Índice de contenido

3MARCO APLICATIVO....3
3.1INTRODUCCIÓN....3
3.2PLANIFICACIÓN....3
3.2.1Historias de usuario....3
3.2.2Plan de entregas....17
3.3PRIMERA ITERACIÓN....18
3.3.1Diseño....18
3.3.1.1Tarjetas CRC....19
3.3.1.2Modelo estructural....21
3.3.2Codificación....21
3.3.2.1Pantallas muertas....21
3.3.3Pruebas....22
3.3.3.1Pruebas de aceptación....22
3.3.3.2Pruebas unitarias....23
3.4SEGUNDA ITERACIÓN....24
3.4.1Diseño....24
3.4.1.1Tarjetas CRC....24
3.4.1.2Modelo estructural....26
3.4.2Codificación....26
3.4.2.1Pantallas muertas....26
3.4.3Pruebas....28
3.4.3.1Pruebas de aceptación....28
3.4.3.2Pruebas unitarias....29
3.5TERCERA ITERACIÓN....29
3.5.1Diseño....30
3.5.1.1Tarjetas CRC....30
3.5.1.2Modelo estructural....31
3.5.2Codificación....31
3.5.2.1Pantallas muertas....31
3.5.3Pruebas....32
3.5.3.1Pruebas de aceptación....32
3.5.3.2Pruebas unitarias....33
3.6CUARTA ITERACIÓN....34
3.6.1Diseño....34
3.6.1.1Tarjetas CRC....34
3.6.1.2Modelo estructural....34
3.6.2Codificación....34
3.6.2.1Pantallas muertas....34
3.6.3Pruebas....34
3.6.3.1Pruebas de aceptación....34

3.6.3.2Pruebas unitarias....35
3.7QUINTA ITERACIÓN....36
3.7.1Diseño....36
3.7.1.1Tarjetas CRC....36
3.7.1.2Modelo estructural....36
3.7.2Codificación....36
3.7.2.1Pantallas muertas....36
3.7.3Pruebas....36
3.7.3.1Pruebas de aceptación....36
3.7.3.2Pruebas unitarias....37
3.8SEXTA ITERACIÓN....38
3.8.1Diseño....38
3.8.1.1Tarjetas CRC....38
3.8.1.2Modelo estructural....38
3.8.2Codificación....38
3.8.2.1Pantallas muertas....38
3.8.3Pruebas....38
3.8.3.1Pruebas de aceptación....38
3.8.3.2Pruebas unitarias....39

CAPITULO 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 por cada fase de la metodología de desarrollo XP, estos artefactos se desarrollaran para cada una de las seis iteración (Ver tabla 3.28) 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

Se formulan las siguientes historias de usuario de los requisitos obtenidos del ministerio para el desarrollo del sistema para 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 como también su par de claves, el acceso a la clave privada sera mediante una contraseña o pin que el usuario ingresara.

La historia de usuario 1 contara con tareas para crear el módulo, la interfaz para escoger tipo de firmado, como también 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, como también para acceder a un archivo 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 muestra el desarrollo del módulo para el acceso al dispositivo criptográfico que puede ser un token o smartcard, en este modulo usaremos la librería de java **sunpkcs11** que sigue las

especificaciones técnicas del estándar PKCS11 que especifica el acceso al dispositivo. 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*

La Tarjeta de Tarea 1.2 de Historia de usuario 1 se elabora una interfaz de manera sencilla para que 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 el 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*

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 o fichero pueden estar incluidos varios certificados 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 almacenada 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 (Hasheo); validación y verificación de certificado; y marca de agua de certificado.

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 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 firmado, 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 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 modulo en el cual se harán las consultas respectivas a los servidores del la entidad certificadora para verificar la validez del certificado, como también la vigencia de la misma. A continuación se describen las Tarjetas de Tarea correspondientes:

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 que dispondrá de un servidor OCSP y una archivo CRL para realizará las consultas correspondientes.	

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 un interfaz simple para el usuario, en el cual el usuario seleccionara si quiere realizar la consulta a un servidor OSCP y si quiere usar un CRL.

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 al cual se quiere 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 la marca de agua a pdf con la información del servidor publico.
Autor: Armin Mesa Sanchez	

Prioridad: Media	
Descripción: Se desarrolla un módulo para poder añadir una marca de agua con la información del servidor público a un documento pdf firmado.	

Tabla 3.17 *Historia de Usuario 5*

Fuente*: Elaboración propia*

En esta historia de usuario crearemos un módulo para añadir una marca de agua con la información del usuario, el usuario sera capaz de escoger la pagina donde que poner la marca de agua, así también podrá dibujar un rectángulo para asignar el tamaño de la marca de agua.

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 asignación de tamaño y ubicación de marca de agua a documento pdf.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realiza el módulo para dibujar un cuadrado en una pagina del documento pdf para poder añadir una marca de agua.	

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 pagina correspondiente donde el usuario desea añadir la marca de agua. En la pagina elegida el usuario dibujara un rectángulo para definir el tamaño de la marca de agua. Esta marca de agua contendrá una imagen QR con la URL de acceso a documento firmado, información del usuario, información extra y fecha de firmado.

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 módulo para adquirir el sello de tiempo de un servidor TSA para firmar un documento pdf. De esta forma se evitara el no repudio a un documento firmado.	

Tabla 3.19 *Historia de Usuario 6*

Fuente*: Elaboración propia*

La Historia de Usuario 6 es un módulo que realiza las consultas al servidor TSA para adquirir la fecha y hora exacta en la que se esta realizando a 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: Realiza el módulo para realizar las consultas al servidor TSA, para ver tipo de autenticación, las politicas 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 CE para poder adquirir la información de tiempo, en esta consulta se genera un hash de tipo SHA-1 y SHA-2 del documento pdf. La respuesta 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, el usuario tendrá la opción de escoger el tipo de autenticación, ingresar su OID correspondiente e ingresar el tipo de resumen que quiere 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 al cual puede puede usar para adquirir el sello de tiempo.

Ademas de estas opciones el usuario tendrá las opciones de añadir su OID para realizar las consultas, como también añadir el tipo de resumen que quiere usar para su documento pdf.

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

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 que sera procesada para ser mostrada al usuario de forma entendible.

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 módulo para obtener la información necesaria como ser: nombre del firmante, fecha de firmado,	

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 podra obtener la información del firmando como también la información del servidor TSA y OCSP.

Tarea	
Numero de Tarea: 7.2	**Numero de Historia:** 7
Nombre de tarea: Desarrollo de interfaz para mostrar información de pdf firmado.	
Tipo de tarea: Desarrollo	
Programador(a) Responsable: Armin Mesa Sanchez	
Descripción: Realizar el desarrollo de la interfaz para mostrar 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 firmante, como algunos aspectos importantes del documento pdf, como ser:

Historias de Usuario	
Numero: 8	**Nombre:** Almacenamiento del historial de firmas realizadas por los servidores públicos y generación QR de URL de acceso a documento pdf firmado.
Autor: Armin Mesa Sanchez	
Prioridad: Media	
Descripción: Se Desarrolla módulo para almacenar los documentos firmados por los usuarios, los documentos firmados incluirán un código QR que contendrán la ubicación del documento respaldado en un servidor ftp.	

Tabla 3.25 *Historia de Usuario 8*

Fuente*: Elaboración propia*

Esta historia de usuario (Tabla 3.25) se desarrollara para los casos en los que el documento tenga que ser impreso, como también para respaldar la información de los usuarios.

A continuación se describe las Tarjetas de Tarea correspondientes:

Tarea	
Numero de Tarea: 8.1	**Numero de Historia:** 8
Nombre de tarea: Desarrollo de modulo de introducción de usuario y contraseña.	
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 la información de documentos firmados en un servidor.	

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

Fuente*: Elaboración propia*

Esta tarea (Tabla 3.26) se desarrolla un módulo para que el usuario pueda añadir un usuario y contraseña, de esta forma almacenar la información del usuario, como también almacenar el historial de firmas realizadas.

Tarea	
Numero de Tarea: 8.2	**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 usuario ingrese un usuario y contraseña para realizar un respaldo de su documento firmado.	

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

Fuente*: Elaboración propia*

Para esta tarea (Tabla 3.27) se realizara una interfaz amigable con un boton en el cual el usuario indicara que documento quiere respaldar, para luego ingresar un usuario y contraseña para confirmar el respaldo.

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 3.28 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	2 Semanas	14/09/2015

	estado del certificado otorgado por la entidad certificadora para tener una constancia del estado del certificado.		
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. 7. Verificación de firmas digitales en documentos firmados, con formato PDF.	2 semanas	12/10/2015
Sexta	8. Almacenamiento del historial de firmas realizadas por los servidores públicos y generación QR de URL de acceso a documento pdf firmado.	2 Semanas	26/10/2015

Tabla 3.28 *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, es por esta razón que 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 3.29).

PKCS11	
Responsabilidad	**Colaboración**
• Usar librería SunPKCS11 para el acceso a token o smartcard. • Registrar acceso a token o smartcard. • Eliminar acceso a token o smartcard.	• Ninguna

Tabla 3.29 *Tarjeta CRC de la clase PKCS11*

Fuente: *Elaboración propia*

La tarjeta CRC de la clase keyStoreU (Tabla 3.30).

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 3.30 *Tarjeta CRC de la clase keyStoreU*

Fuente: *Elaboración propia*

La tarjeta CRC de la clase PropiedadesFirmaF (Tabla 3.31).

PropiedadesArchivoF

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

Tabla 3.31 *Tarjeta CRC de clase PropiedadesArchivoF*

Fuente*: Elaboración propia*

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

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

Tabla 3.32 *Tarjeta CRC de clase TipoAlmacenClaves*

Fuente*: Elaboración propia*

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

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

Tabla 3.33 *Tarjeta CRC de clase InfoClaveP*

Fuente*: Elaboración propia*

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

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

Tabla 3.34 *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) correspondientes a la historia de usuario 1 y definidas por las tarjetas CRC anteriormente diseñadas.

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 representado en las pantallas muertas que se muestran a continuación:

La siguiente interfaz (Figura) 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 (ver figura) 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 para que el usuario tenga un aspecto mas amigable de que certificado esta usando.
- 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.

Imagen 3.1 *Opciones de firma digital*

Fuente*: Elaboración propia*

3.3.3 Pruebas

Para 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 el 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 y diseño de interfaz para selección de tipo de almacenamiento y alias.	
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, ingresar el password correspondiente al estandar, obtener el alias del certificado y selección de 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 3.35 *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:	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

Tabla 3.36 *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 3.37).

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

Tabla 3.37 *Tarjeta CRC de clase Firmar*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase SeleccionarArchivo(Tabla 3.38).

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

Tabla 3.38 *tarjeta CRC de clase SeleccionarArchivo*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase PrincipalController(Tabla 3.39).

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

Tabla 3.39 *Tarjeta CRC de clase PrincipalController*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase PrincipalController(Tabla 3.39).

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

	• TipoAlmacenClaves • KeyStoreU

Tabla 3.40 *Tarjeta CRC de PrincipalController*

Fuente*: Elaboración propia*

3.4.1.2 Modelo estructural

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

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

La interfaces (Imagen 3.3 y 3.2) correspondientes al desarrollo de la historia usuario 2 son las siguientes:

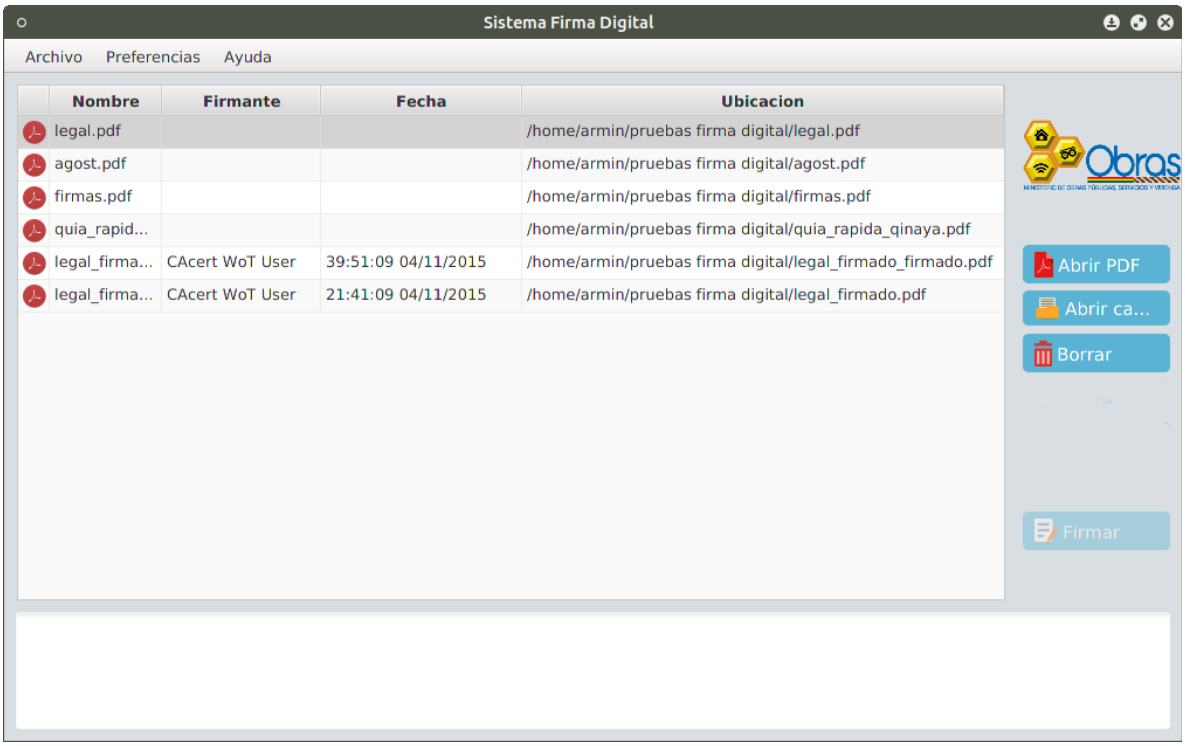

Imagen 3.2 *Carga de archivos pdf*

Fuente*: Elaboración propia*

Imagen 3.3 *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 opciones extras, 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 3.41 *Prueba de aceptación Historia de usuario 2*

Fuente*: Elaboración propia*

3.4.3.2 Pruebas unitarias

Se realizo la prueba unitaria (Tabla) 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 3.42 *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

3.5.1 Diseño

A continuación se desarrollan 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 3.43 *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 3.44 *Tarjeta CRC de clase InformacionCRL*

Fuente*: Elaboración propia*

La tarjeta CRC de la clase Firmar (Tabla 3.45) a la cual se le añaden nuevas responsabilidades.

Firmar	
Responsabilidad	**Colaboración**
• Firmar documento Pdf • Añadir opciones extras a firma digital.	• InformacionCRL • IniciarSSL • AlgoritmoHash

• Generar Hash de documento firmado. • Verificación y soporte de documento pdf. • Verificación entras salida de documento pdf. • Verificación de firma a servidor OSCP • Verificación de firma a documento CRL.	• AutenticacionServer • KeystoreU • OpcionesFirma • PKCS11 • InfoClaveP • TipoAlmacenClaves • PopiedadesArchivoF

Tabla 3.45 *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 .

3.5.2 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, Asi también se establecerá una conexión segura con dicho servidor para que las consultas no sean vulneradas.

Se muestran las capturas del desarrollo de la interfaz (Figura 3.45) para la historia de usuario 3.

3.5.2.1 Pantallas muertas

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

Imagen 3.4 *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 3.46) 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 para verificar la vigencia y validación de certificado digital.	
Resultado esperado: El usuario no podrá firmar un documento si el certificado digital si esta caducado o no vigente.	
Evaluación de prueba: Aceptada	

Tabla 3.46 *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 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:	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

Tabla 3.47 *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 la marca de agua con la información del servidor publico.

3.6.1 Diseño

3.6.1.1 Tarjetas CRC

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

3.6.1.2 Modelo estructural

3.6.2 Codificación

3.6.2.1 Pantallas muertas

3.6.3 Pruebas

3.6.3.1 Pruebas de aceptación

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 y diseño de interfaz para selección de tipo de almacenamiento y alias.	
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, ingresar el password correspondiente al estandar, obtener el alias del certificado y selección de 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	

3.6.3.2 Pruebas unitarias

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:	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

3.7 QUINTA ITERACIÓN

En esta iteración se desarrollaran la siguientes historian de usuario:

6. Incluir sello de tiempo de la entidad certificadora para los documentos firmados en formado pdf.
7. Verificación de firmas digitales en documentos firmados, con formato pdf.

3.7.1 Diseño

3.7.1.1 Tarjetas CRC

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

3.7.1.2 Modelo estructural

3.7.2 Codificación

3.7.2.1 Pantallas muertas

3.7.3 Pruebas

3.7.3.1 Pruebas de aceptación

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 y diseño de interfaz para selección de tipo de almacenamiento y alias.	
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, ingresar el password correspondiente al estandar, obtener el alias del certificado y selección de 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	

3.7.3.2 Pruebas unitarias

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:	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	

3.8 SEXTA ITERACIÓN

En esta iteración se desarrollaran la siguientes historian de usuario:

8. Almacenamiento del historial de firmas realizadas por los servidores públicos y generación QR de URL de acceso a documento pdf firmado.

3.8.1 Diseño

3.8.1.1 Tarjetas CRC

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

3.8.1.2 Modelo estructural

3.8.2 Codificación

3.8.2.1 Pantallas muertas

3.8.3 Pruebas

3.8.3.1 Pruebas de aceptación

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 y diseño de interfaz para selección de tipo de almacenamiento y alias.	
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, ingresar el password correspondiente al estandar, obtener el alias del certificado y selección de 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	

3.8.3.2 Pruebas unitarias

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:	
Resultado Esperado: Los módulos funcionen correctamente.	
Resultado obtenido: Los módulos funcionan correctamente.	