ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS

INNOVACIÓN PARA LA EXCELENCIA

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN

CARRERA INGENIERÍA EN SISTEMAS E INFORMÁTICA

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

TEMA: DESARROLLO DE UN CLIENTE SOAP UTILIZANDO UN WEB SERVICE JAVA PARA DISPOSITIVOS MÓVILES ANDROID, BASADOS EN CERTIFICADOS DIGITALES DE FIRMA ELECTRÓNICA.

AUTOR: DAZA VELÁSQUEZ, FRANCISCO GABRIEL

DIRECTOR: ING. MAURICIO CAMPAÑA

SANGOLQUÍ, OCTUBRE 2015

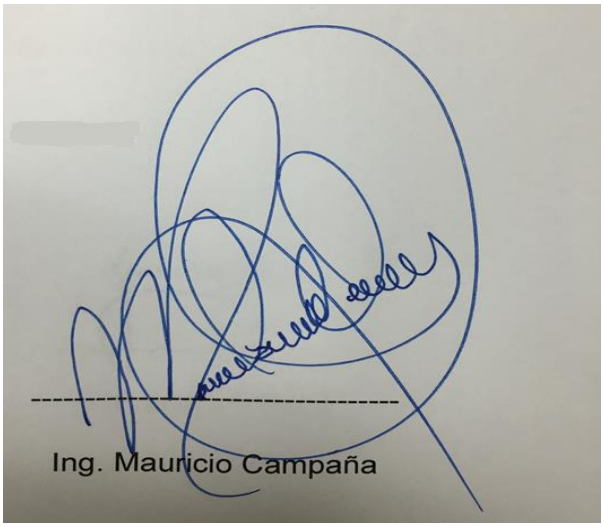
CERTIFICACIÓN

Ing. Mauricio Campaña

CERTIFICA

Que el trabajo titulado "DESARROLLO DE UN CLIENTE SOAP UTILIZANDO UN WEB SERVICE JAVA PARA DISPOSITIVOS MÓVILES ANDROID, BASADOS EN CERTIFICADOS DIGITALES DE FIRMA ELECTRÓNICA" realizado por el señor Francisco Gabriel Daza Velásquez, ha sido guiado y revisado periódicamente y cumple como requerimiento parcial a la obtención del título de INGENIERÍA EN SISTEMAS E INFORMÁTICA.

Sangolquí, Octubre, 01 del 2015



DECLARACIÓN DE RESPONSABILIDAD

Daza Velásquez Francisco Gabriel

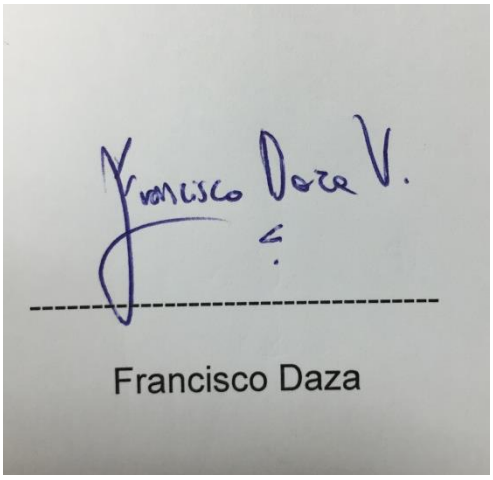
DECLARO QUE:

La presente tesis de grado titulada “DESARROLLO DE UN CLIENTE SOAP UTILIZANDO UN WEB SERVICE JAVA PARA DISPOSITIVOS MÓVILES ANDROID, BASADOS EN CERTIFICADOS DIGITALES DE FIRMA ELECTRÓNICA”, ha sido desarrollada en base a una investigación exhaustiva, respetando derechos intelectuales de terceros, conforme las citas que constan en la bibliografía.

Consecuentemente este trabajo es de nuestra autoría.

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

Sangolquí, Octubre, 01 del 2015



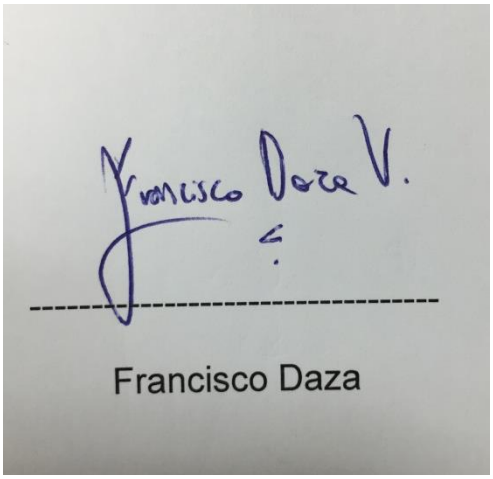
AUTORIZACIÓN DE PUBLICACIÓN

Daza Velásquez Francisco Gabriel

AUTORIZO:

A la UNIVERSIDAD DE LAS FUERZAS ARMADAS la publicación en la Biblioteca Virtual de la Institución, del trabajo titulado “DESARROLLO DE UN CLIENTE SOAP UTILIZANDO UN WEB SERVICE JAVA PARA DISPOSITIVOS MÓVILES ANDROID, BASADOS EN CERTIFICADOS DIGITALES DE FIRMA ELECTRÓNICA”, que es de mi propia autoría y responsabilidad.

Sangolquí, Octubre, 01 del 2015



DEDICATORIA

El presente trabajo dedico a mis padres y sobre todo a mi madre Sra. María Teresa Velásquez que me ha brindado su apoyo incondicional por estar siempre a mi lado en mis éxitos, fracasos y guiándome con buenos consejos sin los cuales no hubiese podido terminar el presente trabajo.

A mi familia por estar siempre a mi lado para darme fuerzas en mi constante crecimiento profesional.

A Geovanna por estar a mi lado y confiar en mi para alcanzar las metas que me propongo.

Francisco Gabriel Daza Velásquez

AGRADECIMIENTO

Agradezco a una persona espiritual Dios, por estar todos los días en mi vida e ir guiándome con sabiduría para culminar exitosamente esta etapa de mi carrera profesional.

Gracias por siempre a mi director de carrera ing. Mauricio Campaña que también fue el director de la tesis por su paciencia, brindar su valioso conocimiento y su constante apoyo para la realización de este presente trabajo.

A la prestigiosa Universidad de las Fuerzas Armadas y a todos sus maestros, por brindarme con profesionalismo sus conocimientos, que transmitiré a lo largo de mi vida profesional.

A la empresa ANF A.C. por su confianza y apoyo en la realización de este proyecto.

Y a todos los que alguna manera estuvieron apoyándome y colaborándome para la elaboración y finalización del presente trabajo.

Francisco Gabriel Daza Velásquez

ÍNDICE DE CONTENIDOS

CERTIFICACIÓN ii
DECLARACIÓN DE RESPONSABILIDAD iii
AUTORIZACIÓN DE PUBLICACIÓN iv
DEDICATORIA v
AGRADECIMIENTO vi
RESUMEN xiv
ABSTRACT xv
1. CAPÍTULO 1 1
INTRODUCCIÓN 1
1.1. TEMA 1
1.2. ANTECEDENTE 1
1.3. PLANTEAMIENTO DEL PROBLEMA 3
1.4. JUSTIFICACIÓN 3
1.5. OBJETIVOS 4
1.5.1. General 4
1.5.2. Específicos 4
1.6. ALCANCE 4
2. CAPÍTULO 2 9
MARCO DE REFERENCIA 9
2.1. Introducción a la firma Electrónica 9
2.1.1. Paradigma de la firma electrónica 9
2.1.2. Que es firma 9
2.1.3. Elementos de la firma 10
2.1.4. Tipos de Firma 11
2.1.5. Firma Electrónica 12
2.2. Introducción a los certificados digitales 15
2.2.1. Certificados Digitales 15
2.2.2. Certificados X.509 16
2.2.3. Autoridades Certificadoras (CA) 18
2.3. Ley de Comercio Electrónico del Ecuador 19
2.4. Introducción a la tecnología móvil Android 21

2.4.1. Que es Android 21
2.4.2. La experiencia Google en los teléfonos móviles 23
2.5. Introducción al Web Service 23
2.5.1. WSDL 25
2.5.2. Estructura 26
2.6. Metodología 27
2.6.1. Análisis de Requisitos 29
2.6.2. Diseño del Sistema y del Software 29
2.6.3. Codificación 29
2.6.4. Prueba 30
2.6.5. Verificación 30
2.6.6. Mantenimiento 30
3. CAPÍTULO 3 32
ANÁLISIS Y DISEÑO DEL SISTEMA 32
3.1. Análisis de Requisitos 32
3.1.1. Conceptualización Del Sistema 32
3.1.2. Ingeniería y Análisis del Sistema 32
o Descripción del Sistema 32
o Funcionalidad 33
o Características de los Usuarios 34
3.1.3. Análisis de los requisitos del Software 34
o Requisitos Interfaces 34
o Requisitos Funcionales 36
o Requisitos no Funcionales 42
3.2. Diseño del Sistema y del Software 43
3.2.1. Diagramas de Comportamiento 43
3.2.2. Diagramas de Estructura Entidad Relación 51
3.2.3. Diccionario de Datos 54
3.2.4. Diseño de Interfaces 57
4. CAPÍTULO 4 70
IMPLEMENTACIÓN DEL SISTEMA 70
4.1. Codificación 70
4.1.1. Cliente SOAP 70

4.1.2. Web Service Firma 71
4.2. Pruebas y Verificación 74
4.2.1. Pruebas Unitarias 74
4.2.2. Pruebas de Integración 91
4.2.3. Pruebas de Sistema 93
4.2.4. Pruebas de Aceptación 95
5. CAPÍTULO 5 98
RESULTADOS 98
5.1. Conclusiones 98
5.2. Recomendaciones 99
BIBLIOGRAFÍA 100
BIOGRAFÍA 101
HOJA DE LEGALIZACIÓN DE FIRMAS 102

ÍNDICE DE FIGURAS

Figura 1 - Esquema Registro de Usuarios y Login de Usuario Administrador 6
Figura 2 - Esquema de Gestión de elaboración, firma de actas de reuniones 6
Figura 3 - Esquema Login Acceso de Usuario 7
Figura 4 - Esquema firma acta de reunión 7
Figura 5 - Esquema de pruebas (Eugenio Juárez Clavín). 8
Figura 6 - Arquitectura de Distribución de componentes Android (Alejandro Nieto González) 22
Figura 7 - Pila de Protocolo Web Service (Miguel Rodríguez) 23
Figura 8 - Proceso de utilización Web Service (Miguel Rodríguez) 24
Figura 9 - pasos de consumo de Web Service (IBM webSphere) 26
Figura 10 - Estructura lenguaje WSDL 27
Figura 11 – Etapas de la Metodología UWE (Raúl Martínez) 28
Figura 12 – Caso de Uso 1 Usuario Administrador 43
Figura 13 - Caso de Uso 2 Usuario Normal 44
Figura 14 - Caso de Uso 3 Cliente SOAP 44
Figura 15 - Caso de Uso 4 Web Service 45
Figura 16 - Diagrama de Secuencia 1 Autenticación Simple Usuario 45
Figura 17 - Diagrama de Secuencia 2 Inicio de Sesión 46
Figura 18 - Diagrama de Secuencia 3 Cierre Sesión 46
Figura 19 - Diagrama de Secuencia 4 Registro Usuario 47
Figura 20 - Diagrama de Secuencia 5 Creación Acta de Reunión 47
Figura 21 - Diagrama de Secuencia 6 Validación de Documentos 48
Figura 22 - Diagrama de Secuencia 7 Validación llaves Publicas Certificado 48
Figura 23 - Diagrama de Secuencia 8 Validación Certificado 49
Figura 24 - Diagrama de Secuencia 9 Firma Acta Administrador 49
Figura 25 - Diagrama de Secuencia 10 Repositorio Documental 50
Figura 26 - Diagrama de Secuencia 11 Envío Notificación 50
Figura 27 - Diagrama Lógico 1 Gestión de Firma y Usuarios 51

Figura 28 - Diagrama Clases 1 Gestión de Firma y Usuarios 52
Figura 29 - Diagrama Físico 1 Gestión de Firma y Usuarios 53
Figura 30- Diseño Aplicación 57
Figura 31- Diseño Interfaz Login 57
Figura 32- Diseño Interfaz Login 2 58
Figura 33- Diseño Interfaz Menú Administrador 58
Figura 34- Diseño Interfaz Registro 59
Figura 35- Diseño Interfaz Registro 2 59
Figura 36-Diseño Interfaz Formulario 60
Figura 37-Diseño Interfaz Menú asistentes 60
Figura 38-Diseño Interfaz Firma 61
Figura 39-Diseño Interfaz Menú Asistentes 61
Figura 40-Diseño Interfaz Firma 2 62
Figura 41-Diseño Interfaz Correo 62
Figura 42-Diseño Interfaz PDF Firmado 63
Figura 43-Diseño Interfaz Correo 2 63
Figura 44-Diseño Interfaz PDF Firma 2 64
Figura 45- Diseño Interfaz Correo 3 64
Figura 46- Diseño Interfaz PDF Firma 3 65
Figura 47-Diseño Interfaz Login Cliente 65
Figura 48-Diseño Interfaz Firma Cliente 66
Figura 49- Diseño Interfaz Firma Cliente 2 66
Figura 50-Diseño Interfaz Correo Cliente 67
Figura 51-Diseño Interfaz PDF Firma Cliente 67
Figura 52-Diseño Interfaz Correo Cliente 2 68
Figura 53-Diseño Interfaz PFD Firma Cliente 2 68
Figura 54-Diseño Interfaz Correo MultiFirma 69
Figura 55- Diseño Interfaz PDF MultiFirma 69
Figura 56-Librerías Consumo WS 70
Figura 57-librerías de Firma ANF 73
Figura 58-Prueba 1 75
Figura 59-Prueba 2 76

Figura 60-Prueba 1 77
Figura 61-Prueba 2 78
Figura 62-Prueba 3 79
Figura 63-Prueba 4 80
Figura 64-Prueba 5 81
Figura 65-Prueba 6 82
Figura 66-Prueba 7 83
Figura 67-Prueba 8 84
Figura 68-Prueba 9 85
Figura 69-Prueba 10 85
Figura 70-Prueba 11 86
Figura 71-Prueba 12 87
Figura 72-Prueba 13 88
Figura 73-Prueba 14 89
Figura 74-Prueba 15 90
Figura 75--Prueba 1 91
Figura 76-Prueba 1.1 92
Figura 77-Prueba 2 92
Figura 78-Prueba 1 93
Figura 79-Prueba 2 94
Figura 80-Prueba 2.1 94
Figura 81-Prueba 1 95
Figura 82-Prueba 2 95
Figura 83-Prueba 4 96
Figura 84-Prueba 4 96
Figura 85-Prueba 4.1 97

ÍNDICE DE TABLAS

Tabla 1 - Requisito Funcional 1 36
Tabla 2 - Requisito Funcional 2 36
Tabla 3 - Requisito Funcional 3 37
Tabla 4 - Requisito Funcional 4 37
Tabla 5 - Requisito Funcional 5 38
Tabla 6 - Requisito Funcional 6 38
Tabla 7 - Requisito Funcional 7 39
Tabla 8 - Requisito Funcional 8 39
Tabla 9 - Requisito Funcional 9 40
Tabla 10 - Requisito Funcional 10 40
Tabla 11 - Requisito Funcional 11 41
Tabla 12 - Requisito Funcional 12 41
Tabla 13 - Requisito Funcional 13 41
Tabla 14 - Requisito Funcional 14 42
Tabla 15 - Tabla Usuario 54
Tabla 16 - Tabla Certificado 55
Tabla 17 - Tabla Documento 55
Tabla 18 - Tabla Información Documento 56
Tabla 19--Prueba 76
Tabla 20-Prueba 90
Tabla 21-Prueba 93
Tabla 22-Prueba 95
Tabla 23-Prueba 97

RESUMEN

El Desarrollo de un Cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica permite simplificar la organización de los recursos al momento de realizar una reunión de cualquier interés dentro o fuera de la empresa. Al aplicar un cliente SOAP móvil relacionado con servicios web y librerías electrónicas tendremos un sistema con la más alta calidad de las tecnologías actuales que permitirá elaborar, firmar y enviar notificaciones vía correo las actas de reuniones para el representante y sus asistentes, obteniendo resultados eficaces al no tener problemas de acceso a internet porque se puede utilizar datos móviles , eliminando el uso del papel físico (uso de documento digital formato PDF), y los más importante dejando en constancia legal (firma electrónica) que todos los asistentes a la reunión estuvieron presentes dejando en conocimiento los puntos tratados dentro del mismo.

PALABRAS CLAVE:

- **SOAP**
- **FORMATO PDF**
- **ANDROIDE**
- **FIRMA ELECTRÓNICA**

ABSTRACT

Developing a SOAP client using a java web service for android mobile devices, based on digital certificates of electronic signature simplifies the organization of resources at the time of a meeting of any interest in or outside the Company.

Applying a mobile client SOAP related with web services and electronics libraries have a system with the highest quality of current technologies that allow prepare, sign and send notifications via mail the meeting minutes for the representative and his assistants, obtaining effective results to not problems of internet access because you can use mobile data, eliminating the use of physical paper (use of digital document PDF format), and most importantly leaving legal proof (electronic signature) that all those attending the meeting were knowledge leaving the points raised therein.

KEYWORDS:

- **SOAP**
- **FORMAT PDF**
- **ANDROID**
- **SIGNATURE ELECTRONIC**

1. CAPÍTULO 1

INTRODUCCIÓN

1.1. TEMA

Desarrollo de un Cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica.

1.2. ANTECEDENTE

En la antigüedad para identificar la autenticidad de las personas en documentos físicos utilizaban sellos, en el transcurso de los siglos esto cambió a la firma manuscrita, la cual ha sido la forma tradicional para identificar a las personas en las transacciones realizadas en varios tipos de documentos como: tributarios, acta de reuniones, contratos, cheques, entre otros. (Zúñiga, 2011)

En la actualidad la mayoría de las personas utilizan el internet como fuente de investigación, entretenimiento, transacciones, almacenamiento y un sin número de actividades logrando una fácil comunicación a nivel mundial, además con el uso de la tecnología facilita la transferencia de robustos papeles físicos a ligeros documentos electrónicos. (Zúñiga, 2011)

A través de la documentación electrónica se realiza un sin número de actividades en la web, pero no toda transacción documental es segura, a esto se creó los certificados digitales de firma electrónica, para dar identidad única a un documento. (Zúñiga, 2011)

El certificado digital es un documento electrónico cifrado con información del adquiriente, que permite firmar electrónicamente, este certificado puede

ser en archivo, en tarjeta DNI electrónica o un dispositivo pen-drive. (Token) (Zúñiga, 2011)

El certificado Digital consta de una pareja de claves criptográficas públicas y privadas, que utiliza algoritmos matemáticos, de tal manera que las claves son dependientes para poder descifrar, obteniendo documentos electrónicos seguros. (Zúñiga, 2011)

La firma electrónica va más allá de la firma manuscrita, dando valores de legitimación, identidad propia y seguridad, permitiendo garantizar la integridad y confidencialidad del documento electrónico y el compromiso del firmante con los datos insertados en el previo documento. Al documento electrónico se lo puede firmar el número de veces que sean necesarias para finalizar su validez, esto se le llama firmas múltiples electrónicas. (Zúñiga, 2011)

En este país (Ecuador) la firma y la firma múltiple electrónica difundida por la Ley de Comercio Electrónico del Ecuador está adquiriendo un valor muy importante para varias utilidades, una de ellas es la seguridad en la trasparencia de la información y mensajes de datos. (Novoa, 2002)

La tecnología se ha convertido el elemento fundamental para el ser humano logrando facilitar las actividades diarias, una de estas se encuentra relacionada con el uso de dispositivos móviles inteligentes basados en la tecnología Android, esta tecnología permite administrar diferentes tipos de aplicaciones con avanzadas capacidades siendo hoy en día competidores con otros sistemas operativos considerados recientemente como líderes a nivel mundial. (Wesley, 2011)

Android cumple todas las características de ser simples y amigables con el usuario impulsando rápidamente hacer importante en el mercado de la tecnología. (Wesley, 2011)

Otro beneficio de la tecnología en la actualidad son los servicios web (web service) y el Cliente SOAP. El web service utiliza un conjunto de

protocolos y estándares para intercambiar datos entre aplicaciones, estas aplicaciones pueden estar desarrolladas en diferentes lenguajes de programación convirtiéndose en multiplataforma. (Club, 2012)

Para comunicarse el web service con otras aplicaciones describirá una interfaz en lenguaje WSDL, al consumir un web service se utiliza un protocolo de comunicación SOAP, esto facilitará intercambiar procesos entre un cliente SOAP y un web service (Club, 2012)

1.3. PLANTEAMIENTO DEL PROBLEMA

En la actualidad existen varias organizaciones, cooperativas, empresas etc. que se reúnen periódicamente para revisar varios puntos de índole laboral, estratégico, comercio, planificación y entre otros casos; a esto cada dirigente elabora actas de reuniones en documentos físicos y los firma manualmente brindando legalidad a los puntos tratados en la junta, estos documentos son elaborados para las personas que asisten a las reuniones , además son guardados en archivadores físicos, el cual se podría perder o deteriorar el documento considerando que se perdería la información de la junta.

Al momento de reunirse en las organizaciones se presentan varias situaciones, una de ellas es la falta de herramientas tecnológicas para crear las actas, poder legalizarlas y tener una constancia de la asistencia de sus oyentes.

1.4. JUSTIFICACIÓN

Con el desarrollo del Cliente SOAP utilizando un web service Java para dispositivos móviles Android, basados en certificados digitales de firma electrónica, se permitirá elaborar actas de reuniones digitales y a su vez

ser firmados electrónicamente. A través de un certificado digital de firmas múltiples, posterior a esto las actas se guardarán en repositorios seguros (base de datos).

1.5. OBJETIVOS

1.5.1. General

- Desarrollar un Cliente SOAP utilizando un web service Java para dispositivos móviles Android, basados en certificados digitales de firma electrónica.

1.5.2. Específicos

- Desarrollar un Cliente SOAP con tecnología Android.
- Consumir un Web Service a través de un Cliente SOAP.
- Analizar las políticas y normas de certificados electrónicos y librerías de firma, basados en la norma X509.
- Aplicar firmas múltiples digitales para actas de reuniones en formato PDF, basados en la Ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador.

1.6. ALCANCE

El tema “Desarrollo de un cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica”; comprende de dos fases de creación y son las siguientes:

a. Web Service

- Se desarrollará un web service en tecnología java que permitirá transformar actas de reuniones en formato PDF a través de un cliente SOAP.
- El web service permitirá la gestión de firmas múltiples digitales para actas de reuniones en formato PDF.

- El web service permitirá el envío de notificaciones a la persona adecuada.
- El web service permitirá la gestión documental y de usuarios en un repositorio seguro (base de datos Mysql).

b. Cliente SOAP

- Se desarrollará un Cliente SOAP con tecnología Android 4.2.2 para consumir un Web Service de gestión de múltiples firmas.
- Con el desarrollo de Cliente SOAP permitirá el registro de usuarios autentificación para el acceso al sistema, este registro lo hará el administrador del sistema.
- Con el desarrollo de Cliente SOAP permitirá al usuario administrador elaborar actas de reuniones digitales.
- Con el desarrollo de Cliente SOAP permitirá realizar firmas múltiples para las actas de reuniones en formato PDF.
- Con el desarrollo de Cliente SOAP permitirá notificar al usuario vía mail su acta firmada para su posterior visualización y descarga.

En los siguientes gráficos representa la arquitectura Cliente SOAP desarrollado con tecnología Android para consumir un servicio web de firma electrónica.

a. Esquema Usuario Administrador

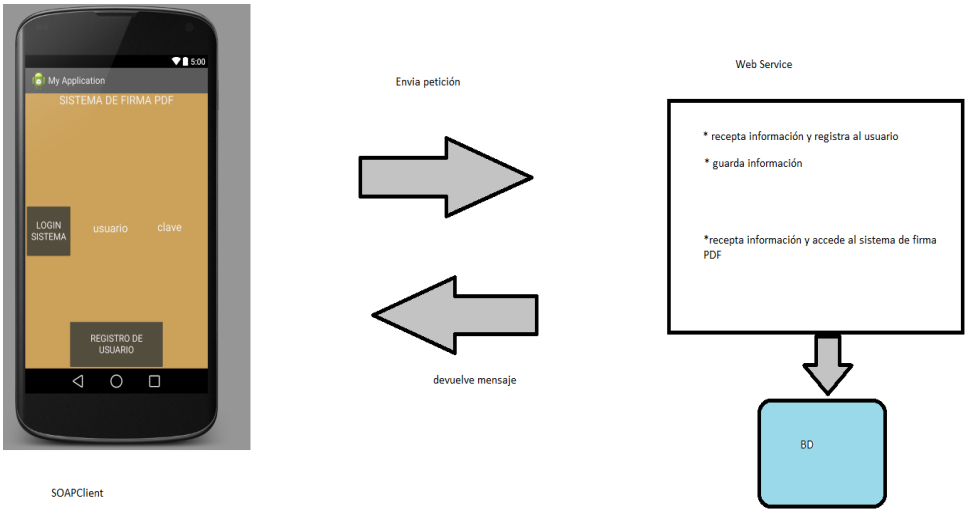


Figura 1. Esquema Registro de Usuarios y Login de Usuario Administrador

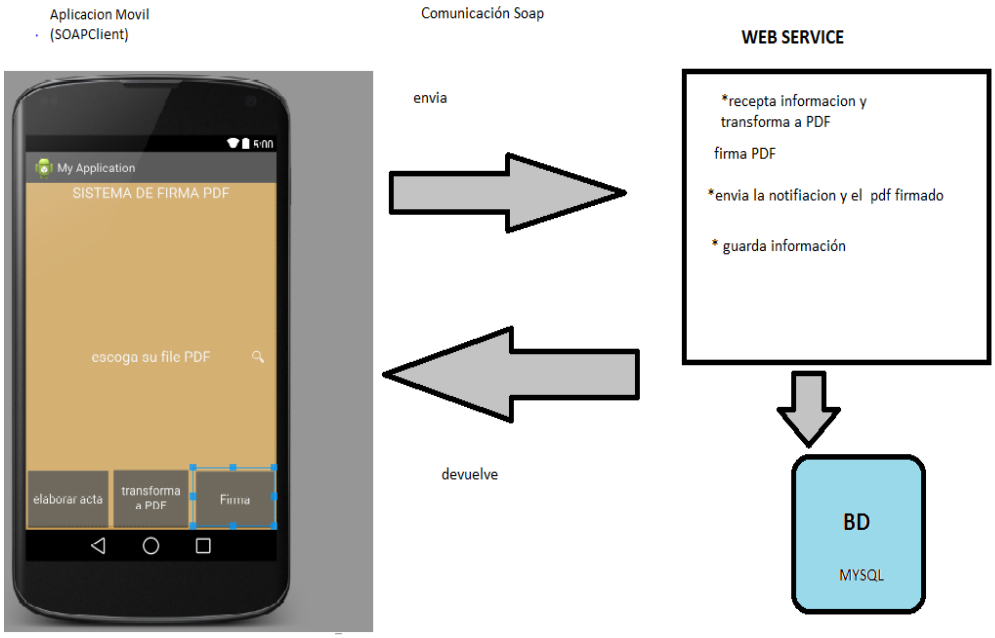


Figura 2. Esquema de Gestión de elaboración, firma de actas de reuniones

b. Esquema Usuario Normal

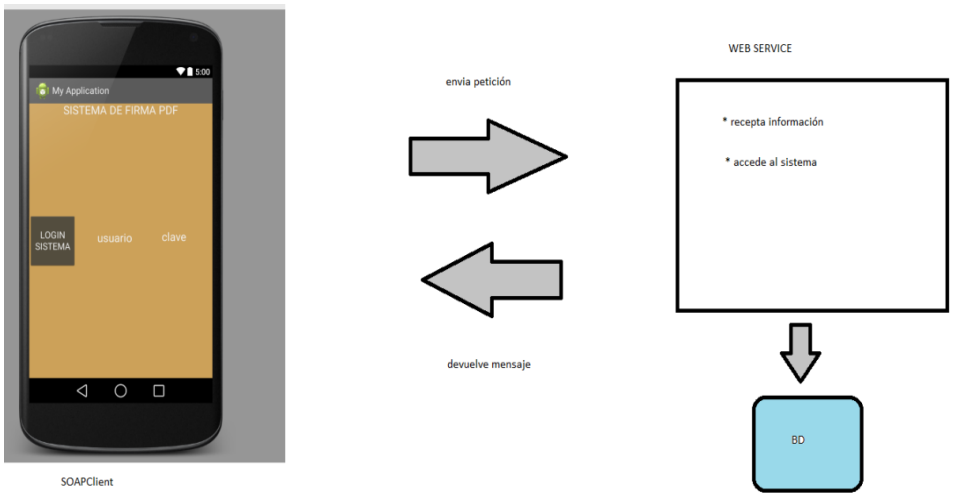


Figura 3. Esquema Login Acceso de Usuario

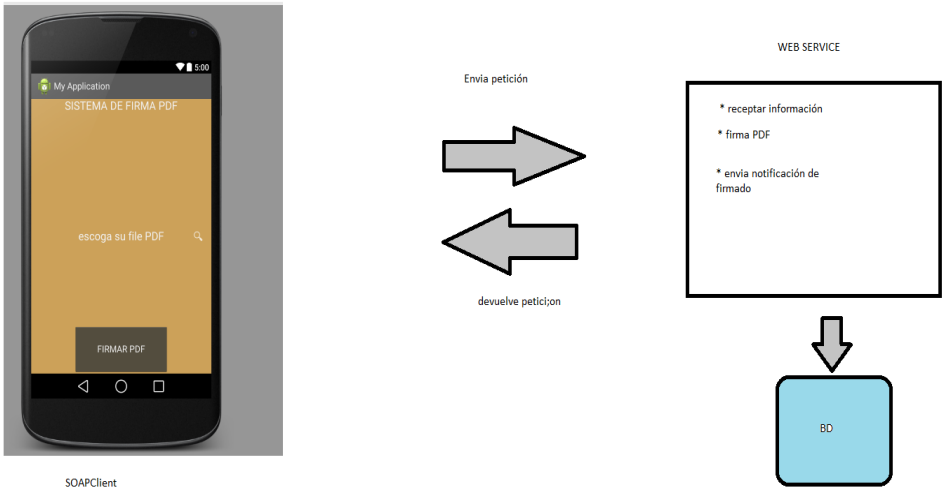


Figura 4. Esquema firma acta de reunión

PRUEBAS

Se realizará pruebas de caja negra y blanca.

Caja Negra: Las pruebas de caja negra son las siguientes:

- Pruebas de partición Equivalente.

- Identificación de las clases equivalentes.
- Identificación de casos de prueba.

Caja Blanca: las pruebas de caja blanca son las siguientes:

- Pruebas de cambio Básico.
- Pruebas de bucles.

En el siguiente gráfico se resume el comportamiento de las pruebas.

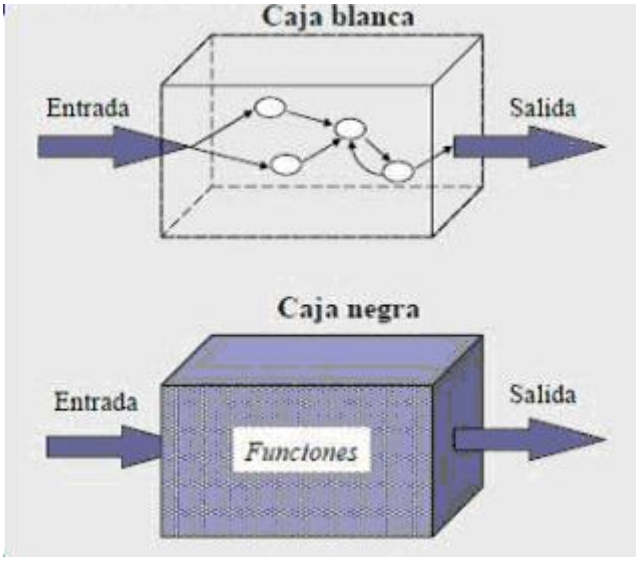


Figura 5 - Esquema de pruebas

Fuente:(Eugenio Juárez Clavín, 2013).

2. CAPÍTULO 2

MARCO DE REFERENCIA

2.1. Introducción a la firma Electrónica

2.1.1. Paradigma de la firma electrónica

Al pasar de los años se refleja el crecimiento y el impacto del comercio y negocios internacionales a nivel mundial, esto surge hace muchos siglos atrás cuando el hombre cambio el régimen de la esclavitud, participación femenina en la vida pública, igualdad de razas y géneros.

Al ubicarse frente a frente estos cambios se tendrá una claridad como dieron vuelta al mundo y como está cambiando actualmente en una milésima del tiempo de cada persona que puede adaptarse a estos cambios.

La parte más importante de estos nuevos cambios es el Internet y a este se debe el comercio electrónico que ha cambiado la forma de comercializar toda clase de productos especialmente se refiere al contacto directo entre dos o más personas.

Cuando se comienza a hablar de una aplicación tecnológica que pueda tener efectos jurídicos recae en el concepto de firma electrónica, para explicar el principio de la tecnología jurídica se hablará sobre las firmas, sus características y la intervención en el mundo del derecho. (Zúñiga, 2011)

2.1.2. Que es firma

Durante siglos la firma ha sido la forma de identificar a las personas para entregar un documento legal a otras personas, además servía como el

identificativo básico para quienes gozaban de poder, la mayoría de Reyes poco sabían leer y escribir, por esta razón utilizaban selladores o estamperos que eran quienes llevaban consigo los signos con los cuales se identificaban al rey.

Originalmente se utilizaba los sellos, este era el medio el que se imponía en el uso comercial, político y social. (Zúñiga, 2011)

2.1.3. Elementos de la firma

A. Identidad

La Firma es un medio de identificación y aceptación entonces hay que preguntarse si es necesario que consten los rasgos caligráficos de la persona, en la mayoría de legislaciones incluida la ecuatoriana se encuentra la obligación de los rasgos incluso a las personas que no saben leer ni escribir les permiten firmar con su huella digital y con un testigo que certifique que esa persona es realmente quien dice ser.

La huella digital es un identificador único que se lo utiliza en el comercio electrónico como la identificación de la persona para el uso de la tecnología criptográfica.

Una parte importante de la firma es la relación con el documento y su contenido.

En la actualidad, se pretende estandarizar el uso de la firma como medio de identificación en las comunicaciones electrónicas el cual hace cambiar la lógica de los abogados y legisladores buscando una salida con la firma electrónica. (México A. d.)

B. Integridad

Uno de los requisitos que se exigen en la firma es que garantice completamente la integridad del documento, ya que se puede modificar

fácilmente el contenido y se dañe el sentido de lo aceptado por el signatario. (México A. d.)

C. Confidencialidad

Al ser un documento público o privado debe existir un grado de confidencialidad, se puede utilizar medios convencionales para proteger la confidencialidad de un documento en el transporte del mismo (sobres)

La confidencialidad resulta entones un medio externo y suplementario al documento el cual da un cierto grado de seguridad (México A. d.)

D. Autenticidad

La autenticidad de la firma sea que esta sea reconocida en proceso legal o ante un notario, busca identificar con seguridad al autor de la firma y de esta manera garantizar el origen de la firma. (México A. d.)

E. No repudio

El no repudio significa que no se puede rechazar. En los casos en los cuales la firma es rechazada, queda la alternativa legal de recurrir a los medios que prueben los rasgos caligráficos se pueda identificar a la persona en base a su caligrafía, la identidad del firmante puede ser utilizada como argumento a favor o en contra que puede alegar de la veracidad de la firma. Hay muchos casos que cualquier persona que tenga habilidades para copiar una firma pueda hacer uso del mismo para hacer actos ilícitos. (México A. d.)

2.1.4. Tipos de Firma

1. Firma Manuscrita

Es la firma propia de la persona, impuesta siguiendo sus rasgos propios al firmar.

2. Firma a Ruego

Cuando una persona no puede firmar, entonces recurre a la firma ruego que sirve para defender los bienes de los socios del negocio, esta firma se presenta en las relaciones profesionales de derecho.

3. Firma Autorizada

Es aquella en la que un tercero autoriza mediante algún documento permitido por la ley, por ejemplo en las personas jurídicas.

4. Rúbrica

Es un conjunto de símbolos o signos utilizados por la persona para identificarse, estos rasgos generalmente son ilegibles, se obliga que sean iguales estos rasgos cuando firman para que se cumpla el objeto de la firma, esto sirve para identificar al firmante

2.1.5. Firma Electrónica

Una de las barreras que encuentra el Comercio Electrónico para su desarrollo es la falta de seguridad en las transacciones realizadas por los medios electrónicos usando el Internet o redes privadas de telecomunicaciones.

La falta de seguridad está en la facilidad con la que la información puede ser alterada, manipulada, incluso robada, de esta manera haciendo daños perjudiciales a firmante, peor aún si no se tiene guardado el documento en medio seguro (guardado en nuestra computadora). (México A. d.)

a. Criptografía

La Obligación de mantener la privacidad y confidencialidad de las comunicaciones viene desde hace mucho tiempo atrás con el uso de la criptografía en los pueblos Egipcios con la llamada escritura o los cambios

en las rubricas de los militares y también durante el mandato de Julio Cesar en Roma.

La Criptografía es una técnica muy útil en la tecnología con el propósito de proteger los códigos fuente de los programas de informática cuando estos debían ser entregados o manipulados a terceras personas era primordial protegerse contra la reproducción.

En la actualidad existen muchos métodos de criptografía con el objetivo de buscar mayor seguridad en la escritura secreta. (Talens, 2014)

Los elementos básicos de los sistemas criptográficos son los algoritmos matemáticos y las claves que permiten su lectura.

La criptografía permite volver ininteligible un documento legible y luego mediante una función inversa volver legible el mismo documento sin cambiar el contenido del mismo, los elementos criptográficos más conocidos son el simétrico y el asimétrico. (México A. d.)

b. Tipos de Criptografía

- **Criptografía Simétrica**

Se basa en el uso de una misma clave para encriptar y desencriptar el mensaje. Este sistema se denomina clave compartida o secreta.

Una de las ventajas de la criptografía simétrica es que los papeles del emisor y receptor se pueden intercambiar con el uso mismo de ese tipo de sistema, al existir una relación previa y un canal seguro de distribución de la claves, existe una seguridad de la identidad que cada partes, esto puede fortalecer el sistema, aunque se debe reconocer que existen maneras de construir la prueba de autoría por el receptor.

La problemática que viene con este sistema es la distribución de la claves ya que al encriptar el mensaje es necesario transmitirla por un canal seguro al destinatario para que este desencripte y pueda ver la información real.

Esto implica que la vulnerabilidad del sistema esté sujeta al mantenimiento en secreto de la clave utilizada. (México A. d.)

Entre los algoritmos destacados de cifrado simétrico en la actualidad se tiene:

- ✓ DES (Data Encryption Standard, base del estándar federal de los USA)
- ✓ IDEA (International Data Encryption Standard)
- ✓ RC-4 (usado en internet para establecer conexiones seguras basadas en el protocolo SSL)
- ✓ AEA (Advanced Encryption Algorithm) que basado en su estándar AES seguramente será el sustituto del DES.

- **Criptografía Asimétrica**

Fue creada en el año 1996 por Whitfield Diffie y Martín Hellman más adelante por Ronald Rivest, Adi Shamir y Len Adelman. La gran ventaja de este sistema era la no necesidad de transferir una clave secreta entre las partes, esto significaba que aumentaba la seguridad al no necesitar del canal confiable como el elemento fundamental de esta tecnología.

El sistema se basa en dos claves, una pública y una privada, la clave pública como se conoce de libre acceso y no existen impedimentos para conocerlas, mientras la clave privada es secreta y solo únicamente la conoce quien creo la firma. Estas dos claves se unen (interactúan) a modo de llaves que abren la información, resguardando con esto la confidencialidad de las claves, es decir la información se puede cifrar o recuperar con la utilización de estas dos claves. De acuerdo a este concepto se podrá decir que la encriptación o cifrado constituye la firma y el descifrado o desencriptación sería la verificación de la firma.

El cálculo del algoritmo es de tal grado de seguridad que resulta casi imposible descifrar las claves mediante derivación o un ataque de fuerza mayor. Un claro ejemplo es una clave de 20 bits contiene 1.048.576 claves posibles.

A pesar de este método ser el mejor tiene sus desventajas es la lentitud en sus operaciones de cifrado y descifrado. Se calcula que la tardanza puede ser entre 5 y 20 veces más que con uno de criptografía simétrica (clave secreta).

En conclusión la criptografía es un sistema tecnológico que colabora para que los documentos guarden integridad, confidencialidad, autenticidad y el no repudio en el envío y recepción de los mensajes de datos.

Entonces la criptografía o sistema de cifrado es simplemente tecnología. (México A. d.)

- **Firma Electrónica en la Legislación Mundial**

Definitivamente la firma electrónica es responsabilidad de quienes lo utilizan y el estado el cual lo están legislando, para dar una adecuada utilización bajos las normas y principios de los derechos de cada ciudadano. ***(Zúñiga, 2011)***

2.2. Introducción a los certificados digitales

Hablar de certificados digitales es referirse a la digital DNI (Documento Nacional de Identidad), en lo que a la autentificación de personas se refiere, ya que permiten a una persona saber sus datos personales y con eso saber su identidad propia, esto quiere decir que tiene potestad de la clave secreta asociada a su certificado.

2.2.1. Certificados Digitales

El certificado de clave pública es un núcleo de unión entre la clave pública de una entidad y uno o más atributos referidos a su identidad. El certificado garantiza que la clave pública pertenece a la entidad identificada y esa entidad posee la correspondiente clave privada.

Los certificados digitales son validados o útiles solo si existe alguna Autoridad Certificadora (CA), ya que no tiene validez si uno mismo se certifica y por lo tanto una tercera persona no lo reconocerá como ente de entidad.

Es primordial ser capaz de verificar que una CA ha emitido un certificado y detectar si el certificado es válido o no, esto sirve para evitar la falsificación de certificados, la CA después de autentificar la identidad de un sujeto, firma el certificado digitalmente.

Los Certificados están compuestos de un mecanismo criptográfico para implementar la autentificación, también proporcionan seguridad y escalabilidad para distribuir claves públicas en grandes sectores. (Talens, 2014)

2.2.2. Certificados X.509

El formato de los certificados X.509 es un estándar del ITU-T (International Telecommunication Union-Telecommunication Standarization Sector) y el ISO/IEC (International Standards Organization /International Electrotechnical Commission) que se publicó por primera ocasión en 1988. Al pasar de los años fueron actualizando de versión dando lugar a la última versión X.509 v3 publicado en 1996. (Talens, 2014)

Los elementos del formato X.509 v3 son:

a. Versión. El campo de versión contiene el número de cuantas veces fue actualizado el certificado los valores son; 1, 2, 3.

b. Número de serie del Certificado. Este campo es un entero asignado por la CA, cada certificado emitido por una CA debe tener un número de serie único.

c. Identificador del algoritmo de firmado. Este campo identifica el algoritmo empleado para firmar el certificado (ejemplo el RSA o DSA).

d. Nombre del Emisor. Este campo señala la CA que ha firmado y emitido el Certificado.

e. Periodo de Validez. Este campo indica la fecha de validez del certificado, esto quiere decir que indica la fecha inicial en la que el certificado comienza a ser válido y la fecha después de la cual el certificado deja de serlo.

f. Nombre del Sujeto. Este campo señala la identidad cuya clave pública está certificada. El nombre debe ser único para cada entidad certificadora, aunque puede emitir más de un certificado con el mismo nombre si es para la misma entidad.

g. Información de clave pública del sujeto. Este campo contiene la clave pública, sus parámetros y el identificador del algoritmo con el que se emplea la clave.

h. Identificador único del emisor. Este es un campo opcional que permite reutilizar nombres de emisor.

i. Identificador único del sujeto. Este es un campo opcional que permite reutilizar nombres de sujeto.

j. Extensiones. Las extensiones proporcionan una manera de asociar información adicional a sujetos, claves públicas, etc.

k. Política de certificado. Este campo contiene las condiciones bajo las que la CA emitió el certificado y el propósito del certificado.

l. Uso de la clave. Este campo restringe el propósito de la clave pública certificada, una de ellas es que la clave solo se debe usar para firmar, para la encriptación de claves y datos, etc. este campo es importante ya que la clave solo está certificada para un propósito y el mal uso no estaría valido en el certificado. (Talens, 2014)

2.2.3. Autoridades Certificadoras (CA)

Una CA es una organización fiable que recepta solicitudes de certificados de entidades, las valida, genera certificados y mantiene la información de su estado. Además las CA se utilizan políticas, normas y practicas se seguridad para responsabilizarse de los datos e identidad del sujeto.

Las labores de un CA son:

Admisión de solicitudes. Una persona rellena un formulario y lo envía a la CA solicitando un certificado. La responsabilidad de la generación de las claves públicas y privadas son responsabilidad de la persona o de un sistema asociado a la CA.

Autentificación del Sujeto. Antes de firmar la información proporcionada por el sujeto la CA debe verificar su identidad, el sujeto puede pedir el nivel de seguridad y el tipo de certificado.

Generación de certificados. Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada. Posteriormente lo manda al subscriptor y si quiere lo envía a un almacén de certificados para su distribución.

Distribución de certificados. La entidad certificadora puede proporcionar un servicio de distribución de certificados para que las aplicaciones tengan acceso y puedan obtener los certificados de sus subscriptores. Los medios de distribución pueden ser: correo electrónico, servicios de directorio como el X.500 o el LDAP, etc.

Anulación de certificados. La CA debe validar el origen y autenticidad de una solicitud de anulación, La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original.

Almacenes de datos. Básicamente es una base de datos este almacén debe tener por objeto señalar que el trabajo con los certificados es fiable y de confianza.

Una de las autoridades de certificación en el Ecuador avalada por la ley de comercio Electrónico, firmas y mensajes de datos del Ecuador es ANF AC (autoridad de certificación) cuyo objetivo es distribuir dispositivos de firma electrónica de certificados digitales con firma asistida y desasistida. (Talens, 2014)

2.3. Ley de Comercio Electrónico del Ecuador

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos del Ecuador, describe en el Artículo I, la regulación de los mensajes de datos, firma electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas.

En cuanto a los principios generales la información que se debe destacar en las especificadas, en los siguientes artículos de la ley:

Artículo II: Reconocimiento jurídico de los mensajes de datos.- los mensajes de datos tendrá igual valor jurídico que los documentos escritos. Su eficacia, valoración y efectos se someterá al cumplimiento de lo establecido en esta ley y su reglamento.

Articulo IX: La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la Republica y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización de titular u orden de autoridad competente.

Artículos más relevantes en la firma Electrónica son:

Articulo XIV: Efectos de la firma electrónica.- la firma electrónica tendrá igual validez y se le reconocerán los mismos efectos jurídicos que a una firma manuscrita en relación con los datos consignados en documentos escritos y será admitida como prueba en juicio.

Con respecto a los certificados digitales de firma electrónica, la ley lo describe como el mensaje de datos que certifica la vinculación de una firma electrónica con una persona específica, a través de un proceso de una comprobación que confirma su identidad y especifica los conceptos relevantes al uso del certificado, sus requisitos, duración, y terminación del certificado (revocación del mismo), además de los requisitos necesarios para que tenga un reconocimiento internacional de firma electrónica.

En relación a las entidades de certificación de información, describe la especificación de lo que constituye una entidad de certificación de información, que corresponde a lo descrito como autoridad de certificación, y determina las obligaciones y responsabilidades de estas entidades para la protección de datos, la terminación contractual de servicios y la notificación de las cese de actividades.

Artículo XXXVI y XXXVII: Se dice que el consejo de Comercio Exterior e inversiones (COMEXI), será el organismo de promoción y difusión de servicios electrónicos y que el Consejo Nacional de Telecomunicaciones (CONATEL), será el organismo de autorización, registro y regulación de las entidades de certificación de información acreditadas.

En cuanto a los servicios electrónicos, la contratación electrónica y telemática, los derechos de los usuarios, e instrumentos públicos, la ley describe el cumplimiento de formalidades, la validez de contratos electrónicos. Describe también el consentimiento para aceptar mensajes de datos y el uso de medios electrónicos, las obligaciones correspondientes a la información del consumidor. En sus últimos artículos describe las

infracciones informáticas incluyendo las reformas al código penal, descritas desde el Artículo LIX hasta el LXIV. (Novoa, 2002)

2.4. Introducción a la tecnología móvil Android

Android era un sistema operativo muy poco conocido para móviles hasta que en 2005 Google lo compró. La posible compra y rumores duro hasta el 2007, pero en esta fecha se lanzó el Open Handset Alliance, esta agrupación asocia a muchos fabricantes de teléfonos móviles, chipsets y Google y se lanzó la primera versión de Android, junto a su id de programación SDK para que los programadores empiecen a crear sus aplicaciones móviles.

Al principio los sistemas y las aplicaciones eran lentos pero rápidamente alcanzo un nivel muy importante en el mercado siendo el sistema operativo más vendido del mundo, las mayores ventas alcanzo en el último trimestre del 2010.

En febrero de 2011 se anunció la versión 3.0 de Android, llamada HoneyComb, básicamente esta versión servía más para Tablets que para teléfonos móviles. (Wesley, 2011)

2.4.1. Que es Android

Android es un sistema operativo inicialmente pensado para teléfonos móviles, al igual que iOS, Symbian y BlackBerry OS. Android lo que le hace diferente a los demás sistemas es que está basado en Linux, ustedes sabrán que decir Linux es sinónimo de libre, gratuito y multiplataforma.

Este sistema permite programar aplicaciones en una variación de java llamada Dalvik (máquina virtual para dispositivos móviles para ejecutar aplicaciones Android programadas en java). (Android, 2011)

El sistema operativo proporciona todas las interfaces necesarias para desarrollar aplicaciones que se puede encontrar en un teléfono (GPS, llamadas, Agenda, etc.)

La libertad es una de las mejores características de este sistema operativo ya que se puede utilizar sin ninguna restricción. Las cosas que se utilizará libremente son: programar, subir las aplicaciones al teléfono, miles de aplicaciones gratuitas, etc. Todo esto hace que los teléfonos tengan un coste bajo en el mercado tecnológico.

Cualquiera puede bajarse el código fuente, utilizarlo, compilarlo e incluso cambiarlo. Con la reutilización de código permite detectar fallos más rápidamente. (Android, 2011)

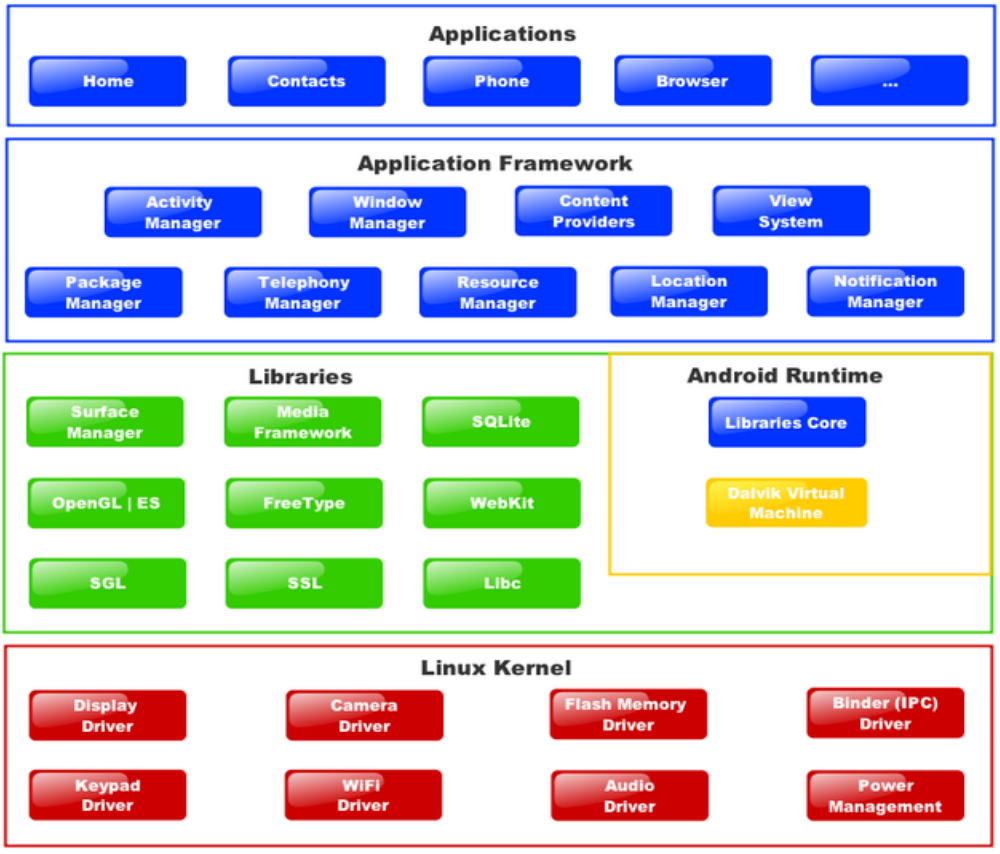


Figura 6. Arquitectura de Distribución de componentes Android

Fuente: (Alejandro Nieto González)

2.4.2. La experiencia Google en los teléfonos móviles

Se puede concluir que Android es la forma de afrontar la telefonía móvil por parte de Google. Las aplicaciones de Google que vienen preinstaladas en el teléfono, permiten acceder a los servicios de Google de forma muy integrada, aparte de la aplicación Google Play que permite instalar aplicaciones desarrolladas por terceros de una forma muy sencilla. (Android, 2011)

2.5. Introducción al Web Service

Un Web Service es un servicio ofrecido por una aplicación que expone su lógica a través de procesos a clientes de cualquier plataforma mediante una interfaz accesible a través de protocolos (HTTP, SOAP, WSDL, UDDI) en el Internet. (Programación, 2012)

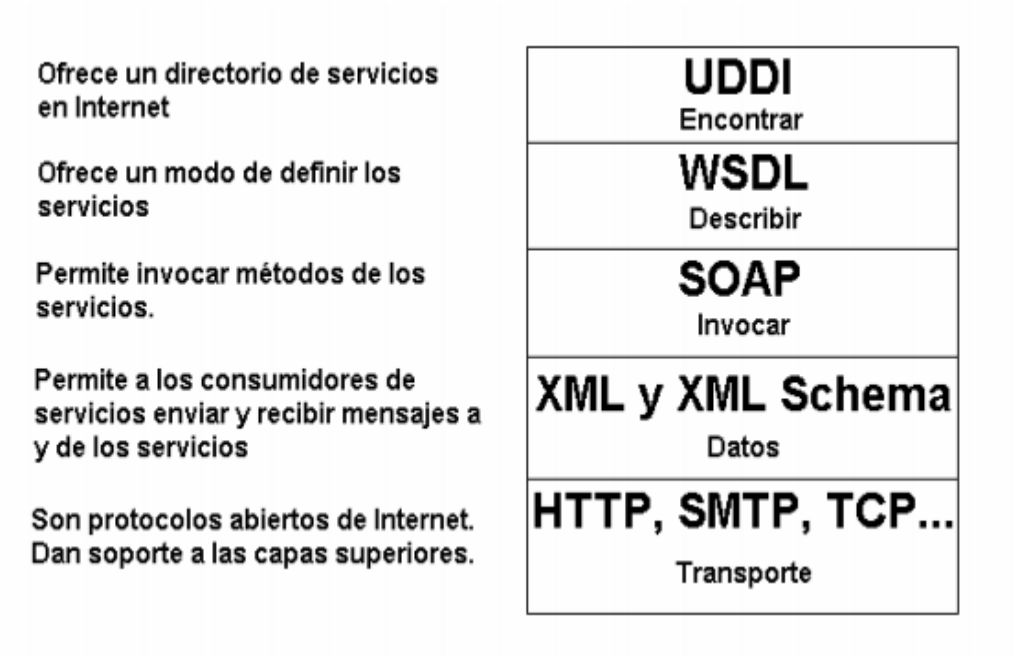


Figura 7. Pila de Protocolo Web Service

Fuente: (Miguel Rodríguez)

Para crear un Web Service puede utilizar cualquier lenguaje disponible en la plataforma .Net, Java, etc.

Una vez creado el servicio, para conseguir que sea accesible por los usuarios, es necesario describirlo utilizando un lenguaje estándar llamado WSDL (Web Service Description Language).

Para poder consumir estos servicios se debe construir un cliente en cualquier lenguaje y ejecutarse sobre cualquier sistema operativo y hardware, único que se necesita que sean capaces de obtener y entender la descripción WSDL de un servicio web.

Una WSDL es un archivo XML en el que se identifica el servicio y se indica el esquema para poder utilizarlo, así como los protocolos que son accesibles a utilizar.

Los protocolos que se dispone para su utilización y se puedan comunicar son: HTTP o SOAP (añade invocación de métodos a HTTP, también se realiza peticiones con HTTP- GET y/o HTTP-POST). (Programación, 2012)

Figura 8. Proceso de utilización Web Service

Fuente: (Miguel Rodríguez)

Porque tantos Protocolos?

Actualmente, publicar un servicio web apenas es necesario tener en cuenta las características del cliente, esto es posible gracias a que HTML y

HTTP son un estándar mundial de diseño, solicitud y transmisión de documentos, el servicio web (www) es universal accesible para cualquier cliente.

Ventajas de los Web Services.

- Ofrecen una tecnología distribuida de componentes optimizada.
- Evitan los problemas inherentes a la existencia de firewalls, ya que SOAP utiliza HTTP como protocolo de comunicación.
- Permiten consumir sencillamente los métodos del Web Service, mediante SOAP.
- Los clientes pueden consumir desde cualquier plataforma y tecnología basta que soporten XML/SOAP o HTTP.

2.5.1. WSDL

WSDL (Web Services Description Language) es un protocolo en XML que describe los accesos al Web Service. Se podría decir también que es el manual de operación del mismo, porque da la pauta de guía de cuáles son las interfaces que provee el servicio y los tipos de datos necesarios para la utilización.

WSDL es un lenguaje propuesto por la W3C (Organización de estándares internacionales para la World Wide Web (www abreviada o W3). Para la descripción de Servicios Web permitiendo describir la interfaz de una servicio web en formato XML, además permite separar la descripción abstracta de la funcionalidad ofrecida por un servicio a través de protocolos de red o un formato de mensaje SOAP, HTTP o MIME.

WSDL describe los servicios web a través de los mensajes que se intercambian entre el proveedor del servicio y el cliente. (Programación, 2012)

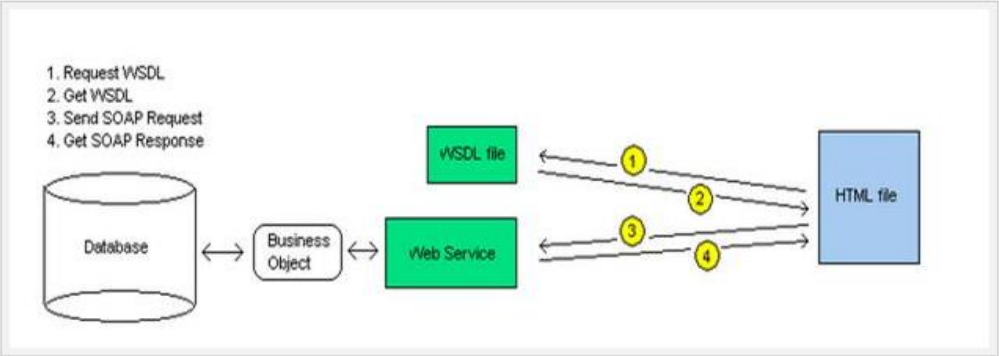


Figura 9. Pasos de consumo de Web Service

Fuente: (IBM webSphere)

1. El cliente primero realiza una solicitud al servicio es tomar la definición del Archivo WSDL.

2. El servidor entrega el archivo WSDL. Esto indica a la petición de métodos y propiedades de ese servicio que están disponibles y listos para su consumo.

3. El cliente hace la petición en el formato que tiene el servicio según la estructura del fichero WSDL en el que indica que parámetros acepta y de qué tipo.

4. El Servidor (servicio web) entrega el resultado de la consulta.

2.5.2. Estructura

Un ejemplo de la estructura es la siguiente:

URL: https://factura.ec/servicio_linea/RepositorioWS?wsdl

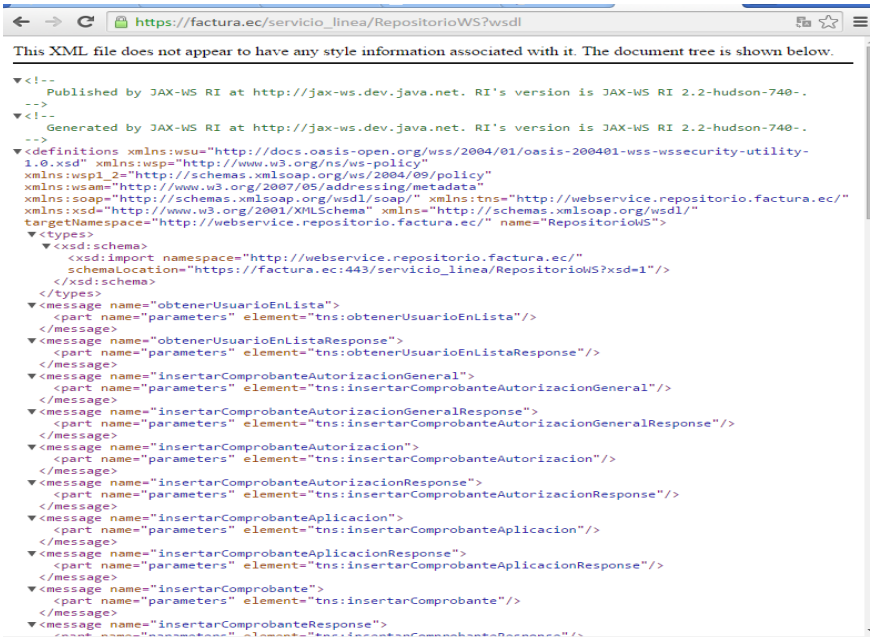


Figura 10. Estructura lenguaje WSDL

2.6. Metodología

Analizando los requisitos de la empresa para cumplir con eficacia y eficiencia la dimensión del proyecto se consideró utilizar metodología de desarrollo ágil UWE

Es una herramienta que nos permitirá modelar aplicaciones web, utilizada en la ingeniería web, prestando especial atención en sistematización y personalización (sistemas adaptativos). UWE es una propuesta basada en el proceso unificado y UML pero adaptados a la web. En requisitos separa las fases de captura, definición y validación. Hace además una clasificación y un tratamiento especial dependiendo del carácter de cada requisito. (Quiroga, 2015)

Entre los principales modelos de UWE podemos citar: el modelo lógico-conceptual, modelo de navegación, modelo de presentación, visualización de Escenarios Web.

UWE define vistas especiales representadas gráficamente por diagramas en UML. Además UWE no limita el número de vistas posibles de una aplicación, UML proporciona mecanismos de extensión basados en estereotipos.

Estos mecanismos de extensión son los que UWE utiliza para definir estereotipos que son lo que finalmente se utilizarán en las vistas especiales para el modelado de aplicaciones Web. (Quiroga, 2015)

La metodología UWE generalmente esta propuesta de la siguiente manera:

1. Análisis de Requisitos
2. Diseño del Sistema y del Software
3. Codificación
4. Pruebas
5. Verificación
6. Mantenimiento

Las fases que se utilizará en este proyecto son:

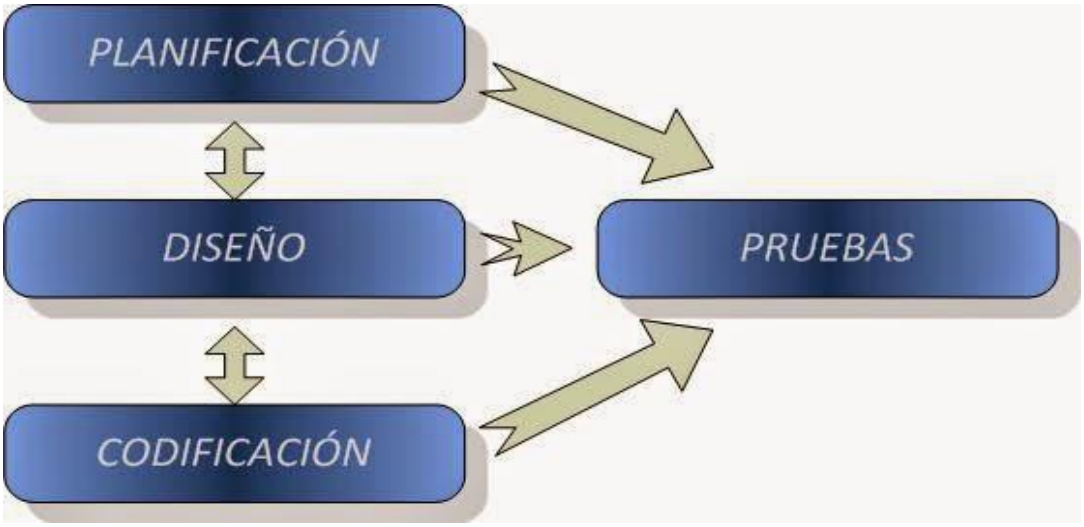


Figura 11. Etapas de la Metodología UWE

Fuente: (Raúl Martínez)

2.6.1. Análisis de Requisitos

Ingeniería y Análisis del Sistema.- En la mayoría de los casos el software es parte de un sistema por eso el trabajo comienza estableciendo los requisitos del sistema y luego dividiendo en subconjuntos de estos requisitos al Software.

Análisis de Requisitos del Software.- El proceso de Recolección de los requisitos se pone énfasis en el Software. El analista debe comprender el ámbito de la información del Software, la función, rendimiento e interfaces que se requiere para la implementación del Software. (Quiroga, 2015)

2.6.2. Diseño del Sistema y del Software

El diseño especifica cuatro atributos del software cuales son:

- la estructura de los datos
- arquitectura del software
- detalle procedimental
- caracterización de la interfaz

Este proceso traduce los requisitos en una presentación del software con la calidad requerida y estructura específica para que le analista comience a codificar. (Quiroga, 2015)

2.6.3. Codificación

La codificación comienza cuando el diseño está bien estructurado y traducido en una forma legible. Si el diseño tiene un alto grado de eficacia la codificación puede realizarse mecánicamente. (Quiroga, 2015)

2.6.4. Prueba

Después de la fase de codificación comienzan las pruebas en el programa.

La prueba se basa en la lógica interna del software y en las funciones externas, el objetivo de estas pruebas es asegurar que cumpla los requisitos funcionales del sistema. (Quiroga, 2015)

2.6.5. Verificación

En esta fase el usuario final ejecuta el sistema construido, sin embargo antes de ejecutar los programadores tienen que realizar un sin número de pruebas para comprobar que el sistema no tenga fallos ante el usuario final. (Quiroga, 2015)

2.6.6. Mantenimiento

El software nunca muere se actualiza o se hace mantenimientos después que se entregue al cliente. Los mantenimiento pueden ser por varias causas, puede ser porque se hayan encontrado errores o que el software deba adaptarse a cambios del entorno externo (sistemas operativos o donde se instale el software requerido), las actualizaciones se hacen cuando el cliente requiera ampliaciones funcionales (nuevos Requisitos) o del rendimiento.

Este modelo es el más utilizado para aplicaciones pequeñas y fáciles de construir además también se utiliza para los ciclos en lo que se tiene un proyecto estable y una visión exacta de la entrega del producto, ayuda a minimizar los gastos de planificación porque permite realizarle sin muchos problemas.

Lo más importante que este modelo te ayuda realizar la construcción del software ordenadamente y sirve para trabajar en con poco personal.

Así como este modelo tiene ventajas también están sus desventajas las cuales son, si se tiene un proyecto pequeño la documentación de va hacer demorosa y excesiva, genera poca claridad de progreso hasta la culminación del sistema, no es imposible volver atrás utilizando este modelo pero si un poco difícil ver lo que ya se realizó, no existe tiempo para corregir fallos y hace compleja la depuración de errores en las fases.

En esta metodología descrita contempla la fase de mantenimiento, sin embargo dentro del alcance del proyecto solo se define el desarrollo hasta la fase de pruebas y Validación. (Quiroga, 2015)

3. CAPÍTULO 3

ANÁLISIS Y DISEÑO DEL SISTEMA

3.1. Análisis de Requisitos

3.1.1. Conceptualización Del Sistema

En la actualidad existen varias organizaciones, cooperativas, empresas etc. que se reúnen periódicamente para revisar varios puntos de índole laboral, estratégico, comercio, planificación y entre otros casos; a esto cada dirigente elabora actas de reuniones en documentos físicos y los firma manualmente brindando legalidad a los puntos tratados en la junta, estos documentos son elaborados para las personas que asisten a las reuniones , además son guardados en archivadores físicos, el cual se podría perder o deteriorar el documento considerando que se perdería la información de la junta.

Al momento de reunirse en las organizaciones se presentan varias situaciones, una de ellas es la falta de herramientas tecnológicas para crear las actas, poder legalizarlas y tener una constancia de la asistencia de sus oyentes.

3.1.2. Ingeniería y Análisis del Sistema

- **Descripción del Sistema**

El Desarrollo de un cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica es un proyecto con visión de innovación para las empresas con el propósito de dar solución a la problemática a las restricciones del internet

y bajar el coste de egresos como reciclando papel, sobre todo uno de los objetivos principales cuidar el medio ambiente.

Otro de los enfoques de este proyecto es la utilidad de la firma electrónica que cada día va creciendo en nuestro país y las diversas formas de firmar documentos electrónicos para cualquier trámite legal o transición de datos por el internet.

- **Funcionalidad**

La característica principal del Desarrollo de un cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica es elaborar actas de reuniones digitales y a su vez ser firmados electrónicamente. A través de un certificado digital de firmas múltiples, posterior a esto las actas se guardarán en repositorios seguros (base de datos) y serán enviadas vial mail a los asistentes de la reunión con el acta firmada.

Para poder utilizar el proyecto móvil y firmar electrónicamente el usuario necesitará adquirir un certificado electrónico

Este proyecto cuenta con cuatro capas tecnológicas el cual integrándose forman la estructura ideal de la lógica del negocio

Sus capas tecnológicas son:

- Cliente SOAP: Básicamente es una aplicación móvil con interfaces amigables que permite interactuar de manera intuitiva al usuario accediendo de manera muy fácil para elaborar actas de reuniones y a su vez ser firmados.

Este cliente SOAP cumple con todas las características de una aplicación móvil Android.

- Web Service: Este servicio web creado con tecnología JAVA que fue estructurado como motor de interacción para realizar los procesos de elaboración, firma y notificación vial mail de actas de reuniones, bajo la petición del Cliente SOAP.

- Almacenamiento: Repositorio documental para guardar todas las actas elaboradas y firmadas por los usuarios que utilicen el Cliente SOAP.

- Notificación Electrónica: Una pequeña aplicación consola JAVA el cual esta añadida como librería al Servicio Web con la finalidad de enviar correos electrónicos notificando al usuario las actas firmadas.

o Características de los Usuarios

El cliente SOAP móvil cuenta con dos perfiles de usuarios que podrán acceder al sistema, cada uno con sus funciones específicas cuales son:

- ✓ Usuario Administrador: Administra el Sistema, Gestiona las cuentas de usuarios, elabora las actas de reuniones, firma las actas de reunión envía notificación de las actas a los asistentes de la reunión.
- ✓ Usuario Normal: Firma la actas correspondientes y envía la notificación de la acta firmada.

3.1.3. Análisis de los requisitos del Software

o Requisitos Interfaces

▪ Interfaces de Usuario

El usuario para poder interactuar con el Cliente SOAP, necesariamente debe tener un teléfono móvil o Tablet con sistema operativo Android. Básicamente debe tener plan de datos o simplemente estar conectados a Internet Wireless.

- **Interfaces de Hardware**

La infraestructura garantiza la seguridad y la disponibilidad del sistema por lo que se hace uso de un servidor robusto y confiable de tal manera que los Servicios Web de firma funcionen sin interrupciones y briden el servicio adecuado.

Además este mismo servidor ayudará con el almacenamiento de toda la información en cuanto respecta a las actas firmadas y los usuarios para la gestión en el sistema.

- **Interfaces de Software**

El desarrollo de este sistema se hará en la plataforma de JAVA con diferentes tecnologías la primera parte que se trata del Cliente SOAP se desarrollará con tecnología Android y la segunda que es el Servicio Web el cual receptará las peticiones del Cliente y tendrá interacción con la base de datos se realizará con tecnología (Web JSF, Hibérnate).

- **Interfaces de Comunicación**

Para la comunicación del Cliente SOAP con el Web Service se utilizará el protocolo HTTP por el puerto 80.

Para acceder a los servidores y hacer sus respectivas configuraciones se accederá vía SSH con el puerto 22, mientras que la comunicación del Web Service a la base de datos será Local Host puerto 3306.

- **Requisitos Funcionales**

Tabla 1

Requisito Funcional 1

Identificador:	**RE01**
Nombre :	Autenticación Simple de Usuario
Descripción:	El Usuario se auténtica en el Cliente SOAP con tecnología Android de una manera sencilla utilizando un ruc/cédula como nombre de usuario y contraseña, a través de una pantalla Login.
Entrada:	○ nombre usuario (ruc/cédula) ○ Contraseña
Salida:	○ Autenticación Correcta ○ Error: El usuario no existe ○ Error: El usuario no tiene certificado para firmar ○ Error: Ingrese todos los datos requeridos

Tabla 2

Requisito Funcional 2

Identificador:	**RE02**
Nombre :	Inicio de Sesión
Descripción:	El Usuario inicia sesión para acceder a todas las funcionalidades de mismo, las funcionalidades se mostrarán según el perfil Usuario de inicio de sesión.
Entrada:	Nombre Usuario (ruc/cedula)
Salida:	Inicio de sesión satisfactorio

Tabla 3

Requisito Funcional 3

Identificador:	**RE03**
Nombre :	Cierre de Sesión
Descripción:	El usuario cierra sesión una vez que de clic en los botones de cerrar de cada pantalla.
Entrada:	Acción Clic Cerrar
Salida:	Cierre de sesión satisfactorio

Tabla 4

Requisito Funcional 4

Identificador:	**RE04**
Nombre :	Registro de Usuarios
Descripción:	El usuario Administrador será la persona encargada de registrar a los demás usuarios
Entrada:	○ Nombres ○ Apellidos ○ Identificación ○ Email ○ Password
Salida:	○ Se registró correctamente ○ El Usuario no tiene certificado para firmar ○ No existe usuario en el sistema ○ Usuario ya registrado en el sistema
Observación	El usuario puede ser registrado siempre y cuando haya adquirido un certificado electrónico.

Tabla 5

Requisito Funcional 5

Identificador:	**RE05**
Nombre :	Creación Acta de Reunión
Descripción:	El Usuario Administrador será el encargado de crear la acta de reunión según los puntos acordados en la misma
Entrada:	○ Número de Reunión ○ Tema Reunión ○ Asistentes ○ Lugar ○ Fecha ○ Detalle
Salida:	○ Se creó correctamente la acta Numero #
Observación:	En el detalle se pondrá los puntos del tema que se trató en el reunión

Tabla 6

Requisito Funcional 6

Identificador:	**RE06**
Nombre :	Validación de Documento
Descripción:	El sistema realizará una validación del formato de la Acta de Reunión (formato PDF)
Entrada:	○ Documento (acta de reunión)
Salida:	○ Validación Correcta ○ El documento no cumple con el Formato (PDF)

Tabla 7

Requisito Funcional 7

Identificador:	**RE07**
Nombre :	Verificación de llaves Publicas del Certificado
Descripción:	El Sistema verifica en el certificado las claves públicas del Certificado para saber si son equivalentes a las registradas en el repositorio
Entrada:	○ Ruc Usuario ○ Clave publica
Salida:	○ Verificación Correcta ○ Las clave pública es errónea

Tabla 8

Requisito Funcional 8

Identificador:	**RE08**
Nombre :	Validación del Certificado
Descripción:	El sistema se conecta al Servidor (OSCP) para verificar si esta valido o no el certificado electrónico.
Entrada:	○ Clave Publica ○ Clave Privada ○ Certificado Electrónico ○ Tipo de Certificado
Salida:	○ Certificado Valido ○ Certificado Invalido
Observación:	El servidor OSCP (Ofensiva Seguridad de Certificación Profesional) es propio de la empresa Emisora de Certificados ANF A.C.

Tabla 9

Requisito Funcional 9

Identificador:	**RE09**
Nombre :	Firma Acta Administrador
Descripción:	El Usuario Administrador y el sistema después de realizar el RE05,RE06,RE07,RE08 procederá a firmar la acta de reunión
Entrada:	○ Identificación del Usuario Administrador ○ Número de Acta ○ Lista de Asistentes en la Reunión
Salida:	○ Se firmó correctamente la acta Numero #

Tabla 10

Requisito Funcional 10

Identificador:	**RE10**
Nombre :	Repositorio Documental
Descripción:	El sistema procederá a Guardar en un contendedor documental seguro (MYSQL) la información del acta y el documento físico firmado.
Entrada:	○ Numero de acta ○ Fecha de acta firmada ○ Asistentes ○ Documento Físico
Salida:	○ Se guardó con éxito ○ No se pudo guardar el documento firmado

Tabla 11

Requisito Funcional 11

Identificador:	**RE11**
Nombre :	Envío de Notificación Vía Correo
Descripción:	El Usuario Administrador después de realizar el RE10 procederá a enviar y notificar la acta firmada a cada asistente de la reunión
Entrada:	○ Email
Salida:	○ Se envió correctamente ○ Correos en el buzón del destinatario

Tabla 12

Requisito Funcional 12

Identificador:	**RE12**
Nombre :	Firma Acta Usuarios Normales
Descripción:	Se repite los Requerimientos RE05,RE06,RE07,RE08 para proceder a firmarlos
Entrada:	○ Identificación del Usuario ○ Número de Acta
Salida:	○ Se firmó correctamente la acta Numero #

Tabla 13

Requisito Funcional 13

Identificador:	**RE13**
Nombre :	Repositorio Documental
Descripción:	El sistema procederá a Guardar en un contendedor documental seguro (MYSQL) la información del acta y el documento físico firmado.
Entrada:	○ Numero de acta ○ Fecha de acta firmada

Continua

	○ Asistentes ○ Documento Físico
Salida:	○ Se guardó con éxito ○ No se pudo guardar el documento firmado

Tabla 14

Requisito Funcional 14

Identificador:	**RE14**
Nombre :	Envío de Notificación Vía Correo
Descripción:	El Usuario Normal después de realizar el RE13 procederá a enviar y notificar la acta firmada a cada asistente de la reunión y al Usuario Administrador
Entrada:	○ Email
Salida:	○ Se envió correctamente ○ Correos en el buzón del destinatario

- **Requisitos no Funcionales**

a. Fácil Uso del Cliente SOAP con tecnología Android: Por ser una aplicación móvil su manejo y utilización debe ser intuitiva, amigable con el usuario para su óptimo funcionamiento.

b. Disponibilidad del Aplicación: por ser una aplicación móvil el usuario podrá utilizar cualquier hora y día de la semana (24/7).

c. Tiempo de Respuesta: los tiempos de respuesta del Cliente SOAP con tecnología Android consumiendo el Servicio Web de firma electrónicas deben ser rápidos para que no afecte la firma y la entrega del documento al Usuario.

d. Seguridad en el Aplicativo: El sistema debe garantizar que solo permita el acceso de los usuarios requeridos, caso contrario la firma electrónica de estos usuarios será alterada y se puede dar mal uso.

e. Comunicación Cifrada: la Comunicación entre el cliente SOAP y el servicio Web debe ser cifrada de tal manera que ningún intruso pueda capturar paquetes de datos en el red y sean mal utilizadas, la petición del Servicio Web viaja por el protocolo HTTP y con codificación mínima de 128 bits.

3.2. Diseño del Sistema y del Software

3.2.1. Diagramas de Comportamiento

- **Diagrama de Casos de Uso**

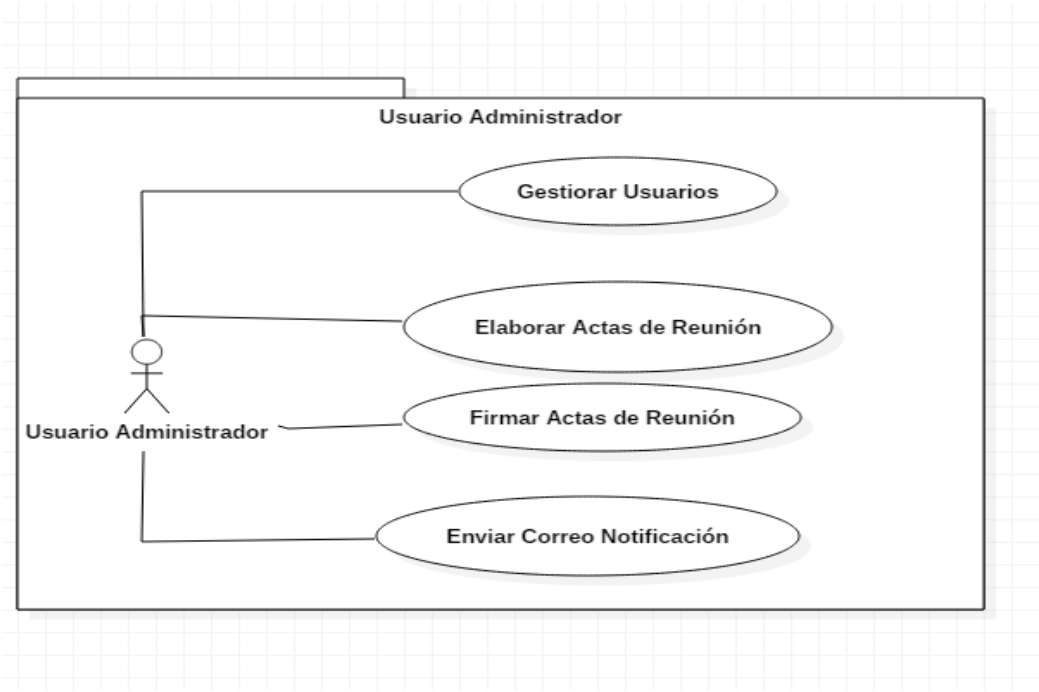


Figura 12. Caso de Uso 1 Usuario Administrador

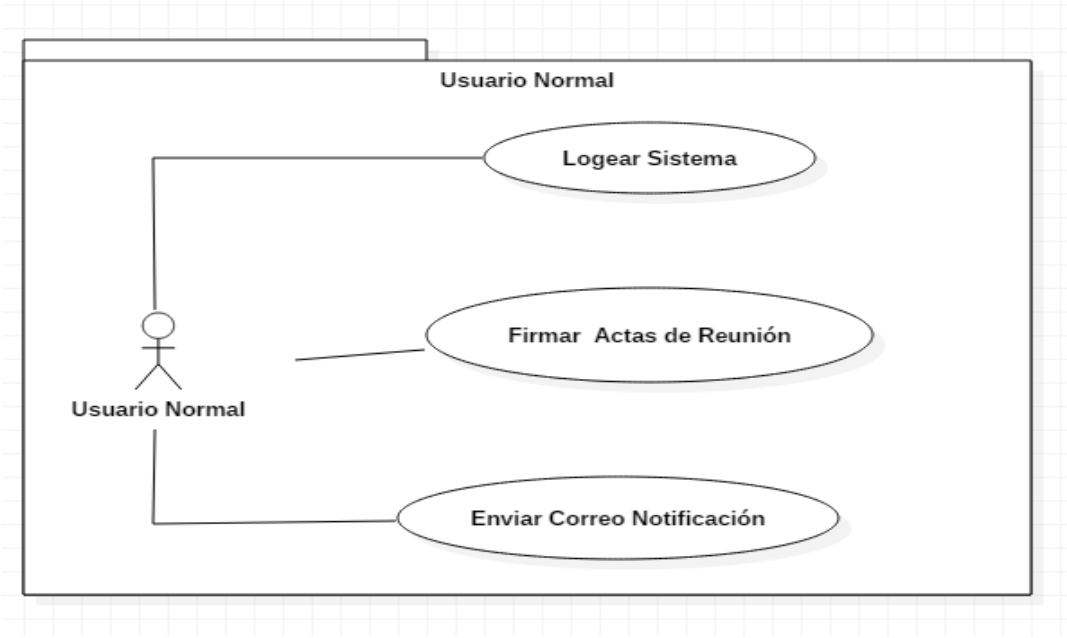


Figura 13. Caso de Uso 2 Usuario Normal

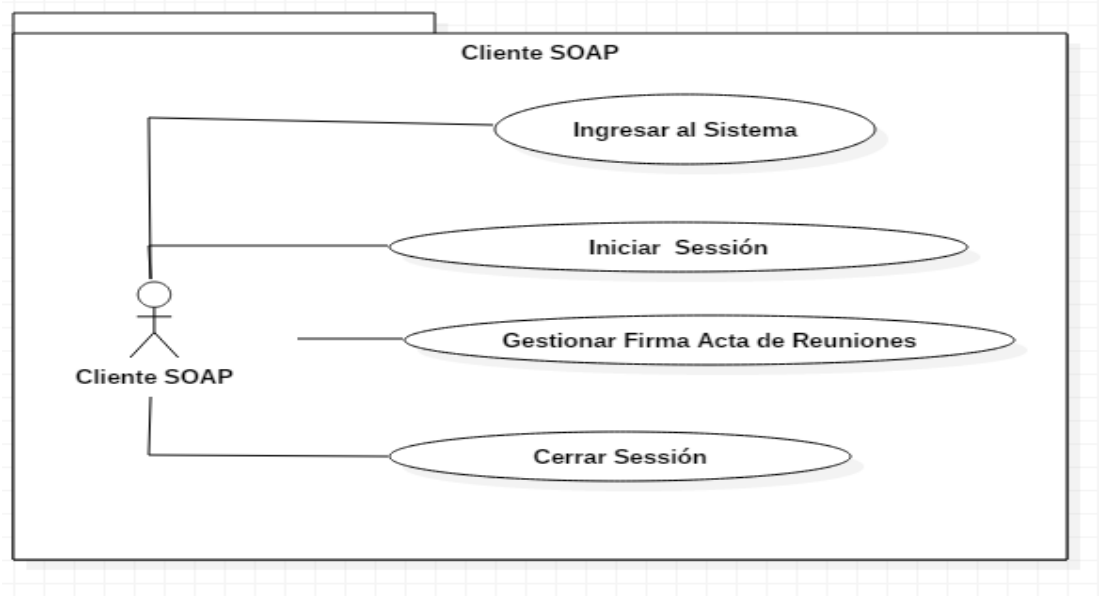


Figura 14. Caso de Uso 3 Cliente SOAP

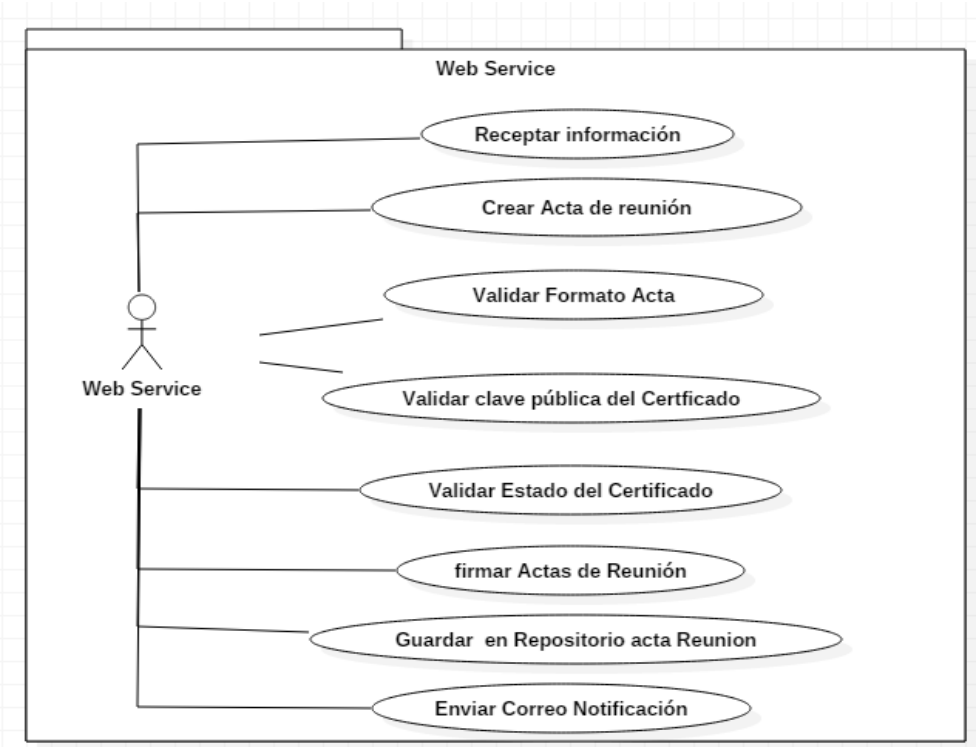


Figura 15. Caso de Uso 4 Web Service

- **Diagrama de Secuencia**

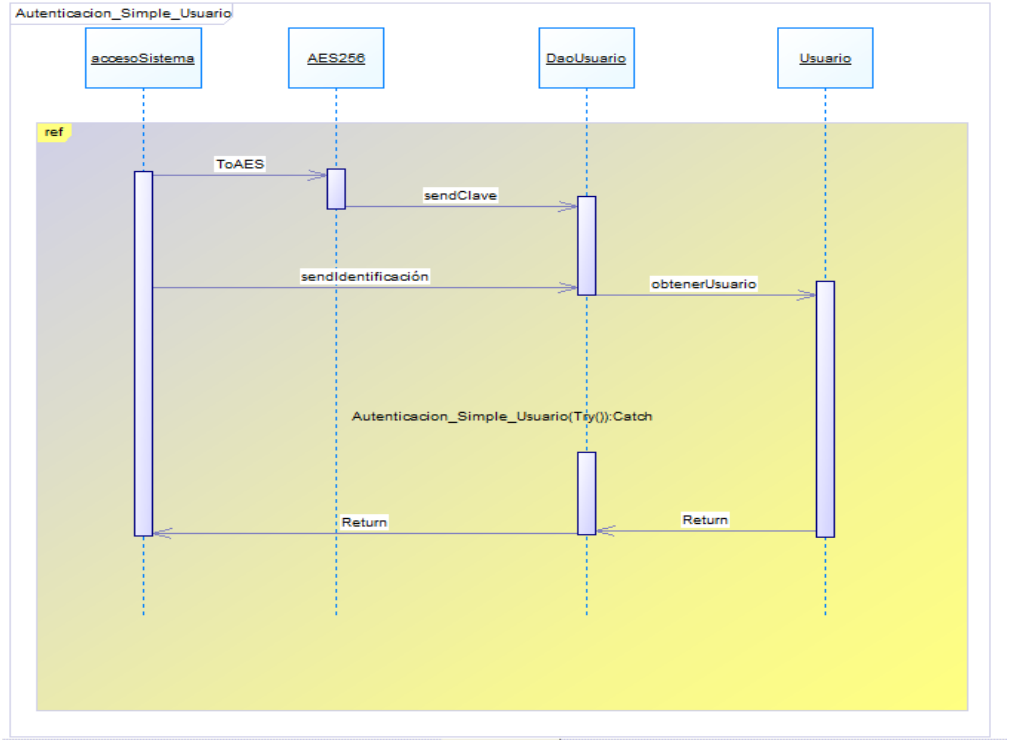


Figura 16. Diagrama de Secuencia 1 Autenticación Simple Usuario

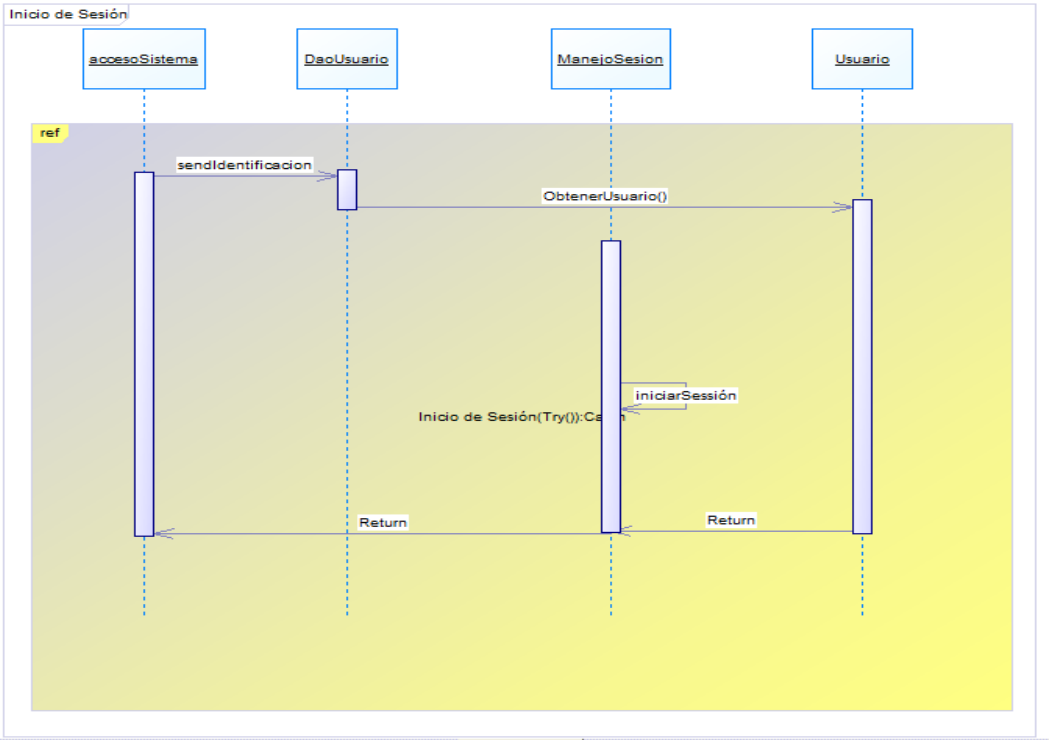


Figura 17. Diagrama de Secuencia 2 Inicio de Sesión

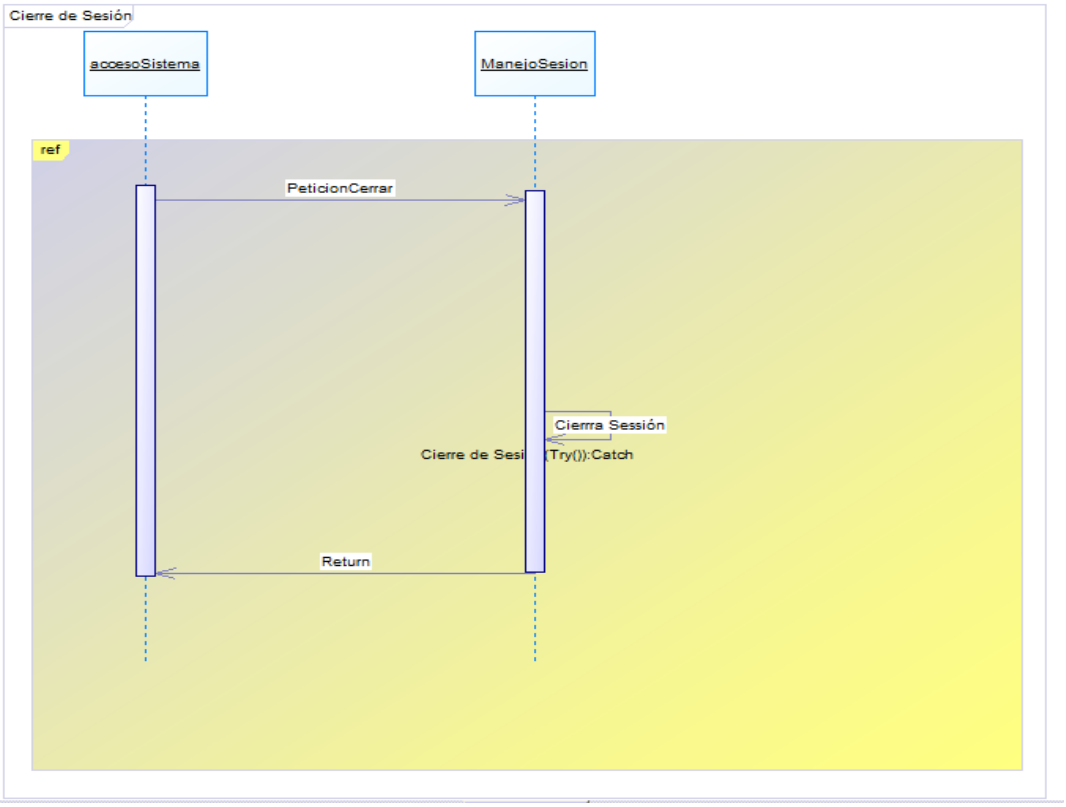


Figura 18. Diagrama de Secuencia 3 Cierre Sesión

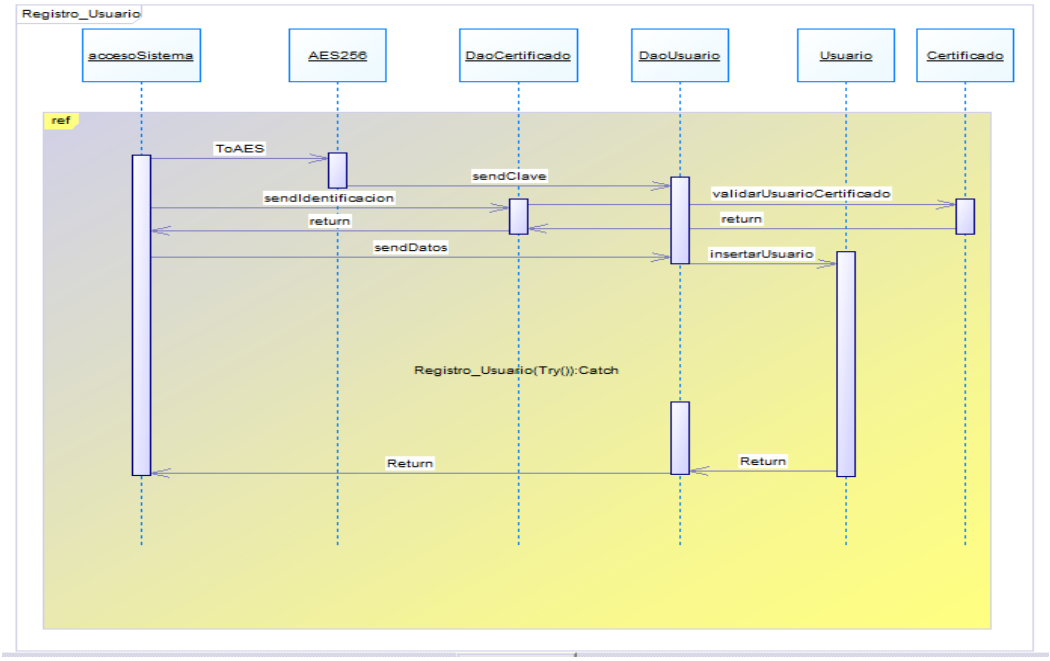


Figura 19. Diagrama de Secuencia 4 Registro Usuario

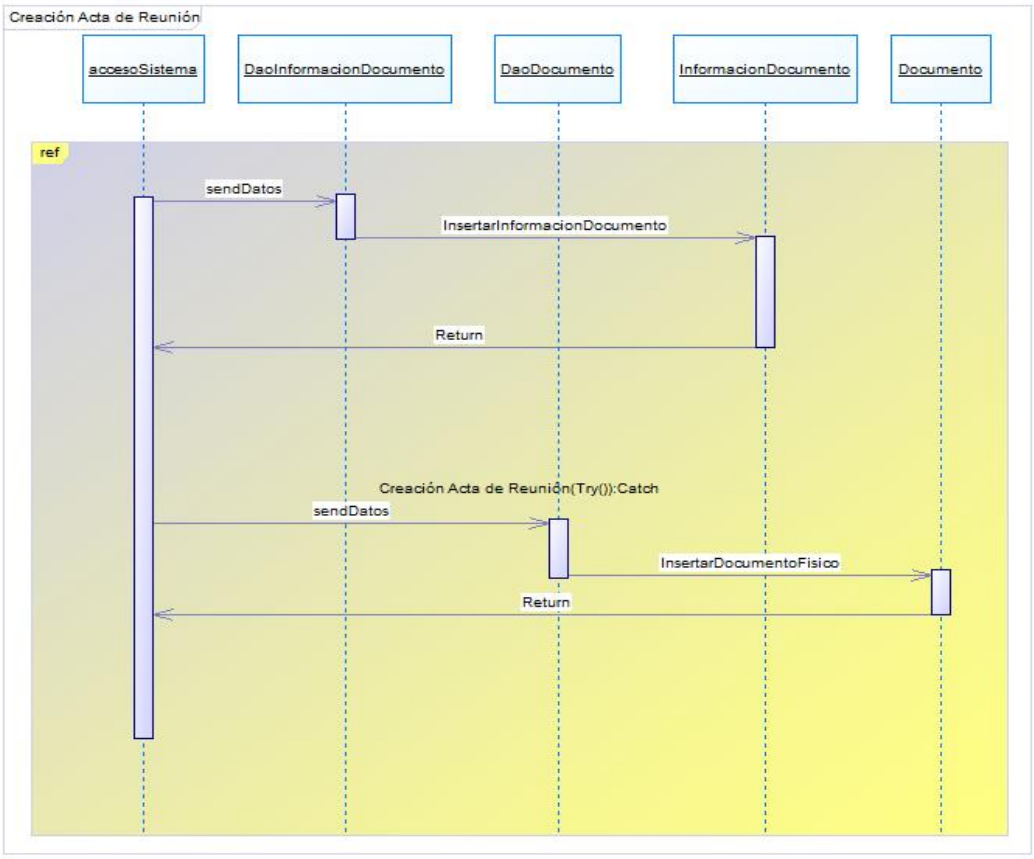


Figura 20 - Diagrama de Secuencia 5 Creación Acta de Reunión

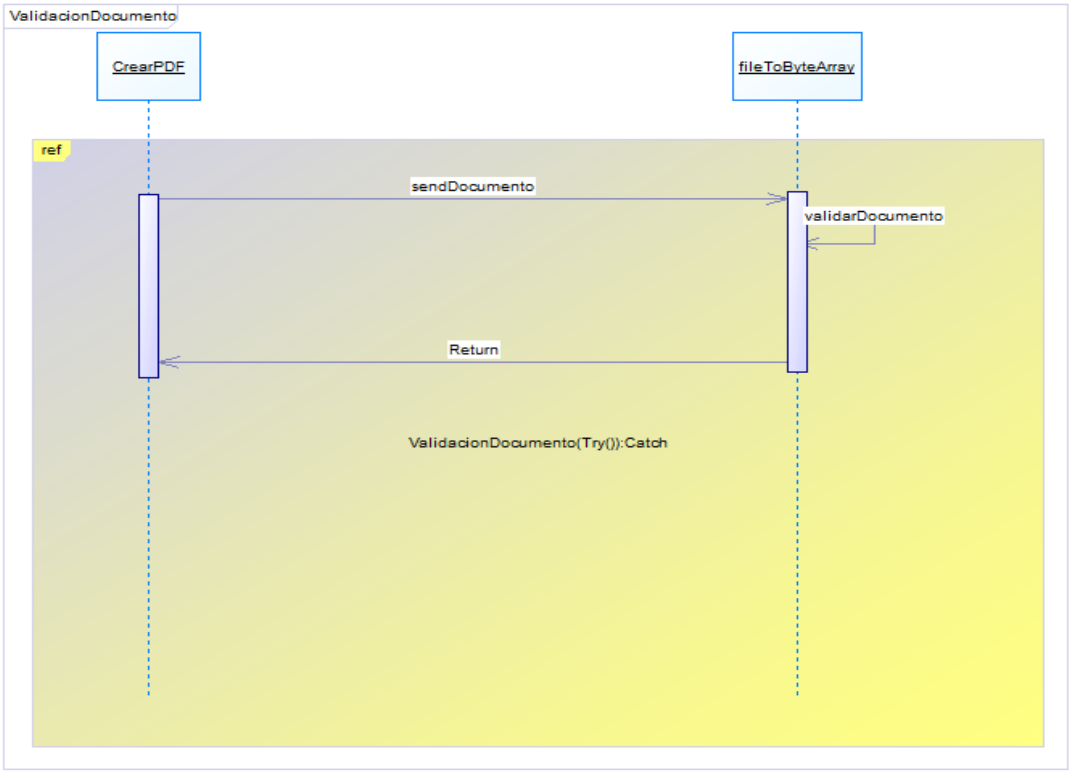


Figura 21. Diagrama de Secuencia 6 Validación de Documentos

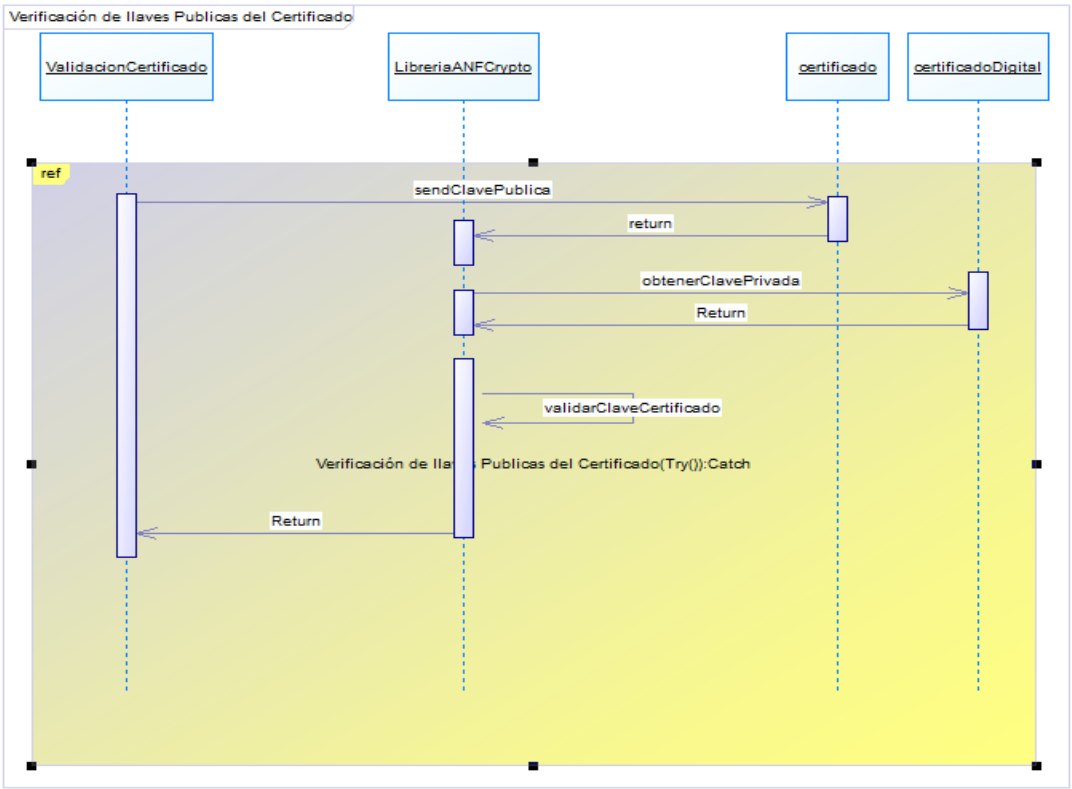


Figura 22. Diagrama de Secuencia 7 Validación llaves Publicas Certificado

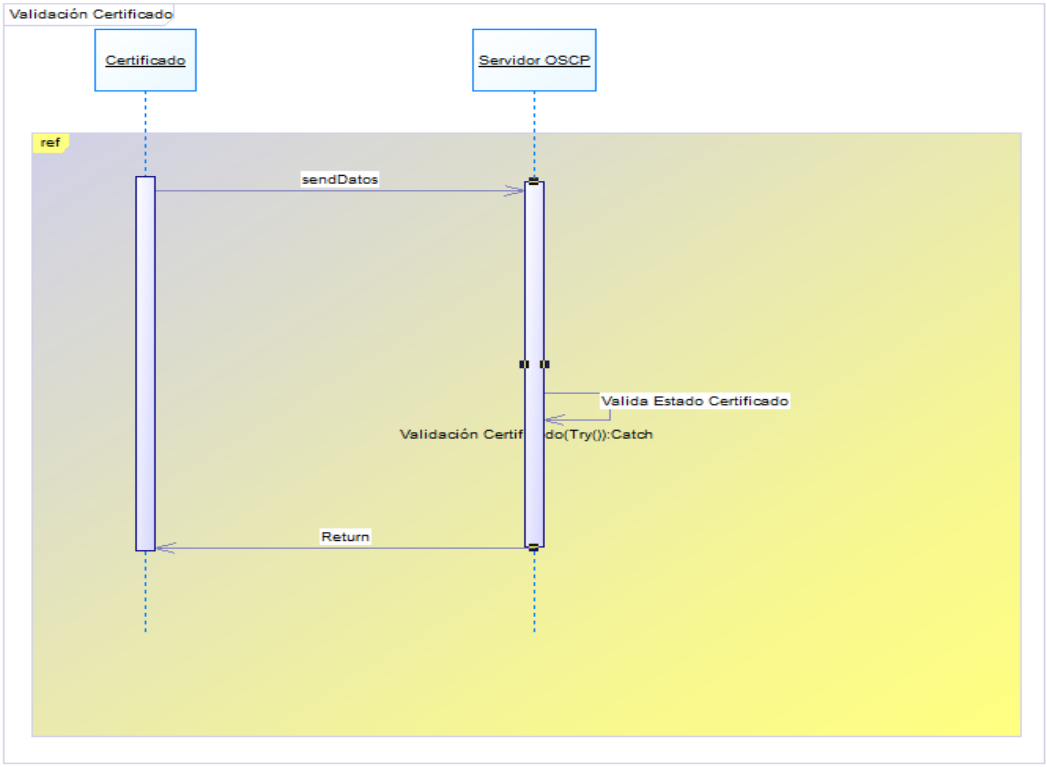


Figura 23. Diagrama de Secuencia 8 Validación Certificado

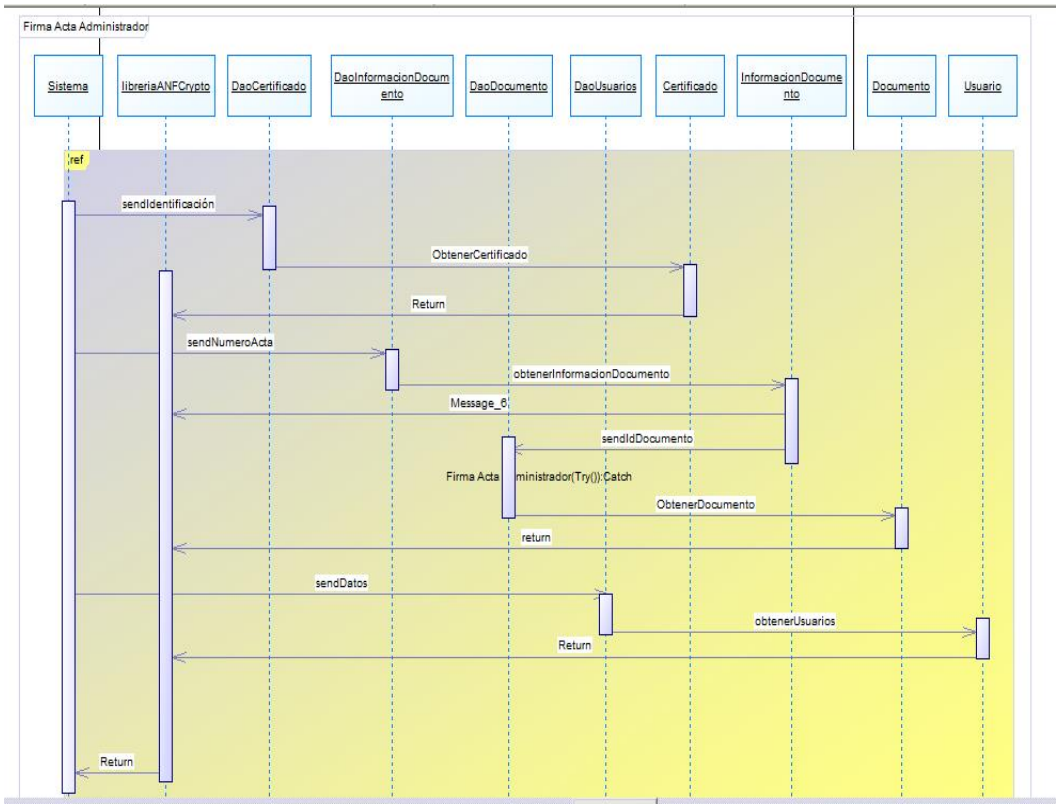


Figura 24. Diagrama de Secuencia 9 Firma Acta Administrador

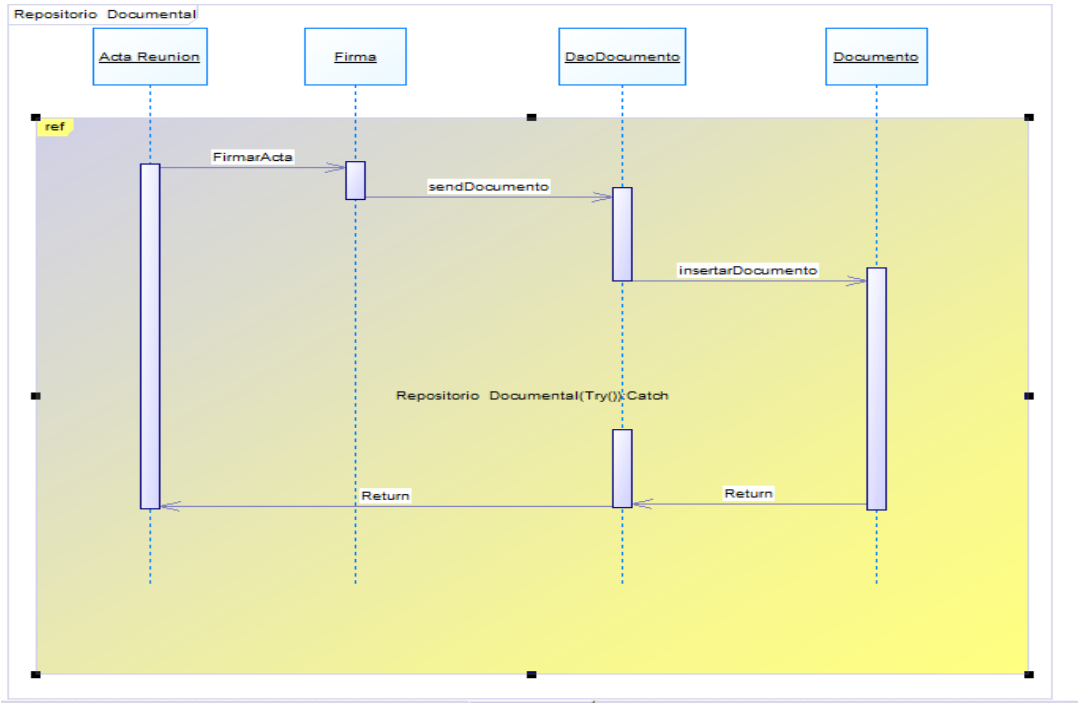


Figura 25. Diagrama de Secuencia 10 Repositorio Documental

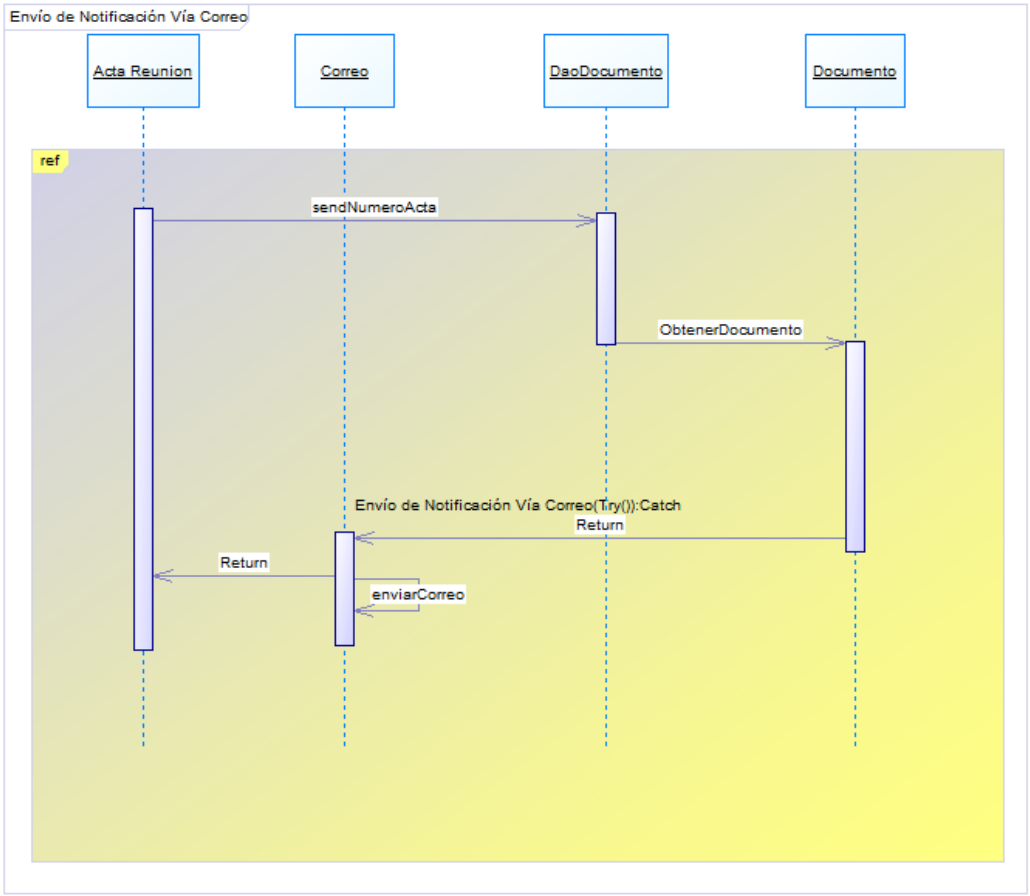


Figura 26. Diagrama de Secuencia 11 Envío Notificación

3.2.2. Diagramas de Estructura Entidad Relación

- **Diagrama Lógico**

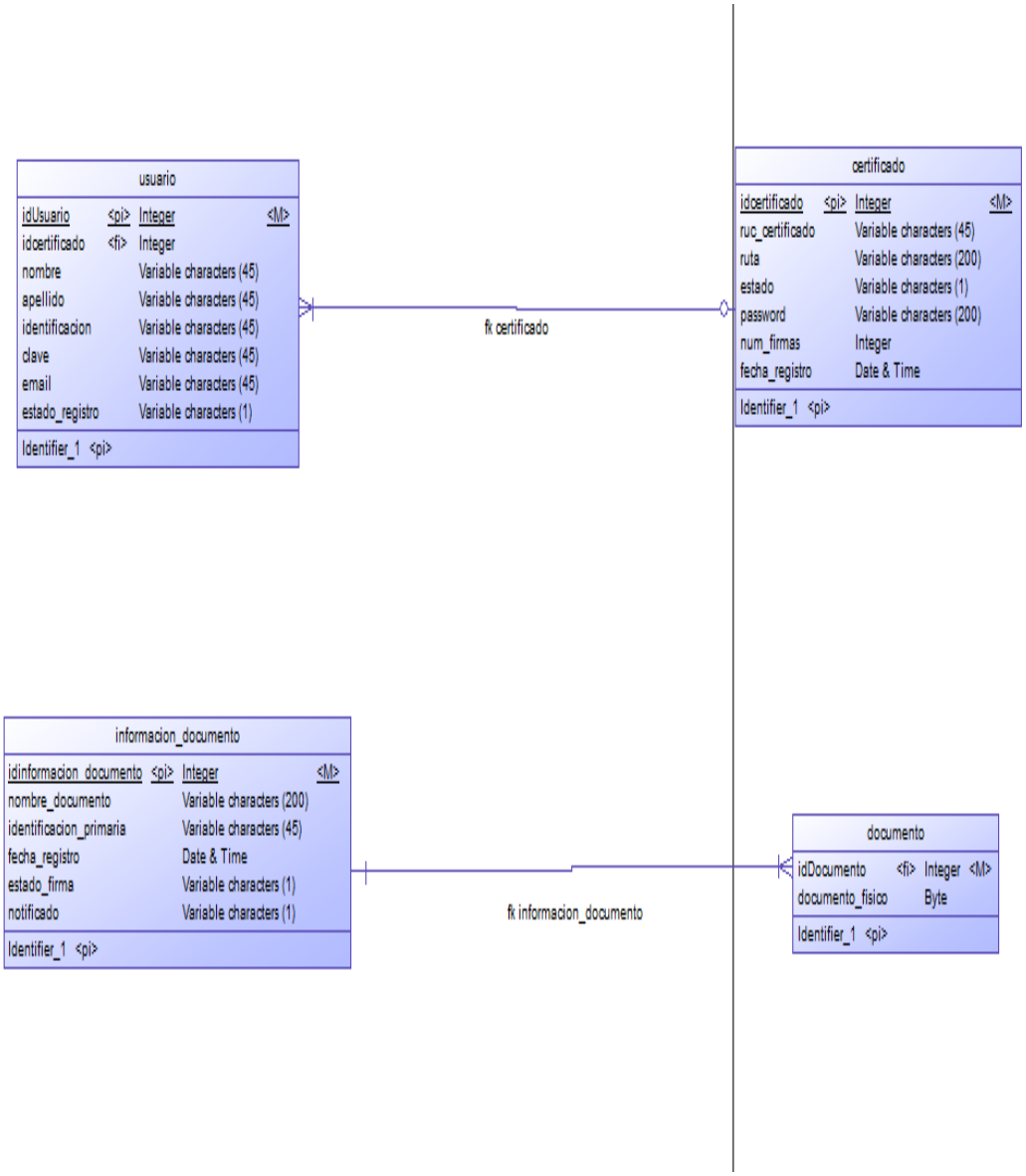


Figura 27. Diagrama Lógico 1 Gestión de Firma y Usuarios

- **Diagrama de Clases**

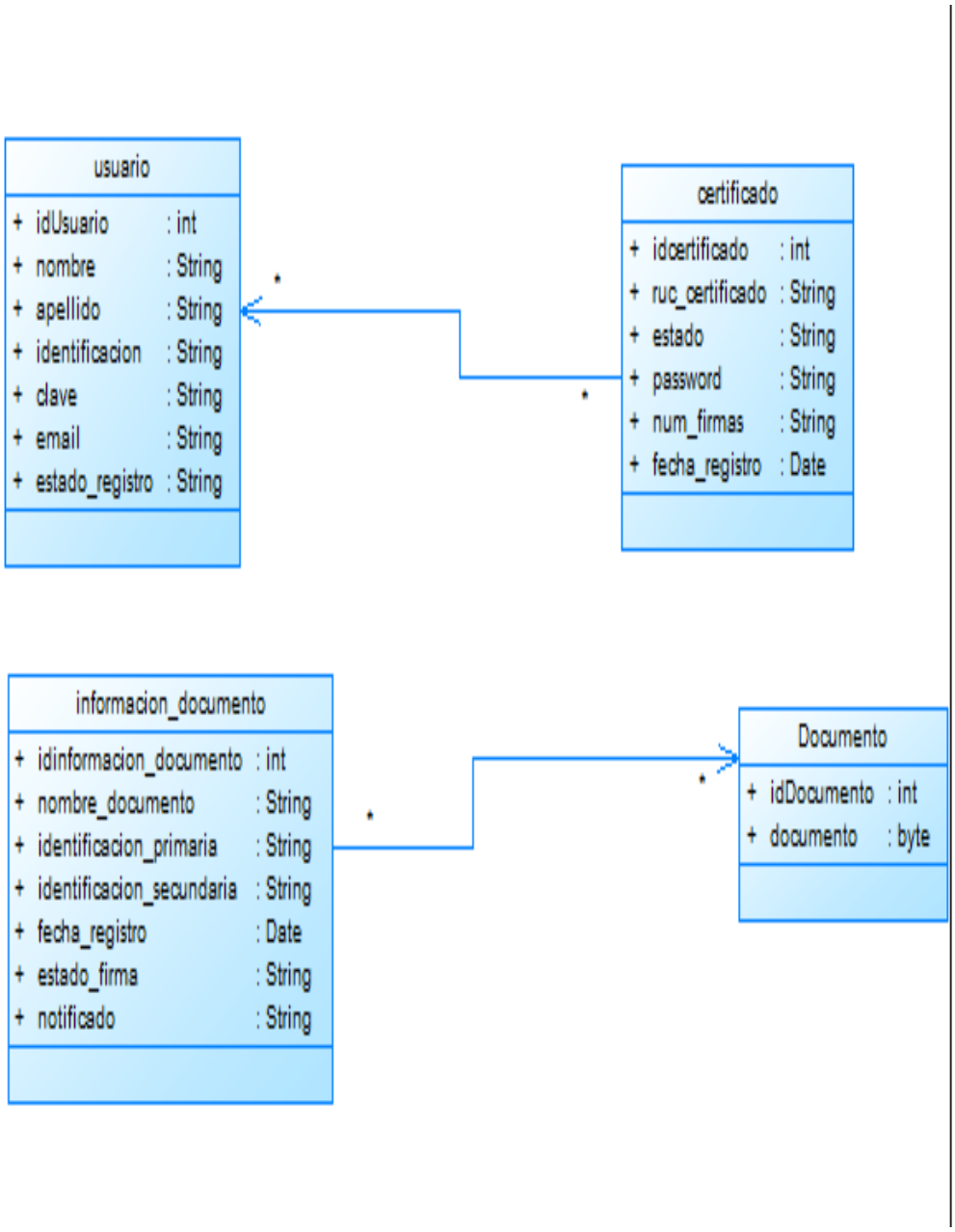


Figura 28. Diagrama Clases 1 Gestión de Firma y Usuarios

- **Diagrama Físico**

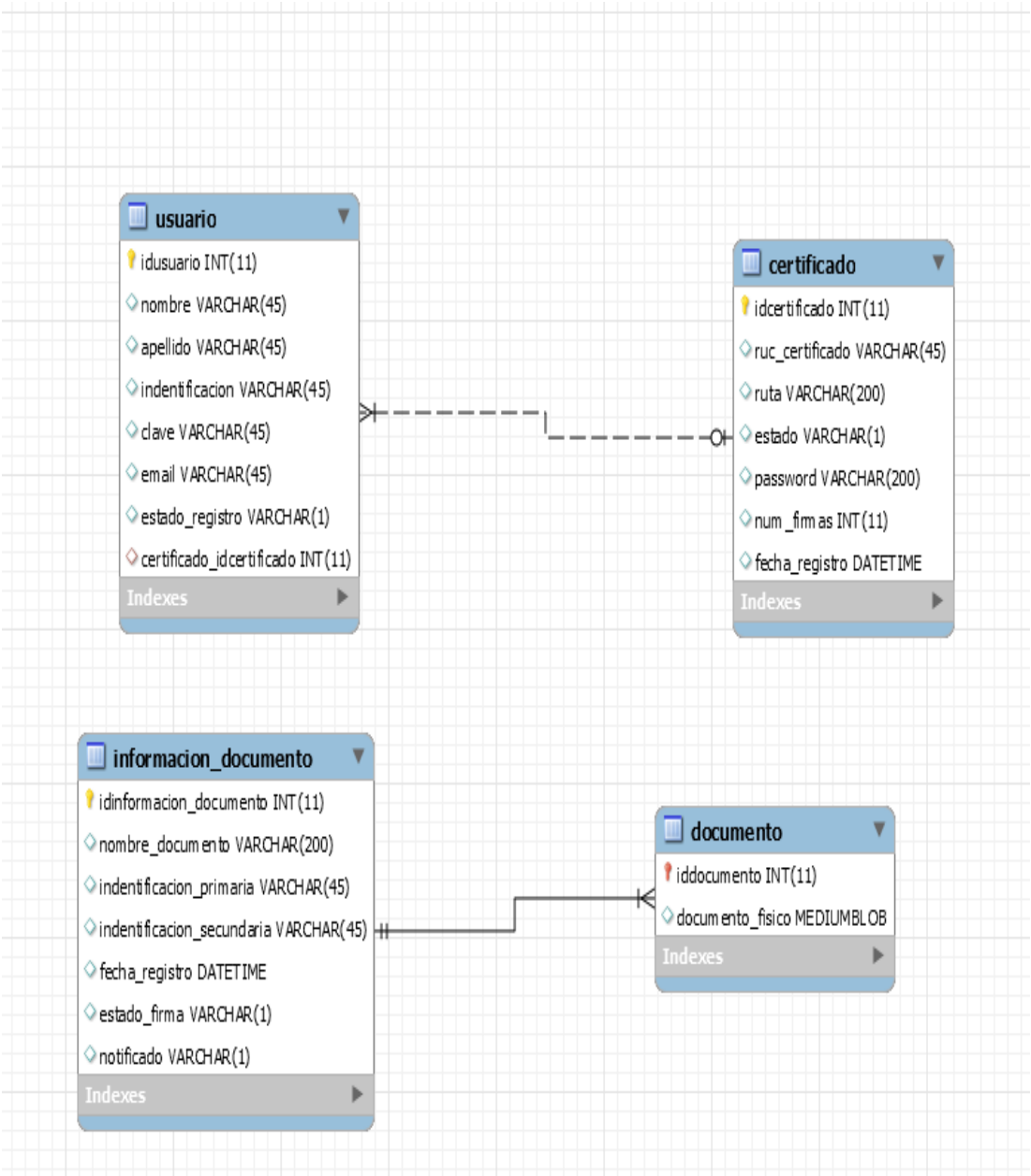


Figura 29. Diagrama Físico 1 Gestión de Firma y Usuarios

3.2.3. Diccionario de Datos

Tabla 15

Tabla Usuario

Columna	Tipo de dato	Pk	NN	AI	NULL	Detalle
Idusuario	INT(11)	SI	SI	SI		Identificador único de la tabla Usuario
Nombre	VARCHAR(45)					Nombre del usuario que se registra
apellido	VARCHAR(45)				NULL	Apellido del usuario que se registra
Identificación	VARCHAR(45)				NULL	Cedula o Ruc del usuario
Clave	VARCHAR(45)				NULL	Clave cifrada del usuario
Email	VARCHAR(45)				NULL	Dirección correo electrónico del usuario
estado_registro	VARCHAR(45)				NULL	Estado registro del usuario
certificado_idcertificado	INT(11)				NULL	Identificador de la tabla certificado

Tabla 16

Tabla Certificado

Columna	Tipo de dato	Pk	NN	AI	Por defecto	Detalle
idcertificado	INT(11)	SI	SI	SI		Identificador único de la tabla Certificado
ruc_certificado	VARCHAR(45)				NULL	Ruc del certificado
Ruta	VARCHAR(200)				NULL	Dirección de ubicación del certificado
estado	VARCHAR(1)				NULL	Estado de validación del certificado
password	VARCHAR(200)				NULL	Clave pública del certificado
num_firmas	INT(11)				NULL	Contador de firmas
fecha_registro	DATETIME				NULL	Fecha de registro del certificado

Tabla 17

Tabla Documento

Columna	Tipo de dato	Pk	NN	UQ	AI	Por defecto	Detalle
Iddocumento	INT(11)	SI	SI				Identificador único de la tabla Documento
Documento_fisico	MEDIUMBLOB					NULL	Documento físico (acta de reunión firmada)

Tabla 18

Tabla Información Documento

Columna	Tipo de dato	Pk	NN	AI	Por defecto	Detalle
Idinformacion_documento	INT(11)	SI	SI	SI		Identificador único de la tabla Información Documento
nombre_documento	VARCHAR(200)				NULL	Número del acta de reunión
identificacion_primaria	VARCHAR(45)				NULL	Ruc del usuario administrador
identificacion_secundaria	VARCHAR(45)				NULL	Ruc/cedula del usuario normal
fecha_registro	DATETIME				NULL	Fecha de registro del acta creada
estado_firma	VARCHAR(1)				NULL	Estado de la firma en la acta
notificado	VARCHAR(1)				NULL	Notificación del envío de correo

3.2.4. Diseño de Interfaces

- **Usuario Administrador**

a) Cliente SOAP móvil

Figura 30. Diseño Aplicación

b) Login al Cliente SOAP móvil

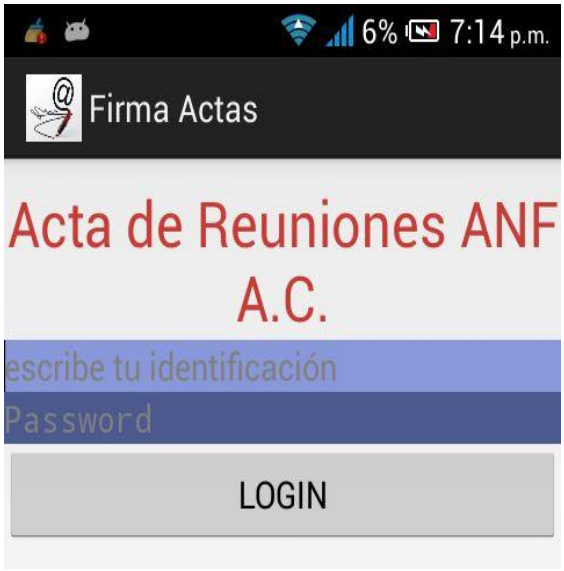


Figura 31. Diseño Interfaz Login

Figura 32. Diseño Interfaz Login 2

c) Menú Administrador

Figura 33. Diseño Interfaz Menú Administrador

d) Registro de Usuario

Figura 34. Diseño Interfaz Registro

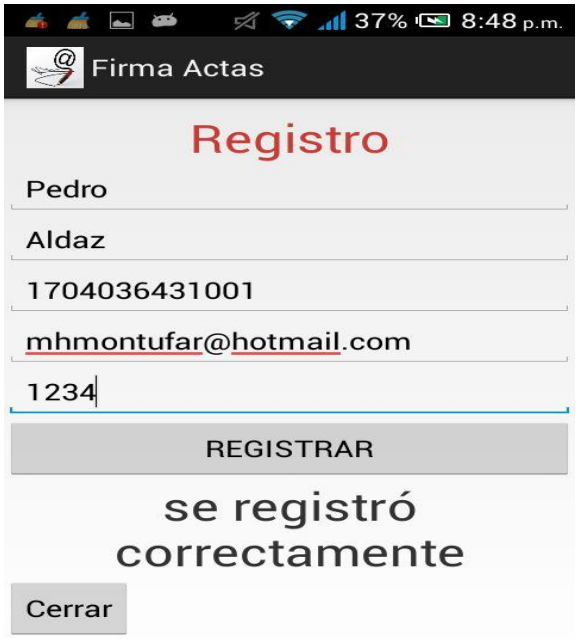


Figura 35. Diseño Interfaz Registro 2

e) Formulario Acta de Reuniones

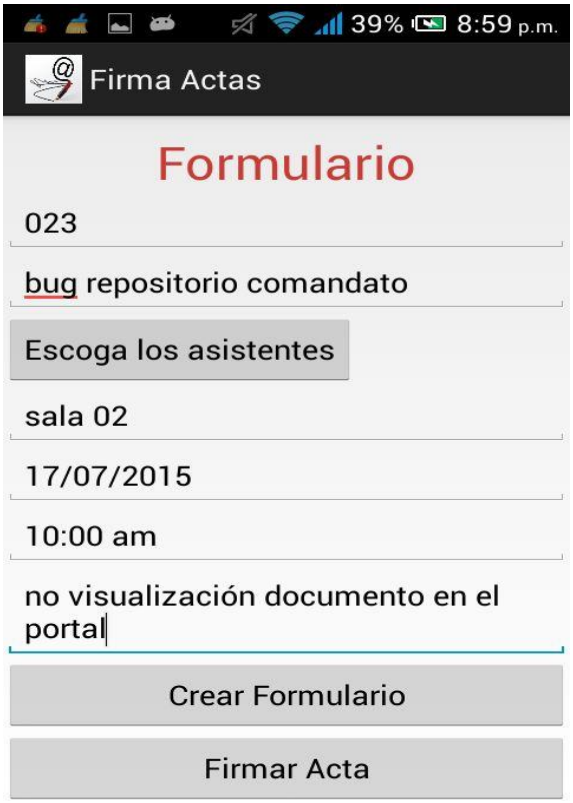


Figura 36. Diseño Interfaz Formulario

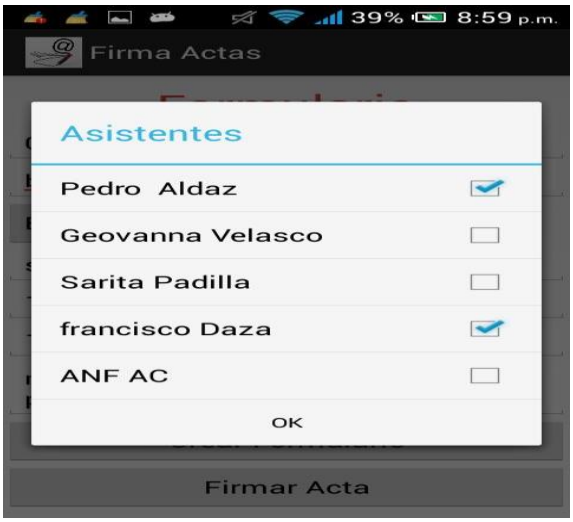


Figura 37. Diseño Interfaz Menú asistentes

f) Firma Acta

Figura 38. Diseño Interfaz Firma

Figura 39. Diseño Interfaz Menú Asistentes

Figura 40. Diseño Interfaz Firma 2

g) Envío de notificación actas firmadas

Figura 41. Diseño Interfaz Correo

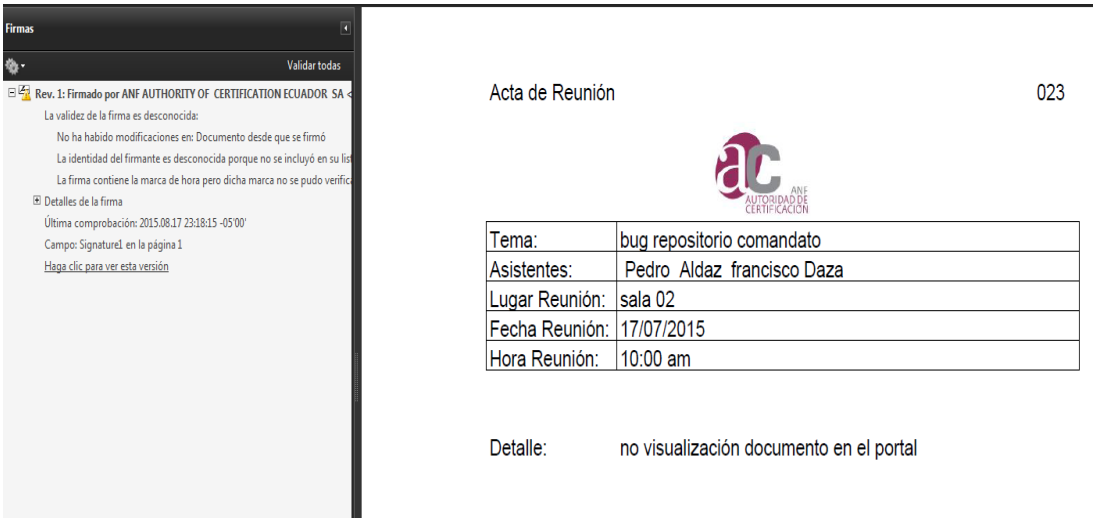


Figura 42. Diseño Interfaz PDF Firmado

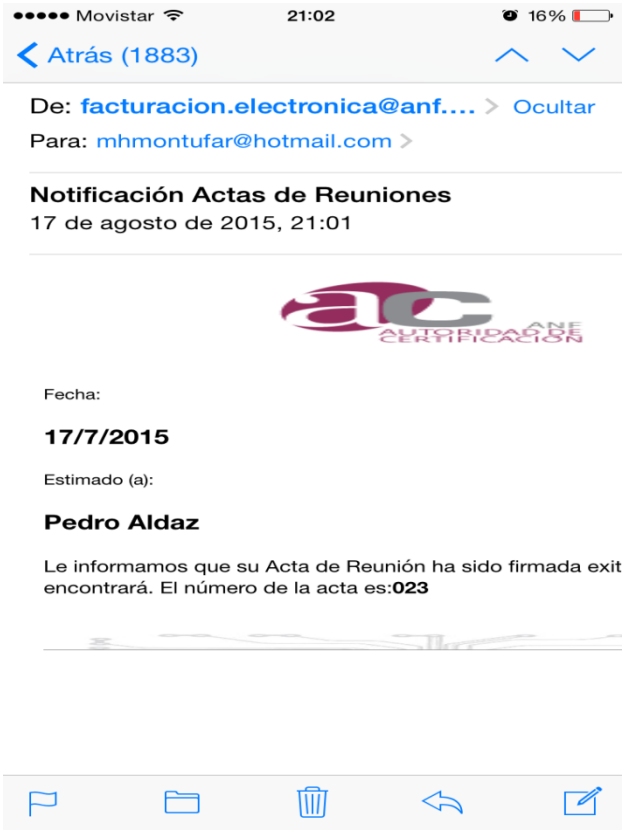


Figura 43. Diseño Interfaz Correo 2

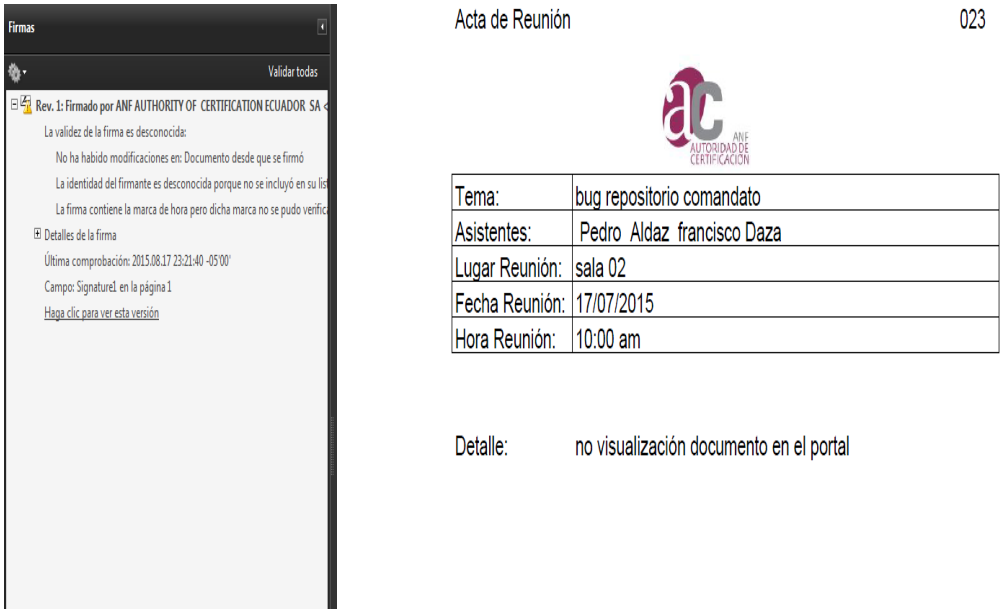


Figura 44. Diseño Interfaz PDF Firma 2

Figura 45. Diseño Interfaz Correo 3

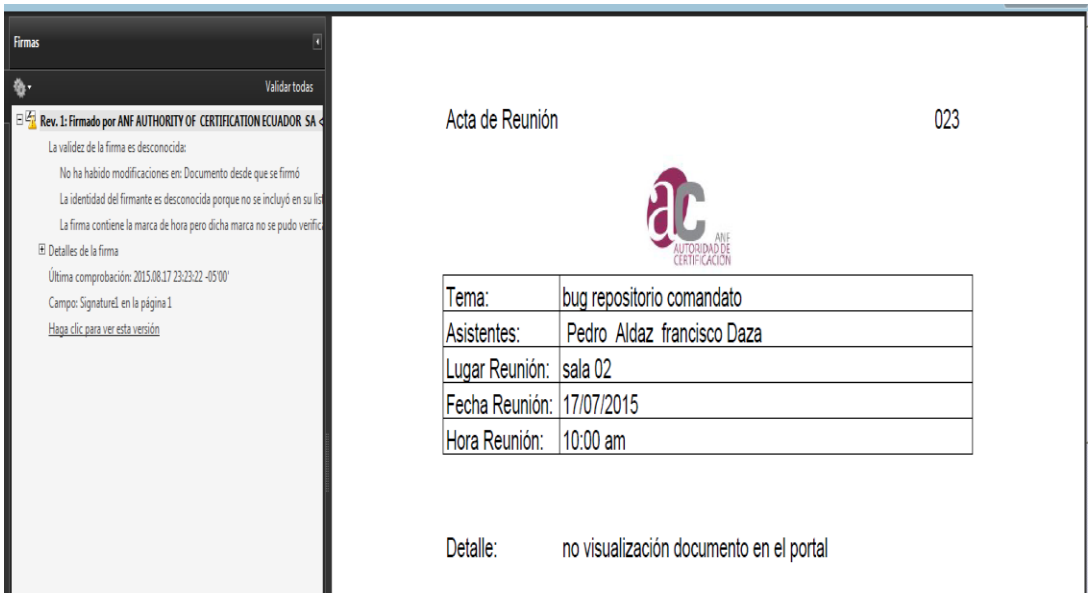


Figura 46. Diseño Interfaz PDF Firma 3

- **Usuario Normal**

h) Login Cliente SOAP móvil

Figura 47. Diseño Interfaz Login Cliente

i) Firmar Acta

Figura 48. Diseño Interfaz Firma Cliente

Figura 49. Diseño Interfaz Firma Cliente 2

j) Envió notificación acta firmada

Figura 50. Diseño Interfaz Correo Cliente

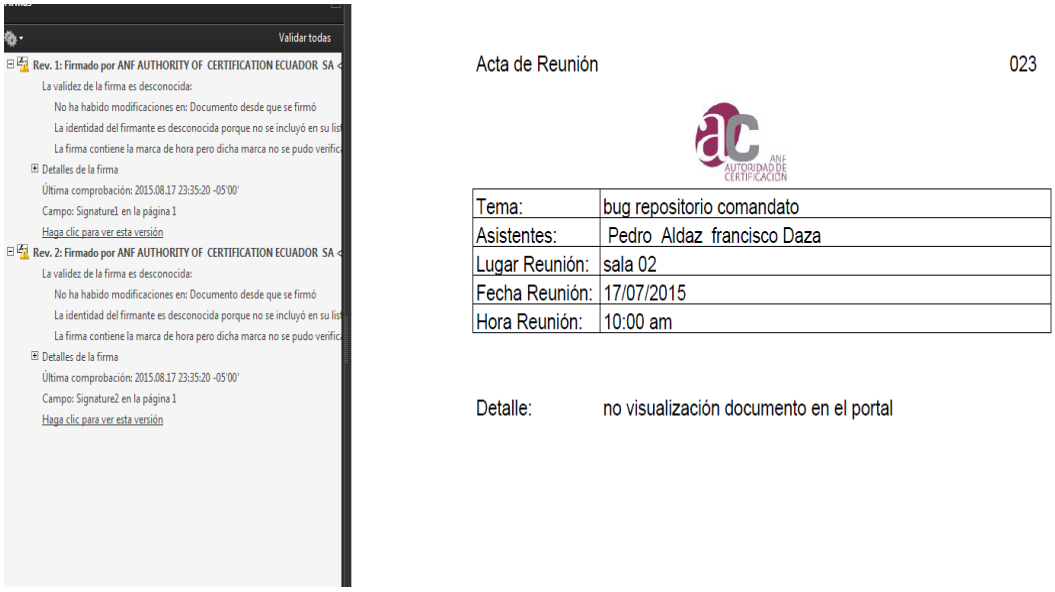


Figura 51. Diseño Interfaz PDF Firma Cliente

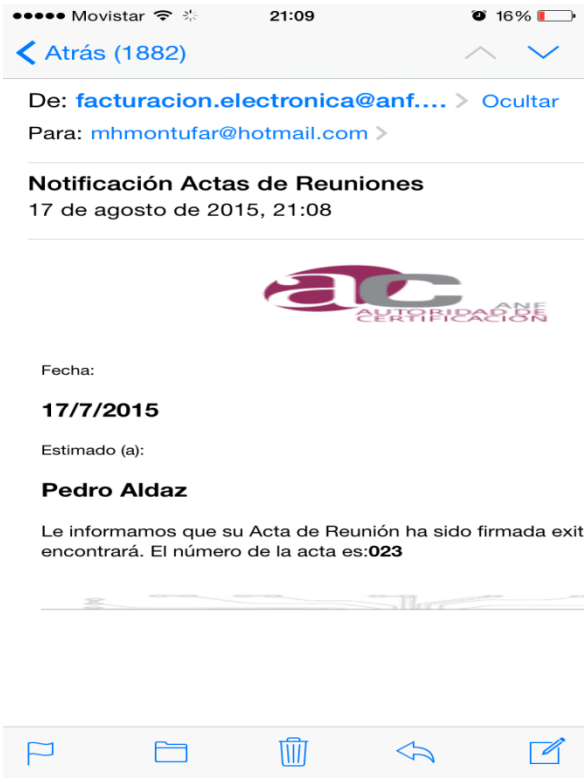


Figura 52. Diseño Interfaz Correo Cliente 2

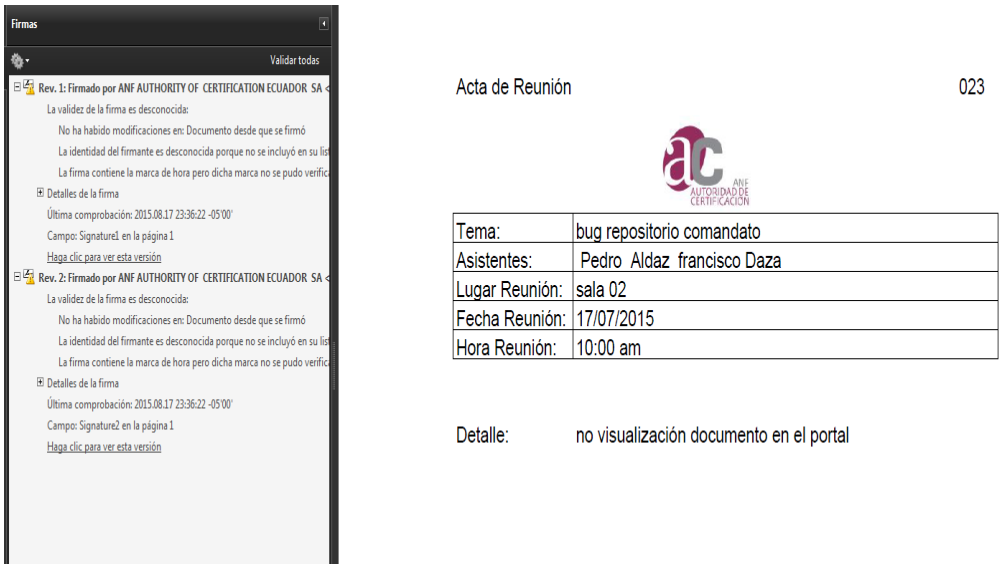


Figura 53. Diseño Interfaz PFD Firma Cliente 2

K) Múltiple Firma Electrónica

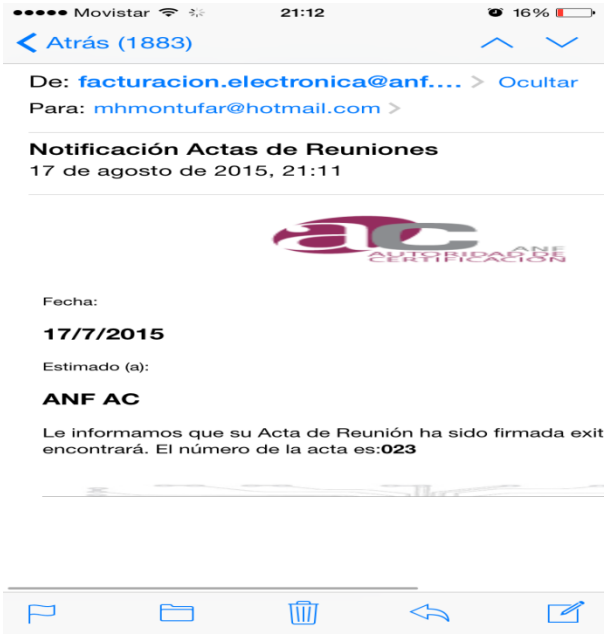


Figura 54.Diseño Interfaz Correo MultiFirma

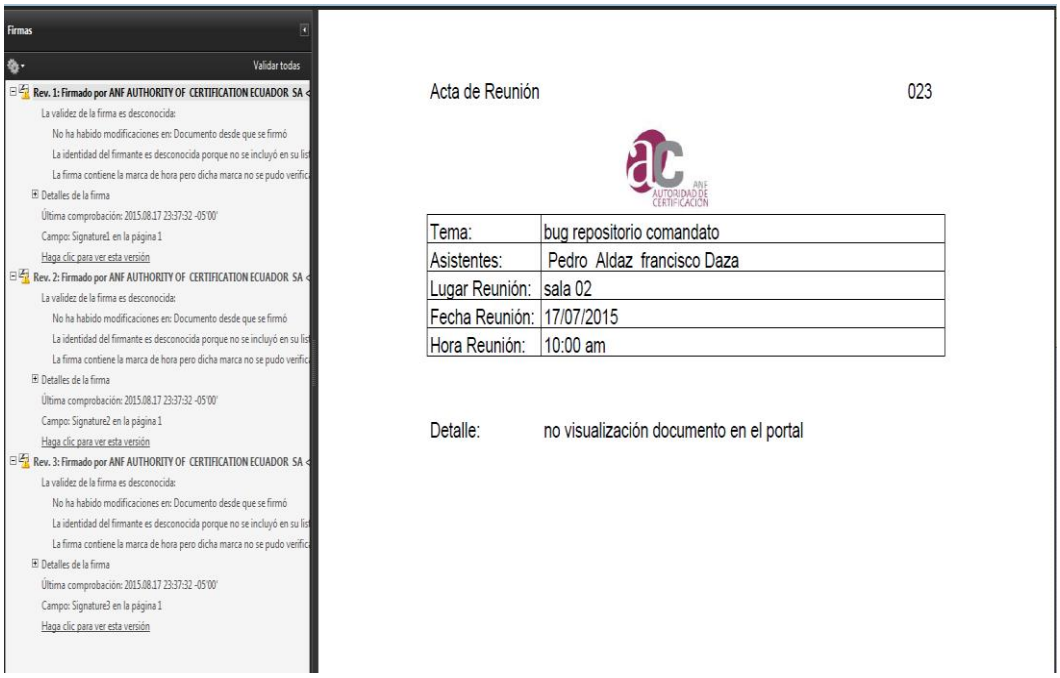


Figura 55. Diseño Interfaz PDF MultiFirma

4. CAPÍTULO 4

IMPLEMENTACIÓN DEL SISTEMA

4.1. Codificación

4.1.1. Cliente SOAP

La Creación del Cliente SOAP con tecnología móvil Android 4.2.2, contempla la funcionalidad de la aplicación a nivel de pantallas (interfaces) para que el usuario pueda gestionar la creación, firmado y envío de notificación de actas de reuniones.

Este desarrollo se basa en varias clases las cuales son para hacer peticiones al Servicio web de firmas electrónicas, esta petición son a través de la tecnología SOAP con protocolo HTTP.

Para conectarse el cliente SOAP al Servicio Web de firmas, utiliza la librería KSOAP2.

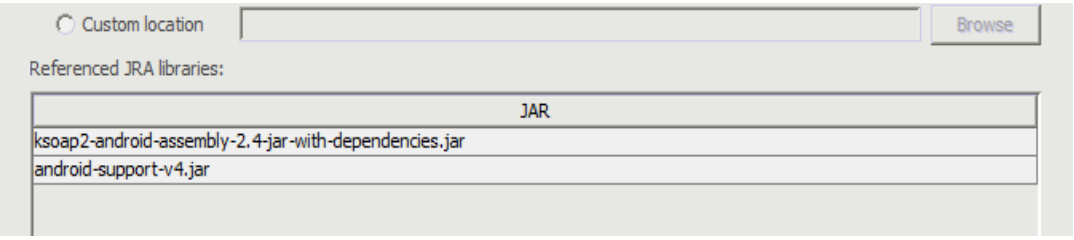


Figura 56. Librerías Consumo WS

Además el servicio de esta aplicación se clasifica en dos Usuarios cuales son:

- ✓ Usuario Administrador
- ✓ Usuario Normal

Las funcionalidades del Cliente SOAP son:

- Login a la aplicación
- Inicio de Sesión
- Gestión de Usuarios
- Elaboración de Actas de reuniones
- Firma de Actas de Reuniones
- Repositorio Documental
- Envío de notificación
- Cierre de Sesión

4.1.2. Web Service Firma

El Web Service o Servicio Web está desarrollado con tecnología SOAP JAVA protocolo HTTP y lenguaje WSDL, al crear ese servicio web facilita a cualquier cliente SOAP hacer peticiones para utilizar varias funcionalidades que en conjunto hacen la gestión de elaboración firma y envío de notificación de actas de reuniones para la empresa ANF A.C.

A continuación la funcionalidad de estos servicios Web lo clasifica de la siguiente manera:

- **Módulo de Certificados**

Este módulo se encarga de la gestión de la firma de las actas de reuniones.

En primera instancia en este módulo guarda la información del certificado electrónico para su futura utilización, al tener esta información el cliente SOAP puede utilizar fácilmente haciendo peticiones y el servicio web se conectará al repositorio para validar los datos.

Las funcionalidades de este módulo son:

- Repositorio de la Información del Certificado
- Validación de estado del Certificado

- Validación del Certificado Electrónico
- Validación del Usuario Certificado

- **Módulo de Usuarios**

Este módulo se encarga de la gestión de los Usuarios.

En primera instancia en este módulo guarda la información del Usuario para su futura utilización, al tener esta información el cliente SOAP puede acceder fácilmente haciendo peticiones y el servicio web se conectará al repositorio para validar los datos.

Las funcionalidades de este módulo son:

- Repositorio de la Información del Usuario
- Validación del Usuario
- Relación del Usuario con el Certificado Electrónico
- Relación del Usuario con el documento acta de reunión

- **Módulo de Documentación**

Este módulo se encarga de la gestión de las Actas de Reuniones.

En primera instancia en este módulo guarda la información de las actas de reunión para su futura utilización, al tener esta información el cliente SOAP puede acceder fácilmente haciendo peticiones y el servicio web se conectará al repositorio para validar los datos.

Las funcionalidades de este módulo son:

- Repositorio de la Información de la acta
- Repositorio de la documento físico de la acta
- Validación del Documento
- Relación del Documento con la firma electrónica

- Relación del Documento con el envío de notificación

- **Módulo Firma**

Este módulo gestiona todo el proceso de firma electrónica para las actas de reuniones, es decir este módulo es el núcleo de este proyecto.

Una vez que el Cliente SOAP elaboró el acta de reunión la fase más importante es la firma electrónica de ese documento.

Para firmar electrónicamente cualquier clase de documento electrónico se necesita de un pequeño proyecto consola elaborado en JAVA donde existe la funcionalidad para firmar electrónicamente además está compuesto de un conjunto de librerías. Estas librerías son exclusivas (propiedad Intelectual) de la Empresa ANF A.C.

Aquel proyecto consola se conecta a los servidores de firma electrónica de esta empresa y valida las credenciales del certificado, el tipo de certificado, validación del estado del certificado, y procede con la firma electrónica.

Las librerías de firma son:

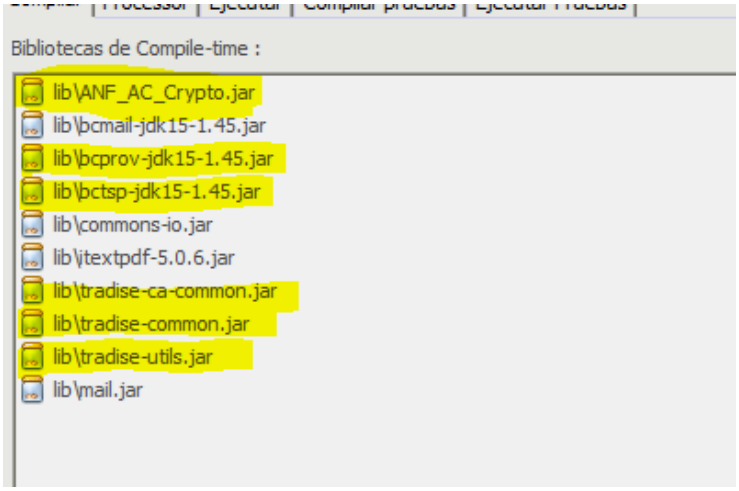


Figura 57. librerías de Firma ANF

- **Módulo envío Notificación**

Este módulo gestiona el proceso de envío de notificación por correo electrónico de las actas firmadas.

Una vez que el Cliente SOAP firmó el acta de reunión este módulo envía un correo notificando a cada usuario que el acta ha sido firmada.

Para enviar la notificación del acta firmada a un usuario, se desarrolló de un pequeño proyecto consola elaborado en JAVA.

- **Módulo de Persistencia**

Este módulo de persistencia gestiona toda la iteración entre el servicio web y el modelo de datos a través de la utilización de un Mapeo Objeto relacional en clases Java (framework Hibernate) y la configuración de persistencia con las librerías C3PO.

La ventaja de utilizar este framework Hibernate para el manejo de persistencia es la creación de múltiples transacciones con una sola sesión y su robustez al momento de conectarse a una base de datos.

4.2.Pruebas y Verificación

4.2.1. Pruebas Unitarias

Básicamente consiste en la ejecución de actividades individuales permitiendo al programador verificar que los componentes unitarios están codificados bajo la calidad que corresponde para soportar datos erróneos o datos inesperados.

Es necesario que por lo básico se realicen dos casos de pruebas unitarias al mismo componente el cual comprobara una positiva y una negativa.

Realizar las pruebas unitarias principales.

- Pruebas de encriptación de bloques de datos

  - Prueba1 `

```
    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            String _clave = AES256.toMessage("12345678");

            System.out.println(_clave);
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
est > main > try >
- servidor_firmaPDF (run) ×
ago 19, 2015 9:42:21 PM Utils.test main
GRAVE: null
javax.crypto.IllegalBlockSizeException: Input length must be multiple of 16 when decrypting with padded cipher
        at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:913)
        at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:913)
        at com.sun.crypto.provider.CipherCore.doFinal(CipherCore.java:824)
        at com.sun.crypto.provider.AESCipher.engineDoFinal(AESCipher.java:436)
        at javax.crypto.Cipher.doFinal(Cipher.java:2121)
        at Utils.AES256.toMessage(AES256.java:59)
        at Utils.test.main(test.java:27)

BUILD SUCCESSFUL (total time: 3 seconds)
```

Figura 58. Prueba 1

- Prueba 2

```
/**
 * @param args the command line arguments
 */
public static void main(String[] args) {
    try {
        Valores.init();

        String _clave = AES256.toMessage("t75CIeQDO11g1fX7HLwj65FGIK1o6lVdnMnlSUOCZl4=");

        System.out.println(_clave);
    } catch (Exception ex) {
        Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
    }

}
}
```

```
servidor_firmaPDF (run) ×
run:
12345678
BUILD SUCCESSFUL (total time: 2 seconds)
```

Figura 59. Prueba 2

Resultados

Tabla 19

Prueba

Número de prueba	Nombre de método	Resultado
1	toMessage()	Fallida
2	toMessage()	OK

- Validación de funciones de peticiones a la base de datos
  - Prueba1

```
    public static void main(String[] args) {
        try {
            Valores.init();

            Certificado cert = new Certificado();
            DAOCertificado daocert = new DAOCertificado();
            cert = daocert.ObtenerCertificado("179221");
            System.out.println(cert.getRucCertificado());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
est > main > try >
a - servidor_firmaPDF (run) ×
ago 19, 2015 10:01:32 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:01:32 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:01:32 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
ago 19, 2015 10:01:33 PM Utils.test main
GRAVE: null
java.lang.NullPointerException
        at Utils.test.main(test.java:30)

BUILD SUCCESSFUL (total time: 6 seconds)
```

Figura 60. Prueba 1

- Prueba2

```
    public static void main(String[] args) {
        try {
            Valores.init();

            Certificado cert = new Certificado();
            DAOCertificado daocert = new DAOCertificado();
            cert = daocert.ObtenerCertificado("www");
            System.out.println(cert.getRucCertificado());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
st > main > try >
- servidor_firmaPDF (run) ×
ago 19, 2015 10:03:31 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:03:31 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:03:31 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
ago 19, 2015 10:03:31 PM Utils.test main
GRAVE: null
java.lang.NullPointerException
        at Utils.test.main(test.java:30)

BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 61. Prueba 2

- Prueba3

```
    public static void main(String[] args) {
        try {
            Valores.init();

            Certificado cert = new Certificado();
            DAOCertificado daocert = new DAOCertificado();
            cert = daocert.ObtenerCertificado("1792218225001");
            System.out.println(cert.getRucCertificado());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
main > try >
servidor_firmaPDF (run) ×
ago 19, 2015 10:04:30 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:04:30 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:04:30 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:04:30 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:04:30 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
1792218225001
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 62. Prueba 3

- Prueba 4

```
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            Usuario us = new Usuario();
            DAOUsuario daus = new DAOUsuario();
            List<Usuario> listaUs = new ArrayList<Usuario>();
            listaUs = daus.ObtenerListaUsuario();
            System.out.println(listaUs.get(1));
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
st > main > try >
- servidor_firmaPDF (run) X
ago 19, 2015 10:10:11 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:10:11 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:10:11 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:10:11 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:10:12 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
firmador.modelo.Usuario@4c583ecf
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 63. Prueba 4

- Prueba 5

```
    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            Usuario us = new Usuario();
            DAOUsuario daus = new DAOUsuario();
           us = daus.ObtenerMailUsuario("1792218");
            System.out.println(us.getNombre());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
main > try >
servidor_firmaPDF (run) ×
go 19, 2015 10:18:48 PM org.hibernate.cfg.SettingsFactory buildSettings
NFORMACIÓN: Named query checking : enabled
go 19, 2015 10:18:48 PM org.hibernate.impl.SessionFactoryImpl <init>
NFORMACIÓN: building session factory
go 19, 2015 10:18:48 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
NFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
go 19, 2015 10:18:49 PM Utils.test main
RAVE: null
ava.lang.NullPointerException
        at Utils.test.main(test.java:32)

UILD SUCCESSFUL (total time: 4 seconds)
```

Figura 64. Prueba 5

- Prueba 6

```
    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            Usuario us = new Usuario();
            DAOUsuario daus = new DAOUsuario();
           us = daus.ObtenerMailUsuario("1792218225001");
            System.out.println(us.getNombre());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
st > main > try >
- servidor_firmaPDF (run) ×
ago 19, 2015 10:19:42 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:19:42 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:19:42 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:19:42 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:19:42 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
ANF
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 65. Prueba 6

- Prueba 7

```
    public static void main(String[] args) {
        try {
            Valores.init();

            InformacionDocumento info = new InformacionDocumento();
            DaoInformacionDocumento dainfo = new DaoInformacionDocumento();
           info = dainfo.ObtenerDocumento("0140");
            System.out.println(info.getNombreDocumento());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
est
- servidor_firmaPDF (run)
ago 19, 2015 10:23:51 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:23:51 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:23:51 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
ago 19, 2015 10:23:51 PM Utils.test main
GRAVE: null
java.lang.NullPointerException
        at Utils.test.main(test.java:34)

BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 66. Prueba 7

- Prueba 8

```
    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            InformacionDocumento info = new InformacionDocumento();
            DaoInformacionDocumento dainfo = new DaoInformacionDocumento();
           info = dainfo.ObtenerDocumento("017");
            System.out.println(info.getNombreDocumento());
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
est > main > try >
- servidor_firmaPDF (run) ×
ago 19, 2015 10:24:39 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:24:39 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:24:39 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:24:39 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:24:39 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
017
BUILD SUCCESSFUL (total time: 3 seconds)
```

Figura 67. Prueba 8

- Prueba 9

```
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            InformacionDocumento info = new InformacionDocumento();
            DaoInformacionDocumento dainfo = new DaoInformacionDocumento();
          boolean aux = dainfo.actualizarNotificado(80,"1");
            System.out.println(aux);
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
ida - servidor_firmaPDF (run) ×
ago 19, 2015 10:28:33 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
ago 19, 2015 10:28:33 PM firmador.dao.DaoInformacionDocumento actualizarNotificado
GRAVE: null
org.hibernate.ObjectNotFoundException: No row with the given identifier exists: [firmador.modelo.InformacionDocumento#80]
        at org.hibernate.impl.SessionFactoryImpl$1.handleEntityNotFound(SessionFactoryImpl.java:377)
        at org.hibernate.proxy.AbstractLazyInitializer.checkTargetState(AbstractLazyInitializer.java:79)
        at org.hibernate.proxy.AbstractLazyInitializer.initialize(AbstractLazyInitializer.java:68)
        at org.hibernate.proxy.AbstractLazyInitializer.getImplementation(AbstractLazyInitializer.java:111)
        at org.hibernate.proxy.pojo.cglib.CGLIBLazyInitializer.invoke(CGLIBLazyInitializer.java:150)
        at firmador.modelo.InformacionDocumento$$EnhancerByCGLIB$$cae8968d.setNotificado(<generated>)
        at firmador.dao.DaoInformacionDocumento.actualizarNotificado(DaoInformacionDocumento.java:131)
        at Utils.test.main(test.java:33)
```

Figura 68. Prueba 9

- Prueba 10

```
     * @param args the command line arguments
     */
    public static void main(String[] args) {
        try {
            Valores.init();

            InformacionDocumento info = new InformacionDocumento();
            DaoInformacionDocumento dainfo = new DaoInformacionDocumento();
          boolean aux = dainfo.actualizarNotificado(15,"1");
            System.out.println(aux);
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
test
lida - servidor_firmaPDF (run) ×
ago 19, 2015 10:29:14 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:29:14 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:29:14 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:29:14 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:29:14 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
true
BUILD SUCCESSFUL (total time: 3 seconds)
```

Figura 69. Prueba 10

- Prueba 11

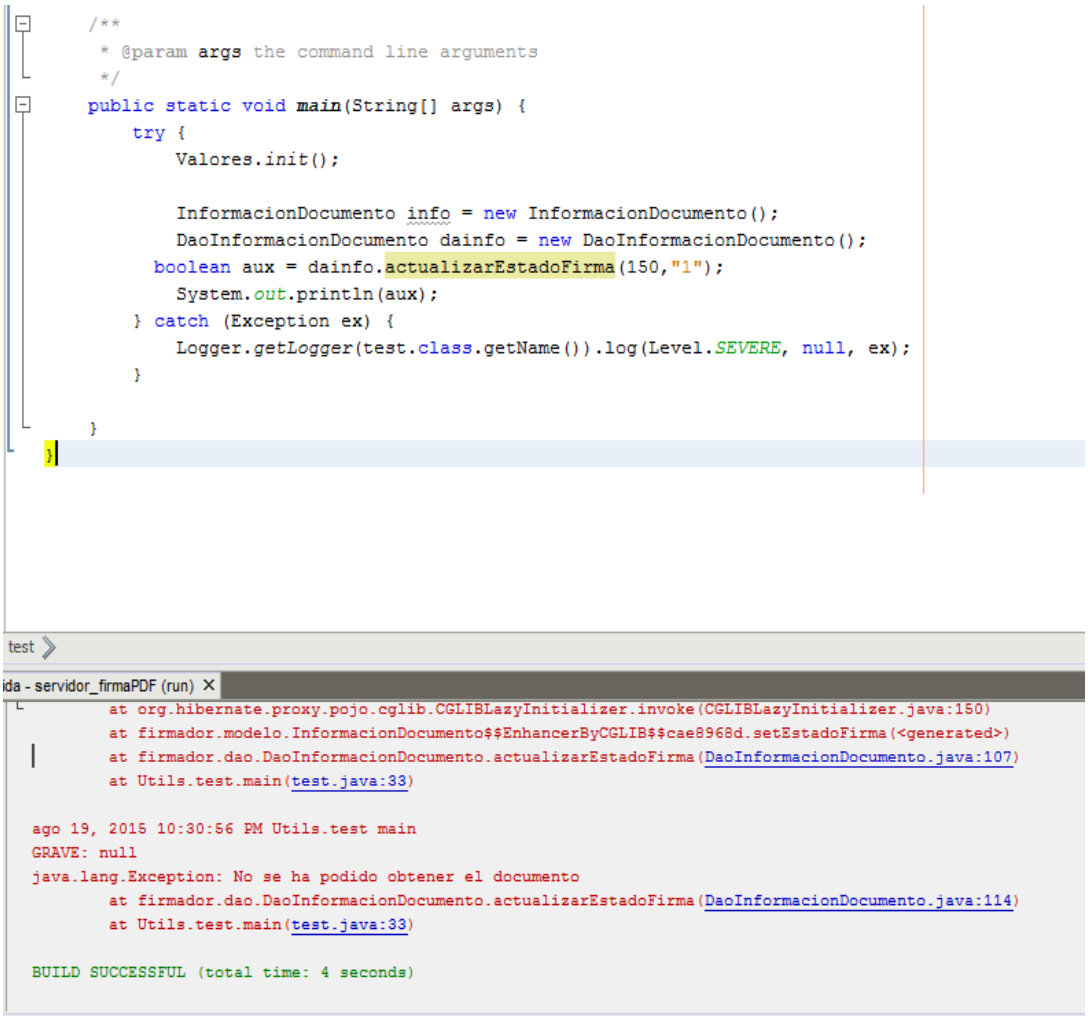


Figura 70. Prueba 11

- Prueba 12

```
/**
 * @param args the command line arguments
 */
public static void main(String[] args) {
    try {
        Valores.init();

        InformacionDocumento info = new InformacionDocumento();
        DaoInformacionDocumento dainfo = new DaoInformacionDocumento();
      boolean aux = dainfo.actualizarEstadoFirma(15,"1");
        System.out.println(aux);
    } catch (Exception ex) {
        Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
    }

}
}
```

```
test
da - servidor_firmaPDF (run)
ago 19, 2015 10:31:24 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:31:24 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:31:24 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:31:24 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:31:24 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
true
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 71. Prueba 12

- Prueba 13

```
    public static void main(String[] args) {
        try {
            Valores.init();
            byte[] documento= null;
            Documento doc = new Documento();
            DaoDocumento daDoc = new DaoDocumento();
          boolean aux = daDoc.actualizarDoc(1,documento);
            System.out.println(aux);
        } catch (Exception ex) {
            Logger.getLogger(test.class.getName()).log(Level.SEVERE, null, ex);
        }

    }
}
```

```
est > main > try >
a - servidor_firmaPDF (run) ×
ago 19, 2015 10:35:21 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Deleted entity synthetic identifier rollback: disabled
ago 19, 2015 10:35:21 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Default entity-mode: pojo
ago 19, 2015 10:35:21 PM org.hibernate.cfg.SettingsFactory buildSettings
INFORMACIÓN: Named query checking : enabled
ago 19, 2015 10:35:21 PM org.hibernate.impl.SessionFactoryImpl <init>
INFORMACIÓN: building session factory
ago 19, 2015 10:35:21 PM org.hibernate.impl.SessionFactoryObjectFactory addInstance
INFORMACIÓN: Not binding factory to JNDI, no JNDI name configured
true
BUILD SUCCESSFUL (total time: 4 seconds)
```

Figura 72. Prueba 13

- Prueba 14

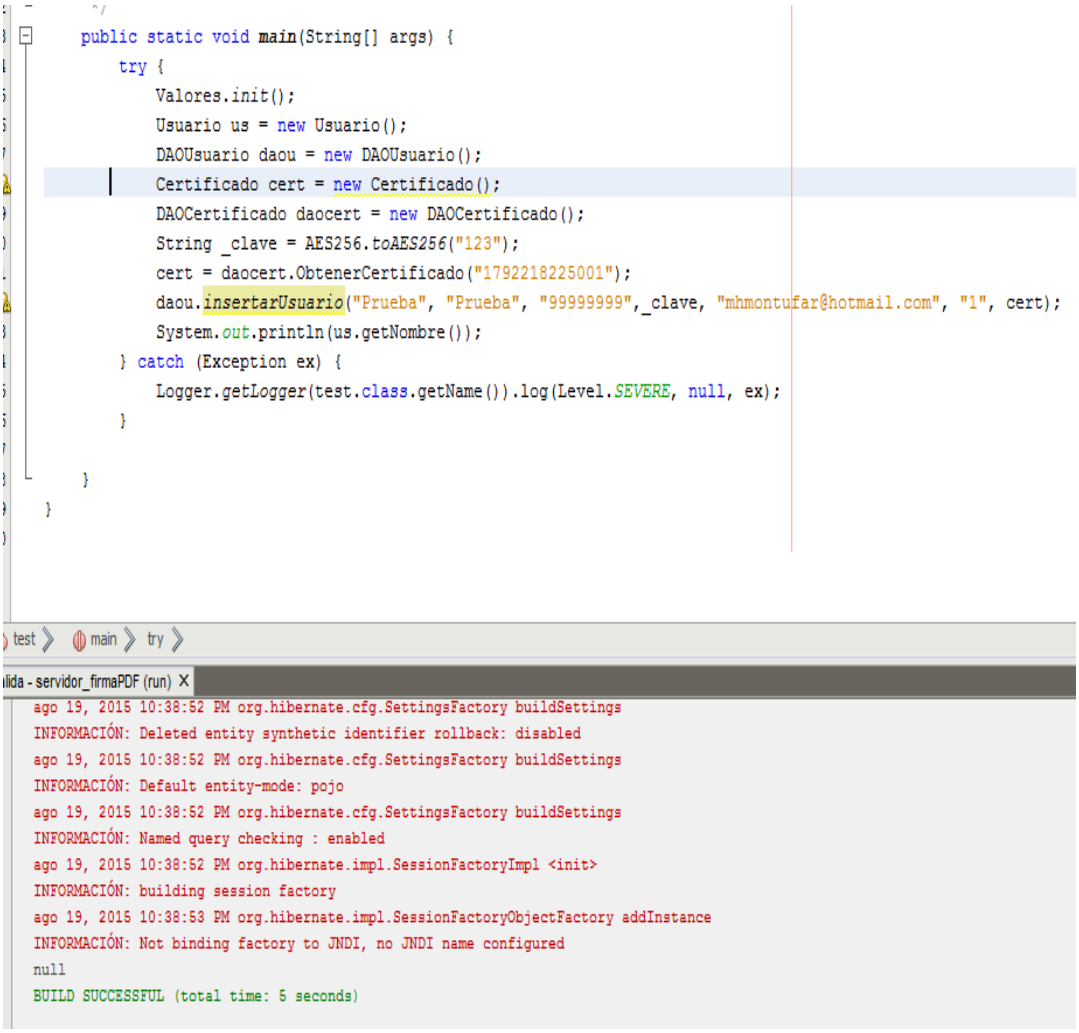


Figura 73. Prueba 14

- Prueba 15

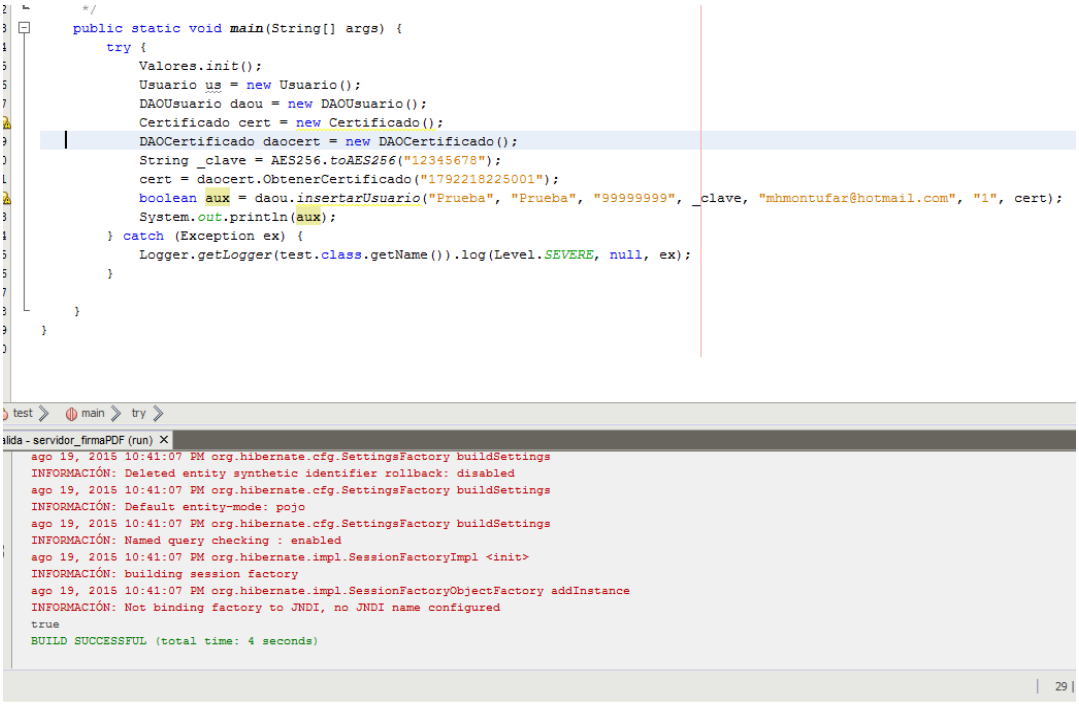


Figura 74. Prueba 15

Resultado

Tabla 20

Prueba

Número de Prueba	Nombre de Método	Resultado
1	obtenerCertificado();	NULL
2	obtenerCertificado();	NUL
3	obtenerCertificado();	NULL
4	obtenerListaUsuario();	OK
5	obtenerMailUsuario();	NULL
6	obtenerMailUsuario();	OK
7	obtenerDocumento();	NULL
8	obtenerDocumento();	OK
9	actualizarNotificado();	NULL
10	actualizarNotificado();	OK
11	actualizarEstadoFirma();	NULL
12	actualizarEstadoFirma();	OK
13	actualizarDocumento();	OK
14	insertarUsuario();	NULL
15	insertarUsuario();	OK

4.2.2. Pruebas de Integración

Estas pruebas se lo realizan en equipo el cual consiste en la comprobación de la integración de los elementos que interactúan y están acoplados entre sí, para saber si funcionan de manera correcta.

- Prueba de Creación de acta de reunión
  - Prueba1

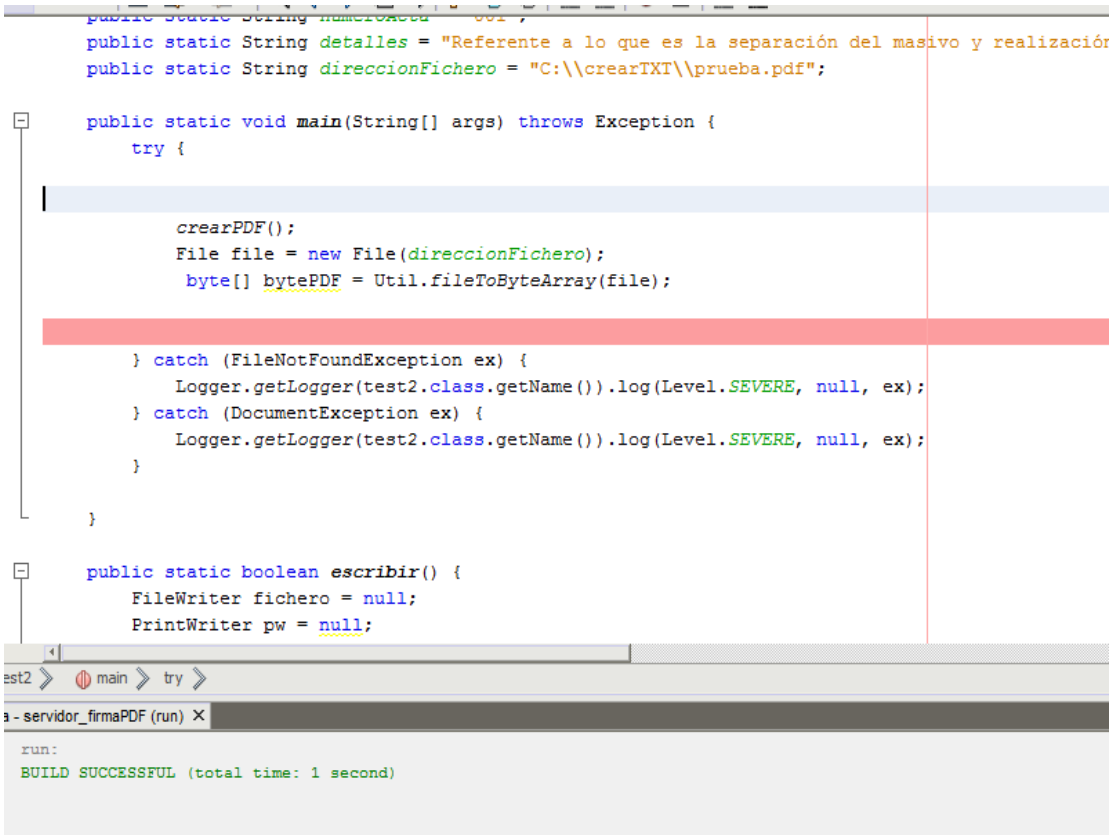
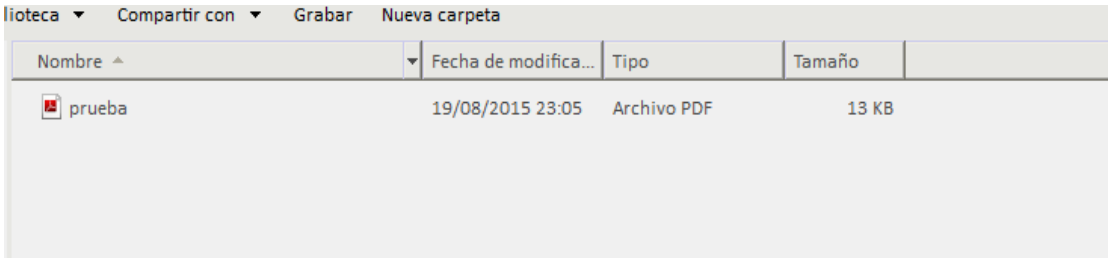


Figura 75.Prueba 1



Acta de Reunión 001

Tema:	Revision Proyectos
Asistentes:	Francisco Daza Pedro Velasco
Identificaciones:	1722995071 0940089279
Lugar Reunión:	sala de reunion 1
Fecha Reunión:	2015-12-12
Hora Reunión:	09:00

Detalle: Referente a lo que es la separación del masivo y realización del txt, el proceso como tal se encuentra en un 70% para lo cual se están afinando detalle entre el cliente y Jorge referente a los archivos de origen, posibles pruebas serán

Figura 76. Prueba 1.1

- Prueba2

```
public static String identificacion1 = "1722995071";
public static String identificacion2 = "0940089279";
public static String lugarReunion = "sala de reunion 1";
public static String fechaReunion = "2015-12-12";
public static String horaReunion = "09:00";
public static String numeroActa = "001";
public static String detalles = "Referente a lo que es la separación del masivo y realización del txt
public static String direccionFichero = "";

public static void main(String[] args) throws Exception {
    try {

        crearPDF();
        File file = new File(direccionFichero);
         byte[] bytePDF = Util.fileToByteArray(file);

    } catch (FileNotFoundException ex) {
        Logger.getLogger(test2.class.getName()).log(Level.SEVERE, null, ex);
    } catch (DocumentException ex) {
        Logger.getLogger(test2.class.getName()).log(Level.SEVERE, null, ex);
    }
```

test2 > main > try

da - servidor_firmaPDF (run)

```
run:
java.io.FileNotFoundException:
        at java.io.FileOutputStream.open(Native Method)
        at java.io.FileOutputStream.<init>(FileOutputStream.java:206)
        at java.io.FileOutputStream.<init>(FileOutputStream.java:95)
        at Utils.test2.crearPDF(test2.java:152)
        at Utils.test2.main(test2.java:46)
BUILD SUCCESSFUL (total time: 2 seconds)
```

Figura. 77 Prueba 2

Resultado

Tabla 21

Prueba

Número de prueba	Nombre de Método	Resultado
1	CrearPDF();	OK
2	CrearPDF();	ERROR

4.2.3. Pruebas de Sistema

Este tipo de prueba lo debe realizar una persona ajena al equipo de trabajo, consiste en la ejecución de las actividades en donde se debe verificar la funcionalidad total de un sistema para ver si cumple o no con los requerimientos funcionales y no funcionales del sistema.

Para estas pruebas se utilizará el Servicio Web y un cliente consola Java.

- Prueba1

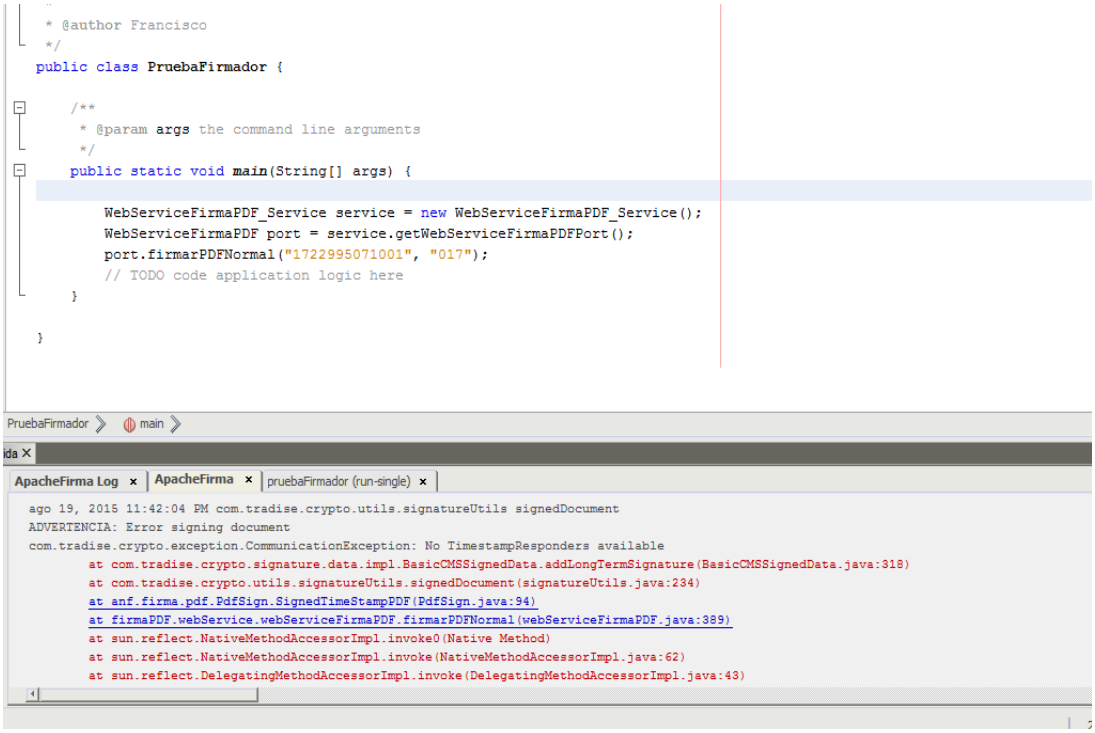


Figura. 78 Prueba 1

- Prueba2

```java
/**
 *
 * @author Francisco
 */
public class PruebaFirmador {

    /**
     * @param args the command line arguments
     */
    public static void main(String[] args) {

        WebServiceFirmaPDF_Service service = new WebServiceFirmaPDF_Service();
        WebServiceFirmaPDF port = service.getWebServiceFirmaPDFPort();
        port.firmarPDFNormal("1722995071001", "017");
        // TODO code application logic here
    }

}
```

PruebaFirmador

Salida

ApacheFirma Log | ApacheFirma | pruebaFirmador (run-single)

```
Updating property file: C:\Users\Francisco\Documents\NetBeansProjects\pruebaFirmador\build\built-jar.properties
wsimport-init:
wsimport-client-webServiceFirmaPDF:
files are up to date
wsimport-client-generate:
Compiling 1 source file to C:\Users\Francisco\Documents\NetBeansProjects\pruebaFirmador\build\classes
compile-single:
run-single:
BUILD SUCCESSFUL (total time: 3 seconds)
```

Figura. 79 Prueba 2

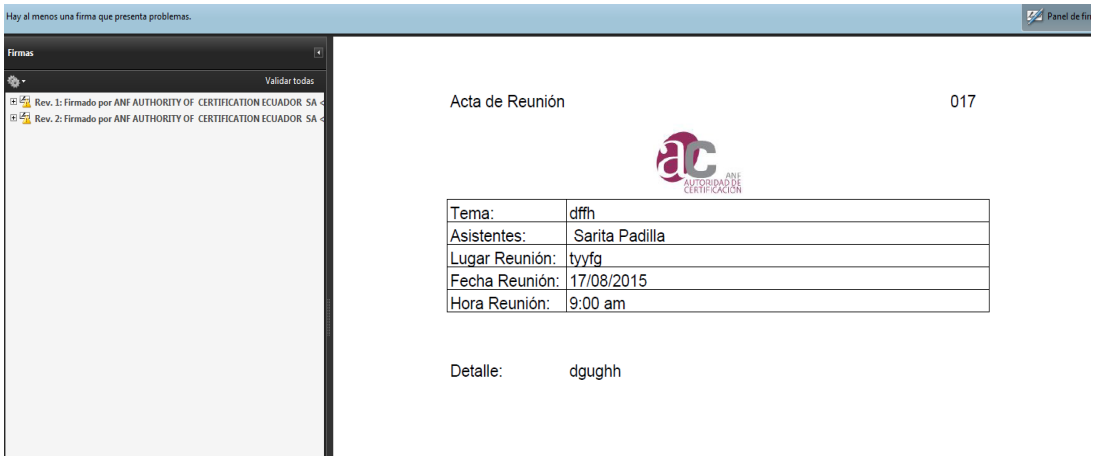


Figura. 80 Prueba 2.1

Resultados

Tabla 22

Prueba

Número de prueba	Nombre de método	Resultado
1	firmarPDFNormal();	Fallida
2	firmarPDFNormal();	OK

4.2.4. Pruebas de Aceptación

- Login Sistema vía Cliente SOAP

  - Prueba1

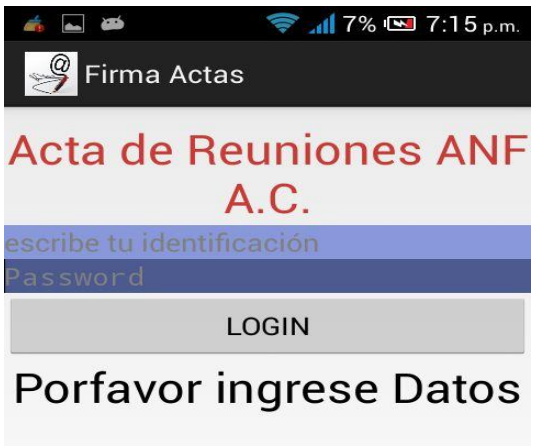


Figura 81. Prueba 1

  - Prueba2

Figura 82. Prueba 2

- Prueba3

Figura 83. Prueba 4

- Prueba 4

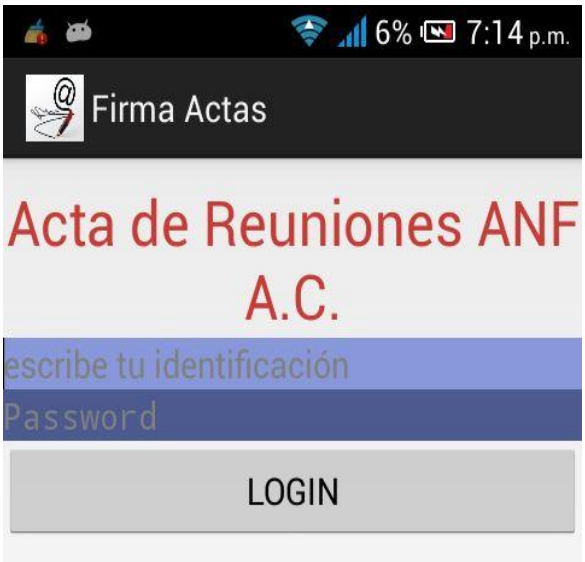


Figura 84. Prueba 4

Figura 85. Prueba 4.1

Resultados

Tabla 23

Prueba

Número de prueba	Nombre de método	Resultado
1	Login Sistema	Fallida
2	Login Sistema	Fallida
3	Login Sistema	Fallida
4	Login Sistema	OK

5. CAPÍTULO 5

RESULTADOS

5.1.Conclusiones

Se concluye que:

- Desarrollar un Cliente SOAP utilizando un web service java para dispositivos móviles Android, basados en certificados digitales de firma electrónica es una solución integral a la gestión y seguridad de la información con el propósito de trasladar los documentos físicos a electrónicos, optimizando el manejo de la información a través del cliente SOAP.

- Demostrar que la firma electrónica basados en la ley de Comercio Electrónico, Firmas y Mensajes de Datos del Ecuador, garantiza la información del documento digital haciendo valido y legal, para que la información viaje por la nube o se traslade de un medio digital a otro.

- Proporcionar una clara explicación que con el avance tecnológico y el comercio digital en la nube, han desarrollado la creación de medios de seguridad uno de ellos es el certificado digital ya que con este se podrá encriptar la información que se está manejando en el internet, la encriptación se realiza por medio de llaves públicas que hacen casi imposible inviolable esta información.

- Crear un modelo de arquitectura cliente SAOP- Web Service para mostrar la importancia del avance de la programación dentro de las comunicaciones en la nube.
- Dar a conocer las relaciones de varias tecnologías de programación, Cliente SOAP móvil Android, Web Service java,

librerías de firma Electrónica y creaciones de archivos pdf, Mysql y programación en consola java, para su fácil utilización.

- Conocer la utilidad de la firma electrónica a nivel de documentos digitales en cualquier empresa, negocio o servicio que se realice en la nube.

5.2.Recomendaciones

` Se recomienda que:

- Adquirir el certificado de firma electrónica de ANF AC para utilizar el cliente SOAP con tecnología móvil Android, caso contrario no podrán realizar ninguna transacción en este sistema.
- Realizar capacitación oportuna sobre la ley de firma electrónica y la utilidad de los certificados digitales, a los posibles usuarios que van a utilizar el Cliente SOAP móvil Android, para que tener un previo conocimiento.
- Tener contenedores seguros (servidores con certificados SSL) para el movimiento de los certificados electrónicos en el repositorio. Estos certificados electrónicos pueden adquirir en la misma empresa auspiciante de este proyecto.
- Consumir un Servicio Web se necesitará el servicio 24/7 colgado en la nube.
- Disponer paquete de datos contratados en su celular o Tablet para el uso y funcionamiento del Cliente SOAP móvil Android.

BIBLIOGRAFÍA

Android, X. (2011). *Xataka Android*. Obtenido de http://www.xatakandroid.com/sistema-operativo/que-es-android

Carrillo, A. (2009). *Metodología RUP.*

Club, S. D. (16 de 01 de 2012). *El club del Programador* . Obtenido de http://www.elclubdelprogramador.com/2012/01/16/soa-introduccion-a-los-servicios-web/

LLC, T. (2015). *Procesos de Software*. Obtenido de http://procesosdesoftware.wikispaces.com/METODOLOGIA+RUP

México, A. d. (s.f.). Obtenido de http://autoridadcertificadora.guerrero.gob.mx/fec/que-es-la-fec.html

México, U. (1 de marzo de 2011). Evolución de la firma autógrafa a la Firma Electrónica Avanzada . *Registra Digital Universitaria* , 9.

Novoa, G. (2002). Ley Comercio Electrónico.

Programación, A. d. (2012). *Apuntes de Programación*. Obtenido de http://programacion.jias.es/2012/01/web-service-definicion-utilizacion-estructura-del-wsdl/

Quiroga, A. (2015). Obtenido de http://proyectogradoingenieriasistemas.blogspot.com/2015/03/metodologia-uwe-uml-uml-based-web.html

Talens, S. (2014). *Certificados Digitales*. Obtenido de http://www.uv.es/~sto/articulos/BEI-2003-11/certificados_digitales.html

Wesley, A. (2011). *Tecnología Android .* Mexico .

Zúñiga. (2011). *Firma Electrónica Avanzada.*

BIOGRAFÍA

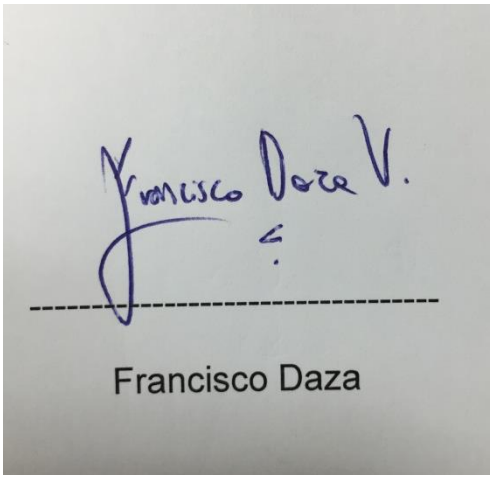
EL SR. Francisco Gabriel Daza Velásquez, nace en la ciudad de Quito, el 13 de Enero del 1989. Cursó sus estudios escolares y colegio hasta el cuarto año en el Instituto Técnico Superior Policía Nacional , en finales del 2004 ingresa a culminar sus estudios en el Colegio Experimental Juan Pio Montufar terminando en el año 2006 y obteniendo el título de Bachiller de Ciencias Especialización Físico Matemáticas.

En el 2007 ingresa en la Carrera de Ingeniería en Sistemas e Informática de la Escuela Politécnica del Ejército y finaliza sus estudios superiores en Diciembre del 2013.

A principios del año 2013 empieza a trabajar brindando sus conocimientos adquiridos de la universidad en la prestigiosa empresa privada ANF AC Ecuador especializada en certificados digitales y firmas electrónicas para desempeñar el trabajo de desarrollador de Software, en donde se ha formado como especialista en firmas electrónicas y líder de proyectos de software.

HOJA DE LEGALIZACIÓN DE FIRMAS

ELABORADA POR:



DIRECTOR DE LA CARRERA

Lugar y Fecha: Sangolquí, Octubre del 2015