ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA DE INGENIERÍA EN SISTEMAS E INFORMÁTICA

TESIS PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA

TEMA: DESARROLLO DE UN BUZÓN DE DOCUMENTOS PARA LOS PROCESOS DEL CONSEJO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE UTILIZANDO FIRMA DIGITAL Y SELLADO DE TIEMPO

AUTOR: BRYAN VÁSQUEZ

DIRECTOR: ING. RON, MARIO

CODIRECTORA: ING. RUIZ, JENNY

SANGOLQUÍ

JUNIO 2015

CERTIFICADO

Ing. Mario Ron

Ing. Jenny Ruiz

CERTIFICAN

Que el trabajo titulado "DESARROLLO DE UN BUZÓN DE DOCUMENTOS PARA LOS PROCESOS DEL CONSEJO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE UTILIZANDO FIRMA DIGITAL Y SELLADO DE TIEMPO" realizado por el Sr. BRYAN FABRICIO VÁSQUEZ GARCÍA, ha sido guiado y revisado periódicamente y cumple normas estatuarias establecidas de la Universidad de las Fuerzas Armadas-ESPE.

Sangolquí, mayo del 2015

Ing. Mario Ron
DIRECTOR

Ing. Jenny Ruiz
CODIRECTOR

DECLARACIÓN DE RESPONSABILIDAD

BRYAN FABRICIO VÁSQUEZ GARCÍA

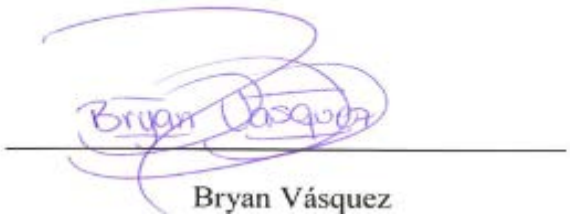
DECLARO QUE:

El proyecto de grado denominado "DESARROLLO DE UN BUZÓN DE DOCUMENTOS PARA LOS PROCESOS DEL CONSEJO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE UTILIZANDO FIRMA DIGITAL Y SELLADO DE TIEMPO", ha sido desarrollado con base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan el pie de las páginas correspondiente, cuyas fuentes se incorporan en la bibliografía.

Consecuentemente este trabajo es mi autoría.

En virtud de esta declaración, me responsabilizo del contenido, veracidad y alcance científico del proyecto de grado en mención.

Sangolquí, mayo del 2015



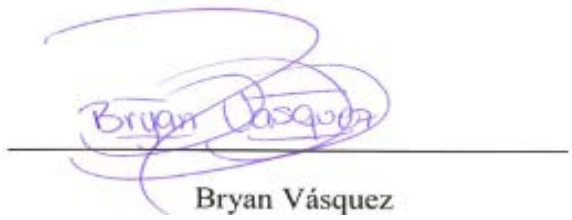
Bryan Vásquez

AUTORIZACIÓN

Yo, BRYAN FABRICIO VÁSQUEZ GARCÍA

Autorizo a la UNIVERSIDAD DE LA FUERZAS ARMADAS-ESPE, la publicación, en la biblioteca virtual de la Institución del trabajo "DESARROLLO DE UN BUZÓN DE DOCUMENTOS PARA LOS PROCESOS DEL CONSEJO DE DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN DE LA UNIVERSIDAD DE LAS FUERZAS ARMADAS ESPE UTILIZANDO FIRMA DIGITAL Y SELLADO DE TIEMPO", cuyo contenido, ideas y criterios son de mi exclusiva responsabilidad y autoría.

Sangolquí, mayo del 2015



Bryan Vásquez

DEDICATORIA

Dedico esta tesis de grado a mis padres Eduardo e Inés cuyo sacrificio me ha brindado lo necesario para convertirme en la persona que soy ahora, por haberme preparado para los retos del día a día, por estar conmigo siempre en los buenos y malos momentos, a mi hermana Nicole que a la distancia ha estado a mi lado brindándome su apoyo constante, a mis familiares que me han apoyado con la motivación para no decaer en este largo camino hacia el éxito, a mis maestros que han compartido su conocimiento y experiencias y a mis amigos por hacerme conocer la perseverancia y valores para superar los obstáculos de la vida.

Bryan Vásquez

AGRADECIMIENTO

Agradezco a la Universidad de las Fuerzas Armadas ESPE por haberme brindado el conocimiento, al Director Ing. Mario Ron y Codirectora Ing. Jenny Ruiz, por haber sido la guía en este camino, a mis familiares que me enseñaron a nunca dejar de soñar, por el sacrificio realizado y por la confianza brindada para alcanzar este logro, a mis amigos y colegas que siempre me permitieron seguir adelante. Les estoy eternamente agradecido.

Bryan Vásquez

ÍNDICE DE CONTENIDO

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

LISTADO DE ANEXOS

RESUMEN

El proyecto “Desarrollo de un Buzón de Documentos para los procesos del Consejo de Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE utilizando firma digital y sellado de tiempo”, el cual se encuentra enfocado en las nuevas tecnologías solventa el inconveniente del almacenamiento físico de los documentos mediante un repositorio en el cual se almacenan los documentos firmados electrónicamente mediante un certificado digital el cual es provisto por una Autoridad de Certificación (AC) en Ecuador dando la misma validez legal que un archivo físico, para este proyecto es ANF AC Ecuador utilizando las herramientas necesarias que permitan el uso correcto del dispositivo de firma digital, con este buzón el usuario puede acceder a los documentos desde cualquier ordenador que tenga conexión a internet. El proyecto fue desarrollado mediante la metodología ágil SCRUM la cual permite que el usuario se encuentre involucrado en el avance del sistema y entregas parciales y funcionales de este. El sistema fue desarrollado en el lenguaje de programación JAVA utilizando herramientas como: Hibernate, Primefaces, y Java Server Faces con el paradigma orientado a objetos y la arquitectura de software MVC. Se utilizó el sistema operativo CentOS en dos servidores uno de aplicación y uno de base de datos usando Apache Tomcat como servidor de aplicaciones y MySQL como gestor de base de datos respectivamente.

PALABRAS CLAVE:

- **AUTORIDAD DE CERTIFICACIÓN**
- **SCRUM**
- **TOKEN**
- **CERTIFICADO**
- **FIRMA ELECTRÓNICA**

ABSTRACT

The project "Development of a document box for the processes of the Council of Department of Computer Science at the University of the Armed Forces ESPE using digital signature and time stamp ", which is focused on new technology overcomes the disadvantage physical storage of documents using a repository in which the signed documents are stored electronically using a digital certificate which is provided by an Aurhority of Certification (AC) in Ecuador giving the same legal validity as a physical file for this project is ANF AC Ecuador using the tools that allow the proper use of digital signature device with this mailbox user can access documents from any computer with internet access. The project was developed using agile methodology SCRUM which allows the user is involved in the advancement of partial and functional system of this delivery. The system was developed in the Java programming language using tools such as Hibernate, Primefaces, and Java Server Faces with the object-oriented paradigm MVC architecture and software. The CentOS operating system used one of two application servers and one database using Apache Tomcat as the application server and MySQL as a database manager respectively.

KEYWORDS:

- **AUTHORITY OF CERTIFICATION**
- **SCRUM**
- **TOKEN**
- **CERTIFICATE**
- **DIGITAL SIGNATURE**

CAPÍTULO 1

GENERALIDADES

1.1. INTRODUCCIÓN

Con el avance de la tecnología actual, se busca a mejorar y automatizar los procesos de negocio de las organizaciones para poder ser más eficientes y de esta manera optimizar recursos y el funcionamiento a través del uso de nuevas herramientas que faciliten esta tarea.

El Internet ha permitido realizar intercambios de información con mayor rapidez, ya que este intercambio de información a través de medios electrónicos ofrece beneficios como ahorro de tinta, papel, almacenamiento y mensajería, además nos evita trasladarnos y porque no considerar que nos ahorre hacer filas.

En ese contexto la firma digital nace de manera justificable desde el momento en que los contratos, las transacciones económicas, las compras o cualquier acto traslativo de dominio entre otras figuras jurídicas de igual importancia, se realizan on-line, es decir sin la presencia física de las partes; por ello los mensajes de datos que ostenta una firma electrónica, tiene el mismo efecto que un documento con una firma autógrafa.

Un punto muy importante acerca de este tema es la seguridad y la garantía que se dé a los usuarios de estas herramientas para poder dar una garantía jurídica de todas las transacciones que se realizan en línea, por lo que se hace necesario el uso de firma electrónica y además que el certificado con el cual se realizó esta firma este avalado por una Autoridad de Certificación.

1.2. PLANTEAMIENTO DEL PROBLEMA

Actualmente la gran cantidad de documentos físicos que maneja el consejo de departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE ocasiona varios problemas: perdida de documentos, alteración de los

mismos, que estos no lleguen a su lugar de destino, el espacio físico se reduce considerablemente en las oficinas y la localización de estos se vuelve complicada, lo cual retrasa significativamente los procesos que se realizan, por lo que cada día se buscan soluciones al trabajo con papel.

1.3. JUSTIFICACIÓN

Con la emisión del certificado de firma digital existe la necesidad de la creación de los documentos mediante una interfaz rápida y fácil de manejar para que estos sean firmados.

La información es uno de los factores más importantes que manejan las organizaciones, se debe buscar métodos que permitan organizar y gestionar la misma, por lo que todos buscan una herramienta que facilita y permita resolver las necesidades, manteniendo una seguridad jurídica.

El manejo de las nuevas tecnologías permite la facilidad de manejar las transacciones del día a día, entre estas tecnologías tenemos la firma digital con la cual podemos tener seguridad al igual que en los medios físicos.

1.4. OBJETIVOS

1.4.1. Objetivo General

Desarrollar un buzón para los procesos del Consejo de Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE utilizando firma digital y sellado de tiempo.

1.4.2. Objetivos Específicos

- Especificar los requerimientos del sistema funcionales y no funcionales
- Diseñar la estructura y arquitectura del sistema a través de diagramas para describir sus elementos y comportamiento.
- Diseñar y desarrollar la aplicación web utilizando la tecnología establecida en los diagramas que se obtienen en la fase de diseño según los requerimientos obtenidos.
- Realizar las pruebas respectivas para validar la funcionalidad de la aplicación.

1.5. ALCANCE

El sistema permitirá almacenar los documentos generados y firmados en un repositorio de estos, lo cual permitirá su fácil acceso y alta disponibilidad de éstos, se permitirá la firma de estos documentos mediante un token o certificado de firma electrónica la cual garantizará la validez de este documento, para lo cual se diseñará y construirá una base de datos con la información necesaria para el manejo de los archivos y usuarios que manejen esta aplicación.

El sistema será totalmente compatible con la tecnología de firmado electrónico, es decir, con los tokens o certificados utilizados para realizar el firmado electrónico, la plataforma de firmado (servidores TSU (*Time-stamp Unit*)).

El sistema contará con una interfaz web, que permitirá la generación de documentos, la misma que incluye funcionalidades como la de visualización, guardado y envío de los mismos.

Los usuarios podrán ver los documentos enviados, recibidos y guardados, cumpliendo con la garantía de que estos lleguen a su lugar de destino y que sean válidos debido a la firma digital que se haya realizado.

En la metodología utilizada, se establece que las fases de desarrollo de la misma llegan hasta el mantenimiento, para el desarrollo de esta aplicación no se realizará una implantación real del sistema.

No se entregarán las APIs de firma de la autoridad certificadora que para el desarrollo de ésta tesis es ANF.

1.6. DESCRIPCIÓN DE MÓDULOS

1.6.1. Módulo de Persistencia

Se encarga de la construcción de las clases generadas a partir de las entidades de la base de datos a través de Hibernate y el de los métodos DAO (Data Access

Object) que permiten las transacciones con la base de datos del sistema y realizar las consultas a la base de datos que se generará.

1.6.2. Módulo de Usuarios

Este módulo abarca toda la gestión de usuarios, como es creación, validación de datos, actualización y eliminación de datos relacionados con el usuario del sistema. Se incluye en este módulo el manejo de perfiles y acceso a la información controlada de acuerdo a los permisos asignados a cada perfil.

1.6.3. Módulo Documental

Este módulo es el encargado de la administración de los documentos que serán realizados por los miembros del consejo de departamento en el cual se controlará el almacenamiento y envío de los archivos.

1.6.4. Módulo Presentación

Este módulo comprende a la creación de las páginas web del Sistema y las clases que manejan dichas páginas con el framework JSF (Java Server Faces) utilizando componentes de Primefaces.

1.7. Módulo de Firma

Este módulo comprende el uso del certificado de firma electrónica y realizar las firmas en los documentos generados con el sello de tiempo, el sistema no firmará los documentos, los archivos se firmarán con la aplicación Plug & Sign de la Autoridad de Certificación ANF AC.

CAPÍTULO 2

MARCO TEÓRICO

2.1. INFRAESTRUCTURA DE CLAVE PÚBLICA

La infraestructura de clave pública (PKI) es un conjunto de personas, políticas, procedimientos, hardware y software los cuales son usados para que los certificados y la firma electrónica tengan seguridad jurídica ya que estos recaen bajo la responsabilidad de un usuario. (Díaz F. , 2010)

También puede definirse "como el conjunto de hardware, software, personas, políticas y procedimientos necesarios para crear, gestionar, almacenar, distribuir y revocar certificados digitales basados en criptografía de clave pública" (Navarro, 2015)

Figura 1 Infraestructura de Clave Pública

Fuente (Díaz, 2010)

2.2. AUTORIDAD DE CERTIFICACIÓN

Es la organización que administra y proporciona la base de confianza de la PKI, está entidad asume la responsabilidad de todos los procedimientos pese a que puede utilizar a otras entidades para gestionar la plataforma de certificación. (Díaz F. , 2010)

Asegura la identidad de los usuarios que poseen certificados digitales, "confiando en la Firma Digital de la Autoridad Certificadora, puede confiarse en cualquier certificado generado por la misma." (EcuRed, 2015)

2.2.1. Tipos de Autoridad de Certificación

2.2.1.1. Autoridad de Certificación de Primer Nivel

Administran un sistema abierto de certificación electrónica, interviene en el uso, la emisión del certificado y determina:

- Vigencia del certificado
- Importe de las operaciones
- Servicio de sellado de tiempo
- Comprobante de autorización
- Asume la responsabilidad de los dispositivos emitidos

2.2.1.2. Autoridad de Certificación de Segundo Nivel

Estas Autoridades de Certificación se dedican únicamente a la emisión de los certificados electrónicos y no asumen responsabilidad del uso de que se la da a éste.

- No permite delimitar la capacidad del uso del certificado
- No puede impedir el uso de certificados que hayan sido revocados
- Verifican el estado del certificado electrónico después de haber realizado la firma

2.2.1.3. Autoridad de Certificación de Tercer Nivel

Estas poseen las mismas características de las autoridades de segundo nivel, pero con la lista de certificados revocados solo son accesibles por las personas suscriptoras y suelen incluir en sus políticas de certificación el apercibimiento de que se trata de un sistema de certificación cerrado y solo autorizado para su grupo de usuarios.

2.2.1.4. Autoridad de Certificación de Cuarto Nivel

Administran un modelo de certificación orientado a la seguridad técnica de las transacciones electrónicas, no asumen el objetivo de garantizar seguridad jurídica tampoco asumen la responsabilidad legal por las identificaciones que expiden. (Díaz F. , 2010)

2.2.2. Autoridades de Certificación en Ecuador

En Ecuador existen tres Autoridades de Certificación

2.2.2.1. ANF AC

Figura 2 ANF Authority of Certification

Fuente (ANF AC, 2015)

"Nace en el seno de la Asociación Nacional de Fabricantes, organización sin ánimo de lucro fundada en 1981. Dedicada a la defensa jurídica e institucional de sus asociados, entre los que se encuentran las primeras empresas nacionales y multinacionales del sector agroalimentario." (XolidoSign, 2015)

En Ecuador es la única Autoridad de Certificación que posee el Sello de tiempo el cual es validado por Instituto Oceanográfico de la Armada INOCAR.

2.2.2.2. Banco Central del Ecuador

Figura 3 Banco Central del Ecuador

Fuente (Banco Central, 2015)

"ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS (ECIBCE).- El Banco Central del Ecuador es la Entidad de Certificación de Información acreditada por el Consejo Nacional de

Telecomunicaciones, mediante Resolución 481-20-CONATEL-2008 de 8 de octubre de 2008 y acto administrativo suscrito el 6 de noviembre de 2008.” (XolidoSign, 2015)

2.2.2.3. Security Data

Figura 4 Security Data

Fuente (Security Data, 2015)

“Security Data Seguridad en Datos y Firma Digital S.A. es una Entidad Certificadora de firma electrónica y servicios relacionados autorizada por el CONATEL según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.” (XolidoSign, 2015)

2.3. POLÍTICAS DE CERTIFICACIÓN Y DE FIRMA ELECTRÓNICA

Es un documento en el cual se encuentran todas las “directrices y normas técnicas las cuales son aplicables al uso de certificados y generación de firmas electrónicas” (Díaz F. , 2010) además provee una validación como evidencia legal y especifica un conjunto de criterios comunes de interoperabilidad de esta manera define las reglas y las obligaciones de los actores involucrados en dichos procesos.

Detalla los formatos de firma electrónica admitidos, especifica todo lo que el firmante incluye al momento de realizar el proceso de firma, también la información que se comprueba al momento de realizar la validación de la firma electrónica.

Presenta una estructura que se encuentra normada por estándares técnicos facilitando la interoperabilidad, además describe el alcance de la firma con el uso al que se encuentra permitido.

2.4. CERTIFICADO ELECTRÓNICO

Conocido también por el nombre de: Certificado digital o Certificado de clave pública. Es un acta de datos firmada electrónicamente y por lo tanto infalsificable, equivale a la cédula de identidad ya que posibilita la autenticación de las personas que

poseen uno mediante la acreditación de que este se encuentra en su posesión y en disposición de que este puede usar la clave que se encuentra asociada al certificado. (Díaz F. , 2010)

El objetivo principal del certificado digital es determinar la identidad del propietario de las claves de firma electrónica.

- El certificado tiene que contener la información necesaria para identificar al firmante.
- La clave pública tiene que estar asociada a una persona de forma indudable.
- Se tiene que garantizar que el usuario se encuentra en posesión del certificado y en disposición de utilizar la clave privada.

2.5. FUNCIONES HASH

Estos algoritmos son utilizados para que los mensajes que se han generado garanticen su autenticidad, estas funciones también son conocidas con el nombre de funciones de resumen de mensajes

Transforman todo un bloque de datos en una longitud de cadena fija, una pequeña modificación en esta cadena puede ocasionar grandes cambios en el mensaje original. Las propiedades de un algoritmo HASH son:

- Son algoritmos de una sola vía.
- Es imposible crear dos documentos que generen el mismo valor hash.
- La más mínima modificación en el documento original genera otro valor hash.

Algoritmos HASH más utilizados

- MD5
- SHA1
- SHA256
- SHA512
- SHA384

(Díaz F. , 2010)

2.6. CRL (Certificate Revocation List - Lista de Revocación de Certificados)

Aquí se encuentran las listas de certificados que han sido revocados antes de tiempo, la autoridad certificadora es la responsable de incluir o no el certificado en la lista de revocación. (Díaz F. , 2010)

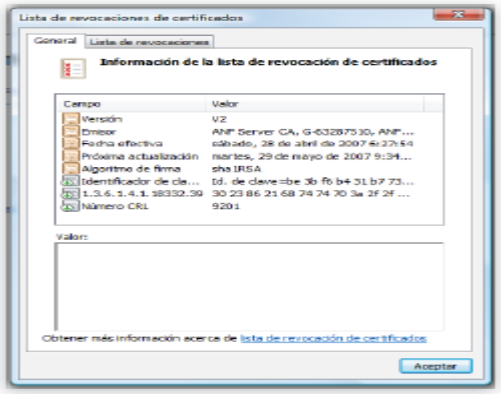


Figura 5 Lista de Revocación de Certificados

Fuente (Díaz F. , 2010)

2.7. SERVICIO OSCP (Online Certificate Status Protocol)

Permite determinar la vigencia del certificado digital realizando una consulta a los servidores de confianza que tiene una Autoridad de Validación, estos son conocidos como OSCP Responder. (Díaz F. , 2010)

Los repositorios a los que se acceden tienen que estar actualizados constantemente ya que las respuestas deben ser rápidas a los usuarios, en el caso de ANF AC se almacenan adicionalmente las consultas realizadas a los servidores de confianza.

2.8. SELLO DE TIEMPO

Es una marca de tiempo la cual necesita de ciertos atributos para que pueda ser una evidencia legal:

- Garantizar la certeza de la fecha que se ha colocado, es decir, que la fuente de tiempo debe ser fiable en el Ecuador esta fuente es el INOCAR.
- Garantizar que los datos que se encuentran asociados a esa fecha no han sufrido algún tipo de variación.
- Garantizar que el método que se utilizó para estampar la fecha no posibilite modificar la esta.

- Determinar la entidad de confianza que emitió el sello de tiempo

(Díaz F. , 2010)

2.9. PROCEDIMIENTO PARA REALIZAR LA FIRMA ELECTRÓNICA

Sobre un determinado conjunto de datos, estos pueden ser el documento original o el hash del documento se aplican los datos de generación de firma es decir que se cifra con la clave privada utilizando algoritmos de firma por ejemplo RSA, el cual asocia el certificado electrónico de la que persona que firma o firmante al cifrado resultante.

Entre los atributos que se tienen que colocar a la firma se encuentran:

- Datos de identificación del dispositivo de creación de firma.
- Políticas de Firma Electrónica a la que está sometida la firma.

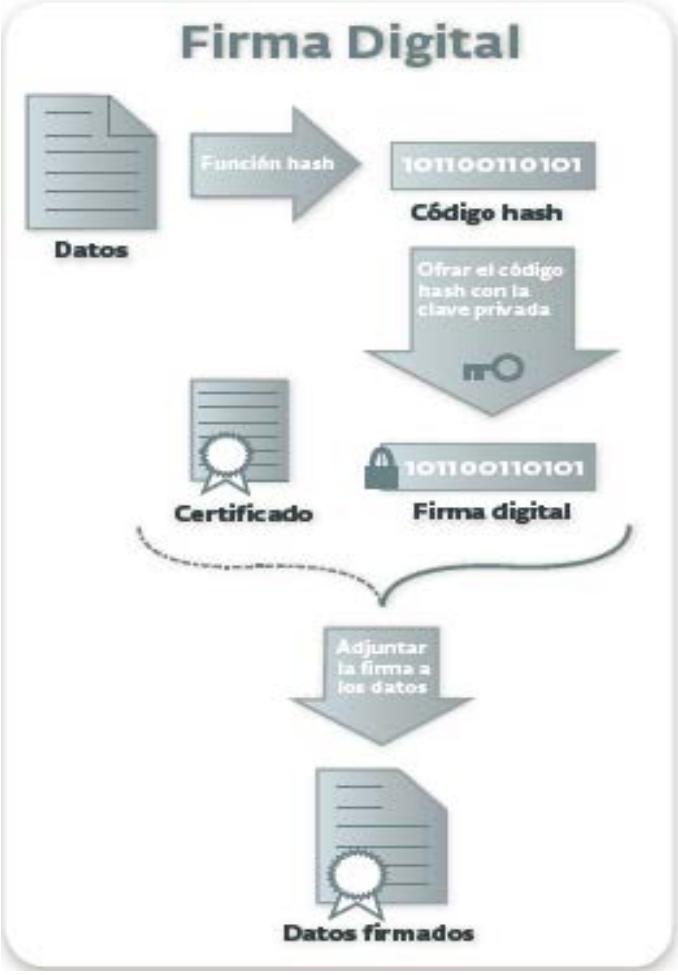


Figura 6 Procedimiento para realizar una firma electrónica

Fuente (Díaz F. , 2010)

2.10. FORMATOS DE FIRMA ELECTRÓNICA

2.10.1. PKCS#7/CMS

Es uno de los principales formatos más extendidos, se trata de un formato de encapsulamiento codificado en ASN-1, permite incluir diferentes firmantes en la firma bajo dos modalidades: mancomunada y encadenada, 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 del formato.
- Tipo de algoritmo hash: SHA2, SHA1, SHA0, MD5.

Información del contenido

- Tipo de contenido: Data

Contenido: Documento a firmar

- Certificado: Certificado del firmante y de toda la cadena
- CRL donde verificar la revocación

Información del firmante

- Versión
- Identificación
  - Emisor del Certificado
  - Número de serie del certificado
- Tipo de algoritmo hash: SHA1
- Atributos autenticados (firmados):
  - Tipo de contenido: Valor fijo (DATA)
  - Certificado del firmante
  - Fecha y hora de la firma
  - Hash del mensaje
  - Política de la firma

- Atributos no firmados (contador de firmas, cargo del emisor, número de firmas, localización, razón, etc.)
- Tipo de algoritmo de firma: RSA o DSA
- Firma digital: PKCS#1

CAdES(CMS Advanced Electronic Signature), ETSI TS 10173

2.10.2. XML DSIG

Es el formato de mayor expansión, es usado frecuentemente en aplicaciones on-line, funcionalmente y estructuralmente al CMS pero la codificación original de firmas y también de los certificados se realiza en B64, ésta posee tres modos de firma:

- **Enveloped:** La firma se añade al final del documento como un elemento extra del archivo de esta manera se firma todo lo inmediatamente anterior al documento
- **Envoloping:** El documento se incluye dentro de la firma en la que se referencia lo firmado de esta manera se puede firmar todo el documento o partes de éste.
- **Detached:** La firma y el documento se encuentran en dos archivos diferentes, la dirección (URL) del documento se encuentra en la propia firma.

2.10.3. MODELO PDF

Es una integración del modelo PKCS#7/CMS con las siguientes características:

- Firma y validación con Acrobat Reader.
- Personalización de la razón de la firma y de una imagen personalizada.
- Incorporación de CRL / OSCP, sello de tiempo y cadena de certificados.
- Firmas visibles / invisibles.
- Integración con el repositorio de confianza de Windows.
- Firma de solo campos seleccionados.

PAdES (PDF Advanced Electronic Signature) ETSI TS 102 778

(Díaz F. , 2010)

2.11. USOS DE LA FIRMA ELECTRÓNICA

La firma electrónica nos permite realizar diferentes tipos de transacciones entre las cuales se destacan:

- Compras publicas
- Tramites ciudadanos
- Gestión documental
- Balances electrónicos
- Comercio electrónico
- Facturación electrónica

(ANALUISA, 2015)

2.12. LEY DE COMERCIO ELECTRÓNICO

"REGLAMENTO GENERAL A LA LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS.

Art. 1.- Incorporación de archivos o mensajes adjuntos.- La incorporación por remisión a que se refiere el artículo 3 de la Ley 67, incluye archivos y mensajes incorporados por remisión o como anexo en un mensaje de datos y a cuyo contenido se accede indirectamente a partir de un enlace electrónico directo incluido en el mismo mensaje de datos y que forma parte del mismo.

La aceptación que hacen las partes del contenido por remisión deberá ser expresada a través de un mensaje de datos que determine inequívocamente tal aceptación. En el caso de contenido incorporado por remisión a través de un enlace electrónico, no podrá ser dinámico ni variable y por tanto la aceptación expresa de las partes se refiere exclusivamente al contenido accesible a través del enlace electrónico al momento de recepción del mensaje de datos.

En las relaciones con consumidores, es responsabilidad del proveedor asegurar la disponibilidad de los remitidos o anexos para que sean accedidos por un medio aceptable para el consumidor cuando éste lo requiera. En las relaciones de otro tipo las partes podrán acordar la forma y accesibilidad de los anexos y remitidos.

Los anexos o remisiones referidas a garantías, derechos, obligaciones o información al consumidor deberán observar lo establecido en la Ley Orgánica de Defensa del Consumidor y su reglamento.

Toda modificación a un anexo o remitido en un mensaje de datos se comunicará al receptor del mismo, a través de un mensaje de datos o por escrito, resaltando las diferencias entre el texto original y el modificado. En el texto modificado se deberá incluir en lugar visible y claramente accesible un enlace al contenido anterior. La comunicación al consumidor acerca de modificaciones no constituye indicación de aceptación de las mismas por su parte. Dicha aceptación deberá ser expresa y remitida por cualquier medio, ya sea éste físico o electrónico.

Cuando las leyes así lo determinen, cierto tipo de información deberá estar directamente incluida en el mensaje de datos y no como anexo o remitido.

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.

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

Ha sido generada y puede ser almacenada en un lenguaje electrónico/informático y formato entendibles 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; y, 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.

Art.4.-Información original y copias certificadas.- Los mensajes de datos y los documentos desmaterializados, cuando las leyes así lo determinen y de acuerdo al caso, deberán ser certificados ante un Notario, autoridad competente o persona autorizada a través de la respectiva firma electrónica, mecanismo o procedimiento autorizado.

Los documentos desmaterializados se considerarán, para todos los efectos, copia idéntica del documento físico a partir del cual se generaron y deberán contener adicionalmente la indicación de que son desmaterializados o copia electrónica de un documento físico. Se emplearán y tendrán los mismos efectos que las copias impresas certificadas por autoridad competente.

Art.5.-Desmaterialización.- El acuerdo expreso para desmaterializar documentos deberá constar en un documento físico o electrónico con las firmas de las partes aceptando tal desmaterialización y confirmando que el documento original y el documento desmaterializado son idénticos. En caso que las partes lo acuerden o la ley lo exija, las partes acudirán ante Notario o autoridad competente para que certifique electrónicamente que el documento desmaterializado corresponde al documento original que se acuerda desmaterializar. Esta certificación electrónica se la realiza a través de la respectiva firma electrónica del Notario o autoridad competente.

Los documentos desmaterializados deberán señalar que se trata de la desmaterialización del documento original. Este señalamiento se constituye en la única diferencia que el documento desmaterializado tendrá con el documento original.

En el caso de documentos que contengan obligaciones, se entiende que tanto el documento original como el desmaterializado son la expresión de un mismo acuerdo de las partes intervinientes y por tanto, no existe duplicación de obligaciones. De existir multiplicidad de documentos desmaterializados y originales, con la misma información u obligación, se entenderá que se trata del mismo, salvo prueba en contrario.

La desmaterialización de los documentos de identificación personal estará sujeta a las disposiciones especiales y procedimiento que las entidades competentes determinen.

Art.6.-Integridad de un mensaje de datos.- La consideración de integridad de un mensaje de datos, establecida en el inciso segundo del artículo 7 de la Ley 67, se cumple si dicho mensaje de datos está firmado electrónicamente. El encabezado o la información adicional en un mensaje de datos que contenga exclusivamente información técnica relativa al envío o recepción del mensaje de datos, y que no altere en forma alguna su contenido, no constituye parte sustancial de la información.

Para efectos del presente artículo, se considerará que la información consignada en un mensaje de datos es íntegra, si ésta ha permanecido completa e inalterada, salvo la adición de algún cambio que sea inherente al proceso de comunicación, archivo o presentación.

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.

El aviso de un posible riesgo sobre la vulnerabilidad o inseguridad de una firma, su certificado o el mensaje de datos y los anexos relacionados podrá ser realizado por el titular de los mismos, mediante cualquier tipo de advertencia que permita, de manera inequívoca a quien realiza la verificación o recibe un mensaje de datos, tomar las precauciones necesarias para evitar perjuicios y prevenir fallas de seguridad. Este aviso deberá ser realizado antes de iniciar cualquier proceso de transacción comercial negociación, o contratación electrónica.

De acuerdo a las leyes, se podrá recurrir a peritos para determinar la procedencia y otro tipo de relaciones de un mensaje de datos con quien lo remite de modo directo o indirecto.

Art.8.-Responsabilidad por el contenido de los mensajes de datos.- (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- La prestación de servicios electrónicos de cualquier tipo por parte de terceros, relacionados con envío y recepción de comunicaciones electrónicas, alojamiento de bases de datos, registro electrónico de datos, alojamiento de sitios en medios electrónicos o servicios similares o relacionados, no implica responsabilidad sobre el contenido de los mensajes de datos por parte de quien presta estos servicios, siendo la responsabilidad exclusivamente del propietario de la información.

De acuerdo a la ley y por orden de la autoridad competente, el órgano regulador podrá ordenar la suspensión del acceso a cualquier información en redes electrónicas que se declare ilegal y/o que atente contra las leyes o la seguridad nacionales. El proveedor de servicios electrónicos deberá cumplir con la orden de suspender el acceso al contenido en forma inmediata, y en caso de no hacerlo será sancionado con sujeción a la ley por el CONATEL.

Art.9.-Prestación de servicios de conservación de mensajes de datos.- La conservación, incluido el almacenamiento y custodia de mensajes de datos, podrá realizarse a través de terceros, de acuerdo a lo que establece el Art. 8 de la Ley 67. Los sistemas, políticas y procedimientos que permiten realizar las funciones de conservación de mensajes de datos se denominan Registro Electrónico de Datos. Una vez cumplidos los requisitos establecidos en las leyes, cualquier persona puede prestar servicios de Registro Electrónico de Datos que incluyen:

Conservación, almacenamiento y custodia de la información en formato electrónico con las debidas seguridades; Preservación de la integridad de la información conservada; Administración del acceso a la información y la reproducción de la misma cuando se requiera; Respaldo y recuperación de información; y, Otros servicios relacionados con la conservación de los mensajes de datos. La prestación de servicios de Registro Electrónico de Datos se realizará bajo el régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios, podrán determinar las condiciones que regulan su relación.

La prestación del servicio de Registro Electrónico de Datos deberá observar todas las normas contempladas en la Ley 67, este reglamento y demás disposiciones legales vigentes.

En los procesos de conservación de los mensajes de datos, se debe garantizar la integridad de los mismos al menos por el mismo tiempo que las leyes y reglamentos exijan su almacenamiento.

Por orden de autoridad competente, podrá ordenarse a los proveedores de servicios de Registro Electrónico de Datos mantener en sus sistemas respaldos de los mensajes de datos que tramite por el tiempo que se considere necesario.

Art. 10.- Elementos de la infraestructura de firma electrónica.- La firma electrónica es aceptada bajo el principio de neutralidad tecnológica. Las disposiciones contenidas en la Ley 67 y el presente reglamento no restringen la autonomía privada

para el uso de otras firmas electrónicas generadas fuera de la infraestructura de llave pública, ni afecta los pactos que acuerden las partes sobre validez y eficacia jurídica de la firma electrónica conforme a lo establecido en la ley y este reglamento.

Los principios y elementos que respaldan a la firma electrónica son:

No-discriminación a cualquier tipo de firma electrónica, así como a sus medios de verificación o tecnología empleada; Prácticas de certificación basadas en estándares internacionales o compatibles a los empleados internacionalmente 1; El soporte lógico o conjunto de instrucciones para los equipos de cómputo y comunicaciones, los elementos físicos y demás componentes adecuados al uso de las firmas electrónicas, a las prácticas de certificación y a las condiciones de seguridad adicionales, comprendidas en los estándares señalados en el literal b); Sistema de gestión que permita el mantenimiento de las condiciones señaladas en los literales anteriores, así como la seguridad, confidencialidad, transparencia y no-discriminación en la prestación de sus servicios; y, Organismos de promoción y difusión de los servicios electrónicos, y de regulación y control de las entidades de certificación.

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 las leyes.

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.

Los períodos de actualización de las listas de certificados suspendidos, revocados o no vigentes por cualquier causa se establecerán contractualmente.

Art. 13.- Revocación del certificado de firma electrónica.- Establecidas las circunstancias determinadas en la Ley 67, se producirá la revocación, que tendrá también como consecuencia la respectiva publicación y la desactivación del enlace que informa sobre el certificado.

En caso de que las actividades de certificación vayan a cesar, la entidad de certificación deberá notificar con por lo menos noventa días de anticipación a los usuarios de los certificados de firma electrónica y a los organismos de regulación control sobre la terminación de sus actividades.

La cesión de certificados de firma electrónica de una entidad de certificación a otra, contará con la autorización expresa del titular del certificado.

La entidad de certificación que asuma los certificados deberá cumplir con los mismos requisitos tecnológicos exigidos a las entidades de certificación por la Ley 67 y este reglamento.

Art. 14.- De la notificación por extinción, suspensión o revocación del certificado de firma electrónica.-La notificación inmediata al titular del certificado de firma electrónica, de acuerdo al artículo 26 de la Ley 67, se hará a la dirección electrónica y a la dirección física que hubiere señalado en el contrato de servicio, luego de la extinción, suspensión o revocación del certificado.

Art. 15.- Publicación de la extinción, revocación y suspensión de los certificados de firma electrónica y digital.- La publicación a la que se refiere el artículo 27 de la Ley 67, se deberá hacer por cualquiera de los siguientes medios:

(Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005) Siempre en la página electrónica determinada por el CONATEL en la que se reporta la situación y la validez de los certificados, así como en la página WEB de la entidad certificadora; y, Mediante un aviso al acceder al certificado de firma electrónica desde el hipervínculo de verificación, sea que éste forme parte de la firma electrónica, que conste en un directorio electrónico o por cualquier procedimiento por el cual se consulta los datos del certificado de firma electrónica. Opcionalmente, en caso de que la entidad certificadora o la entidad de registro relacionada crean conveniente, se podrá hacer la publicación en uno de los medios de comunicación pública.

Art. 16.-Reconocimiento internacional de certificados de firma electrónica.- (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Los certificados de firma electrónica emitidos en el extranjero tendrán validez legal en Ecuador una vez obtenida la revalidación respectiva emitida por el CONATEL, él deberá comprobar el grado de fiabilidad de los certificados y la solvencia técnica de quien los emite.

Art. 17.-Régimen de acreditación de entidades de certificación de información.- (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Para obtener autorización de operar directamente o a través de terceros relacionados en Ecuador, las entidades de certificación de información deberán registrarse en el CONATEL.

Los certificados de firma electrónica emitidos por las entidades de certificación de información que, además de registrarse, se acrediten voluntariamente en el CONATEL, tienen carácter probatorio.

Las entidades que habiéndose registrado y obtenido autorización para operar, directamente o a través de terceros relacionados en Ecuador, no se acrediten en el CONATEL, tendrán la calidad de entidades de certificación de información no acreditadas y están obligadas a informar de esta condición a quienes soliciten o hagan

uso de sus servicios, debiendo también, a solicitud de autoridad competente, probar la suficiencia técnica y fiabilidad de los certificados que emiten.

Art. 18.- Responsabilidades de las entidades de certificación de información.- Es responsabilidad de la entidad certificadora de información o de la entidad de registro que actúe en su nombre, verificar la autenticidad y exactitud de todos los datos que consten en el certificado de firma electrónica.

El CONATEL podrá requerir en cualquier momento de la entidad de certificación de información, de la entidad de registro que actúe en su nombre, o del titular del certificado de firma electrónica los documentos de respaldo que confirmen la autenticidad y exactitud de los datos que contiene.

Art. 19.- Obligaciones del titular de la firma electrónica.- A más de las consideradas en la Ley 67 y su reglamento, serán las mismas previstas en las leyes por el empleo de la firma manuscrita.

El órgano que ejerce las funciones de control prevista en la Ley 67, desarrollará los mecanismos, políticas y procedimientos para auditar técnicamente la actividad de las entidades bajo su control.

Art. 20.- Información al usuario.- La información sobre los programas o equipos que se requiere para acceder a registros o mensajes de datos deberá ser proporcionada mediante medios electrónicos o materiales. En el caso de uso de medios electrónicos se contará con la confirmación de recepción de la información por parte del usuario, cuando se usen medios materiales, los que formarán parte de la documentación que se le deberá entregar al usuario.

Para demostrar el acceso a la información el usuario deberá manifestar expresamente que conoce la información objeto de su consentimiento y que sus sistemas le permiten el acceso tecnológico a la misma.

Art. 21.- De la seguridad en la prestación de servicios electrónicos.- La prestación de servicios electrónicos que impliquen el envío por parte del usuario de información personal, confidencial o privada, requerirá el empleo de sistemas seguros en todas las etapas del proceso de prestación de dicho servicio. Es obligación de quien presta los servicios, informar en detalle a los usuarios sobre el tipo de seguridad que utiliza, sus alcances y limitaciones, así como sobre los requisitos de seguridad exigidos legalmente y si el sistema puesto a disposición del usuario cumple con los mismos. En caso de no contar con seguridades se deberá informar a los usuarios de este hecho en forma clara y anticipada previo el acceso a los sistemas o a la información e instruir claramente sobre los posibles riesgos en que puede incurrir por la falta de dichas seguridades.

Se consideran datos sensibles del consumidor sus datos personales, información financiera de cualquier tipo como números de tarjetas de crédito, o similares que involucren transferencias de dinero o datos a través de los cuales puedan cometerse fraudes o ilícitos que le afecten.

Por el incumplimiento de las disposiciones contenidas en el presente artículo o por falta de veracidad o exactitud en la información sobre seguridades, certificaciones o mecanismos para garantizar la confiabilidad de las transacciones o intercambio de datos ofrecida al consumidor o usuario, el organismo de control podrá exigir al proveedor de los servicios electrónicos la rectificación necesaria y en caso de reiterarse el incumplimiento o la publicación de información falsa o inexacta, podrá ordenar la suspensión del acceso al sitio con la dirección electrónica del proveedor de servicios electrónicos mientras se mantengan dichas condiciones.

Art. 22.- Envío de mensajes de datos no solicitados.- El envío periódico de información, publicidad o noticias promocionando productos o servicios de cualquier tipo observará las siguientes disposiciones:

Todo mensaje de datos periódico deberá incluir mecanismos de suscripción y de suscripción (SIC); Se deberá incluir una nota indicando el derecho del receptor a

solicitar se le deje de enviar información no solicitada; Deberá contener información clara del remitente que permita determinar inequívocamente el origen del mensaje de datos; A solicitud del destinatario se deberá eliminar toda información que de él se tenga en bases de datos o en cualquier otra fuente de información empleada para el envío de mensajes de datos periódicos u otros fines no expresamente autorizados por el titular de los datos; y, Inmediatamente de recibido por cualquier medio la solicitud del destinatario para suscribirse del servicio o expresando su deseo de no continuar recibiendo mensajes de datos periódicos, el emisor deberá cesar el envío de los mismos a la dirección electrónica correspondiente. Las solicitudes de no envío de mensajes de datos periódicos, se harán directamente por parte del titular de la dirección electrónica de destino.

Los proveedores de servicios electrónicos o comunicaciones electrónicas, a solicitud de cualquiera de sus titulares de una dirección electrónica afectado por el envío periódico de mensajes de datos no solicitados, procederán a notificar al remitente de dichos correos sobre el requerimiento del cese de dichos envíos y de comprobarse que el remitente persiste en enviar mensajes de datos periódicos no solicitados podrá bloquear el acceso del remitente a la dirección electrónica afectada.

Art. 23.-Sellado de tiempo.- (Reformado por el art. 1 del D.E. 908, R.O. 168, 19-XII-2005).- Para la prestación de los servicios de sellado de tiempo, el mensaje de datos debe ser enviado a través de la entidad certificadora o un tercero debidamente registrado en el CONATEL para prestar este servicio. El sellado de tiempo únicamente establecerá para los fines legales pertinentes, la hora y fecha exacta en que el mensaje de datos fue recibido por la entidad certificadora o el tercero registrado por el CONATEL; y la fecha y hora exacta en dicho mensaje de datos fue entregado al destinatario.

Para efectos legales el servicio de sellado de tiempo se prestará tomando como referencia el huso horario del territorio continental ecuatoriano.

La prestación de servicios, de sellado de tiempo se realizará en régimen de libre competencia y contratación. Las partes que intervengan en la contratación de este tipo de servicios podrán determinar las condiciones que regulan su relación.

Artículo Final.- El presente reglamento entrará en vigencia a partir de su publicación en el Registro Oficial". (ECUADOR, 2014)

2.13. METODOLOGÍA SCRUM

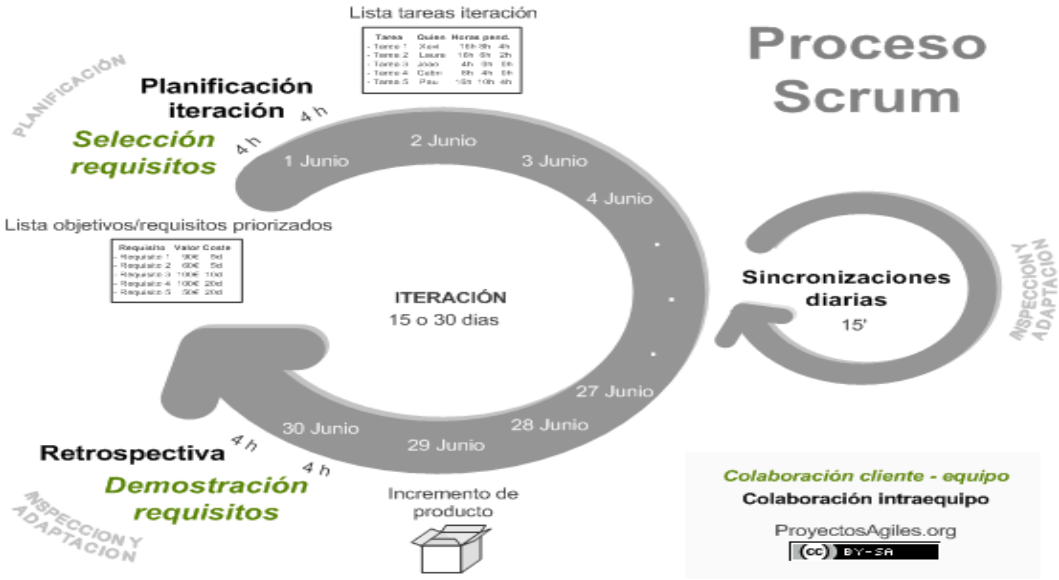


Figura 7 Metodología SCRUM

Fuente (Albaladejo, 2014)

Es una metodología ágil de desarrollo en la cual se realizan entregas parciales del producto las cuales son probadas y validadas por el receptor del proyecto.

Los proyectos se ejecutan en iteraciones, cada una de estas debe proporcionar resultados completos los cuales son entregados al cliente cuando esté lo solicite. (Albaladejo, 2014)

2.13.1. Roles de SCRUM

2.13.1.1. Product Owner (Cliente)

Es el cliente final del producto actúa como interlocutor único del equipo, tiene la autoridad para tomar decisiones.

Las características son:

- Encargado de definir los objetivos del proyecto
- Crea y mantiene toda la lista de requerimientos del producto, priorizando las tareas y funcionalidades que necesita.
- Establece el calendario de entregas de cada una de las iteraciones y funcionalidades.
- Colabora con el equipo dando los detalles en cada reunión y respondiendo las dudas que puedan tener con respecto al proyecto.
- Revisa todas las funcionalidades del producto terminadas.

(Albaladejo, 2014)

2.13.1.2. SCRUM Master (Facilitador)

Es el líder del equipo el cual tiene las siguientes responsabilidades:

- Verificar la lista de requerimientos priorizada para cada iteración.
- Debe guiar las reuniones del equipo de trabajo haciendo que estás cumplan el objetivo en el menor tiempo posible.
- Ayuda al equipo a ser auto gestionable y que se encuentren en la capacidad de resolver los problemas que se presentan.

(Albaladejo, 2014)

2.13.1.3. SCRUM Team (Equipo)

Es el grupo encargado los cuales desarrollan el producto, es un equipo auto organizado, el tamaño del equipo está entre 5 y 9 personas aunque puede ser un número diferente según los requisitos de las iteraciones, las actividades que realiza son:

- Selecciona los requisitos que tiene que completar en cada iteración.
- Estimar prioridades, y el esfuerzo que va a tomar desarrollar cada uno de los requerimientos para poder completar la iteración en el tiempo adecuado.
- Desarrollar las funcionalidades del sistema de manera conjunta.
- Demostrar al cliente los requerimientos, estos deben ser funcionales.

El equipo tiene que ser estable durante el desarrollo del proyecto, es decir que los miembros del equipo deben cambiar lo mínimo posible, es mejor que estos no

cambien, los miembros del equipo tienen que trabajar en el proyecto a tiempo completo así se evitan distracciones externas y requisitos de otros proyectos que pueden retrasar las tareas asignadas.

(Albaladejo, 2014)

2.13.2. Elementos de SCRUM

2.13.2.1. Product Backlog

Es una lista de objetivos o requerimientos en el cual se ve reflejada la visión y necesidades del cliente del producto a desarrollar permitiendo de esta manera involucrar al Product Owner en la validación de todas las funcionalidades del proyecto.

Se indican cuáles son las iteraciones y los entregables en cada una de ellas, no es necesario que en la lista se encuentren detallados los requerimientos pero sí que se encuentren todos ellos.

La lista permite ver el progreso del equipo ya que cada iteración con sus requerimientos tienen que tener un esfuerzo parecido. (Albaladejo, 2014)

2.13.2.2. Sprint Backlog

Es la lista de tareas el SCRUM Team realiza al momento de planificar cada sprint para posteriormente ser verificada por el cliente al finalizar cada una de las iteraciones mediante un producto funcional.

Permite ver en qué lugar del sprint el equipo tiene problemas para que estos puedan ser mitigados.

Las tareas deben ser divididas por prioridad colocando las tareas que dependen de otras por debajo de las más importantes. (Albaladejo, 2014)

2.13.2.3. Incremento

Es el final de cada iteración mostrando funcionalidades del sistema al cliente las cuales tienen que ser validadas y aprobadas, de esta manera se planifican las tareas que se van a realizar en el siguiente sprint según los resultados obtenidos al momento de realizar las pruebas con el cliente. (Albaladejo, 2014)

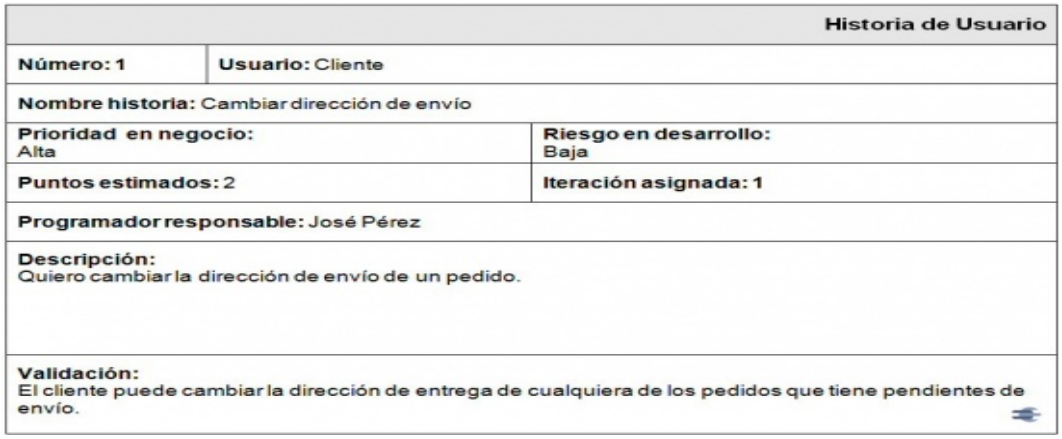
2.13.2.4. Historias de Usuario

Describen alguna funcionalidad que va a tener el sistema que se va a desarrollar, la implementación genera valor al cliente.

Su estructura comprende:

- Nombre de la historia de usuario el cual debe ser descriptivo.
- Descripción de la funcionalidad.
- Algún criterio de validación y forma de evaluación del usuario final del sistema.
- Prioridad.
- En SCRUM se le puede asignar el número de Iteración en la cual se va a desarrollar dicha funcionalidad.

(Scrummanager, 2015)



Historia de Usuario	
Número: 1	**Usuario:** Cliente
Nombre historia: Cambiar dirección de envío	
Prioridad en negocio: Alta	**Riesgo en desarrollo:** Baja
Puntos estimados: 2	**Iteración asignada:** 1
Programador responsable: José Pérez	
Descripción: Quiero cambiar la dirección de envío de un pedido.	
Validación: El cliente puede cambiar la dirección de entrega de cualquiera de los pedidos que tiene pendientes de envío.	

Figura 8 Historia de Usuario

Fuente (Scrummanager, 2015)

Tabla 1

Descripción de un Sprint SCRUM

SCRUM	ROLES	ENTREGABLE	FUNCIONES
ANÁLISIS	ANALISTA SCRUM MASTER PRODUCT OWNER	Especificación de requerimientos (IEEE - 830)	Se realiza la obtención de requerimientos, y su análisis, determinando requisitos funcionales y no funcionales del sistema
DISEÑO	DISEÑADOR SCRUM MASTER	Diagrama de Casos de Uso Diagrama de Clases Modelo de Base de Datos Arquitectura del Sistema	Se realiza el modelado del sistema de acuerdo a los requerimientos que se han obtenido en la fase previa
IMPLEMENTACIÓN	EQUIPO DE DESARROLLO	Módulo funcional del sistema Plan de pruebas	Se desarrolla un módulo del sistema
PRUEBAS	TESTER SCRUM MASTER PRODUCT OWNER	Informe de las pruebas realizadas	Se realizan las pruebas del módulo funcional obtenido.

2.14. HERRAMIENTAS DE DESARROLLO

2.14.1. Java Enterprise Edition (Java EE) V.6

Es una solución la cual fue desarrollada por SUN la que permite el desarrollo de aplicaciones distribuidas en capas en el lenguaje de programación JAVA, describe los elementos que se presentan en las aplicaciones que son desarrolladas en capas. (Groussard, 2010)

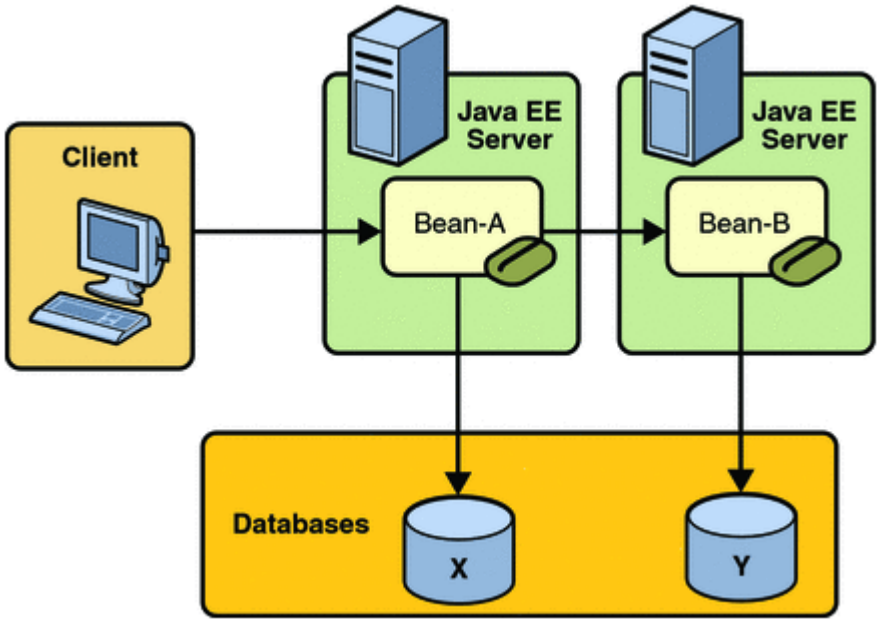


Figura 9 Diagrama Aplicación Multicapas

Fuente (Oracle, 2015)

2.14.2. Apache Tomcat 7.0.52

Es un contenedor de servlets, el cual funciona como un servidor web, el cual es de “uso libre y usado en entornos web con alto nivel de tráfico y alta disponibilidad”. (Díaz E. , 2014)

2.14.3. Netbeans 7.4

Es un IDE de desarrollo de código abierto que soporta el “desarrollo de todos los tipos de aplicación Java (J2SE, web, EJB y aplicaciones móviles)” (EcuRed, 2015)

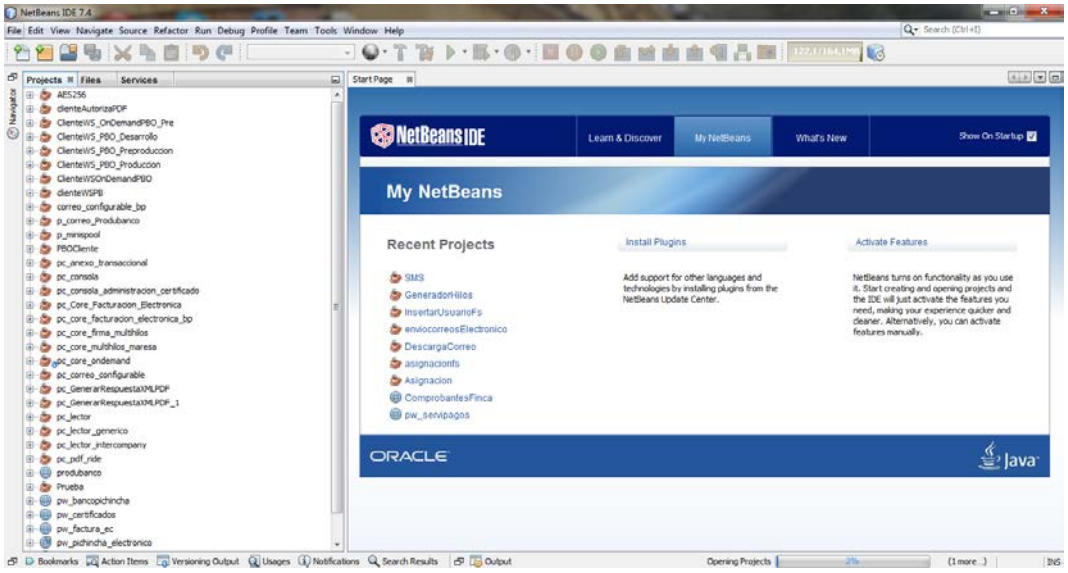


Figura 10 NetBeans IDE 7.4

2.14.4. Primefaces 4.0

"Es un componente para Java Server Faces (JSF) de código abierto que cuenta con un conjunto de componentes enriquecidos que facilitan la creación de las aplicaciones web. Primefaces está bajo la licencia de Apache License V2Hibernate." (Quijano, 2015)

2.14.5. Power Designer 16

Power Designer es una herramienta de modelado realizada por Sybase, permite la construcción de diagramas de base de datos y del desarrollo utilizando objetos y brinda a los desarrolladores crear aplicaciones que brinden un alto rendimiento. (EcuRed, 2015)

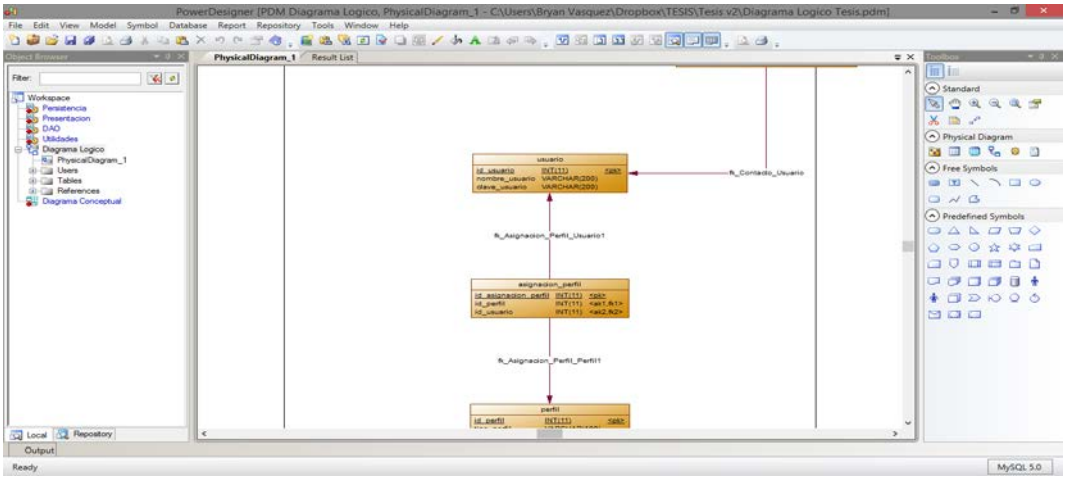


Figura 11 Interfaz de Power Designer

2.14.6. MySQL 5.6.16

"Es un sistema de administración de base de datos relacionales y multiusuario" (EcuRed, 2015) lo que permite que algunos usuarios en varias estaciones de trabajo puedan ejecutar consultas simultaneas, utiliza el lenguaje de consultas estructurado SQL. (Eduardo, 2015)

2.14.7. Hibernate

Herramienta mediante la cual se realiza el mapeo objeto relacional permitiendo el manejo de la base de datos mediante objetos en java, permite dejar de lado los datos primitivos que son usados por la base de datos. (Carrero, 2015)

2.14.8. Plug & Sign

Herramienta de ANF AC que permite firmar electrónicamente los archivos y colocar el sellado de tiempo.

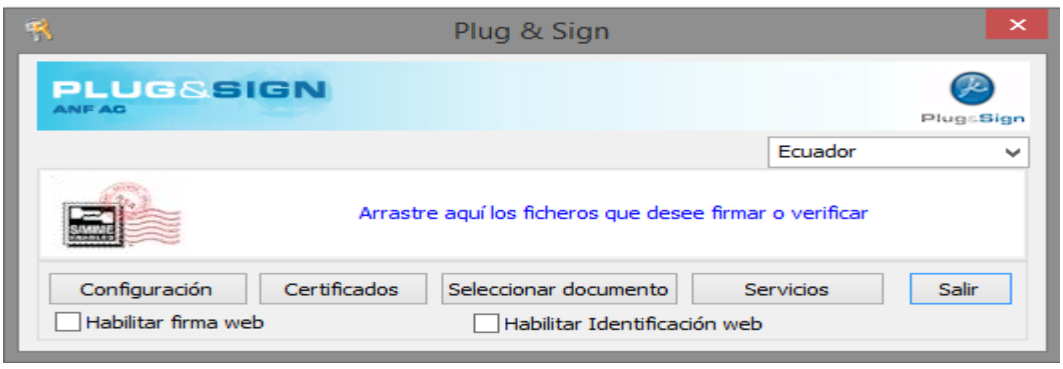


Figura 12 Pantalla de Inicio Plug & Sign

2.14.9. Xolido Sign

Herramienta gratuita que permite realizar una validación de la firma electrónica que se realiza en los archivos; además de insertar la firma en estos documentos utilizando un certificado emitido por una Autoridad de Certificación.

CAPÍTULO 3

ANÁLISIS, DISEÑO Y DESARROLLO DEL CASO PRÁCTICO

Antes de empezar con el desarrollo de la aplicación, se necesita realizar la especificación de los requerimientos de ésta manera definir funcionalmente lo que el sistema tiene que realizar.

3.1. ESPECIFICACIÓN DE REQUERIMIENTOS

3.1.1. Introducción

La presente especificación de requerimientos se ha realizado con el propósito de definir los requerimientos para el desarrollo del proyecto de grado titulado "Desarrollo de un buzón de documentos para los procesos del consejo de departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE utilizando firma digital y sellado de tiempo"

3.1.2. Propósito

El objeto de la especificación de requerimientos es definir de manera clara, precisa y verificable todas las funcionalidades y restricciones del sistema que se va a construir.

3.1.3. Ámbito del sistema

El Consejo de Departamento de Ciencias de la Computación se ha visto en la necesidad de diseñar un sistema el cual pueda cubrir las necesidades de ahorro de papel con los documentos que manejan, estos documentos deben tener la validez jurídica y legal para lo cual se hará uso de la firma electrónica.

Los documentos electrónicos que se manejen serán enviados a sus destinatarios, para lo cual se debe contar con buzones los cuales permitan visualizar los archivos y manejarlos de forma apropiada mediante el uso de perfiles de usuario y permisos asignados a estos perfiles.

3.1.4. Definiciones, Acrónimos y Abreviaturas

a. Definiciones

- **Administrador:** Persona encargada de la administración del sistema
- **Usuario:** Persona que tendrá acceso a las funcionalidades del sistema
- **Desarrollador:** Es el encargo del análisis, diseño, implantación y pruebas del sistema.

b. Acrónimos

- **ERS:** Especificación de Requerimientos de Software
- **AC:** Autoridad de Certificación
- **ANF:** Asociación Nacional de Fabricantes, es una Autoridad de Certificación de Ecuador
- **IEEE:** Instituto de Ingenieros Eléctricos y Electrónicos
- **TCP/IP:** Transfer Control Protocol / Internet Protocol (Protocolo de Control de Transporte / Protocolo de Internet)

3.1.5. Visión general del documento

Este documento consta de tres secciones. Esta sección es la introducción y proporciona una visión general del ERS. En la sección 2 se da una descripción general del sistema, con el fin de conocer las principales funciones que debe realizar, los datos asociados y los factores, restricciones, supuestos y dependencias que afectan al desarrollo, sin entrar en excesivos detalles. En la sección 3 se definen detalladamente los requisitos que debe satisfacer el sistema.

3.1.6. Descripción general

3.1.6.1. Perspectiva del producto

El sistema permitirá la gestión documental del Consejo de Departamento de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE almacenando todos los archivos y enviándolos a los miembros que necesiten estos documentos.

La firma electrónica dará la validez legal y jurídica a todos los documentos que sean emitidos por los miembros del Consejo de Departamento por lo cual es necesario que las personas encargadas de firmar los archivos obtengan el certificado de firma electrónica en una Autoridad de Certificación en este caso ANF-AC.

Permitirá la carga sólo de documentos firmados electrónicamente y descarga de los mismo para la validación de la firma y visualización del documento.

3.1.6.2. Funciones del Producto

Las funciones del producto se clasificarán de acuerdo al módulo y son las siguientes:

Módulo de usuarios

- Ingreso de usuarios
- Ingreso de perfiles
- Asignación de perfiles a usuarios
- Eliminación lógica de usuarios
- Consulta de usuarios
- Eliminación de perfiles asignados

Módulo Documental

- Subir archivos firmados electrónicamente
- Enviar archivos firmados electrónicamente
- Descarga de archivos

Módulo de Firma

- Firma de archivos
- Validación de la firma digital

3.1.6.3. Características de los Usuarios

El sistema tendrá tres tipos de usuario:

- Administrador

- Usuario Normal
- Usuario Firmador

El administrador será el encargado de manejar el sistema, el usuario normal el que haga uso de las funcionalidades de manejo de archivos electrónicos y el usuario firmador será aquel que realice firme los documentos el cual tiene que poseer el certificado de firma digital.

3.1.6.4. Restricciones

El sistema no realizará la firma de los documentos, esta se realizará mediante la aplicación de la autoridad certificadora en este caso ANF-AC Ecuador.

3.1.6.5. Suposiciones y Dependencias

Para realizar la firma electrónica en los documentos es necesaria una conexión a internet en un computador.

La aplicación de firma de la autoridad certificadora funciona únicamente bajo plataformas Windows

El buzón de documentos firmados funcionará en distintas plataformas, pero las pruebas se realizarán con Google Chrome.

3.1.6.6. Requisitos Futuros

- Escalabilidad en el sistema para poder integrarse a un buzón de documentos firmados electrónicamente para toda la Universidad de las Fuerzas Armadas ESPE
- Mejora en las interfaces de presentación al cliente.

3.1.7. Requisitos Específicos

En esta sección se detallarán los requerimientos que deben cumplir el sistema, contiene todos los requerimientos detallados de tal manera que los involucrados puedan diseñar un sistema que satisfaga las necesidades del cliente de tal y que servirán para las pruebas de funcionalidad del proyecto.

3.1.7.1. Interfaces Externas

a. Interfaces de Usuario

El sistema deberá contar con las siguientes características:

- Pantalla de ingreso mediante usuario y contraseña
- Menú para seleccionar las distintas tareas a las que pueda acceder el usuario
- Mensajes de error, advertencia y de información
- Interfaces de acceso según el perfil al que se le haya asignado

b. Interfaces de Hardware

Para las interfaces de hardware se toma en cuenta las características de los computadores en los cuales se vaya a utilizar la aplicación como son:

- Mouse
- Teclado
- Conexión a internet 512kbps.
- Monitor
- Computador

c. Interfaz de Comunicación

El sistema tendrá una conexión mediante el protocolo TCP/IP el cual es un protocolo de internet que permitirá la comunicación de los datos.

d. Interfaz de Software

El computador del usuario que va a visualizar los documentos deberá tener instalado un navegador web actualizado para utilización del repositorio de documentos.

3.1.7.2. Requerimientos Funcionales

REQ 01 Ingreso al sistema

El sistema deberá permitir el ingreso mediante un nombre de usuario y contraseña, la contraseña en la base de datos deberá estar cifrada.

Entrada

Nombre de Usuario, Contraseña

Salida

Si el usuario se encuentra registrado correctamente ingresará a la pantalla correspondiente según el perfil asignado, caso contrario mostrará un mensaje de error.

REQ 02 Registro de usuarios

El sistema permitirá que el usuario se registre, teniendo en cuenta que el usuario administrador será el encargado de activar el estado del usuario para que pueda acceder a las funcionalidades del sistema.

Entrada

Los datos que deberá ingresar el usuario para su registro son los siguientes:

- Nombres
- Apellidos
- Fecha de nacimiento (no obligatoria)
- Número de cédula
- Correo electrónico
- Sexo
- Cargo que ocupa en el Departamento de Ciencias de la Computación
- Número de teléfono convencional
- Número de teléfono celular
- Nombre de usuario
- Contraseña

Salida

Si ha ingresado correctamente los datos se registrará el usuario y se mostrará un mensaje de registro correcto, coso contrario un mensaje de error.

REQ 03 Activación de usuarios

El usuario administrador colocará un estado de activado al usuario y le asignará un perfil para que este pueda acceder al sistema

Entrada

- Perfil registrado en el sistema
- El estado de activado al nuevo usuario

Salida

Si se realizó correctamente se activará el usuario y se mostrará un mensaje de usuario activado, caso contrario un mensaje de error

REQ 04 Desactivación de usuarios

El usuario administrador colocará un estado de desactivado a algún usuario del sistema ya que solo se permitirá el borrado lógico de los registros

Entrada

- Usuario registrado en el sistema
- El estado de desactivado al usuario

Salida

Si se realizó correctamente se eliminará lógicamente al usuario y se mostrará un mensaje de usuario desactivado, caso contrario un mensaje de error.

REQ 04 Crear perfil de usuario

El usuario administrador puede crear nuevos perfiles de usuario.

Entrada

- Permisos registrados en el sistema según las funcionalidades

- Nombre de perfil
- Descripción del perfil

Salida

Si los datos se encuentran registrados correctamente se ingresará el nuevo perfil con sus permisos y se mostrará un mensaje de ingreso correcto caso contrario un mensaje de error.

REQ 05 Eliminar perfil de usuario

El usuario podrá eliminar perfiles de usuario del sistema siempre y cuando no esté asignado a algún usuario

Entrada

- Perfil de usuario a eliminar

Salida

Si se eliminó correctamente un mensaje de confirmación caso contrario un mensaje de error.

REQ 06 Modificar perfil de usuario

El usuario administrador puede cambiar los permisos asignados al perfil de usuario.

ENTRADA

- Permiso a eliminar o a asignar
- Perfil que va a modificar

SALIDA

Si los datos son correctos se actualizará el perfil y se mostrará un mensaje de confirmación caso contrario un mensaje de error.

REQ 07 Envío de documentos

El usuario normal puede enviar documentos a los usuarios siempre y cuando estos hayan sido firmados electrónicamente mediante la aplicación de firma de la AC.

La plataforma realizará una validación de la firma previo se suba el documento.

ENTRADA

- Documento firmado electrónicamente
- Usuarios registrados a enviar el archivo

SALIDA

Si se validó correctamente la firma se procede a enviar el documento caso contrario se mostrará un mensaje de error de firma, una vez enviados los documentos se mostrará un mensaje de envío correcto.

REQ 08 Buzón de entrada

El usuario normal puede visualizar los documentos que le hayan sido enviados.

ENTRADA

- Ingresar al buzón de entrada

SALIDA

Los documentos que le hayan sido enviados, en una bandeja con nombre del documento, fecha de emisión y emisor.

REQ 09 Buzón de salida

El usuario normal puede visualizar los documentos que les haya enviado a los usuarios.

ENTRADA

- Ingresar al buzón de salida

SALIDA

Los documentos que ha enviado el usuario, en una bandeja con nombre del documento, fecha de emisión y receptor.

REQ 10 Guardar documentos

El usuario normal puede subir documentos sin tener que enviarlos a ningún otro usuario del sistema, previo firmado electrónico.

ENTRADA

- Documento firmado electrónicamente

SALIDA

Si la validación de la firma se ha realizado correctamente se procederá a guardar el archivo mostrando un mensaje de confirmación, caso contrario se mostrará un mensaje de error de firma inválida.

REQ 11 Buzón de documentos guardados

El usuario normal puede visualizar los documentos que haya subido y hayan sido guardados.

ENTRADA

- Ingresar al buzón de guardados

SALIDA

Los documentos que ha enviado el usuario, en una bandeja con nombre del documento, fecha en la que se subió el documento

REQ 12 Descarga de documentos

El usuario normal desde cada uno de los buzones

- Buzón de entrada
- Buzón de salida
- Buzón de guardados

Podrá descargar los documentos.

ENTRADA

- Documento firmado electrónicamente a descargar

SALIDA

El documento si se descargó correctamente, caso contrario un mensaje de error de descarga.

REQ 13 Eliminado de documentos

El usuario normal desde cada uno de los buzones

- Buzón de entrada
- Buzón de salida
- Buzón de guardados

Podrá eliminar los documentos, el eliminado solo va a ser lógico es decir que los archivos permanecerán en la base de datos con un estado de eliminado.

ENTRADA

- Documento firmado electrónicamente a eliminar

SALIDA

Si se eliminó correctamente se cambiará el estado en la base de datos y se mostrará un mensaje de confirmación, caso contrario un mensaje de error.

REQ 14 Buzón de documentos eliminados

El usuario normal podrá ver todos sus documentos que hayan sido eliminados de los buzones.

ENTRADA

- Ingresar al buzón de eliminados

SALIDA

Todos los documentos que hayan sido eliminados, en una bandeja con la fecha de emisión, nombre del documento.

REQ 15 Restaurar documentos eliminados

El usuario normal restaurar los documentos que hayan sido eliminados colocándolos el estado de visible.

ENTRADA

- Documento a restaurar

- Nuevo estado del documento

SALIDA

El documento en el buzón del que fue eliminado si la transacción se realizó correctamente, caso contrario un mensaje de error.

REQ 16 Publicación de documentos

El usuario normal puede subir documentos sin tener que enviarlos a ningún otro usuario del sistema, previo firmado electrónico, estos documentos podrán ser visualizados sin la necesidad de estar registrado en el sistema, además debe contar con un menú de administración de estos según el usuario que haya publicado el documento.

ENTRADA

- Documento firmado electrónicamente

SALIDA

Si la validación de la firma se ha realizado correctamente se procederá a publicar el archivo mostrando un mensaje de confirmación, caso contrario se mostrará un mensaje de error de firma inválida; además se mostrará en el buzón de documentos publicados.

3.1.7.3. Requerimientos No Funcionales

Modularidad

El sistema deberá ser dividido en módulos, los cuales pueden funcionar independientemente

Desempeño

La firma de los archivos tanto la carga y descarga de estos dependerá de la velocidad del ancho de banda donde se encuentre alojada la aplicación y del internet al igual dependerá del tamaño del tamaño del fichero firmado.

Disponibilidad

El sistema se encontrará en la web mediante alta disponibilidad del servidor de aplicaciones y siempre estará accesible

Compatibilidad

El buzón será accedido mediante un browser por lo tanto tiene que ser compatible con los diferentes estos tipos de navegadores

- Google Chrome 20.0.1132.42 o superior
- Mozilla Firefox 5 o superior
- Internet Explorer 9 o superior

La aplicación de firmado electrónico Plug&Sign proporcionada por la Autoridad Certificadora es compatible solamente con Windows.

Usuarios Concurrentes

El sistema deberá permitir por lo menos 50 usuarios concurrentes

3.2. DISEÑO DEL SISTEMA

3.2.1. Casos de Uso

Los diagramas de casos de uso describen las relaciones que van a tener los usuarios o actores con las diferentes funcionalidades del sistema.

3.2.1.1. Descripción General de los Actores

El sistema a desarrollar tendrá tres actores:

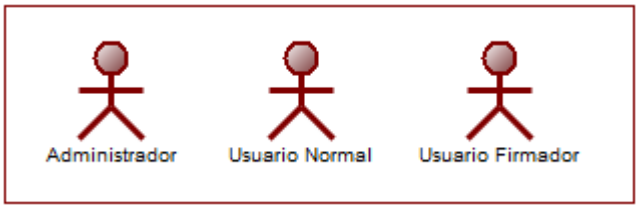


Figura 13 Actores del Sistema

Administrador: Es el encargado de gestionar la información relacionada con los usuarios, perfiles, permisos y reportes que se generan.

Usuario Normal: Es el usuario del buzón de documentos firmados electrónicamente el cual accede a los buzones de entrada, salida, guardados y eliminados.

Usuario Firmador: Es el que además de tener acceso a las funcionalidades del buzón de documentos firmados electrónicamente envía archivos firmados a otros usuarios sean estos normales o firmadores.

3.2.1.2. Diagrama de Casos de Uso

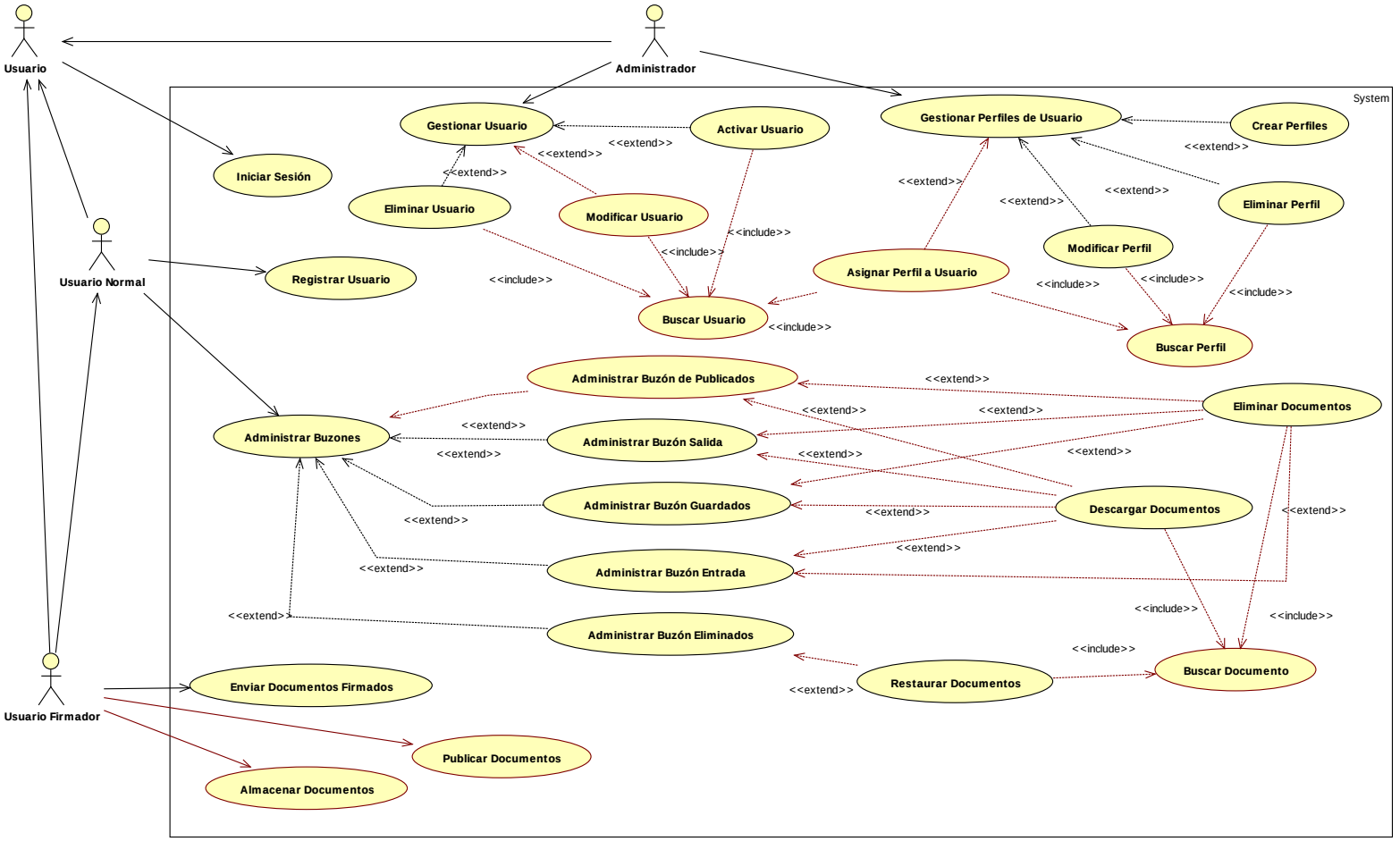


Figura 14 Diagrama de Casos de Uso

CASO DE USO: Iniciar sesión

a. Resumen: Realizar la autentificación del usuario para que este puede ingresar al sistema mediante un nombre de usuario y una contraseña

b. Actores: Usuario Normal, Usuario Firmador, Administrador

c. Precondición:

- El usuario tiene que estar registrado y activado en el sistema

d. Descripción:

Flujo Básico:

- Ingreso de nombre de usuario
- Ingreso de contraseña

Flujo Alternativo:

- El usuario no ingresa al sistema

Condición de éxito:

- Ingreso al sistema
- En caso de tener más de un perfil asignado, procederá a una pantalla para la verificación del perfil con el que desea ingresar al sistema
- Acceso a las funcionalidades del sistema según perfil

Condición de fallo:

Se despliega un mensaje de error según el problema:

- Error en datos
- Usuario no activado

CASO DE USO: Activar usuario

a. Resumen: Se realizará la activación de un usuario que se haya registrado

b. Actores: Administrador

c. Precondición:

- El usuario a activar tiene que estar registrado en el sistema

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de usuarios
- Buscar usuarios desactivados
- Seleccionar el usuario a dar de alta
- Guardar nuevo estado del usuario

Flujo Alternativo:

- Mensaje de error en caso de que no se haya podido activar

Condición de éxito:

- Registro en la base de datos
- Mensaje de confirmación de que el usuario ha sido activado

Condición de fallo:

- Se despliega un mensaje de error según el problema

CASO DE USO: Eliminar usuario

a. Resumen: Se realizará el eliminado lógico del usuario

b. Actores: Administrador

c. Precondición:

- El usuario a eliminar deberá estar registrado en el sistema con un estado activo

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de usuarios
- Buscar usuarios activados

- Seleccionar el usuario a dar de baja
- Guardar nuevo estado del usuario

Flujo Alternativo:

- Mensaje de error en caso de que no se haya podido eliminar

Condición de éxito:

- Registro en la base de datos
- Mensaje de confirmación de que el usuario ha sido desactivado

Condición de fallo:

- Se despliega un mensaje de error según el problema

CASO DE USO: Modificar usuario

a. Resumen: Se realizará cambios en los datos de los usuarios registrados

b. Actores: Administrador

c. Precondición:

- El usuario a modificar deberá estar registrado en el sistema

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de usuarios
- Buscar usuario a modificar
- Ingresar los datos que se van a modificar
- Guardar las modificaciones al usuario

Flujo Alternativo:

- Mensaje de error en caso de que no se haya podido actualizar los datos

Condición de éxito:

- Registro en la base de datos

- Mensaje de confirmación de que el usuario ha sido modificado

Condición de fallo:

- Se despliega un mensaje de error según el problema

CASO DE USO: Crear perfil

a. Resumen: Se realizará la creación de un nuevo perfil

b. Actores: Administrador

c. Precondición:

- No tener registrado un perfil con el mismo nombre al que se le va a crear

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de perfiles
- Ingreso de nombre de perfil
- Ingreso de una descripción del perfil
- Asignar permisos al perfil

Flujo Alternativo:

- Mensaje de error en caso de que no se haya podido crear el perfil

Condición de éxito:

- Registro en la base de datos
- Mensaje de confirmación de que el perfil ha sido creado correctamente

Condición de fallo:

- Se despliega un mensaje de error según el problema
    - Perfil ya registrado

CASO DE USO: Modificar perfil

a. Resumen: Se realizará el cambio de los permisos asignados al perfil y de la descripción del mismo

b. Actores: Administrador

c. Precondición:

- El perfil tiene que estar registrado en el sistema

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de perfiles
- Seleccionar el perfil a modificar
- Seleccionar nuevos permisos a asignar
- En caso de que se desee quitar permisos seleccionar permisos a eliminar
- Guardar los datos

Flujo Alternativo:

- Mensaje de error en caso de que no se hayan guardado las modificaciones al perfil

Condición de éxito:

- Registro en la base de datos
- Mensaje de confirmación de que el perfil ha sido modificado

Condición de fallo:

- Se despliega un mensaje de error según el problema

CASO DE USO: Eliminar perfil

a. Resumen: Se realizará la eliminación de perfiles de usuario del sistema

b. Actores: Administrador

c. Precondición:

- El perfil no tiene que estar asignado a ningún usuario

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de administración de perfiles
- Seleccionar el perfil a eliminar
- Elimina permisos asignados
- Guardar cambios en la base de datos

Flujo Alternativo:

- Mensaje de error en caso de que no se haya podido eliminar el perfil

Condición de éxito:

- Registro en la base de datos
- Mensaje de confirmación de que el perfil ha sido eliminado

Condición de fallo:

- Se despliega un mensaje de error según el problema
    - Perfil asignado a algún usuario
- Ver reporte en formato PDF.

Condición de fallo:

- Se despliega un mensaje de error

CASO DE USO: Registrar usuario

a. Resumen: El usuario tiene que registrarse en el sistema

b. Actores: Usuario

c. Precondición:

- El usuario no tiene que estar registrado en el sistema

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de registro
- Ingresar a los datos para el registro del usuario
    - Nombres
    - Apellidos
    - Fecha de nacimiento
    - Cédula
    - Correo Electrónico
    - Sexo
    - Cargo
    - Teléfono convencional
    - Teléfono celular
    - Nombre de usuario
    - Contraseña
- La contraseña será cifrada y los datos guardados en la base de datos

Flujo Alternativo:

- Mensaje de error de registro de usuario incorrecto

Condición de éxito:

- Almacenamiento en la base de datos, con el estado de cuenta desactivado
- Mensaje de confirmación de registro correcto

Condición de fallo:

- Se despliega un mensaje de error de falla de registro

CASO DE USO: Enviar documentos

a. Resumen: El usuario envía documentos firmados electrónicamente a otros usuarios del sistema

b. Actores: Usuario Firmador

c. Precondición:

- El usuario tiene que tener el perfil de usuario firmador
- El documento a enviar tiene que estar firmado electrónicamente

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de envío de documentos
- Seleccionar el documento que se desea enviar
- Seleccionar los usuarios receptores del documento
- Enviar documento
- Validación de la firma

Flujo Alternativo:

- Mensaje de error al enviar el documento

Condición de éxito:

- Almacenamiento en la base de datos del documento con sus destinatarios
- Mensaje de envío correcto

Condición de fallo:

- Se despliega un mensaje de error de falla de envío
    - No seleccionó un usuario
    - No seleccionó un documento
    - El documento no se encuentra firmado electrónicamente

CASO DE USO: Guardar documentos

a. Resumen: El usuario guardará los documentos firmados electrónicamente sin la necesidad de que estos sean enviados

b. Actores: Usuario Firmador

c. Precondición:

- El usuario debe tener el perfil de usuario firmador
- El documento a enviar tiene que estar firmado electrónicamente

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de envío de documentos
- Seleccionar el documento que se desea guardar
- Guardar documento
- Validación de la firma

Flujo Alternativo:

- Mensaje de error al guardar el documento

Condición de éxito:

- Almacenamiento en la base de datos del documento
- Mensaje de almacenamiento correcto

Condición de fallo:

- Se despliega un mensaje de error de falla de almacenamiento
    - No seleccionó un documento
    - El documento no se encuentra firmado electrónicamente

CASO DE USO: Descargar documentos

a. Resumen: El usuario podrá descargar los documentos para su visualización de los buzones de guardados, de enviados y de recibidos

b. Actores: Usuario Firmador, Usuario normal

c. Precondición:

- El usuario tiene que encontrarse en la pantalla de alguno de los buzones
    - Buzón de entrada
    - Buzón de salida

- Buzón de guardados
- Buzón de documentos publicados

d. Descripción:

Flujo Básico:

- Seleccionar el documento que va a ser descargado
- Descargar Documento

Flujo Alternativo:

- Mensaje de error al descargar el documento

Condición de éxito:

- Documento descargado
- Mensaje de descarga correcta

Condición de fallo:

- Se despliega un mensaje de error de en la descarga

CASO DE USO: Eliminar documento

a. Resumen: El usuario eliminará un documento lógicamente pudiendo verlo en el buzón de eliminados

b. Actores: Usuario Firmador, Usuario normal

c. Precondición:

- El usuario tiene que encontrarse en la pantalla de alguno de los buzones
  - Buzón de entrada
  - Buzón de salida
  - Buzón de guardados

d. Descripción:

Flujo Básico:

- Seleccionar el documento que va a ser eliminado

- Eliminar documento

Flujo Alternativo:

- Mensaje de error al eliminar el documento

Condición de éxito:

- Almacenamiento del nuevo estado del documento
- Mensaje de descarga correcta
- Visualización en el buzón de eliminados

Condición de fallo:

- Se despliega un mensaje de error en la eliminación

CASO DE USO: Restaurar documento

a. Resumen: El usuario podrá restaurar el documento del buzón de eliminados

b. Actores: Usuario Firmador, Usuario normal

c. Precondición:

- El usuario tiene que encontrarse en la pantalla del buzón de eliminados

d. Descripción:

Flujo Básico:

- Seleccionar el documento que va a ser restaurado
- Restaurar documento

Flujo Alternativo:

- Mensaje de error al restaurar el documento

Condición de éxito:

- Almacenamiento del nuevo estado del documento
- Mensaje de restauración del documento
- Visualización en el buzón del cual haya sido eliminado

Condición de fallo:

- Se despliega un mensaje de error en la eliminación

CASO DE USO: Publicar documento

a. Resumen: El usuario publicará los documentos firmados electrónicamente sin la necesidad de que estos sean enviados, estos se mostrarán en el buzón de documentos publicados y en una pantalla en la cual sean visibles sin la necesidad de ingresar al sistema.

b. Actores: Usuario Firmador

c. Precondición:

- El usuario debe tener el perfil de usuario firmador
- El documento a publicar tiene que estar firmado electrónicamente

d. Descripción:

Flujo Básico:

- Ingresar a la pantalla de envío de documentos
- Seleccionar el documento que se desea publicar
- Publicar documento
- Validación de la firma

Flujo Alternativo:

- Mensaje de error al guardar el documento

Condición de éxito:

- Almacenamiento en la base de datos del documento
- Mensaje de almacenamiento correcto

Condición de fallo:

- Se despliega un mensaje de error de falla en la publicación
    - No seleccionó un documento
    - El documento no se encuentra firmado electrónicamente

3.2.2. Modelo de Datos

3.2.2.1. Modelo Conceptual

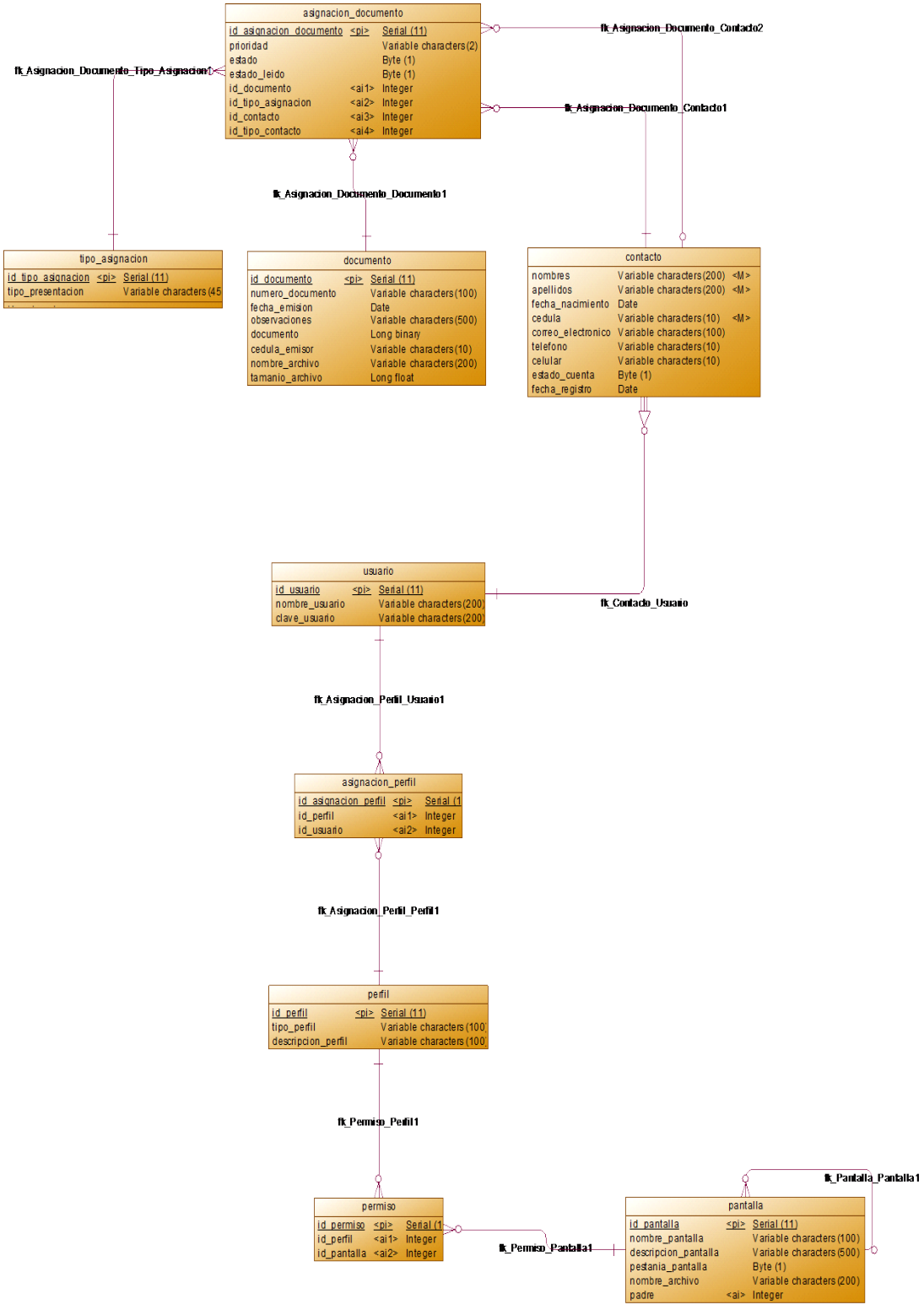


Figura 15 Modelo Conceptual de Base de Datos

3.2.2.2. Modelo Lógico

Figura 16 Modelo Lógico de Base de Datos

3.2.2.3. Diagrama Físico

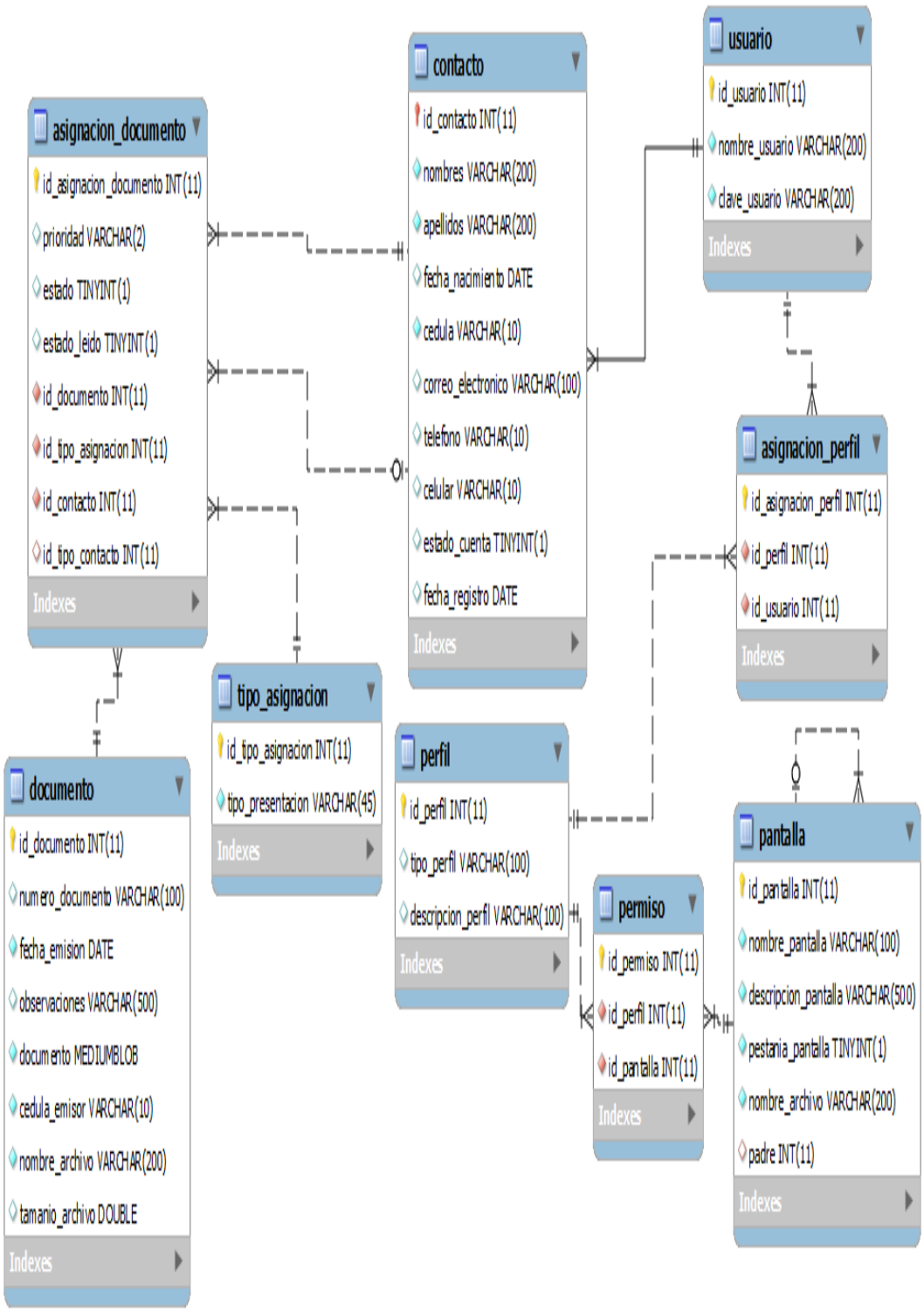


Figura 17 Modelo Físico de Base de Datos

3.2.3. Diccionario de Datos

Tabla 2

Tabla usuario

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_usuario	INT(11)	X	X	X	Clave primaria
nombre_usuario	VARCHAR(200)		X		Nombre de usuario
clave_usuario	VARCHAR(200)		X		Clave de usuario

Tabla 3

Tabla contacto

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_contacto	INT(11)	X	X	X	Clave primaria
nombres	VARCHAR(200)		X		Nombre de usuario
apellidos	VARCHAR(200)		X		Clave de usuario
fecha_nacimiento	DATE				Fecha de nacimiento del usuario
cedula	VARCHAR(10)		X		Cédula del usuario
correo_electrónico	VARCHAR(100)				Correo electrónico del usuario
teléfono	VARCHAR(10)				Teléfono convencional
celular	VARCHAR(10)				Teléfono celular
estado_cuenta	TINYINT(1)				Estado de la cuenta
fecha_registro	DATE				Fecha en la que se registró el usuario

Tabla 4

Tabla perfil

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_perfil	INT(11)	X	X	X	Clave primaria
tipo_perfil	VARCHAR(100)		X		Nombre del perfil
descripción_perfil	VARCHAR(100)		X		Descripción de las funcionalidades del perfil

Tabla 5

Tabla pantalla

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_pantalla	INT(11)	X	X	X	Clave primaria
nombre_pantalla	VARCHAR(100)		X		Nombre de la pantalla
descripción_pantalla	VARCHAR(500)		X		Descripción de la pantalla
pestania_pantalla	TINYINT(1)		X		Si es pestaña para el menú
nombre_archivo	VARCHAR(200)		X		Dirección del archivo .xhtml
Padre	INT(11)				Id de la pestaña

Tabla 6

Tabla documento

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_documento	INT(11)	X	X	X	Clave primaria
fecha_emisión	DATE		X		Fecha en la que se emitió el documento
observaciones	VARCHAR(500)				Descripción adicional del documento
Documento	MEDIUMBLOB		X		Archivo
cédula_emisor	VARCHAR(10)		X		Cédula de la persona que envió el documento
nombre_archivo	VARCHAR(200)		X		Nombre del archivo subido
tamanio_archivo	DOUBLE				Tamaño del archivo

Tabla 7

Tabla permiso

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_permiso	INT(11)	X	X	X	Clave primaria
id_perfil	VARCHAR(100)		X		Id del perfil FK
id_pantalla	VARCHAR(500)		X		Id de la pantalla a asignar permisos FK

Tabla 8

Tabla asignación_documento

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_asignación_documento	INT(11)	X	X	X	Clave primaria
Estado	TINYINT(1)				Estado del documento, eliminado, visible
Prioridad	VARCHAR(2)				Define la prioridad del documento enviado ALTA, MEDIA, BAJA
estado_leído	TINYINT(1)				Estado del documento cuando ha sido leído
id_documento	INT(11)		X		Id del documento asignado FK
id_tipo_asignación	INT(11)		X		Tipo de asignación (Guardado, Enviado, Recibido) FK
id_contacto	INT(11)		X		Id del contacto asignado al documento

Tabla 9

Tabla asignación_perfil

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_asignación_perfil	INT(11)	X	X	X	Clave primaria
id_perfil	INT(11)		X		Id del perfil FK
id_usuario	INT(11)		X		Id del usuario FK

Tabla 10

Tabla tipo_asignación

Columna	Tipo de Dato	PK	NN	AI	Comentario
id_tipo_asignación	INT(11)	X	X	X	Clave primaria
tipo_presentación	INT(11)		X		Tipo de asignación (Guardado, Enviado, Recibido)

3.2.4. Diagrama de Clases

Los diagramas de clases se dividieron en los siguientes módulos:

- **Módulo de Persistencia:** Comprende las clases que hacen referencia a la base de datos, es decir las que fueron creadas por la herramienta de persistencia Hibernate.
- **Módulo de Presentación:** En este módulo se muestran las clases que se usarán al momento de crear la capa de presentación con el framework JSF que permite la creación de JavaBeans para gestionar la interfaz al usuario.
- **Clases DAO:** Son las clases en las que se encuentran las reglas de negocio del sistema.
- **Utilidades:** Clases utilitarias en las que se encuentran validaciones y constantes son utilizadas en el sistema.

3.2.4.1. Módulo de Persistencia

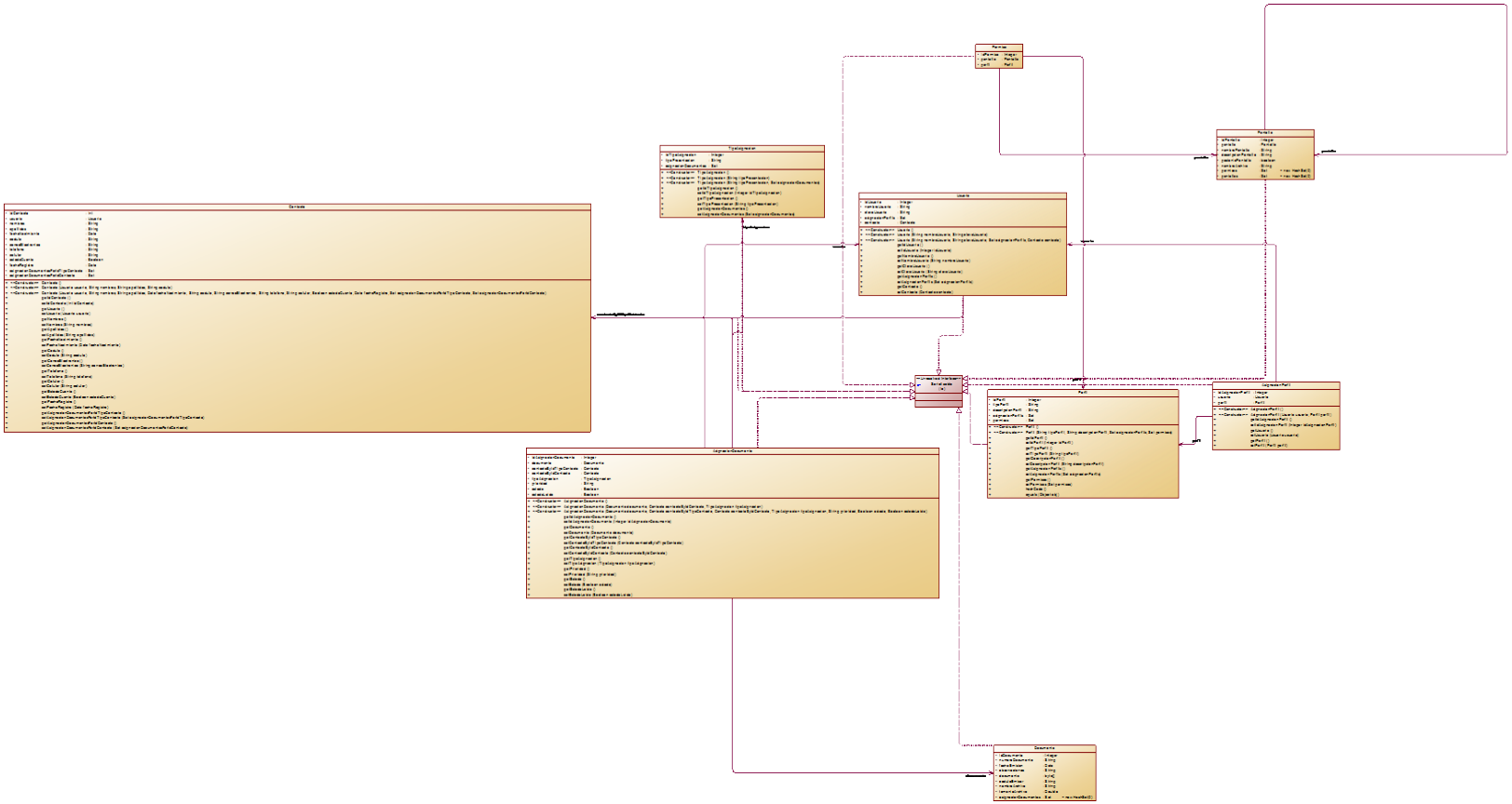


Figura 18 Diagrama de Clases Módulo de Persistencia

3.2.4.2. Módulo de Presentación

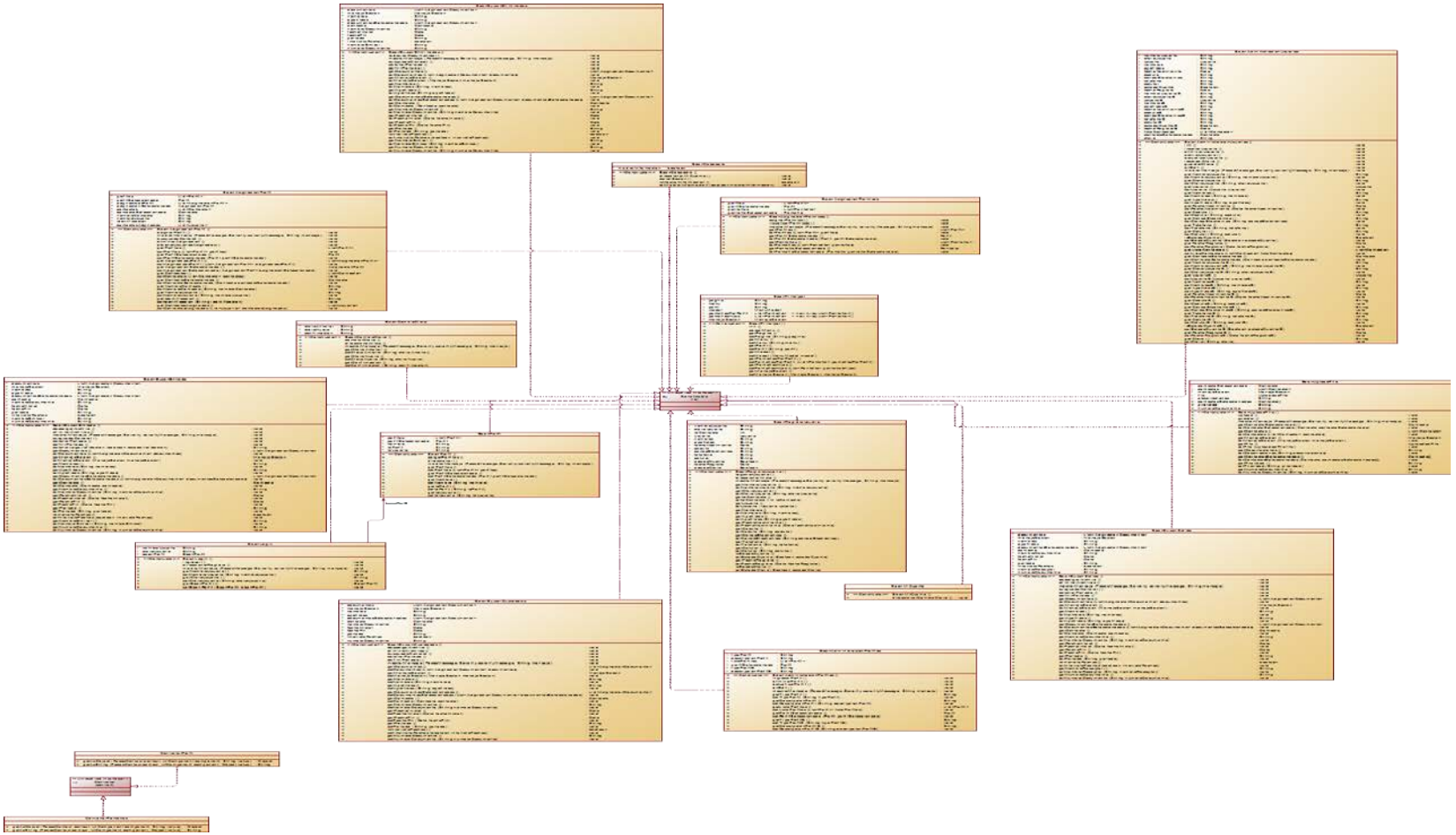


Figura 19 Diagrama de Clases Módulo Presentación

3.2.4.3. Data Access Object

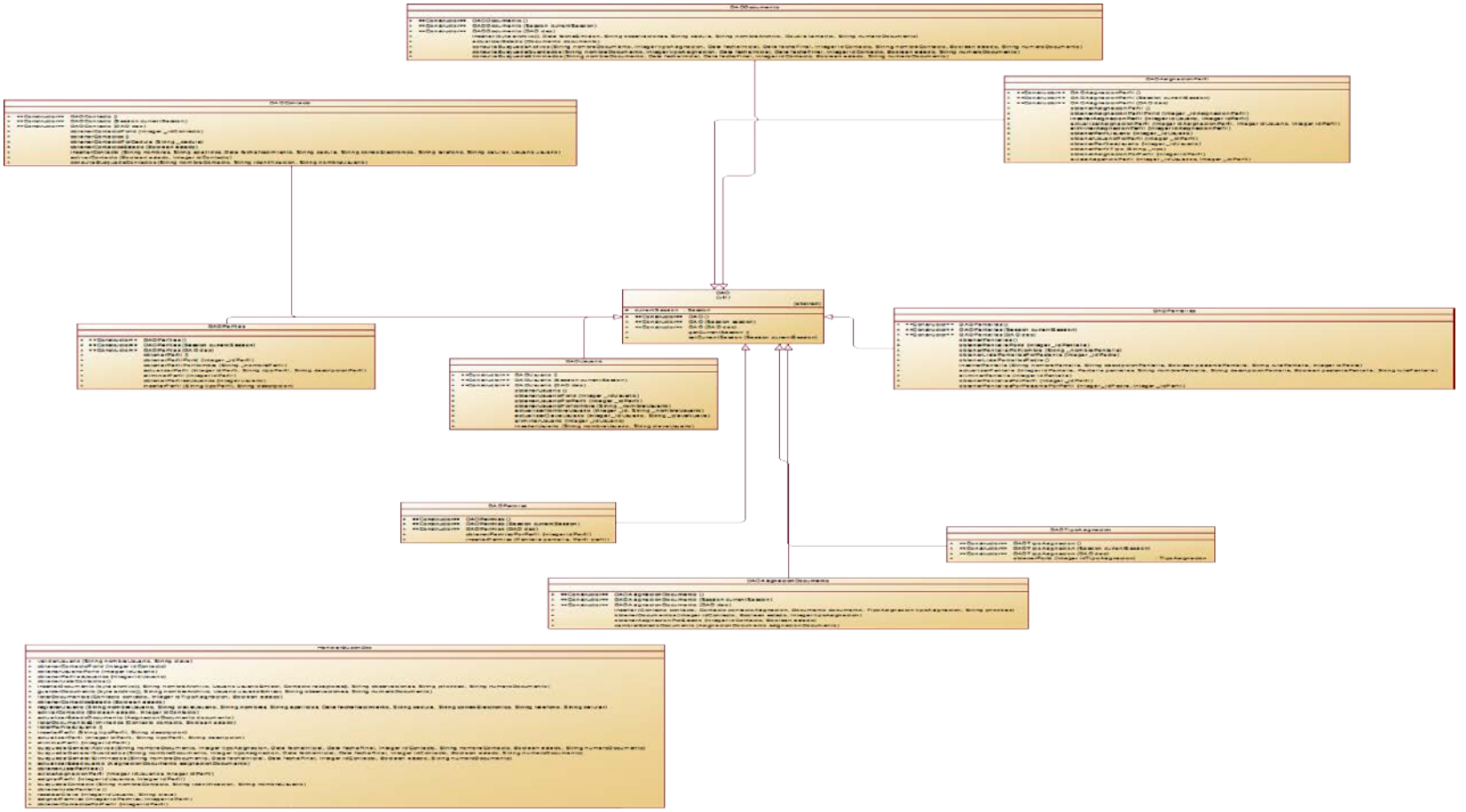


Figura 20 Diagrama de Clases DAO

3.2.4.4. Utilidades

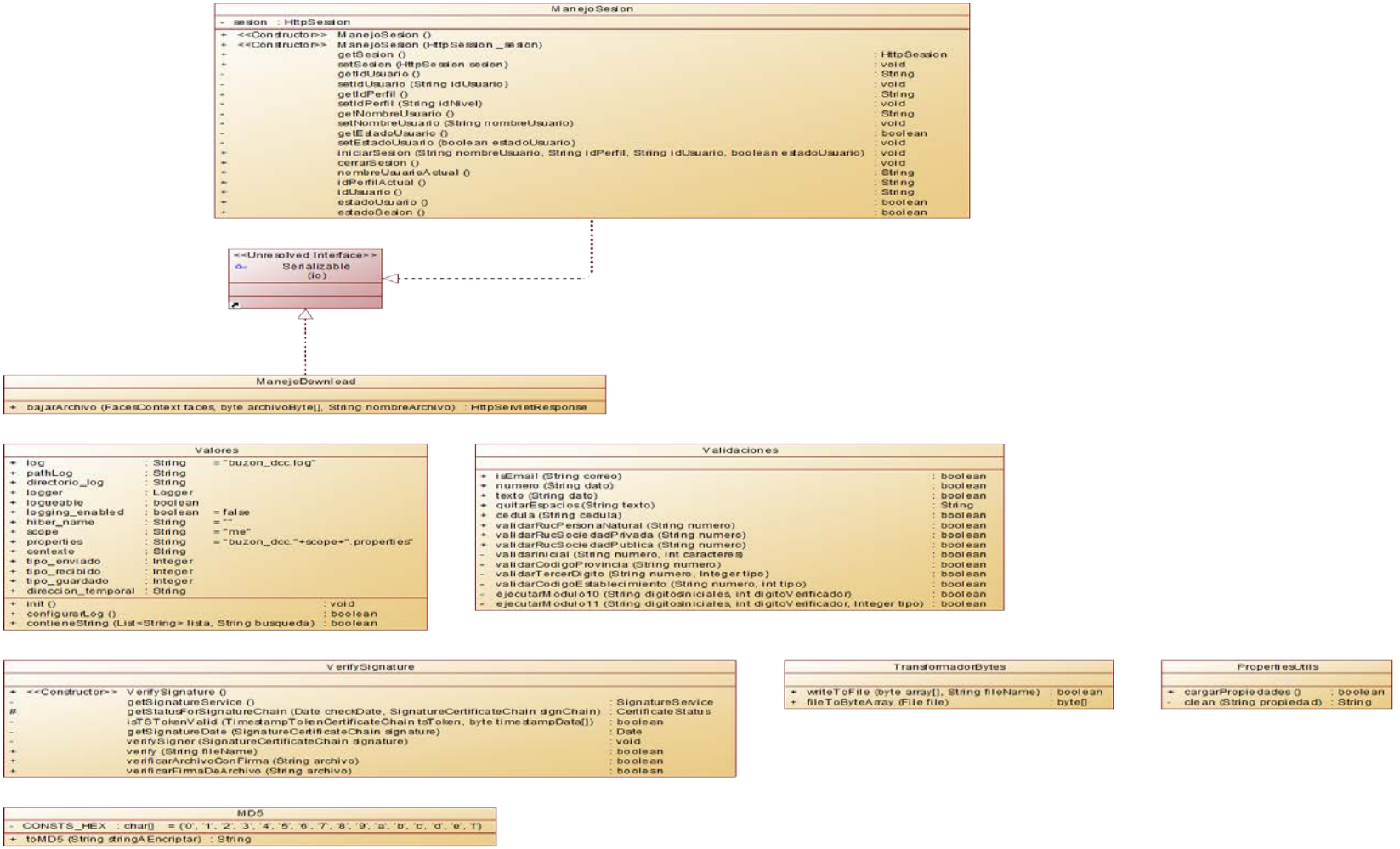


Figura 21 Diagrama de Clases Utilidades

3.2.5. Diseño de Arquitectura

El sistema manejará el patrón de arquitectura de software MVC (Modelo Vista Controlador), el cual permite separar la lógica de negocio de la interfaz de usuario y la capa de almacenamiento facilitando la tarea de desarrollo.

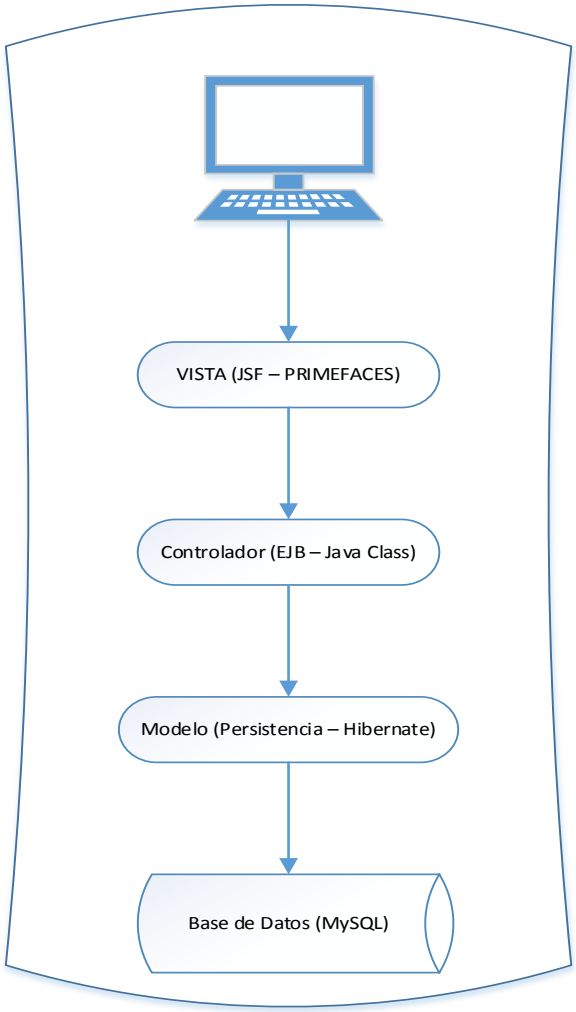


Figura 22 Arquitectura del Sistema

3.2.6. Diseño de Interfaces

Figura 23 Pantalla de Inicio

Figura 24 Pantalla de Registro de Usuarios

Figura 25 Buzón de Entrada

Figura 26 Buzón de Salida

Figura 27 Buzón de Documentos Guardados

Figura 28 Buzón de Documentos Eliminados

Figura 29 Pantalla de Envío de Documentos

Figura 30 Administración de Perfiles de Usuario

Figura 31 Administración de Permisos

Figura 32 Administración de Usuarios

Figura 33 Asignación de Perfiles de Usuario

Figura 34 Cambio de Clave de Usuario

Figura 35 Buzón de Documentos Publicados

Figura 36 Archivos Publicados

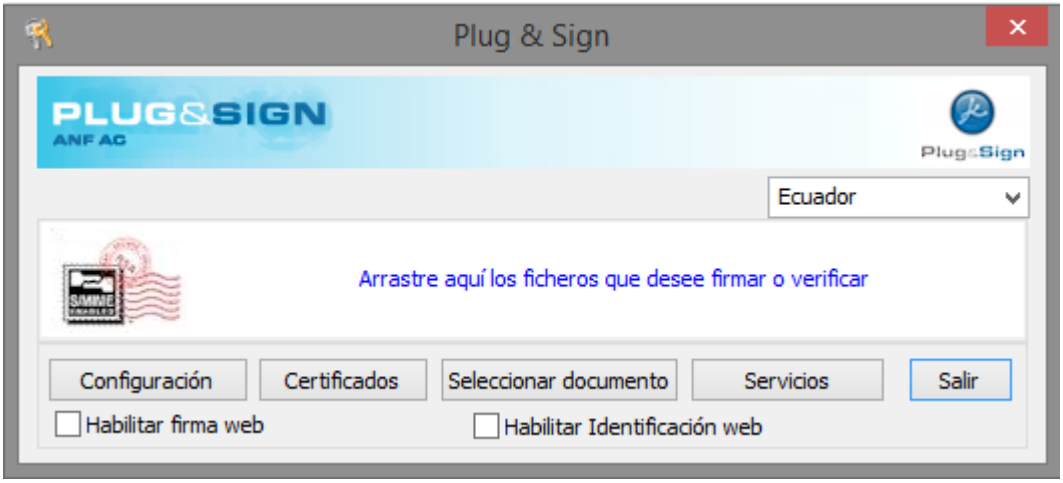


Figura 37 Plug & Sign

CAPÍTULO 4

IMPLEMENTACIÓN Y PRUEBAS

4.1. PROCESO PARA LA OBTENCIÓN DEL CERTIFICADO

En la autoridad de certificación ANF-AC existen tres tipos de certificado:

- Certificado de persona jurídica.
- Certificado de persona jurídica en sede administrativa
- Certificado de persona natural

Cada uno de estos tiene requisitos que cumplir para su obtención los cuales se detallan a continuación:

Certificado de Persona Jurídica

- Original de cédula ciudanía o pasaporte del Representan Legal.
- Original de la papeleta de votación del Representante Legal.
- Original o copia certificada del Nombramiento del Representante Legal inscrito en el Registro Mercantil.
- Original o copia certificada de la Constitución de la Compañía debidamente inscrita ante el organismo competente (en caso de existir reformas a los estatutos, se deberá presentar original o copia certificada de la última codificación de los estatutos sociales de la compañía)
- Original o copia certificado del Registro Único de Contribuyentes RUC de la Persona Jurídica.
- Original del recibo de pago del último mes de un servicio básico (agua, luz, teléfono) que se encuentre a nombre de la entidad solicitante (este documento es con la finalidad de poder verificar si la dirección que consta en el RUC, se encuentra actualizada). El Representante Legal deberá aportar los siguientes medios de recepción de mensajes:
    - Dirección de correo electrónico que califique como personal y segura.
    - Número de teléfono móvil y otros posibles teléfonos de contacto.

- Certificado bancario de una cuenta corriente o cuenta de ahorros de la Persona Jurídica.

Certificado de Persona Jurídica en Sede Administrativa

- Original de cédula ciudanía o pasaporte del Representan Legal y Persona Delegada para administrar el certificado.
- Original de la papeleta de votación del Representante Legal y Persona Delegada
- Original o copia certificada del Nombramiento del Representante Legal inscrito en el Registro Mercantil.
- Original o copia certificada de la Constitución de la Compañía debidamente inscrita ante el organismo competente (en caso de existir reformas a los estatutos, se deberá presentar original o copia certificada de la última codificación de los estatutos sociales de la compañía)
- Original o copia certificado del Registro Único de Contribuyentes RUC de la Persona Jurídica.
- Original del recibo de pago del último mes de un servicio básico (agua, luz, teléfono) que se encuentre a nombre de la entidad solicitante (este documento es con la finalidad de poder verificar si la dirección que consta en el RUC, se encuentra actualizada).
- El Representante Legal deberá aportar los siguientes medios de recepción de mensajes:
    - Dirección de correo electrónico que califique como personal y segura.
    - Número de teléfono móvil y otros posibles teléfonos de contacto.
- La Persona Delegada para la administración del certificado de firma electrónica deberá aportar los siguientes medios de recepción de mensajes.
    - Dirección de correo electrónico que califique como personal y segura.
    - Número de teléfono móvil y otros posibles teléfonos de contacto.
- Poder o Carta de Delegación donde se especifique las atribuciones de la persona delegada que administrará el certificado de firma electrónica en nombre la Persona Jurídica.

- Certificado bancario de una cuenta corriente o cuenta de ahorros de la Persona Jurídica.
- Nombre del Área Administrativa a la cual pertenece el Delegado del Certificado: (Estructura Organizacional de la Empresa)
- Cargo del Delegado de la Administración del Certificado.

Nota: Este tipo de certificados se utilizan para ser instalados en un servidor seguro (HSM) para realizar firmas desasistidas si la necesidad de que una persona esté ingresando el PIN del certificado (integración con sistemas contables) y además para que el certificado sea administrado por un Delegado del Represente Legal de la Persona Jurídica con poder para ello.

Certificado de Persona Natural

- Original de Cédula o Pasaporte
- Certificado de Trabajo
- Recibo original del último pago de un servicio básico
- Comprobante que acredite la titularidad de una cuenta bancaria
- Certificado de Votación
- Para extranjeros (permiso de residencia o trabajo y censo)
- RUC si tuviere
- El suscriptor del certificado deberá aportar los siguientes medios de recepción de mensajes:
    - Dirección de correo electrónico que califique como personal y segura.
    - Número de teléfono móvil y otros posibles teléfonos de contacto.

Posterior a la entrega de documentos la autoridad de certificación ANF AC envía estos a una validación de estos en el departamento legal la cual tarda 48 horas, después de esto la persona se acerca a las oficinas para realizar la emisión del certificado.

Figura 38 Certificado Electrónico

4.2. IMPLEMENTACIÓN

4.2.1. Instalación del Sistema Operativo CentOS

La instalación del sistema operativo CentOS inicia con la pantalla en la cual se escoge el tipo de instalación, en este caso la primera opción ya que es una nueva instalación en el servidor

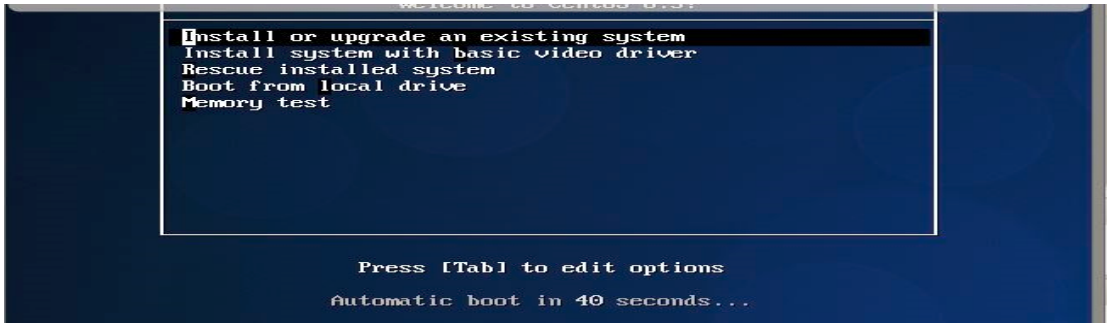


Figura 39 Tipo de Instalación CentOS

El sistema solicita una revisión del servidor antes de realizar la instalación del sistema la cual es aceptada.

Figura 40 Revisión del Servidor

Se selecciona el idioma en el cual se va a manejar el sistema operativo.

Figura 41 Selección de Idioma

Se coloca un nombre de host al servidor y se continúa con la instalación seleccionando el huso horario.

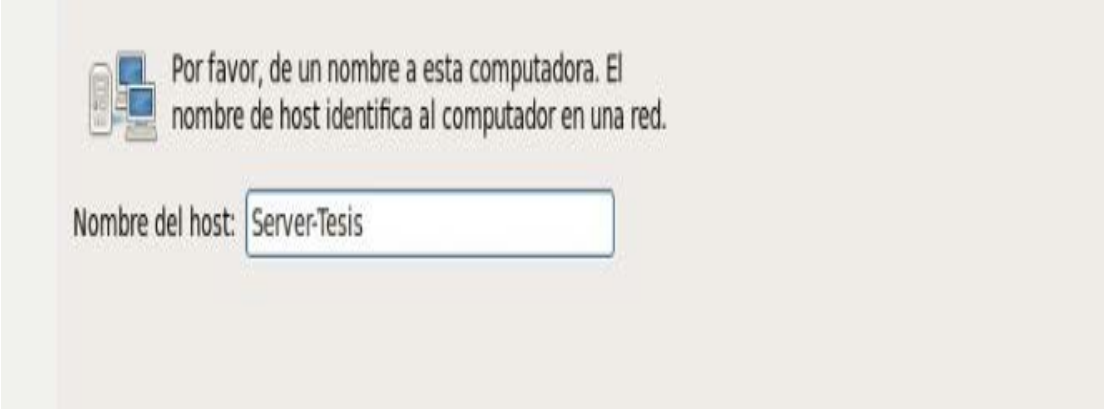


Figura 42 Nombre del Servidor

Se selecciona la ciudad más cercana al huso horario.

Figura 43 Selección de Huso Horario

Una vez seleccionado el huso horario la instalación pedirá la contraseña para el usuario administrador o ROOT

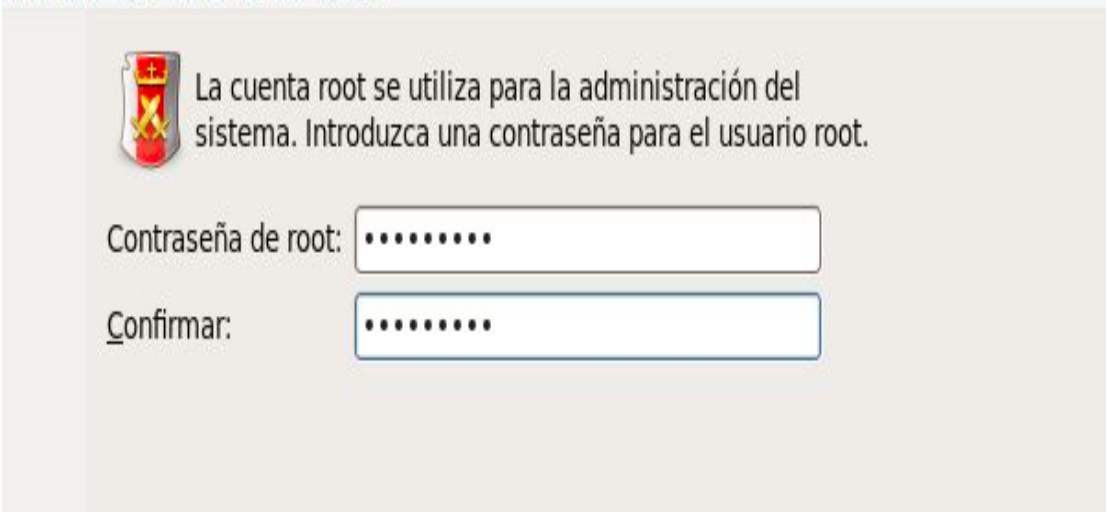


Figura 44 Contraseña de Usuario ROOT

Se selecciona el tipo de partición para almacenaje que se va a crear en el disco duro del servidor.

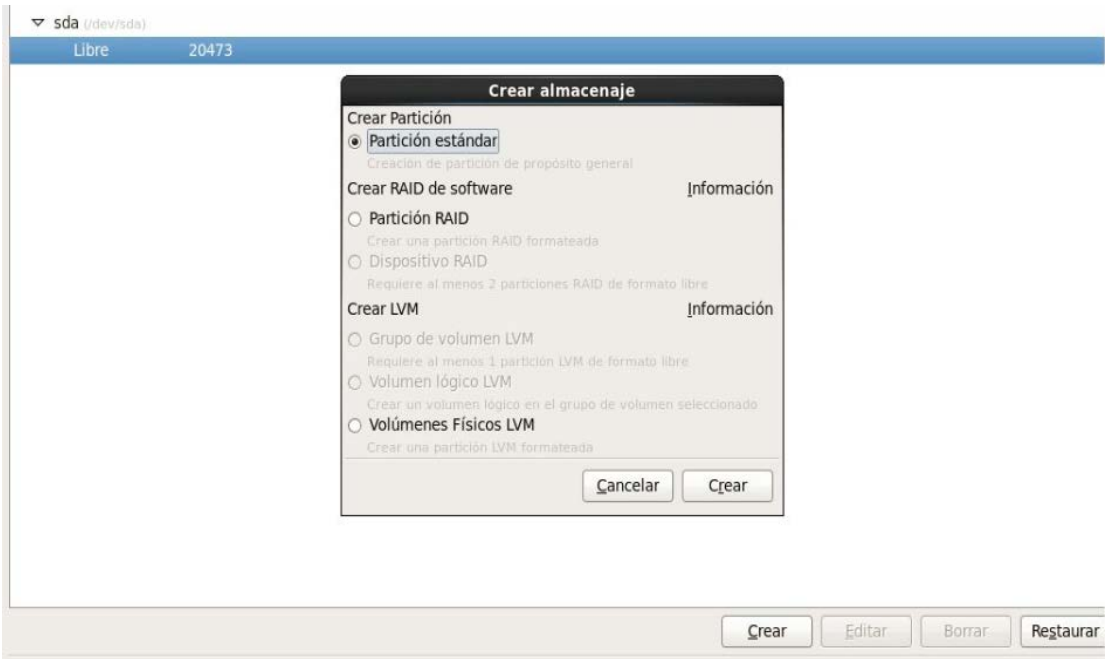


Figura 45 Particiones del Servidor

El sistema iniciará la instalación del sistema operativo.

Figura 46 Instalación de CentOS

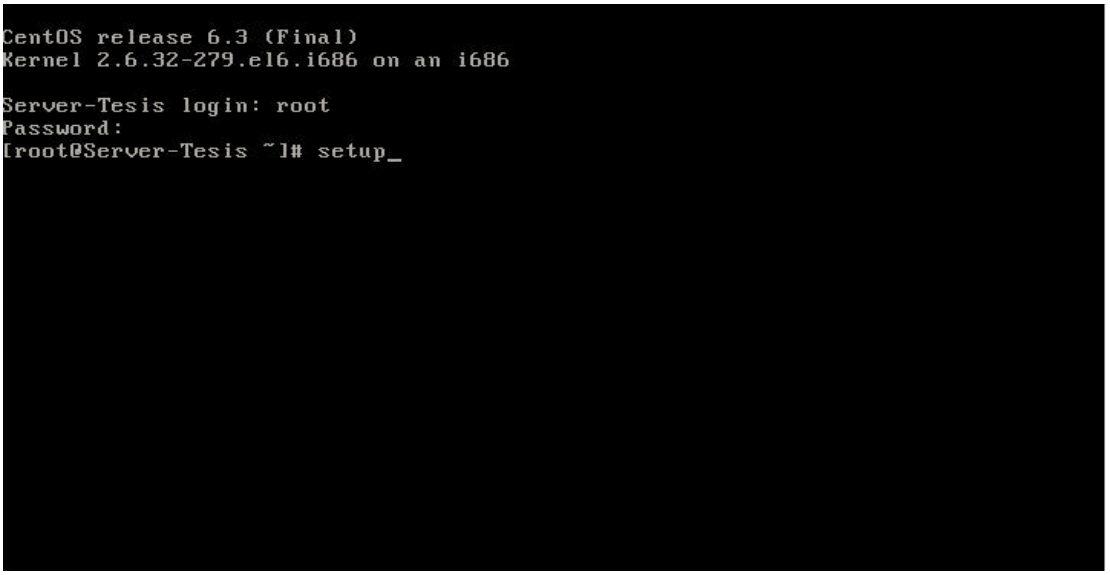


Figura 47 Pantalla de Inicio de CentOS

4.2.2. Instalación de MySQL en CentOS

yum -y install mysql mysql-server

4.2.3. Instalación de Apache Tomcat en CentOS

La instalación de Apache Tomcat el cual funciona como un contenedor de servlets permitirá el despliegue de la aplicación.

Para instalar en el sistema operativo CentOS se utiliza los siguientes comandos:

cd /tmp

Ir al directorio en el cual se va a descargar el contenedor de servlets apache tomcat, se lo puede descargar directamente desde la página principal

http://tomcat.apache.org/download-70.cgi, en este caso se usó el comando wget para la descarga.

wget http://www.us.apache.org/dist/tomcat/tomcat-7/v7.0.42/bin/apache-tomcat7.0.42.gz

Una vez que la descarga se haya completado ir al directorio tomcat7

cd /usr/local/tomcat7

en el directorio se ejecuta:

./bin/startup.sh

para que el contenedor Apache Tomcat arranque y pueda ser utilizado.

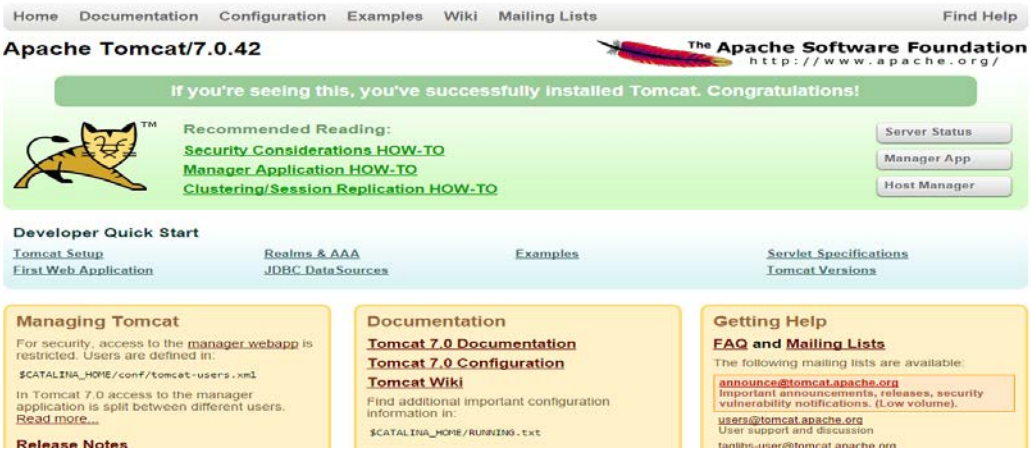


Figura 48 Pantalla de Inicio de Apache Tomcat

4.2.4. Instalación de Java en CentOS

Cambie al directorio en el que desee efectuar la instalación.

cd <nombre_ruta_acceso_directorio>

Por ejemplo, para instalar el software en el directorio /usr/java/

cd /usr/java

Desinstale todas las instalaciones anteriores de los paquetes Java.

rpm -e <nombre_paquete>

Se instala el paquete.

rpm -ivh jre-7u7-linux-x64.rpm

Para actualizar un paquete:

rpm -Uvh jre-7u7-linux-x64.rpm

4.2.5. Instalación de XolidoSign

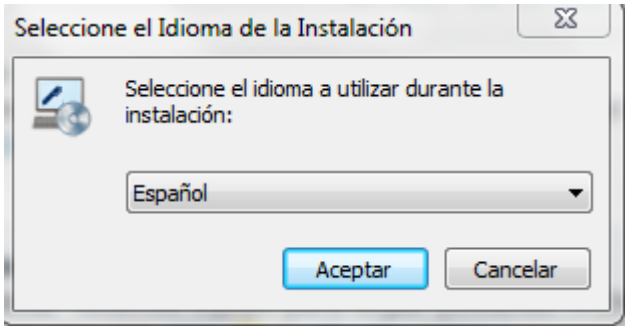


Figura 49 Selección de Idioma

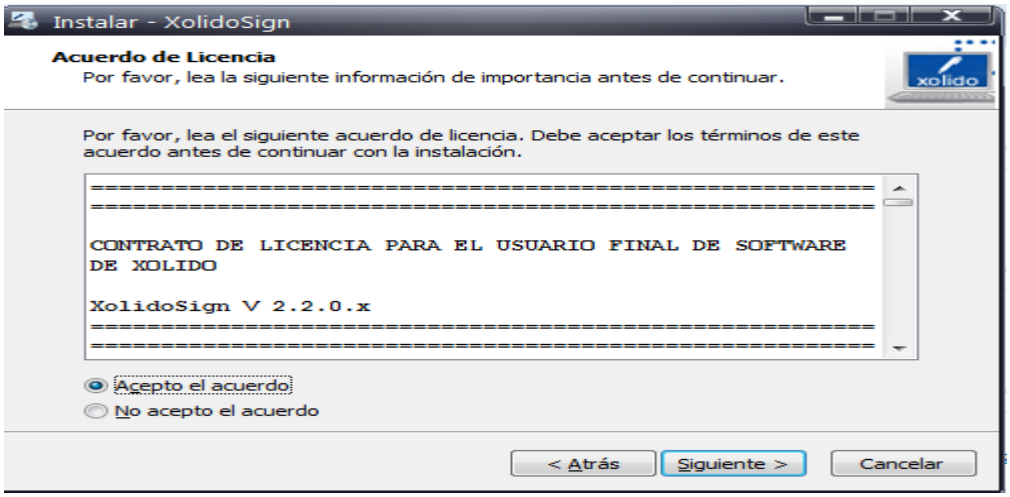


Figura 50 Acuerdo de Licencia

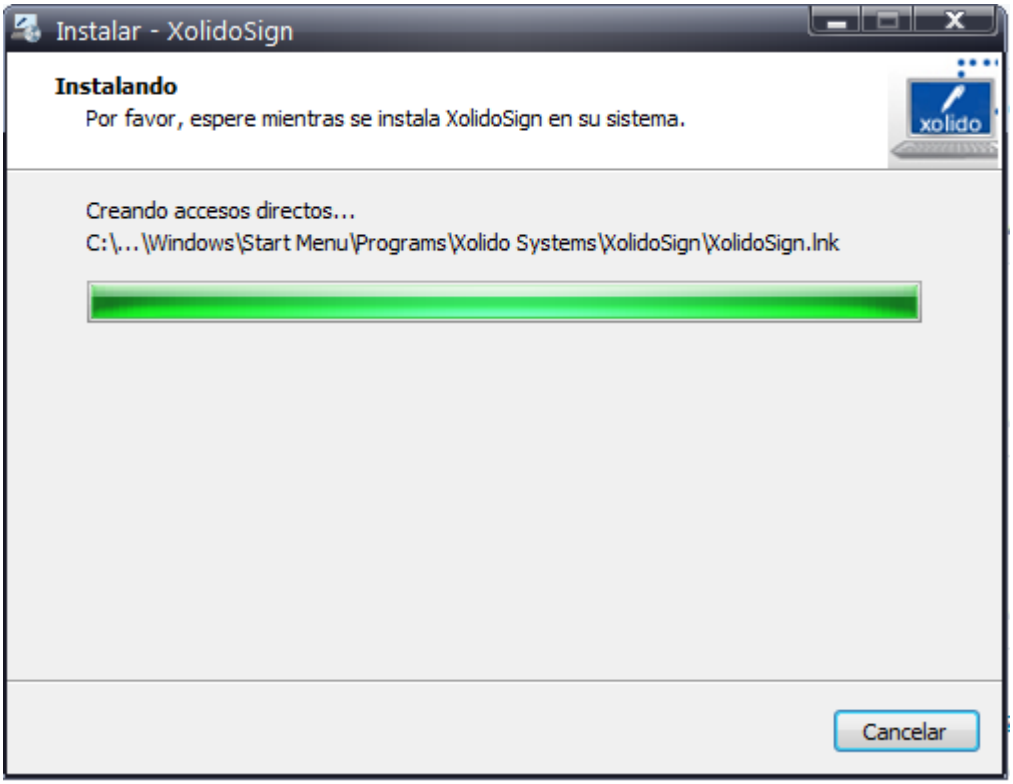


Figura 51 Instalación de Xolido Sign

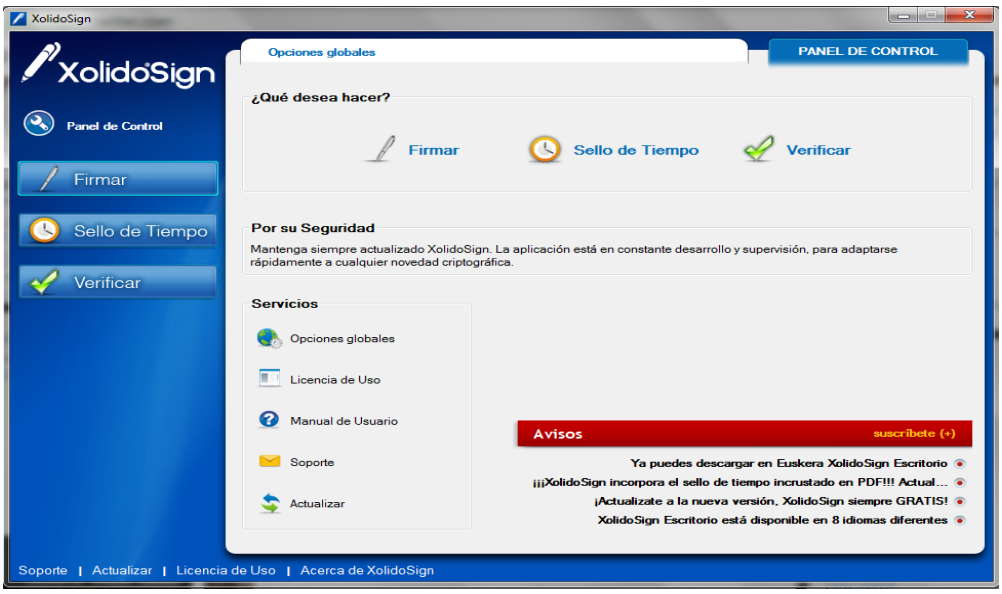


Figura 52 Pantalla de Inicio de XolidoSign

4.3. PRUEBAS

4.3.1. Pruebas Funcionales

Para realizar las pruebas funcionales de la aplicación del buzón de documentos firmados electrónicamente se han seleccionado varios casos de prueba con las funcionalidades que fueron especificadas en el levantamiento de requerimientos y la especificación de casos de uso.

4.3.1.1. Plan de Pruebas

Introducción

Este documento pretende describir las pruebas que se van a realizar en el buzón de documentos firmados electrónicamente para el Departamento de Ciencias de la Computación con el fin de comprobar que se cumplan los requerimientos del sistema

Propósito

El plan de pruebas establecerá estándares de prueba los cuales van a ser aplicados al buzón de documentos firmados electrónicamente para el Departamento de Ciencias de la Computación planteando una estrategia que conduzca al aseguramiento de calidad del software.

Alcance

El plan de pruebas describe el detalle de las diferentes pruebas a ser aplicadas, así como también las herramientas a utilizar en cada una de estas. Las pruebas que serán realizadas son:

- Ingreso al sistema
- Registro de usuarios
- Activación de usuarios
- Desactivación de usuarios
- Eliminar Usuarios
- Modificar Usuarios
- Creación de perfil de usuarios
- Eliminación de perfil de usuarios

- Modificar perfil de usuarios
- Envío de documentos
- Buzón de entrada
- Buzón de salida
- Guardar documentos
- Buzón de documentos guardados
- Descarga de documentos
- Eliminación de documentos
- Buzón de documentos eliminados
- Restauración de documentos eliminados
- Publicación de documentos
- Buzón de documentos publicados

Referencias

- Especificación de requerimientos de software
- Especificación de casos de uso

Recursos

- Procesador intel Dual Core 2.4 GHz
- Memoria RAM 2 GB
- Sistema Operativo Windows XP o Superior.
- Conexión a Internet 512kb mínimo
- Token de Firma Electrónica emitido por ANF AC

4.3.1.2. Casos de Prueba

Tabla 11

Caso de Prueba CP01

Código de Identificación:	INGRESO AL SISTEMA CP01
Descripción:	Ingresar al sistema
Requisitos asociados	Estar registrado en el sistema
Variables de Entrada (Inputs):	• Nombre de Usuario • Contraseña
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Acceder
Resultado esperado:	Ingresar al sistema
Flujo alterno	• No ingresar correctamente los datos • Usuario no registrado
Resultado alternativo esperado:	• Mensaje de error • No ingresar al sistema
Evaluación de prueba	
Fecha de Ejecución:	27 – agosto – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro
Notas del programador	
Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 12

Caso de Prueba CP02

Código de Identificación:	REGISTRO DE USUARIOS CP02
Descripción:	Registrar usuario
Requisitos asociados	No estar registrado en el sistema
Variables de Entrada (Inputs):	• Nombres • Apellidos • Fecha de Nacimiento • Número de cédula • Correo Electrónico • Número Telefónico • Número Celular • Nombre de Usuario • Contraseña
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Registrar
Resultado esperado:	Ingresar al sistema
Flujo alterno	• No ingresar correctamente los datos • Usuario no registrado
Resultado alternativo esperado:	• Mensaje de error • No ingresar al sistema

Evaluación de prueba

Fecha de Ejecución:	04 – febrero – 2015
Ejecutado por:	Ing. Jenny Ruiz
Lugar de ejecución	Departamento de Ciencias de la Computación

Notas del programador

Estado:	El usuario no mostró mensaje de error al no ingresar datos obligatorios
Acciones de corrección:	Revisión y cambios en el código del sistema
Corregido por:	Bryan Vásquez

Tabla 13

Caso de Prueba CP03

Código de Identificación:	ACTIVACIÓN DE USUARIOS CP03
Descripción:	Activación de Usuarios
Requisitos asociados	El usuario tiene que estar desactivado
Variables de Entrada (Inputs):	• Usuario • Nuevo Estado
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Activar
Resultado esperado:	Cambio de estado en el sistema
Flujo alterno	• Usuario activado previamente
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 14

Caso de Prueba CP04

Código de Identificación:	DESACTIVACIÓN DE USUARIOS CP04
Descripción:	Desactivación de Usuarios
Requisitos asociados	El usuario tiene que estar activado
Variables de Entrada (Inputs):	• Usuario • Nuevo Estado
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Activar
Resultado esperado:	Cambio de estado en el sistema
Flujo alterno	• Usuario desactivado previamente
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 15

Caso de Prueba CP05

Código de Identificación:	MODIFICACIÓN DE USUARIOS CP05
Descripción:	Modificación de los datos de un usuario
Requisitos asociados	Estar registrado en el sistema
Variables de Entrada (Inputs):	• Usuario • Nombres • Apellidos • Fecha de Nacimiento • Número de cédula • Correo Electrónico • Número Telefónico • Número Celular • Nombre de Usuario
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Actualizar
Resultado esperado:	Cambio de datos en el sistema
Flujo alterno	• No ingresar correctamente los datos • Usuario no registrado
Resultado alternativo esperado:	• Mensaje de error • No ingresar al sistema

Evaluación de prueba

Fecha de Ejecución:	17 – agosto – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 16

Caso de Prueba CP06

Código de Identificación:	ELIMINACIÓN DE USUARIOS CP06
Descripción:	Eliminación de Usuarios
Requisitos asociados	El usuario tiene que estar activo
Variables de Entrada (Inputs):	• Usuario • Nuevo Estado
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Eliminar
Resultado esperado:	Cambio de estado del usuario
Flujo alterno	• Usuario eliminado previamente
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 17

Caso de Prueba CP07

Código de Identificación:	CREACIÓN PERFIL DE USUARIO CP07
Descripción:	Creación de un nuevo perfil de usuario
Requisitos asociados	El usuario tiene que estar activo
Variables de Entrada (Inputs):	• Usuario • Nuevo Estado
Flujo normal del evento	• Seleccionar los datos de entrada • Clic en el botón Eliminar
Resultado esperado:	Cambio de estado del usuario
Flujo alterno	• Usuario eliminado previamente
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 18

Caso de Prueba CP08

Código de Identificación:	ELIMINACIÓN PERFIL DE USUARIO CP08
Descripción:	Eliminar un perfil de usuario que se encuentre creado en el sistema
Requisitos asociados	El perfil no tiene que estar asignado a ningún usuario
Variables de Entrada (Inputs):	• Perfil de Usuario
Flujo normal del evento	• Seleccionar el perfil de usuario a eliminar • Clic en el botón Eliminar
Resultado esperado:	Elimina el perfil de usuario en el sistema
Flujo alterno	• Perfil asignado a un usuario
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	Perfil se eliminó pero no mostró mensaje de confirmación
Acciones de corrección:	Colocar mensaje informativo en el sistema
Corregido por:	Bryan Vásquez

Tabla 19

Caso de Prueba CP09

Código de Identificación:	MODIFICACIÓN PERFIL DE USUARIO CP09
Descripción:	Cambiar datos de un perfil de usuario
Requisitos asociados	El perfil tiene que estar registrado
Variables de Entrada (Inputs):	• Nombre del Perfil • Descripción del perfil
Flujo normal del evento	• Seleccionar el perfil de usuario a modificar • Cambio de datos • Actualización en la base de datos
Resultado esperado:	• Actualización de datos • Mensaje de actualización
Flujo alterno	• Perfil no modificado
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 20

Caso de Prueba CP10

Código de Identificación:	ENVÍO DE DOCUMENTOS CP10
Descripción:	Enviar un documento firmado a un usuario
Requisitos asociados	• El usuario a enviar tiene que estar registrado • El documento tiene que estar firmado electrónicamente
Variables de Entrada (Inputs):	• Usuario a enviar el documento • Documento firmado • Prioridad
Flujo normal del evento	• Documento se envía al usuario • Documento se visualiza en el buzón de documentos enviados • Documento se visualiza en el buzón de entrada del usuario
Resultado esperado:	• Mensaje de actualización • Documento se visualiza en el buzón de documentos enviados • Documento se visualiza en el buzón de entrada del usuario
Flujo alterno	• Documento no firmado
Resultado alternativo esperado:	• Mensaje de error

Evaluación de prueba	
Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador	
Estado:	--
Acciones de corrección:	--

Tabla 21

Caso de Prueba CP11

Código de Identificación:	BUZÓN DE ENTRADA CP11
Descripción:	Visualización de los documentos enviados, filtros de búsqueda
Requisitos asociados	• Tener documentos recibidos
Variables de Entrada (Inputs):	• Fecha • Nombre del documento • Numero de documento • Nombre del receptor
Flujo normal del evento	• Ingreso de parámetros de búsqueda • Click en el botón de búsqueda • Visualización de los documentos enviados según los filtros de búsqueda
Resultado esperado:	• Visualización de los documentos enviados según los filtros de búsqueda
Flujo alterno	• No exista documento según los filtros ingresados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba	
Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro
Notas del programador	
Estado:	--
Acciones de corrección:	--
Corregido por:	--

Tabla 22

Caso de Prueba CP12

Código de Identificación:	BUZÓN DE SALIDA CP12
Descripción:	Visualización de los documentos recibidos, filtros de búsqueda
Requisitos asociados	• Tener documentos recibidos
Variables de Entrada (Inputs):	• Fecha • Nombre del documento • Numero de documento
Flujo normal del evento	• Ingreso de parámetros de búsqueda • Click en el botón de búsqueda • Visualización de los documentos recibidos según los filtros de búsqueda
Resultado esperado:	• Visualización de los documentos recibidos según los filtros de búsqueda
Flujo alterno	• No exista documento según los filtros ingresados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	No realiza la búsqueda por número de documento
Acciones de corrección:	Cambio en la consulta que realiza la búsqueda
Corregido por:	Bryan Vásquez

Tabla 23

Caso de Prueba CP13

Código de Identificación:	GUARDAR DOCUMENTOS CP13
Descripción:	Almacenamiento de Documentos
Requisitos asociados	• El documento tiene que estar firmado electrónicamente
Variables de Entrada (Inputs):	• Documento
Flujo normal del evento	• Seleccionar documento • Click en el botón guardar • Mensaje de almacenamiento
Resultado esperado:	• Visualización del documento en el buzón de documentos guardados
Flujo alterno	• Documento no esté firmado electrónicamente
Resultado alternativo esperado:	• Mensaje de Error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

Tabla 24

Caso de Prueba CP14

Código de Identificación:	BUZÓN DE DOCUMENTOS GUARDADOS CP14
Descripción:	Visualización de los documentos almacenados, filtros de búsqueda
Requisitos asociados	• Tener documentos almacenados
Variables de Entrada (Inputs):	• Fecha • Fecha de almacenamiento • Numero de documento
Flujo normal del evento	• Ingreso de parámetros de búsqueda • Click en el botón de búsqueda • Visualización de los documentos guardados según los filtros de búsqueda
Resultado esperado:	• Visualización de los documentos guardados según los filtros de búsqueda
Flujo alterno	• No exista documento según los filtros ingresados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

Tabla 25

Caso de Prueba CP15

Código de Identificación:	DESCARGA DE DOCUMENTOS CP15
Descripción:	Descargar los documentos firmados desde los buzones de entrada, salida y guardados
Requisitos asociados	• Tener documentos almacenados en los buzones
Variables de Entrada (Inputs):	• Documento a descargar
Flujo normal del evento	• Seleccionar el documento a descargar • Click en el botón con la imagen de descarga
Resultado esperado:	• Documento descargado
Flujo alterno	• No seleccione un documento
Resultado alternativo esperado:	• Muestra mensaje de error de descarga

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

Tabla 26

Caso de Prueba CP16

Código de Identificación:	ELIMINAR DOCUMENTO CP16
Descripción:	Eliminar un documento de los buzones de entrada, salida y/o guardados
Requisitos asociados	• Tener documentos almacenados en los buzones
Variables de Entrada (Inputs):	• Documento a eliminar
Flujo normal del evento	• Seleccionar el documento a eliminar • Click en el botón de eliminar
Resultado esperado:	• Documento descargado
Flujo alterno	• No seleccione un documento
Resultado alternativo esperado:	• Muestra mensaje de error al eliminar

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

Tabla 27

Caso de Prueba CP17

Código de Identificación:	BUZÓN DE ELIMINADOS CP17
Descripción:	Visualización de los documentos eliminados, filtros de búsqueda
Requisitos asociados	• Tener documentos eliminados
Variables de Entrada (Inputs):	• Fecha • Nombre del documento • Numero de documento
Flujo normal del evento	• Ingreso de parámetros de búsqueda • Click en el botón de búsqueda • Visualización de los documentos recibidos según los filtros de búsqueda
Resultado esperado:	• Visualización de los documentos recibidos según los filtros de búsqueda
Flujo alterno	• No exista documento según los filtros ingresados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	No realiza la búsqueda por número de documento
Acciones de corrección:	Cambio en la consulta que realiza la búsqueda
Corregido por:	Bryan Vásquez

Tabla 28

Caso de Prueba CP18

Código de Identificación:	RESTAURAR DOCUMENTOS CP18
Descripción:	Un documento eliminado posterior a la restauración debe poder verse y descargarse desde el buzón original
Requisitos asociados	• Tener documentos eliminados
Variables de Entrada (Inputs):	• Documento eliminado
Flujo normal del evento	• Seleccionar el documento • Click en el botón restaurar
Resultado esperado:	• Visualización del documento en el buzón del cual fue eliminado
Flujo alterno	• No exista el documento en el buzón de eliminados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	No muestra mensajes de error
Acciones de corrección:	Colocación de mensajes de error en el código los cuales deben mostrarse en pantalla
Corregido por:	Bryan Vásquez

Tabla 29

Caso de Prueba CP19

Código de Identificación:	PUBLICAR DOCUMENTOS CP19
Descripción:	Publicar de Documentos
Requisitos asociados	• El documento tiene que estar firmado electrónicamente
Variables de Entrada (Inputs):	• Documento
Flujo normal del evento	• Seleccionar documento • Click en el botón publicar • Mensaje de almacenamiento
Resultado esperado:	• Visualización del documento en la opción publica de documentos publicados
Flujo alterno	• Documento no esté firmado electrónicamente
Resultado alternativo esperado:	• Mensaje de Error

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

Tabla 30

Caso de Prueba CP20

Código de Identificación:	BUZÓN DE DOCUMENTOS PUBLICADOS CP20
Descripción:	Visualización de los documentos publicados, filtros de búsqueda
Requisitos asociados	• Tener documentos publicados
Variables de Entrada (Inputs):	• Fecha • Fecha de almacenamiento • Numero de documento
Flujo normal del evento	• Ingreso de parámetros de búsqueda • Click en el botón de búsqueda • Visualización de los documentos publicados según los filtros de búsqueda
Resultado esperado:	• Visualización de los documentos publicados según los filtros de búsqueda
Flujo alterno	• No exista documento según los filtros ingresados
Resultado alternativo esperado:	• Buzón muestra un mensaje de no existe documento

Evaluación de prueba

Fecha de Ejecución:	22 – junio – 2014
Ejecutado por:	Ab. Alexandra Duque
Lugar de ejecución	Unidad de Admisión y Registro

Notas del programador

Estado:	
Acciones de corrección:	
Corregido por:	

4.3.2. Resultados

4.3.2.1. Pruebas de Ingreso al Sistema

Se han establecido los siguientes casos de prueba para verificar el acceso al sistema:

- Usuario y Clave correctos
- Usuario inexistente
- Clave errónea

Tabla 31

Pruebas de Ingreso al Sistema

Caso de prueba	Información Errónea o Faltante	Resultado
1	Ninguna	Ingreso correcto
2	Usuario Inexistente	Error
3	Clave	Error

4.3.2.2. Pruebas de registro en el sistema

Para la prueba de registro en el sistema de los usuarios se ha realizado se han determinado los siguientes casos de prueba entre los que tenemos:

- Ingreso de datos correctos y completos
- Ingreso de datos no válidos:
    - Cédula errónea
    - Correo electrónico no válido
    - Número telefónico no válido
- Información obligatoria faltante
    - Nombres
    - Apellidos
    - Cédula
    - Nombre de Usuario
    - Contraseña

Resultado de las pruebas de registro de usuarios

Tabla 32

Pruebas de Registro de Usuarios

Caso de prueba	Información Errónea o Faltante	Resultado
1	Ninguna	Registro correcto
2.1	Cédula	Error
2.2	Correo Electrónico	Error
2.3	Número telefónico	Error
3.1	Nombres	Error
3.2	Apellidos	Error
3.3	Cédula	Error
3.4	Nombre de Usuario	Error
3.5	Contraseña	Error

4.3.2.3. Pruebas de activación de usuarios

Para la prueba de activación de usuarios se establecieron los siguientes casos

- Activación de un usuario desactivado
- Activación de un usuario previamente activado

Tabla 33

Pruebas de Activación de Usuarios

Caso de prueba	Información	Resultado
1	Usuario desactivado	Activación correcta
2	Usuario activado	Error

4.3.2.4. Pruebas de desactivación de usuarios

Para la prueba de desactivación de usuarios se establecieron los siguientes casos

- Desactivación de un usuario previamente desactivado
- Desactivación de un usuario activado

Tabla 34

Pruebas de Desactivación de Usuarios

Caso de prueba	Información	Resultado
1	Usuario desactivado	Error
2	Usuario activado	Desactivación Correcta

4.3.2.5. Pruebas de modificación de usuarios

Para la prueba de actualización en el sistema de los usuarios se ha realizado se han determinado los siguientes casos de prueba entre los que tenemos una vez seleccionado el usuario a modificar:

- Ingreso de datos correctos y completos
- Ingreso de datos no válidos:
    - Cédula errónea
    - Correo electrónico no válido
    - Número telefónico no válido
- Información obligatoria faltante
    - Nombres
    - Apellidos
    - Cédula
    - Nombre de Usuario

Resultado de las pruebas de registro de usuarios

Tabla 35

Pruebas de Modificación de Usuarios

Caso de prueba	Información Errónea o Faltante	Resultado
1	Ninguna	Registro correcto
2.1	Cédula	Error
2.2	Correo Electrónico	Error
2.3	Número telefónico	Error

3.1	Nombres	Error
3.2	Apellidos	Error
3.3	Cédula	Error
3.4	Nombre de Usuario	Error

4.3.2.6. Pruebas de creación de perfil de usuario

Para las pruebas de creación de perfiles de usuario se crearon los siguientes casos

- Ingreso de datos completos y correctos
- Datos faltantes
    - Nombre del Perfil
    - Descripción del Perfil

Resultados de las pruebas de creación de perfiles de usuario

Tabla 36

Pruebas de Creación de Perfil de Usuario

Caso de prueba	Información Errónea o Faltante	Resultado
1	Ninguna	Registro correcto
2.1	Nombre del Perfil	Error
2.2	Descripción del Perfil	Error

4.3.2.7. Pruebas de modificación de perfil de usuario

Para las pruebas de modificación de perfiles de usuario se crearon los siguientes casos una vez seleccionado el perfil de usuario a modificar

- Ingreso de datos completos y correctos
- Datos faltantes
    - Nombre del Perfil
    - Descripción del Perfil

Resultados de las pruebas de actualización de perfiles de usuario

Tabla 37

Pruebas de Modificación de Perfil de Usuario

Caso de prueba	Información Errónea o Faltante	Resultado
1	Ninguna	Modificación correcta
2.1	Nombre del Perfil	Error
2.2	Descripción del Perfil	Error

4.3.2.8. Pruebas de eliminación de usuarios

Para las pruebas de eliminación de perfiles de usuario se crearon los siguientes casos una vez seleccionado el perfil de usuario a eliminar

- Eliminación de un perfil sin asignar a un usuario
- Eliminación de un perfil asignado a un usuario

Resultados de las pruebas de eliminación de perfiles de usuario

Tabla 38

Pruebas de Eliminación de Usuarios

Caso de prueba	Información	Resultado
1	Perfil sin asignar	Eliminación correcta
2	Perfil asignado	Error

4.3.2.9. Pruebas de envío de documentos

Para el envío de documentos los casos de prueba que se establecieron fueron los siguientes:

- Envío de archivos firmados
    - Firma CAdES
    - Firma XAdES
    - Firma PAdES
- Envío de archivos sin Firma

Resultados de la prueba de envío de documentos

Tabla 39

Pruebas de Envío de Documentos

Documento	Tipo de Documento	Firma	Resultado
1	.doc	NO	Error
2	.xls	NO	Error
3	.scl	CAdES	OK
4	.slc	XAdES	OK
5	.pdf	PAdES	OK
6	.pdf	NO	Error
7	.xml	NO	Error

4.3.2.10. Pruebas del buzón de entrada

En el buzón de entrada se estableció el caso de prueba:

- Carga únicamente de documentos recibidos según el usuario que inició sesión en el sistema

Resultado de las pruebas en el buzón de entrada

Tabla 40

Pruebas del Buzón de Entrada

Caso de prueba	Información	Resultado
1	Inicio de Sesión	Documentos Recibidos

4.3.2.11. Pruebas del buzón de salida

En el buzón de salida se estableció el caso de prueba:

- Carga únicamente de documentos enviados según el usuario que inició sesión en el sistema

Resultado de las pruebas en el buzón de salida

Tabla 41

Pruebas del Buzón de Salida

Caso de prueba	Información	Resultado
1	Inicio de Sesión	Documentos Enviados

4.3.2.12. Pruebas de almacenamiento de documentos

Para el almacenamiento de documentos los casos de prueba que se establecieron fueron los siguientes:

- Almacenamiento de archivos firmados
  - Firma CAdES
  - Firma XAdES
  - Firma PAdES
- Almacenamiento de archivos sin Firma

Resultados de las pruebas de almacenamiento de archivos.

Tabla 42

Pruebas de Almacenamiento de Documentos

Documento	Tipo de Documento	Firma	Resultado
1	.xls	NO	Error
2	.pdf	NO	Error
3	.scl	XAdES	OK
4	.slc	CAdES	OK
5	.pdf	PAdES	OK
6	.jpg	NO	Error
7	.doc	NO	Error

4.3.2.13. Pruebas de descarga de documentos

Para la descarga de documentos se establecieron los casos de prueba:

- Descarga desde el buzón de entrada
    - Archivo PDF
    - Archivo SLC
- Descarga desde el buzón de salida
    - Archivo PDF
    - Archivo SLC
- Descarga desde el buzón de guardados
    - Archivo PDF
    - Archivo SLC

Resultados de las pruebas de descarga de documentos

Tabla 43

Pruebas de Descarga de Documentos

Documento	Tipo de Documento	Firma	Resultado
1.1	.slc	PAdES	OK
1.2	.pdf	CAdES	OK
2.1	.scl	PAdES	OK
2.2	.pdf	CAdES	OK
3.1	.slc	PAdES	OK
3.2	.pdf	CAdES	OK

4.3.2.14. Pruebas de eliminación de documentos

Para la eliminación de documentos se establecieron los casos de prueba:

- Eliminación desde el buzón de entrada
    - Archivo PDF
    - Archivo SLC
- Eliminación desde el buzón de salida
    - Archivo PDF
    - Archivo SLC
- Eliminación desde el buzón de guardados
    - Archivo PDF

- Archivo SLC

Resultados de las pruebas de eliminación de documentos

Tabla 44

Pruebas de Eliminación de Documentos

Documento	Tipo de Documento	Firma	Resultado
1.1	.pdf	PAdES	OK
1.2	.slc	CAdES	OK
2.1	.pdf	PAdES	OK
2.2	.slc	CAdES	OK
3.1	.pdf	PAdES	OK
3.2	.slc	CAdES	OK

4.3.2.15. Pruebas del buzón de documentos eliminados

En el buzón de eliminados se estableció el caso de prueba:

- Carga únicamente de documentos eliminados según el usuario que inició sesión en el sistema

Resultado de las pruebas en el buzón de eliminados

Tabla 45

Pruebas del Buzón de Documentos Eliminados

Caso de prueba	Información	Resultado
1	Inicio de Sesión	Documentos Eliminados

4.3.2.16. Pruebas de restauración de documentos

Para la eliminación de documentos se establecieron desde el buzón de documentos eliminados los casos de prueba:

- Restauración de documentos
  - Archivo PDF
  - Archivo SLC

Resultado de las pruebas de la restauración de documentos

Tabla 46

Pruebas de Restauración de Documentos

Documento	Tipo de Documento	Firma	Resultado
1.1	.pdf	PAdES	OK
1.2	.slc	CAdES	OK

4.3.2.17. Pruebas del buzón de documentos guardados

En el buzón de documentos guardados se estableció el caso de prueba:

- Carga únicamente de documentos guardados según el usuario que inició sesión en el sistema

Resultado de las pruebas en el buzón de guardados

Tabla 47

Pruebas del Buzón de Documentos Guardados

Caso de prueba	Información	Resultado
1	Inicio de Sesión	Documentos Guardados

4.3.2.18. Pruebas de publicación de documentos

Para la publicación de documentos los casos de prueba que se establecieron fueron los siguientes:

- Publicación de archivos firmados
    - Firma CAdES
    - Firma XAdES
    - Firma PAdES
- Publicación de archivos sin Firma

Resultados de las pruebas de publicación de archivos.

Tabla 48

Pruebas de Publicación de Documentos

Documento	Tipo de Documento	Firma	Resultado
1	.xls	NO	Error
2	.pdf	NO	Error
3	.scl	XAdES	OK
4	.slc	CAdES	OK
5	.pdf	PAdES	OK
6	.jpg	NO	Error
7	.doc	NO	Error

4.3.2.19. Pruebas del buzón de documentos publicados

En el buzón de documentos publicados se estableció el caso de prueba:

- Carga únicamente de documentos publicados según el usuario que inició sesión en el sistema

Resultado de las pruebas en el buzón de publicados

Tabla 49

Pruebas de Documentos Publicados

Caso de prueba	Información	Resultado
1	Inicio de Sesión	Documentos Publicados

4.3.2.20. Pruebas de Firma

El proceso de firma se realiza mediante la aplicación de la Autoridad de Certificación ANF llamada Plug & Sign para lo cual se van a realizar los tres tipos de firma especificados que son CAdES, PAdES y XAdES; para lo cual se han creado 6 documentos con distintos formatos para dichas pruebas.

Resultados de la prueba de firma

Tabla 50

Pruebas de Firma

Documento	Nombre	Tipo de Firma	Resultado
1	Prueba de Firma 1	CAdES	OK
2	Prueba de Firma 2	CAdES	OK
3	Prueba de Firma 3	PAdES	OK
4	Prueba de Firma 4	PAdES	OK
5	Prueba de Firma 5	XAdES	OK
6	Prueba de Firma 6	XAdES	OK

4.3.2.21. Pruebas de validación

El proceso de validación de firma consiste en utilizar la herramienta proporcionada por ANF llamada Plug & Sign y una herramienta externa cuyo nombre es XolidoSign mediante las cuales se va a poder verificar la validez del documento firmado para lo cual se han obtenido 6 documentos con los distintos formatos CAdES, PAdES y XAdES.

Resultados de las pruebas de validación de firma utilizando herramienta Plug & Sign

Tabla 51

Pruebas de Validación

Documento	Sello de Tiempo	Tipo de Firma	Resultado
1	SI	CAdES	OK
2	SI	CAdES	OK
3	NO	CAdES	No Válida
4	NO	PAdES	No Válida
5	SI	PAdES	OK
6	SI	PAdES	OK
7	NO	XAdES	No Válida
8	SI	XAdES	OK

9	SI	XAdES	OK

4.3.2.22. Pruebas de validación con XolidoSign

Se selecciona el documento a verificar.

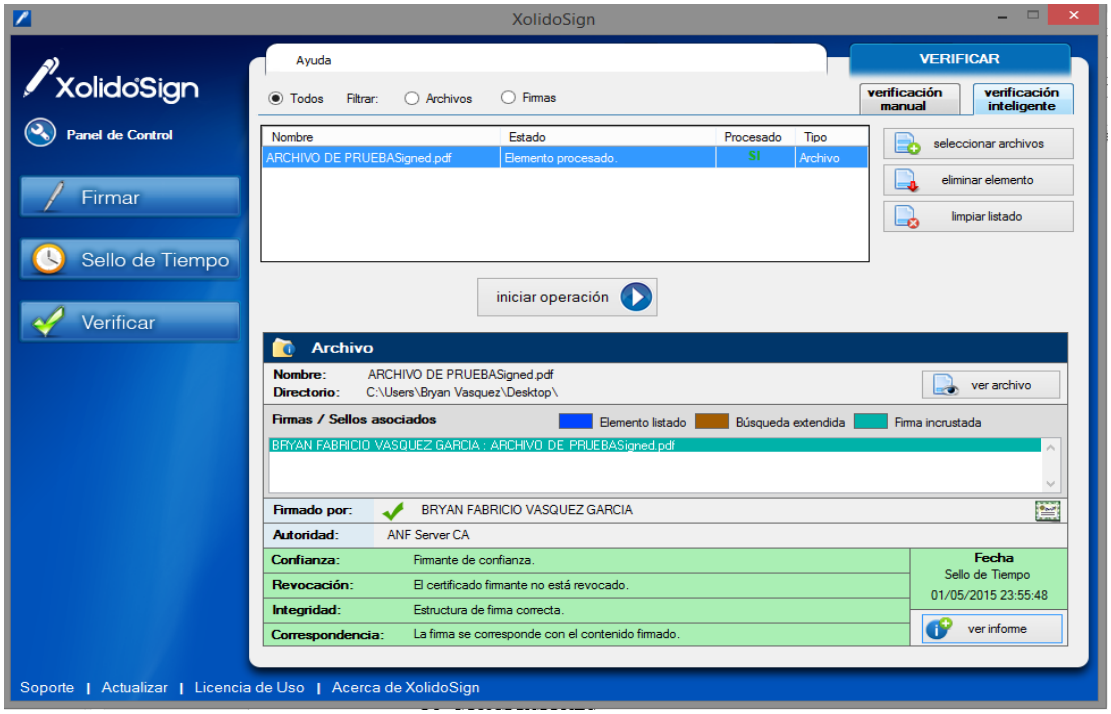


Figura 53 Verificación de Firma con XolidoSign

Mediante la opción ver archivo se puede abrir este y verificar la firma del documento.

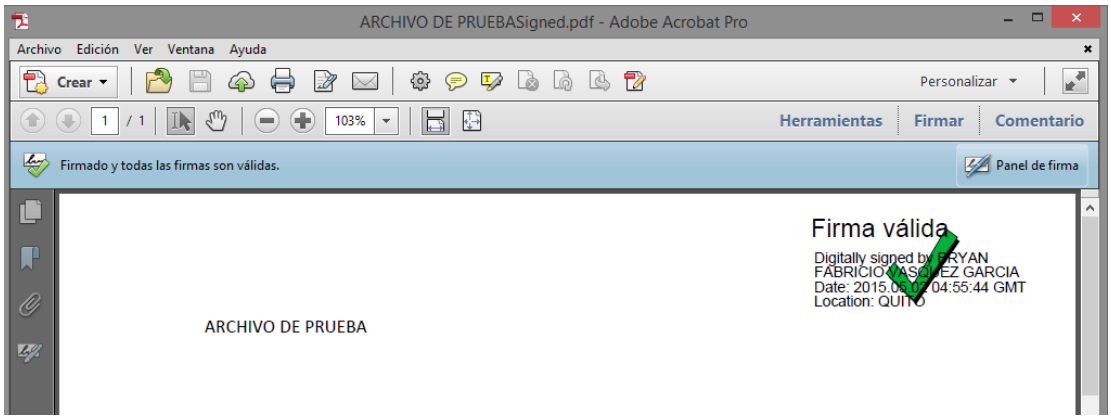


Figura 54 Archivo Firmado

En la opción ver certificado se puede verificar los datos del firmante y del certificado; además del sello de tiempo estampado en el documento.

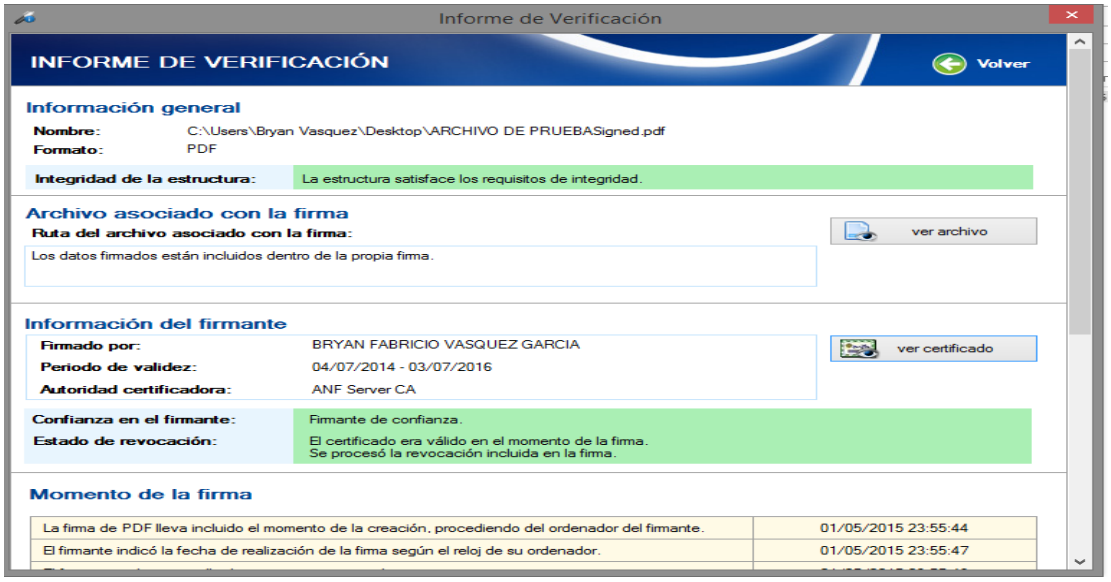


Figura 55 Identidad del Firmante

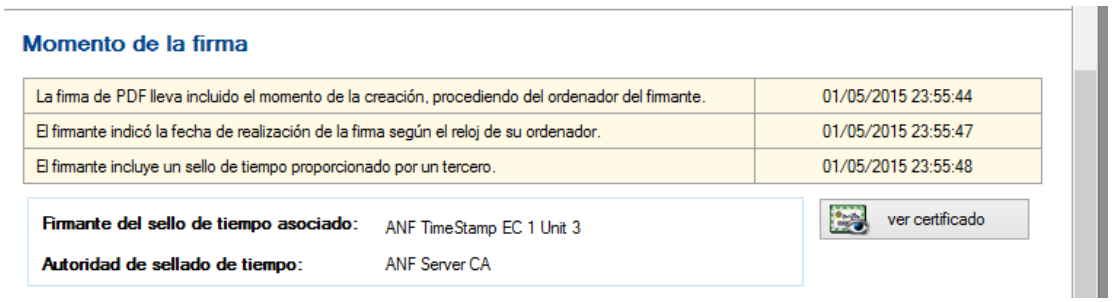


Figura 56 Sello de Tiempo

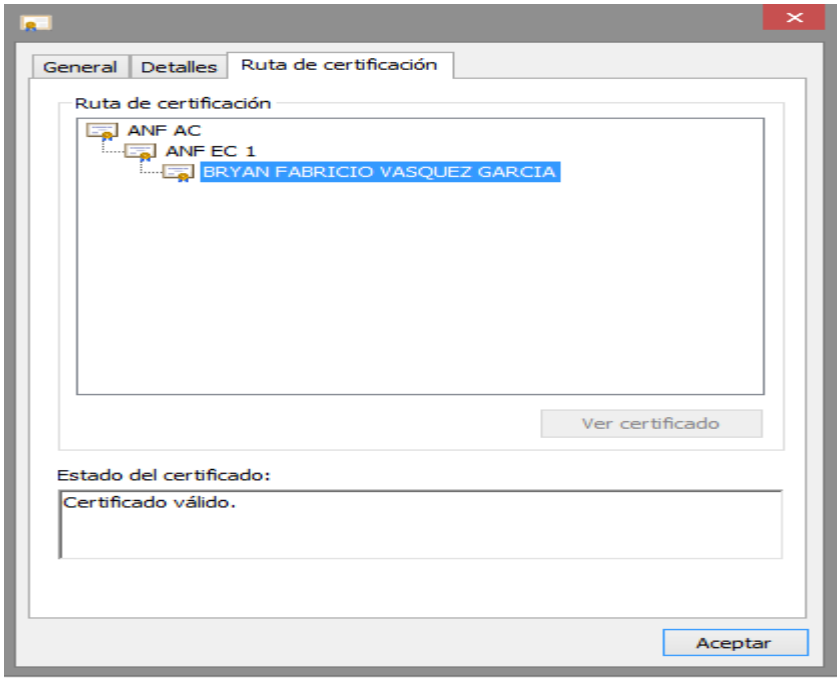


Figura 57 Ruta de Certificación

CAPÍTULO 5

CONCLUSIONES Y RECOMENDACIONES

5.1. CONCLUSIONES

Una vez finalizado el tema de tesis se han obtenido las siguientes conclusiones:

- La gran cantidad de documentos que se manejan de forma física en la actualidad ocasiona retrasos y pérdida de estos por lo que se debe tener las herramientas que faciliten los procesos de las organizaciones mediante nueva tecnología de esta manera mejorando los tiempos y organización de los documentos.
- Los certificados electrónicos proporcionan al documento firmado las garantías jurídicas y legales que estos necesitan como son: identidad, integridad y no repudio permitiendo que estos documentos tengan la misma validez jurídica que los documentos que hayan sido firmados de forma manuscrita.
- La metodología de desarrollo SCRUM permite realizar el sistema de una manera rápida entregando funcionalidades probadas por el usuario es decir de manera incremental con la intervención de este, de esta manera cumplir con sus requerimientos y cambios priorizando el beneficio de cada una de estas entregas.
- El Buzón de Documentos Firmados Electrónicamente ha sido desarrollado como solución a la gestión de la información garantizando la seguridad y manejo de esta a través de la integración de herramientas de infraestructura; además de frameworks de desarrollo facilitando el manejo de esta plataforma digital.
- Se utilizaron las APIs y herramientas de firma digital de ANF AC las cuales permiten la validación de los documentos electrónicos emitidos y recibidos, se ha utilizado además herramientas de software libre para facilitar el desarrollo de la aplicación.

5.2. RECOMENDACIONES

La culminación del proyecto ha llevado a obtener las siguientes recomendaciones:

- Los usuarios del Buzón de Documentos Firmados Electrónicamente el uso de certificados de firma electrónica de ANF AC Ecuador que permite aprovechar de mejor manera la gestión de documentos.
- Difundir el conocimiento de todo lo que representan las firmas electrónicas hacia los usuarios de los certificados digitales ya que en la Universidad de las Fuerzas Armadas no existe la información suficiente, permitiendo avanzar a la par de las nuevas tecnologías implementadas.
- La actualización periódica de las herramientas implementadas de esta manera obtener un correcto funcionamiento de la aplicación mejorando los tiempos de respuesta.
- Actualizar los conocimientos en el ámbito legal en el manejo de los certificados electrónicos ya que un mal manejo de estos puede traer problemas de carácter legal y jurídico; además de mantener en vigencia este dispositivo y conocer los procedimientos en caso de renovación y revocación en caso de ser necesario.
- Los usuarios deben mantener actualizadas las versiones de los exploradores facilitando de esta manera el correcto funcionamiento de la aplicación WEB.

BIBLIOGRAFÍA

Agut, R. M. (s.f.). Especificación de Requisitos Software según el estándar de IEEE 830.

Albaladejo, X. (31 de Enero de 2014). *Proyectos Agiles* . Obtenido de http://www.proyectosagiles.org

ANALUISA, V. (18 de Mayo de 2015). Obtenido de https://vicenteanaluisa.wordpress.com/2010/07/06/ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos/

ANF AC. (18 de Mayo de 2015). Obtenido de http://www.anf.es/

Banco Central. (18 de Mayo de 2015). Obtenido de https://www.eci.bce.ec/firma-electronica

Carrero, A. (18 de Mayo de 2015). *Programación en Castellano*. Obtenido de http://programacion.net/articulo/conceptos_basicos_de_orm_object_relational_mapping_349

Çivici, Ç. (17 de Marzo de 2015). *Primefaces.* Obtenido de http://www.primefaces.org/docs/guide/primefaces_user_guide_5_0.pdf

Díaz, E. (27 de Diciembre de 2014). *EiTheL Inside*. Obtenido de http://eithel-inside.blogspot.com/2010/04/apache-tomcat-en-ubuntu-jakarta-tomcat.html

Díaz, F. (2010). *Curso Director de Sistemas de Certificacion y Firma Electronica.* Barcelona, España: IBD, SA.

Dueñas, J. B. (21 de Septiembre de 2014). *Alcance Libre*. Obtenido de http://www.alcancelibre.org/staticpages/index.php/como-mysql-quickstart

ECUADOR, C. N. (25 de Junio de 2014). *Red GEALC*. Obtenido de http://www.redgealc.net/ecuador-reglamento-a-la-ley-de-comercio-electronico-firmas-electronicas-y-mensajes-de-datos/contenido/2251/es/

EcuRed. (18 de Mayo de 2015). Obtenido de http://www.ecured.cu/index.php/NetBeans

EcuRed. (18 de Mayo de 2015). Obtenido de http://www.ecured.cu/index.php/PKI

EcuRed. (18 de Mayo de 2015). Obtenido de http://www.ecured.cu/index.php/PowerDesigner

EcuRed. (18 de Mayo de 2015). Obtenido de http://www.ecured.cu/index.php/Mysql

Eduardo. (18 de Mayo de 2015). *Indira*. Obtenido de http://indira-informatica.blogspot.com/2007/09/qu-es-mysql.html

Esteban, E. A. (28 de Abril de 2010). *Programacion en castellano*. Obtenido de http://programacion.net/articulo/tomcat_-_introduccion_134#tomcat1

González, H. S. (30 de Abril de 2015). *Manual Hibernate.* Obtenido de http://static1.1.sqspcdn.com/static/f/923743/14427535/1317484934257/ManualHibernate.pdf?token=vcyGecQ0xB%2Fx0%2BW7YXMaHGM07YE%3D

Groussard, T. (2010). *Java Enterprise Edition: Desarrollo de aplicaciones web con JEE 6.* Ediciones ENI.

Hibernate. (30 de Marzo de 2015). Obtenido de http://www.cartagena99.com/recursos/programacion/apuntes/ManualHibernate.pdf

Ileana Patricia Loaisiga Hernández, C. E. (20 de Noviembre de 2014). *CentOS.* Obtenido de http://latecnologiasocial.bligoo.es/media/users/14/745746/files/117525/Manual_CentOS5_6.pdf

Navarro, Á. N. (18 de Mayo de 2015). *LEFISPedia*. Obtenido de http://lefis.unizar.es/wiki/doku.php?id=es:infraestructura_de_clave_publica_pki

Oracle. (18 de Mayo de 2015). Obtenido de http://docs.oracle.com/cd/E19226-01/820-7627/gijue/index.html

Pressman, R. S. (2010). *Ingenieria del Software, un enfoque práctico.* Mexico: McGRAW HILL INTERAMERICADA EDITORES.

Quijano, J. A. (18 de Mayo de 2015). *TECNOLOGIAS PARA LA WEB*. Obtenido de https://prezi.com/lbs-mggizrgo/tecnologias-para-la-web/

Rahul. (10 de Abril de 2015). *Tecadmin*. Obtenido de http://tecadmin.net/steps-to-install-tomcat-server-on-centos-rhel/

Scrummanager. (18 de Mayo de 2015). Obtenido de http://www.scrummanager.net/bok/index.php?title=Historia_de_usuario

Security Data. (18 de Mayo de 2015). Obtenido de https://www.securitydata.net.ec/

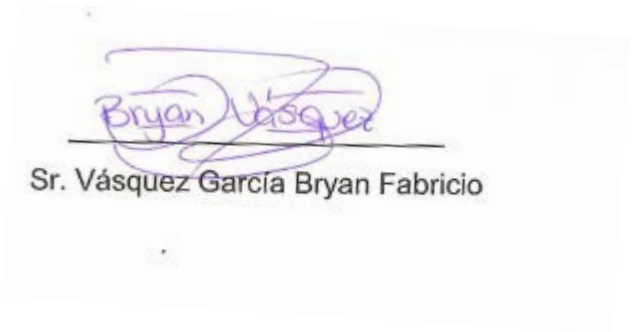
Systems, P. S. (15 de Marzo de 2015). *Modelado de Sistemas com UML*. Obtenido de http://es.tldp.org/Tutoriales/doc-modelado-sistemas-UML/doc-modelado-sistemas-uml.pdf

Xavier Ferré Grau, M. I. (30 de Marzo de 2015). *Desarrollo Orientado a Objetos con UML*. Obtenido de http://www.uv.mx/personal/maymendez/files/2011/05/umlTotal.pdf

XolidoSign. (18 de Mayo de 2015). Obtenido de http://www.en.xolido.com/lang/productosxolidosign/pais/modulo/ecuador/?refsec=ecu_autoridades

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADO POR



Sangolquí, Junio del 2015