CAPÍTULO III

3 MARCO APLICATIVO

3.1 INTRODUCCIÓN

El objetivo del presente capitulo es formalizar el desarrollo del software denominado "Sistema de firma digital para el Ministerio de Obras Públicas, Servicios y Vivienda", haciendo uso de la metodología XP y otras herramientas descritos anteriormente, que nos ayudaran a desarrollar el sistema y todos sus módulos.

En la Tabla 3.1 se establece los artefactos que se utilizaran en cada fase de la metodología de desarrollo XP, estos artefactos se desarrollaran para cada una de las seis iteraciones planteadas en la fase planificación.

Fase		**Artefactos**
Planificación		• Historias de usuarios • Plan de entregas • Iteraciones
Iteración	Diseño	• Tarjetas CRC
	Codificación	• Cliente siempre presente
	Pruebas	• Pruebas unitarias • Pruebas de aceptación

Tabla 3.1 *Fases y artefactos a desarrollar*

Fuente*: Elaboración propia*

3.2 PLANIFICACIÓN

En esta fase se mostrara el modo de trabajo actual mediante los requisitos de software obtenidos de las historias de usuario que a su vez se obtuvieron de las reuniones realizadas con los clientes, además se definirán todas la tareas que serán necesarias para poder desarrollar el software mediante las tarjetas de tarea y por ultimo se realizara un plan de entregas que contendrá las iteraciones a realizar para el desarrollo del presente proyecto.

3.2.1 Historias de usuario

De los requisitos obtenidos del ministerio se formulan las siguientes historias de usuario para el desarrollo del sistema de la firma digital.

Historias de Usuario	
Numero: 1	**Nombre:** Usar la firma digital de un

	servidor público almacenada en un token para firmar documentos en formato PDF.
Autor: Armin Mesa Sanchez	
Prioridad: Alta	
Descripción: Se desarrollara el Módulo para usar la firma digital de un servidor público almacenada en un token o fichero de almacenamiento de par de claves para firmar documentos en formato PDF.	

Tabla 3.2 *Historia de Usuario 1*

Fuente*: Elaboración propia*

El firmado digital de un documento en formato pdf debe ser realizado desde un token, el cual contiene un certificado otorgado por una CE, este certificado contiene la información del servidor público y su par de claves, el acceso a la clave privada sera mediante una contraseña o pin que el usuario ingresará.

La historia de usuario 1 contara con tareas para crear el módulo, la interfaz para escoger tipo de firmado y el acceso al token.

Tarea	
Numero de Tarea: 1.1	**Numero de Historia:** 1
Nombre de tarea: Desarrollo de módulo para acceso al tipo de firma digital.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo en especifico para poder acceder al token o smartcard y un módulo para acceder a un fichero de claves con extensión pxf o p12.	

Tabla 3.3 *Tarjeta de Tarea 1.1 de Historia de Usuario 1*

Fuente*: Elaboración propia*

En la tarjeta de tarea 1.1 (Tabla 3.3 Tarjeta de Tarea 1.1 de Historia de Usuario 1) se desarrolla el módulo para el acceso al dispositivo criptográfico que puede ser un token o smartcard, en este modulo se usará la librería de java **sunpkcs11** que sigue las especificaciones técnicas del estándar PKCS11 que especifica el acceso a un dispositivo criptográfico. De la misma forma se desarrolla una sección para acceder a un fichero de

almacenamiento de clave pública y privada del estándar PKCS12.

Tarea	
Numero de Tarea: 1.2	**Numero de Historia:** 1
Nombre de tarea: Diseño de interfaz para acceso al tipo de firma digital.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo en especifico para poder cargar el fichero de almacenamiento de claves.	

Tabla 3.4 *Tarjeta de Tarea 1.2 de Historia de usuario 1*

Fuente*: Elaboración propia*

En la Tarjeta de Tarea 1.2 de Historia de usuario 1 se elabora una interfaz amigable en la cual el funcionario público pueda escoger el tipo de firma digital quiera usar, en el caso del estándar PKCS11 el funcionario público contara con una casilla donde ingresar su pin. En el caso del estándar PKCS12 el funcionario contara con las casillas para escoger la ubicación del fichero de almacenamiento de claves y la contraseña del acceso al fichero.

Tarea	
Numero de Tarea: 1.3	**Numero de Historia:** 1
Nombre de tarea: Módulo para cargar el Alias del certificado para firma digital.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo para obtener el Alias del usuario del certificado contenido en un fichero de claves o un token.	

Tabla 3.5: *Tarjeta de Tarea 1.3 de Historia de Usuario 1*

Fuente: *Elaboración propia*

En la Tarjeta de Tarea 1.3 de Historia de Usuario 1 se desarrolla el módulo para poder obtener el alias del certificado de un fichero de claves o un token, esto debido a que en un token y fichero pueden estar incluidos varios certificados digitales para un mismo funcionario, de esta forma el usuario podrá elegir con que certificado firmar.

Historias de Usuario	
Numero: 2	**Nombre:** Firmar documento en formato PDF
Autor: Armin Mesa Sanchez	
Prioridad: Alta	
Descripción: Se desarrollara el Módulo para usar el certificado de un servidor público almacenado en un token o fichero de claves para firmar documentos en formato PDF.	

Tabla 3.6 *Historia de Usuario 2*

Fuente*: Elaboración propia*

Esta historia de usuario es la más importante de todo el proyecto, ya que permitirá realizar la función principal que es la de firmar digitalmente un documento, el firmado sera de tipo avanzado, lo que quiere decir que a la firma del documento se le incluirán algunas características adicionales como: un sello de tiempo de un TSA; campos extras para añadir la razón de la firma, lugar y contacto; nivel de certificación; resumen del contenido del pdf (Hash); validación y verificación de certificado; y marca de agua del signatario.

A continuación se describen las tarjetas de tarea:

Tarea	
Numero de Tarea: 2.1	**Numero de Historia:** 2
Nombre de tarea: Módulo para cargar documento pdf	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo para cargar los documentos al sistema en formato pdf para ser firmados.	

Tabla 3.7 *Tarjeta de Tarea 2.1 de Historia de usuario 2*

Fuente: *Elaboración propia*

La Tarjeta de Tarea 2.1 de Historia de usuario 2 permite cargar el o los documentos en formato pdf para ser firmados, validando que el documento sea pdf.

Tarea	
Numero de Tarea: 2.2	**Numero de Historia:** 2
Nombre de tarea: Módulo para adicionar opciones extras a la firma digital y nivel de certificación.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo para adicionar opciones extras como ser la razón de la firma, lugar o ubicación y contacto o email a la firma digital; ademas de adicionar el nivel de certificación de la firma digital.	

Tabla 3.8 *Tarjeta de Tarea 2.2 de Historia de Usuario 2*

Fuente: *Elaboración propia*

La Tarjeta de Tarea 2.2 de Historia de Usuario 2 permite adicionar a la firma los siguientes aspectos como ser: razón, lugar y contacto. Un aspecto importante de esta tarea es el nivel de certificación que se le dará a los documentos firmados, los niveles de certificación serán:

- Crear una firma ordinaria o sin certificación, el documento puede ser firmado a la aprobación de uno o mas destinatarios.
- No permitir cambios en el pdf, una vez aplicada la firma el documento no podrá ser sometido a cambios.
- Permitir completar formularios, otros usuarios pueden rellenar campos o añadir su firma de aprobación sin invalidar la firma actual.
- Permitir completar formularios y notas, es similar al anterior con la diferencia que en este caso se pueden añadir notas sin invalidar la firma actual.

Tarea	
Numero de Tarea: 2.3	**Numero de Historia:** 2
Nombre de tarea: Módulo para crear un hash de documento firmado.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo para crear el resumen hash del documento pdf	

firmado.

Tabla 3.9 *Tarjeta de Tarea 2.3 de Historia de Usuario 2*

Fuente: *Elaboración propia*

La Tarjeta de Tarea 2.3 de Historia de Usuario 2 permite crear un hash del documento pdf para evitar ediciones o falsificaciones del documento, en este caso tomaremos los tipos de hasheo SHA-1 y SHA-2 que son los adecuados para trabajar los formatos de pdf 1.3, 1.4, 1.5 y 1.6.

Tarea	
Numero de Tarea: 2.4	**Numero de Historia:** 2
Nombre de tarea: Módulo para firmar un documento pdf.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un modulo siguiendo el estándar PKCS7 para firmar un documento pdf.	

Tabla 3.10 *Tarjeta de de Tarea 2.4 de Tarjeta de Usuario*

Fuente: *Elaboración propia*

La Tarjeta de de Tarea 2.4 de Tarjeta de Usuario es la tarea mas importante ya que es aquí donde se desarrolla el módulo para el proceso de firmado digital, siguiendo el estándar PKCS7.

Tarea	
Numero de Tarea: 2.5	**Numero de Historia:** 2
Nombre de tarea: Diseño de interfaz para cargar el documento pdf, adicionar extras a la firma, agregar nivel de certificación y crear hash de documento firmado.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla una interfaz para adicionar el lugar, razón y contacto a la firma digital. El nivel de certificación del documento firmado y el hash del documento para que	

no pueda ser vulnerado o modificado.

Tabla 3.11 *Tarjeta de Tarea 2.5 de Historia de Usuario 2*

Fuente: *Elaboración propia*

La Tarjeta de Tarea 2.5 de Historia de Usuario 2 permite crear una interfaz fácil para el usuario para llenar las opciones extras al documento, como también escoger el tipo de hash que se aplicara al documento y escoger el nivel de certificación.

Historias de Usuario	
Numero: 3	**Nombre:** Verificación de certificado digital en documentos firmados.
Autor: Armin Mesa Sanchez	
Prioridad: Alta	
Descripción: Se desarrollara un módulo para validar y verificar la firma de un funcionario publico, esta consulta se la hará a la Entidad Certificadora, el cual contendrá un CRL o un servidor OCSP.	

Tabla 3.12 *Historia de Usuario 3*

Fuente: *Elaboración propia*

La Historia de Usuario 3 es el módulo en el cual se harán las consultas respectivas a los servidores del la entidad certificadora (CE) para verificar la validez del certificado, y la vigencia de la misma.

A continuación se describen las Tarjetas de Tarea correspondientes a esta historia de usuario 3:

Tarea	
Numero de Tarea: 3.1	**Numero de Historia:** 3
Nombre de tarea: Desarrollo de módulo para realizar las consultas al servidor OCSP y obtener información de un CRL.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla un módulo para verificar la vigencia y validez de un	

certificado emitido por una entidad certificadora, misma que dispondrá de un servidor OCSP y un archivo CRL para realizará las consultas mecionadas.

Tabla 3.13 *Tarjeta de Tarea 3.1 de Historia de Usuario 3*

Fuente: *Elaboración propia*

La Tarjeta de Tarea 3.1 de Historia de Usuario 3 es el módulo que permitirá realizar la verificación del certificado del funcionario público, las consultas se realizaran con el ID del funcionario tanto al servidor OCSP como al CRL.

Tarea	
Numero de Tarea: 3.2	**Numero de Historia:** 3
Nombre de tarea: Desarrollo de interfaz para realizar las consultas al servidor OCSP y obtener información de un CRL.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla una interfaz para verificar la vigencia y validez de un certificado emitido por una entidad certificadora, el usuario ingresara la url del servidor OCSP.	

Tabla 3.14 *Tarjeta de Tarea 3.2 de Historia de Usuario 3*

Fuente*: Elaboración propia*

La Tarjeta de Tarea 3.2 de Historia de Usuario 3 sera una interfaz simple para el usuario, en la que el usuario ingresara la URL del servidor OSCP para realizar las consultas, también se contara con la opción de usar el archivo CRL de la entidad certificadora.

Historias de Usuario	
Numero: 4	**Nombre:** Visualización de documento pdf.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se desarrollara un módulo para poder visualizar un documento pdf.	

Tabla 3.15 *Historia de Usuario 4*

Fuente*: Elaboración propia*

Esta historia de usuario permite visualizar el documento pdf para verificar si es el documento correcto que se desea firmar digitalmente.

A continuación se describe la Tarjeta de Tarea correspondiente:

Tarea	
Numero de Tarea: 4.1	**Numero de Historia:** 4
Nombre de tarea: Desarrollo de interfaz para realizar la visualización de documento pdf a ser firmado.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Se desarrolla una interfaz para visualizar el documento pdf que sera firmado.	

Tabla 3.16 *Tarjeta de Tarea 4.1 de Historia de Usuario*

Fuente*: Elaboración propia*

En la Tarjeta de Tarea 4.1 de Historia de Usuario se desarrolla la visualización del documento pdf a ser firmado pero sin realizar modificaciones al documento original.

Historias de Usuario	
Numero: 5	**Nombre:** Incluir marca de agua con la información de certificado digital del funcionario público.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se desarrolla un módulo para poder añadir una marca de agua a un documento pdf firmado con la información del certificado digital perteneciente al servidor público.	

Tabla 3.17 *Historia de Usuario 5*

Fuente*: Elaboración propia*

En esta historia de usuario se crea un módulo para añadir una marca de agua con la información del usuario extraída del certificado digital del mismo, el usuario podrá

seleccionar la página donde desea añadir la marca de agua, así mismo podrá dibujar un rectángulo para el tamaño de la marca de agua y la ubicación en la hoja.

A continuación se describe las Tarjetas de Tarea correspondientes:

Tarea	
Numero de Tarea: 5.1	**Numero de Historia:** 5
Nombre de tarea: Desarrollo de interfaz para realizar el dibujo de un área rectangular para la marca de agua en un documento pdf.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realiza el módulo para dibujar un cuadrado o rectángulo en una pagina del documento pdf para poder añadir una marca de agua en dicha área.	

Tabla 3.18 *Tarjeta de Tarea 5.1 de Historia de Usuario 5*

Fuente*: Elaboración propia*

La Tarjeta de tarea 5.1 (Tabla 3.18) trabajara conjuntamente con la tarjeta de tarea 4.1 (Tabla 3.16), ya que con el visualizador de pdf podremos avanzar a la página correspondiente donde el usuario desea añadir la marca de agua. En la página elegida el usuario dibujara un rectángulo para definir el tamaño de la marca de agua. Esta marca de agua contendrá: una Figura QR (URL de acceso a servidor ftp de documento firmado respaldado), información del signatario, información extra (razón, lugar y email) y fecha de firmado obtenida de un servidor TSA o PC.

Historias de Usuario	
Numero: 6	**Nombre:** Incluir sello de tiempo de la entidad certificadora para los documentos firmados en formato PDF.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se Desarrolla un módulo para adquirir el sello de tiempo de un servidor TSA para firmar un documento pdf. De esta forma se garantiza el no repudio del documento firmado.	

Tabla 3.19 *Historia de Usuario 6*

Fuente*: Elaboración propia*

La Historia de Usuario 6 es un módulo en el que se realiza las consultas al servidor TSA para adquirir la fecha y hora exacta en la que se esta realizando la firma, este dato es añadido al documento pdf.

A continuación se describe las Tarjetas de Tarea correspondientes:

Tarea	
Numero de Tarea: 6.1	**Numero de Historia:** 6
Nombre de tarea: Desarrollo de modulo para consulta a servidor TSA	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Desarrollar un módulo para realizar las consultas a servidor TSA, con las opciones de autenticación, políticas de OID y algoritmo hash que usa el servidor.	

Tabla 3.20 *Tarjeta de Tarea 6.1 de Historia de Usuario 6*

Fuente*: Elaboración propia*

En la Tarea 6.1 (Tabla 3.20) se desarrolla el módulo para consultar al TSA de la entidad certificadora para poder adquirir la información de hora y fecha, en esta consulta se escoge la opción de hash (SHA-1 y SHA-2) del documento pdf con al que trabajara el servidor TSA. La respuesta obtenida del servidor es añadida a la firma del documento pdf y es visible desde la marca de agua.

Tarea	
Numero de Tarea: 6.2	**Numero de Historia:** 6
Nombre de tarea: Desarrollo de interfaz para consulta a servidor TSA	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de la interfaz para consultar al servidor TSA, añadiendo la URL del servidor; el usuario tendrá la opción de elegir el tipo de autenticación y elegir el tipo de hash del documento que desea usar.	

Tabla 3.21 *Tarjeta de Tarea 6.2 de Historia de Usuario 6*

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.21) se desarrolla la interfaz para añadir la URL del servidor TSA, escoger el tipo de autenticación que puede ser del tipo:

- Ninguno, no es necesario añadir algún dato excepto la URL del servidor.
- Usuario y contraseña, es necesario un usuario y contraseña para realizar la consulta.
- Certificado, el usuario tiene un certificado en el servidor TSA que puede usar para adquirir el sello de tiempo.

Ademas de estas opciones el usuario podrá añadir su OID (opcional) para realizar las consultas y añadir el tipo de hash que quiere usar para su documento pdf.

Historias de Usuario	
Numero: 7	**Nombre:** Validación y verificación de firmas digitales en documentos firmados con formato PDF.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se Desarrolla un módulo para obtener la información de un documento pdf firmado, como ser: sello de tiempo, información del signatario, nivel de certificación, hash de documento y número de revisiones o firmas del documento.	

Tabla 3.22 *Historia de Usuario 7*

Fuente*: Elaboración propia*

En esta historia de usuario (Tabla 3.22) se desarrolla el módulo para obtener información de un documento pdf firmado que sera procesada para ser mostrada al usuario de forma comprensible.

A continuación se describe las Tarjetas de Tarea correspondientes:

Tarea	
Numero de Tarea: 7.1	**Numero de Historia:** 7
Nombre de tarea: Desarrollo de módulo para obtener información de pdf firmado.	

Tipo de tarea: Desarrollo
Programador(a) Responsable: Armin Mesa Sanchez
Descripción: Realizar el desarrollo de un módulo para obtener la información necesaria como ser: nombre del firmante, número de serie del signatario, sello de tiempo, vigencia de certificado digital, verificación de servidor OCSP y modificaciones hechas al documento.

Tabla 3.23 *Tarjeta de Tarea 7.1 para Historia de Usuario 7*

Fuente*: Elaboración propia*

En esta tarea (Tabla 3.23) se realizara lo inverso de todo lo realizado hasta ahora, se podrá obtener la información del signatario, fecha en que se realizo la firma (información TSA), verificación de validación y vigencia de certificado (información servidor OCSP).

Tarea	
Numero de Tarea: 7.2	**Numero de Historia:** 7
Nombre de tarea: Desarrollo de interfaz para desplegar información de pdf firmado.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de la interfaz para deplegar la información de un pdf firmado.	

Tabla 3.24 *Tarjeta de Tarea 7.2 de Historia de Usuario 7*

Fuente*: Elaboración propia*

En esta tarea (Tabla 3.24) mostraremos la información del signatario y algunos aspectos importantes del documento pdf, como ser: número de serie del signatario, nombre del o los signatarios, sello de tiempo, validación de servidor OCSP, modificaciones realizadas al documento, fechas de vigencia de certificado digital y nombre de emisor de certificado digital,

Historias de Usuario	
Numero: 8	**Nombre:** Almacenamiento de documentos firmados realizadas por los signatarios y generación QR con URL de acceso al

	documento pdf firmado.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se Desarrolla un módulo para almacenar los documentos firmados por los signatarios, los documentos firmados incluirán un código QR que contendrá una URL con la ubicación del documento respaldado en un servidor FTP, este servidor contara con un usuario y contraseña para autenticar a los signatarios y solo se realizaran los respaldos de documentos con firmas digitales.	

Tabla 3.25 *Historia de Usuario 8*

Fuente*: Elaboración propia*

Esta historia de usuario (Tabla 3.25) se desarrolla para los casos en los que el documento tenga que ser impreso y se requiera verificar la firma digital de la misma, por otra parte se respaldará el documento firmado que podrá ser visto desde en un servidor FTP.

A continuación se describen las correspondientes Tarjetas de Tarea:

Tarea	
Numero de Tarea: 8.1	**Numero de Historia:** 8
Nombre de tarea: Desarrollo de modulo de autenticación de signatario.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de un módulo en el cual se introduce un usuario y contraseña para poder respaldar el o los documentos firmados.	

Tabla 3.26 *Tarjeta de Tarea 8.1 de Historia de Usuario 8*

Fuente*: Elaboración propia*

En esta tarea (Tabla 3.26) se desarrolla un módulo para que el usuario pueda añadir un usuario y contraseña para autenticarse en el servidor ftp, de esta forma almacenar los documentos firmados, por consiguiente almacenar el historial de documentos firmados.

Tarea	
Numero de Tarea: 8.2	**Numero de Historia:**

Nombre de tarea: Desarrollo de sistema web para almacenamiento de documentos firmados.
Tipo de tarea: Desarrollo
Programador(a) Responsable: Armin Mesa Sanchez
Descripción: Desarrollar un sistema web para desplegar la información del signatario y que este sistema este integrado con un servidor FTP para obtener la información de los documentos firmados.

Tabla 3.27 *Tarjeta de tarea 8.2 de Historia de Usuario 8*

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.27) se desarrolla un pequeño sistema web para desplegar la información de los signatarios y realizar los reportes necesarios como ser: número de documentos firmados y lista de signatarios.

Tarea	
Numero de Tarea: 8.3	**Numero de Historia:**
Nombre de tarea: Desarrollo de interfaz para introducir usuario y contraseña.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de la interfaz para que el signatario ingrese un usuario y contraseña para realizar un respaldo de su documento firmado.	

Tabla 3.28 *Tarjeta de Tarea 8.3 de Historia de Usuario 8*

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.28) se realizara una interfaz simple en la que el signatario ingresara el nombre de usuario y su contraseña con el cual se conectara al servidor FTP, para poder respaldar el documento firmado.

Tarea	
Numero de Tarea: 8.4	**Numero de Historia:**
Nombre de tarea: Desarrollo de sistema web para realizar los reportes de numero de documentos firmados y lista de signatarios.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de una pequeño sistema web integrado con el servidor FTP para realizar las consultas de autenticación, generar reporte de número de documentos firmados y número de signatarios.	

Tabla 3.29 *Tarea 8.4 de Historia de Usuario 8*

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.29) se desarrolla un pequeño sistema necesario para desplegar la información del signatario e integración con un servidor FTP.

Tarea	
Numero de Tarea: 8.5	**Numero de Historia:**
Nombre de tarea: Desarrollo de módulo para generar un QR en documento firmado con una URL de acceso a dicho documento.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo para generar un código QR en el documento firmado, mismo que contendrá la URL para el acceso vía web al documento.	

Tabla 3.30 *Tarea 8.5 de Historia de Usuario 8*

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.30) se desarrollara un módulo para generar el código QR con la URL del documento para que pueda ser visualizado desde cualquier navegador para realizar las verificaciones correspondientes. Este código sera visible en la marca de agua del documento firmado.

3.2.2 Plan de entregas

Una característica muy útil de la metodología de desarrollo XP es la programación incremental, estas iteraciones consisten en un ciclo completo de trabajo en las que se va definiendo las historias de usuario que van a ser atendidas en dicho ciclo, en este sentido se planifica la distribución de tiempo para cada modulo que se desarrollara.

Cada una de las iteraciones responden a una cantidad de requisitos definidos para el desarrollo de los módulos, estos son los artefactos de la metodología XP, usando también el lenguaje de modelado UML para el diseño de diagramas de clases. En la Tabla 3.31 Plan de entregas se detalla la planificación de las seis iteraciones a desarrollar.

Iteraciones	**Historias de usuario**	**Duración**	**Fecha inicio**
Primera	1. Usar la firma digital de un servidor público almacenada en un token para firmar documentos en formato PDF.	2 Semanas	17/08/2015
Segunda	2. Firmar documentos en formato PDF.	2 Semanas	31/08/2015
Tercera	3. Validación y comprobación de estado del certificado otorgado por la entidad certificadora para tener una constancia del estado del certificado.	2 Semanas	14/09/2015
Cuarta	4. Visualizar un documento en formato PDF. 5. Incluir la marca de agua con la información del servidor publico.	2 Semanas	28/09/2015
Quinta	6. Incluir sello de tiempo de la entidad certificadora para los documentos firmados en formato PDF.	2 semanas	12/10/2015
Sexta	7. Verificación de firmas digitales en documentos firmados, con formato PDF.	2 Semanas	26/10/2015

	8. Almacenamiento de documentos firmados realizadas por los signatarios y generación QR con URL de acceso al documento pdf firmado.		

Tabla 3.31 *Plan de entregas*

Fuente*: Elaboración propia*

A continuación se presentan las seis iteraciones realizadas en el proyecto.

3.3 PRIMERA ITERACIÓN

En esta iteración se contempla la realización del primer prototipo del sistema, resolviendo las siguiente historia de usuario:

1. Usar la firma digital de un servidor público almacenada en un token para firmar documentos en formato PDF.

Para esta historia de usuario se resolverán las tres tareas (Tabla 3.3, 3.4 y 3.5) asignadas a la misma.

3.3.1 Diseño

En esta fase el diseño nos sirve para visualizar, especificar, construir y documentar los aspectos estáticos del sistema en la primera iteración y en las siguientes iteraciones, haremos uso de las tarjetas de usuario para crear las clases y las representaremos en diagramas estructurales, que en este caso serán los diagramas de clases.

3.3.1.1 Tarjetas CRC

El sistema en desarrollo esta orientado a objetos, por lo cual, las tarjetas CRC nos facilitaran la implementación de las clases definidas en esta sección.

A continuación se describen las tarjetas CRC con sus respectivas responsabilidades y colaboraciones correspondientes a la historia de usuario 1:

La tarjeta CRC de la clase PKCS11 (Tabla 3.32).

PKCS11	
Responsabilidad	**Colaboración**
• Usar librería SunPKCS11 para el	• Ninguna

acceso a token o smartcard. • Registrar acceso a token o smartcard. • Eliminar acceso a token o smartcard.	

Tabla 3.32 *Tarjeta CRC de la clase PKCS11*

Fuente: *Elaboración propia*

La tarjeta CRC de la clase keyStoreU (Tabla 3.33).

keyStoreU	
Responsabilidad	**Colaboración**
• Acceso a almacén de claves. • Obtención de alias de almacén de claves. • Validación de certificado. • Obtención de certificación de alias. • Cargar almacén de claves.	• OpcionesFirma • Constantes • InfoClaveP • PKCS11

Tabla 3.33 *Tarjeta CRC de la clase keyStoreU*

Fuente: *Elaboración propia*

La tarjeta CRC de la clase PropiedadesFirmaF (Tabla 3.34).

PropiedadesArchivoF	
Responsabilidad	**Colaboración**
• Almacenamiento de propiedades temporales de firma digital. • Creación de archivo para almacenamiento de propiedades de firma.	• ConfigurarPro

Tabla 3.34 *Tarjeta CRC de clase PropiedadesArchivoF*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase TipoAlmacenCLaves (Tabla 3.35).

TipoAlmacenClaves	
Responsabilidad	**Colaboración**
• Cargar tipo de almacén de claves	• Niguna

Tabla 3.35 *Tarjeta CRC de clase TipoAlmacenClaves*

***Fuente**: Elaboración propia*

La tarjeta CRC de la clase InfoClaveP (Tabla 3.36).

InfoClaveP	
Responsabilidad	**Colaboración**
• Acceso a la información de clave publica.	• Ninguna

***Tabla 3.36** Tarjeta CRC de clase InfoClaveP*

***Fuente**: Elaboración propia*

La tarjeta CRC de la clase OpcionesFirma (Tabla 3.37).

OpcionesFirma	
Responsabilidad	**Colaboración**
• Obtención de opciones para firma digital • Almacenamiento de opciones para firma digital.	• PropiedadesArchivoF • TipoAlmacenClaves • ConfigurarPro • Constantes

***Tabla 3.37** Tarjeta CRC de clase OpcionesFirma*

Fuente: Elaboración propia

3.3.1.2 Modelo estructural

El diagrama de clases muestra un conjunto de clases, interfaces, colaboraciones y sus relaciones (Figura 3.1) correspondientes a la historia de usuario 1 y definidas por las tarjetas CRC anteriormente diseñadas.

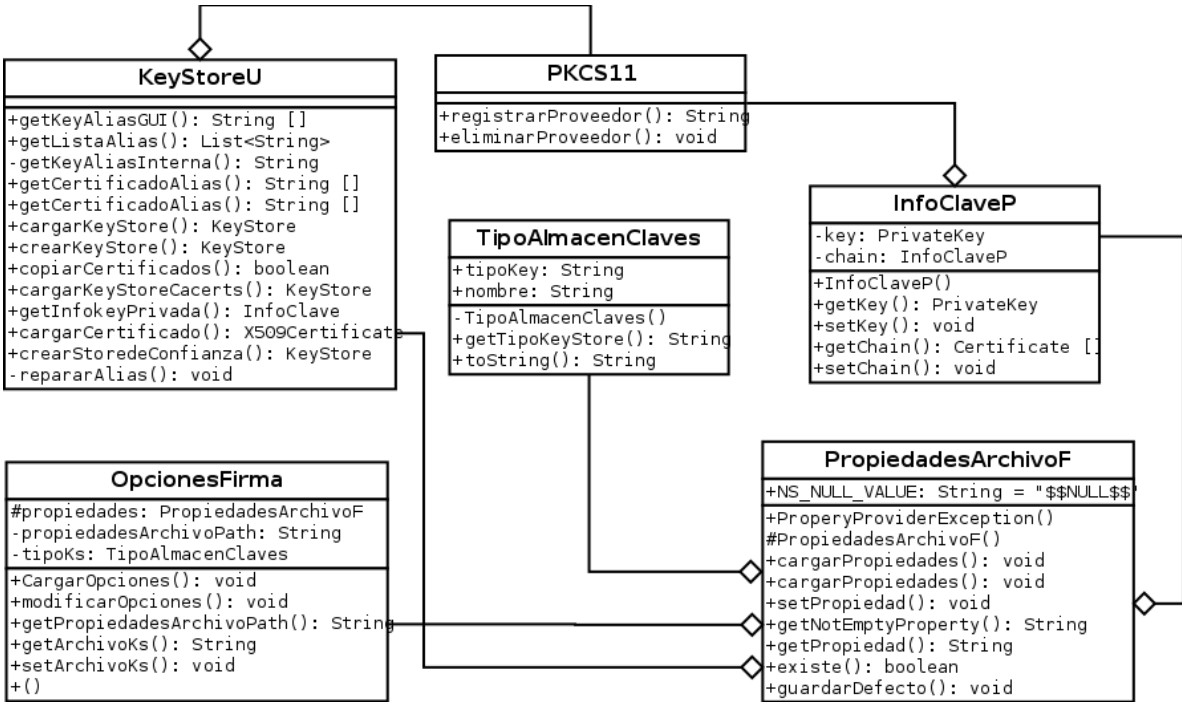

Figura 3.1 *Diagrama de Clases Primera iteración*

Fuente*: Elaboración propia*

3.3.2 Codificación

En esta fase se realiza la programación de la primera historia de usuario acorde a la primera iteración teniendo las características que se presentaron y diseñaron anteriormente.

3.3.2.1 Pantallas muertas

La historia de usuario 1 se vera representada en las pantallas muertas que se muestran a continuación:

La siguiente interfaz (Figura 3.2) hace referencia a la historias de usuario 1 (Tabla 3.2), resolviendo las tarjetas de tarea correspondientes. Se puede apreciar los siguientes aspectos resueltos:

- Opciones de selección de tipo de firma; se puede apreciar que se tienen dos opciones que corresponden a los estándares PKCS12 y PKCS11, con las opciones necesarias como es en el caso del estándar PKCS12 que se requiere el acceso al fichero de claves y la introducción de contraseña del fichero, por otro lado en el caso del PKCS11 se cuenta con la clase PKCS11 (Figura 3.1) que es la encargada

de conectar el sistema con la librería del smartcard o token.

- Obtención de alias de certificado; obtenemos el nombre común del certificado (nombre completo del signatario) para que el usuario identifique el nombre del signatario contenido en el certificado digital.
- Opción para cargar un archivo en formato pdf; esta opción tiene los métodos de filtrado y existencia del archivo.
- Opciones extras para adicionar a la firma digital; por normas del estándar PKCS7 estas opciones están habilitadas.
- Nivel de certificación de firma digital; opción para poder elegir el nivel de certificación de documento firmado digitalmente.
- Algoritmo Hash para resumen de documento firmado; se usan los hash SHA-1 y SHA-256 que son permitidos para los formatos de pdf 1.3 a 1.7.

Figura 3.2 *Opciones de firma digital*

Fuente*: Elaboración propia*

3.3.3 Pruebas

En esta fase se realizaran pruebas a los módulos desarrollados para esta iteración, se

utilizaran las tarjetas de aceptación o pruebas de aceptación y pruebas unitarias.

3.3.3.1 Pruebas de aceptación

Se define la prueba de aceptación (Tabla 23) para la historia de usuario 1, en la que se realizaron las pruebas de funcionamiento por parte de los usuarios, de esta forma las pruebas son aceptadas.

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 1
Nombre: Usar la firma digital de un servidor público almacenada en un token para firmar documentos en formato PDF.	
Descripción: Desarrollo de opciones para tipo de firma digital, obtención de alias de certificado digital.	
Condiciones de Ejecución: Cliente ejecutándose, módulo para acceso al tipo de firma digital.	
Pasos de Ejecución: El usuario escoge el tipo de estándar que quiere usar, ingresa la contraseña correspondiente al tipo de firma, obtienes el alias del certificado y selecciona el alias en caso de contar con varios certificados.	
Resultado esperado: El usuario tiene opción de escoger el estándar para firmar, seleccionar el alias del certificado a usar en la firma digital.	
Evaluación de prueba: Aceptada	

Tabla 3.38 *Prueba de aceptación Historia de Usuario 1*

Fuente*: Elaboración propia*

3.3.3.2 Pruebas unitarias

Estas pruebas se realizaran para comprobar el correcto funcionamiento de los módulos de código, esto sirve para asegurar que cada uno de los módulos desarrollados funcione correctamente por separado.

Pruebas Unitarias	Módulos para selección de tipo de almacenamiento.
Prueba: 1	
Descripción: Al escoger el tipo de almacenamiento de clave la obtención y selección del alias correspondiente sea el correcto.	
Objetivos: Comprobar lo siguiente:	

• Seleccionar el tipo de almacén de claves • Abrir documento en formato p12 o pfx • Validación de contraseña • Validar Alias de certificado • Seleccionar Alias de certificado
Condiciones: Usar la herramienta jUnit
Resultado Esperado: Los módulos funcionen correctamente.
Resultado obtenido: Los módulos funcionan correctamente.

Tabla 3.39 *Prueba unitaria para módulos de Historia de Usuario 1*

Fuente*: Elaboración propia*

3.4 SEGUNDA ITERACIÓN

Se desarrolla los módulos, clases y métodos necesarios en las tareas asignadas (ver tablas 3.7, 3.8, 3.9, 3.10 y 3.11) a la historia de usuario:

2. Firmar documento en formato PDF.

Esta iteración es una de las más importantes porque es en esta iteración donde se realiza la función base de todo el sistema.

3.4.1 Diseño

En los siguientes artefactos se describen las tarjetas CRC, modelo estructural y pantallas muertas del diseño de la segunda historia de usuario.

3.4.1.1 Tarjetas CRC

A continuación se describen las tarjetas CRC con sus respectivas responsabilidades y colaboraciones correspondientes a la historia de usuario 2:

La tarjeta CRC de la clase firmar (Tabla 3.40).

Firmar	
Responsabilidad	**Colaboración**
• Firmar documento Pdf • Añadir opciones extras a firma digital. • Generar Hash de documento firmado. • Verificación y soporte de documento pdf. • Verificación de entrada y salida de documento pdf.	• InformacionCRL • IniciarSSL • AlgoritmoHash • AutenticacionServer • KeystoreU • OpcionesFirma • PKCS11 • InfoClaveP • TipoAlmacenClaves • PopiedadesArchivoF

Tabla 3.40 *Tarjeta CRC de clase Firmar*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase SeleccionarArchivo(Tabla 3.41).

SeleccionarArchivo	
Responsabilidad	**Colaboración**
• Cargar documento pdf • Cargar carpeta de documentos pdf • Abrir documento p12 o pfx	• Ninguna

Tabla 3.41 *tarjeta CRC de clase SeleccionarArchivo*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase PrincipalController(Tabla 3.42).

PrincipalController	
Responsabilidad	**Colaboración**
• Cargar la interfaz del sistema	• SeleccionarArchivo • Firmar • Constantes • OpcionesFirma • AlgoritmoHash • AutenticacionServer • NivelCertificacion • TipoAlmacenClaves • KeyStoreU

Tabla 3.42 *Tarjeta CRC de clase PrincipalController*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase Pdf (Tabla 3.42).

Pdf	
Responsabilidad	**Colaboración**
• Cagar documento pdf	• Ninguno

Tabla 3.43 *Tarjeta CRC de Pdf*

Fuente*: Elaboración propia*

3.4.1.2 Modelo estructural

El siguiente diagrama de clases (Figura 3.3) es el correspondiente a la historia de usuario 2 y las tarjetas CRC definidas anteriormente.

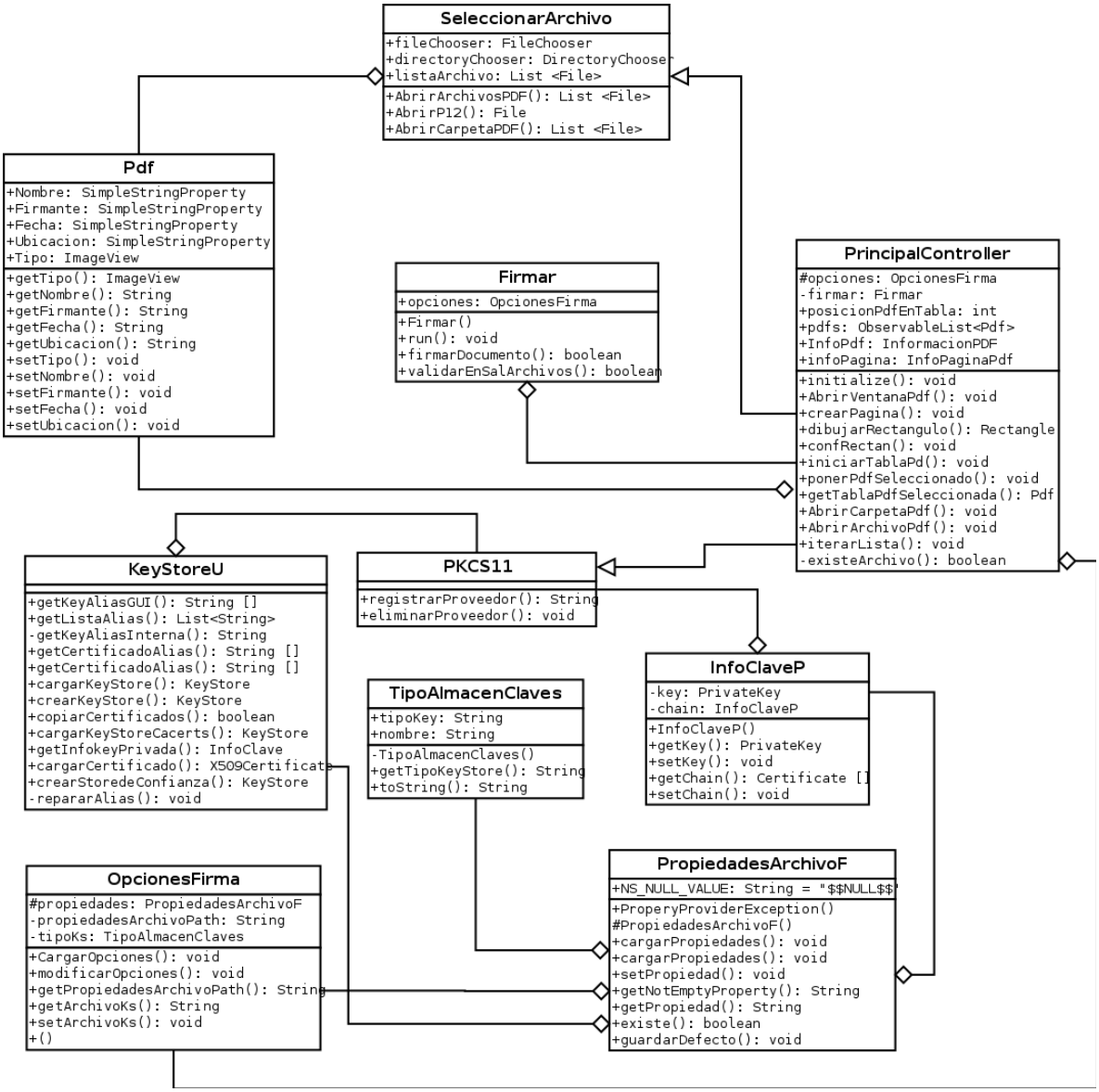

Figura 3.3 *Diagrama de Clases Segunda iteración*

Fuente*: Elaboración propia*

3.4.2 Codificación

Se realiza la programación de la segunda historia de usuario teniendo en cuenta las características que se presentaron y diseñaron anteriormente.

3.4.2.1 Pantallas muertas

Las pantallas (Figura 3.5 y 3.4) correspondientes al desarrollo de la historia usuario 2 son las siguientes:

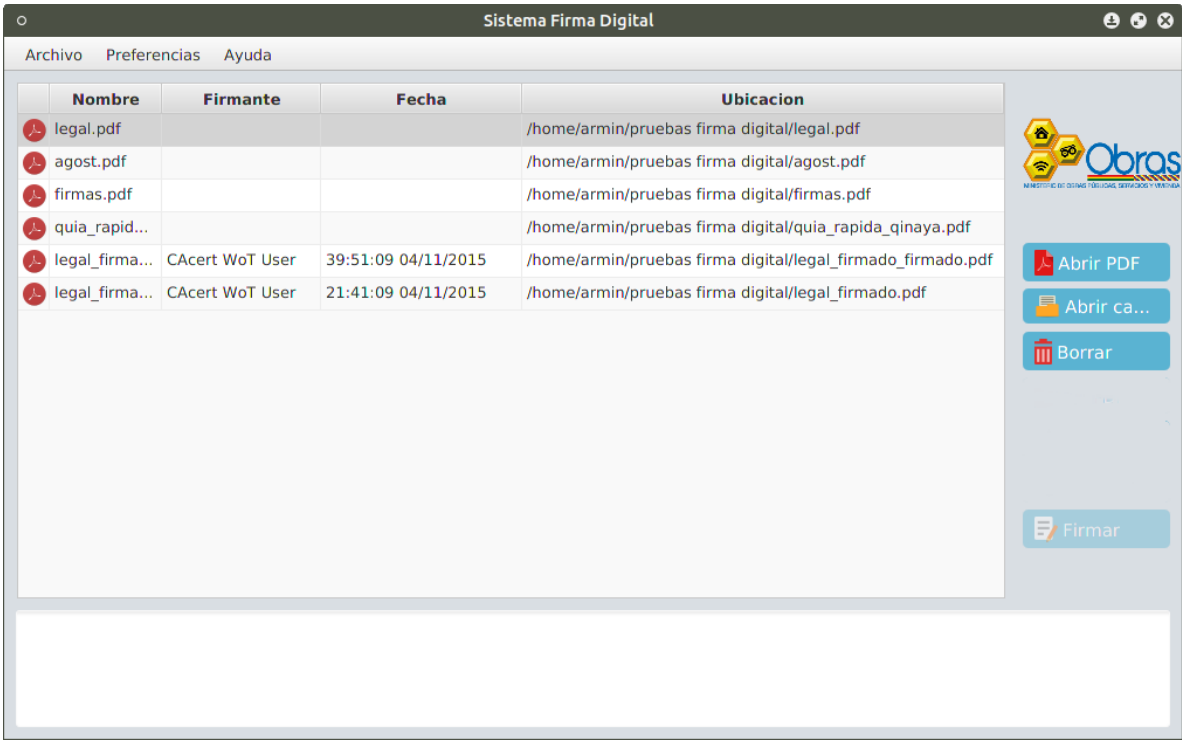

Figura 3.4 *Carga de archivos pdf*

Fuente*: Elaboración propia*

Figura 3.5 *Opciones adicionales para firma digital*

Fuente*: Elaboración propia*

3.4.3 Pruebas

Se realizaran las pruebas de aceptación y pruebas unitarias pertinentes a la historia de usuario 2.

3.4.3.1 Pruebas de aceptación

Se muestra la prueba de aceptación para la historia de usuario 2 (Tabla).

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 2
Nombre: Firmar documento en formato pdf	
Descripción: Desarrollo para poder firmar digitalmente un documento pdf, con las opciones para añadir extras (razón, lugar y email), nivel de certificación y hash de documento firmado.	
Condiciones de Ejecución: Cliente ejecutándose, módulo firmar documento, adición de opciones extras, selección de nivel de certificación, selección de tipo de hash.	

Pasos de Ejecución: El usuario selecciona la carpeta o archivo en formato pdf, añade las opciones extras para la firma, selecciona el nivel de certificación de documento firmado, selecciona el tipo de hash para documento pdf.
Resultado esperado: El usuario firma un documento en formato pdf, escogiendo las opciones adicionales como ser tipo de hash, nivel de certificación y opciones extras.
Evaluación de prueba: Aceptada

Tabla 3.44 *Prueba de aceptación Historia de usuario 2*

Fuente*: Elaboración propia*

3.4.3.2 Pruebas unitarias

Se realizó la prueba unitaria (Tabla 3.45) los módulos generados para la historia de usuario 2.

Pruebas Unitarias	Módulos para firmar un documento pdf.
Prueba: 1	
Descripción: Firmar un documento pdf.	
Objetivos: Comprobar lo siguiente: • Selección de documento pdf • Abrir carpeta de documentos pdf • Selección de tipo de nivel de certificación • Selección de tipo de hash • Adición de opciones extras para la firma	
Condiciones:	
Resultado Esperado: Los módulos funcionen correctamente, el hash aplicado al documento firmado sea adecuado.	
Resultado obtenido: Los módulos funcionan correctamente.	

Tabla 3.45 *Pruebas unitarias Historia de Usuario 2*

Fuente*: Elaboración propia*

3.5 TERCERA ITERACIÓN

En esta iteración se desarrollara la siguiente historia de usuario:

3. Validación y comprobación de estado del certificado otorgado por la entidad certificadora para tener una constancia del estado del certificado.

Las tarjetas de tareas (Tabla 3.13 y 3.14) asignadas a esta historia de usuario serán desarrolladas en la correspondiente iteración.

3.5.1 Diseño

A continuación se realizan las tarjetas CRC y diagrama de clases para representar las clases a ser desarrolladas para esta iteración.

3.5.1.1 Tarjetas CRC

Se detallan las tarjetas CRC a implementarse:

La tarjeta CRC de la clase IniciarSSL (Tabla).

IniciarSSL	
Responsabilidad	**Colaboración**
• Crear conexión SSL con servidor OCSP y servidor CRL.	• OpcionesFirma • AutenticacionServer • OpcionesFirma

Tabla 3.46 *Tarjeta CRC de clase IniciarSSL*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase InformacionCRL (Tabla).

InformacionCRL	
Responsabilidad	**Colaboración**
• Obtener información de usuario de CRL • Iniciar CRL • Descargar archivo CRL • Consultar servidor CRL	• KeyStoreU

Tabla 3.47 *Tarjeta CRC de clase InformacionCRL*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase Firmar (Tabla 3.48) a la cual se le añaden nuevas responsabilidades.

Firmar	
Responsabilidad	**Colaboración**
• Firmar documento Pdf	• InformacionCRL

• Añadir opciones extras a firma digital. • Generar Hash de documento firmado. • Verificación y soporte de documento pdf. • Verificación entrada y salida de documento pdf. • Verificación de firma a servidor OSCP • Verificación de firma a documento CRL.	• IniciarSSL • AlgoritmoHash • AutenticacionServer • KeystoreU • OpcionesFirma • PKCS11 • InfoClaveP • TipoAlmacenClaves • PopiedadesArchivoF

Tabla 3.48 *Tarjeta CRC de clase Firmar con opciones OCSP y CRL*

Fuente*: Elaboración propia*

3.5.1.2 Modelo estructural

El diagrama de clases para el diseño del sistema se muestra en la Figura 3.6.

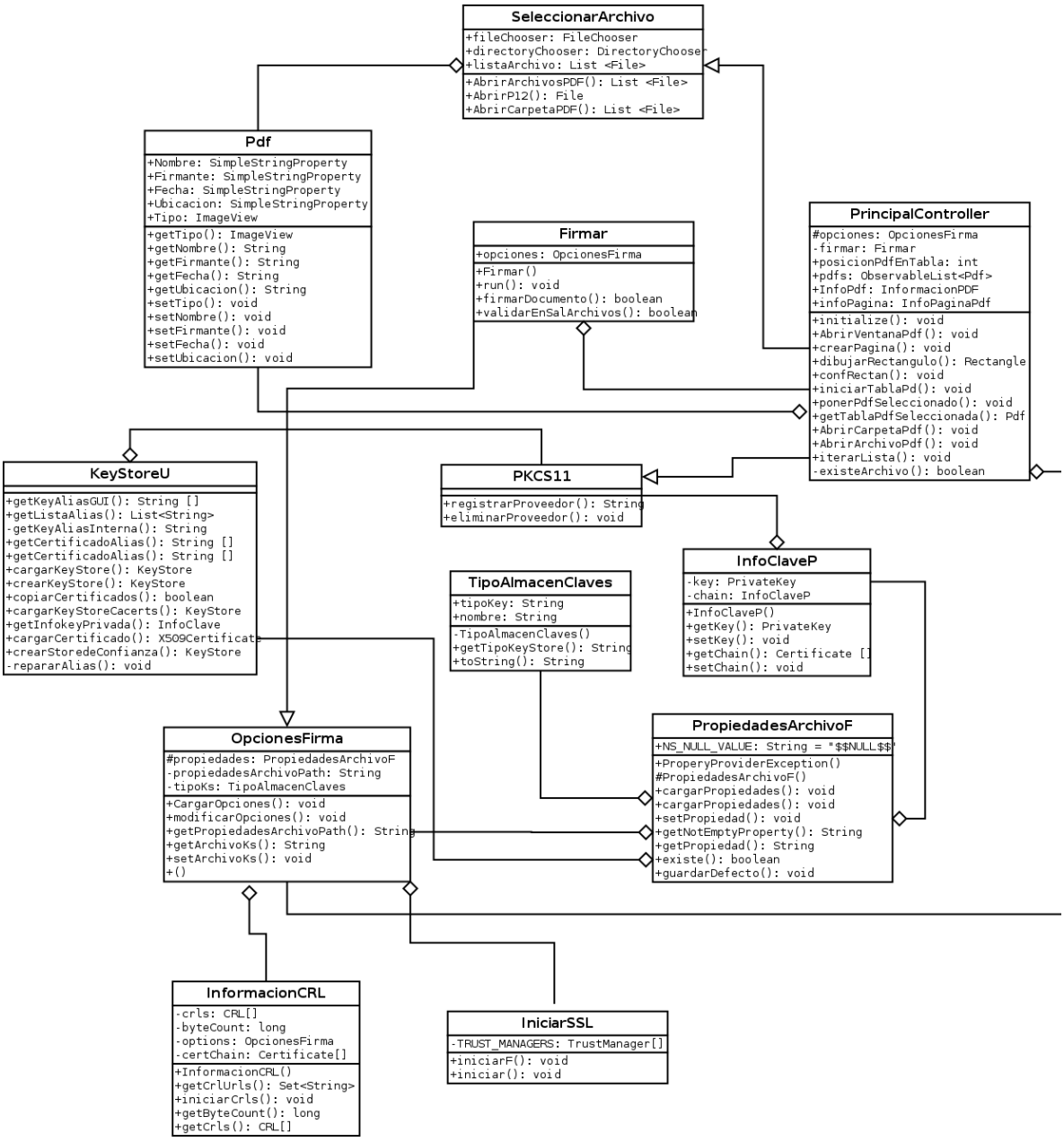

Figura 3.6 *Diagrama de Clases Tercera Iteración*

Fuente*: Elaboración propia*

3.5.2 Codificación

Las clases diseñadas serán desarrolladas para poder establecer consultas al servidor OCSP o CRL de entidad certificadora, para verificar la validez y vigencia del certificado digital, Así mismo, se establecerá una conexión segura con dicho servidor para que las consultas no

sean vulneradas.

Se muestran las capturas de pantalla de la interfaz (Figura 3.48) para la historia de usuario 3.

3.5.2.1 Pantallas muertas

En la pantalla correspondiente a la historia de usuario 3 se puede observar la opción para añadir la URL del servidor OCSP y habilitar el uso de un CRL.

Figura 3.7 *Interfaz de consulta a servidor OCSP y CRL*

Fuente*: Elaboración propia*

3.5.3 Pruebas

Se realizan las pruebas de aceptación a la historia de usuario 3 y las correspondientes pruebas unitarias a los módulos desarrollados para esta historia.

3.5.3.1 Pruebas de aceptación

Prueba de aceptación (Tabla 3.49) de la historia de usuario 3.

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 3
Nombre: Realizar consultas a servidor OCSP y a Archivo CRL con una conexión SSL segura.	
Descripción: Desarrollo de opciones para ingresar la URL de servidor OCSP para realizar consultas de vigencia y validación de certificado digital.	
Condiciones de Ejecución: Cliente ejecutándose, módulo de consulta de servidor OCSP.	
Pasos de Ejecución: El usuario ingresa la URL del servidor OCSP para realizar las consultas de verificación, vigencia y validación de certificado digital.	
Resultado esperado: El usuario no podrá firmar un documento si el certificado digital esta caducado o no vigente, se obtendrá un hash del documento firmado y se le podrá asignar un nivel de certificación.	
Evaluación de prueba: Aceptada	

Tabla 3.49 *Prueba de aceptación de Historia de Usuario 3*

Fuente*: Elaboración propia*

3.5.3.2 Pruebas unitarias

Se realizan las pruebas unitarias (Tabla) a los módulos de consulta a servidor OCSP y archivo CRL.

Pruebas Unitarias	Módulos para validación de certificado digital y consultas SSL a servidor OCSP y CRL.
Prueba: 1	
Descripción: Al ingresar la URL del servidor OCSP, el sistema podrá hacer las consultas necesarias para la validación y verificación de certificado digital.	
Objetivos: Comprobar lo siguiente: • Consultas a servidor OCSP. • Consulta a archivo CRL • Validación y verificación de certificado digital • Conexión cifrada entre servidor y sistema.	
Condiciones: Saber usar la herramienta jUnit.	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente de acuerdo a las	

especificaciones hechas..

Tabla 3.50 *Pruebas unitarias a Modulo de consulta a servidor OCSP y CRL*

Fuente*: Elaboración propia*

3.6 CUARTA ITERACIÓN

En esta iteración se desarrollaran la siguientes historias de usuario:

4. Visualizar un documento en formato pdf.
5. Incluir marca de agua con la información de certificado digital del funcionario público.

Las tareas asignadas a estas historias de usuario (Tablas 3.16 y 3.18) se resumen en desarrollar un visualizador de pdf y asignación de marca de agua.

3.6.1 Diseño

En esta iteración de igual forma se hará uso de las tarjetas CRC para representar las clases, como también haremos el uso de los diagramas de clases.

3.6.1.1 Tarjetas CRC

Se detallan las tarjetas CRC para el desarrollo de las historias de usuario 4 y 5:

La tarjeta CRC de la clase InformacionPDF (Tabla 3.51).

InformacionPDF	
Responsabilidad	**Colaboración**
• Obtener información de documento pdf. • Obtener el numero de pagina de documento pdf.	• InfoPaginaPdf

Tabla 3.51 *Tarjeta CRC de clase InformacionPDF*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase PdfaImagen (Tabla 3.52).

PdfaImagen	
Responsabilidad	**Colaboración**
•	• InfoPaginaPdf

Tabla 3.52 *Tarjeta CRC de clase PdfaImagen*

Fuente*: Elaboración propia*

La adición de responsabilidades de la tarjeta CRC de la clase Firmar (Tabla 3.53).

Firmar	
Responsabilidad	**Colaboración**
• Firmar documento Pdf • Añadir opciones extras a firma digital. • Generar Hash de documento firmado. • Verificación y soporte de documento pdf. • Verificación entrada y salida de documento pdf. • Asignación de marca de agua.	• InformacionCRL • IniciarSSL • AlgoritmoHash • AutenticacionServer • KeystoreU • OpcionesFirma • PKCS11 • InfoClaveP • TipoAlmacenClaves • PopiedadesArchivoF • PdfaImagen • PrincipalController

Tabla 3.53 *Tarjeta CRC de clase Firmar con opción de marca de agua*

Fuente*: Elaboración propia*

3.6.1.2 Modelo estructural

Como ya definieron las clases adicionales al sistema, el diagrama de clases sera representado de la siguiente forma:

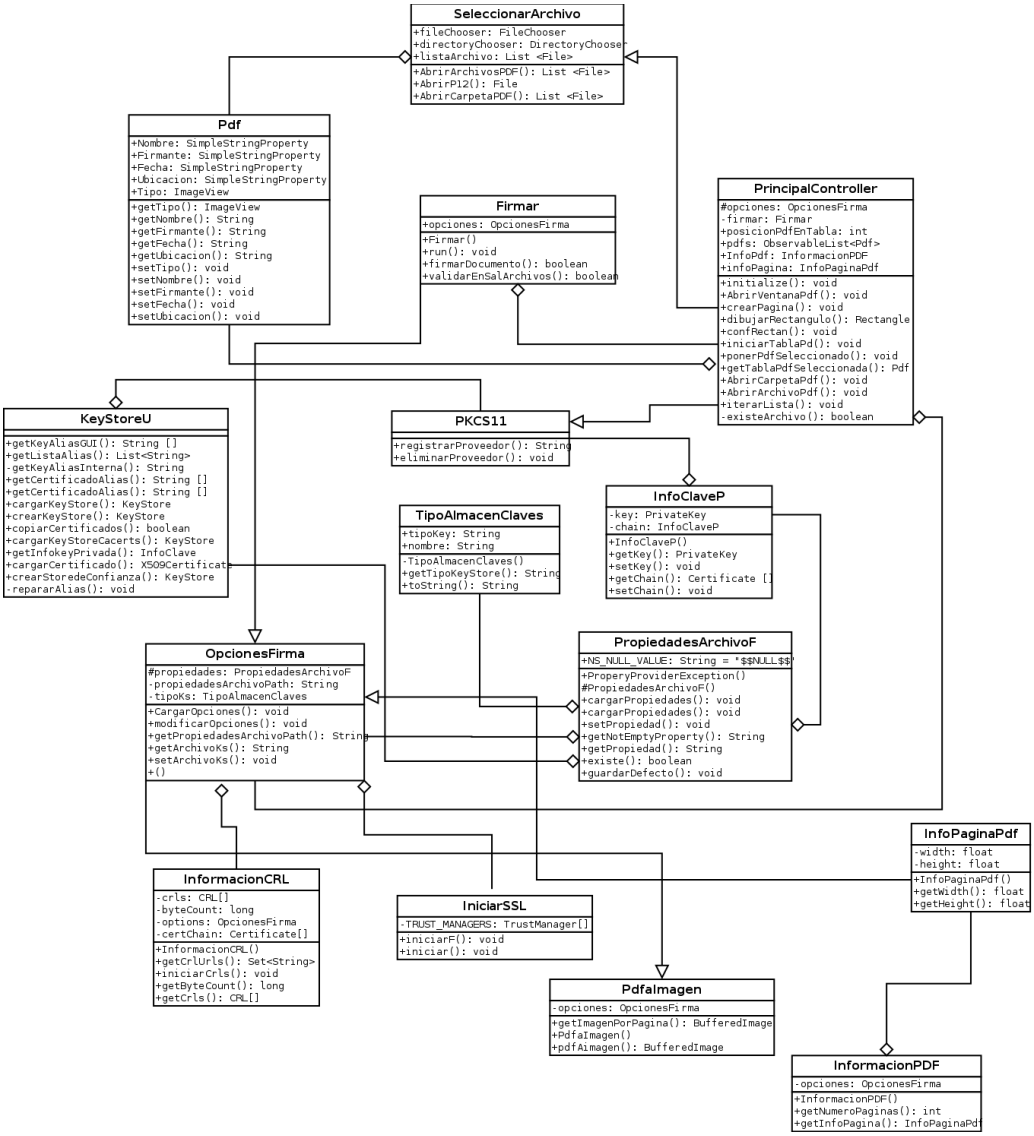

Figura 3.8 *Diagrama de Clases Cuarta Iteración*

Fuente*: Elaboración propia*

3.6.2 Codificación

La interfaz de desarrollo para la visualización de un documento pdf es simple, es solo para asignar un área para la marca de agua (Figura 3.9). El documento pdf no es modificado, la conversión de pdf a imagen se realiza para cada hoja del documento pdf,

3.6.2.1 Pantallas muertas

Vista de documento pdf y asignación de área para marca de agua:

Figura 3.9 *Visualización de Pdf y asignación de área para marca de agua*

Fuente*: Elaboración propia*

3.6.3 Pruebas

Se realizan las pruebas de aceptación y pruebas unitarias, detalladas a continuación.

3.6.3.1 Pruebas de aceptación

Prueba de aceptación para la historia de usuario 4 (Tabla 3.54).

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 4
Nombre: Visualización de documento pdf a ser firmado.	
Descripción: Desarrollo de módulo para visualizar un documento con formato pdf.	
Condiciones de Ejecución: Cliente ejecutándose, botón para visualizar documento pdf seleccionado.	
Pasos de Ejecución: El usuario selecciona el documento pdf, presiona el botón de ver pdf, se visualiza el documento pdf.	
Resultado esperado: El usuario visualizara un documento en formato pdf.	
Evaluación de prueba: Aceptada	

Tabla 3.54 *Prueba de aceptación Historia de Usuario 4*

Fuente*: Elaboración propia*

Prueba de aceptación para la historia de usuario 5 (Tabla 3.55).

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 5
Nombre: Incluir marca de agua a documento pdf.	
Descripción: Desarrollo de módulo para asignar área para marca de agua en documento pdf visualizado.	
Condiciones de Ejecución: Cliente ejecutándose, presionar para dibujar área para marca de agua.	
Pasos de Ejecución: El usuario selecciona el documento pdf, presiona el botón de ver pdf, dibuja un área rectangular donde sera la marca de agua.	
Resultado esperado: El usuario dibujara un área rectangular donde se incluirá la marca de agua.	
Evaluación de prueba: Aceptada	

Tabla 3.55 *Prueba de aceptación de Historia de Usuario 5*

Fuente*: Elaboración propia*

3.6.3.2 Pruebas unitarias

Las pruebas unitarias (Tabla 3.56) para los módulos encargados de visualizar y dibujar el área para marca de agua en documento con formato pdf.

Pruebas Unitarias	Módulos para visualizar documento pdf y dibujar el área para marca de agua.
Prueba: 1	
Descripción: Visualización de documento con formato pdf y asignación de área para añadir la marca de agua a documento.	
Objetivos: Comprobar lo siguiente: • Visualización de documento pdf • Dibujo de área rectangular para marca de agua	
Condiciones: Saber usar la herramienta jUnit.	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

Tabla 3.56 *Pruebas unitarias Historia de usuario 4 y 5*

Fuente*: Elaboración propia*

3.7 QUINTA ITERACIÓN

En esta iteración se desarrollara la siguiente historia de usuario:

6. Incluir sello de tiempo de la entidad certificadora para los documentos firmados en formado pdf.

3.7.1 Diseño

Se diseñan las clases correspondientes a la historias de usuario 6 con sus respectivas tarjetas de tarea (Tablas 3.20 y 3.21).

3.7.1.1 Tarjetas CRC

Se detallan las tarjetas CRC de la historia de usuario 6 con sus responsabilidades y colaboradores:

La adición de nuevas responsabilidades a la clase Firmar (Tabla 3.57).

Firmar	
Responsabilidad	**Colaboración**
• Firmar documento Pdf • Añadir opciones extras a firma digital. • Generar Hash de documento firmado. • Verificación y soporte de documento pdf. • Verificación entrada y salida de documento pdf. • Dibujo de área para marca de agua. • Incluir sello de tiempo a documento pdf.	• InformacionCRL • IniciarSSL • AlgoritmoHash • AutenticacionServer • KeystoreU • OpcionesFirma • PKCS11 • InfoClaveP • TipoAlmacenClaves • PopiedadesArchivoF • PdfaImagen • PrincipalController

Tabla 3.57 *Tarjeta CRC de clase Firmar con opciones para TSA*

Fuente*: Elaboración propia*

3.7.1.2 Modelo estructural

Para esta historia de usuario 6 se diseña el diagrama de clases (Figura), el cual sufre cambios en los métodos de las clases principales.

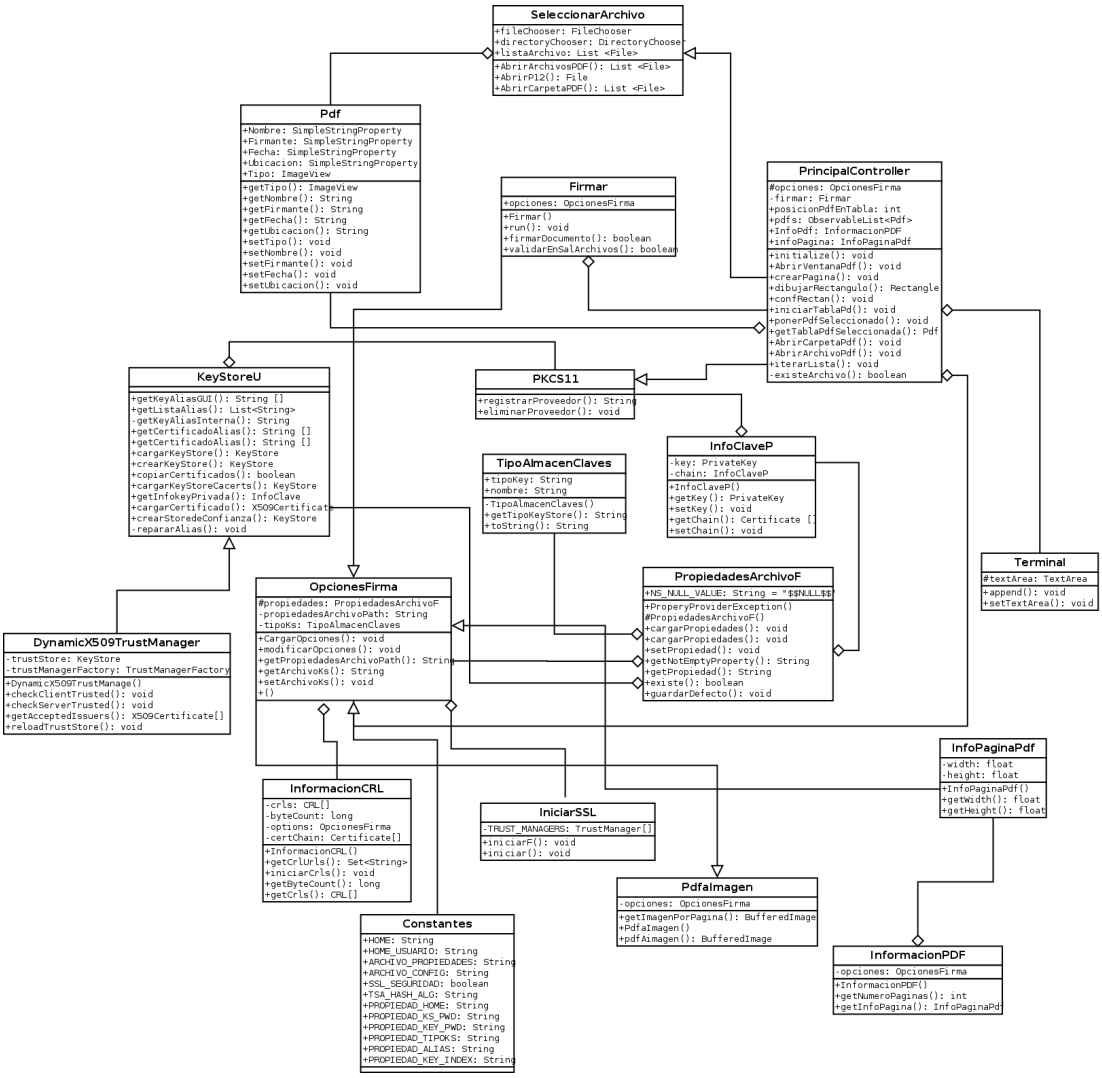

Figura 3.10 *Diagrama de Clases Quinta Iteración*

Fuente*: Elaboración propia*

3.7.2 Codificación

Se desarrollan tres tipos de autenticación para el servidor TSA, las opciones son: ninguno, con certificado y con usuario y contraseña; ademas de seleccionar el tipo algoritmo hash (SHA-1 o SHA-2) que se aplicara al documento para luego obtener el sello de tiempo.

3.7.2.1 Pantallas muertas

En la siguiente figura (Figura 3.11) se denotan las opciones para la obtención del sello de tiempo al servidor TSA:

Figura 3.11 *Configuración de opciones para servidor TSA*

Fuente*: Elaboración propia*

3.7.3 Pruebas

Se detallan a continuación las correspondientes pruebas de aceptación y pruebas unitarias que responden a la historia de usuario 6.

3.7.3.1 Pruebas de aceptación

Pruebas de aceptación de la historia de usuario 6 (Tabla 3.58).

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 6
Nombre: Incluir sello de tiempo de la entidad certificadora para los documentos firmados en formato pdf.	
Descripción: Desarrollo de módulo de autenticación para servidor TSA, asignación de tipo de hash de documento a ser firmado.	
Condiciones de Ejecución: Cliente ejecutándose, autenticación con el servidor TSA, asignación de tipo resumen de documento y obtención de sello de tiempo.	

Pasos de Ejecución: El usuario escoge el tipo de autenticación a servidor TSA, selecciona el tipo de hash del documento firmado y obtiene el sello de tiempo.
Resultado esperado: El usuario se autentifica y obtiene el sello de tiempo.
Evaluación de prueba: Aceptada

Tabla 3.58 *Prueba de aceptación Historia de Usuario 6*

Fuente*: Elaboración propia*

3.7.3.2 Pruebas unitarias

Pruebas unitarias a módulos desarrollados para la historia de usuario 6 (tabla).

Pruebas Unitarias	Módulos obtener el sello de tiempo de un servidor TSA.
Prueba: 1	
Descripción: Autenticación a servidor TSA para obtener el sello de tiempo, realizando el hash de documento firmado.	
Objetivos: Comprobar lo siguiente: • Tipo de autenticación • Hash de documento pdf • Obtención de sello de tiempo	
Condiciones: Saber usar la herramienta jUnit.	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

Tabla 3.59 *Pruebas unitarias a Módulos para obtener sello de tiempo*

Fuente*: Elaboración propia*

3.8 SEXTA ITERACIÓN

En esta iteración se desarrollaran la siguientes historias de usuario:

7. Verificación de firmas digitales en documentos firmados, con formato pdf.
8. Almacenamiento del historial de firmas realizadas por los servidores públicos y generación QR de URL de acceso a documento pdf firmado.

Para la historia de usuario 7 se resolverán las tareas asignadas (Tablas 3.23 y 3.24) y de la misma forma para la historia de usuario 8 se resolverán las respectivas tareas asignadas(Tablas 3.26, 3.27 y 3.28).

3.8.1 Diseño

Para las historias de usuario asignadas a esta iteración, se diseñan las tarjetas CRC y diagrama de clases, necesarias para resolver las tareas asignadas.

3.8.1.1 Tarjetas CRC

Se detallan a continuación las tarjetas CRC correspondientes a las historias de usuario 7 y 8:

Tarjeta CRC de la clase ResultVerificacion (Tabla 3.60).

ResultVerificacion	
Responsabilidad	**Colaboración**
• Contar el numero de verificaciones de documento firmado. • Mostrar resultado de verificación de firmas.	• VerificacionFirma

Tabla 3.60 *Tarjeta CRC de clase ResultVerificacion*

Fuente*: Elaboración propia*

Tarjeta CRC de la clase VerificacionFirma (Tabla 3.61).

VerificacionFirma	
Responsabilidad	**Colaboración**
• Guardar y obtener información de verificación de firmas.	• NivelCertificacion

Tabla 3.61 *Tarjeta CRC clase VerificacionFirma*

Fuente*: Elaboración propia*

Tarjeta CRC de la clase Verificar (Tabla 3.62).

Verificar	
Responsabilidad	**Colaboración**
• Verificar firmas en documento firmado. • Verificar sello de tiempo. • Verificar certificado digital con servidor OCSP.	• KeyStoreU • VerificacionFirma • ResultVerificacion

• Obtener información certificado digital de documento pdf firmado.	

Tabla 3.62 *Tarjeta CRC clase Verificar*

Fuente*: Elaboración propia*

3.8.1.2 Modelo estructural

Se diseña el diagrama de clases correspondiente a la historia de usuario 7 y 8 (Figura 3.12):

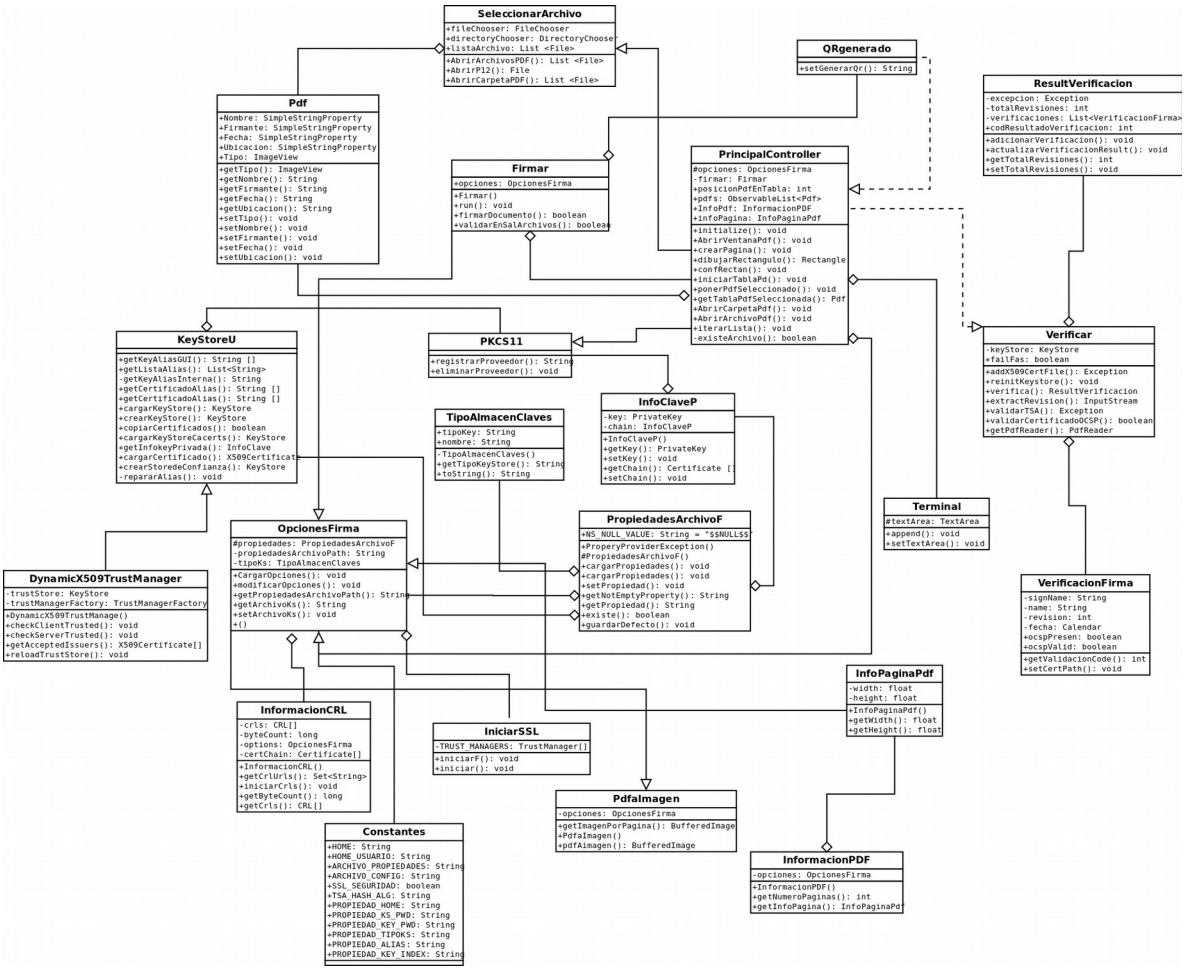

Figura 3.12 *Diagrama de clases sexta iteración*

Fuente*: Elaboración propia*

El diagrama Entidad Relación para el almacenamiento de información de firmas es el siguiente (Figura 3.13):

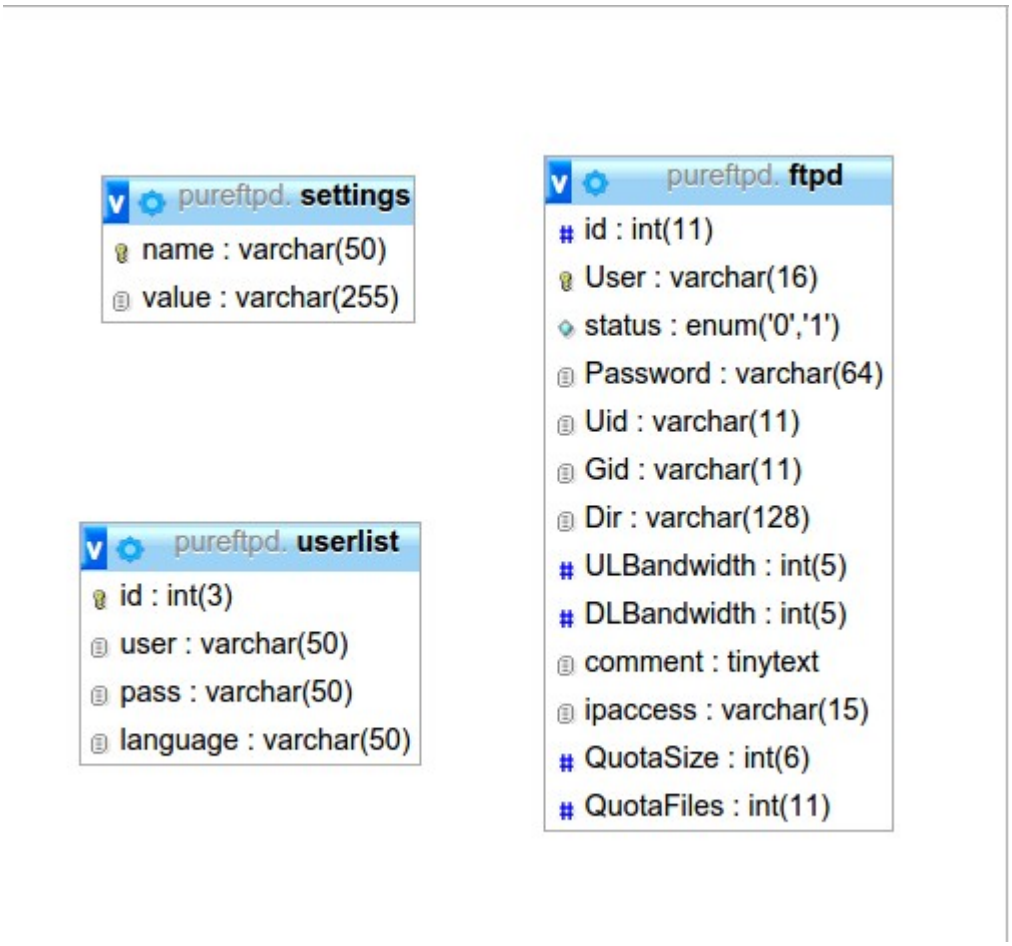

Figura 3.13 *ER de Sistema Web*

Fuente*: Elaboración propia*

3.8.2 Codificación

Para la historia de usuario 7 se desarrolla una pantalla simple (Figura 3.14), en el que se puede apreciar la información de los signatarios del documento.

Para la historia de usuario 8 se dio la necesidad de desarrollar un pequeño sistema web integrado con el servidor FTP (Pure-ftpd) para ver la lista de documentos firmados, administrar usuarios de servidor ftp, usuarios administradores del sistema web y manejo de servidor FTP. El respaldo es solo de documentos firmados y la interfaz para autenticarse es simple (Figura 3.15). Se genera una imagen QR en el documento firmado, esta imagen contiene una dirección URL de acceso al documento.

3.8.2.1 Pantallas muertas

Se detallan a continuación las pantallas muertas para esta iteración:

Interfaz para mostrar la información de los signatarios (Figura 3.14):

Figura 3.14 *Información de signatarios de documento firmado*

Fuente*: Elaboración propia*

QR generado en el documento firmado (Figura):

Autenticación de usuario para respaldar documento firmado (Figura 3.15):

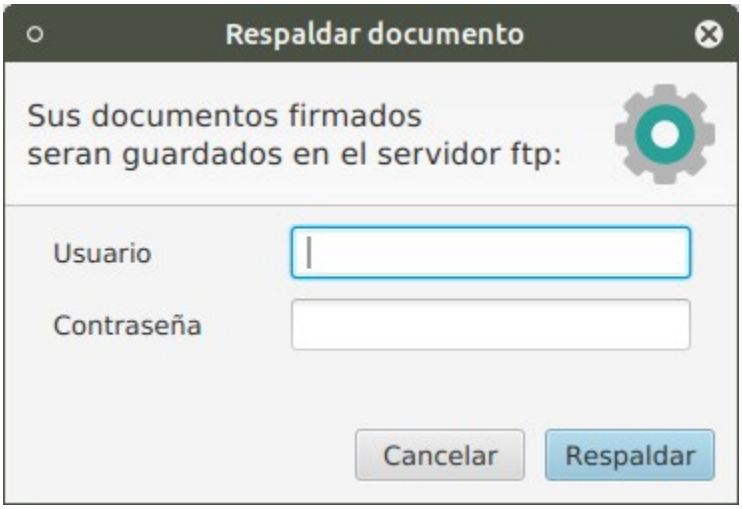

Figura 3.15 *Autenticación para servidor FTP*

Fuente*: Elaboración propia*

Verificación de respaldo de documento (Figura 3.16):

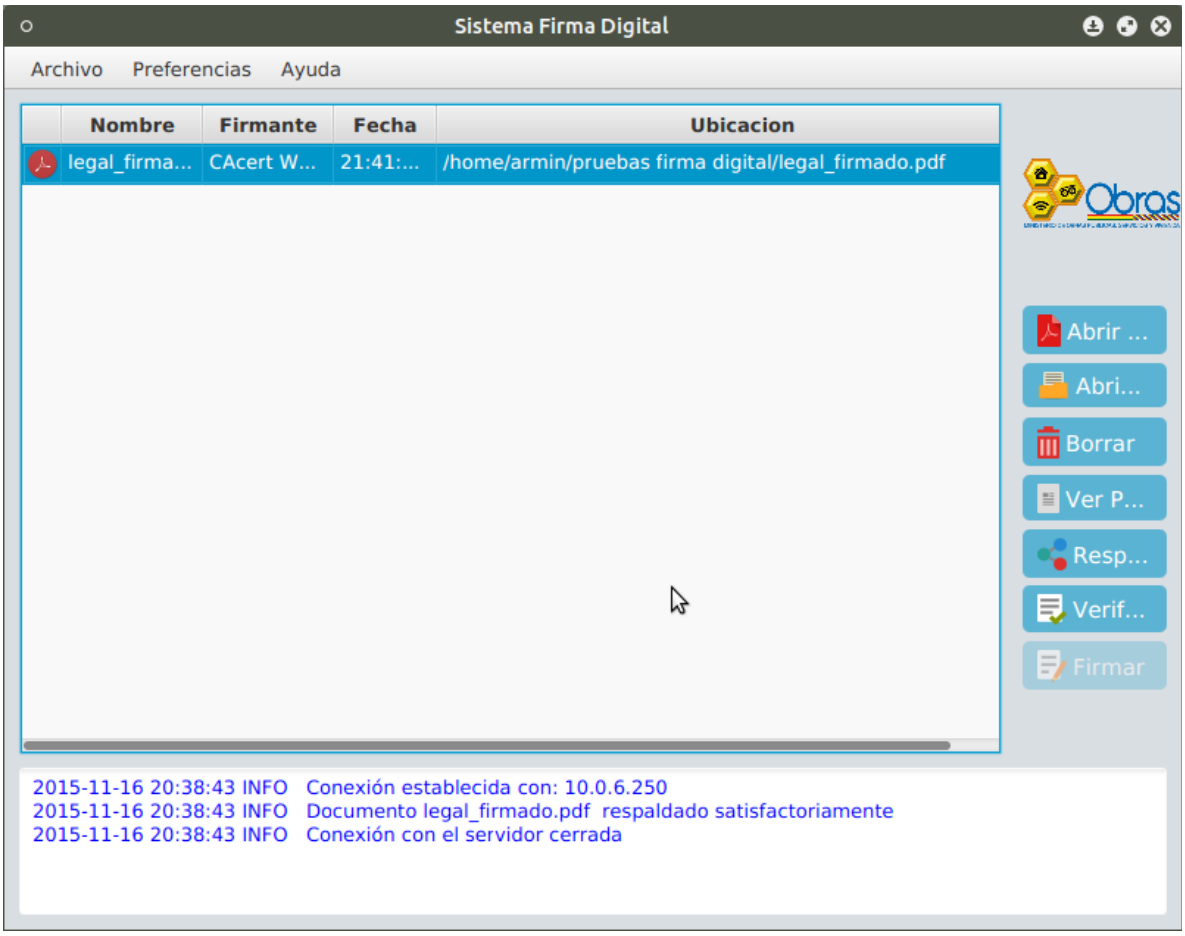

Figura 3.16 *Verificación de respaldo de documento*

Fuente*: Elaboración propia*

Sistema web con integración con servidor FTP:

- Administración de usuarios FTP (Figura 3.17):

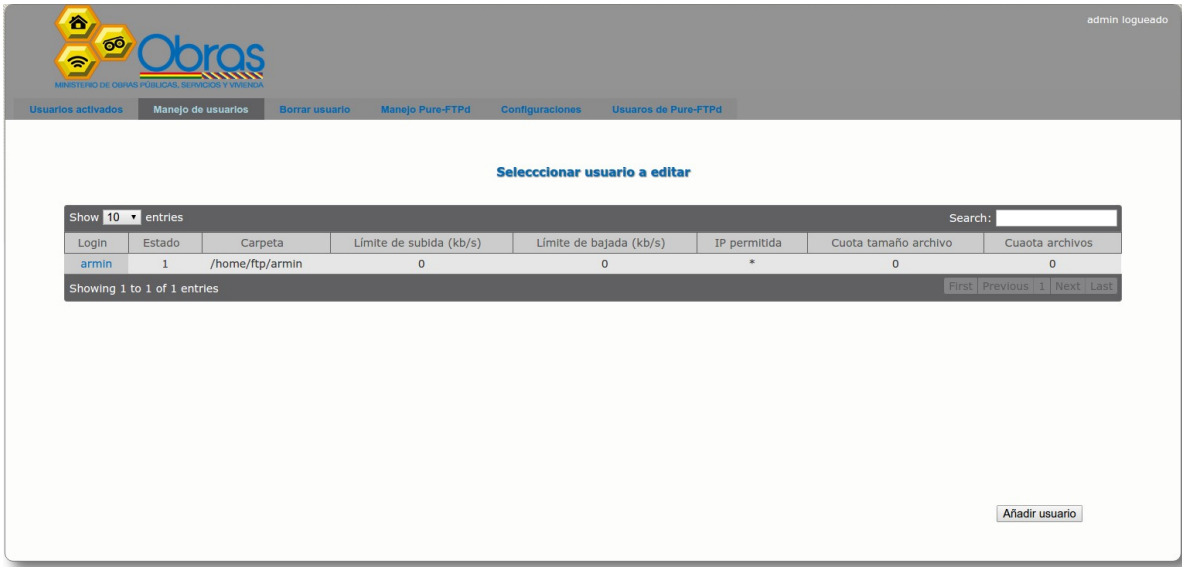

Figura 3.17 *Administración de usuarios*

Fuente*: Elaboración propia*

- Integración sistema web con servidor FTP (Figura 3.18).

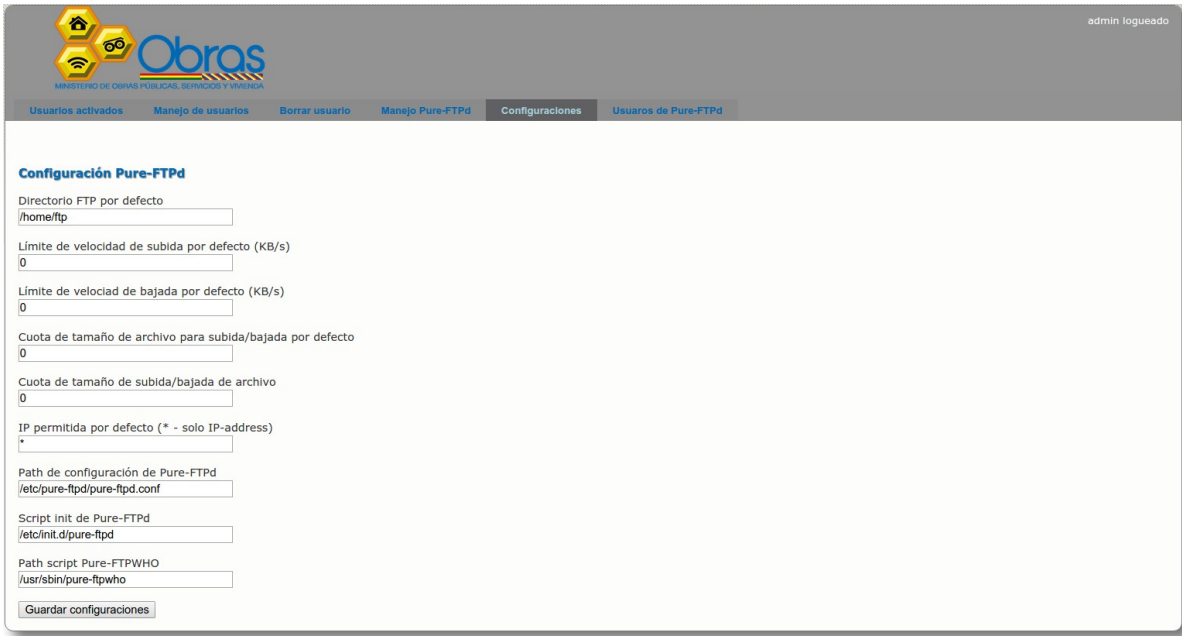

Figura 3.18 *Integración con servidor FTP*

Fuente*: Elaboración propia*

- Administración de usuarios del sistema web (Figura 3.19).

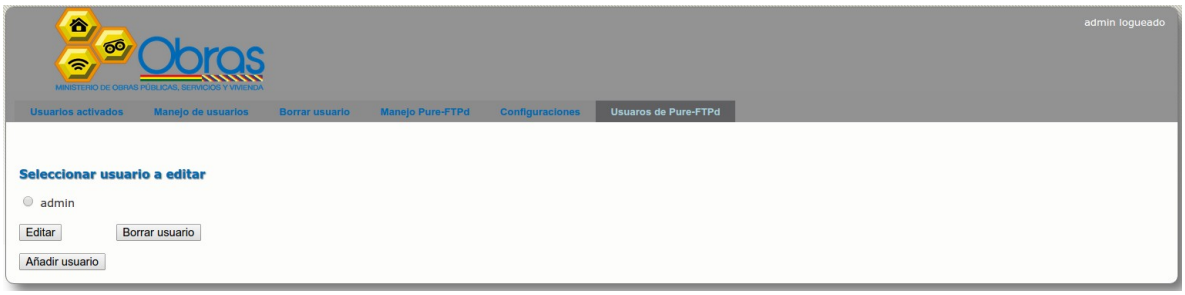

Figura 3.19 *Administración de usuarios de sistema web*

Fuente*: Elaboración propia*

3.8.3 Pruebas

Las pruebas unitarias y pruebas de aceptación de las historias de usuario 7 y 8 se detallan a continuación.

3.8.3.1 Pruebas de aceptación

Prueba de aceptación para la historia número 7 (Tabla 3.63):

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 7
Nombre: Verificación de firmas digitales en documentos firmados con formato PDF.	
Descripción: Desarrollo de módulo para desplegar la información de los signatarios de un documento firmado.	
Condiciones de Ejecución: Cliente ejecutándose, módulo para desplegar información de signatarios de documento.	
Pasos de Ejecución: El usuario selecciona el documento firmado, presiona el botón verificar y se despliega la información de los signatarios del documento.	
Resultado esperado: El usuario puede observar la información de los signatarios del documento firmado.	
Evaluación de prueba: Aceptada	

Tabla 3.63 *Prueba de aceptación Historia de usuario 7*

Fuente*: Elaboración propia*

Prueba de aceptación para la historia número 8 (Tabla 3.64):

Prueba de Aceptación	
Numero: 1	**Historia de Usuario:** 8
Nombre: Almacenamiento de documentos firmados, realizadas por los signatarios y generación QR con URL de acceso al documento.	
Descripción: Desarrollo de módulo para resguardo de documentos pdf y generación de QR.	
Condiciones de Ejecución: Cliente ejecutándose, módulo para subir documento pdf firmado a servidor FTP, generación de QR con la URL de acceso al documento.	
Pasos de Ejecución: El usuario selecciona el documento firmado y presiona el botón respaldar, ingresa el usuario y contraseña de acceso al servidor FTP y respalda el documento, se genera automáticamente un código QR con la URL de acceso al documento.	
Resultado esperado: El usuario respalda el documento pdf firmado en el servidor FTP y se genera un QR en el documento, que contiene una URL de acceso al documento.	
Evaluación de prueba: Aceptada	

Tabla 3.64 *Prueba de aceptación para Historia de usuario 8*

Fuente*: Elaboración propia*

3.8.3.2 Pruebas unitarias

Pruebas unitarias al módulo de la historia de usuario 7 (Tabla 3.65):

Pruebas Unitarias	Módulo para desplegar la información de signatarios de documento pdf.
Prueba: 1	
Descripción: La información del signatario es desplegada en un nuevo dialogo, esta información esta contenida en la firma digital de un documento pdf.	
Objetivos: Comprobar lo siguiente: • Desplegar información solo de documentos firmados. • Mostrar todos los signatarios de un documento firmado.	
Condiciones: Saber usar la herramienta jUnit.	
Resultado Esperado: El módulo funcione correctamente.	
Resultado obtenido: El módulo funciona correctamente.	

Tabla 3.65 *Prueba unitaria Módulo de Historia de usuario 7*

Fuente*: Elaboración propia*

Prueba unitaria de módulo de historia de usuario 8 (Tabla 3.66).

Pruebas Unitarias	Módulo para respaldar documentos firmados.
Prueba: 1	
Descripción: El signatario selecciona el documento firmado a respaldar en el servidor FTP, para luego ser consultada desde el QR generado en el documento.	
Objetivos: Comprobar lo siguiente: • Generación de QR con URL de acceso a archivo correcto. • Respaldo de documento firmadoo	
Condiciones: Saber usar la herramienta jUnit.	
Resultado Esperado: El módulo funcione correctamente.	
Resultado obtenido: El módulo funciona correctamente.	

Tabla 3.66 *Prueba unitaria Módulo de Historia de usuario 8*

Fuente*: Elaboración propia*

3.9 Pruebas de Integración

Con las pruebas unitarias aceptadas de las iteraciones anteriores se procederá a realizar las pruebas de integración, estas pruebas se realizan para verificar que un gran conjunto de partes de software del sistema funcionan juntos.

La pruebas de integración serán de tipo no incremental , es decir que se combinaran todos los módulos desarrollados y probara todo el sistema en su conjunto.

A continuación se muestra la tabla de integración de los módulos desarrollados (Tabla 3.67):

Módulo	**Nro.**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**
Módulos para selección de tipo de almacenamiento.	**1**	X	X						
Módulos para firmar un documento pdf.	**2**	X	X	X	X	X	X		
Módulos para validación de certificado digital y consultas SSL a servidor OCSP y CRL.	**3**		X	X				X	

Módulos para visualizar documento pdf.	**4**		X		X	X			
Módulo para dibujar el área para marca de agua.	**5**		X		X	X	X		
Módulos obtener el sello de tiempo de un servidor TSA.	**6**		X	X			X	X	
Módulo para desplegar la información de signatarios de documento pdf.	**7**			X			X	X	
Módulo para respaldar documentos firmados.	**8**		X						X

Tabla 3.67 *Integración de Módulos*

Fuente*: Elaboración propia*