En ningún caso y bajo ninguna circunstancia, se

[49] **Fuente:** http://www.eci.bce.ec/documents/10155/34572/modeloContratoPersonaNatural.pdf

podrá renovar un certificado más de dos veces consecutivas, es decir, una emisión y dos renovaciones. Transcurrido ese período se tendrá necesariamente que solicitar la emisión de un nuevo certificado.

En el caso de pérdida del Dispositivo Portable Seguro-Token, la vigencia del nuevo Certificado de Firma Electrónica, correrá a partir de la fecha de emisión del mismo.[50]

2.7.8. Accesibilidad de la información

En la ley de comercio electrónico se definen varios aspectos sobre negociaciones, uso regulado, responsabilidades, y requisitos que deben ser cumplidos para el adecuado uso de estas herramientas, tanto para la prestación de servicios como el consumo de ellos.

En la ley se considera que el mensaje es íntegro si es que se mantiene completo y su contenido no ha sido alterado, salvo algún cambio de forma que sea propio del proceso de comunicación.

"**Art. 2** Accesibilidad de la información: Se considerará que un mensaje de datos, sus anexos y remitidos, son accesibles para consulta posterior cuando se puede recuperar su contenido en forma íntegra en cualquier momento empleando los mecanismos y procedimientos previstos para el efecto, los cuales deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo" (Ley de Comercio Exterior, 2002)

"**Art. 3** Información escrita.- Se entiende que la información contenida en un mensaje de datos es accesible para su posterior consulta cuando:

a) Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendible por las partes involucradas en el intercambio de información y sus respectivos sistemas informáticos de procesamiento de la información, pudiéndose recuperar su contenido y el de los remitidos o anexos correspondientes en cualquier momento empleando los mecanismos previstos y reconocidos para el efecto.

[50]**Fuente:** http://www.eci.bce.ec/documents/10155/34572/modeloContratoPersonaNatural.pdf

b) Se puede recuperar o se puede acceder a la información empleando los mecanismos previstos al momento de recibirlo y almacenarlo, y que deberán detallarse y proporcionarse independientemente del mensaje de datos a fin de garantizar el posterior acceso al mismo. Las publicaciones que las leyes exijan por escrito, sin perjuicio de lo establecido en dichas leyes, podrán adicionalmente efectuarse en medios electrónicos en forma de mensajes de datos.
Cumplidos los requisitos de accesibilidad, el mensaje de datos tiene iguales efectos jurídicos que los documentos que constan por escrito. "
(Ley de Comercio Exterior, 2002)

2.7.9. Procedencia e identidad

"**Art. 7** Procedencia e identidad de un mensaje de datos. La verificación de la concordancia entre el emisor del mensaje de datos y su firma electrónica se realizará comprobando la vigencia y los datos del certificado de firma electrónica que la respalda. En otros tipos de firmas o sistemas de identificación y autenticación, esta verificación se realizará mediante la verificación de los registros acordados o requeridos." (Ley de Comercio Exterior, 2002)

"**Art. 11** Duración del certificado de firma electrónica. La duración del certificado de firma electrónica se establecerá contractualmente entre el titular de la firma electrónica y la entidad certificadora de información o quien haga sus veces. En caso de que las partes no acuerden nada al respecto, el certificado de firma electrónica se emitirá con una validez de dos años a partir de su expedición. Al tratarse de certificados de firma electrónica emitidos con relación al ejercicio de cargos públicos o privados, la duración del certificado de firma electrónica podrá ser superior a los dos años pero no podrá exceder el tiempo de duración de dicho cargo público o privado a menos que exista una de las prórrogas de funciones establecidas en la leyes." (Ley de Comercio Exterior, 2002)

La AC debe garantizar que lista de certificados revocados (CRL) se encuentre operativa, y así evitar el uso de certificados que se encuentren revocados. Caso contrario deberán informar a los suscriptores que no es posible

verificar la CRL, y que existe la posibilidad de que se pueda utilizar un certificado digital que ya haya sido revocado.

"**Art. 12** Listas de revocación. Las entidades de certificación de información proporcionarán mecanismos automáticos de acceso a listas de certificados revocados o suspendidos de acuerdo al artículo 26 de la Ley 67. Cuando la verificación de la validez de los certificados de firma electrónica no sea posible de realizar en tiempo real, la entidad de certificación de información comunicará de este hecho tanto al emisor como al receptor del mensaje de datos." (Ley de Comercio Exterior, 2002)

Por acuerdo de las partes y cumpliendo con todas las obligaciones previstas en esta ley, se podrán desmaterializar los documentos que por ley deban ser instrumentados físicamente, es decir, los documentos desmaterializados deberán contener las firmas electrónicas correspondientes debidamente certificadas ante una de las entidades autorizadas según lo dispuesto en el artículo 29 de la ley.

"Art. 29.- Entidades de certificación de información.- Son las empresas unipersonales o personas jurídicas que emiten certificados de firma electrónica y pueden prestar otros servicios relacionados con la firma electrónica, autorizadas por el Consejo Nacional de Telecomunicaciones, según lo dispuesto en esta ley y el reglamento que deberá expedir el Presidente de la República." (Ley de Comercio Exterior, 2002)

A continuación se muestran los artículos de la ley de comercio electrónico que definen a la firma electrónica y al certificado digital, su validez legal, y las responsabilidades que tiene el titular desde el momento que ejerce su derecho de usar su certificado digital:

"Art. 13.- Firma electrónica.- Son los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos. " (Ley de Comercio Exterior, 2002)

Como se define en el artículo 13 se garantiza el origen del mensaje de datos y el no repudio del mismo, lo que conlleva a que el individuo no puede desconocer la información que dicho mensaje adjunto posee.

"Art.14.- Efectos de la firma electrónica.- La firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos, y será admitida como prueba en juicio. " (Ley de Comercio Exterior, 2002)

La Firma electrónica se ha convertido en una significativa herramienta, ya que al tener igual validez que una firma manuscrita, puede facilitar procesos empresariales bilaterales entre personas naturales o personas jurídicas, por ejemplo si la persona jurídica de la empresa EMC se encuentra fuera del país y tenía pendiente la firma de un contrato por prestación de servicios con la empresa CBA, entonces las personas jurídicas de cada empresa podrán concluir el negocio firmando electrónicamente el medio magnético en el que constan las cláusulas del contrato.A este medio magnético firmado por ambas personas jurídicas recae la validez legal y jurídica, es decir, aplica el no repudio, se garantiza la identidad de las personas que celebran el presente contrato y en caso de incumplir con las cláusulas mencionadas, el medio magnético será admitido como prueba en un juicio por incumplimiento de sus obligaciones.

"Art. 15.- Requisitos de la firma electrónica.- Para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes:

- Ser individual y estar vinculada exclusivamente a su titular.
- Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos.
- Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.

- Que al momento de creación de la firma electrónica, los datos con los que se creare se hallen bajo control exclusivo del signatario.
- Que la firma sea controlada por la persona a quien pertenece."
  (Ley de Comercio Exterior, 2002)

Para cumplimento de estos requisitos que menciona el Articulo 15, las AC se encargan de verificar y constatar que los datos entregados por el suscriptor son reales, es decir verifican la identidad del individuo previa la emisión del certificado digital, es por eso que la emisión de certificados digitales constituye la responsabilidad primaria de una AC, ya que es ella, quien certificará que la persona a la que se le emitió el certificado es quien asegura ser.

"Art. 17.- Obligaciones del titular de la firma electrónica.- El titular de la firma electrónica deberá:

- Cumplir con las obligaciones derivadas del uso de la firma electrónica.
- Actuar con la debida diligencia y tomar las medidas de seguridad necesarias, para mantener la firma electrónica bajo su estricto control y evitar toda utilización no autorizada.
- Notificar por cualquier medio a las personas vinculadas, cuando exista el riesgo de que su firma sea controlada por terceros no autorizados y utilizada indebidamente.
- Verificar la exactitud de sus declaraciones.
- Responder por las obligaciones derivadas del uso no autorizado de su firma, cuando no hubiere obrado con la debida diligencia para impedir su utilización, salvo que el destinatario conociere de la inseguridad de la firma electrónica o no hubiere actuado con la debida diligencia.
- Notificar a la entidad de certificación de información los riesgos sobre su firma y solicitar oportunamente la cancelación de los certificados
- Las demás señaladas en la ley y sus reglamentos."
  (Ley de Comercio Exterior, 2002)

Tal y como menciona el artículo 15 de la ley, la firma electrónica es única de su titular e intransferible, en el caso de que su titular bajo consentimiento entregase o permitiera el uso de su certificado digital a un tercero, de aplicar el caso, deberá asumir las responsabilidades del mal uso dado del mismo, ya que como una de las características principales del certificado es el no repudio, por lo que cualquier acción no autorizada automáticamente pertenecerá a su titular, ya que al momento de solicitar el certificado se compromete a asumir con sus obligaciones y responsabilidades estipuladas en el contrato de prestación de servicios y en las políticas de uso del certificado digital.

CAPÍTULO 3

DESARROLLO DEL SISTEMA

Previo al desarrollo del aplicativo, es necesario realizar la especificación de requerimientos del mismo, para definir funcionalmente lo que el sistema debe realizar, entendiendo las funciones y limitaciones que el mismo debe tener.

3.1. Análisis de Requerimientos

3.1.1. Especificación de Requisitos (IEEE-830)[51]

I. Introducción

La presente especificación de requisitos se ha realizado con el propósito de definir los requerimientos funcionales necesarios para el desarrollo del proyecto de Grado Titulado "Desarrollo del Web Site Corporativo para la gestión y validación de la documentación legal de Unatec; mediante el uso de la Firma Electrónica".

II. Propósito

1. Con el fin de establecer los requerimientos y funcionalidades que el aplicativo debe realizar se ha redactado este documento en el cual se recopilará la información necesaria para cumplir con el objetivo planteado y suplir las necesidades del cliente.
2. Por medio de la colaboración de la parte funcional y técnica, este documento servirá para establecer las especificaciones funcionales y así mantener un adecuado canal de comunicación entre las partes involucradas.

[51] **Fuente:** http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.pdf

3. Además tiene como finalidad optimizar la gestión de documentación de los socios que pertenecen a la Organización (UNATEC) y validarla mediante el uso de la firma electrónica, la misma que la poseerá el representante de la organización.
4. Dentro de la propuesta de desarrollo se encuentra contemplado el soporte y la capacitación al usuario para mantener claro los siguientes puntos: alcance, funcionalidades y procedimientos del sistema propuesto.

III. Alcance

El sistema se desarrollara en Netbeans y podrá ser ejecutado en plataformas Windows, Linux, y MacOS

El Web Site Corporativo será levantado en base a Joomla v1.5, en donde se podrá cargar los datos de carácter informativos de la empresa, que permitirá conocer la misión, visión y objetivos de la Organización, y se dejará a disposición la administración del Web Site Corporativo al personal de Unatec.

El sistema contará con los módulos de Usuarios, Socios, Vehículos, Compañías, Perfiles, Mantenimiento, Documentos, Firma Electrónica y Consultas, desde el cual se podrán ingresar todos los datos requeridos por Unatec.

Módulo de Usuarios: Permitirá administrar usuarios y asignar roles de acceso al sistema, ya sean como Socios o Usuarios Administrativos.

Módulo de Socios: Permitirá administrar los Socios de la Organización, asignarlos a una Compañía, a sus respectivos vehículos e ingresar los datos de sus licencias correspondientes.

Módulo de Perfiles de Seguridad: Permitirá administrar perfiles de acceso y definir las tareas a las que el perfil tendrá luz verde para operar.

Módulo de Compañías: Permitirá la administración de las compañías afiliadas a Unatec con sus respectivos representantes, y en cada compañía existirá un número autorizado de Socio.

Módulo de Vehículos: Permitirá la administración de los vehículos de los Socios que forman parte de Unatec, el vehículo como tal toma la función de la herramienta de trabajo para los socios, y se debe tener el control de los datos del vehículo que un Socio utiliza para ejercer sus labores de Taxi Ejecutivo.

Módulo de Mantenimiento: Permitirá administrar diferentes ítems que corresponden a la parte administrativa de Socios, Vehículos y Tipos de Documento

Módulo de Documentos: Permitirá cargar documentos en formato PDF a los que el sistema automáticamente le hará un proceso de reconocimiento para extraer firmas digitales contenidas en el documento.

Módulo de Firma Electrónica: Permitirá cargar certificados de firma electrónica en el sistema para efectos de validación de ficheros PDF y para identificar usuarios autorizados.

Módulo de Consultas: Permitirá generar consultas de forma dinámica, es decir, el usuario seleccionará los campos que necesite y podrá filtrar la información por cualquiera de ellos, adicional se pueden consultar las estadísticas del módulo.

IV. Definiciones, Acrónimos y Abreviaturas

a. Definiciones

- **Administrador** (Persona encargada del manejo total del sistemas)
- **Usuario**(Persona que tendrá acceso al sistema para consulta y actualización de datos)
- **Socio** (Persona que tendrá acceso a la consulta de sus datos personales)
- **Desarrollador** (Personas que se encargan del análisis, diseño, implementación y mantenimiento del sistema)

- **Garantía de Software** (Garantiza que los Productos Software licenciados al cliente, en condiciones normales de uso y servicio, y durante un periodo de noventa días a partir de la fecha de envío del software al cliente. No garantiza la operación ininterrumpida del Software, que esté libre de errores, que sea compatible con otros productos software, que cumpla los requisitos del cliente, ni que su uso sea ininterrumpido)
- **Licencia de Software** (es la autorización o permiso concedido por el titular del derecho de autor, en cualquier forma contractual, al usuario de un programa informático, para utilizar éste en una forma determinada y de conformidad con unas condiciones convenidas)
- **MySQL** (Servidor de Base de Datos)
- **Upgrade** (Nombre que reciben las nuevas versiones de una aplicación o un hardware y son diseñadas para reemplazar una versión previa del mismo producto.)

b. Acrónimos

AC: Autoridad de Certificación.

AR: Autoridad de Registro.

BCE: Banco Central del Ecuador.

C: Country (País). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.509.

CN: Common Name (Nombre Común). Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

CRL: Certificate Revocation List (Lista de Certificados Revocados).

DN: Distinguished Name (Nombre Distintivo). Identificación unívoca de una entrada dentro de la estructura de directorio X.500.

DPC: Declaraciones de Prácticas de Certificación.

ECI: Entidad de Certificación de Información.

ECIBCE: Entidad de Información del Banco Central del Ecuador.

HSM: Hardware Security Module. Módulo de seguridad criptográfico empleado para almacenar claves y realizar operaciones criptográficas de modo seguro.

ISO: International Organizational for Standarization.

O: Organization. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

OCSP: Online Certificate Status Protocol. Este protocolo permite comprobar en línea la vigencia de un certificado electrónico.

OID: Object identifier (Identificador de objeto único).

OU: Organizational Unit. Atributo del Nombre Distintivo (DN) de un objeto dentro de la estructura de directorio X.500.

ERS: Especificación de Requisitos Software.

GUI: Interfaz Gráfica de Usuario, que presentan iconos y zonas activas pulsando con el ratón.

HTML: Hyper Text Mark-up Language. Lenguaje de programación para armar páginas.

HTTP: Protocolo de transferencia de hipertexto (HTTP, Hyper Text Transfer Protocol) es el protocolo usado en cada transacción de la Web (WWW).

IEEE: (The Institute of Electrical and Electronics Engineers / Instituto de Ingenieros Eléctricos y Electrónicos) una institución americana responsable de la creación de una gran cantidad de estándares en electrónica e informática.

IU: Interfaz de usuario.

JDBC: Java Database Connectivity. Conectividad de bases de datos Java. Las interfaces de acceso a datos basadas en ODBC para utilizar con el lenguaje Java.

SQL: Lenguaje de consulta estructurado – Structured Query Language.

TCP/IP: Transfer Control Protocol / Internet Protocol (Protocolo de Control de Transporte / Protocolo de Internet).

UWE: Ingeniería Web basada en UML (UML-Based Web Enginering).

UML: Lenguaje Unificado de Modelamiento (Unified Modeling Language).

XML: eXtensible Markup Language – Lenguaje de Etiquetado Extensible.

V. Visión General del Documento

El presente documento consta de 3 secciones. En la primera sección se ha realizado una introducción al mismo y se proporciona una visión general de la especificación de los recursos del sistema.

En la segunda sección del documento se realiza una descripción general del sistema, con el fin de conocer las principales funciones que éste debe realizar, los datos asociados y factores, restricciones y herramientas que se necesitan para el desarrollo, sin entrar en profundidad en los detalles.

Finalmente, en la tercera sección del documento será donde se definirá detalladamente los requisitos y funcionalidades que debe cumplir el sistema.

VI. Descripción General del Sistema

a. Perspectiva del Producto

El sistema para la gestión y validación de documentos permitirá a la organización mantener un control adecuado de los datos personales de los socios, de sus vehículos y de sus compañías, además de almacenar la documentación correspondiente a cada uno de ellos.

La firma electrónica será la que le proporcionará el valor jurídico legal a la documentación emitida por la organización, para esto es necesario que el representante legal realice el trámite para la obtención del certificado de firma electrónica en el Banco Central del Ecuador.

El sistema permitirá cargar el certificado de firma electrónica emitida por el BCE y posteriormente validarlo con los documentos que hayan sido firmados con este mismo certificado.

Permitirá digitalizar los documentos de los socios para su posterior consulta, lo cual facilitará la búsqueda, el control y ayudara a disminuir considerablemente el uso de papel.

b. Funciones del Producto

Las funciones se las clasificará de acuerdo al módulo y son las siguientes:

Módulo de Usuarios

- Ingresar nuevo usuario
- Actualización de datos de usuario
- Asignar Perfil de Usuario
- Consultar Usuarios

Módulo de Socios

- Ingresar nuevo Socio a la organización.
- Actualizar datos del Socio.
- Eliminar Socio de la Organización.
- Asignar Fotografía a Socio.
- Consultar Socios de la Organización.
- Asignar Socio a una Compañía.
- Asignar Licencia a Socio.
- Ver Licencia de Socio.
- Asignación /Retiro de Vehículo a Socio.
- Ver Vehículo (Datos Básicos del Vehículo).
- Asignación /Retiro de Compañía.
- Ver Compañía (Datos Básicos de la Compañía).
- Cargar Socios.

Módulo de Compañías

- Ingresar nuevas Compañías a la organización.
- Actualizar los datos de las Compañías.
- Asignar Representante Legal a Compañía.
- Actualizar Datos de Representante de Compañía.
- Eliminar Compañía (No debe tener Socios Asignados para. realizar esta operación).
- Control de Pago de cuotas mensuales.
- Consulta Compañías.

Módulo de Vehículos

- Ingreso Nuevos Vehículos.
- Eliminar Vehículos.
- Actualización de Vehículos.
- Control de Caducidad de Matriculas.
- Consultar Vehículos.

Módulo de Perfiles

- Crear Nuevo perfil de Acceso.
- Actualizar perfil de Acceso.
- Eliminar Perfil de Acceso.
- Actualizar Funciones del Perfil de Acceso.

Módulo de Documentos

- Ingresar nuevo Oficio.
  - Cargar documentos PDF.
  - Verificador de Firma Electrónica.
- Ver Oficios Ingresados.
- Descargar Oficios.

Módulo de Mantenimiento

- Mantenimiento Módulo Socios
  - Administrar Estados de Socios
  - Administrar Categorías de Socios
  - Administrar Tipos de Licencia
- Mantenimiento Módulo Vehículos
  - Administrar Clases Vehículos
  - Administrar Colores
  - Administrar Combustibles
  - Administrar Marca y Modelo
  - Administrar Letreros
  - Administrar Tipo de Placa
  - Administrar Tipo de Vehículo
- Mantenimiento de Documentos
  - Administrar Tipos de Oficios

Módulo de Firma Electrónica

- Carga de nuevo Certificado de Firma Electrónica
- Activar / Desactivar Firma Electrónica como Autorizada
- Ver Información de Certificado

Módulo de Consulta

- Consulta Dinámica de Socios
- Consulta Dinámica de Vehículos
- Consulta Dinámica de Compañías
- Consulta de Oficio
- Ver Estadísticas

VII. Características de Usuarios

USUARIO	NIVEL DE EDUCACIÓN	NIVEL DE CONOCIMIENTOS	EXPERIENCIA	CONOCIMIENTOS TÉCNICOS
Administrador	Título de Cuarto Nivel – Universidad	Conocimiento en gestión de Recursos Humanos y económicos, planificación y administración de Negocios, liderazgo.	No poseen mucha experiencia en el tema de manejo de aplicaciones Web, tienen conocimientos medios en computación pero alta experiencia en negocios y gestión de recursos Humanos	Medio
Usuario	Cuarto Nivel – Universidad Tercer Nivel -Secundaria	Conocimiento en gestión de Recursos Humanos, atención al cliente, políticas y procesos internos de la organización	Tiene experiencia en el tema de atención al cliente y conocimientos medios en computación	Medio
Socio	No Aplica	Requiere conocimientos de computación Básica	Experiencia en manejo de aplicaciones básicas de ofimática	Bajo

Tabla 3.1: Características de Usuarios del Sistema

VIII. Restricciones

En caso de que el cliente y el desarrollador establezcan un tiempo para la entrega del proyecto, este deberá cumplirse y se requerirá del tiempo del usuario funcional para realizar las respectivas pruebas de validación del Sistema.

IX. Requerimientos de Hardware

Equipo Servidor

Para asegurar la eficacia del Sistema en el equipo cliente se requiere las siguientes características recomendadas:

- Intel Xeon 2.5Ghz
- 4GB de Memoria RAM
- Espacio disponible en Disco duro de 100GB
- Tipo de monitor: VGA, SVG

Equipo Cliente

Para asegurar la eficacia del Sistema en el equipo cliente se requiere las siguientes características recomendadas:

- Intel Core i3 de 2.4Ghz
- 2GB de Memoria RAM
- Espacio disponible en Disco duro de 1GB
- Tipo de monitor: VGA, SVG
- eToken Pro 72k (Java): Dispositivo USB que contiene el certificado de Firma Electrónica (Si es que Aplica)

X. Requerimientos de Software

Equipo Servidor

- Netbeans 7.2
- Servidor de Aplicaciones Web Glassfish 3.1 o superior
- Primefaces 3.4
- Base de datos MySql v5.1 o superior
- Tipo de monitor: VGA, SVG

Equipo Cliente

- SafeNet (Aplicación y driver del dispositivo eToken)
- Intisign (Aplicación para firmar electrónicamente documentos PDF)
- Google Chrome 27.0 o superior
- Mozilla Firefox 21.0 o superior
- Internet Explorer 9.0 o superior

XI. Funcionamiento Paralelo

Mientras se trabaja en las interfaces web del software, en las ventanas de inserción, modificación, eliminado lógico y otras, estos cambios se almacenarán en el motor de base de datos. De esta manera la operación será paralela, a la que vez que se confirmen los cambio en las interfaces del software se verá reflejado en la Base de datos de Mysql.

XII. Requisitos del lenguaje

Para el desarrollo del Sistema se utilizara el IDE de Oracle Netbeans, ya que ofrece varias herramientas y plugins, los mismos que se pueden importar fácilmente debido a la interfaz intuitiva que posee.

Para el desarrollo se utilizara el Framework PrimeFaces, el mismo que es gratuito y soportado por el IDE de desarrollo, adicional se usaran aplicaciones para elaboración y ediciones de imágenes que el software va a utilizar en su interfaz de usuario.

XIII. Protocolos

El protocolo que se utilizara será el TCP/IP, el cual permitirá una conexión cliente/servidor ágil. Sencilla y estándar. Además que es un protocolo indirectamente conocido por todos los usuarios, esto facilita su desarrollo y mantenimiento.

XIV. Restricciones de uso del sistema

En este punto de definirá lo que el sistema no hará, enumerando los siguientes puntos a tomar en cuenta:

1. El sistema no permitirá ninguna modificación en los documentos digitalizados ya sea que estén o no firmados electrónicamente
2. El sistema no firmará electrónicamente ningún documento, se utilizara la herramienta otorgada por el Banco Central del Ecuador para este proceso
3. El sistema no permitirá cargar otro tipo de extensión de documentos conocidos como docx, odt, etc solo permitirá la carga de documentos en formato PDF y en el caso de fotografías de socios será el formato jpg o jpeg.
4. El sistema no ingresará información contable ni generará facturas de ningún tipo, ni se ingresará valores monetarios de ningún tipo.

XV. Atenciones y Dependencias

El sistema correrá sobre cualquier plataforma, pero las pruebas se realizarán con interfaz web Mozilla Firefox, Además se tendrá dependencia directa con el servidor web GlassFish y a MySQL como motor de base de datos

XVI. Requisitos Futuros

- Mejora de la interfaz Gráfica.
- Añadir más graficas estadísticas.
- Posibilidad de integrar con un módulo de facturación.
- Escalabilidad en el sistema para posicionarse a nivel nacional.

XVII. Requisitos Específicos

a. Interfaces Externos (Requerimientos No Funcionales)

En esta sección se va a describir los requisitos no funcionales para el desarrollo de sistema, a un nivel de detalle para que sirva de soporte para el diseño del sistema; es decir se va a mencionar la entrada, proceso y salida involucrada para cumplir con un requisito en especial.

b. Interfaz de Usuarios

Tomando en cuenta que estas interfaces son las más importantes para la satisfacción de clientes finales, deberán tener la funcionalidad suficiente que permita el desempeño correcto de personas con bajos niveles de conocimiento de informática.

Pudiendo mencionar las siguientes:

- Menús de selección para acceso a las distintas tareas; que estarán disponibles
- Mensajes de error y advertencia.
- Pantallas de ingreso de datos que faciliten la tarea del usuario.
- Mensajes de resultados, mismas que serán fácilmente entendibles e interpretables.
- Interfaces de acceso según el perfil de acceso de los usuarios. Así el cliente tendrá acceso a diferentes actividades como es el caso de ingresar, modificar, eliminar y buscar cualquier elemento dentro de la pantalla a la que pueda ingresar.

➢ Pantalla de Ingreso de clave y usuario

La pantalla de Registro se ingresará su nombre de usuario para poder validarlo en la Base de Datos y así podrá acceder únicamente a las tareas que le son asignadas.

➢ Entradas y Salidas

Los datos se capturarán por pantalla y serán almacenados en las Bases de Datos correspondientes

Entrada:

- ✓ Nombre de Usuario
- ✓ Clave

Salida:

- ✓ Perfil el Usuario para cargar su Información.

Rangos:

Los rangos dependerán de las actividades que el usuario podrá ejercer, por ejemplo, el administrador puede acceder a todas las tareas del sistema.

c. Interfaz de Hardware

En cuestión de hardware, se deberá tomar en cuenta que los equipos donde se va a trabajar cumplan con las especificaciones mínimas de hardware como es:

- Ratón (mouse).
- Teclado estándar.
- Disco duro de 500GB.
- Conexión de Internet de 600kbps.

d. Interfaces de Comunicación

Se pretende que el software tenga acceso a la comunicación en red con el respectivo protocolo TCP/IP (Protocolo de Internet), el cual permite la comunicación de datos a través de una red de paquetes conmutados.

XVIII. Requerimientos Funcionales

Ver Anexo A

XIX. Requerimientos no Funcionales

- Desempeño. El tiempo para carga de documentos dependerá del ancho de banda del host y del servidor web en donde está alojada la aplicación y dependerá del tamaño del documento PDF que se vaya a cargar a la aplicación.
- Seguridad: El sistema validara la sesión de acuerdo al perfil de seguridad pre-asignado al usuario.

- Disponibilidad. El Sistema se encontrará alojado en la Web y siempre estará accesible.
- Escalabilidad. El sistema será fácilmente escalable en caso de un incremento en la cantidad de Socios y de documentos PDF
- Mantenibilidad. La verificación y procesamiento de Firmas electrónicas se encuentra parametrizada y adecuada para la infraestructura de certificados digitales emitidos por el Banco Central del Ecuador; Sin Embargo en caso de que la organización desee operar con certificados digitales de otra AC, es posible re-parametrizar la configuración y adecuarla a la infraestructura de certificados de la nueva AC.

3.2. DISEÑO DEL SISTEMA

3.2.1. Arquitectura del Sistema

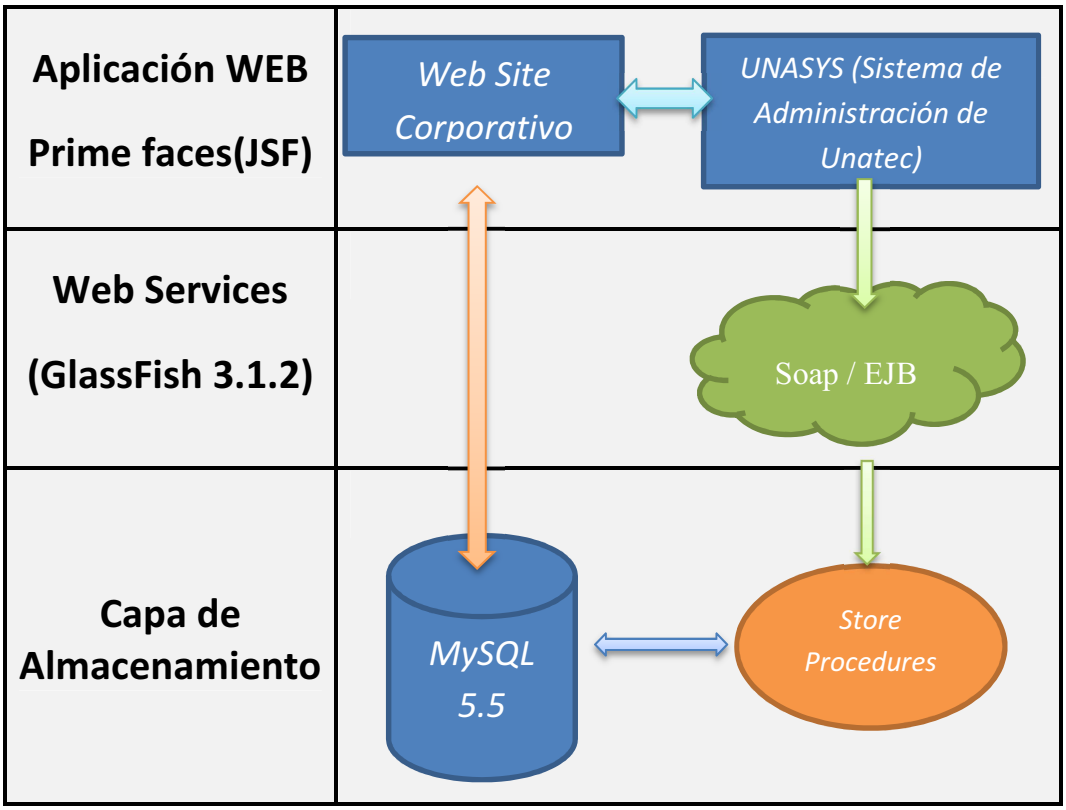


Tabla 3.2: Arquitectura del sistema

3.2.2. Modelos de caso de uso

I. Identificación de actores

Actores que intervienen en el sistema

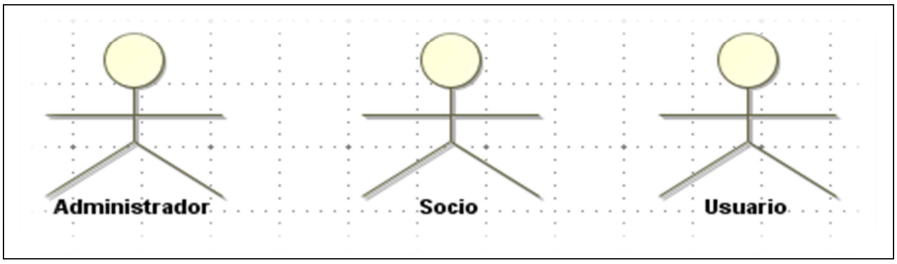


Figura 3.1*:* **Actores que intervienen en el sistema**

Espacio en Blanco
Intencional

II. Diagramas de Casos de Uso

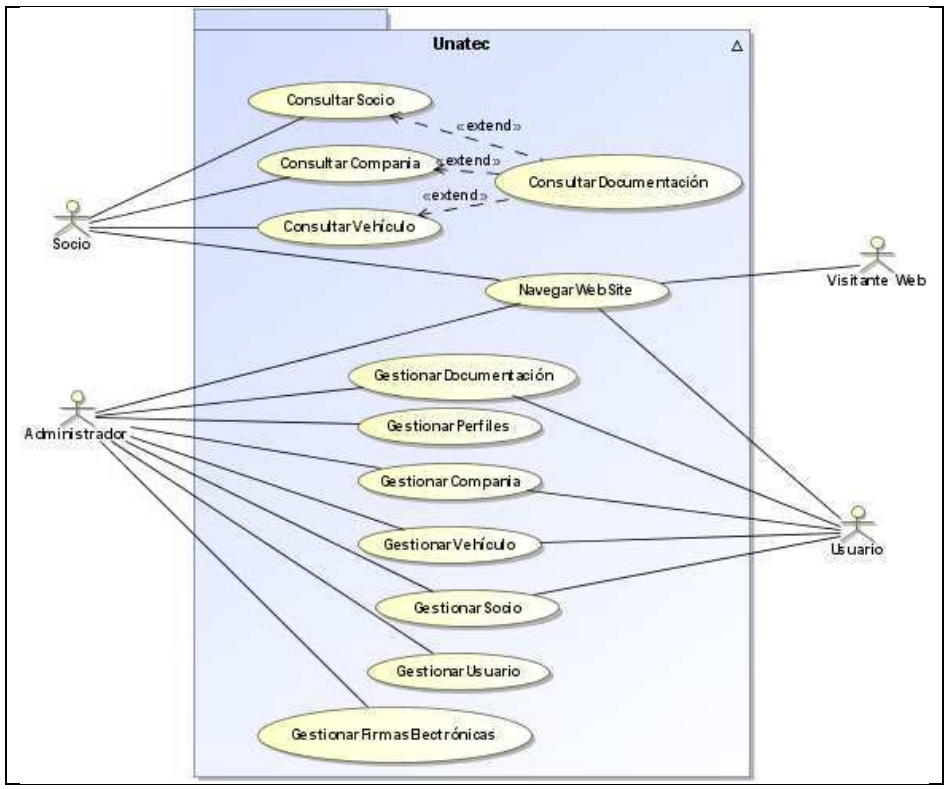


Figura 3.2*:* Modelo de Casos de Uso General

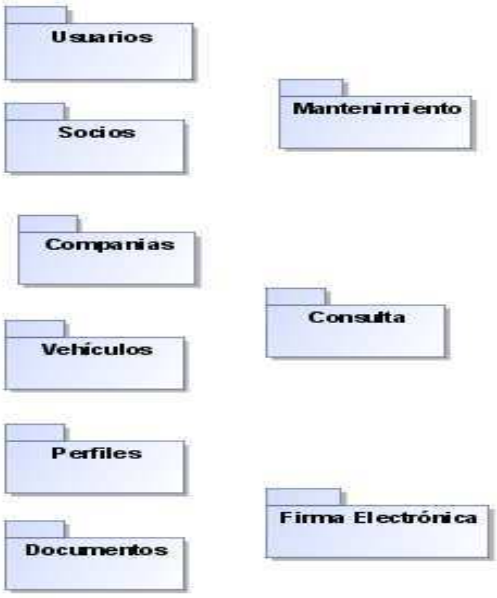


Figura 3.3*:* Módulos del Sistema

III. Diagramas de Casos de Uso Específicos

a. Administración General de Registros A

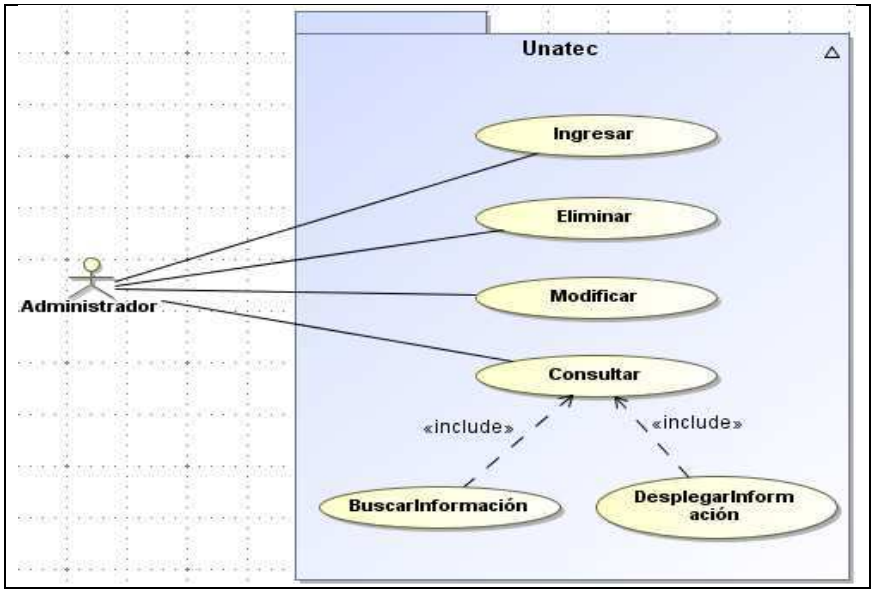


Figura 3.4: Administración General de Registros A

b. Administración General de Registros B

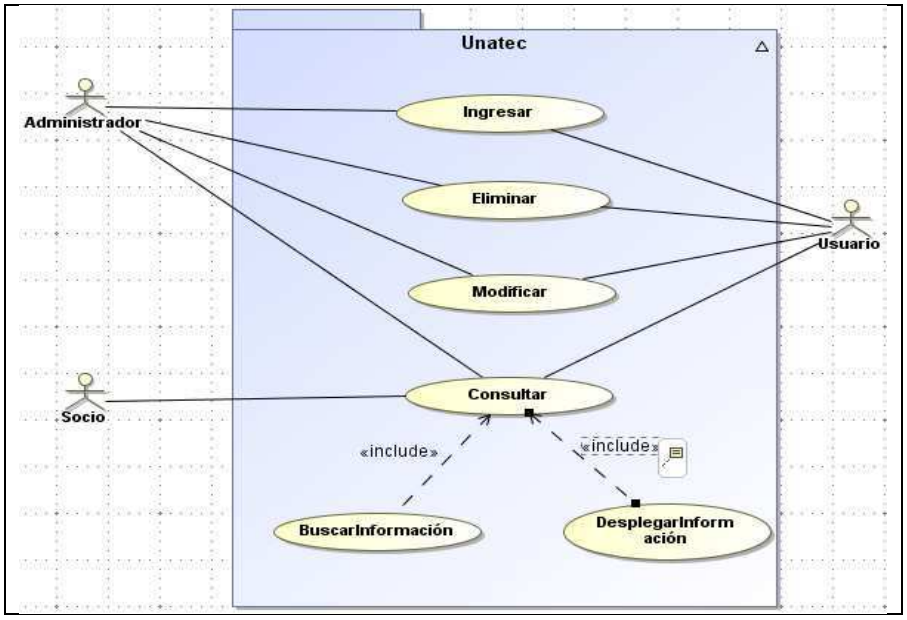


Figura 3.5: Administración General de Registros B

c. Administración Asignación a Socios

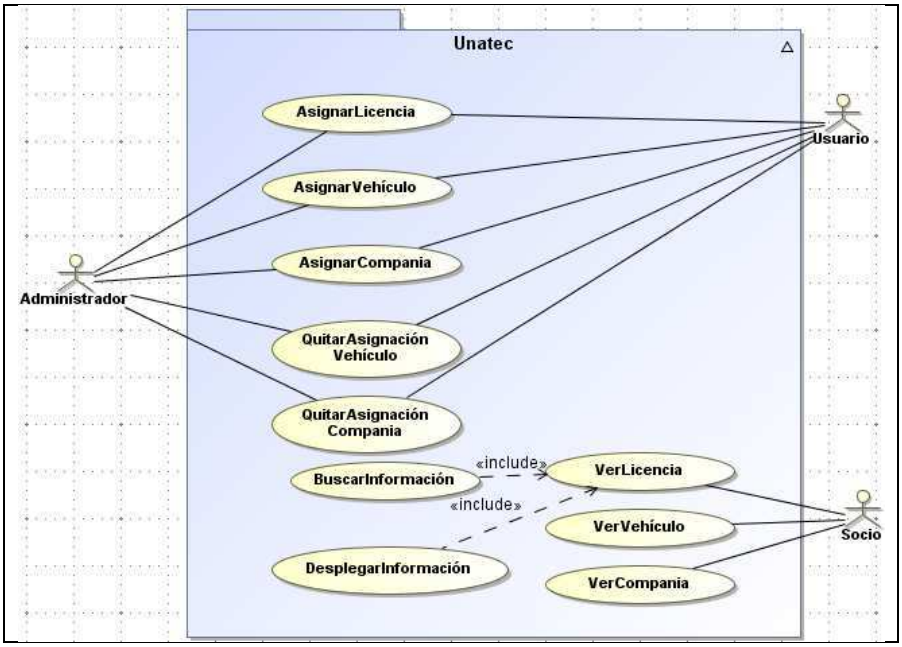


Figura 3.6: Administración Asignación a Socios

d. Administración de Representante de Compañía

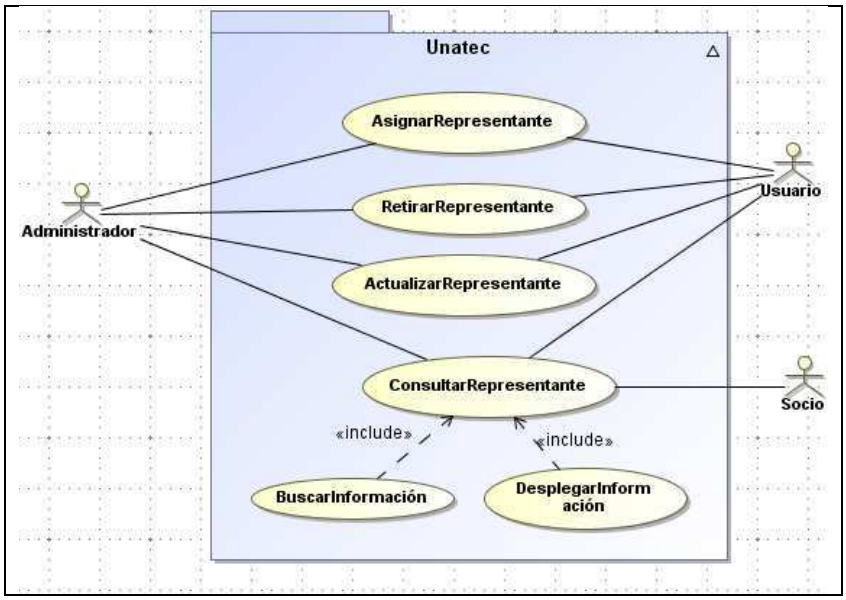


Figura 3.7: Administración de Representante de Compañía

e. Administración de Oficios

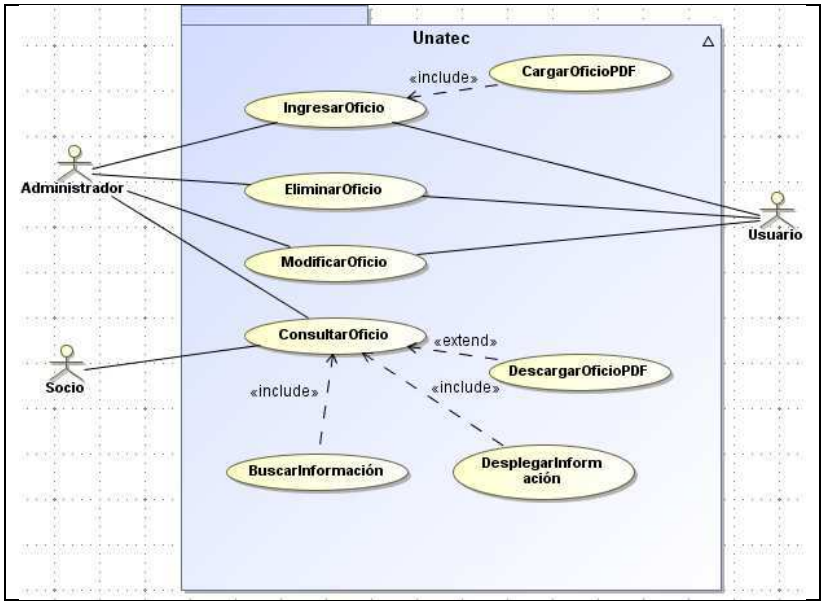


Figura 3.8: Administración de Oficios

f. Gestión de Firma Electrónica

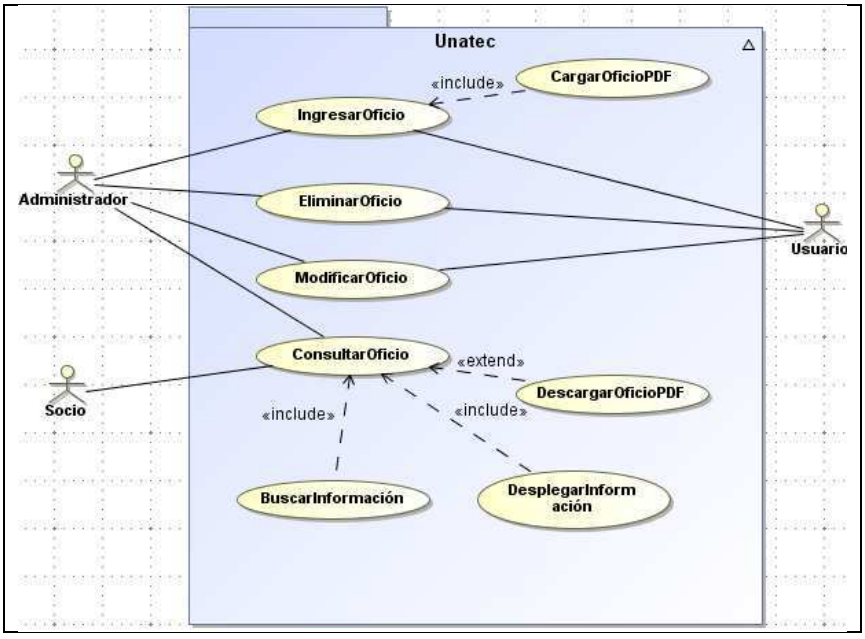


Figura 3.9: Gestión de Firma Electrónica

g. Consulta

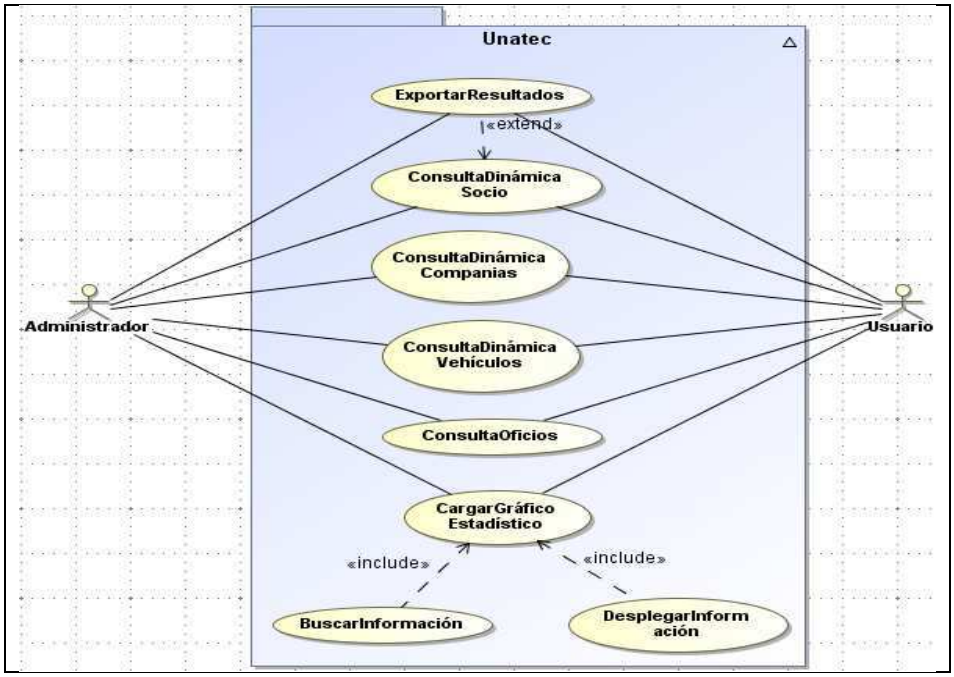


Figura 3.10: Módulo de Consultas

Espacio en Blanco
Intencional

3.2.3. Diagrama de Clases Lógico

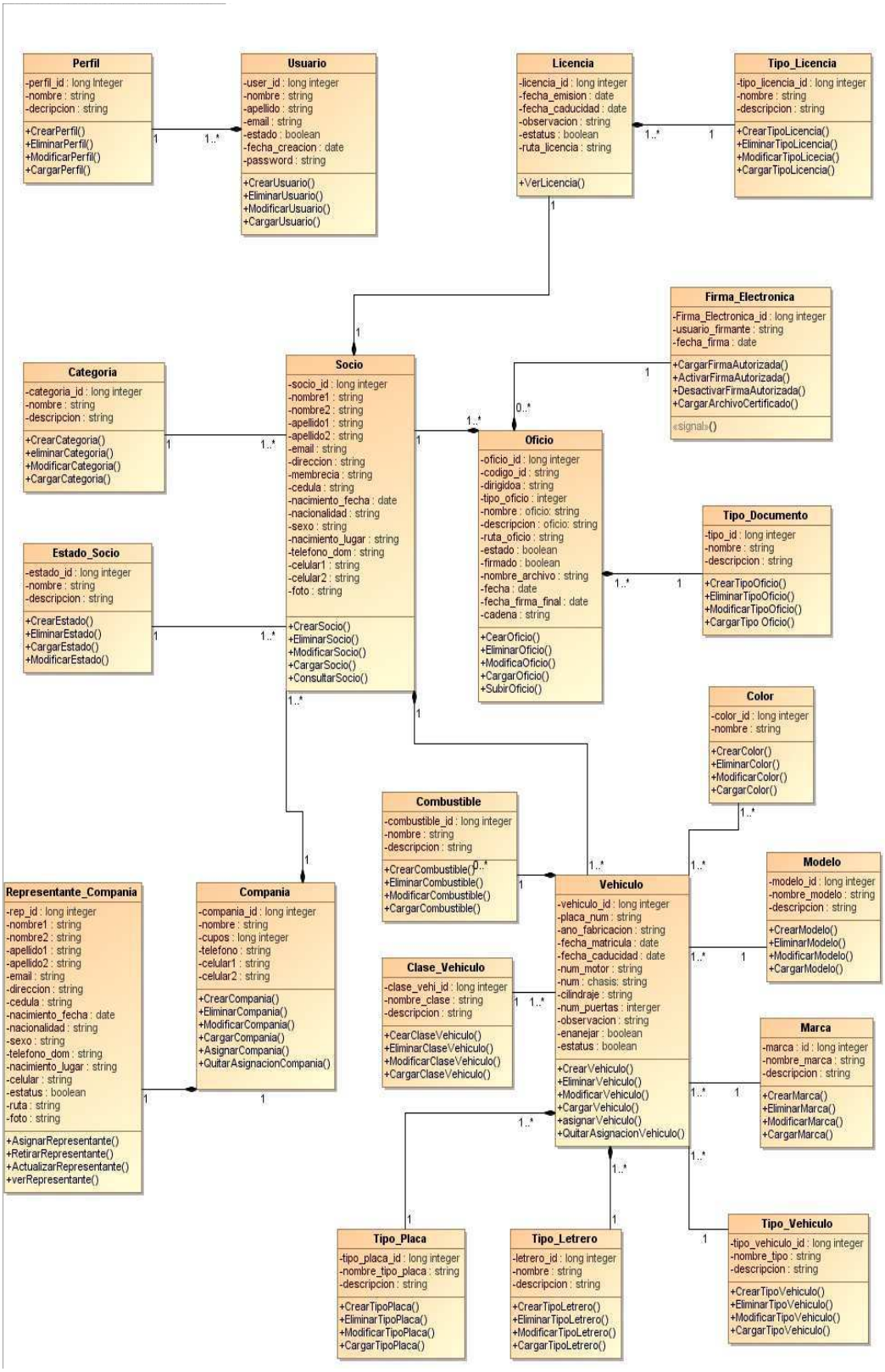


Figura 3.11: Diagrama de Clases Lógico

3.2.4. Diagrama Entidad Relación

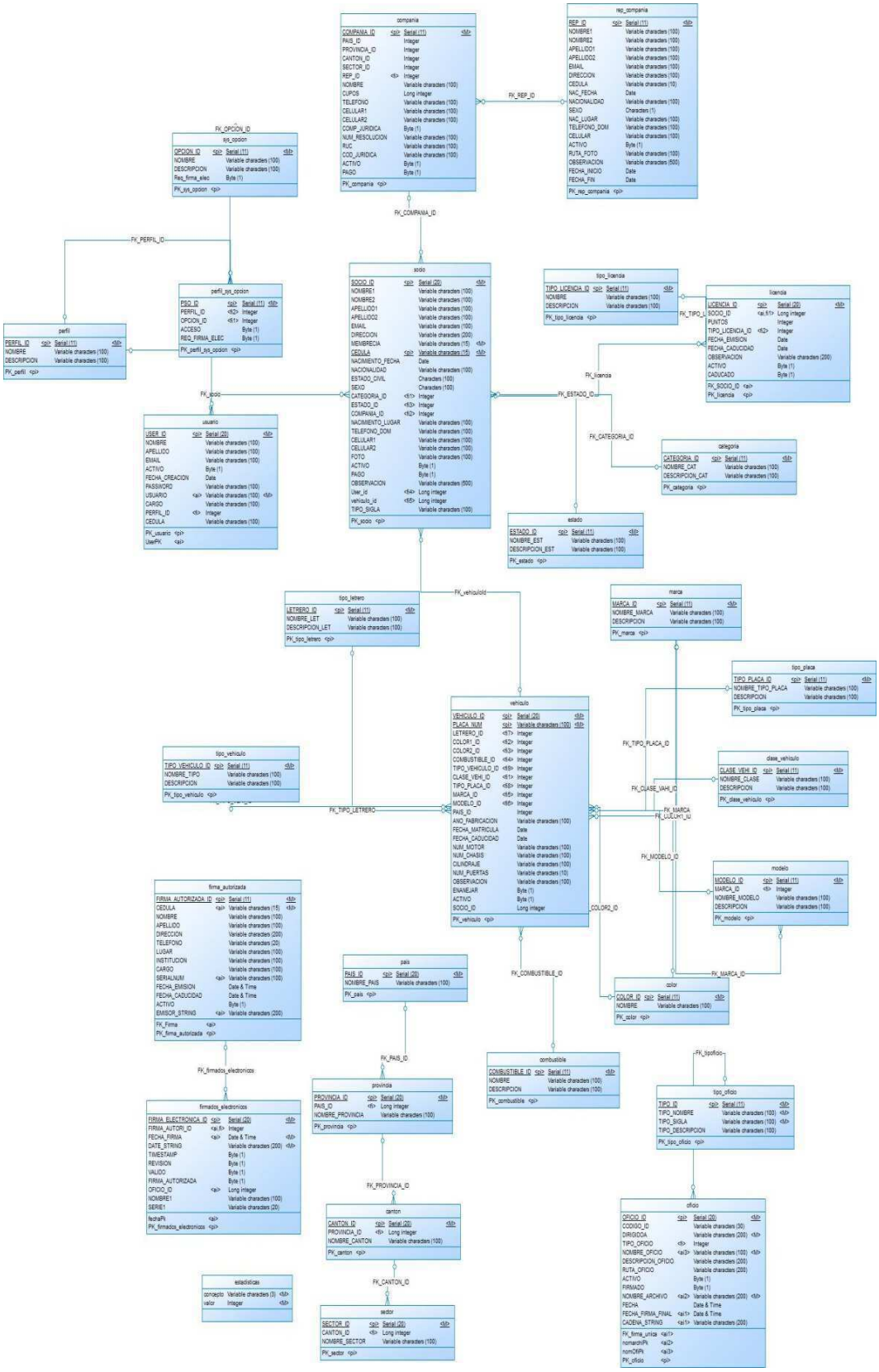


Figura 3.12: Diagrama Entidad Relación

3.2.5. Diagrama de Navegación

I. Diagrama de Navegación de Administrador

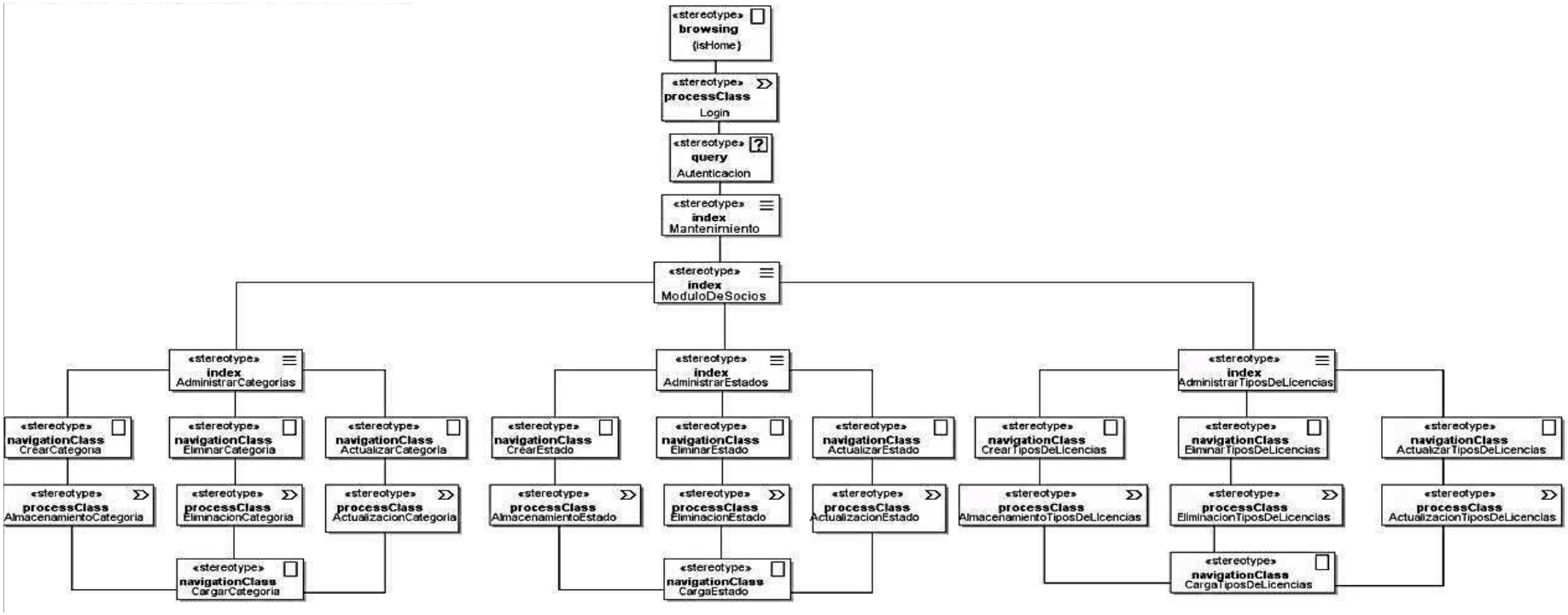


Figura 3.12: Diagrama de Navegación de Administrador #1

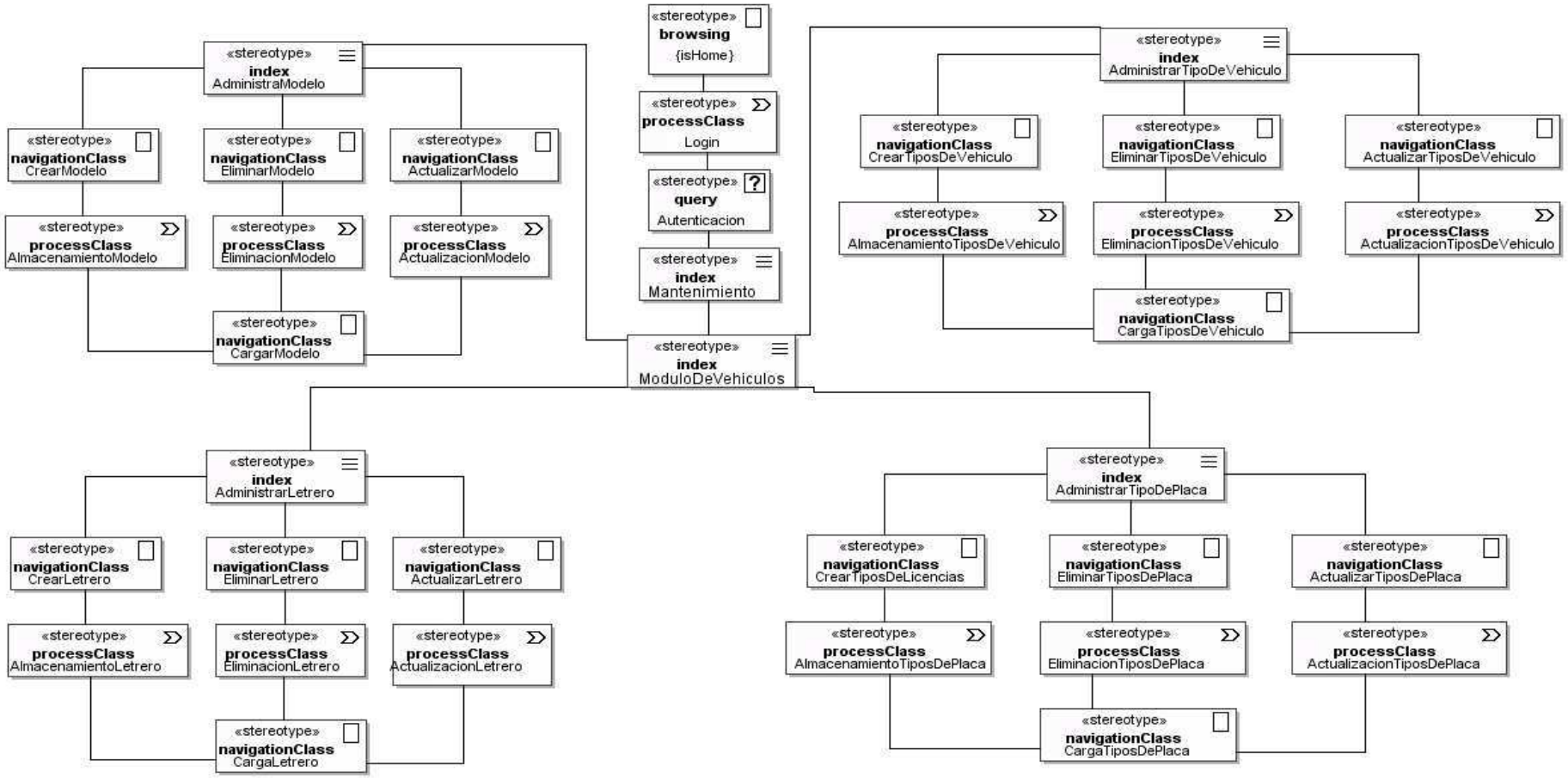


Figura 3.13: Diagrama de Navegación de Administrador #2

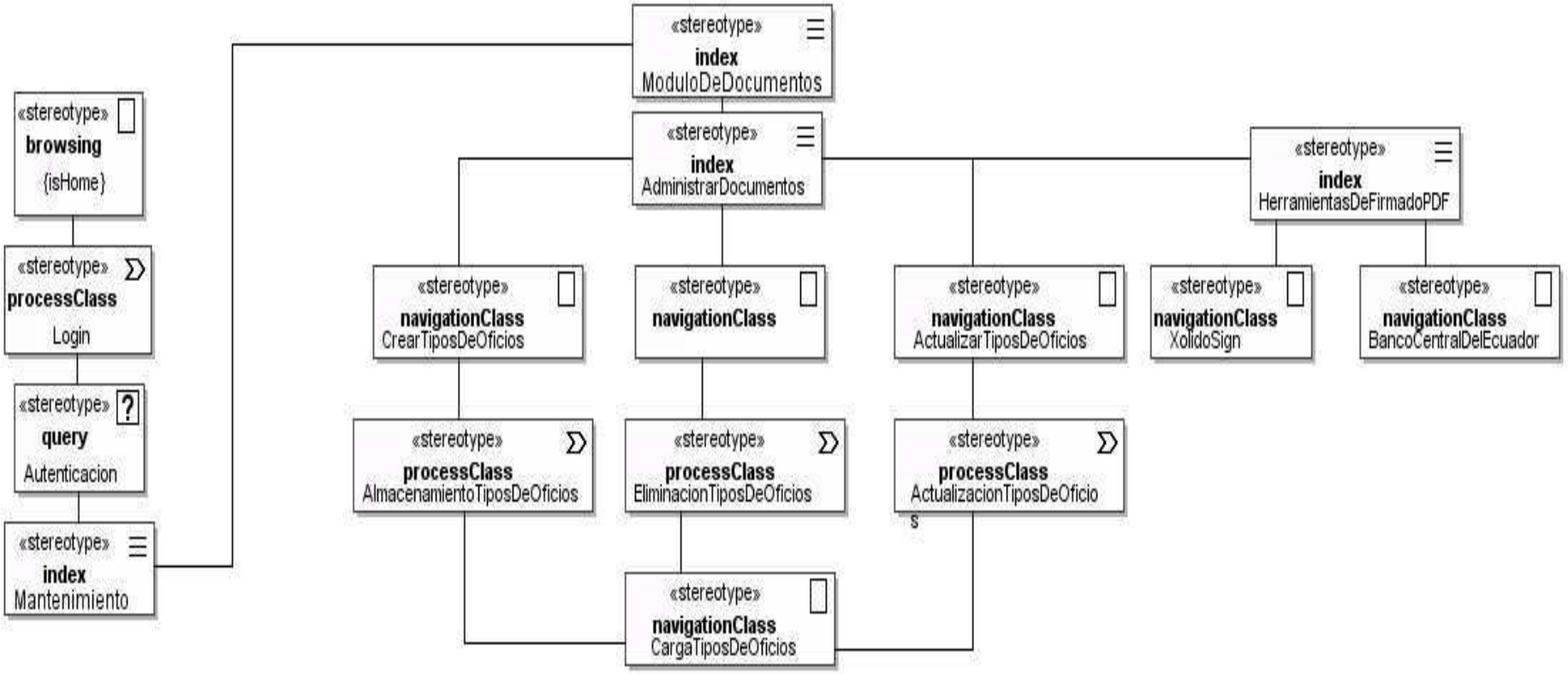


Figura 3.14: Diagrama de Navegación de Administrador #3

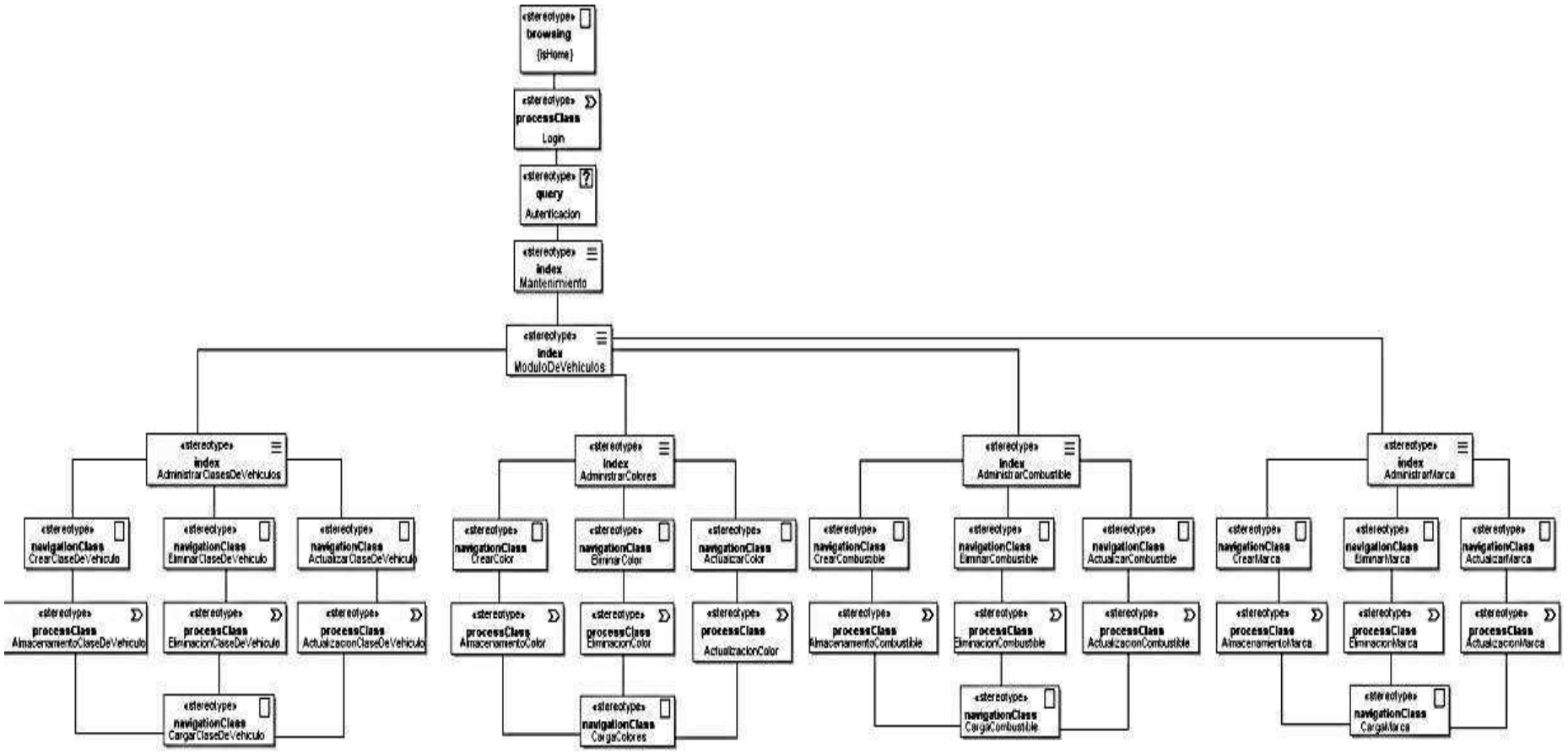


Figura 3.15: Diagrama de Navegación Administrador #4

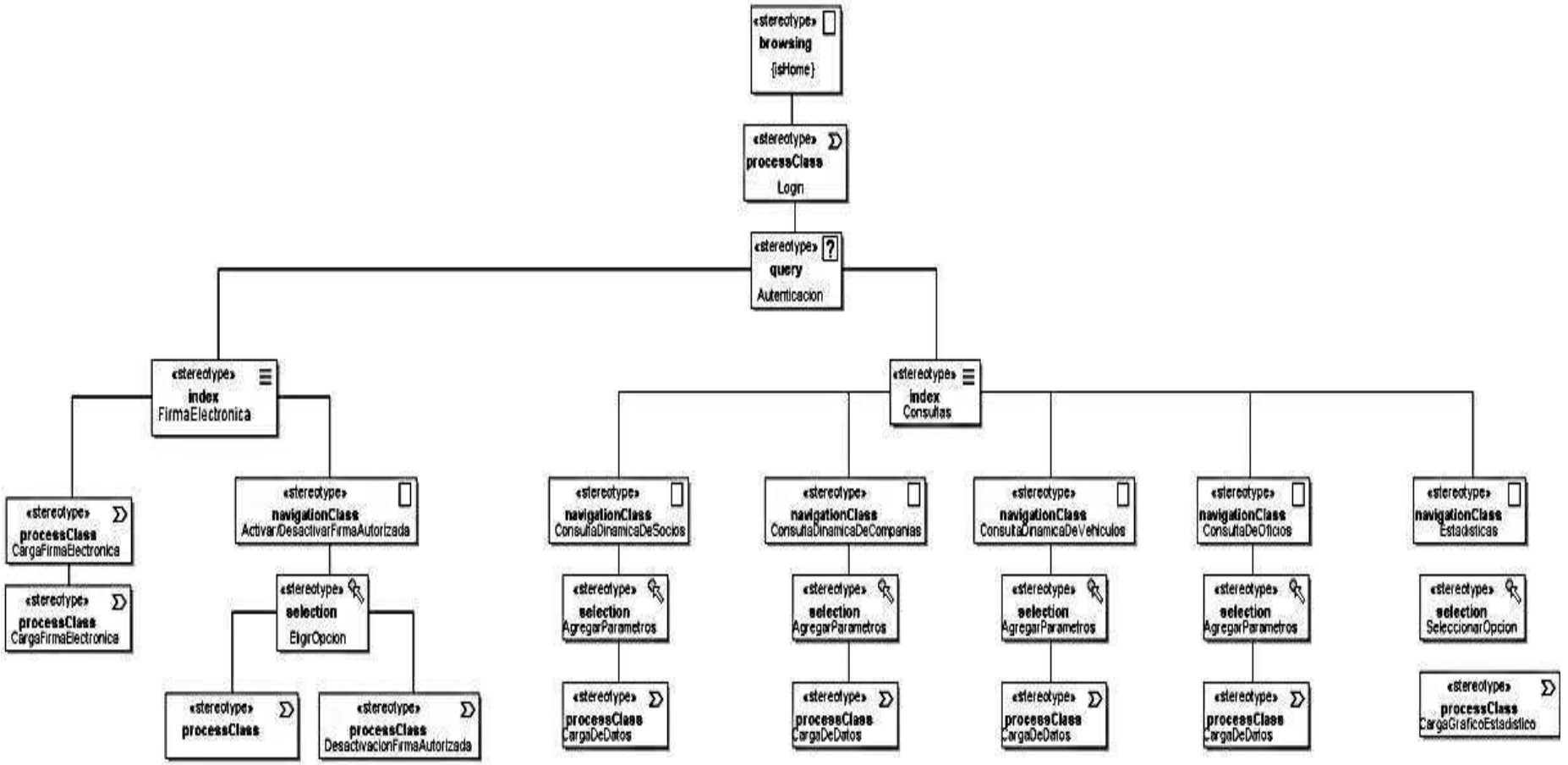


Figura 3.16: Diagrama de Navegación Administrador #5

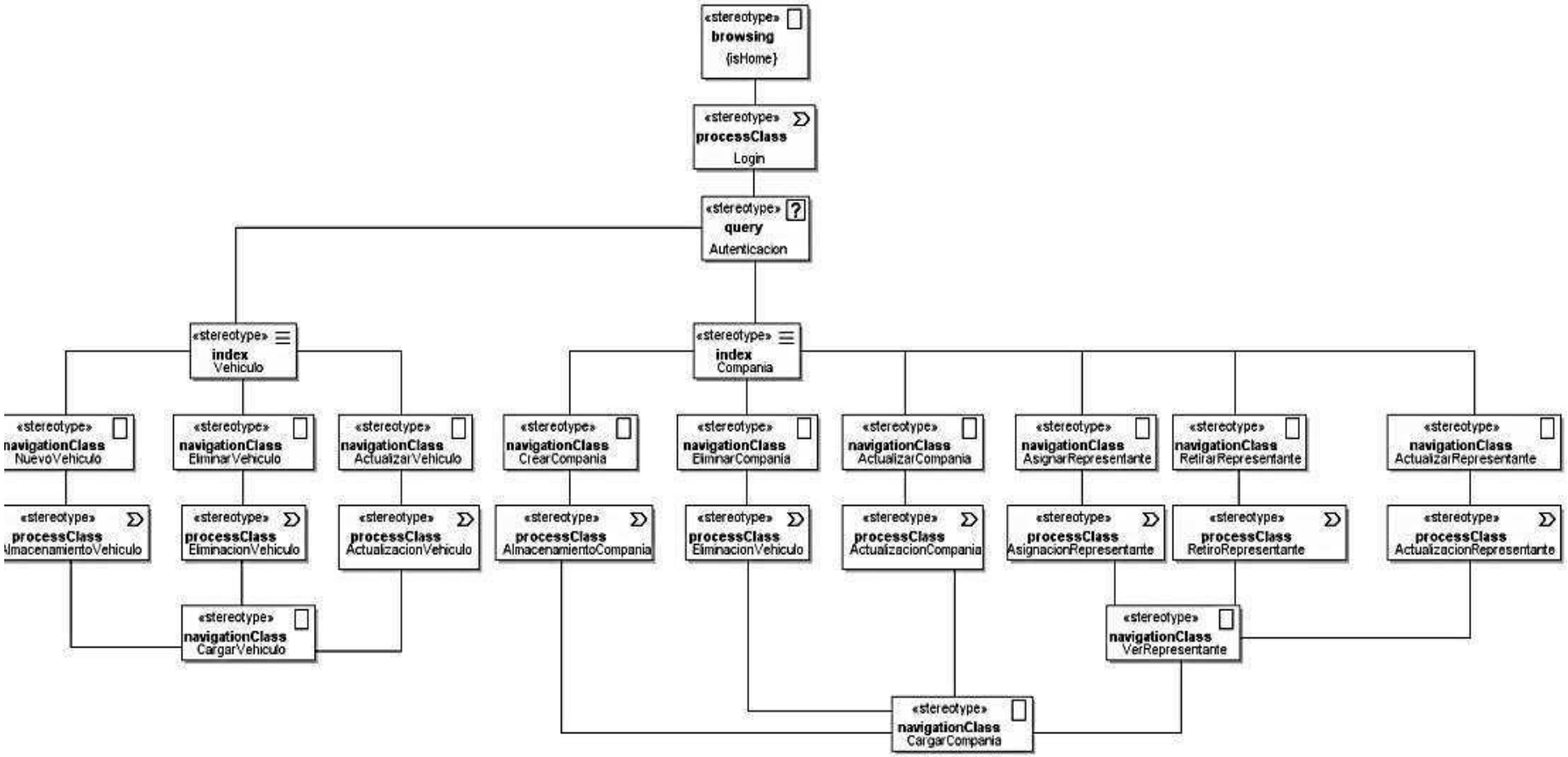


Figura 3.16: Diagrama de Navegación de Administrador #6

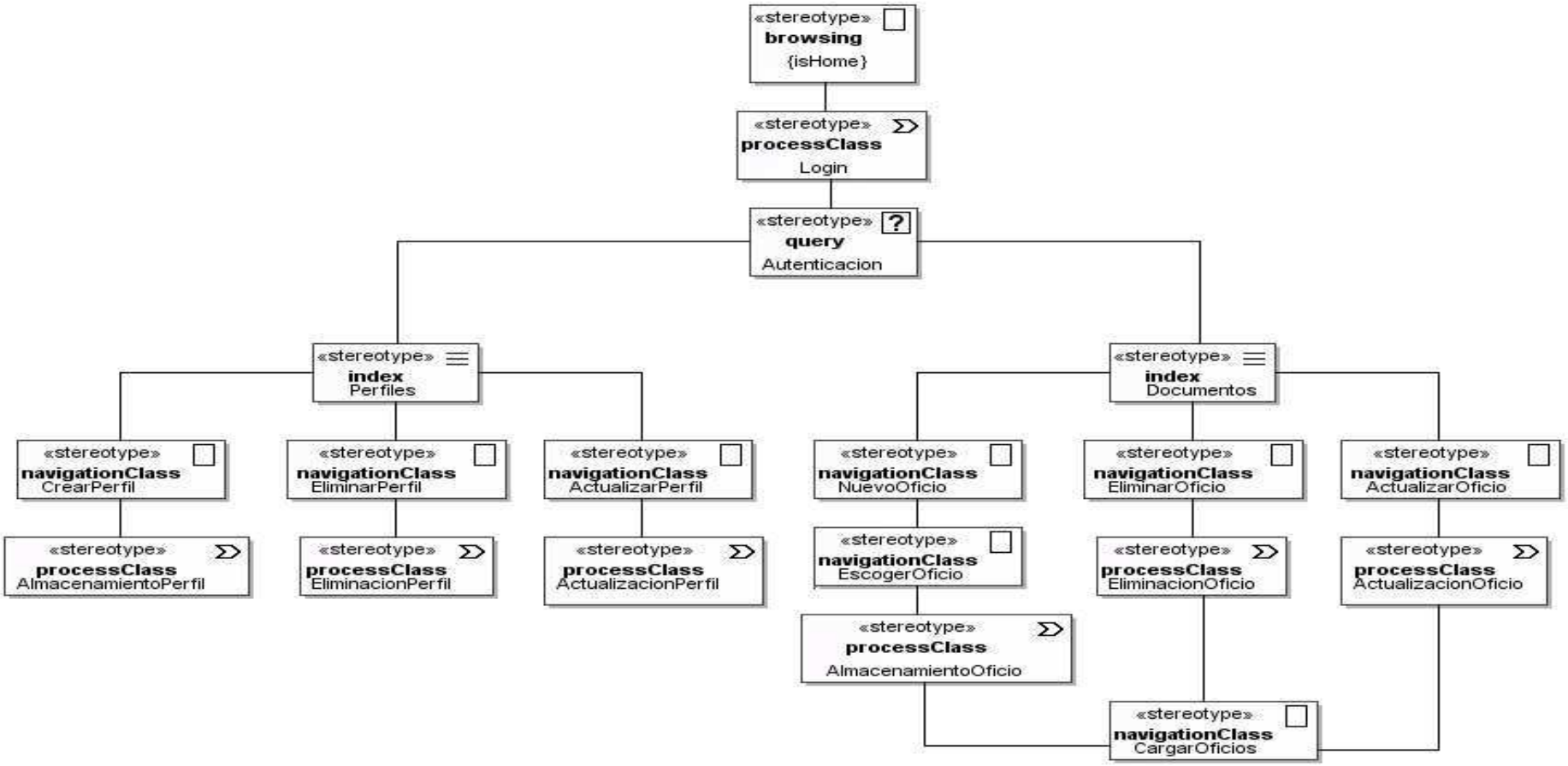


Figura 3.17: Diagrama de Navegación de Administrador #7

II. Diagrama de Navegación Usuario

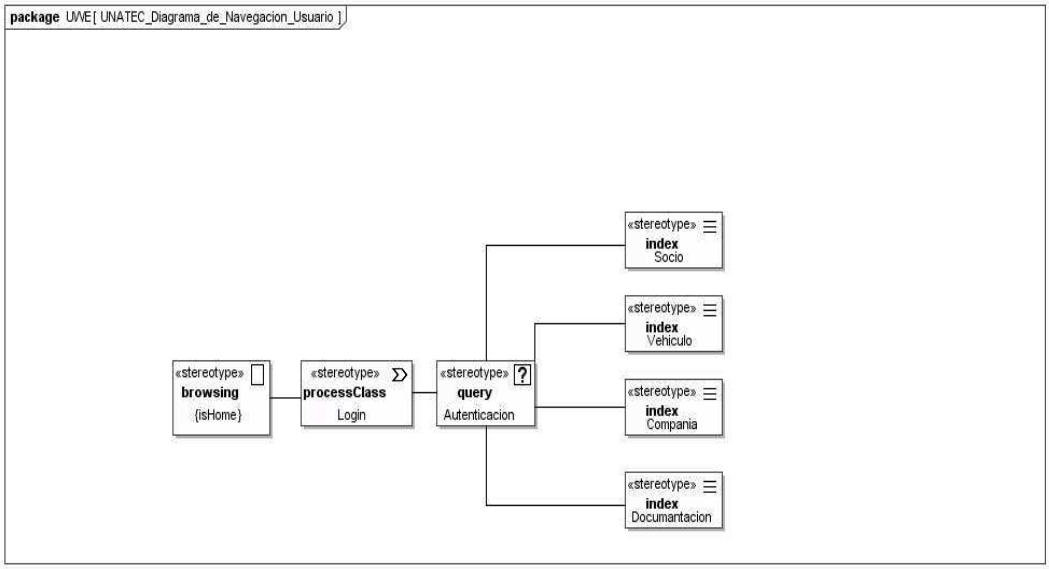


Figura 3.18 Diagrama de Navegación de Usuario

III. Diagrama de Navegación de Socio

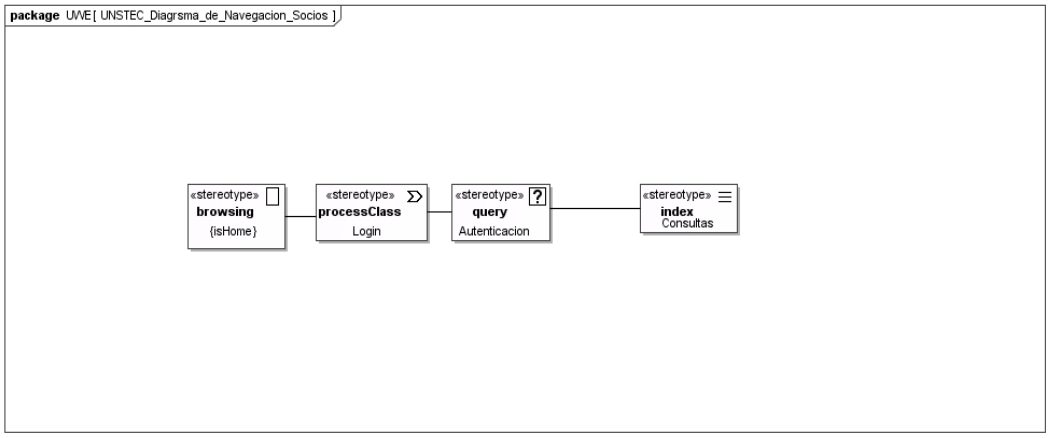


Figura 3.19 Diagrama de Navegación de Usuario

3.2.6. Diagramas de Secuencia

I. Administrar Usuario

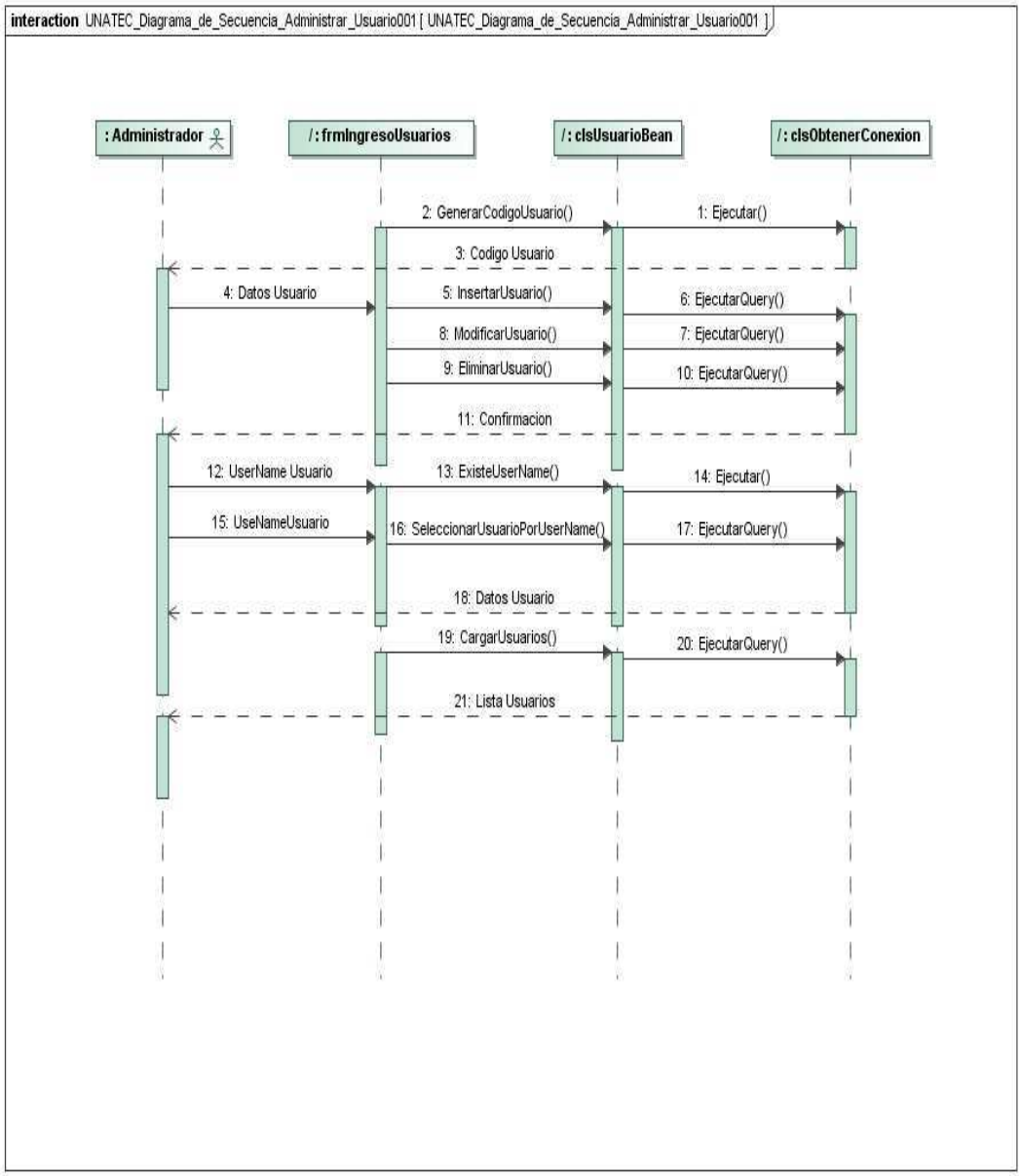


Figura 3.20 Diagrama de Secuencia Administrar Usuario

II. Administrar Socio

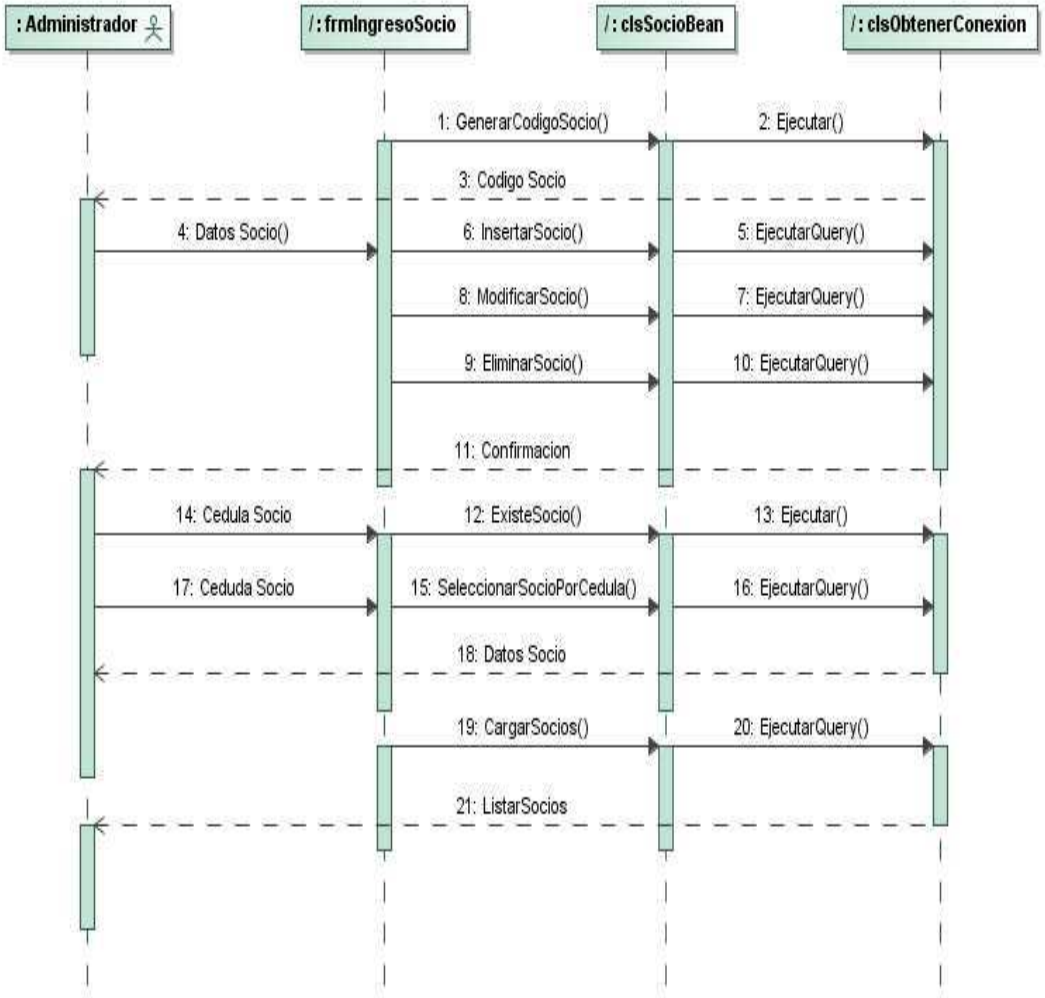


Figura 3.21 Diagrama de Secuencia de Administrar Socio

III. Asignar Socio

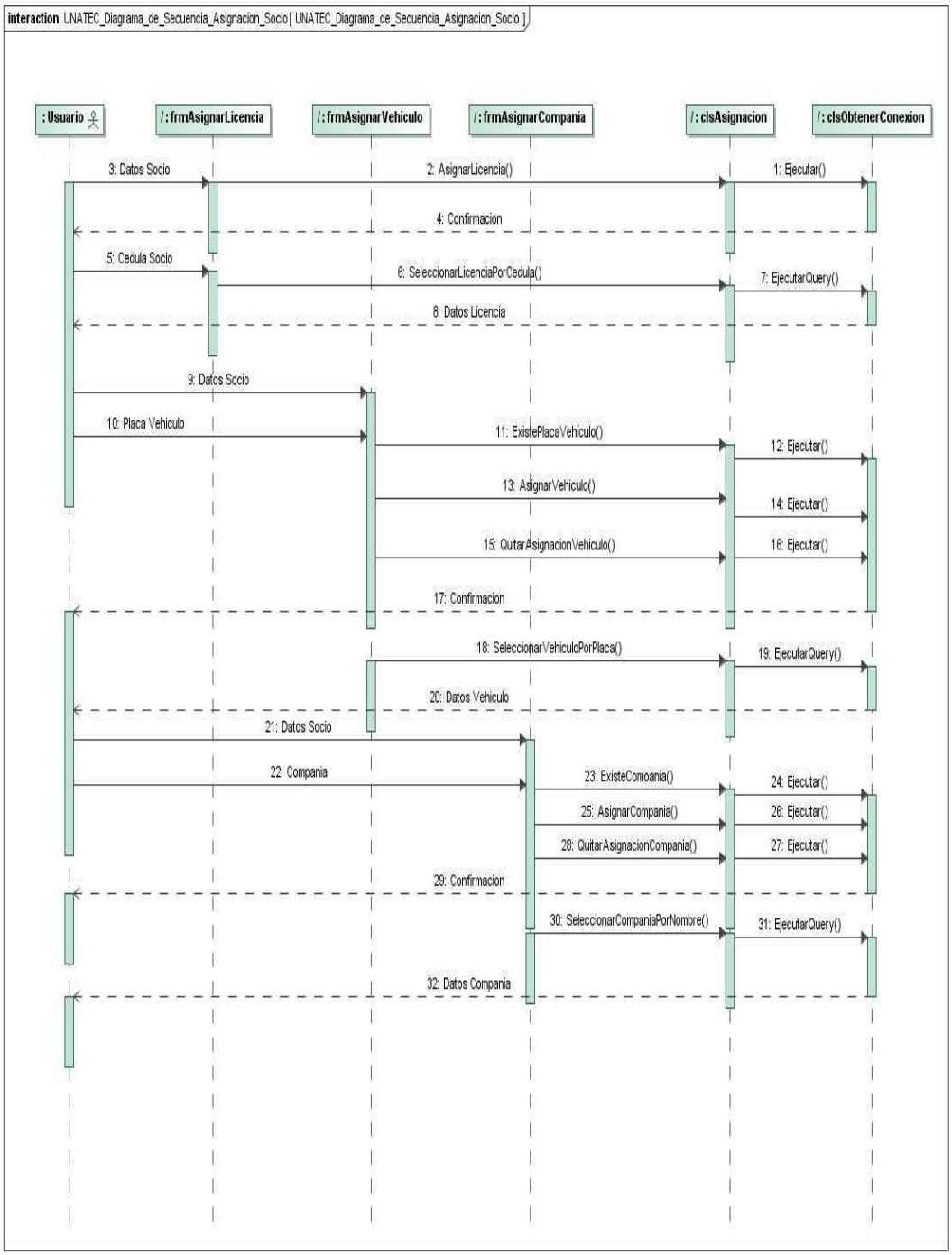


Figura 3.22 Diagrama de Secuencia de Asignación Socio

IV. Administrar Vehículo

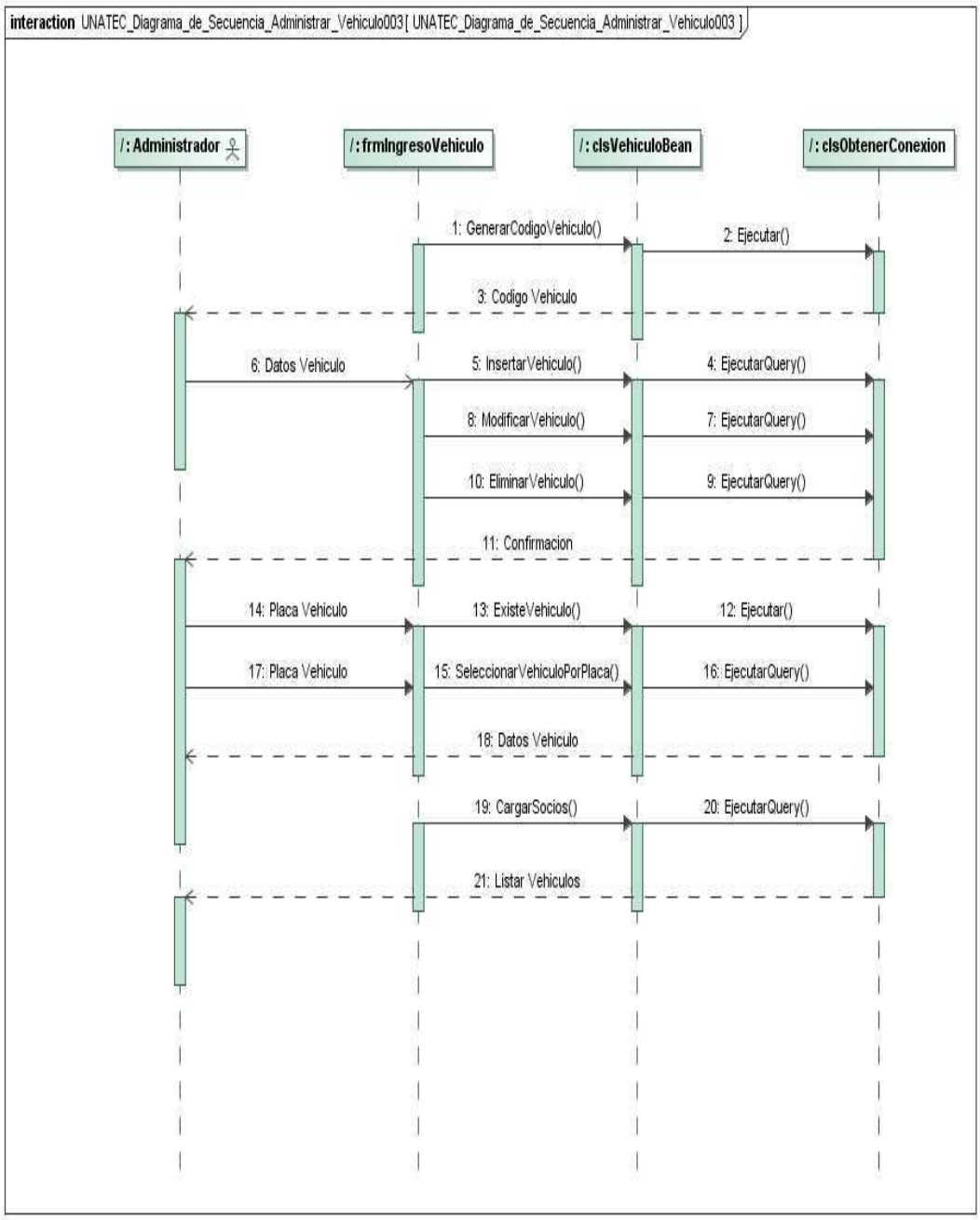


Figura 3.23 Diagrama de Secuencia Administrar Vehículo

V. Administrar Compañía

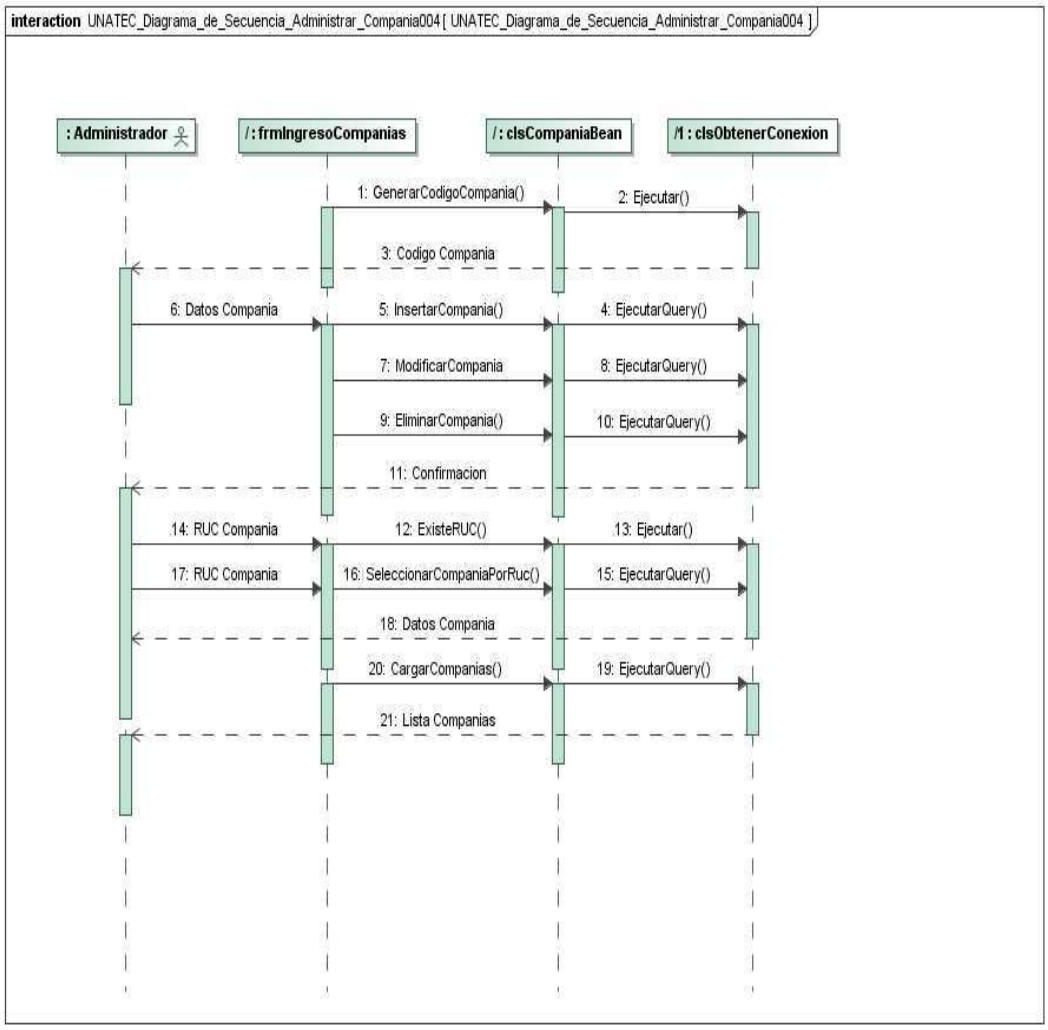


Figura 3.24 Diagrama de Secuencia Administrar Compañía

VI. Asignar Representante

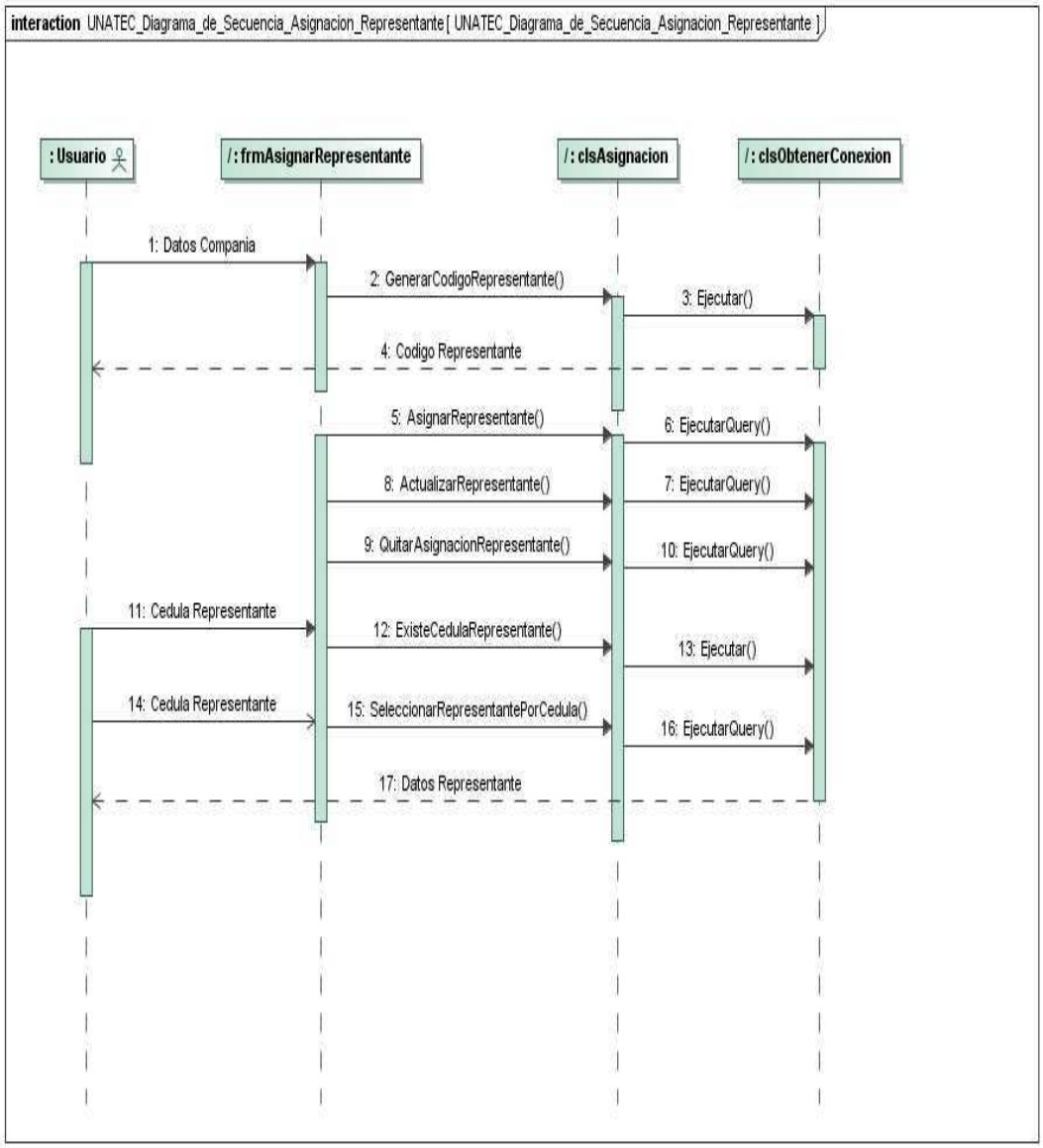


Figura 3.25 Diagrama de Secuencia Asignación Representante

VII. Administrar Perfil

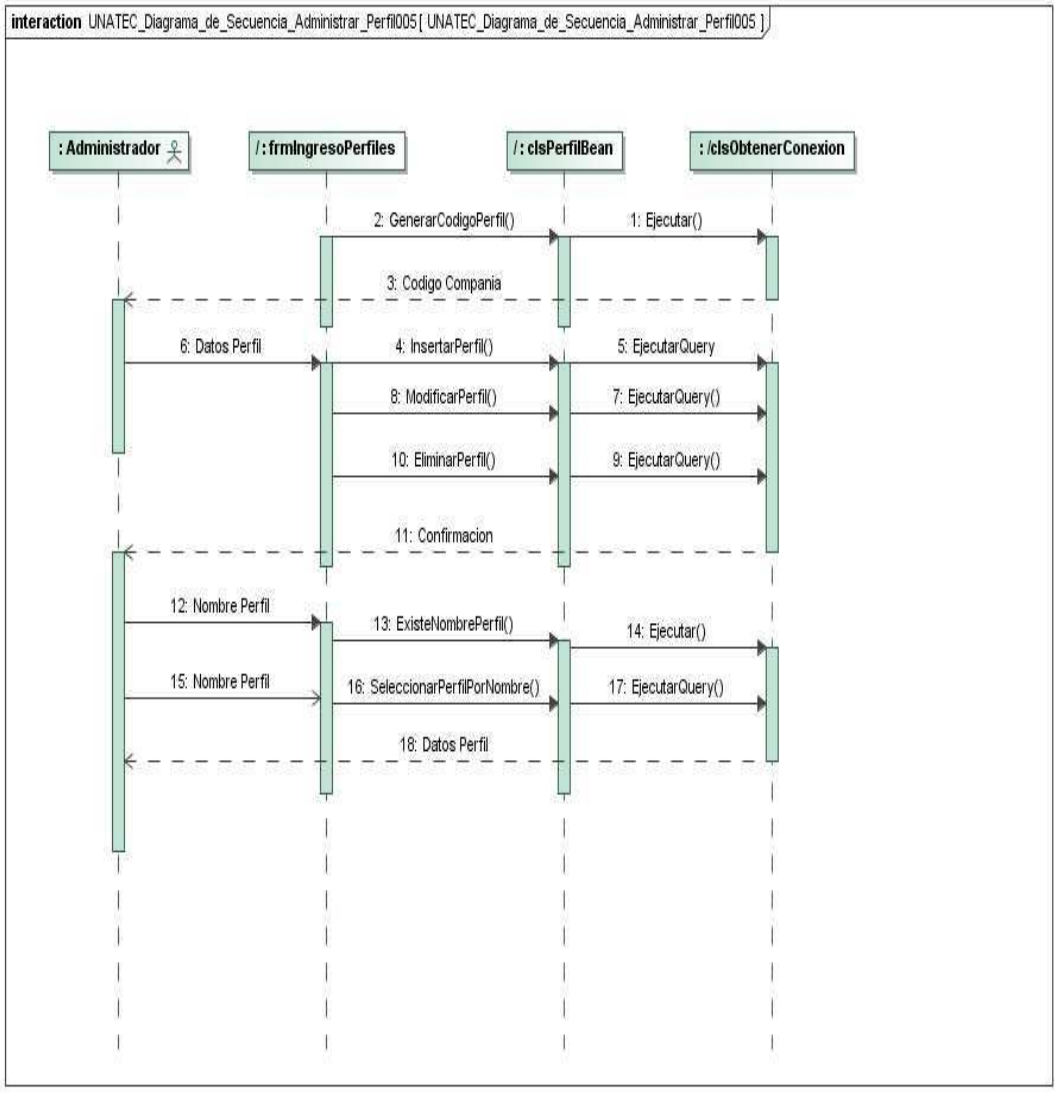


Figura 3.26 Diagrama de Secuencia Administrar Perfil de Seguridad

VIII. Administrar Documento

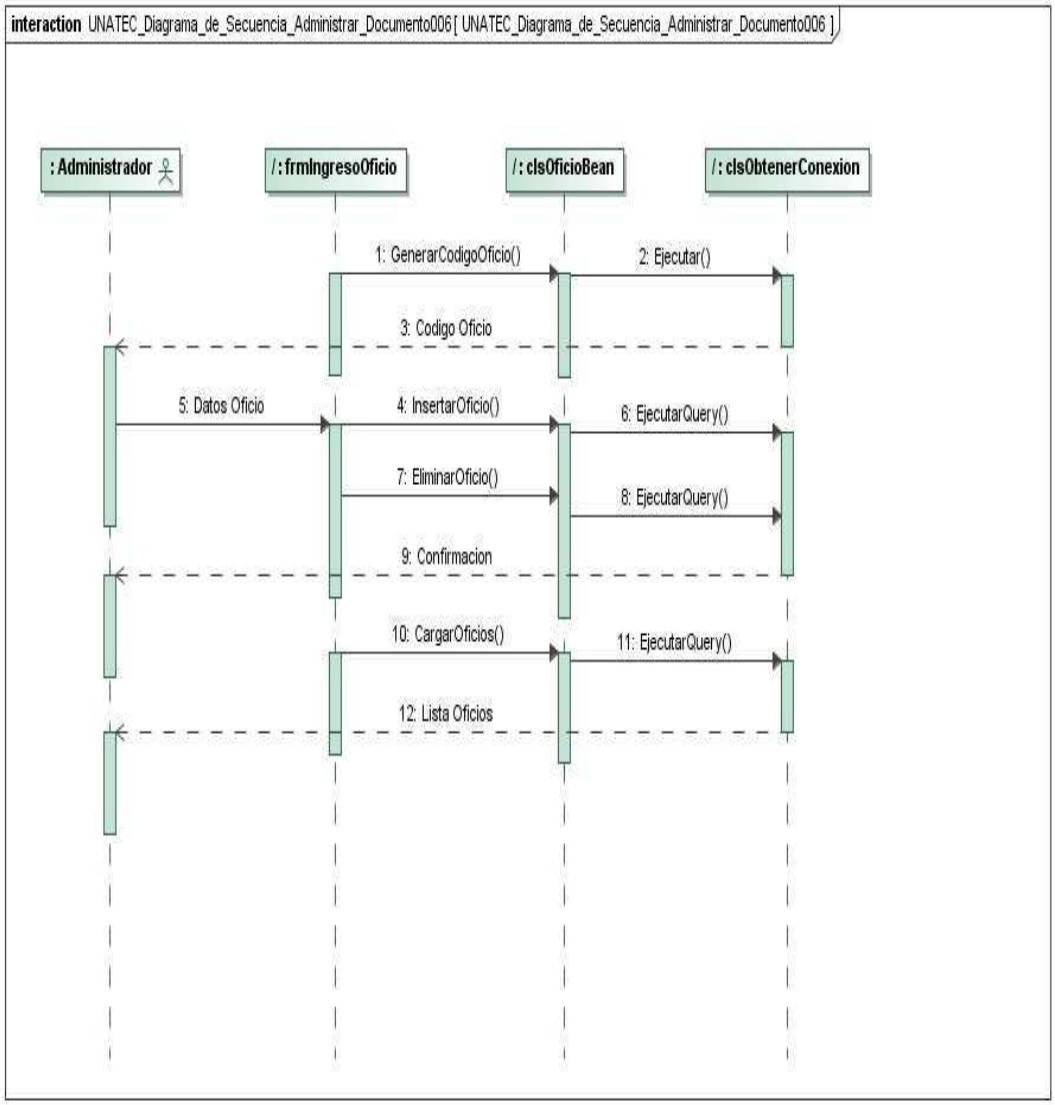


Figura 3.27 Diagrama de Secuencia Administrar Documento

IX. Firma Electrónica

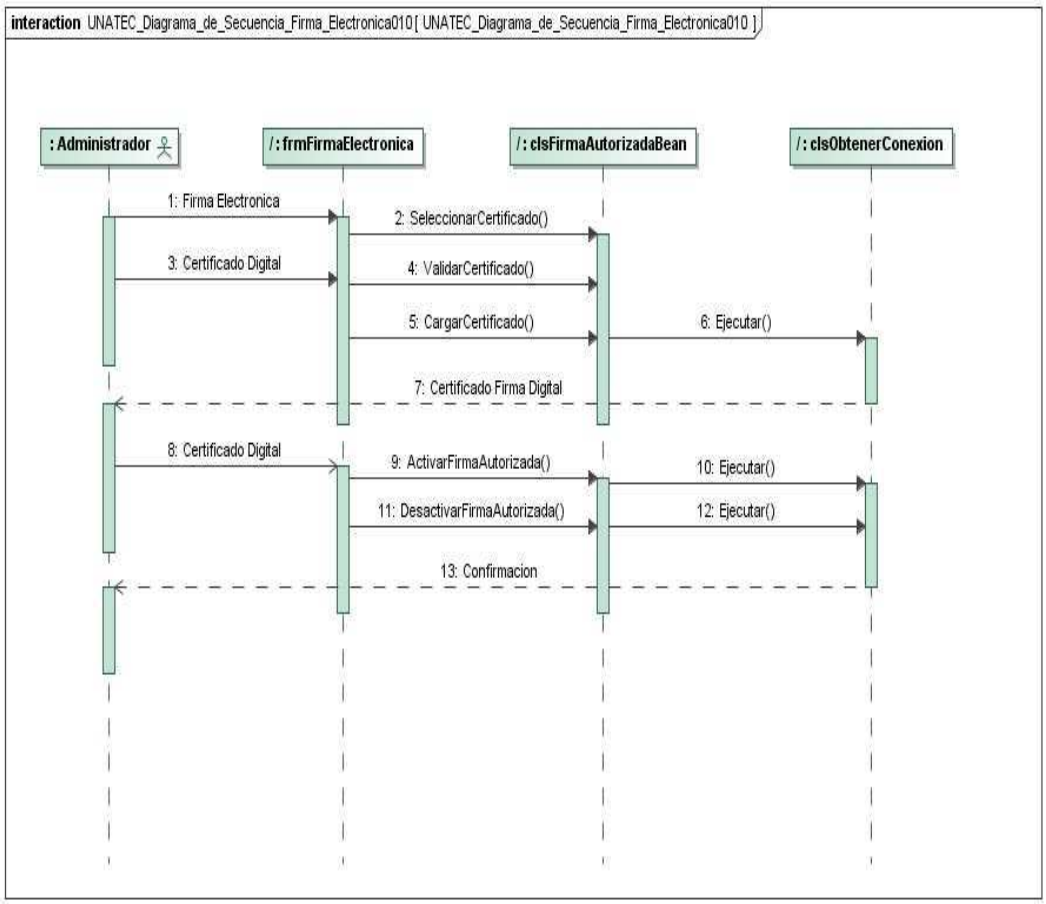


Figura 3.28 Diagrama de Secuencia Firma Electrónica

X. Mantenimiento

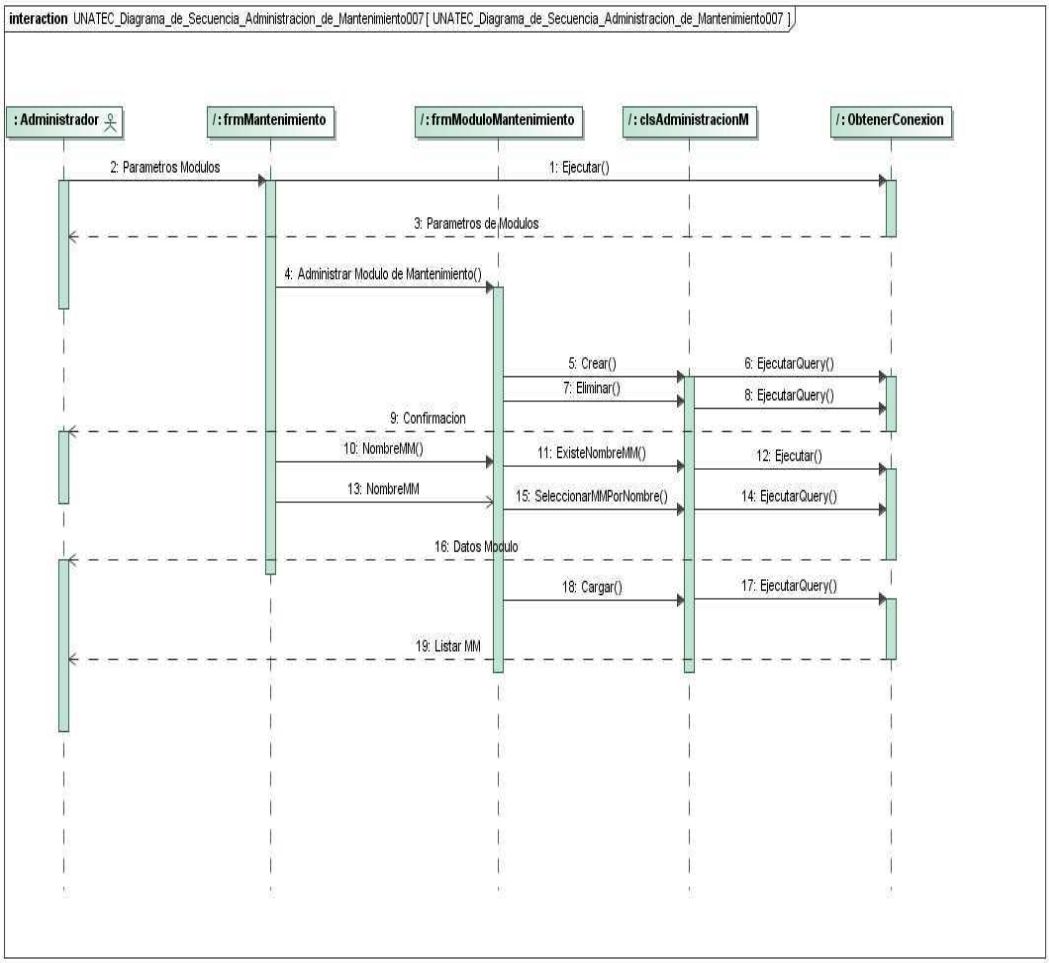


Figura 3.29 Diagrama de Secuencia Módulo de Mantenimiento

XI. Consultas

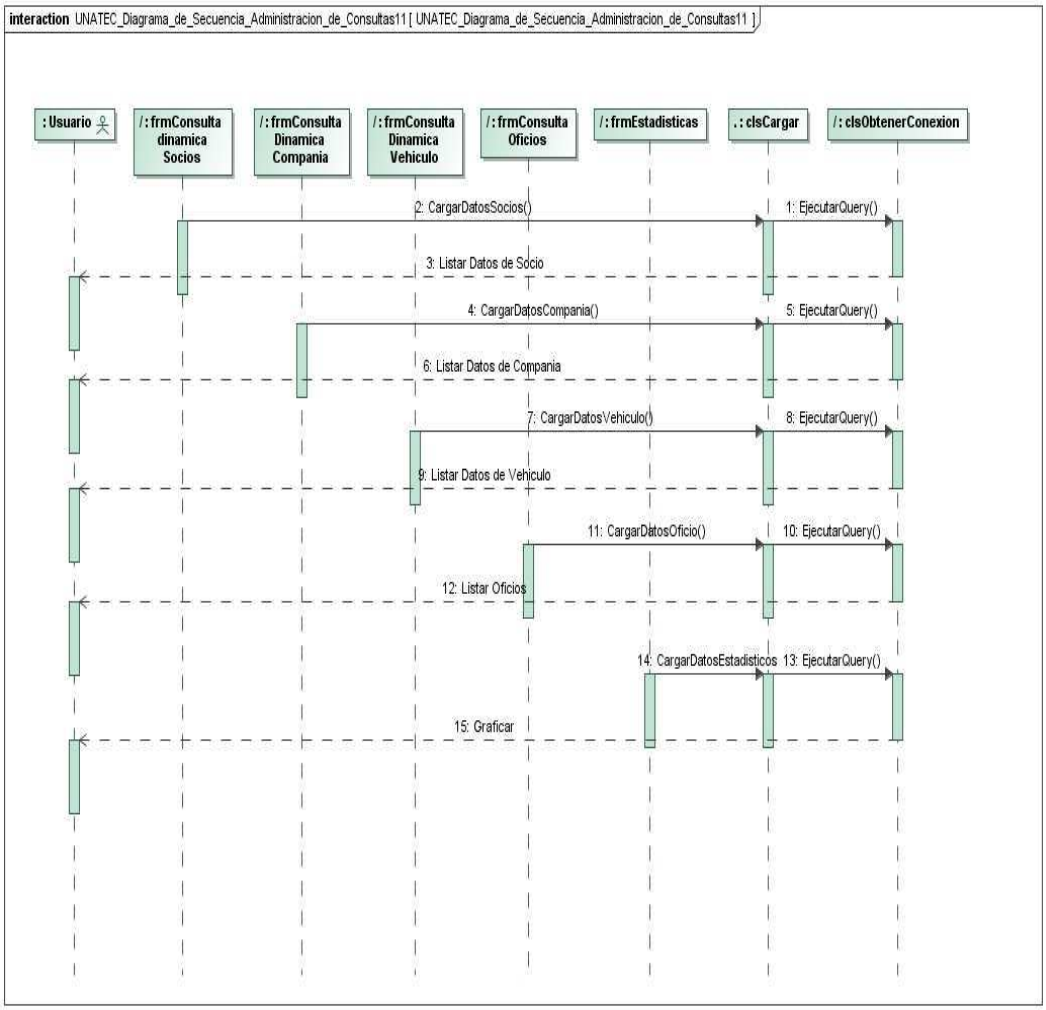


Figura 3.30 Diagrama de Secuencia Módulo de Consultas

3.2.7. Diagramas de Estado

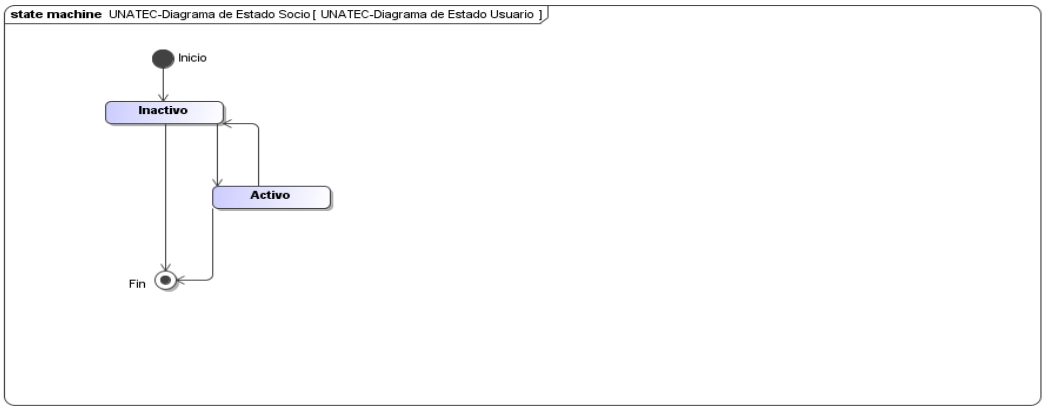


Figura 3.31: Diagrama de Estado de Usuario

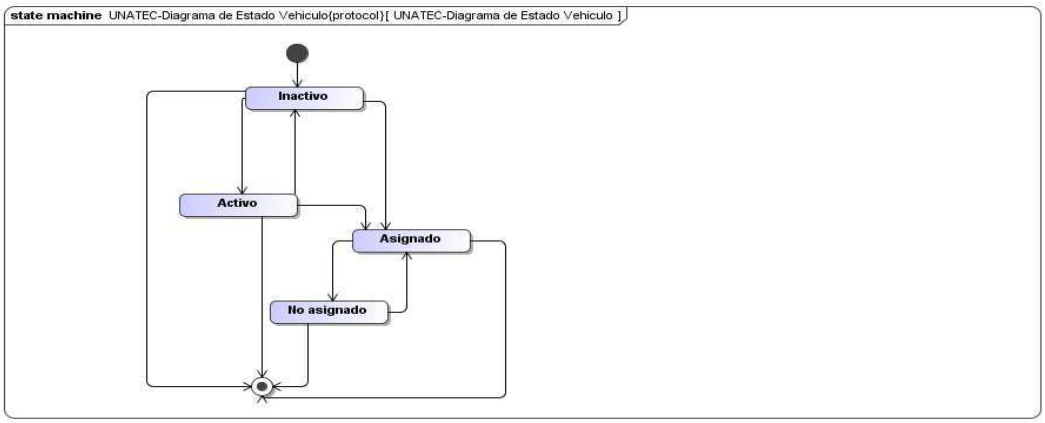


Figura3.32: Diagrama de Estado de Socio

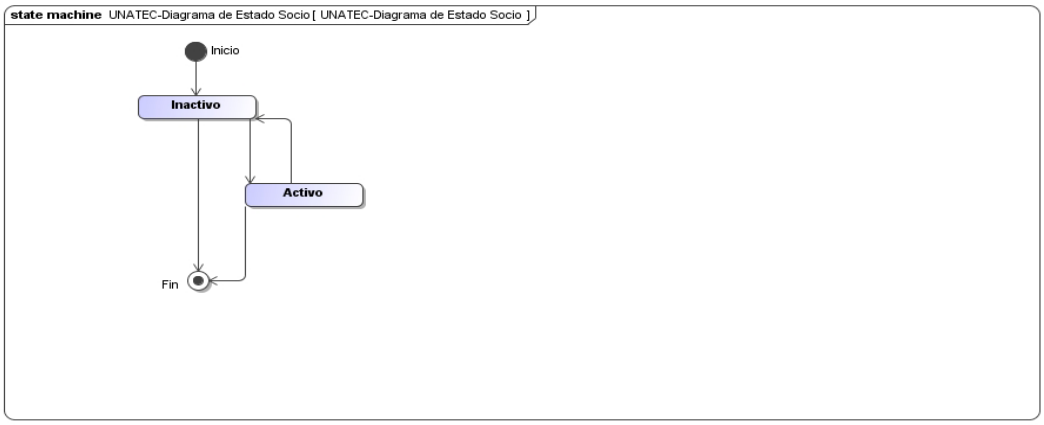


Figura 3.33: Diagrama de Estado de Vehículo

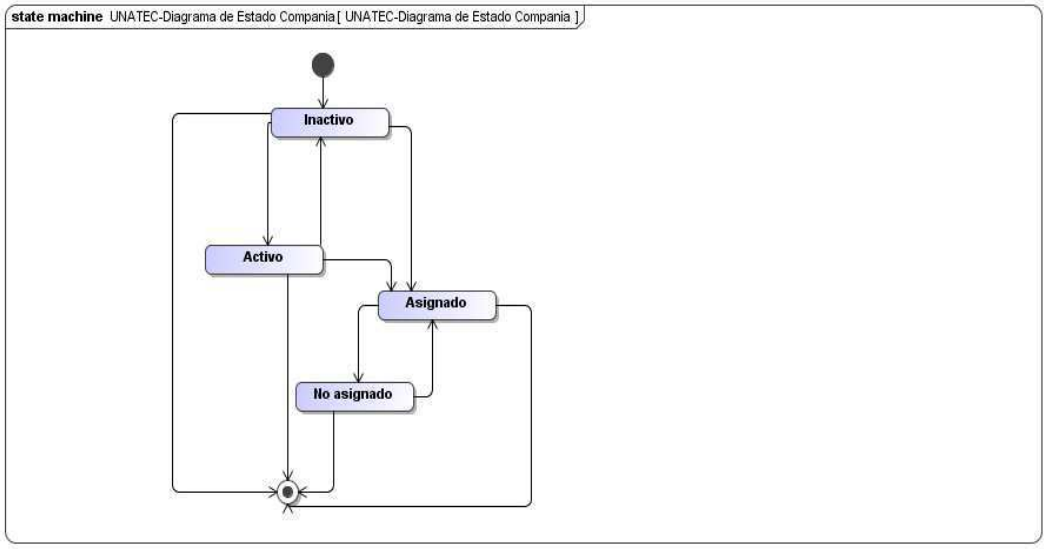


Figura 3.34: Diagrama de Estado de Compañía

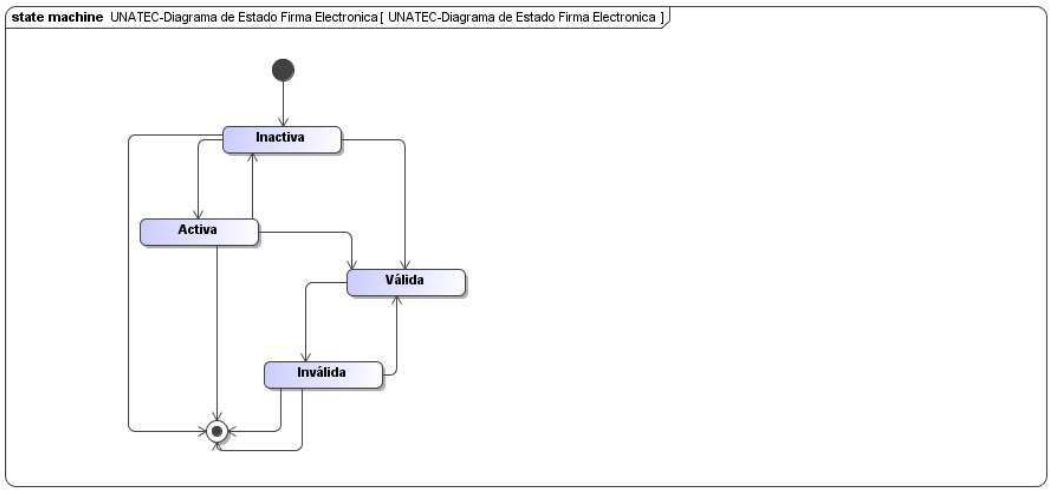


Figura 3.35: Diagrama de Estado de Firma Electrónica

3.2.8. Diagrama de Despliegue

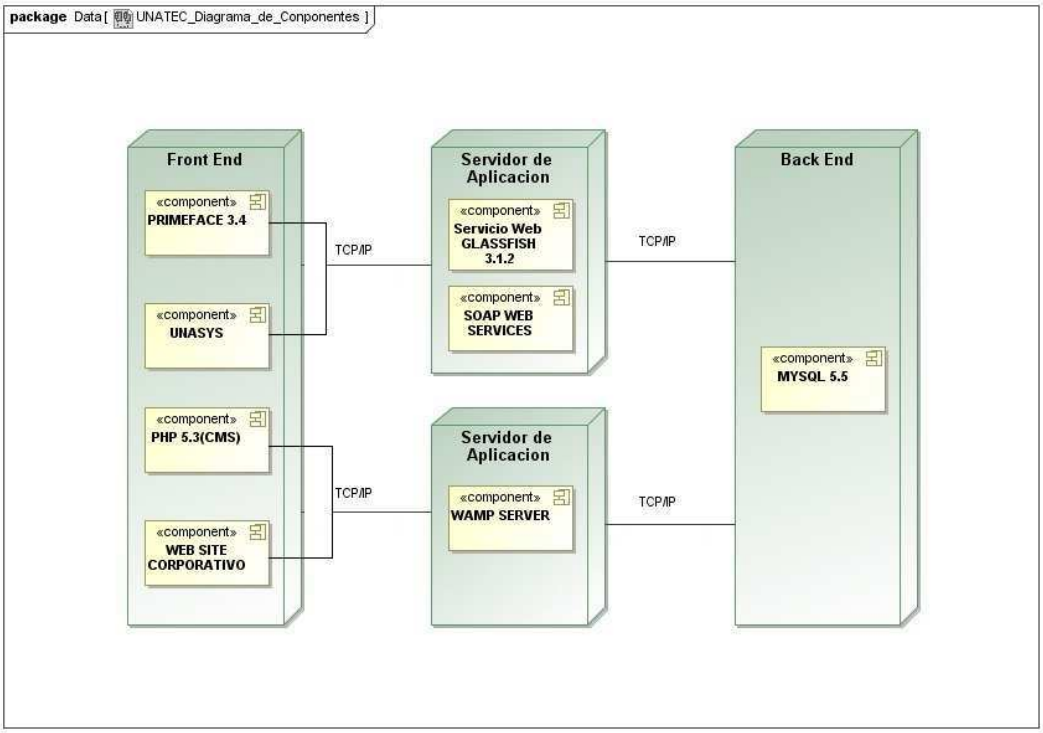


Figura3.36: Diagrama de Despliegue

3.2.9. Diagrama de Implementación

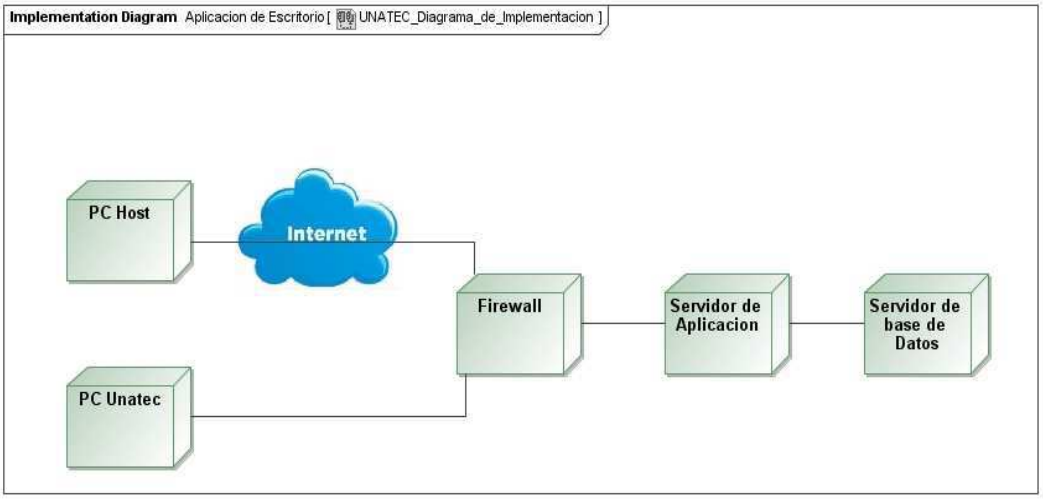


Figura 3.37: Diagrama de Implementación

3.2.10. Diagrama de Paquetes

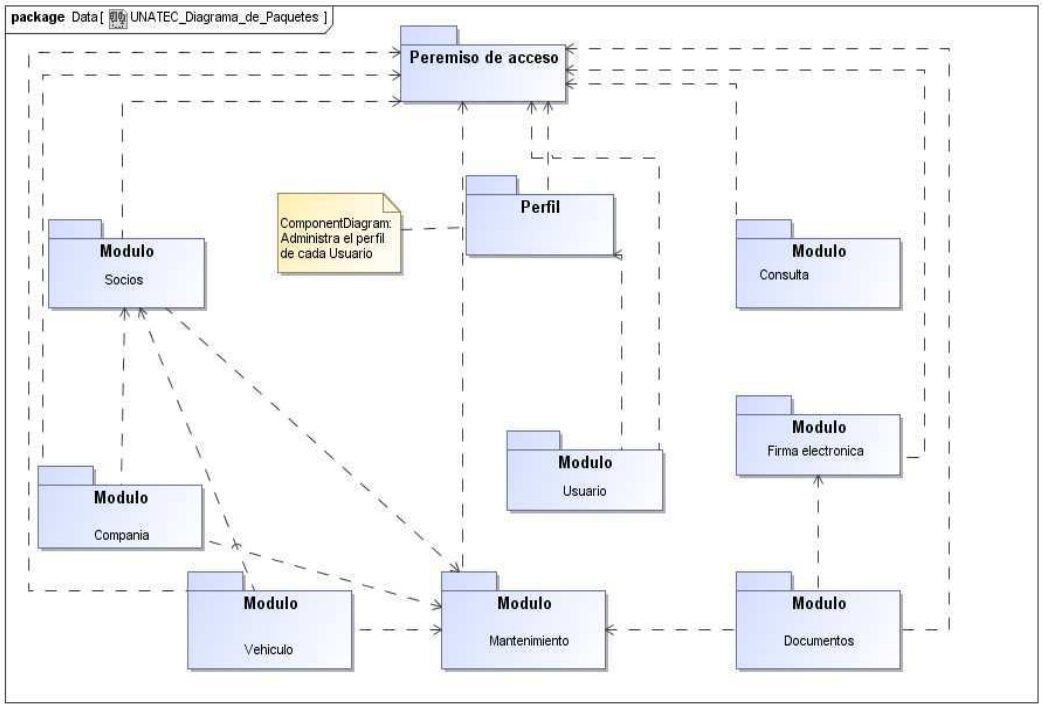


Figura 3.38 Diagrama de Paquetes

CAPÍTULO 4

IMPLEMENTACIÓN Y PRUEBAS

4.1. Levantamiento de infraestructura

4.1.1. Herramientas y aplicaciones requeridas

Para la implementación del proyecto es necesario tener a disponibilidad las herramientas y aplicaciones enumeradas a continuación:

- .Net Framework 4.0 (Necesario para instalar MySql, SafeNet, etc).
- SafeNetClientAuthentication: Aplicación que posee el driver del eTokenAladdin.
- IntiSign: Aplicación para firmar documentos PDF utilizando un certificado digital.
- XolidoSign: Aplicación para firmar documentos PDF con TimeStamp gratuitamente utilizando un certificado digital.
- MySql 5.5: Motor de Base de datos con el que trabaja la aplicación.
- SqlYog Enterprise: Gestor Intuitivo para MySql.
- JDK 1.7: Paquete de desarrollo de Java, necesario para la instalación de NetBeans 7.2
- NetBeans 7.2: IDE de desarrollo para aplicaciones utilizando tecnología JEE6
- GlassFish 3.1.2(Incluido con NetBeans): Servidor de aplicaciones Web
- PrimeFaces 3.4: Framework que simplifica el desarrollo de interfaces Web utiliza tecnología JSF para el despliegue de páginas web.
- Itext 5.4: Librería que permite procesar ficheros PDF, y extraer firmas incrustadas.

- BouncyCastle 1.48: Librerías Open Source para lectura y procesamiento de certificados Digitales x.509
- WampServer: Plataforma de desarrollo web que permite utilizar Apache, Php y MySql para crear aplicaciones web dinámicas.
- Joomla 1.5: Permite construir sitios web y gestionar contenidos.
- Certificados de AC Raíz y AC subordinada: Certificados de cadena de confianza que otorga la AC.

4.1.2. Instalación de .Net Framework 4.0

La instalación del framework versión 4.0 permitirá la posterior instalación de las aplicaciones, MySql (Motor de Base de Datos), IntiSign (Firma de documentos PDF), y SafeNet(Driver Token-Hardware), por lo que se procede a ejecutar el instalador versión completa en el ordenador.

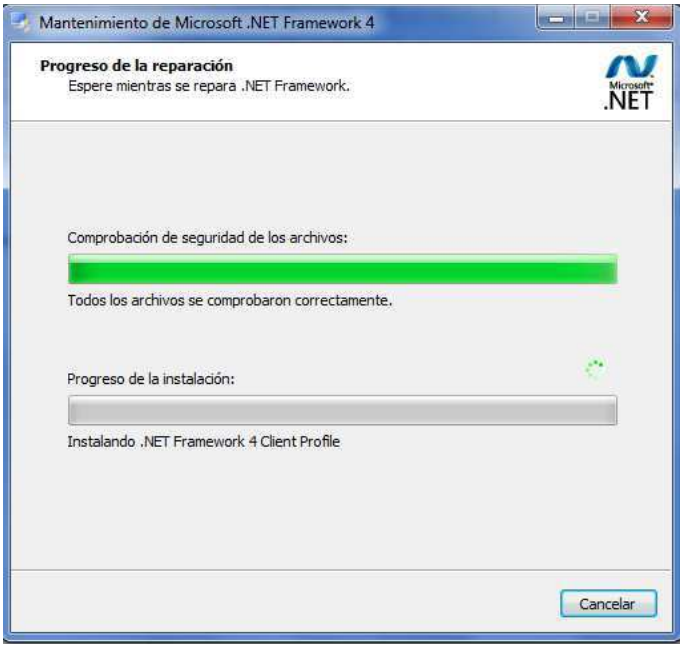


Figura 4.1.2.1 Instalación .Net Framework 4.0

Al ejecutar el instalador se acepta los términos y condiciones de uso y se continúa con la instalación sin ningún tipo de parametrización adicional.

Al finalizar la instalación es necesario reiniciar el equipo para efectuar nuevos cambios en el equipo.

Con la instalación del Framework, se puede continuar con la instalación del resto de aplicaciones sin ninguna restricción.

4.1.3. Instalación de Safe Net AuthenticationClient

La instalación de SafeNet es sencilla y rápida, se procede con ejecutar el instalador, de igual forma se aceptan los términos y condiciones de uso.

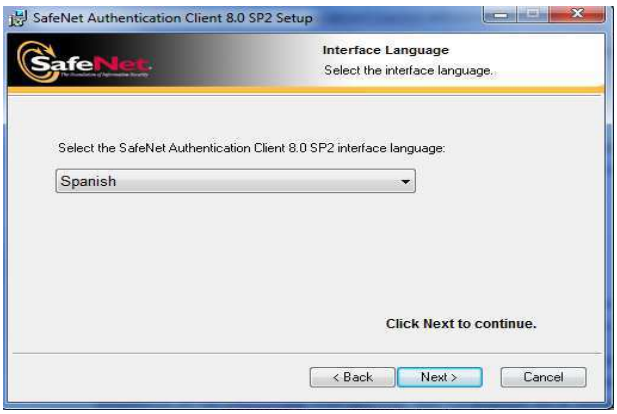


Figura 4.1.3.1 Instalación SafeNet #1

Se selecciona el idioma deseado y se procede con la instalación. SafeNet es necesario por los drivers del dispositivo eToken que otorga el Banco Central del Ecuador, una vez instalado se pueden verificar los datos del contenedor Token.

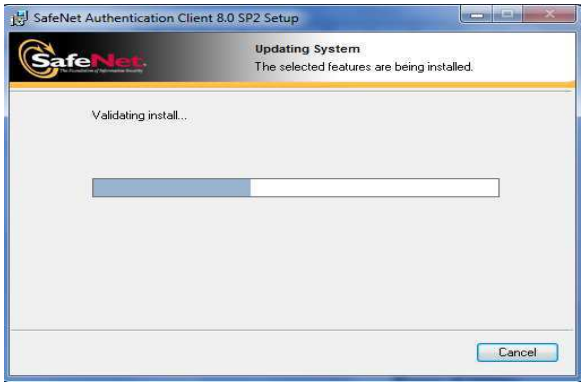


Figura 4.1.3.2 Instalación SafeNet #2

Tomar en cuenta que los navegadores no deben estar abiertos para la instalación para continuar sin problemas. Una vez Finalizada la instalación se acepta y se tieneSafeNet listo para detectar los dispositivos eToken.

4.1.4. Instalación de Aplicaciones para firma de documentos

4.1.4.1. Instalación de IntiSign del Banco Central del Ecuador

El Banco Central del Ecuador pone a disposición esta herramienta para el firmado de documentos, la misma que se encarga de verificar la vigencia del certificado, y la revocación, es decir, revisa las CRL para garantizar que un certificado no haya sido revocado y así continuar con el proceso de firma de documentos.

Se ejecuta el instalador de Intisign y de igual forma se acepta los términos y condiciones de uso y se procede con la instalación.

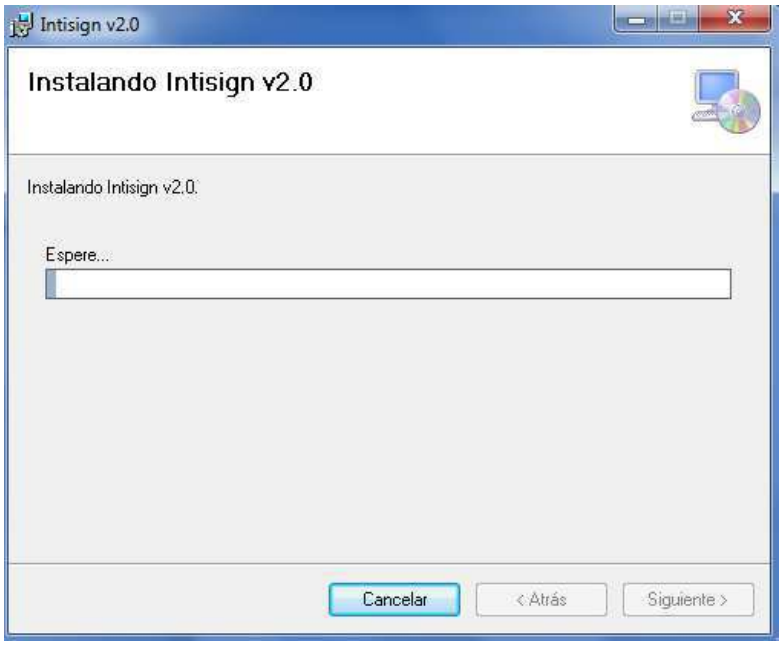


Figura 4.1.4.1 Instalación de IntiSign

No es necesario ningún tipo de parametrización adicional para el aplicativo, solamente se debe haber instalado previamente el .Net Framework 4.0 para concluir la instalación.

Con IntiSign instalado es posible firmar ficheros PDF utilizando el certificado digital en un contenedor de archivo o token.

4.1.4.2. Instalación de XolidoSign.

Existen varias herramientas que permiten el firmado de documentos, pero XolidoSign destaca entre otras por su servicio gratuito de TimeStamp, XolidoSign es una herramienta completa que permite incrustar en la firma digital un sello de tiempo, el mismo que es soportado y visualizado únicamente por versiones de Adobe Reader X o superior.

Se ejecuta el instalador de XolidoSign y se empieza con el proceso de instalación.

Figura 4.1.4.2.1 Instalación de XolidoSign #1

Se selecciona el idioma que se desea para XolidoSign y se continúa con la aceptación del acuerdo de licencia y condiciones de uso.

Figura 4.1.4.2.2 Instalación de XolidoSign #2

Se selecciona la ruta de ubicación y se continúa con la instalación.

Figura 4.1.4.2.3 Instalación de XolidoSign #3

Al finalizar la instalación se dispone de una poderosa herramienta de firma de documentos, y posiblemente la mejor que se encuentra disponible con licencia gratuita.

4.1.5. Instalación y configuración de MySql 5.5

Se inicia ejecutando el instalador de MySql 5.5 de licencia gratuita.

Figura 4.1.5.1 Inicio de Instalación de MySql

Ahora se continúa instalando los productos de MySql, necesarios para el levantamiento de la Base de datos.

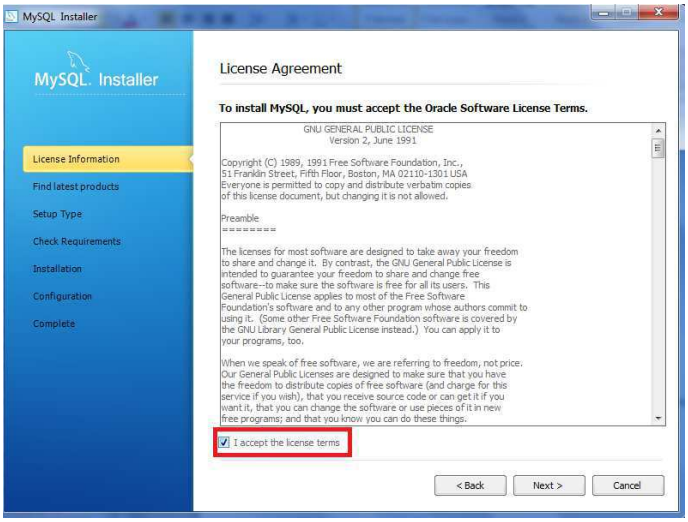


Figura 4.1.5.2 Acuerdo de términos de licencia.

Se acepta los términos de licencia que plantea Oracle para el uso de MySql, y se continúa con la instalación.

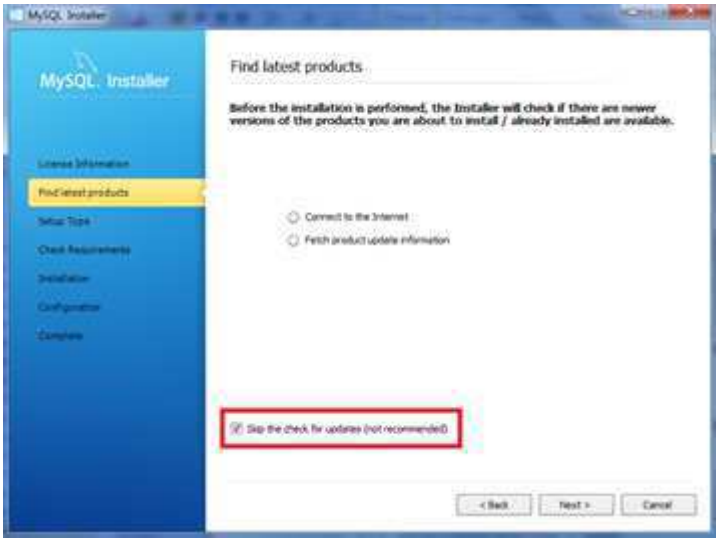


Figura 4.1.5.3 Verificar Actualizaciones de MySql

Se puede omitir la verificación de actualizaciones, ya que no afecta al proceso de levantamiento de la base de datos.

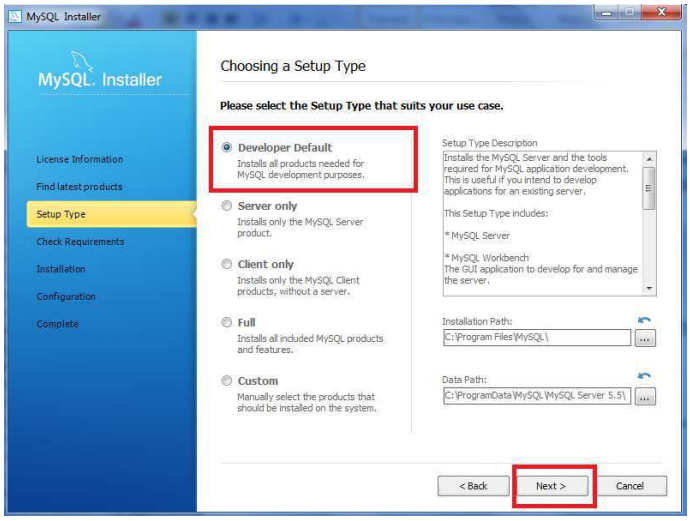


Figura 4.1.5.4 Tipo de Instancia de MySql

Dependiendo del equipo o del tipo de uso que se vaya a aplicar a la base de datos, se selecciona la instancia.Para efectos del levantamiento del proyecto se seleccionará la instancia **Developer Default** y se continúa con la instalación.

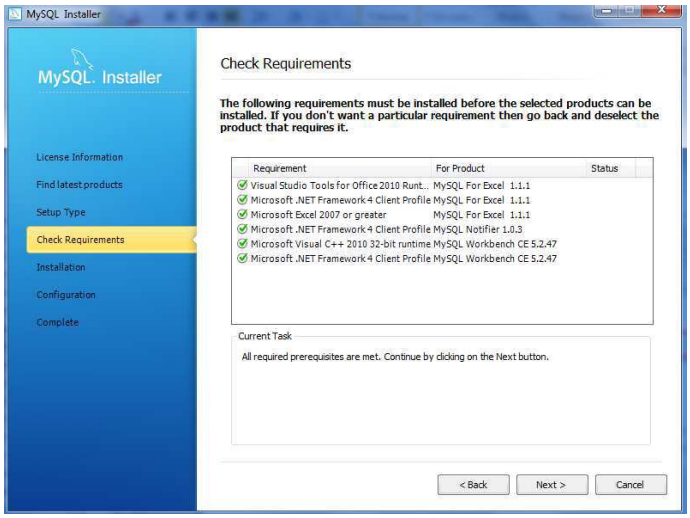


Figura 4.1.5.5 Plugins y paquetes adicionales de MySql

A continuación de desplegar la lista de paquetes que se instalarán junto con MySql. La instalación de estos paquetes adicionales no afecta el proceso de implementación.

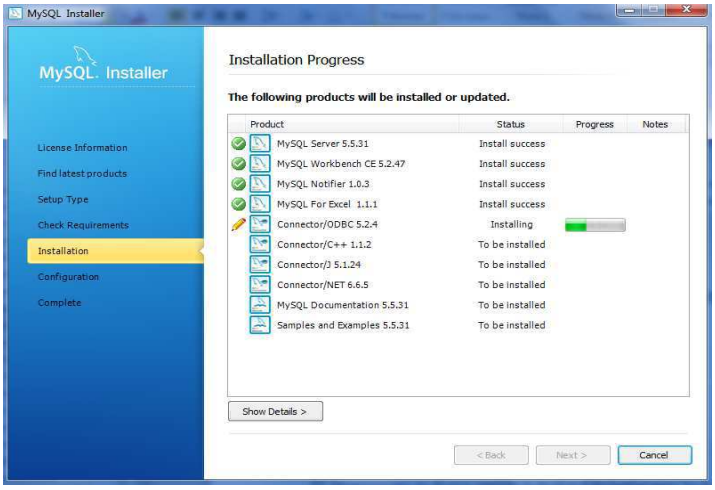


Figura 4.1.5.6 Instalación de productos MySql

Una vez concluido todo el proceso anterior se empieza la instalación de productos MySql, entre los cuales se cuenta con el conector jdbc que permitirá la conexión entre la aplicación web de firma electrónica y la base de datos.

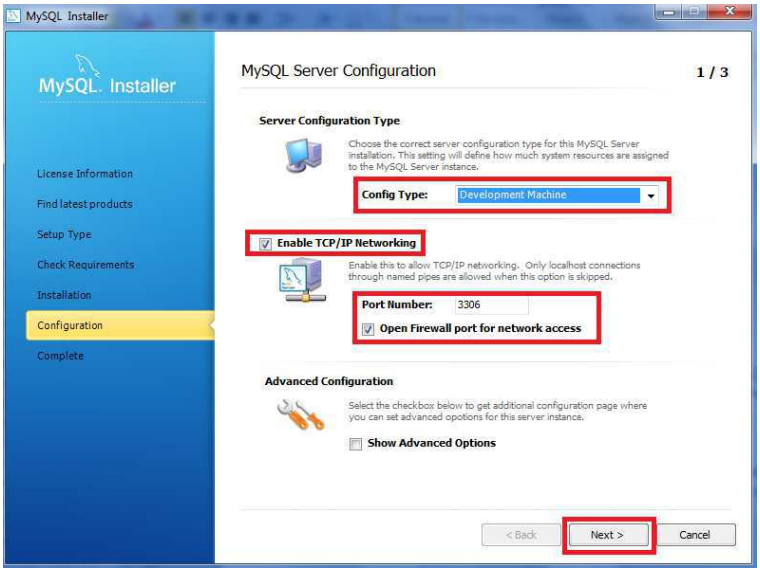


Figura 4.1.5.7 Configuración del Servidor MySql

Se configura el tipo de servidor como **Development Machine,**se habilita la opción de **TCP/IP Networking** para permitir conexiones remotas y no solo a nivel de localhost, se configura el puerto escucha del servidor a 3306 que es el puerto por defecto.

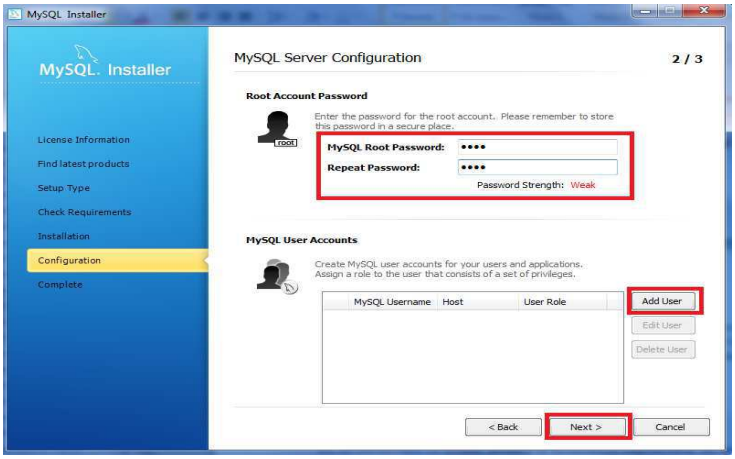


Figura 4.1.5.8 Configuración de User y Password

Primero se define la contraseña que tendrá el super-usuario (root), para este caso se ha definido la contraseña como “espe” para el usuario root, de ser necesario se pueden crear nuevos usuarios con la opción **AddUser**en caso de requerirlo, pero se mantendrá para efectos de la implementación la contraseña para root como “espe”. Al terminar el proceso del levantamiento de infraestructura se puede restablecer las contraseñas a las que se desea.

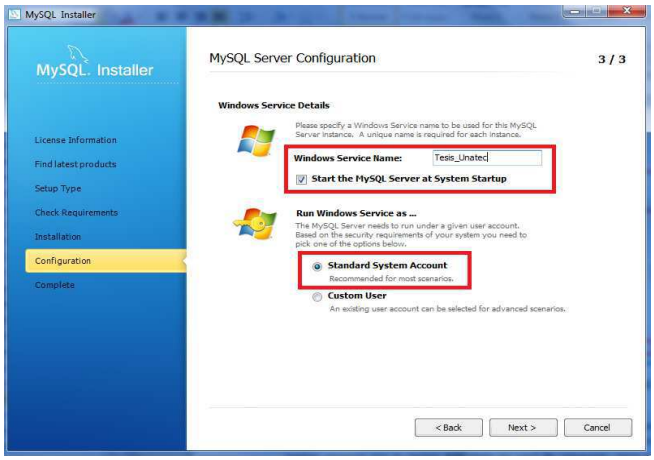


Figura 4.1.5.9 Configuración de Servicio de MySql

MySql brinda la opción de instanciar la base de datos como un servicio, y que se inicie como una tarea del sistema operativo, se asigna un nombre a este servicio de MySqly se mantiene la opción **Standard SystemAccount** activa que es compatible con la mayoría de escenarios en Windows.

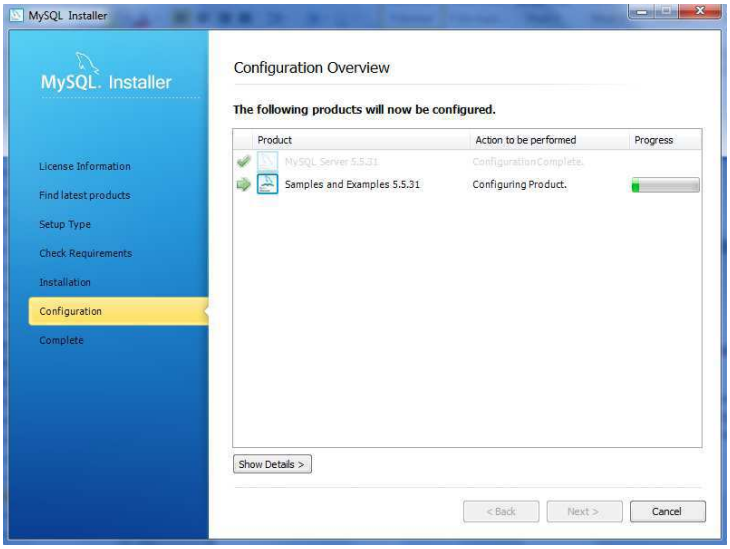


Figura 4.1.5.10 Proceso de configuración automático

Una vez concluida la paremetrización de la base de datos, el instalador comienza a implementar la instancia en base a los parámetros entregados.

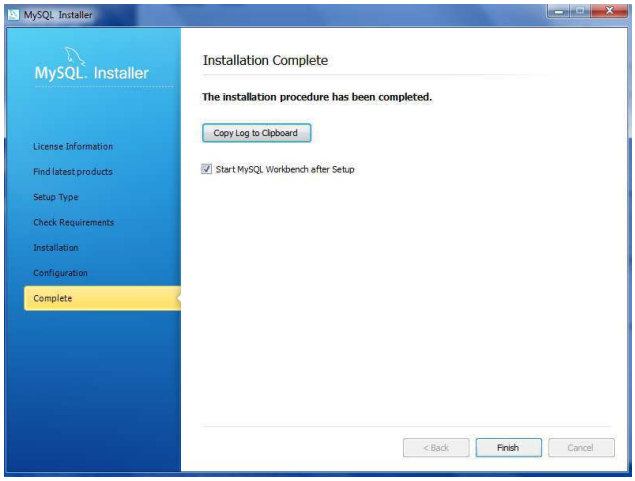


Figura 4.1.5.11 Finalización de Instalación de MySql

Finalmente el asistente de instalación indica que la instalación se ha completado correctamente. Ahora se tiene a MySql listo para operar y para levantar la estructura de datos de la aplicación.

4.1.6. Instalación del Gestor de MySql

Para gestionar los recursos de bases de datos se utilizó SqlYog Enterprise, una herramienta intuitiva y fácil de utilizar. Se inicia la instalación corriendo el instalador de la aplicación.

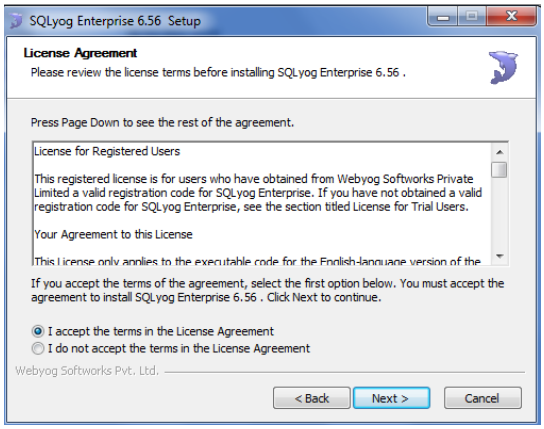


Figura 4.1.6.1 Instalación de SqlYog Enterprise #1

El proceso de instalación es sencillo, se empieza aceptando los términos de licencia para continuar con la instalación.

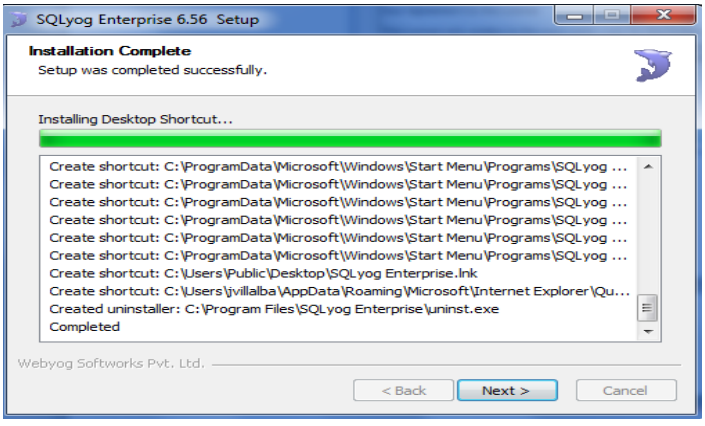


Figura 4.1.6.2 Instalación de SqlYog Enterprise #2

Al terminar la instalación, se ejecuta la aplicación y la misma solicitará el ingreso del código serial de activación, se ejecuta el archivo con nombre serial.txt que viene junto al paquete de instalación y se procede a activar el gestor de MySql.

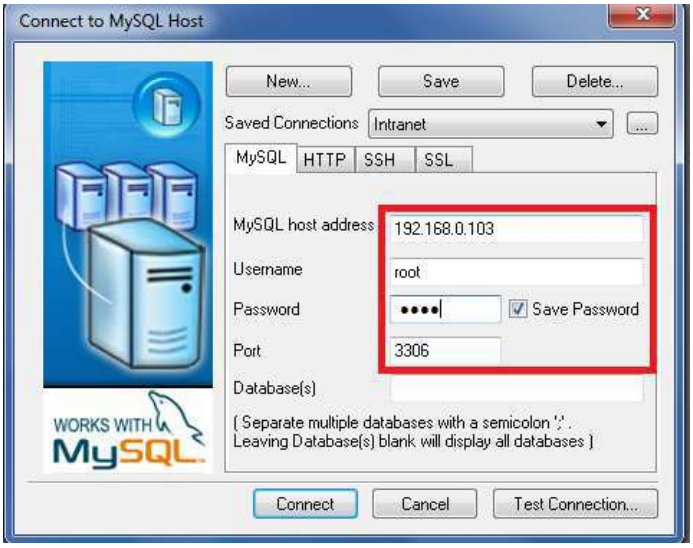


Figura 4.1.6.3 Configuración de SqlYog

Al activar el producto se procede a configurarlo para enlazarlo a la instancia de MySql previamente configurada, para ello se define el **MySql Host Address**que es la Ip del equipo o servidor en donde está instalada la instancia de MySql, en caso de que sea local, entonces se define el **host address** como localhost. Se ingresan las credenciales **Username**, **Password**y **Port** configurados anteriormente en la instalación de MySql. Para verificar la conexión, hacerclic en **Test Connection** y si todo se encuentra correctamente entonces la prueba será exitosa y se podrá ingresar a la instancia.

4.1.7. Instalación de JDK y configuración Netbeans (IDE)

Para el desarrollo de la aplicación se utilizó NetBeans 7.2 de Oracle, es necesario descargar e instalar el JDK antes de iniciar con la instalación del IDE. Se procede a ejecutar el instalador del JDK 1.7 incluido en los paquetes de instalación.

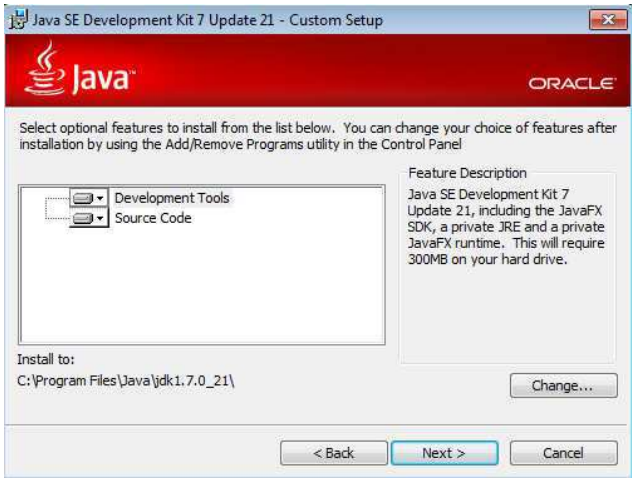


Figura 4.1.7.1 Instalación JDK 1.7

Se seleccionan todas las características disponibles del Jdk y se continúa hasta finalizar la instalación.

Al finalizar se puede iniciar el asistente de instalación de NetBeans sin restricciones.

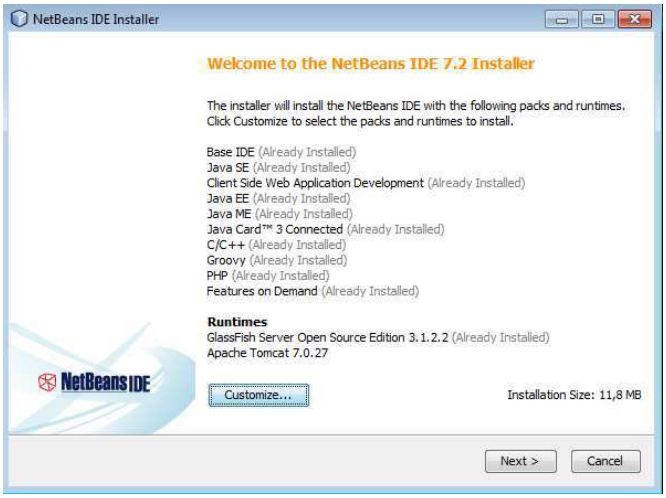


Figura 4.1.7.2 Instalación de Netbeans #1

La instalación se la realiza seleccionando todos los paquetes java y el servidor Web GlassFish que se instala junto con NetBeans, se debe configurar en caso de ser solicitado el usuario y el password para entrar a la página de administración de la consola de GlassFish, por defecto el usuario es “admin” y la

clave “adminadmin” en el puerto escucha 4848, se mantiene con la configuración por defecto y se continúa con la instalación de los paquetes.

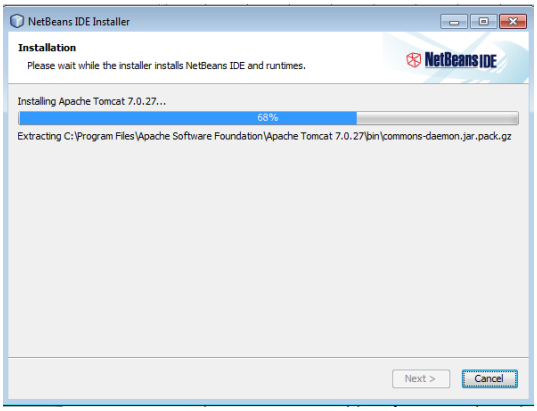


Figura 4.1.7.3 Instalación de Netbeans #2

Al terminar la instalación se habrá instalado Netbeans 7.2 con los paquetes java y con el servidor web GlassFish que alojará a la aplicación.

Ahora se copia el proyecto proporcionado **UnatecSoftWS**en la carpeta de proyectos de NetBeans**C:\Users\Usuario\Documents\NetBeansProjects,** se ejecutaNetBeans y se instancia el proyecto.

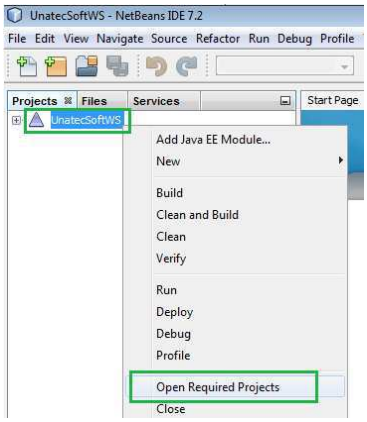


Figura 4.1.7.4 Proyectos Requeridos

Ahora clic derecho en el Enterprise Web Application y se abren los proyectos requeridos para que opere la aplicación.

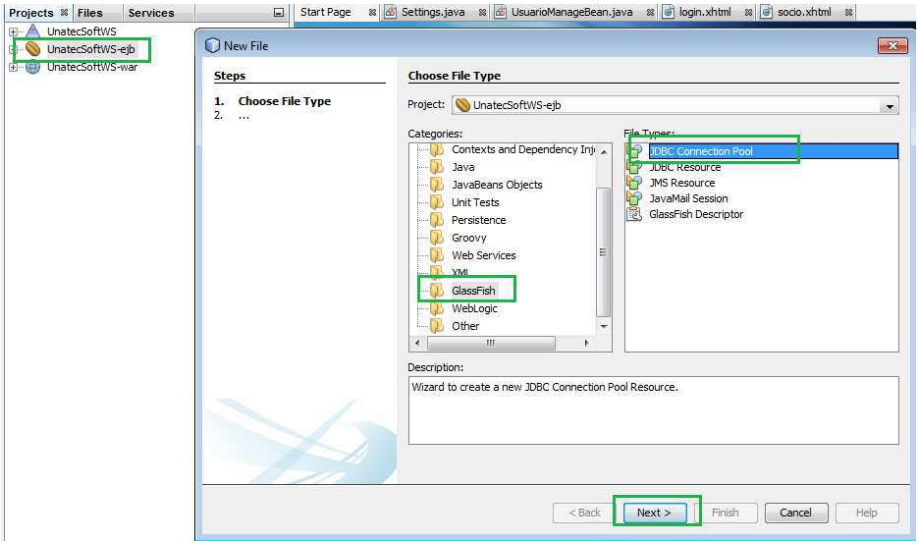


Figura 4.1.7.5 Nuevo JDBC Connection Pool

Hacerclic derecho en el proyecto EJB ->**New** ->**Others** y se selecciona la categoría **GlassFish** - >tipo de archivo **JDBC Connection Pool**

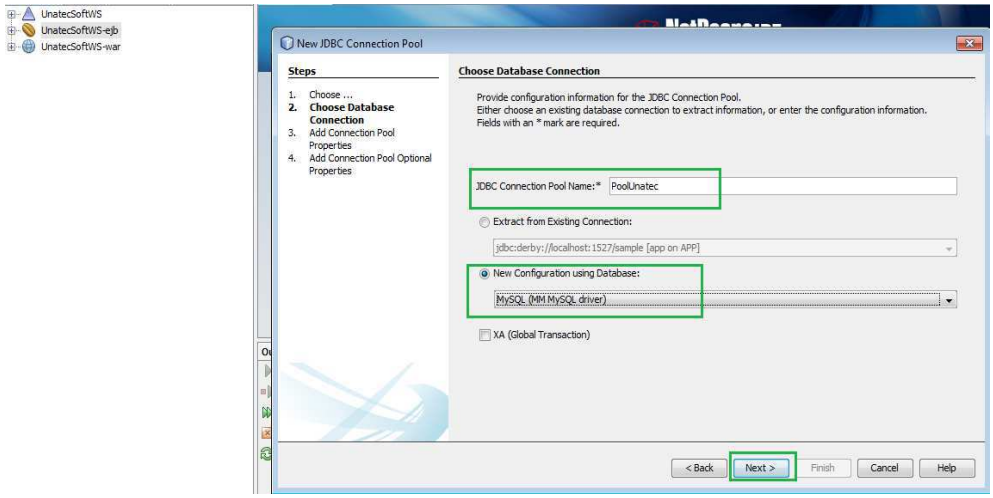


Figura 4.1.7.6 Configurar Pool de Conexión

Se escribe el nombre del pool y se selecciona la base de datos a la que a parametrizar la conexión.

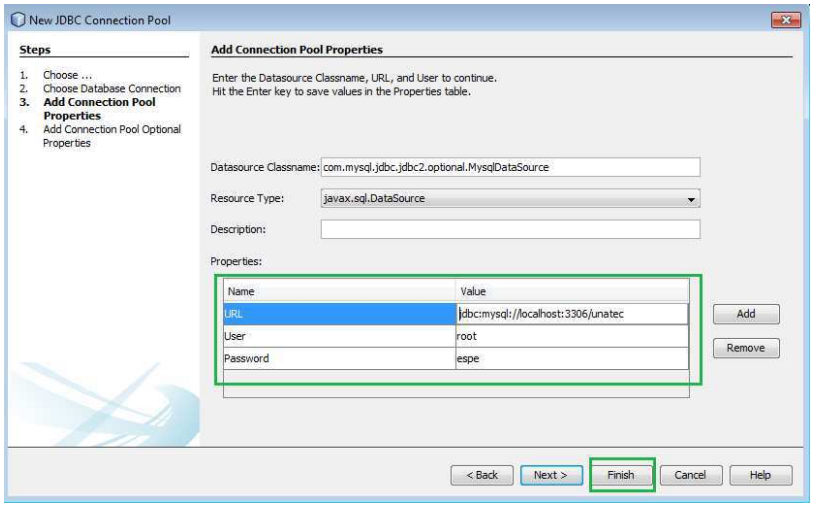


Figura 4.1.7.7 Parametrización de Pool de Conexión

Ahora se llenan los parámetros solicitados con las credenciales de la base de datos, la misma que tiene por nombre definido **unatec,** Se ingresan el usuario y la clave previamente configurados en la instancia de MySql y se finaliza el asistente para crear el pool de conexión.

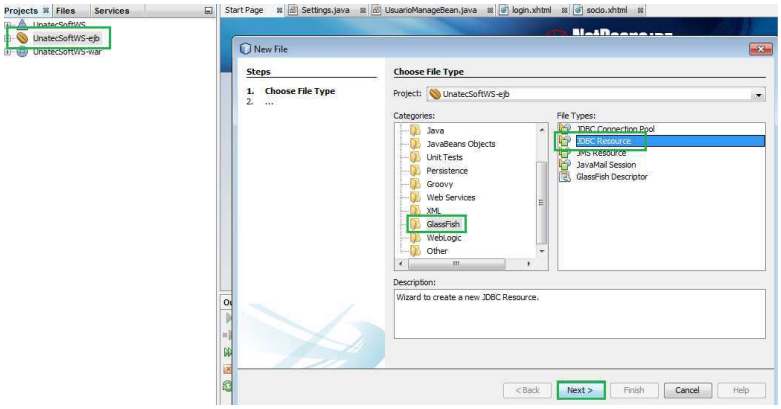


Figura 4.1.7.8 Nuevo JDBC Resource

Hacer clic derecho en el proyecto EJB ->**New** ->**Others** y se selecciona la categoría **GlassFish**-> tipo de archivo **JDBC Resource.**

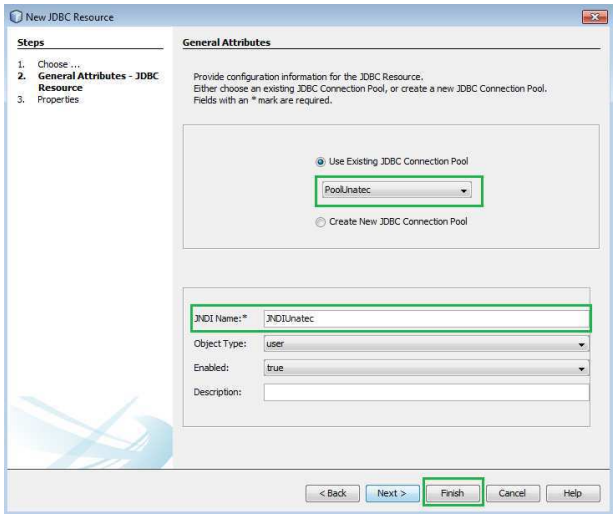


Figura 4.1.7.9 Configuración JDBC Resource

Para configurar el recurso, se selecciona el pool de conexión que se creó en el paso anterior y se coloca el nombre del JNDI definido como **JNDIUnatec,** el nombre tiene que ser tal cual está escrito, ya que el código realiza la conexión de la base de datos mediante este nombre del recurso.

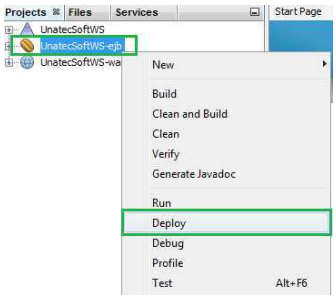


Figura 4.1.7.10 Desplegar EJB

El proyecto EJB contiene las clases entidades y la lógica de negocio, en la que se encuentran programados los servicios web que interactúan con la capa de presentación del proyecto.

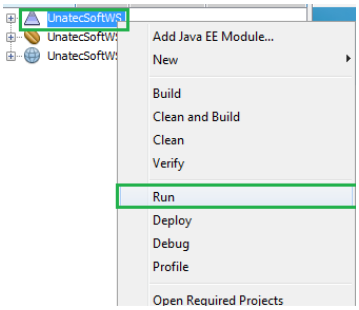


Figura 4.1.7.11 Ejecución del Enterprise Java Web Application

Ahora con el EJB desplegado en el servidor Web, se puede ejecutar el proyecto y empezar a utilizar la aplicación Web, la página inicial será el Login.jsf en la que se podrá iniciar la sesión con el usuario y la contraseña definidas como "admin".

4.1.8. Instalación de WampServer

Se ejecuta el paquete de instalación de Wampserver 2.2 que instalará Apache y PHP. MySql también es parte del paquete pero al tenerlo ya instalado en el equipo, no se instalará por segunda vez.

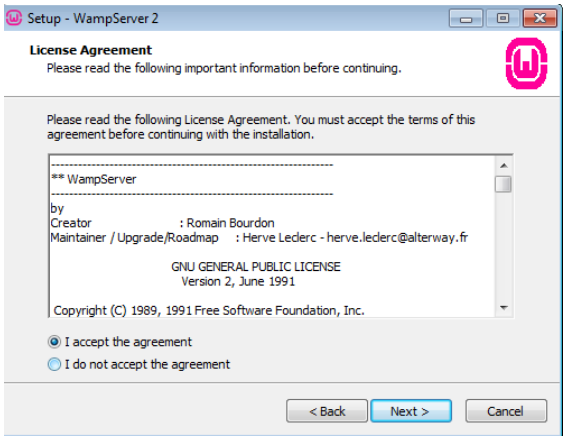


Figura 4.1.8.1 Instalación de Wampserver

Se acepta los términos de acuerdo de licencia y se continúa con la instalación. Ahora con Wampserver instalado se procede a ejecutarlo, en la barra de tareas aparecerá el icono de la aplicación, al hacer clic se podrá gestionar sus

herramientas, como son detener y reiniciar los servicios. Para que el servidor sea visible se va a configurar el archivo httpd.conf.

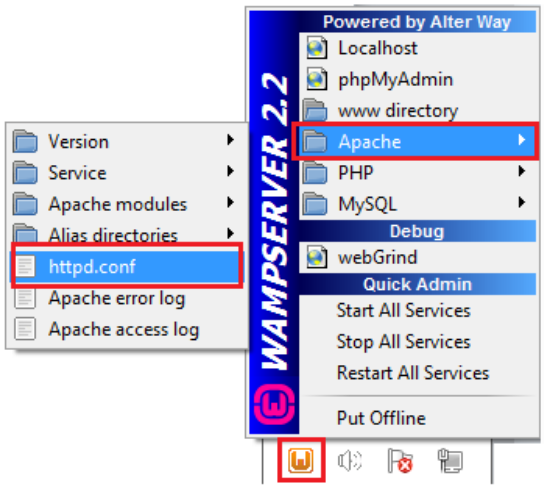


Figura 4.1.8.2 Gestionar WampServer 2.2

El icono de wampserver desplegará un menú de administración, el objetivo es configurar el archivo httpd.conf para dar permisos de acceso a los servicios del servidor.

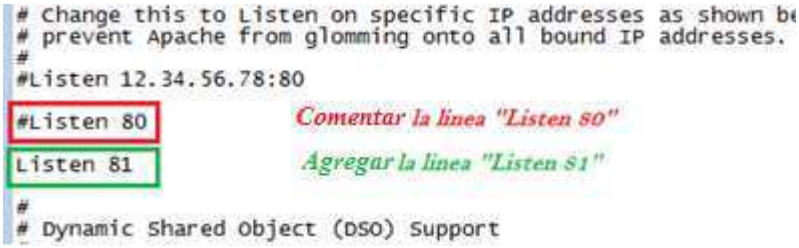


Figura 4.1.8.3 Configuración Apache #1

Se debe comentar la línea “Listen 80” que es el puerto escucha predeterminado de apache y agregar la línea Listen 81, esta configuración tiene como objetivo implementar el hosting In-House.

```
# "C:/Program Files/Apache Software Foundation/Apache
# CGI directory exists, if you have that configured.
#
<Directory "cgi-bin">
    AllowOverride None
    Options None
    Order allow,deny
    #Allow from None
    Allow from all
</Directory>

#
```

Comentar línea, otorga permiso solo a localhost

Agregar línea, otorga permisos de acceso

Figura 4.1.8.4 Garantizar permisos de acceso

Se busca y se reemplazan las líneas de la figura 4.1.8.4 para otorgar permisos, caso contrario únicamente el localhost puede acceder, con esta configuración otros equipos de la red pueden visualizar los servicios de Apache.

4.1.9. Instalación y configuración de Joomla

Para la instalación de Joomla es necesario tener previamente instalado wampserver, el primer paso es ir a la ubicación C:\Wamp\www y crear una nueva carpeta con el nombre que se desea, en este caso se hará con el nombre **Intranet**, ahora se descomprime el archivo **Joomla_Instalador.zip** en la nueva carpeta creada.

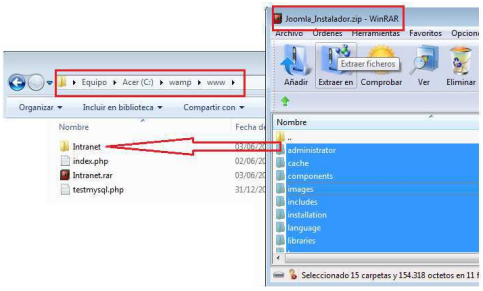


Figura 4.1.9.1 Instalación Joomla

Al ingresar a la ruta, lo primero que se ejecuta es el instalador del joomla, el cual se compone de 7 pasos, el primero es la elección del idioma, para el cual se seleccionará:**es-ES - Spanish (Español internacional)** y se pulsa siguiente.

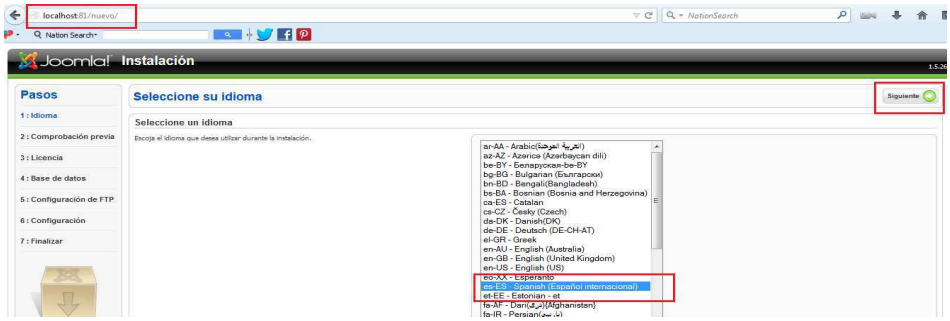


Figura 4.1.9.2 Selección de Idioma

Joomla comprobará que todos los requisitos necesarios estén completos, si todos los requerimientos se cumplen, no aparecerá ninguna notificación en rojo en la parte derecha de cada requerimiento.

Figura 4.1.9.3 Comprobación de requisitos

Normalmente se debe tener en cuenta los valores recomendados que se muestran en la parte inferior, sin embargo, si alguno de estos se encuentra en rojo el instalador permitirá continuar con la instalación ya que no son obligatorios.

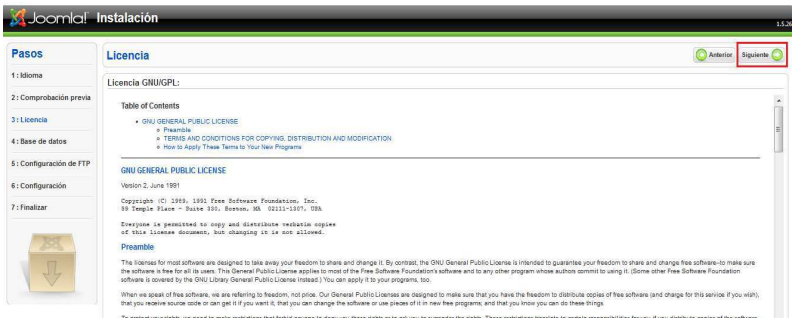


Figura 4.1.9.4 Aprobación de Licencia Joomla

Joomla cuenta con una licencia pública general la cual es aceptada en el momento que se da clic en el botón siguiente.

En el siguiente paso se debe poner los valores para la conexión a la base de datos ya creada.

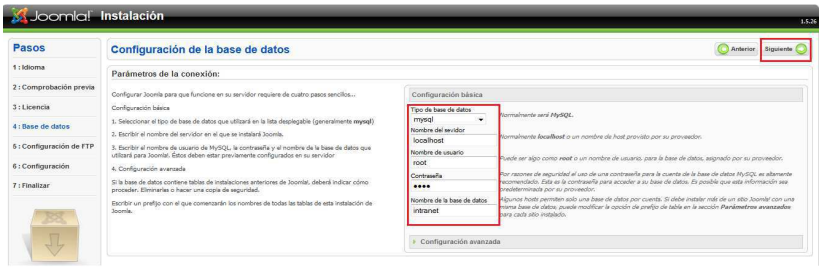


Figura 4.1.9.5 Conexión a MySql

Tipo de base de datos: **mySql**

Nombre del servidor: **localhost**

Nombre de usuario: **root**

Contraseña: **“espe”**

Nombre de base de datos: **Intranet**

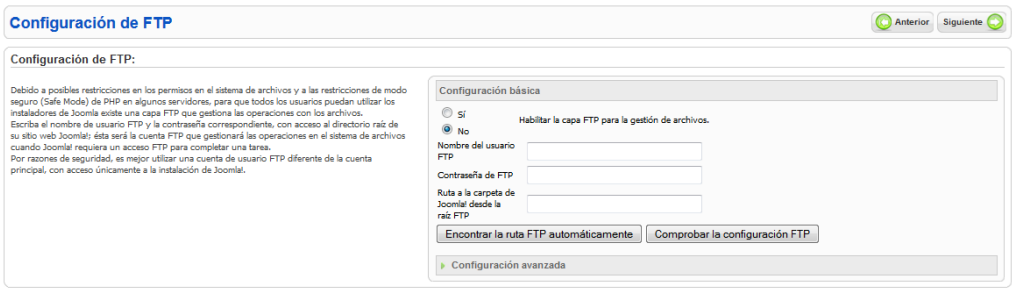


Figura 4.1.9.6 Configuración FTP

La configuración FTP es una opción que se mantiene **deshabilitada** y se continúa normalmente con la instalación.

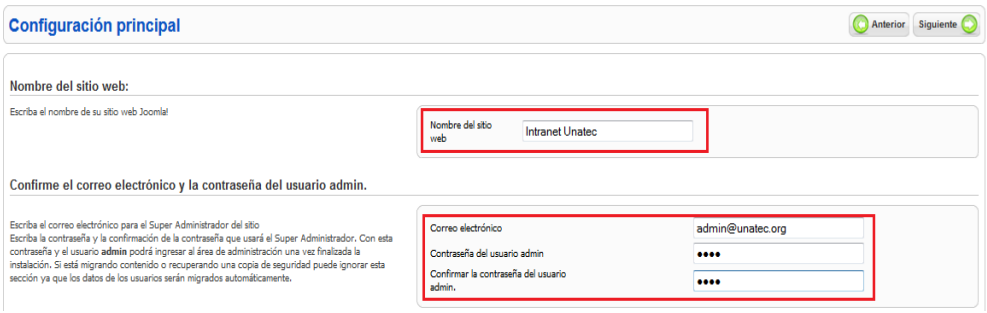


Figura 4.1.9.7 Configuración de Email y Contraseña

Se continúa con la configuración de nombre del sitio web y de correo electrónico, se utiliza el dominio unatec.org adquirido en el correo, en la contraseña en este caso será “espe”

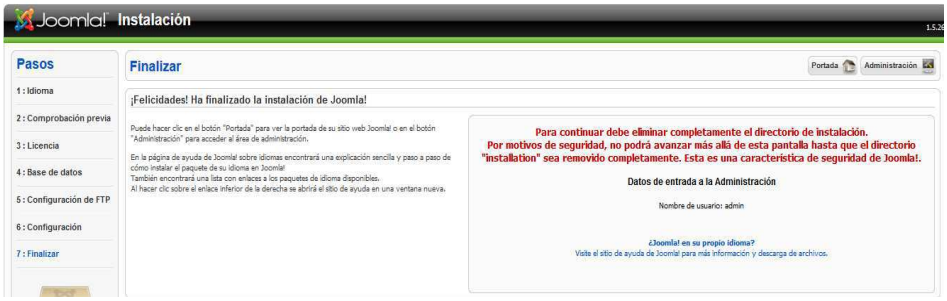


Figura 4.1.9.8 Finalización de Instalación de Joomla

En este último paso, el instalador de Joomla indica que la instalación termino correctamente, sin embargo se tiene que ir al directorio del proyecto **C:\wamp\www\Intranet** y elimina la carpeta llamada **installation** para que permita acceder a la administración del sitio.

Para acceder al sitio se tiene que escribir en la barra de direcciones del browser **http://localhost:81/Intranet**

Para acceder al administrador del sitio se debe ir a la url**http://localhost:81/Intranet/administrator** y acceder con los datos de usuario y contraseña parametrizados.

Nota: Esta versión de joomla deja por defecto el usuario **admin** y la contraseña es la proporcionada en la Figura 4.1.9.7

Figura 4.1.9.9 Inicio de Sesión en Joomla

Ahora para levantar Joomla con las plantillas configuradas, se debe seleccionar la carpeta **Intranet** que viene con los paquetes de instalación proporcionados, se copia y se reemplaza la carpeta **templates**en la carpeta **C:\wamp\www\Intranet.**

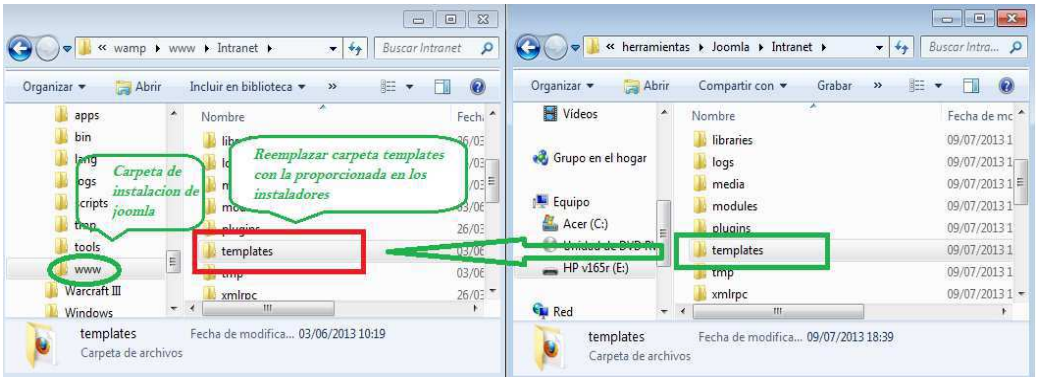


Figura 4.1.9.10 Instalación de Plantillas

Al instalar las plantillas se puede visualizar la página inicial de Joomla, en la que se podrá gestionar contenidos, artículos, etc, es el web site corporativo de la Unión Nacional de Taxi Ejecutivo Comercial que permitirá a la organización dar a conocer de sus servicios.

Ahora se carga el script proporcionado utilizando SQLYog, para ello se inicia la aplicación, y se inserta las credenciales para acceder a la instancia de MySql.

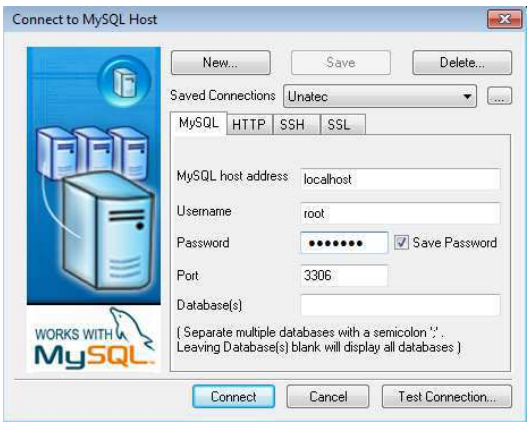


Figura 4.1.9.11 Conexión a MySql

Iniciada la sesión a MySqlse puede administrar la base de datos y cargar los script proporcionados para el levantamiento de la aplicación.

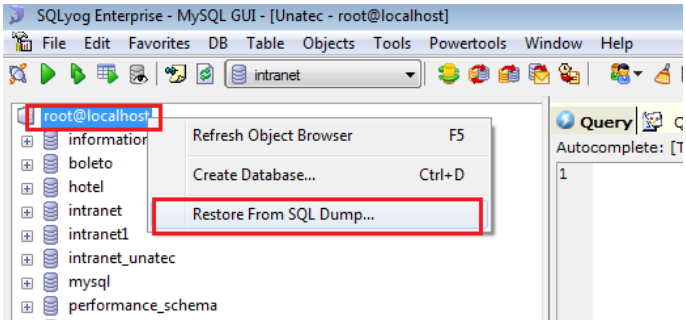


Figura 4.1.9.12 Restaurar Base de datos

Para restaurar, hacer clic derecho en la instancia (root@localhost) y se selecciona la opción **RestoreFrom SQL Dump**

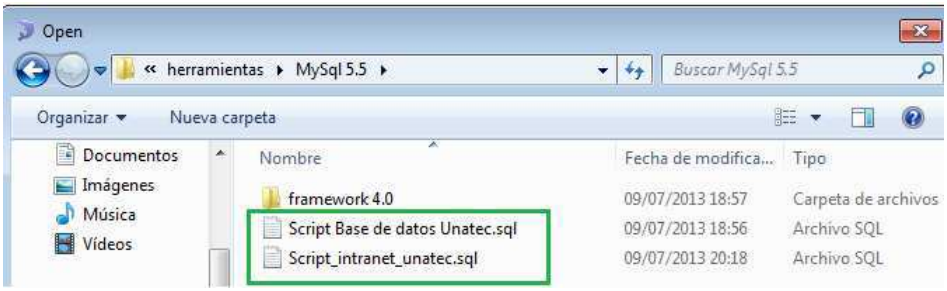


Figura 4.1.9.13 Selección de Scripts

Se cargan los 2 archivos proporcionados para levantar las bases de datos que utiliza la aplicación.

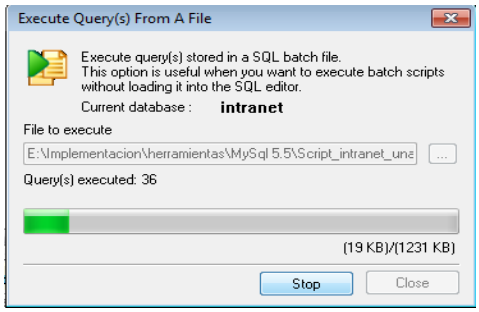


Figura 4.1.9.14 Ejecución de Scripts SQL

Al terminar el proceso de carga, se tienen preparadas las bases de datos de la aplicación Web de firma electrónica como del Web Site Corporativo.

Figura 4.1.9.11 Página de Inicio de UNATEC

Al ingresar la dirección http://localhost:81/Intranet/se visualiza el home de Unatec y para clientes externos se debe utilizar la dirección http://www.unatec.org:3389/Intranet, que es la dirección disponible en la web.

4.1.10. Levantamiento de Hosting In-House

El levantamiento In-House, permite la facilidad de implementar las herramientas en la infraestructura que dispone la empresa, organización, individuo.

La ventaja radica en la total independencia del levantamiento, sin embargo, el tiempo del levantamiento se ve retrasado por el mismo hecho de este levantamiento, a diferencia de un Outsoursing web hosting, que ya dispone de la infraestructura necesaria y disminuye el tiempo de implementación, con el fin de ahorrar recursos económicos y de demostrar la factibilidad de un levantamiento independiente se optó por el hosting in House, que permite al dueño o responsable o de su pequeña empresa administrar a voluntad sus recursos.

4.1.10.1. Adquisición y configuración de Dominio

Para el levantamiento es necesario adquirir y configurar un dominio que sea visible en la Web, la compra del dominio se la gestionó con www.godaddy.com.

Figura 4.1.10.1 Disponibilidad del Dominio en GoDaddy.com

Si el dominio está disponible entonces se procede a comprarlo con las condiciones de uso del dominio y con la forma de pago más conveniente, GoDaddy ofrece servicios adiciones como web hosting o correo electrónico, pero ara efecto e implementación de este proyecto solo se adquirirá el dominio.

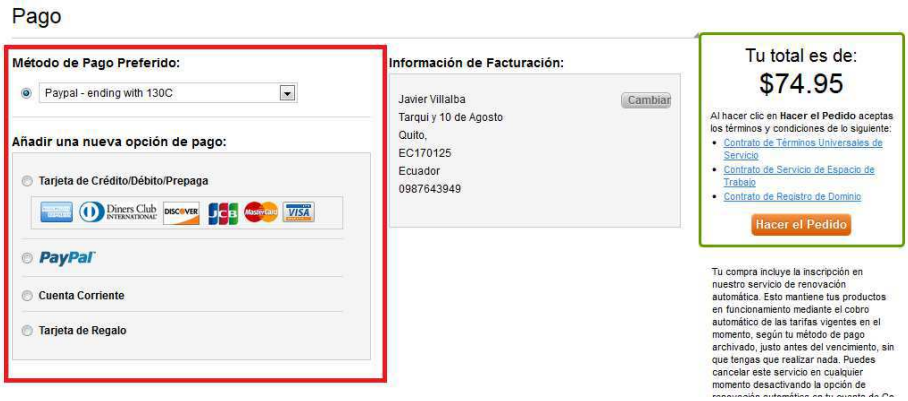


Figura 4.1.10.2 Pago de Dominio

Se selecciona la forma de pago más conveniente y se tiene el dominio www.unatec.org disponible por 1 año, al realizar la compra,GoDaddysolicitará los datos para crear una cuenta de acceso para poder acceder a la administración del dominio.

Figura 4.1.10.3 Menú de Administración de dominio

Al terminar el pago y recibir la confirmación por correo, se procede a ingresar a la cuenta que se creó enGoDaddy y se selecciona en el menú **Todos los Productos,** se dirige a la opción **Gestión de Dominio.**

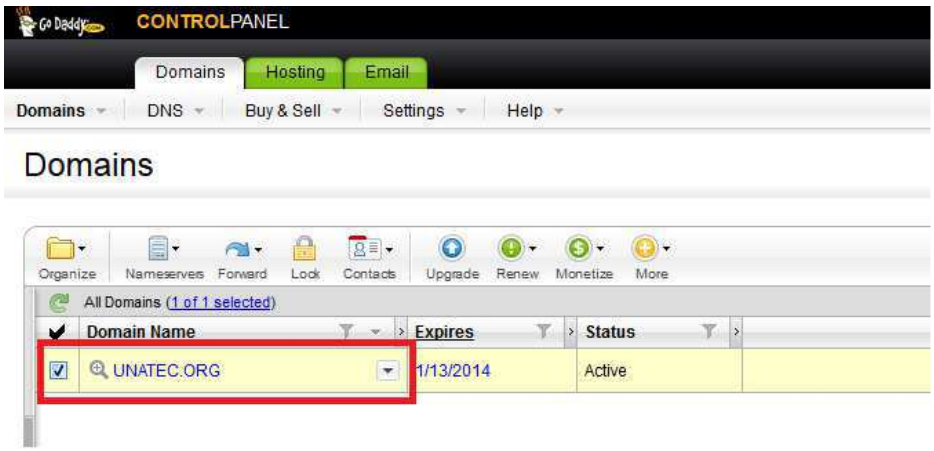


Figura 4.1.10.4 Dominios Disponibles

Se tiene disponible los dominios adquiridos y ahora se puede configurarlo de acuerdo a las necesidades, se marca el dominio y se haceclic en el nombre para a la configuración de DNS.

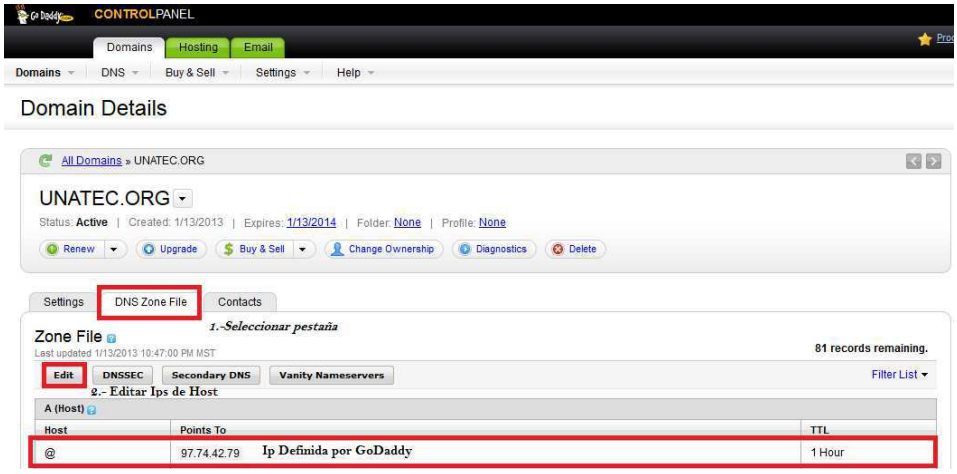


Figura 4.1.10.5 Configuración DNS

En la pestaña DNS Zone File se puede verificar la configuración actual definida por GoDaddy, para editarla, hacer clic en el botón **Edit.**

Figura 4.1.10.6 Edición de DNS de dominio

Hacer clic en **Apunta A** para modificar la dirección IP del Host definido como @ y se coloca laip pública que asigna el Proveedor de Internet, en este caso la dirección utilizada es la 190.155.37.244, con esto el dominio www.unatec.org apuntará a la dirección IP mencionada, para que esta configuración tenga efecto se debe esperar aproximadamente 1 hora. Ahora se debe configurar el re direccionamiento a los puertos que utiliza la aplicación.

Si es que es el caso de que el proveedor de internet únicamente proporciona el servicio directamente a un equipo entonces no es necesario ningún direccionamiento de puertos, únicamente se deben verificar los puertos abiertos para utilizarlos directamente.

En caso de tener una conexión en cascada mediante un router, se debe configurar una ruta de direccionamiento para cuando públicamente se especifique un puerto para conectarse al dominio, por ejemplo www.unatec.org:443, en la ruta se debe especificar a qué equipo de la red se deben direccionar los paquetes en el puerto especificado.

Figura 4.1.10.7 Pagina Web www.puertosabiertos.com

Para verificar los puertos se tiene a disposición la página de puertosabiertos.com que verifica determinados grupos de puertos abiertos, con los resultados finales se sabrá que puertos públicos se puede utilizar para implementar hosting in-House

Figura 4.1.10.8 Escanear Conjunto de Puertos

Se puede realizar el escaneo por un grupo de puertos determinado por la aplicación web o se puede digitar un puerto específico, una vez publicados los resultados se podrá determinar que puertos públicos se puede utilizar para el re direccionamiento a los servicios.

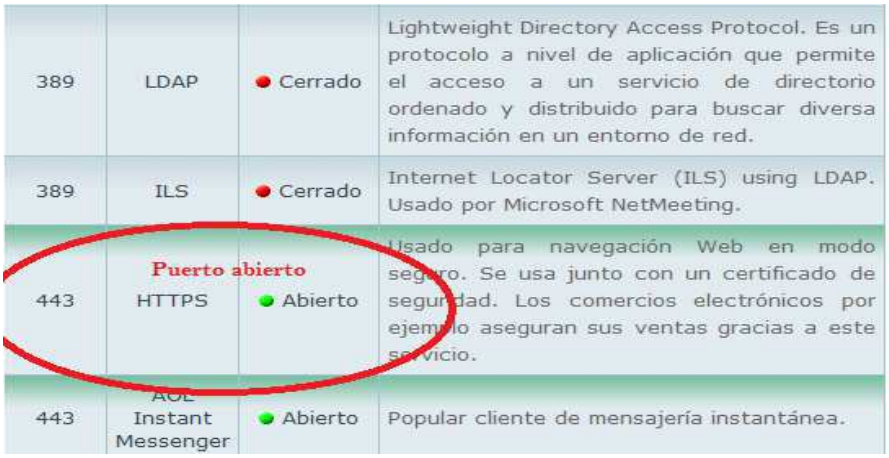


Figura 4.1.10.9 Resultado de Escaneo de puertos

La lista de resultados indica los puertos escaneados y el estado del mismo, en este caso se deberán utilizar los puertos que se encuentran abiertos.

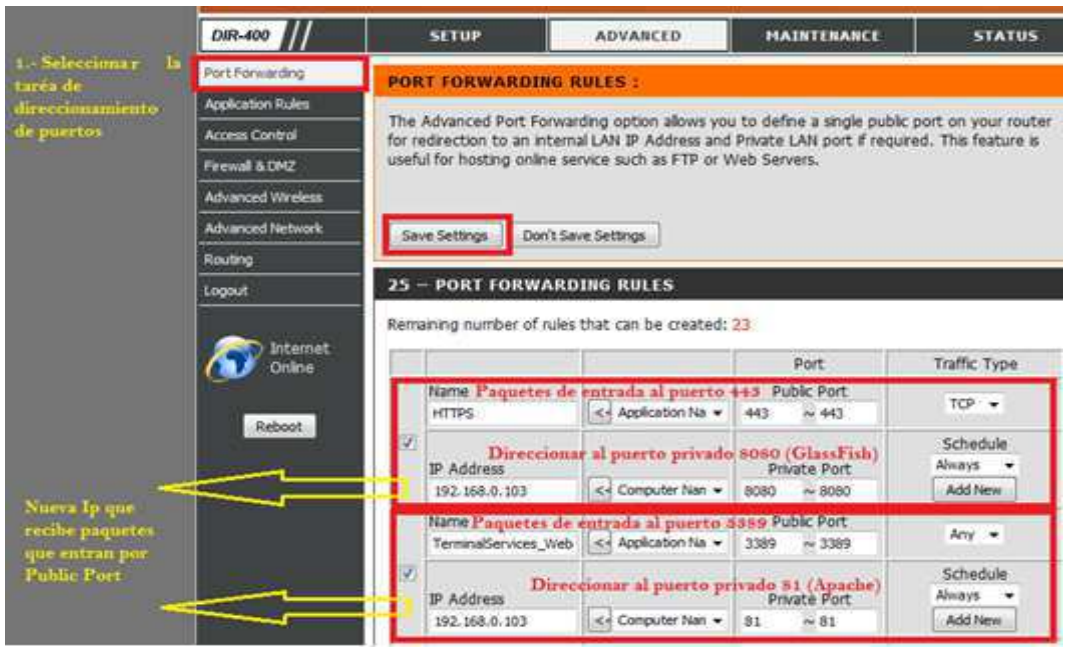


Figura 4.1.10.10 Direccionamiento de Ip y Puertos Privados

Se selecciona la tarea de **Port Forwarding** para establecer los nuevos parámetros de direccionamiento de Ips y de puertos, antes de la configuración se debe asegurar que los puertos públicos que se va a utilizar se encuentren abiertos, caso contrario no habrá conexión con los servicios.

Como puerto público se utiliza el 443 y el 3389, los cuales se encuentran abiertos por parte del proveedor de internet. La lógica de direccionamiento será que los paquetes dirigidos al puerto 443 sean direccionados a la IP 192.168.0.103 y al puerto 8080, en donde se encuentra levantando el servidor Web Glasshfish con la aplicación Web de firma electrónica y los paquetes dirigidos al puerto 3389 sean direccionados a la IP 192.168.0.103 y al puerto 81, en donde se encuentra levantado Apache que aloja a Joomla para el gestor de contenidos. Se guardan los cambios y se puede realizar pruebas desde un browser para verificar que la configuración ya esté operando.

Con esta configuración de direccionamiento el dominio apunta a laIp Pública y los paquetes dirigidos a los puertos libres del proveedor de internet serán re direccionados a los puertos privados de la máquina en donde se levantó la infraestructura de servicios. Hay que tomar en cuenta que los equipos utilizados deben estar encendidos en todo momento para poder acceder a los servicios. Si se interrumpe el servicio de internet en el área local entonces no serán visibles en la nube. Se deben tomar en cuenta los riesgos al levantar un hosting In-House, se depende totalmente de una infraestructura propia, y no hay terceros que garanticen calidad de servicio.

4.2. IMPLEMENTACIÓN DE LA FIRMA ELECTRÓNICA

4.2.1. Proceso de obtención de firma electrónica

4.2.1.1. La Autoridad de Certificación

La Autoridad de Certificación (AC)Por sí misma o mediante la intervención de una Autoridad de Registro, verifica la identidad del solicitante de un certificado antes de su expedición o, en caso de certificados expedidos con la

condición de revocados, elimina la revocación de los certificados al comprobar dicha identidad. Los certificados son documentos que recogen ciertos datos de su titular y su clave pública y están firmados electrónicamente por la Autoridad de Certificación utilizando su clave privada.

La Autoridad de Certificación es un tipo particular de Prestador de Servicios de Certificación que legitima ante los terceros que confían en sus certificados la relación entre la identidad de un usuario y su clave pública. La confianza de los usuarios en la **CA** es importante para el funcionamiento del servicio y justifica la filosofía de su existencia.

En el ecuador se tiene a la ECIBCE como entidad certificadora, la misma que se encarga de garantizar la identidad de los solicitantes de certificados y de la renovación o revocación de los mismos.

El BCE dispone de su propio dominio y Web site para que las personas naturales, jurídicas o funcionarios públicos puedan realizar la solicitud de su certificado de firma electrónica.

El proceso empieza en la página del BCE http://www.eci.bce.ecen la que se puede ver los servicios que ofrecen a la ciudadanía, entre ellos se tiene la "Solicitud de Certificado digital de Firma Electrónica"

Figura 4.2.1.1 Página Principal de la ECIBCE

Antes de iniciar con la solicitud el BCE se encarga de informar al usuario sobre las normativas correspondientes a cada tipo de certificado, la Declaración de Practicas de Certificación (DPC) y las Políticas de Certificados (PC), por lo cual es obligación del suscriptor leer y conocer cuáles son sus derechos, sus obligaciones, las obligaciones de la entidad certificadora, y que hacer en determinados casos que puedan suscitarse con su certificado.

Los puede realizar la solicitud del certificado en las siguientes formas:

- Persona Natural
- Persona Jurídica
- Funcionario Publico

Para efectos del presente proyecto se lo realizará como persona Natural, y se procede a ingresar a la solicitud del certificado

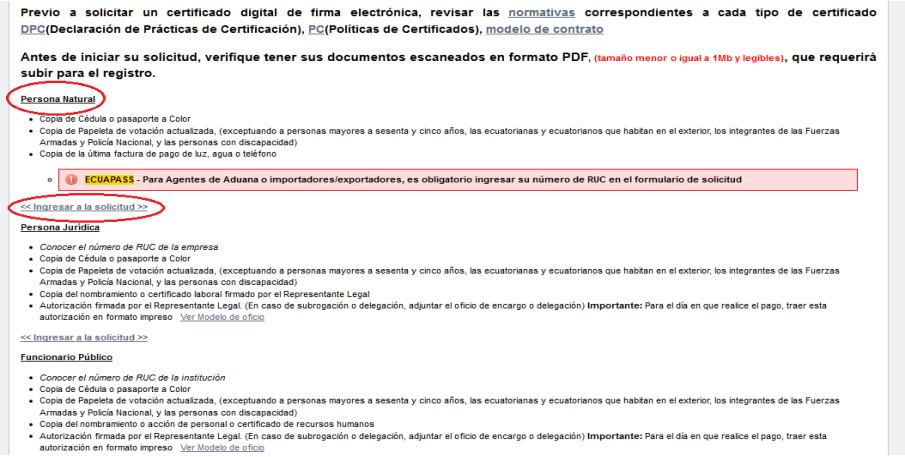


Figura 4.2.1.2 Página de Solicitud de Certificado de Firma Electrónica

En el formulario de acuerdo a las necesidades e ingresan los siguientes datos:

Tipo de Certificado:

- Persona Natural
- Persona Jurídica
- Funcionario Publico

Tipo de Contenedor de Certificado

- Token
- Archivo
- HSM
- ROAMING

Lugar de Entrega

- Quito
- Guayaquil
- Cuenca

Tipo de Identificación

- Cédula
- Pasaporte

Figura 4.2.1.3 Registro de Solicitud

Al aceptar se tiene este nuevo formulario en el que se deben llenar los datos personales

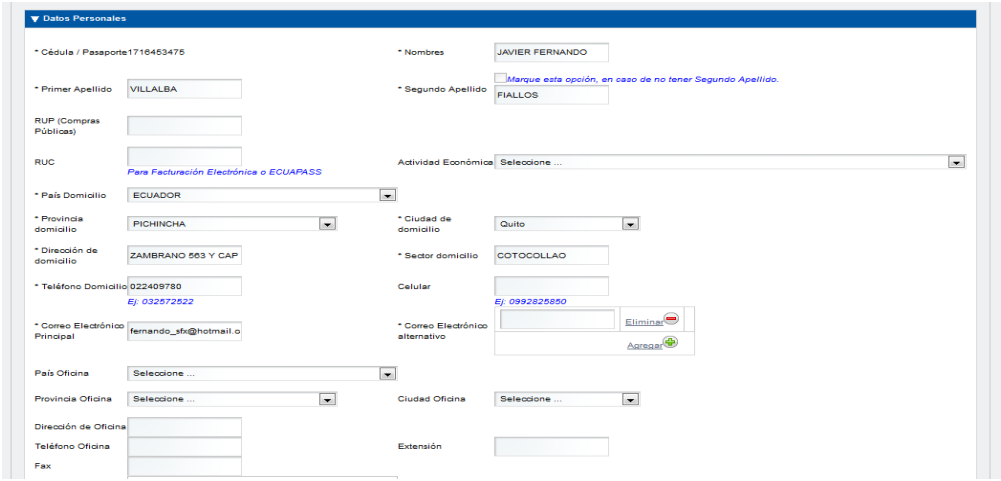


Figura 4.2.1.4 Formulario de Datos Personales #1

Y además se aclara el uso para el que se va a emplear el certificado de firma electrónica solicitado.

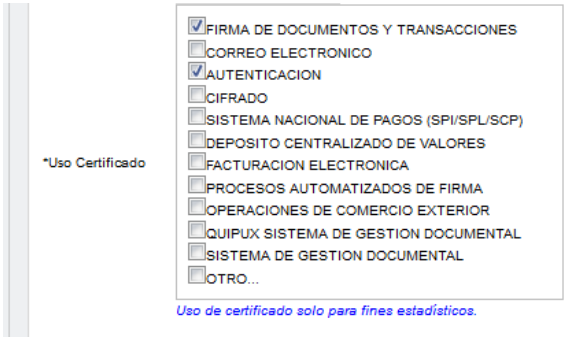


Figura 4.2.1.5 Uso de Certificado de Firma Electrónica

Se cargan las copias escaneadas de la cedula o pasaporte, papeleta de votación, y de la última factura de pago de luz, agua y teléfono.

Se certifica que la información entregada es real y que corresponde al solicitante.

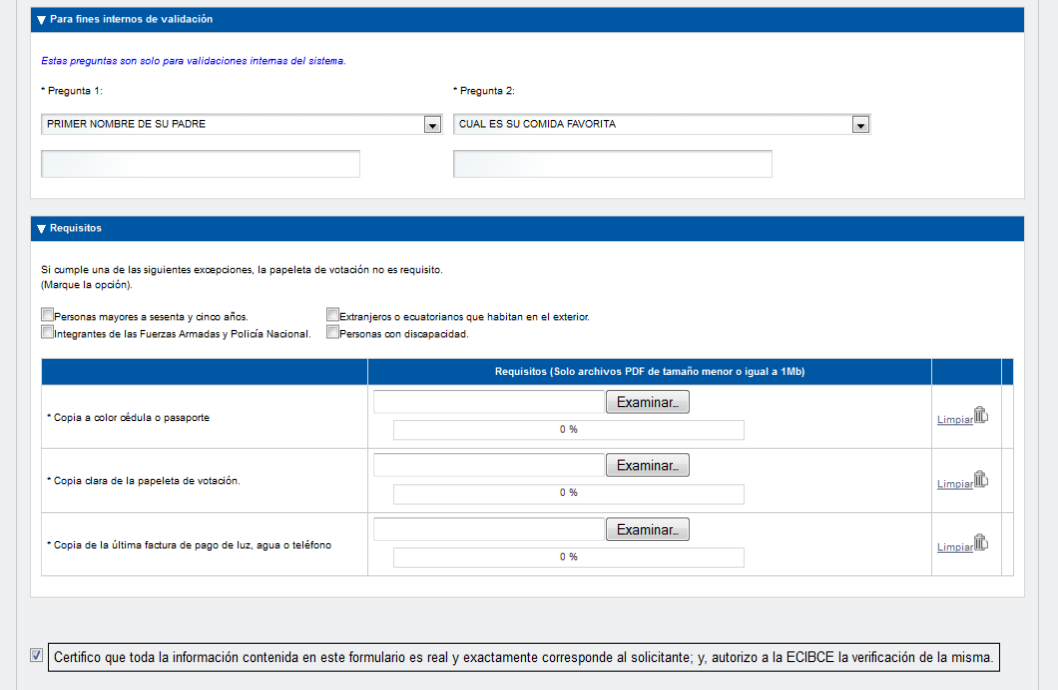
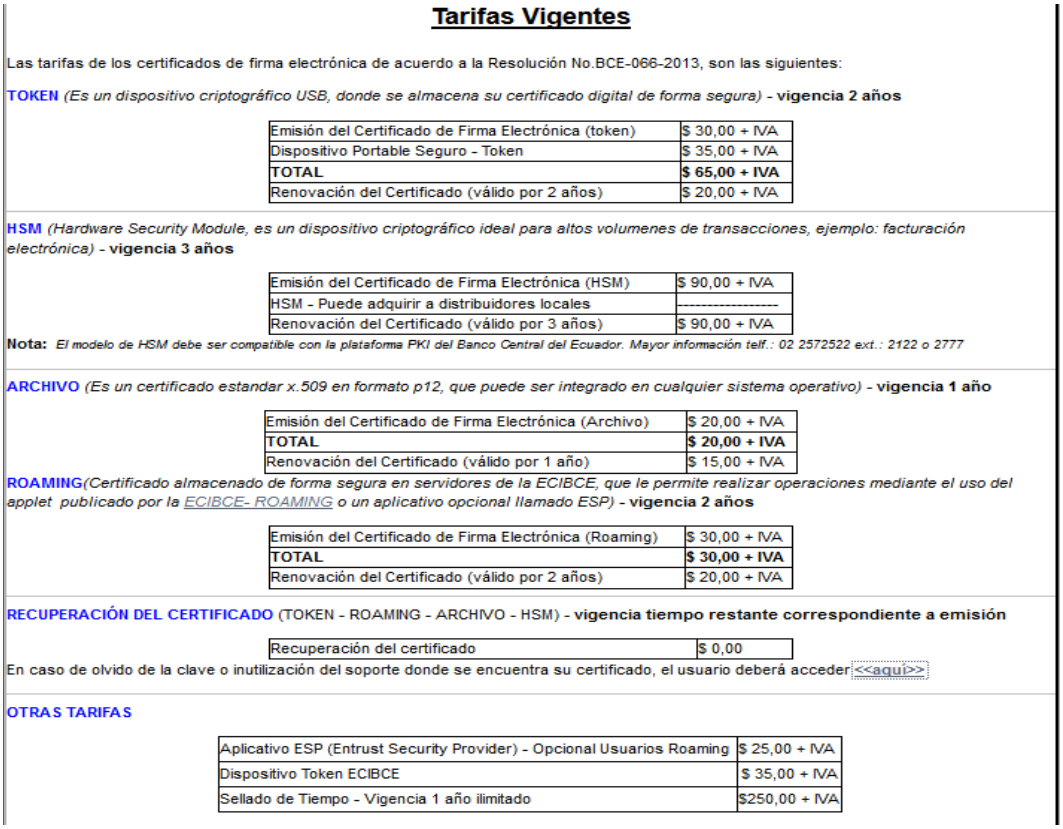


Figura 4.2.1.6 Formulario de Datos Personales 2

Una vez finalizada la solicitud de firma electrónica se deberá esperar la respuesta por parte de la ECIBCE en la que se rechaza o se aprueba la solicitud del certificado de firma electrónica, en el caso de que la solicitud se aprueba se recibirá un correo como el que se muestra en el siguiente en la figura

Figura 4.2.1.7 Correo de Aprobación de Certificado de Firma Electrónica

En el Banco Central de Ecuador se debe cancelar el monto que indica en la siguiente tabla



Tarifas Vigentes

Las tarifas de los certificados de firma electrónica de acuerdo a la Resolución No.BCE-066-2013, son las siguientes:

TOKEN *(Es un dispositivo criptográfico USB, donde se almacena su certificado digital de forma segura)* - **vigencia 2 años**

Emisión del Certificado de Firma Electrónica (token)	$ 30,00 + IVA
Dispositivo Portable Seguro - Token	$ 35,00 + IVA
TOTAL	**$ 65,00 + IVA**
Renovación del Certificado (válido por 2 años)	$ 20,00 + IVA

HSM *(Hardware Security Module, es un dispositivo criptográfico ideal para altos volumenes de transacciones, ejemplo: facturación electrónica)* - **vigencia 3 años**

Emisión del Certificado de Firma Electrónica (HSM)	$ 90,00 + IVA
HSM - Puede adquirir a distribuidores locales	----------
Renovación del Certificado (válido por 3 años)	$ 90,00 + IVA

Nota: *El modelo de HSM debe ser compatible con la plataforma PKI del Banco Central del Ecuador. Mayor información telf.: 02 2572522 ext.: 2122 o 2777*

ARCHIVO *(Es un certificado estandar x.509 en formato p12, que puede ser integrado en cualquier sistema operativo)* - **vigencia 1 año**

Emisión del Certificado de Firma Electrónica (Archivo)	$ 20,00 + IVA
TOTAL	**$ 20,00 + IVA**
Renovación del Certificado (válido por 1 año)	$ 15,00 + IVA

ROAMING*(Certificado almacenado de forma segura en servidores de la ECIBCE, que le permite realizar operaciones mediante el uso del applet publicado por la ECIBCE- ROAMING o un aplicativo opcional llamado ESP)* - **vigencia 2 años**

Emisión del Certificado de Firma Electrónica (Roaming)	$ 30,00 + IVA
TOTAL	**$ 30,00 + IVA**
Renovación del Certificado (válido por 2 años)	$ 20,00 + IVA

RECUPERACIÓN DEL CERTIFICADO (TOKEN - ROAMING - ARCHIVO - HSM) - **vigencia tiempo restante correspondiente a emisión**

Recuperación del certificado	$ 0,00

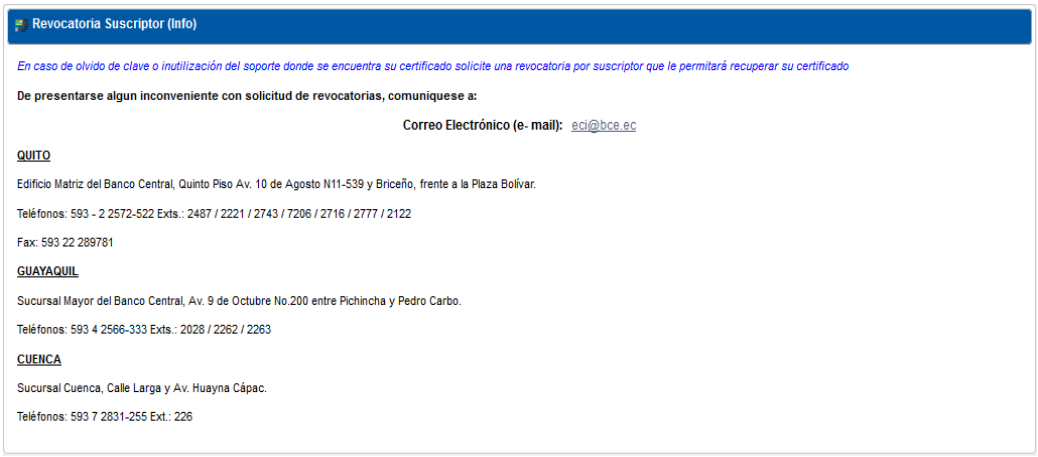
En caso de olvido de la clave o inutilización del soporte donde se encuentra su certificado, el usuario deberá acceder <<aquí>>

OTRAS TARIFAS

Aplicativo ESP (Entrust Security Provider) - Opcional Usuarios Roaming	$ 25,00 + IVA
Dispositivo Token ECIBCE	$ 35,00 + IVA
Sellado de Tiempo - Vigencia 1 año ilimitado	$250,00 + IVA

Figura 4.2.1.8 Tarifas de Certificados de Firma Electrónica

En caso de olvidar la clave privada o perdida de cualquiera de los tipos de certificado se deberá solicitar la revocatoria por suscriptor que le permitirá recuperar al individuo el certificado.



Revocatoria Suscriptor (Info)

En caso de olvido de clave o inutilización del soporte donde se encuentra su certificado solicite una revocatoria por suscriptor que le permitará recuperar su certificado

De presentarse algun inconveniente con solicitud de revocatorias, comuniquese a:

Correo Electrónico (e- mail): eci@bce.ec

QUITO

Edificio Matriz del Banco Central, Quinto Piso Av. 10 de Agosto N11-539 y Briceño, frente a la Plaza Bolívar.

Teléfonos: 593 - 2 2572-522 Exts.: 2487 / 2221 / 2743 / 7206 / 2716 / 2777 / 2122

Fax: 593 22 289781

GUAYAQUIL

Sucursal Mayor del Banco Central, Av. 9 de Octubre No.200 entre Pichincha y Pedro Carbo.

Teléfonos: 593 4 2566-333 Exts.: 2028 / 2262 / 2263

CUENCA

Sucursal Cuenca, Calle Larga y Av. Huayna Cápac.

Teléfonos: 593 7 2831-255 Ext.: 226

Figura 4.2.1.9 Información de Revocatoria Suscriptor

Concluido el proceso de la solicitud del certificado de firma electrónica se debe acudir a las oficinas, realizar el pago correspondiente y continuar con la entrega formal del certificado, el mismo en el que ambas partes, la ECIBCE y el suscriptor celebran el contrato de prestación de servicios, en el que las funciones y obligaciones que deben cumplir las partes se encuentran estipuladas y bien definidas para así conllevar al correcto uso del certificado de firma electrónica.

4.2.2. Importar Certificados Digitales

El proceso de importación de Certificados permite añadir un certificado Digital a la lista de certificados de Confianza. El certificado emitido por la AC al suscriptor posee una cadena de confianza, la misma que tiene varios niveles conocidas como AC subordinadas.

Las AC disponen de sus propios certificados públicos, y sus claves privadas asociadas son empleadas por las AC para firmar los certificados que ellos mismo emiten. Un certificado de una AC puede estar auto-firmado cuando no hay ninguna AC de rango superior que lo firme.

En el caso de los certificados de AC Raíz, es el elemento inicial de cualquier jerarquía de certificación y pueden autorizar a otras AC subordinadas la emisión de certificados digitales con la respectiva firma de la AC Raíz. Una jerarquía de certificación consiste en una estructura jerárquica de ACs en la que se parte de una AC Raíz auto-firmada, y en cada nivel, existe una o más ACs que pueden firmar certificados de entidad final (titular de certificado: servidor web, persona, aplicación de software) o bien certificados de otras AC subordinadas plenamente identificadas y cuya Política de Certificación sea compatible con las **AC**s de rango superior.

El proceso de instalación puede hacerse, en sistemas operativos de tipo Windows, haciendo doble clic en el fichero que contiene el certificado e iniciando así el "asistente para la importación de certificados". Por regla general el proceso hay que repetirlo por cada uno de los navegadores que existan en el

sistema, tales como Opera (navegador), Firefox o Internet Explorer, y en cada caso con sus funciones específicas de importación de certificados.

Figura 4.2.2.1 Asistente de importación de Certificados

Mediante el uso del asistente se puede cargar un certifciado digital a la librería de certificados de confianza de Windows, y dependiendo del tipo de certificado se lo puede almacenar en un determinado grupo, que puede ser, de Entidades Certificadoras de Confianza, certificados de identificacion individual y personal, etc.

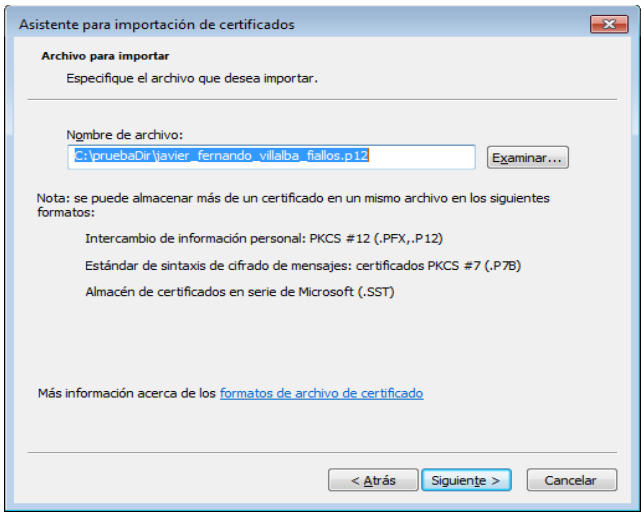


Figura 4.2.2.2 Selección de certificado de Firma Electrónica

Se selecciona y escribe la clave privada del certificado emitido por el Banco Central del Ecuador.

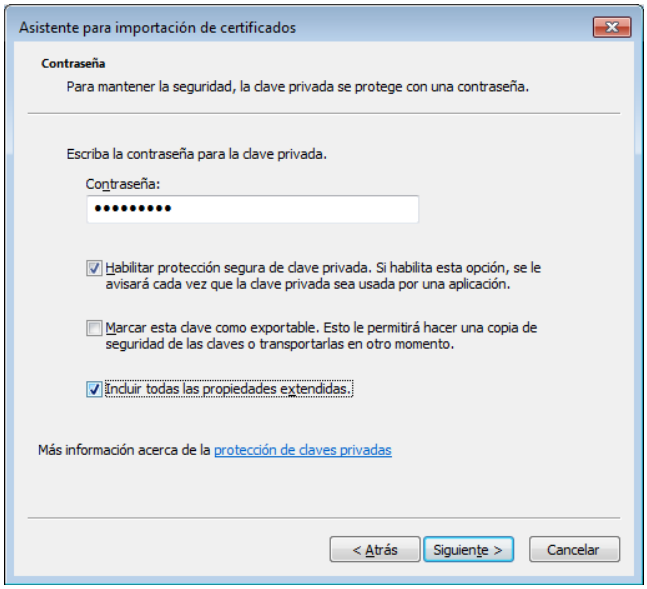


Figura 4.2.2.3 Ingreso de Clave privada de Certificado

Posteriormente se deberá seleccionar la ubicación en donde se guardara el certificado que se está importando, de preferencia se marca la opción de selección automática de ubicación de acuerdo al tipo de certificado.

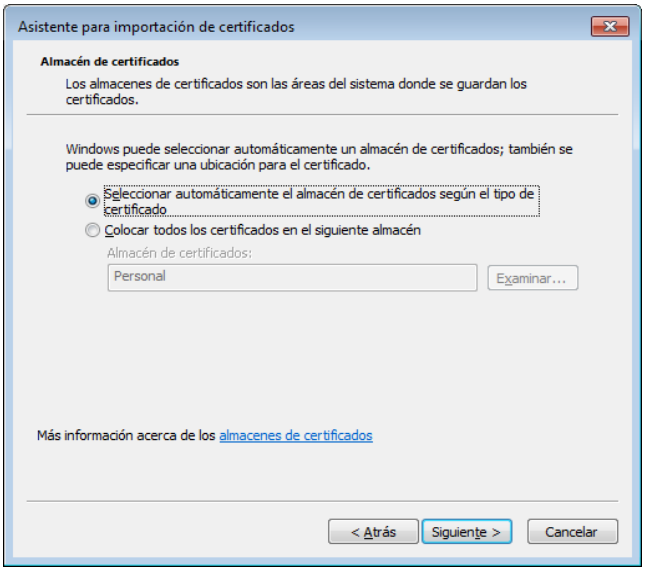


Figura 4.2.2.4 Selección de almacén de Certificados

Finalmente se termina el proceso de importación y la próxima vez que se visualice un archivo PDF con su respectiva firma electrónica, indicará que el certificado con el que fue firmado el documento es de confianza en el equipo que se realiza el proceso, al importar el certificado se tiene la cadena de confianza, que identifica a la AC Raiz del certificado, a la AC subordinada que emitió el certificado, en este caso se tiene como AC Raiz al Banco Central del Ecuador y como AC Subordinada la ECIBCE, la cual es la que emite el certificado que garantiza que un individuo es quien asegura ser.

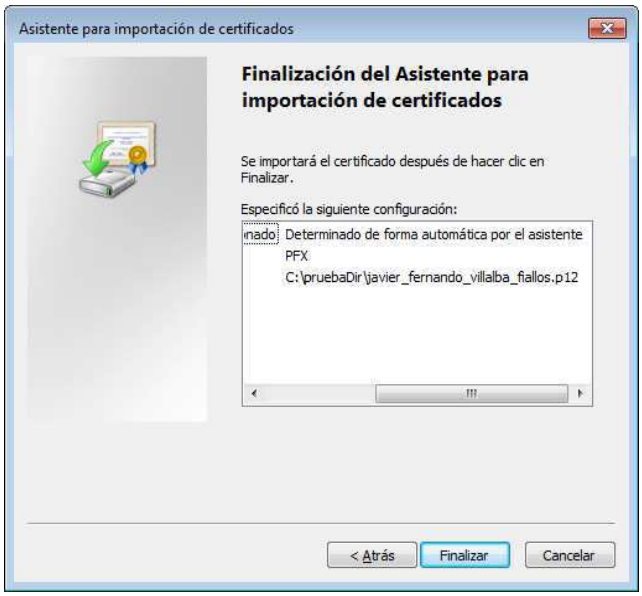


Figura 4.2.2.5 Finalización de Asistente

Para la instalación de los certificados de AC Raíz y AC Subordinada se sigue el mismo proceso detallado, con la diferencia de que no se debe escribir ninguna clave para importar el certificado. Cuando el certificado de la AC Raíz y Subordinada se encuentren en la librería de certificados de confianza de Windows, es decir, todos los certificados emitidos por estas AC serán considerados de confianza y se garantiza la identidad de los terceros que posean mencionados certificados.

4.2.3. Estructura del certificado digital de Firma Electrónica

Para procesar el certificado digital es necesaria la importación de librerías .jar de bouncyCastle, librerías de libre distribución que hacen posible el procesamiento del certificado digital de firma electrónica.

La estructura interna del certificado y específicamente los campos denominados identificadores de objeto único (OID) contienen los atributos del suscriptor. Estos difieren ligeramente dependiendo del tipo de certificado digital que se ha solicitado a la autoridad certificadora, por ejemplo, si el certificado solicitado es del tipo de Persona Natural, entonces los atributos (OID) serán exclusivamente los datos de identificación del individuo, el banco certificará su identidad una vez se haya cumplido con los requisitos solicitados, para el caso de funcionarios públicos o personas jurídicas se tendrán OIDs adicionales que indicarán el RUC, el nombre de la empresa y el cargo que desempeña.

A continuación se describe la estructura del certificado digital de firma electrónica.

Campo	Descripción	Valor
Serial Number	Número que identifica unívocamente al certificado	Número de serie del certificado
Algoritmo de firma	Algoritmo utilizado por la ECIBCE para firmar el certificado	sha256RSA
Emisor (issuer)	CN (CommonName)	AC BANCO CENTRAL DEL ECUADOR
	L (Localidad)	QUITO

	OU (OrganizationalUnit.)	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O (Organization)	BANCO CENTRAL DEL ECUADOR
	C (Country)	EC
Válido desde	Fecha y hora UTC desde que es válido el certificado	Fecha de inicio de la validez del certificado de Persona natural
Válido hasta	Fecha y hora hasta la cual es válido el certificado.	Fecha final de la validez del certificado de Persona Natural
Asunto (Suscriptor)	CN	NOMBRES Y APELLIDOS + Número de Serie
	L (Localidad)	QUITO
	OU (OrganizationalUnit.)	ENTIDAD DE CERTIFICACION DE INFORMACIÓN-ECIBCE
	O (Organization)	BANCO CENTRAL DEL ECUADOR
	C (Country)	EC
Clave pública	Clave pública del Suscriptor	Clave Pública
Directivas o Bases del Certificado	Identificador de Objetos según la normalización internacional de la IANA	1.3.6.1.4.1.37947.2.1.1 http://www.eci.bce.ec/politica-certificado/persona-natural.PDF

X509v3 CRL DistributionPoints	Puntos de distribución de CRL	Dirección donde se publica la lista de revocación de Certificados
X509v3 Subject Alternative Name	Nombre alternativo	Correo electrónico del suscriptor
Periodo de uso de clave privada		Tiempo en que estará vigente la clave privada
Identificador de clave de entidad emisora		Extensión del estándar X509
Restricciones Básicas		Determina a que está destinada la AC, la ruta de certificación como entidad final de ECI
Algoritmo de identificación	Algoritmo Hash que genera una síntesis de datos o huella digital.	sha1
1.3.6.1.4.1.37947.3.1	OID atributo cédula o pasaporte	CEDULA/PASAPORTE (Obligatorio)
1.3.6.1.4.1.37947.3.2	OID atributo Nombres	NOMBRES COMPLETOS (Obligatorio)
1.3.6.1.4.1.37947.3.3	OID atributo Apellido 1	APELLIDO1 (Obligatorio)
1.3.6.1.4.1.37947.3.4	OID atributo Apellido 2	APELLIDO2 (Obligatorio)
1.3.6.1.4.1.37947.3.7	OID atributo dirección	DIRECCIÓN (Obligatorio)
1.3.6.1.4.1.37947.3.8	OID atributo teléfono	TELÉFONO (Obligatorio)
1.3.6.1.4.1.37947.3.9	OID atributo ciudad	CIUDAD (Obligatorio)

1.3.6.1.4.1.37947.3.12	OID atributo País	PAIS (Ecuador)
1.3.6.1.4.1.37947.3.51	OID atributo Contenedor	Dispositivo Criptográfico - "1"/ Archivo - "2" (Obligatorio)

Tabla 4.2.2.1 Estructura del Certificado Digital de Firma Electrónica[52]

4.2.4. Manual de Implementación de Firma Electrónica

El token entregado por el Banco Central del Ecuador contiene los datos del certificado, la AC pone a disponibilidad la herramienta SafeNet que contiene el driver para acceder al dispositivo USB, este aplicativo se encuentra disponible para Linux, Mac y Windows y se lo puede descargar y es necesario para que el aplicativo web pueda acceder a los datos del dispositivo.

Figura 4.2.4.1 Aplicación SafeNet para Token

[52] **Fuente:** http://www.eci.bce.ec/c/document_library/get_file?uuid=b8cc5bde-8b8b-48dc-9b96-b625a5ce8e84&groupId=10155

Una vez instalada la aplicación SafeNet se puede proceder con la carga del certificado digital en la aplicación Web.

Figura 4.2.4.2 Módulo de Firma Electrónica

En el módulo de firma electrónica del sistema se escoge la tarea **Cargar Nuevo Certificado,** se selecciona el tipo de contenedor en el que se encuentra que puede ser en Token o Archivo y se digitará la clave privada del dispositivo.

Figura 4.2.4.3 Cargar Firma Autorizada

Si es que los datos proporcionados son correctos entonces el certificado se cargará exitosamente y los atributos OID del token o archivo se guardarán en la base de datos.

Los atributos OID, que contienen en formato byte hexadecimal los datos del suscriptor, la infraestructura se los puede visualizar en la siguiente de la siguiente ventana:

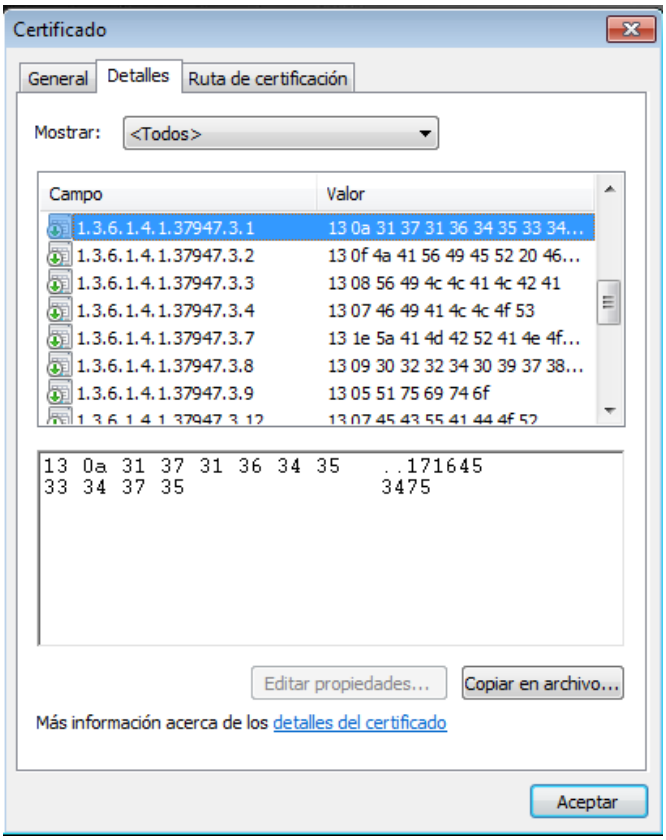


Figura 4.2.4.4 Detalles del Certificado (Atributos OID)

Para poder procesar estos datos del certificado es necesaria generar una clase de tipo certificado y añadir sus atributos con el respectivo nombre del campo, es necesario identificar que datos del certificado que se va a utilizar, si los datos se han ingresado correctamente, se procede a procesar el certificado utilizando librerías BouncyCastle:

```
111
113                 Security.addProvider(new BouncyCastleProvider());
```

Figura 4.2.4.5 Proveedor de Seguridad BouncyCastle

La línea de código de la figura 4.1.4 permite instanciar como proveedor de seguridad a BouncyCastle, las librerías de este proveedor permiten extraer la información del contenedor del certificado digital (Archivo, Token, Etc)

```
Source  History
229     ////////////////////////////////////////////////////////////////////
230     ////Obtener informacion del certificado
231     certificado = new  InfoCertificado(x509);
232
233
234      System.out.println( "Cedula: "+certificado.getCedula());
235      System.out.println( "Nombres: "+certificado.getNombre());
236      System.out.println( "Apellidos: "+certificado.getApellido());
237      System.out.println( "Direccion: "+certificado.getDireccion());
238      System.out.println( "Telefono: "+certificado.getTelefono());
239      System.out.println( "Lugar: "+certificado.getLugar());
240      System.out.println( "Institucion: "+certificado.getInstitucion());
241      System.out.println( "Cargo: "+certificado.getCargo());
242       System.out.println( "Serie: "+certificado.getSerial());
243       System.out.println( "Emision: "+certificado.getFechainicio());
244       System.out.println( "Hasta: "+certificado.getFechafin());
245       System.out.println( "Valido: "+certificado.isActivo());
246       System.out.println( "EmisorString: "+certificado.getEmisor());
```

Figura 4.2.4.6 Información del Certificado

El constructor de la clase InfoCertificado recibe como parámetro una variable de tipo certificado x509, esta devuelve los atributos definidos por el OID, lo que lo adecua a la infraestructura de certificado digital que utiliza el Banco Central del Ecuador.

```
45      public InfoCertificado(X509Certificate signingCert) throws CertificateEncodingException {
46
47          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.1") != null) {
48              setCedula(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.1")).trim()    );
49          }
50          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.2") != null) {
51              setNombre(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.2")).trim());
52          }
53          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.3") != null) {
54          setApellido(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.3")).trim() +" "+ n
55          }
56          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.7") != null) {
57              setDireccion(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.7")).trim());
58          }
59          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.8") != null){
60              setTelefono(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.8")).trim());
61          }
62          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.12") != null) {
63              setLugar(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.12")).trim() + "
64          }
65          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.6") != null) {
66              setInstitucion(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.6")).trim()
67          }
68          if (signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.5") != null) {
69              setCargo(new String(signingCert.getExtensionValue("1.3.6.1.4.1.37947.3.5")).trim());
```

Figura 4.2.4.7 Parámetros OID del Certificado

El parámetro recibido en el constructor corresponde al certificado y se puede extraer sus atributos especificando los OID del certificado digital. Se retorna los valores de las OID correspondiente en una variable de tipo certificado y se almacenará en la base de datos.

Certificados de Usuarios Autorizados

1

Nombre	Apellido	Cedula	Vigente	Activo	Contenedor
JAVIER FERNANDO	VILLALBA FIALLOS	1716453475	✓	✗	SOFTWARE-ARCHIVO
JAVIER FERNANDO	VILLALBA FIALLOS	1716453475	✓	✓	HARDWARE-TOKEN

1

Figura 4.2.4.8 Certificados de firma electrónica disponibles

Una vez concluido el proceso de carga del certificado, se tiene disponible la información que contenía y ahora es visible en el módulo.

Figura 4.2.4.9 Activación del Certificado

Se puede activar o desactivar el certificado de firma electrónica, en caso de estar activado, se verificara cada firma electrónica incrustada en un fichero PDF y si se utilizó un certificado cargado en la aplicación entonces se lo considerará revisado y/o emitido por un usuario autorizado.

Con los datos del certificado almacenados en el sistema se podrá discriminar los documentos firmados por un usuario autorizado, se puede activar o desactivar el certificado, en el menú de tareas

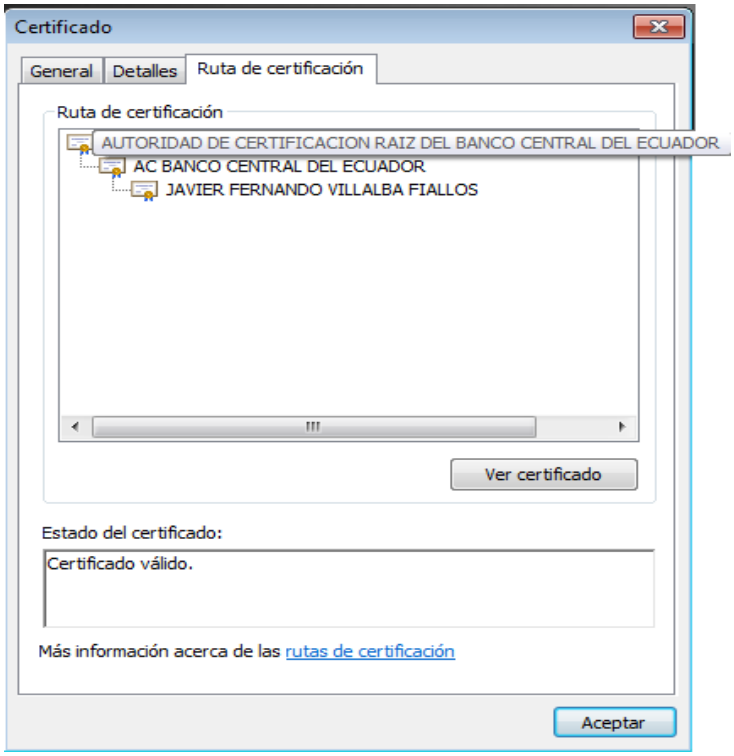
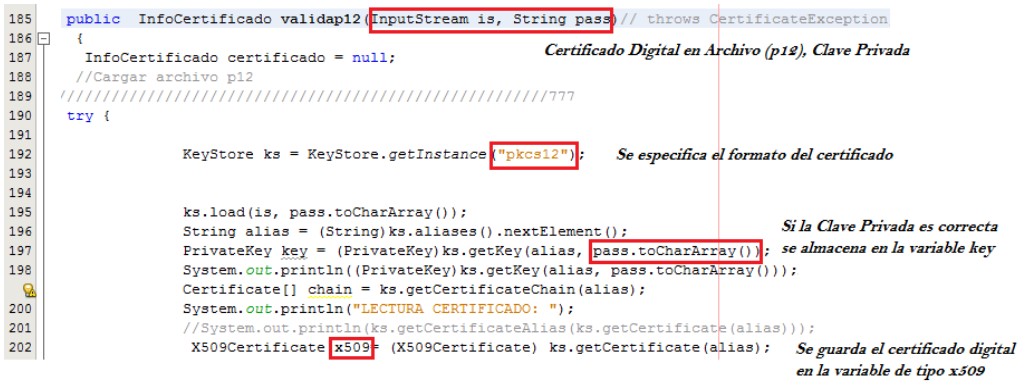


Figura 4.2.4.10 Cadena de Confianza del certificado

Un certificado digital debe tener su ruta de certificación compuesta de la siguiente manera:

1. Autoridad Certificadora Raíz (AC Raíz), es la cabeza de la jerarquía.
2. Autoridad Subordinada de Certificación, la cual es certificada por la AC Raíz
3. Suscriptor, su identidad es certificada por la Autoridad subordinada.

En el módulo de firma Electrónica se encuentra la funcionalidad de cargar certificados digitales de firma electrónica en formato de archivo o Hardware (Token), para esto es necesario instalar la aplicación SafeNet que posee el driver del dispositivo Token USB




```
185   public  InfoCertificado validap12(InputStream is, String pass)// throws CertificateException
186    {
187     InfoCertificado certificado = null;
188    //Cargar archivo p12
189   ////////////////////////////////////////////////////777
190    try {
191
192                 KeyStore ks = KeyStore.getInstance("pkcs12");
193
194
195                 ks.load(is, pass.toCharArray());
196                 String alias = (String)ks.aliases().nextElement();
197                 PrivateKey key = (PrivateKey)ks.getKey(alias, pass.toCharArray());
198                 System.out.println((PrivateKey)ks.getKey(alias, pass.toCharArray()));
                    Certificate[] chain = ks.getCertificateChain(alias);
200                 System.out.println("LECTURA CERTIFICADO: ");
201                 //System.out.println(ks.getCertificateAlias(ks.getCertificate(alias)));
202                  X509Certificate x509= (X509Certificate) ks.getCertificate(alias);
```

Figura 4.2.4.11 Código de acceso al certificado digital

La función **validap12** recibe como parámetros el archivo que contiene el certificado digital y la contraseña, si los parámetros están correctamente ingresados se empezará a procesar el certificado digital.

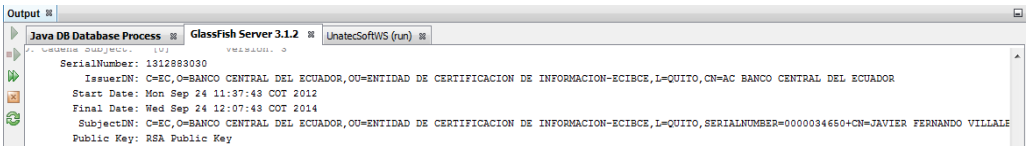


Figura 4.2.4.12 Información del certificado digital

Tal y como muestra la figura $, los datos del certificado son procesados en el servidor indicando los atributos: Número de Serie, País (C), Organización (O), Unidad Organizacional (OU) , Localidad (L), Fecha de Emisión, Fecha de Caducidad y Nombre Común (CN) tanto del emisor como del suscriptor.

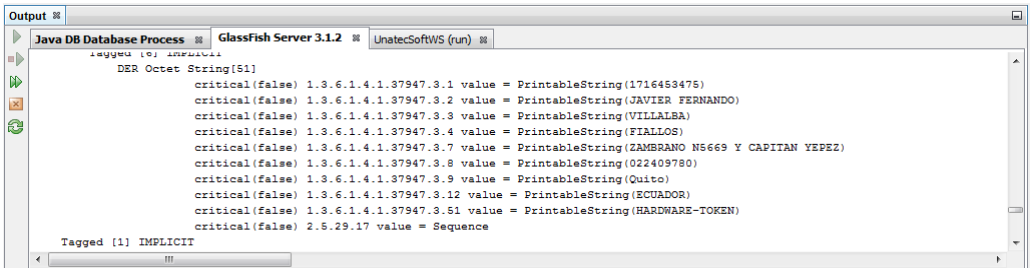


Figura 4.2.4.13 OIDs del Certificado Digital

En la figura se aprecia la estructura de datos que mantiene el certificado junto a su respectivo valor en formato de texto, cabe recalcar que cuando un documento es firmado electrónicamente con un certificado digital, se puede verificar la misma información que se encuentra en un certificado y en un documento PDF firmado con el mismo certificado. Los certificados digitales emitidos por el Banco Central se encuentran firmados con un algoritmo sha256RSA que pertenece al grupo Sha-2, actualmente el grupo Sha-2 es uno de los certificados más robustos, anteriormente con md5 y Sha-0 se han encontrados problemas colisión, es decir, que existe la posibilidad de que 2 conjuntos de datos totalmente distintos pueden llegar a tomar exactamente el mismo valor una vez realizado el cálculo hash, con Sha-1 existe actualmente una colisión teórica de 2^(60), probabilidades bajas de colisión pero teóricamente existente, con Sha-2 estos riesgos de colisión son inexistentes, cada conjunto de datos distintos tomará un único valor hash aplicando este algoritmo.

Una vez cargado el certificado digital se puede visualizar los datos en la aplicación, es totalmente transparente para el usuario, en pantalla visualizará los datos ya procesados del certificado digital.

4.2.4.1. Proceso para Firmar un fichero PDF con un certificado digital de Firma Electrónica

El Banco Central del Ecuador además emitir certificados digitales, también pone a disposición las herramientas para poder hacer uso de estos certificados digitales, en este caso dispone de la herramienta IntiSign Open

Source que permite firmar ficheros en formato PDF utilizando un certificado digital emitido por la AC.

Figura 4.2.4.1.1 IntiSign Aplicación para firma de Archivos

Una vez instalado la aplicación IntiSignse debe importar el certificado emitido por el Banco Central y seleccionar el fichero PDF que se necesita firmar.

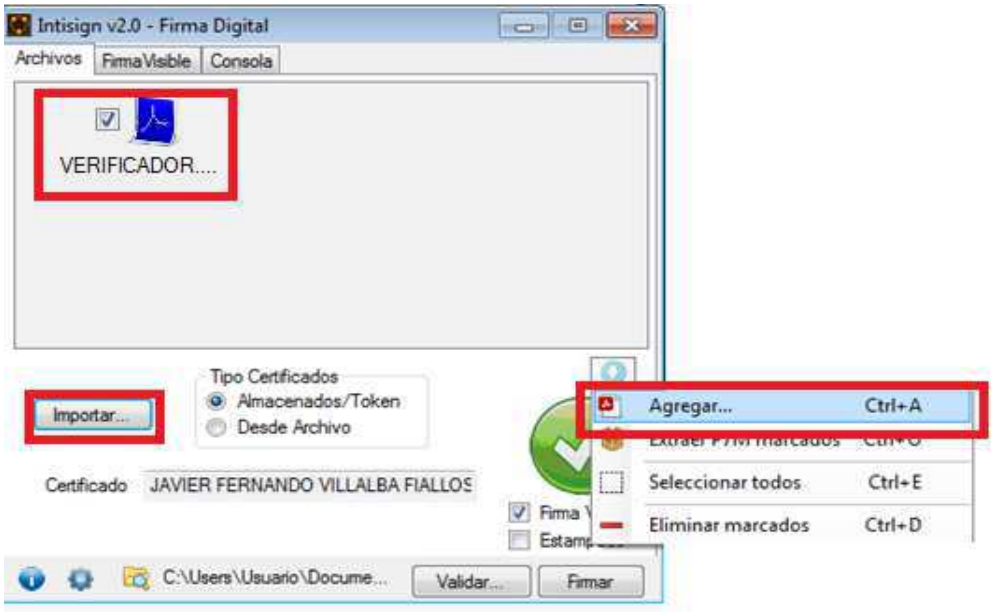


Figura 4.2.4.1.2 Selección de Certificado y fichero PDF

Una vez importado el certificado y seleccionado el fichero PDF, se procede a establecer la ubicación de la firma en el fichero PDF.

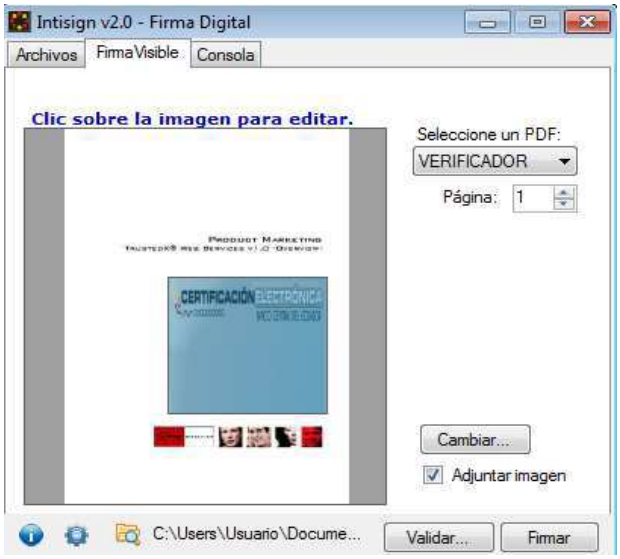


Figura 4.2.4.1.3 Ubicación de firma digital visible

En la aplicación se despliega la primera página del fichero PDF y el recuadro azul indica la ubicación en donde estará la firma digital en caso de que sea visible, al hacer clic en **validar** se revisara la lista de revocación de certificados (CRL) del Banco Central para verificar que el certificado se encuentre vigente y al activar el botón **firmar** la aplicación solicitará la clave privada del certificado e incrustará la firma en el fichero PDF.

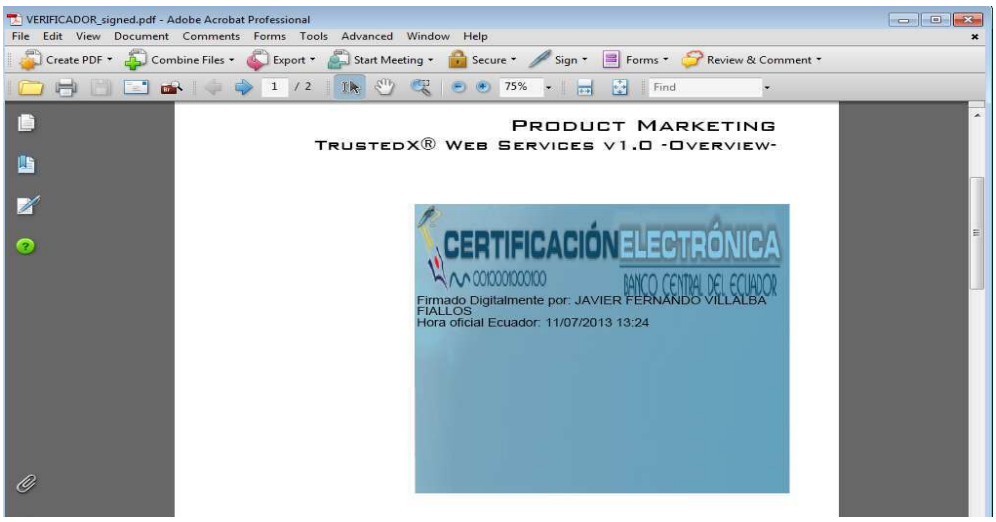


Figura 4.2.4.1.4 Fichero PDF firmado

Al finalizar el proceso se muestra el fichero PDF con la firma ubicada en el lugar seleccionado, al poseer una firma digital, el individuo que firmó el documento no puede repudiarlo de ninguna manera, no si es que el certificado se encuentra vigente y si es que no se encuentra en las CRL.

4.2.4.2. Carga de ficheros PDF en el módulo de Documentos

Ahora que se tiene un fichero PDF firmado con un certificado digital, se puede cargarlo en el módulo de documentos del aplicativo web,

Figura 4.2.4.2.1 Módulo de Documentos

En la tarea **Nuevo Oficio** se puede acceder al formulario para cargar el fichero PDF y llenando los campos solicitados por la aplicación.

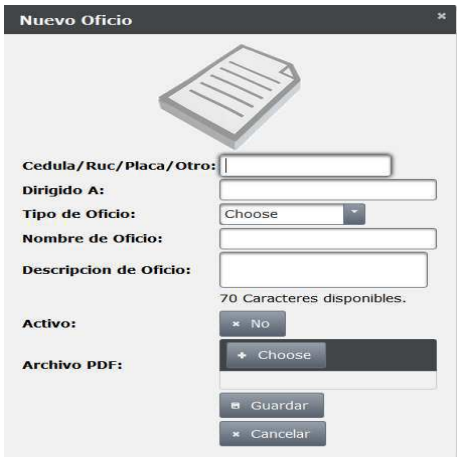


Figura 4.2.4.2.2 Formulario de Ingreso de Oficio

Se llenan los datos solicitados en el formulario y se selecciona el fichero PDF, el aplicativo verificará las firmas incrustadas en el documento y mostrará sus características al usuario.

Figura 4.2.4.2.3 Verificador de Firmas Digitales

Las firmas en un fichero PDF poseen las siguientes características:

- Revisión
- TimeStamp
- Cobertura total del Documento
- Identidad
- Vigencia
- Estado de Revocación de Certificado

4.2.4.3. Revisión

Una firma digital en un documento PDF permite el control de versiones, es decir, si un fichero tiene incrustadas 3 firmas digitales, es factible revisar el estado del documento antes de aplicada la 3ra o la 2da firma. Cada vez que una firma es aplicada, esta cubrirá únicamente el estado en el que se haya encontrado el fichero ese preciso momento. Se debe aclarar que el hecho de agregar cambios en un PDF firmado no implica que la revisión deje de ser válida, al agregar líneas

de texto en el fichero la primera firma digital aplicada anteriormente no cubrirá estos nuevos cambios ya que para firmarlo la primera vez se realizó al cálculo del código hash del conjunto de datos que se tenía en primera instancia. El sistema está en la capacidad de detectar este tipo de comportamiento, procesando las firmas de un fichero PDF una por una.

4.2.4.4. Sellado de Tiempo o TimeStamp

El Sellado de tiempo es otra característica de seguridad de las firmas digitales, esto permite garantizar la fecha y hora de la firma, se lo realiza por medio de una entidad certificadora, pero que no garantiza identidad, sino garantiza el tiempo exacto en el que se implanto la firma digital en un documento.

Figura 4.2.20 Sellado de Tiempo[53]

Tal y como muestra la figura existe un intermediario denominado Transmisor de la Autoridad de Estampado Cronológico (TTSA)[54], que recibe la solicitud de estampas de un cliente final, y la transmite a un proveedor de dichos servicios. Al proveedor de los servicios de estampado cronológico se la denomina Autoridad de Estampado Cronológico (TSA)[55]

Para este servicio comprende igualmente la solicitud de un certificado digital de Estampado Cronológico, esto se lo realiza por medio de una TSA o Time Stamp Autority, la misma que procesará las solicitudes de sellado de

[53] **Fuente:** http://www.eci.bce.ec/web/guest/estampado-de-tiempo
[54]**TTSA:** Transmission TimeStamp Authority
[55]**TSA:**TimeStamp Authority

tiempo y lo implantará en el documento firmado, es otra garantía de integridad para los ficheros PDF.

4.2.4.5. Cobertura total del fichero PDF

Un fichero PDF puede tener incrustado más de una firma digital, en el caso que aplique la condición entonces es necesario identificar cual es la firma que cubre todo el documento, esta será la que dé como resultado el código hash incluidas las demás firmas digitales, es decir, en el fichero que existen 5 firmas digitales, la firma que cubre todo el documento será la que incluya las 4 primeras revisiones en el cálculo del código hash. Tomar en cuenta que cada revisión se encarga de garantizar la integridad de su conjunto de datos, el sistema está en la capacidad de verificar la integridad de cada revisión del documento.

4.2.4.6. Firmar un fichero PDF con TimeStamp utilizando XolidoSign

XolidoSign es una aplicación gratuita que además de la funcionalidad de firmado digital permite incorporar a la firma un sello de tiempo que garantiza la fecha y la hora de la firma.

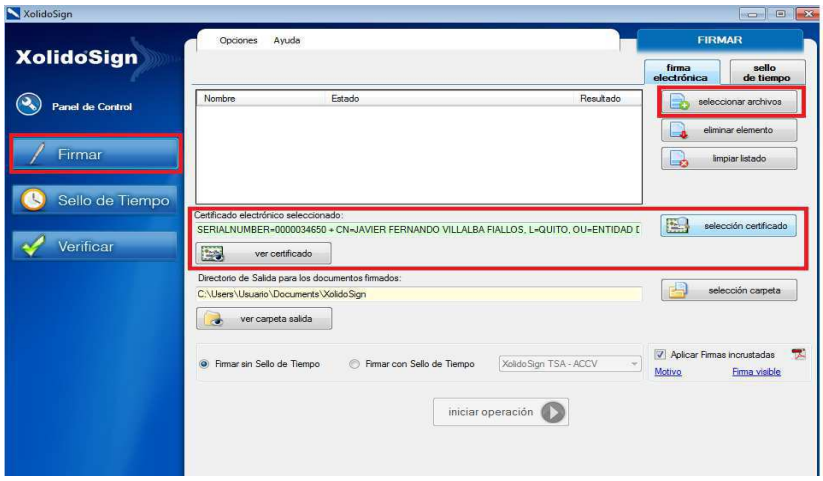


Figura 4.2.4.6.1 Firmar con XolidoSign 1

Para firmar con XolidoSign es necesario importar el certificado digital mediante la opción **Selección Certificado** ya sea con un contenedor USB o en Archivo.

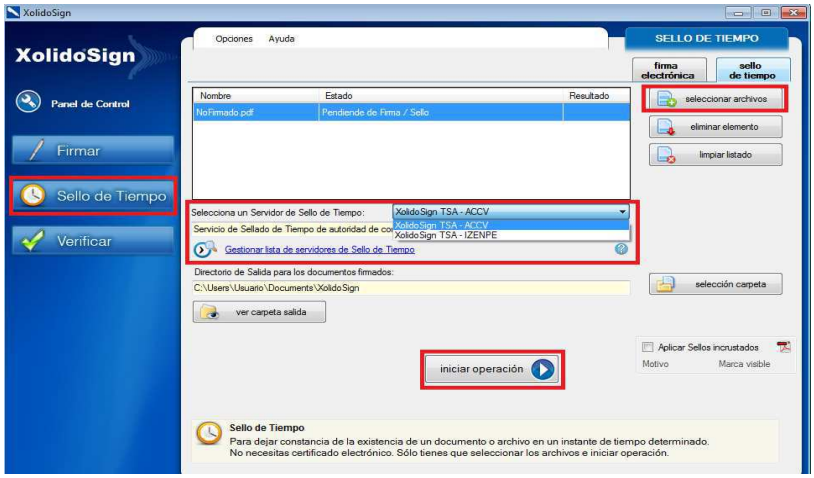


Figura 4.2.4.6.2 Firmar con XolidoSign

Para firmar con sello de tiempo se selecciona los certificados de las TSA con las que dispone XolidoSign, el estampado de tiempo utilizando esta herramienta no tiene ningún costo, a diferencia del Banco Central del Ecuador, en el que se debe solicitar un certificado adicional de Estampado de Tiempo que tiene costo adicional dependiendo del número de solicitudes de estampado que se solicite.

Al hacer clic en **Iniciar Operación** la aplicación procede a firmar el fichero PDF seleccionado incrustando el estampado de tiempo en la firma de manera gratuita.

Figura 4.2.4.6.3 Detalle del documento

En la figura 4.2.21 se visualiza la descripción que indica a quien está dirigido el documento, la fecha de carga y la descripción del contenido, para realizar la comprobación de las firmas que se encuentran en el documento, se selecciona la opción de Firmas Digitales.

La aplicación permite volver verificar las firmas digitales y de Estampado Cronológico en el documento PDF.

Para resolver si el certificado posee TimeStamp, la aplicación lo desplegará mediante indicadores visuales, al seleccionar la firma digital se detallará las características del certificado.

Figura 4.2.4.6.4 Detalle de firma digital

En el atributo **Información TimeStamp** se resolverá si el fichero fue firmado con un certificado correspondiente a una TSA, en caso de aplicar la

condición, se desplegará la cadena de confianza del emisor del certificado de TimeStamp, caso contrario, indicará que se firmó el fichero con la fecha y hora del ordenador local. Se debe tomar en cuenta de que el TimeStamp no asegura la integridad del documento, ni cubre otras firmas digitales en el documento, este estampado es parte de la firma digital aplicada al fichero y garantiza la fecha y hora de la firma. Por medio de esta característica se evita la alteración de la fecha y hora en un equipo cualquiera, debido a que al aplicar el certificado de estampado, la autoridad pertinente se encarga de certificar esta hora, lo que evita que 2 o varios ficheros, sean firmados exactamente en la misma fecha y en la misma hora.

```
308             PdfReader reader = new PdfReader(ruta);
309
310             AcroFields af = reader.getAcroFields();
311
312             // Busqueda de todas las firmas Digitales
313             ArrayList names = af.getSignatureNames();
314             // Para cada Firma electronica:
315             for (int k = 0; k < names.size(); ++k) {
316
317                 String name = (String)names.get(k);
318
319                 InfoFirmaDigital firma= new InfoFirmaDigital(af,name);
320
321                 firmainfo.add(firma);
322
```

Figura 4.2.4.6.5 Código para recorrer firmas digitales en PDF

En la figura se aprecia las variables de tipo que permiten extraer las firmas digitales de un archivo PDF, la variable de tipo **PDFReader** recibe como parámetro el archivo, y la variable de tipo **AcroFields** permite extraer los campos disponibles del fichero PDF, se guarda el identificador de las firmas digitales en el ArrayList y se recorre almacenando los datos de la firma en una lista de objetos de tipo InfoFirmaDigital.

El TimeStamp se lo puede procesar y mostrar en formato de calendario. El estampado al ser certificado por una TSA el posee valores detallados que no posee un calendario que tomo la hora y fecha del equipo local.

Si la firma digital posee timeStamp, la aplicación desplegará la fecha y hora de la firma, además de la cadena de la TSA del certificado de TimeStamp utilizado.

Figura 4.2.4.6.6 Detalle de firmas con TimeStamp

En los detalles de la firma se aprecia que las características de integridad están completas la identidad de la persona que firmo el documento, la revisión que cubre es válida, la fecha y hora de la firma son certificadas por una TSA, la firma cubre todo el documento, es decir, cubre todas las revisiones que contenga el fichero PDF, el certificado utilizado está en el rango de su fecha de vigencia y está comprobada la cadena de confianza del emisor. Por lo que se garantiza que el fichero es integro en todas sus características.

```
            setTimestamp(pk.verifyTimestampImprint());   Verifica si existe TimeStamp
            setFecha_firma(pk.getTimeStampDate().getTime());  Recupera la fecha y hora de la firma
344          System.out.println("nombre sellado de tiempo "  +pk.getTimeStampToken().getSID().getIssuer());
        setTimestampinfo(pk.getTimeStampToken().getSID().getIssuer().toString());  Recupera la cadena del emisor del
346      }                                                                          certificado de TimeStamp
347      else
348      {
            setTimestamp(pk.verifyTimestampImprint());
            setFecha_firma(cal.getTime());
            setTimestampinfo("Fecha y Hora de firma tomada del equipo local");  En caso de no existir TimeStamp se advierte
352          }                                                                      que se uso la hora local del Equipo.
353    } catch (GeneralSecurityException ex) {
354        Logger.getLogger(InfoFirmaDigital.class.getName()).log(Level.SEVERE, null, ex);
355    }
```

Figura 4.2.4.6.7 Código verificador de TimeStamp

Con la validación del fichero PDF completo, queda únicamente verificar si es que el certificado digital con el que fue firmado, se encuentra en listas de revocación de certificados (CRL).

Figura 4.2.4.6.8 Estado de Revocación de Certificado

La verificación se realizará mediante la URL que la ECIBCE pone a disposición para los suscriptores, si es que el número de serie se encuentra en la Lista de Revocación de Certificados entonces se recibirá una cadena que la aplicación procesará para definir el estado del certificado. En caso de que el certificado digital se encuentre en listas de revocación este perderá todo valor jurídico y a su vez exentará al suscriptor de toda obligación y responsabilidad que certificado conlleva.

Espacio en Blanco
Intencional

4.3. Pruebas Funcionales

4.3.1. Ingreso al Sistema

ESCENARIO Nro. 1 Ingreso al Sistema Web, Permisos de Acceso		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios y Socios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Ingresar al Sistema con el respectiva username y contraseña	Validar el ingreso al sistema, y Permisos de Acceso	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
La prueba de ingreso fue exitosa. Se obtuvo los resultados deseados en cuanto a validación de usuario y contraseña, y se desplegaron las alertas correspondientes al momento de ingresar con usuarios no registrados y con contraseñas incorrectas. El sistema validó correctamente el perfil de Acceso de cada usuario, limitando o permitiendo el uso de determinadas funcionalidades.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.2. Módulo de Administración de Usuarios

ESCENARIO Nro. 2 Módulo de Usuarios		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios y Socios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Crear Nuevo Usuario	Ingreso Exitoso	Ok
Actualizar Datos de Usuario, Asignación de Perfil de Seguridad, y Activación de Usuario	Actualización Exitosa (Cumple Condiciones)	Ok
Eliminar Usuario	Eliminado exitoso (Cumple condiciones)	Ok
Buscar Usuario	Exitoso	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se obtuvo los resultados deseados en cuanto a las funciones del módulo, se confirmó que el perfil de seguridad efectivamente limita o autoriza funciones del sistema al usuario.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.3. Módulo de Administración de Socios

ESCENARIO Nro. 3 Módulo de Socios		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios y Socios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Ingreso de Nuevo Socio	Ingreso Exitoso	Ok
Generación de cuenta de usuario al nuevo Socio.	Generación de cuenta de Usuario Exitoso	Ok
Actualizar/Activar Socio	Actualización Exitosa	Ok
Eliminar Socio	Eliminado exitoso	Ok
Buscar Socio	Exitoso	Ok
Cargar Fotografía a Socio	Carga Exitosa	Ok
Asignar Licencia de Conducir	Asignación Exitosa	Ok
Actualizar Licencia de Conducir	Actualización Exitosa	Ok
Indicador de Licencia Caducada	Indicador Visual Exitoso	Ok
Asignar/Retiro de Vehículo a Socio	Asignación y Retiro Exitoso (cumple Condiciones)	Ok
Ver Vehículo de Socio	Exitoso	Ok
Asignar/Retiro de Compañía a Socio	Asignación y Retiro Exitoso (cumple Condiciones)	Ok
Ver Compañía de Socio	Exitoso	Ok
Consultar todos los Socios	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se verificó y se validaron indicadores visuales, datos de vehículos, compañías y licencias, se realizó la verificación de los permisos de acceso y todo se encuentra operando con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.4. Módulo de Administración de Vehículos

ESCENARIO Nro. 4 Módulo de Vehículos		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios y Socios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Ingreso de Nuevo Vehículo	Ingreso Exitoso	Ok
Actualizar Datos y Activación de Vehículo	Actualización Exitosa (Cumple condiciones)	Ok
Eliminar Vehículo	Eliminado exitoso (Cumple condiciones)	Ok
Buscar Vehículo	Consulta Exitosa	Ok
Indicador de caducidad de Matriculo	Indicador Visual Exitoso	Ok
Indicador de Estatus de Actividad del Vehículo	Indicador Visual Exitoso	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se verificaron los datos ingresados, los indicadores visuales de actividad del vehículo y se obtuvieron los resultados esperados, las funciones del módulo están operando con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.5. Módulo de Administración de Compañías

ESCENARIO Nro. 5 Módulo de Compañías		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios y Socios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Ingreso de Nueva Compañía	Ingreso Exitoso	Ok
Actualizar Datos y Activación de Compañía	Actualización Exitosa (Cumple condiciones	Ok
Eliminar Compañía	Eliminado exitoso (Cumple condiciones)	Ok
Buscar Compañía	Exitoso	Ok
Asignar/Retiro de Representante Legal	Asignación y Retiro Exitoso (cumple Condiciones)	Ok
Actualizar Datos y Actividad de Representante	Actualización Exitosa	Ok
Indicadores Visuales de Actividad Compañía	Indicador Visual Exitoso	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se verificó y se validaron indicadores visuales, datos de compañías y representantes, todo se encuentra consistente, se realizó la verificación de los permisos de acceso y todo se encuentra operando con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.6. Módulo de Administración de Perfiles de Seguridad

ESCENARIO Nro. 6 Módulo de Perfiles de Seguridad

Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Crear Nuevo Perfil de Seguridad	Creación Exitosa	Ok
Actualizar Datos Informativos del Perfil	Actualización Exitosa	Ok
Actualizar Permisos de Acceso del Perfil	Actualización Exitosa	Ok
Eliminar Perfil de Seguridad	Eliminado exitoso (Cumple condiciones)	Ok
Consultar Permiso de Acceso	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se verificaron los cambios en los permisos de acceso y se verificó que efectivamente el aplicativo otorga o deniega el acceso a las funcionalidades que se encuentran listadas en la lista de permisos de acceso.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.7. Módulo de Documentos

ESCENARIO Nro. 7 Módulo de Documentos		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Ingreso de Documentos	Ingreso Exitoso	Ok
Verificador de Firma Electrónica	Verificación Exitosa	Ok
Eliminar Documento	Eliminado exitoso (Cumple condiciones)	Ok
Actualizar Datos Básicos de Documentos	Actualización Exitosa	Ok
Indicador de Estatus de Documentos Firmado	Indicador Visual Exitoso	Ok
Consultar Documento	Consulta Exitosa	Ok
Descargar Documento PDF	Descarga Exitosa	Ok
Ver Documento PDF	Vista Exitosa	Ok
Indicadores de Estatus de Firmas Electrónicas	Indicadores Correctos	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se verificaron los documentos cargados en el módulo y se validó los datos de las firmas electrónicas en el mismo (en caso de aplicar). Los datos fueron consistentes. El Módulo opera con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.8. Módulo de Mantenimiento

4.3.8.1. Mantenimiento de Módulo de Socios

ESCENARIO Nro. 8 Módulo de Mantenimiento - Administración del Módulo de Socios		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Administración de Estado de Socio		
Ingreso de Nuevo Estado de Socio	Ingreso Exitoso	Ok
Actualización de Estado de Socio	Actualización Exitosa	Ok
Eliminar Estado de Socio	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Estado de Socio	Consulta exitosa	Ok
Administración de Categoría de Socio		
Ingreso de Nueva Categoría de Socio	Ingreso Exitoso	Ok
Actualización de Categoría de Socio	Actualización Exitosa	Ok
Eliminar Categoría de Socio	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Categoría de Socio	Consulta exitosa	Ok
Administración de Tipo de Licencia de Socio		
Ingreso de Nuevo Tipo de Licencia	Ingreso Exitoso	Ok

Actualización de Tipo de Licencia	Actualización Exitosa	Ok
Eliminar Tipo de Licencia	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Tipo de Licencia	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se Ingresaron nuevos registros de cada caso (Estado, Categoría y Tipo de Licencia)y se verificó que se encuentren disponibles en el módulo de Socios. El módulo opera con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

Espacio en Blanco Intencional

4.3.8.2. Mantenimiento de Módulo de Vehículos

ESCENARIO Nro. 9 Módulo de Mantenimiento - Administración del Módulo de Vehículos		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Administración de Clases de Vehículo		
Ingreso de Nuevo Clase de Vehículo	Ingreso Exitoso	Ok
Actualización de Clase de Vehículo	Actualización Exitosa	Ok
Eliminar Clase de Vehículo	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Clase de Vehículo	Consulta exitosa	Ok
Administración de Colores		
Ingreso de Nuevo Color	Ingreso Exitoso	Ok
Actualización de Color	Actualización Exitosa	Ok
Eliminar Color	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Color	Consulta exitosa	Ok
Administración de Combustible		
Ingreso de Nuevo Combustible	Ingreso Exitoso	Ok
Actualización de Combustible	Actualización Exitosa	Ok
Eliminar Combustible	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Combustible	Consulta exitosa	Ok

Administración de Marca y Modelo de Vehículo		
Ingreso de Nueva Marca	Ingreso Exitoso	Ok
Actualización de Marca	Actualización Exitosa	Ok
Eliminar Marca	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Marca	Consulta exitosa	Ok
Ingreso de Nuevo Modelo	Ingreso Exitoso (Cumple Condiciones)	Ok
Actualización de Modelo	Actualización Exitosa	Ok
Eliminar Modelo	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Modelo	Consulta exitosa	Ok
Administración de Letreros		
Ingreso de Nuevo Letrero	Ingreso Exitoso	Ok
Actualización de Letrero	Actualización Exitosa	Ok
Eliminar Letrero	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Letrero	Consulta exitosa	Ok
Administración de Tipos de Placa		
Ingreso de Nuevo Tipo de Placa	Ingreso Exitoso	Ok
Actualización de Tipo de Placa	Actualización Exitosa	Ok
Eliminar Tipo de Placa	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Tipo de Placa	Consulta exitosa	Ok
Administración de Tipos de Placa		
Ingreso de Nuevo Tipo de Vehículo	Ingreso Exitoso	Ok
Actualización de Tipo de Vehículo	Actualización Exitosa	Ok
Eliminar Tipo de Vehículo	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Tipo de Vehículo	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se realizaron varias pruebas de todos los ítems mencionados en estas pruebas y se pudo apreciar los cambios realizados en el módulo de mantenimiento de vehículos en el propio módulo de Vehículos, los datos fueron consistentes y cumplen las condiciones para su administración. El módulo opera con normalidad		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.8.3. Mantenimiento de Módulo de Documentos

ESCENARIO Nro10 Módulo de Mantenimiento - Administración del Módulo de Documentos		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Administración de Tipos de Oficio		
Ingreso de Nuevo Tipo de Oficio	Ingreso Exitoso	Ok
Actualización de Tipo de Oficio	Actualización Exitosa	Ok
Eliminar Tipo de Oficio	Eliminado exitoso (Cumple Condiciones)	Ok
Consultar Tipo de Oficio	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Las pruebas fueron exitosas. Se Ingresaron nuevos registros de este caso y se verificó que se encuentren disponibles en el módulo de Documentos. El módulo opera con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.9. Módulo de Firma Electrónica

ESCENARIO Nro. 11 Módulo de Firma Electrónica		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Carga de Certificado de Firma Electrónica (Archivo)	Ingreso Exitoso	Ok
Carga de Certificado de Firma Electrónica (Token)	Ingreso Exitoso	Ok
Validar Certificado de Firma Electrónica	Validación Exitosa	Ok
Autorizar / No Autorizar Certificado de Firma Electrónica	Actualización Exitosa	Ok
Consultar Certificado de Firma Electrónica	Consulta exitosa	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Nota: Los certificados no son eliminados, ya que en el caso de existir documentos firmados electrónicamente por un Certificado, los usuarios del sistema deben verificar la identidad del firmante, con eso se garantiza el origen del documento firmado aun tiempo después de que las personas abandonen su cargo. El módulo opera con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

4.3.10. Módulo de Consultas

ESCENARIO Nro12 Módulo de Consultas		
Procedimiento	**Descripción**	**Status**
Pruebas Previas Requeridas:	Ninguna	Ok
Requisitos Funcionales:	Usuarios: Administrador, Usuarios.	Ok
Ambiente Técnico Previo Requerido:	Servidor WEB GlassFish v3.1.2, 2,0GB RAM, 50 GB libre en disco, Windows XP, Windows VISTA, Windows 7, Internet Explorer 9+, Mozilla Firefox 21.0+, Google Chrome 27.0+	Ok
Nota: Las pruebas se realizarán en el browser utilizando las URL: http://www.unatec.org:443/UnatecSoftWS-war/ que direccionará a la aplicación Web o mediante la URL: http://www.unatec.org:3389/Intranet/ que direccionará al Web Site Corporativo.		
Secuencia de la Prueba		
Procedimientos	**Resultados Esperados**	**Status**
Consulta Dinámica de Socios		
Selección de Tabla Socio	Selección Exitosa	Ok
Selección de Tabla Vehículo	Selección Exitosa	Ok
Selección de Tabla Compañía	Selección Exitosa	Ok
Selección de Tabla Licencia	Selección Exitosa	Ok
Consulta Dinámica de Compañías		
Selección de Tabla Compañía	Selección Exitosa	Ok
Selección de Tabla Representante	Selección Exitosa	Ok
Consulta Dinámica de Vehículos		
Selección de Tabla Vehículo	Selección Exitosa	Ok
Selección de Tabla Socio	Selección Exitosa	Ok
Selección de Tabla Matricula	Selección Exitosa	Ok
Consulta de Documentos		
Carga de Documentos	Carga Exitosa	Ok
Indicador de Firmas electrónicas en documentos	Indicadores Exitosos	Ok
Estadísticas		
Categorías de Socios	Estadística Correcta	Ok
Estados de Socios	Estadística Correcta	Ok
Tipos de Licencias	Estadística Correcta	Ok
No. De documentos firmados Electrónicamente	Estadística Correcta	Ok

Exportación de Datos		
Exportación a documento Excel	Exportación Exitosa	Ok
Exportación a documento PDF	Exportación Exitosa	Ok
Carga de Datos		
Consulta de Datos por Columna	Consulta Exitosa	Ok
Filtro de Datos	Filtro Exitoso	Ok
Ordenamiento de Columnas	Ordenamiento Exitoso	Ok
Fallas Encontradas	**Descripción**	**Gravedad**
Ninguna	Ninguna	-
Comentarios Respecto a la Prueba:		
Todas las pruebas dieron un resultado satisfactorio, ya que el usuario supo indicar la facilidad de la herramienta, y que le permitirá extraer y filtrar la información a su necesidad. El usuario quedo extremadamente satisfecho. Las pruebas fueron positivas y se validó que el módulo funcione con normalidad.		
Prueba realizada por: Dina Aracely Aleaga	_____ Firma Usuario	

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1 CONCLUSIONES

Una vez finalizado el proyecto de tesis propuesto, se han obtenido las siguientes conclusiones.

- El crecimiento de la información en las organizaciones o empresas hoy en día es acelerado por lo que se deben disponer de herramientas que permitan disminuir el tiempo de respuesta de consultas mediante el uso de nuevas tecnologías que ayudan a simplificar estos tiempos.

- El Ecuador en el tema del uso de certificados digitales se encuentra con un gran margen de retraso, sin embargo se puede ver en la actualidad que el gobierno, el SRI, e incluso el sector privado se encuentra implementando aplicaciones y servicios que se complementan con el uso de certificados digitales, tanto para la seguridad de la información y para el comercio electrónico, con el que se pueden realizar transacciones utilizando certificados digitales.

- Los estándares en conjunto con la metodología UWE de desarrollo han permitido materializar las ideas de los usuarios funcionales de acuerdo a su necesidad y ha hecho factible en este caso implementar una solución para ellos que les permitirá reducir tiempos de respuesta de consultas, integridad de la información, y principalmente mantener organizado su patrimonio documental.

- El uso de certificados de firma electrónica permite validar varios aspectos de un documento firmado electrónicamente, estos son: Identidad, Integridad, Fecha del Documento, Revisión de documento y Vigencia de

certificado, esto garantiza el no repudio de los documentos firmados electrónicamente y constituye que posean el mismo valor jurídico que un documento firmado de forma manuscrita.

- La implementación del Web Sitefacilitará la consulta de datos para los Socios de la organización y esta a su vez, tendrá como objetivo dar a conocer al País sobre su existencia y sobre los servicios de transporte que ofrece, además que se le ha proporcionado una solución que le permitirá implementar a futuro mejoras conforme a su crecimiento.

- El conocimiento de las leyes, normativas, políticas y regulaciones de los certificados digitales es de suma importancia, ya que en un futuro no tan lejano, y según mi criterio, se implementaran herramientas para que el gobierno y el comercio electrónico sea la primera vía de transacciones y de identificación de Personas Naturales, Jurídicos e incluso funcionarios públicos a nivel nacional e internacional.

5.2 RECOMENDACIONES

La culminación del proyecto ha conllevado a tener varias recomendaciones con respecto a varios temas, entre ellos se tiene los siguientes:

- Se recomienda el mantenimiento y actualización de las herramientas que se implementaron, manteniendo así el óptimo tiempo de respuesta en el manejo de la aplicación WEB.

- Se recomienda la capacitación del personal e incluso de los miembros de la organización, sobre el correcto uso, los beneficios y las obligaciones que poseen el suscriptor y la AC para el manejo de los certificados digitales.

- El uso de las buenas prácticas de desarrollo, entre ellos las anotaciones, comentarios, optimización de código fuente y entre otros facilitan temas como

son; el mantenimiento, control de cambios, migraciones e incluso integraciones con otros sistemas, por lo tanto las buenas prácticas desembocan en el incremento del ciclo de vida del sistema.

- El mal uso de documentos firmados electrónicamente puede conllevar a problemas de carácter legal, ya que el suscriptor debe cumplir con las normas de renovación y revocación de su certificado digital, mantenerlo siempre en vigencia y conocer los procedimientos para revocarlo en caso de que se requiera, como por ejemplo evitar que un funcionario público siga haciendo uso de su certificado digital a pesar de la cesación de sus funciones en la organización.

- Para facilitar a los usuarios, el correcto funcionamiento del aplicativo WEB en los diferentes sistemas operativos; se recomienda mantener actualizado los exploradores a sus versiones más recientes, y así evitar un mal funcionamiento del aplicativo.

- Se recomienda actualizar los conocimientos brindados a los Socios de la organización, sobre el tema de la firma electrónica para en un futuro tener bases de conocimiento en caso de nuevas implementaciones y proyectos que conlleven el uso de certificados digitales.

BIBLIOGRAFÍA

Ley de Comercio Exterio, Registro of (2002).

Ley de Comercio Exterior, Decreto Ejecutivo 3496 (Registro Oficial 735 2002).

Ley de Comercio Exterior (Decreto Ejecutivo 3496 ed.). (2002). Quito: Registro Oficial 735.

Busch, M., & Koch, N. (24 de Junio de 2009). Obtenido de UWE – UML-based Web Engineering: http://www.pst.ifi.lmu.de/personen/kochn/presentations/busch_MagicUWE_icwe2009.pdf

Entidad de Certificación de Información. (s.f.). Recuperado el 10 de 11 de 2012, de Banco Central del Ecuador: http://www.eci.bce.ec/c/document_library/get_file?uuid=911072aa-6647-4a0b-b03e-447a13d00bab&groupId=10155

Entidad de Certificación de Información. (s.f.). Recuperado el 4 de Marzo de 2013, de Banco Central del Ecuador: http://www.eci.bce.ec/web/guest/estampado-de-tiempo

Entidad de Certificación de Información. (s.f.). Recuperado el 10 de Noviembre de 2012, de Banco Central del Ecuador: http://www.eci.bce.ec/c/document_library/get_file?uuid=1e2b063c-ca7f-48fe-b330-e4af597b845c&groupId=10155

Entidad de Certificación de Información. (s.f.). *Banco Central del Ecuador*. Recuperado el 07 de 2013, de http://www.eci.bce.ec/documents/10155/34572/modeloContratoPersonaNatural.pdf

Koch, N. (3 de Junio de 2010). Obtenido de UWE – UML-based Web Engineering: http://www.pst.ifi.lmu.de/personen/kochn/presentations/UWE_03062010_almeria.pdf

Teknoloji, P. (3 de Septiembre de 2012). Obtenido de Prime Faces: primefaces.googlecode.com/files/primefaces_users_guide_3_4.pdf

Text Software Corp. (2 de Agosto de 2012). Obtenido de iTextPdf: http://stackoverflow.com/questions/tagged/itext

The Legion of the Bouncy Castle. (s.f.). Recuperado el 4 de Septiembre de 2012, de Bouncy Castle: http://www.bouncycastle.org/documentation.html

Universidad Complutense de Madrid. (22 de Octubre de 2008). Recuperado el 10 de Julio de 2012, de Facultad de Informática: http://www.fdi.ucm.es/profesor/gmendez/docs/is0809/ieee830.PDF

Tabla 4.2.2.1 Estructura del Certificado Digital de Firma Electrónica

Campo	Descripción	Valor
Serial Number	Número que identifica unívocamente al certificado	Número de serie del certificado
Algoritmo de firma	Algoritmo utilizado por la ECIBCE para firmar el certificado	sha256RSA
Emisor (issuer)	CN (CommonName)	AC BANCO CENTRAL DEL ECUADOR
	L (Localidad)	QUITO
	OU (OrganizationalUnit.)	ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN-ECIBCE
	O (Organization)	BANCO CENTRAL DEL ECUADOR
	C (Country)	EC

Fuente: Banco Central del Ecuador, Entidad de Certificación de Información, Estructura de Certificado Digital de Firma Electrónica, Junio del 2010, Nueva Infraestructura de Certificados digitales del Banco Central

HOJA DE LEGALIZACIÓN DE FIRMAS

Elaborado por:

_____

Javier Villalba

DIRECTOR DE LA CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

_____

Ing. Mauricio Campaña