



ESPE

UNIVERSIDAD DE LAS FUERZAS ARMADAS
INNOVACIÓN PARA LA EXCELENCIA

**DEPARTAMENTO DE CIENCIAS DE LA
COMPUTACIÓN**

**CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN
(SISTEMAS E INFORMÁTICA)**

**TRABAJO DE TITULACIÓN PREVIO A LA OBTENCIÓN DEL
TÍTULO DE INGENIERO EN SISTEMAS E INFORMÁTICA**

**TEMA: DESARROLLO DE UNA APLICACION WEB DE TIME
STAMPING PARA EL PROCESO DE FACTORING
ELECTRÓNICO EN EL ECUADOR APLICADO EN LA
EMPRESA BIGDATA C.A**

AUTOR: MENDOZA MACIAS, JESÚS IVÁN

DIRECTOR: SANG GUUN YOO, PH.D.

SANGOLQUÍ

2017

CERTIFICADO**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN****CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA****CERTIFICACIÓN**

Certifico que el trabajo de titulación, “**DESARROLLO DE UNA APLICACION WEB DE TIME STAMPING PARA EL PROCESO DE FACTORING ELECTRÓNICO EN EL ECUADOR APLICADO EN LA EMPRESA BIGDATA C.A**” realizado por el señor Jesús Iván Mendoza Macías, ha sido revisado en su totalidad y analizado por el software anti-plagio, el mismo cumple con requisitos teóricos, científicos, técnicos, metodológicos y legales establecidos por la Universidad de las Fuerzas Armadas ESPE, por lo tanto me permito acreditarlo y autorizar al señor Jesús Iván Mendoza Macías para que lo sustente públicamente.

Sangolquí, 18 de octubre del 2017

Atentamente,

Director: Sang Guun Yoo, Ph.D.

AUTORÍA**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN****CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA****AUTORÍA DE RESPONSABILIDAD**

Yo, JESÚS IVÁN MENDOZA MACIAS, con cédula de identidad N°1719973016, declaro que este trabajo de titulación "DESARROLLO DE UNA APLICACION WEB DE TIME STAMPING PARA EL PROCESO DE FACTORING ELECTRÓNICO EN EL ECUADOR APLICADO EN LA EMPRESA BIGDATA C.A" ha sido desarrollado considerando los métodos de investigación existentes, así como también se ha respetado los derechos intelectuales de terceros considerándose en las citas bibliográficas.

Consecuentemente declaro que este trabajo es de mi autoría, en virtud de ello me declaro responsable del contenido, veracidad y alcance de la investigación mencionada.

Sangolquí, 08 de noviembre del 2017

JESÚS IVÁN MENDOZA MACIAS

CC:1719973016

AUTORIZACIÓN**DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN****CARRERA DE INGENIERÍA DE SISTEMAS E INFORMÁTICA****AUTORIZACIÓN**

Yo, JESÚS IVÁN MENDOZA MACIAS, autorizo a la Universidad de las Fuerzas Armadas ESPE publicar en la biblioteca virtual de la institución el presente trabajo "DESARROLLO DE UNA APLICACION WEB DE TIME STAMPING PARA EL PROCESO DE FACTORING ELECTRÓNICO EN EL ECUADOR APLICADO EN LA EMPRESA BIGDATA C.A" cuyo contenido, ideas y criterios son de mi autoría y responsabilidad.

Sangolquí, 08 de noviembre del 2017

JESÚS IVÁN MENDOZA MACÍAS

CC:1719973016

DEDICATORIA

El presente proyecto va dedicado a mis padres, por su esfuerzo y constante apoyo a lo largo de esta etapa.

AGRADECIMIENTO

A mis padres, hermanos y amigos por haberme brindado su constante apoyo y consejos.

A los Ingenieros Sang Guun Yoo y Walter Fuertes, por su esfuerzo y dedicación, quien con sus conocimientos, su experiencia y su paciencia, hicieron posible culminar esta etapa de mi vida.

ÍNDICE DE CONTENIDO

CERTIFICADO	i
AUTORÍA	ii
AUTORIZACIÓN	iii
DEDICATORIA.....	iv
AGRADECIMIENTO	v
CAPÍTULO I.....	1
INTRODUCCIÓN	1
1.1. PLANTEAMIENTO DEL PROBLEMA	2
1.2. JUSTIFICACIÓN E IMPORTANCIA	3
1.3. OBJETIVOS	4
1.3.1. OBJETIVO GENERAL.....	4
1.3.2. OBJETIVOS ESPECÍFICOS	4
1.4. ALCANCE	5
CAPÍTULO II.....	6
2.1 FIRMA ELECTRÓNICA	6
2.1.1 Documentos en los cuales se puede usar una firma electrónica.....	8
2.1.2 Formatos de firma.....	8
2.1.3 Validez de una firma electrónica	9
2.2 FORMAS DE FIRMA BAJO EL FORMATO XADES	10
2.2.1 Firma Electrónica Básica (XAdES-BES).....	10
2.2.2 Firma Electrónica basada en la Política Explícita (XAdES-EPES).....	11
2.2.3 Firma Electrónica con Datos de Validación XAdES-T	11
2.2.4 Firma Electrónica con Datos de Validación XAdES-C.....	11
2.3 CERTIFICADO DE FIRMA ELECTRÓNICA.....	11
2.3.1 Solicitud de certificado de firma electrónica	12
2.3.1.1 Proceso de solicitud de certificado de firma electrónica en la AC del Banco Central del Ecuador	13
2.3.1.2 Proceso de solicitud de certificado de firma electrónica en la AC Security Data	14
2.3.1.3 Proceso de solicitud de certificado de firma electrónica en la AC del Consejo de la Judicatura.....	16
2.4 ONLINE CERTIFICATE STATUS PROTOCOL	17
2.5 CERTIFICATE REVOCATION LIST.....	18
2.6 AUTORIDAD DE SELLADO DE TIEMPO (TSA)	18
2.7 SELLADO DE TIEMPO O TIME-STAMPING	19

2.7.1	Proceso contratación del servicio de sellos de tiempo con la TSA del Banco Central del Ecuador	20
2.8	SELLOS DE TIEMPO Y SU RELACIÓN CON FIRMA ELECTRÓNICA.....	21
2.9	COMPROBANTES ELECTRÓNICOS	21
2.10	XMLDigSig	23
2.11	ALGORITMO RSA	24
2.12	FACTORING.....	24
2.11.1	Factoring Convencional	25
2.11.2	Factoring Electrónico	26
2.13	Unified Modelling Language.....	27
2.14	METODOLOGÍA Y HERRAMIENTAS DE DESARROLLO.....	28
2.13.1	UML-based Web Engineering	28
2.13.2	NetBeans IDE	29
2.13.3	Java y Java Enterprise Edition.....	29
2.13.4	Apache Tomcat.....	30
2.13.5	Java Server Faces	30
2.13.6	PrimeFaces	30
2.13.7	PolygonESL-2.0.....	30
2.13.8	MariaDB.....	30
2.13.9	Hibernate.....	31
2.13.10	ERS.....	31
	CAPÍTULO III.....	32
3.1	PROCESO ACTUAL DE FACTORING ELECTRÓNICO IMPLEMENTADO POR BIGDATA CA.....	32
3.2	ANÁLISIS Y DISEÑO DE LA APLICACIÓN WEB DE TIME STAMPING	37
3.2.1	Análisis de requerimientos	37
3.2.1.1	Registro de usuario (RF01).....	37
3.2.1.2	Autenticación de usuario (RF02)	38
3.2.1.3	Solicitar nueva contraseña (RF03)	38
3.2.1.4	Recordar nombre de usuario (RF04).....	39
3.2.1.5	Actualizar información de usuario (RF05).....	39
3.2.1.6	Firmar y sellar documentos en formato XML (RF06).....	39
3.2.1.7	Repositorio de documentos firmados (RF07).....	40
3.2.1.8	Actualizar parámetros de la aplicación (RF08).....	40
3.2.1.9	Interfaz de la aplicación (RNF01)	40

3.2.1.10	Conexión a internet del dispositivo donde se use la aplicación (RNF02)	41
3.2.1.11	Seguridad de la información (RNF03)	41
3.2.1.12	PIN del certificado (RNF04)	41
3.2.1.13	Otros requisitos	41
3.2.2	Diseño del proceso de firma electrónica y sellado de tiempo para la aplicación Web de Time Stamping	41
3.2.2.1	Proceso de la aplicación	41
3.2.3	Diagramas de Casos de Uso	42
3.2.3.1	Definición de Actores del Sistema	42
3.2.3.2	Definición de tareas por actor	43
3.2.3.3	Diagrama de caso de uso general	43
3.2.4	Descripción de Casos de Uso	44
3.2.4.1	Caso de uso Registrarse	44
3.2.4.2	Caso de uso Autenticarse	44
3.2.4.3	Caso de uso Solicitar nueva contraseña	45
3.2.4.4	Caso de uso Recordar nombre de usuario	46
3.2.4.5	Caso de uso Actualizar información	46
3.2.4.6	Caso de uso Firmar y sellar documento XML	47
3.2.4.7	Caso de uso Repositorio de documentos	48
3.2.4.8	Caso de uso Actualizar parámetros de la aplicación	48
3.2.5	Diagramas de Secuencia	49
3.2.5.1	Diagrama de secuencia "Registro de usuario"	49
3.2.5.2	Diagrama de secuencia "Autenticación de usuario"	50
3.2.5.3	Diagrama de secuencia "Solicitar nueva contraseña"	51
3.2.5.4	Diagrama de secuencia "Recordar nombre usuario"	51
3.2.5.5	Diagrama de secuencia "Actualizar información"	52
3.2.5.6	Diagrama de secuencia "Firmar y sellar documento XML"	52
3.2.5.7	Diagrama de secuencia "Repositorio Documentos"	53
3.2.5.8	Diagrama de secuencia "Actualizar parámetros de la aplicación"	53
3.2.6	Diagramas de Actividades	54
3.2.6.1	Diagrama de actividad "Registro de usuario"	54
3.2.6.2	Diagrama de actividad "Autenticación de usuario"	54
3.2.6.3	Diagrama de actividad "Solicitar nueva contraseña"	55
3.2.6.4	Diagrama de actividad "Recordar nombre de usuario"	55
3.2.6.5	Diagrama de actividad "Actualizar información"	55

3.2.6.6	Diagrama de actividad “Firmar y sellar documento XML”	56
3.2.6.7	Diagrama de actividad “Repositorio documentos”	57
3.2.6.8	Diagrama de actividad “Visualizar detalle de firma y sello de tiempo”	57
3.2.6.9	Diagrama de actividad “Actualizar parámetros de la aplicación”	58
3.2.7	Diagrama de Despliegue	58
3.2.8	Modelo de datos	59
3.2.8.1	Modelo conceptual de base de datos	59
3.2.8.2	Modelo lógico de base de datos	59
3.2.8.3	Modelo físico de base de datos	60
3.2.9	Diagramas navegación	61
3.2.9.1	Diagrama de navegación usuario general	61
3.2.9.2	Diagrama de navegación usuario administrador	61
CAPÍTULO IV		62
4.1	IMPLEMENTACIÓN DE LA APLICACIÓN WEB DE TIME STAMPING	62
4.1.1	Script de base de datos	62
4.1.2	Paquetes y clases la aplicación	62
4.1.3	Ejecución de la aplicación	64
4.1.4	Casos de Pruebas	69
4.1.5	Pruebas adicionales	76
4.1.5.1	Prueba de contenido	77
4.1.5.2	Prueba de interfaz	78
4.1.5.3	Prueba de navegación	78
4.1.5.4	Prueba de componentes	79
4.2	ADAPTACIÓN DE LA FUNCIONALIDAD DE FIRMA Y SELLADO DE TIEMPO EN EL SISTEMA DE FACTORING ELECTRÓNICO DESARROLLADO POR LA EMPRESA BIGDATA C.A	80
4.2.1	Selección del paquete del sistema de Factoring Electrónico donde se adaptó el proceso de firma y sellado de tiempo de la aplicación de Time Stamping	80
4.2.2	Clase FacturasConfirmarDeudorBean.java	81
4.2.3	Clase ConfirmarVentaFacturaVendedorBean.java	82
CAPÍTULO V		84
RESULTADOS OBTENIDOS, CONCLUSIONES Y RECOMENDACIONES		84
5.1	RESULTADOS OBTENIDOS	84
5.2	CONCLUSIONES	85

5.3	RECOMENDACIONES.....	86
	BIBLIOGRAFÍA Y WEBGRAFÍA.....	88

ÍNDICE DE TABLAS

Tabla 1 Estructura de una firma bajo XMLDSIG	23
Tabla 2 Estructura del documento de confirmación de pago del paso 2.....	34
Tabla 3 Estructura del documento de cesión de la factura del paso 5.....	35
Tabla 4 Descripción caso de uso “Registrarse”	44
Tabla 5 Descripción caso de uso “Autenticarse”	44
Tabla 6 Descripción caso de uso “Solicitar nueva contraseña”	45
Tabla 7 Descripción caso de uso “Recordar nombre de usuario”	46
Tabla 8 Descripción caso de uso “Actualizar información”	46
Tabla 9 Descripción caso de uso “Firmar y sellar documento XML”	47
Tabla 10 Descripción caso de uso “Repositorio de documentos”	48
Tabla 11 Descripción caso de uso “Actualizar parámetros de la aplicación”	48
Tabla 12 Paquete Bean	62
Tabla 13 Paquete Configuraciones	63
Tabla 14 Paquete Dao	63
Tabla 15 Paquete Firma	63
Tabla 16 Paquete Modelo	63
Tabla 17 Paquete Utilidades	64
Tabla 18 Descripción caso de prueba “Registro de usuario”	69
Tabla 19 Descripción caso de prueba “Autenticación de usuario”	70
Tabla 20 Descripción caso de prueba “Solicitar nueva contraseña”	71
Tabla 21 Descripción caso de prueba “Recordar nombre de usuario”	71
Tabla 22 Descripción caso de prueba “Actualizar información de usuario” .	72
Tabla 23 Descripción caso de prueba “Firmar y sellar documentos XML” ...	73
Tabla 24 Descripción caso de prueba “Repositorio de documentos”	74
Tabla 25 Descripción caso de prueba “Actualizar parámetros de la aplicación”	75
Tabla 26 Prueba de contenido	77
Tabla 27 Prueba de interfaz	78
Tabla 28 Prueba de Navegación	79
Tabla 29 Prueba de componentes	79

Tabla 30 Comparación documentos XML sin firma, con firma y con firma en conjunto son sellos de tiempo	84
---	----

ÍNDICE DE FIGURAS

Figura 1 Proceso de firma electrónica	7
Figura 2 Proceso básico de validación de un certificado	18
Figura 3 Primer mecanismo de consumo de sellos de tiempo.....	19
Figura 4 Segundo mecanismo de consumo de sellos de tiempo	20
Figura 5 Proceso de firma con Sello de Tiempo	21
Figura 6 Especificaciones técnicas relacionadas al estándar XadES_BES.	22
Figura 7 Modelo Factoring convencional	26
Figura 8 Principales modelos de la metodología UWE	29
Figura 9 Proceso Factoring Electrónico Empresa BIGDATA C.A	33
Figura 10 Ejemplo del documento de confirmación de pago del paso 2.....	36
Figura 11 Ejemplo del documento de cesión de la factura del paso 5.....	37
Figura 12 Proceso para la aplicación Web de Time Stamping.....	42
Figura 13 Definición de actores	42
Figura 14 Diagrama de caso de uso general	43
Figura 15 Diagrama de secuencia Registrar usuario	50
Figura 16 Diagrama de secuencia Autenticar usuario	50
Figura 17 Diagrama de Solicitar nueva contraseña	51
Figura 18 Diagrama de secuencia Recordar nombre usuario.....	51
Figura 19 Diagrama de secuencia Actualizar información	52
Figura 20 Diagrama de secuencia Firmar y sellar documento XML.....	52
Figura 21 Diagrama de secuencia Repositorio documentos.....	53
Figura 22 Diagrama de secuencia Actualizar parámetros de la aplicación..	53
Figura 23 Diagrama de actividad Registro de usuario	54
Figura 24 Diagrama de actividad Autenticación de usuario	54
Figura 25 Diagrama de actividad Solicitar nueva contraseña	55
Figura 26 Diagrama de actividad Recordar nombre de usuario.....	55
Figura 27 Diagrama de Actualizar información	56
Figura 28 Diagrama de actividad Firmar y sellar documento XML.....	56
Figura 29 Diagrama de actividad Repositorio documentos.....	57
Figura 30 Diagrama de actividad Visualizar detalle firma y sello de tiempo	57
Figura 31 Diagrama de actividad Actualizar parámetros de la aplicación....	58

Figura 32 Diagrama de despliegue	59
Figura 33 Modelo conceptual de Base Datos	59
Figura 34 Modelo lógico de Base Datos	60
Figura 35 Modelo físico de Base Datos	60
Figura 36 Diagrama de navegación usuario general	61
Figura 37 Diagrama de navegación usuario administrador.....	61
Figura 38 Paquetes creados para la aplicación	62
Figura 39 Página de registro para nuevo usuario	65
Figura 40 Página de inicio de sesión	65
Figura 41 Página principal de la aplicación.....	66
Figura 42 Página de actualización de parámetros	66
Figura 43 Página de firma y sellado de tiempo.....	67
Figura 44 Página de repositorio de documentos firmados	67
Figura 45 Página de repositorio de documentos firmados.....	68
Figura 46 Página para recordar nombre de usuario	68
Figura 47 Proceso de pruebas de aplicaciones Web.....	77
Figura 48 Distribución de paquetes del sistema de Factoring Electrónico...	80
Figura 49 Clases en las cuales se adoptó el proceso de firma y sellado de tiempo para el sistema de Factoring Electrónico	81
Figura 50 Interfaz de facturas pendientes de confirmación de pago en el sistema de Factoring Electrónico.....	82
Figura 51 Interfaz de firma y sellado de tiempo de la confirmación de pago de una factura en el sistema de Factoring Electrónico	82
Figura 52 Interfaz de facturas pendientes de confirmación de venta en el sistema de Factoring Electrónico.....	83
Figura 53 Interfaz de firma y sellado de tiempo de la confirmación de venta de una factura en el sistema de Factoring Electrónico	83

RESUMEN

Este documento describe la experiencia en desarrollar una aplicación de Time Stamping para el proceso de Factoring Electrónico en el Ecuador, la cual permite realizar el proceso de firma electrónica con sello de tiempo en documentos en formato XML, la necesidad de contar con esta aplicación tiene su origen en una plataforma de Factoring Electrónico desarrollada por la empresa BIGDATA C.A, donde se buscaba contar con un mecanismo que permita garantizar la integridad y validez de la información a través del tiempo de ciertos documentos generados por el sistema. Se empleó la metodología UWE por su enfoque a procesos, obtención de requisitos, y soporte con herramientas CASE que brindan apoyo para el tratamiento de los mismos, permitiendo así desarrollar aplicaciones de mejor calidad. La utilización de firmas electrónica en conjunto con los sellos de tiempo, permitió brindar mayor validez jurídica e integridad a la información contenida en los documentos firmados, para que puedan ser usados en procesos judiciales o para evitar la alteración de los mismos, el uso de estos dos mecanismos contribuyó a dar mayor seguridad y agilidad al proceso de Factoring Electrónico, ya que el proceso de firma ahora se realiza en un ambiente totalmente en línea y no de manera manual como se venía realizando.

Palabras Clave:

- **TIME STAMPING**
- **UWE**
- **FACTORING**
- **XML**

ABSTRACT

This document describes the experience in developing a Time Stamping application for the Electronic Factoring process in Ecuador, which allows the process of electronic signature with time stamp in documents in XML format, the need to have this application has its origin in an Electronic Factoring platform developed by the company BIGDATA CA, where it was sought to have a mechanism that allows to guarantee the integrity and validity of the information over time of certain documents generated by the system. The UWE methodology was used for its approach to processes, obtaining requirements, and support with CASE tools that provide support for the treatment of the same, allowing to develop applications of better quality. The use of electronic signatures in conjunction with time stamps allowed greater legal validity and integrity to the information contained in the signed documents, so that they can be used in judicial proceedings or to avoid alteration of the same, the use of these Two mechanisms contributed to give greater security and agility to the process of Electronic Factoring, since the process of signing now is done in an entirely online environment and not in a manual way as it was being done.

KeyWords:

- **TIME STAMPING**
- **UWE**
- **FACTORING**
- **XML**

CAPÍTULO I

INTRODUCCIÓN

El uso de las tecnologías de la información ha crecido enormemente en los últimos años tanto en Ecuador como en el mundo entero, y cada día juega un papel más importante en la sociedad, tanto ayudando a tener un mayor desenvolvimiento a las actividades de las empresas, como reduciendo considerablemente el uso de recursos y por ende aumentando la productividad de sus procesos.

Uno de los hitos más importantes relacionados a las tecnologías de la información en Ecuador, es el uso del certificado de firma electrónica, el mismo que garantiza la validez de la identidad de una persona, organización o máquina (Hrvoje, Boris, & Hrvoje, 2013). Una de las principales aplicaciones de los certificados de firma electrónica en nuestro país es la facturación electrónica, la misma que ha sido implementada extendidamente hasta que ha reemplazado casi por completo la facturación tradicional basada en facturas físicas (Muñoz Guerrero, 2013). El uso de los certificados de firma electrónica no se limita únicamente al proceso de facturación electrónica; su uso también se aplica a la firma de correos electrónicos y documentos digitales (por ejemplo PDF, archivos de texto, hojas de cálculo), para garantizar la autenticidad, integridad y no repudio de los mismos (ECIBCE, 2016).

Un valor adicional que hace a la firma electrónica aún más confiable y segura es el uso de sello de tiempo (Time Stamping). Su uso permite probar que un conjunto de datos existió antes del momento del sellado y que los mismos no han sido modificados desde entonces (Buldas, Laud, Lipmaa, & Villemson, 1998; Wallace, Pordesch, & Brandner, 2007). El sellado de tiempo se vuelve necesario ya que la firma electrónica por sí misma no proporciona la confiabilidad y seguridad del momento de creación de la misma, puesto que la fecha de la computadora o servidor del firmante puede ser alterada; en esta situación, lo recomendable sería que la marca de tiempo que forma parte de la firma sea proporcionada por una fuente confiable, como una Autoridad de

Sellado de Tiempo, TSA (Time Stamping Authority, por sus siglas en inglés) (Días, Macia, Molinari, Venosa, & Sabolansky, 2010).

Tomando en cuenta los beneficios que aportan el sello de tiempo en conjunto con la firma electrónica, la empresa BIGDATA C.A ha decidido incorporar estos elementos en una plataforma de Factoring Electrónico, la cual es una herramienta en línea que permitirá a los proveedores realizar el cobro anticipado de sus facturas a cambio de un porcentaje de descuento aplicado a las mismas, obteniendo así liquidez inmediata sin afectar la relación cliente-proveedor (Camara de comercio de Ambato, 2016). Durante el proceso de Factoring se generan ciertos documentos, a los cuales se desea brindar mayor seguridad jurídica para que puedan ser usados como evidencia ante posibles procesos legales o judiciales donde se desee demostrar su integridad.

1.1. PLANTEAMIENTO DEL PROBLEMA

En los últimos años el uso de firmas electrónicas ha ido creciendo en Ecuador, esto se debe principalmente a la implementación de facturación electrónica impulsada por el Servicio de Rentas Internas (SRI), la misma que ha tomado mucha fuerza, y hoy por hoy es una obligación para la mayoría de contribuyentes, tanto del sector público como privado y se encuentra en constante crecimiento debido a los beneficios que aporta para las empresas y para el país (SRI, 2016).

BIGDATA C.A es una empresa dedicada al análisis, diseño e implementación de soluciones informáticas, especialmente en el área de facturación electrónica, actualmente cuenta con un sistema de Factoring Electrónico orientado a la Web de su propia autoría, el cual se especializa en la comercialización de facturas electrónicas autorizadas por el SRI. En cada proceso de Factoring se generan varios documentos donde se detallan la información, compromisos u obligaciones adquiridas de cada uno de los actores involucrados (vendedor, comprador y confirmador)¹.

¹ Actores involucrados:

Vendedor.- Sube facturas emitidas a sus clientes al sistema, para luego ser vendidas.

Como condición inicial para un proceso de Factoring Electrónico se requiere la emisión de una factura a crédito a un cliente, para que esta sea almacenada en el sistema, posteriormente el vendedor deberá solicitar la confirmación del compromiso de pago de la misma a la empresa deudora, para luego iniciar una negociación con una entidad financiera (comprador), la cual aplicará un porcentaje de descuento en base al monto y la fecha de pago de la factura, una vez aceptado descuento la empresa vendedora procederá a ceder los derechos de cobro del comprobante electrónico y el comprador procederá a pagar el valor acordado por la factura negociada a la empresa vendedora, mientras el sistema notificará a la empresa deudora el nuevo propietario de la factura, a quien deberá realizar el pago de la misma en la fecha previamente acordada, dando así por finalizado el proceso.

La empresa prevé que los documentos generados en el proceso de Factoring Electrónico puedan ser usados en juicios o demandas ante intentos de estafas o incumplimiento de las obligaciones adquiridas (como faltas de pago o pagos atrasados), razón por la cual es preciso que dichos documentos garanticen el no repudio de la información contenida en ellos a través del tiempo.

1.2. JUSTIFICACIÓN E IMPORTANCIA

Actualmente el sistema de Factoring Electrónico desarrollado por la empresa BIGDATA C.A no cuenta con un mecanismo de seguridad que permita garantizar la integridad de los documentos generados en el proceso de Factoring, lo que sin duda puede generar complicaciones en casos donde sea necesario utilizar dichos documentos como evidencia para proceso judiciales, motivo por la cual la empresa ha visto la necesidad de brindar mayor confianza y seguridad jurídica a estos documentos.

Por las razones expresadas anteriormente la empresa ha decidido incorporar el uso de firmas electrónicas y sellos de tiempo para la firma de los

Comprador.- Compra facturas subidas por el vendedor, aplicando un porcentaje de descuento a las mismas, generalmente este actor es una entidad financiera.

Confirmador.- Es el deudor de las facturas, debe confirmar el pago de las facturas que han sido cargadas por el vendedor.

documentos generados por su sistema para brindar una mayor seguridad jurídica a los mismos, dado que permitirá garantizar que los documentos generados fueron firmados por una persona en una fecha y hora determinada, obteniendo estos dos últimos datos de una fuente confiable, como puede ser una Autoridad de Sellado de Tiempo (TSA).

La investigación y resultados obtenidos en este proyecto permitirán beneficiar a otras personas o empresas que cuenten con sistemas o procesos similares, donde deseen garantizar la validez de los documentos generados a través del tiempo y disminuir el riesgo de que estos sean desestimados ante posibles procesos judiciales.

Para el desarrollo del presente proyecto se ha tomado como referencia la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos vigente en el Ecuador, que regula este tipo de procesos (SRI, 2016).

1.3. OBJETIVOS

1.3.1. OBJETIVO GENERAL

- Desarrollar una aplicación Web de Time Stamping para el proceso de Factoring Electrónico en el Ecuador aplicado en la empresa BIGDATA C.A.

1.3.2. OBJETIVOS ESPECÍFICOS

- Conocer los formatos existentes de firma electrónica y determinar cuál es el más adecuado para ser usado en el actual proceso de Factoring Electrónico en Ecuador.
- Determinar el proceso que se debe seguir con la Autoridad de Certificación y la Autoridad de Sellado de Tiempo para poder hacer uso de firmas electrónicas y sellos de tiempo.
- Implementar una aplicación Web para realizar los procesos de firma electrónica y sello de tiempo (Time Stamping) en documentos electrónicos.
- Adaptar la funcionalidad de firma y sellos de tiempo del aplicativo Web implementado, en el proceso de Factoring Electrónico aplicado en la empresa BIGDATA C.A.

- Establecer conclusiones y recomendaciones de los resultados obtenidos en el presente proyecto.

1.4. ALCANCE

El tema “Desarrollo de una aplicación Web de Time Stamping para el proceso de Factoring Electrónico en el Ecuador aplicado en la empresa BIGDATA C.A”, comprende el proceso desde la etapa de investigación y análisis de los sellos de tiempo y de los diferentes formatos de firmas electrónicas, pasando por la selección de la forma de firma que en conjunto con los sellos de tiempo permitan brindar mayor seguridad jurídica a los documentos generados, hasta la implementación de una aplicación Web para realizar el proceso de firma electrónica y sellado de tiempo, para su posterior adaptación en el actual proceso de Factoring Electrónico desarrollado por la empresa BIGDATA C.A.

La aplicación Web de sellado de tiempo será desarrollada en el lenguaje de programación Java 7, sobre el sistema operativo Windows 10, utilizando NetBeans 7.4 y Apache Tomcat 7.0.41 como contenedor de la aplicación, con la finalidad de tener compatibilidad con el sistema de Factoring Electrónico desarrollado por la empresa.

CAPÍTULO II

MARCO TEÓRICO

2.1 FIRMA ELECTRÓNICA

Una firma electrónica es un patrón de bits que depende del mensaje que se está firmando y utiliza alguna información única para el firmante. El mensaje es cifrado mediante una función hash para obtener un resumen del mismo. El valor del hash es cifrado usando la clave privada del firmante, y el resultado de ese proceso es la firma electrónica (Maykin & Pramote, 2012).

Según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos vigente en Ecuador, en el artículo número 13, define a la firma electrónica como: “los datos en forma electrónica consignados en un mensaje de datos, adjuntados o lógicamente asociados al mismo, y que puedan ser utilizados para identificar al titular de la firma en relación con el mensaje de datos, e indicar que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos” (SRI, 2016).

Maykin Warasart y Pramote Kuacharoen (Maykin & Pramote, 2012) detallan las siguientes propiedades de una firma electrónica:

- **Autenticación:** El valor hash del mensaje original está encriptado con la clave privada del remitente que sólo es conocida por el remitente. Por lo tanto, una firma válida implica que el mensaje fue creado por el remitente. La clave pública correspondiente se utiliza para verificar la firma. Si la firma no es válida, el destinatario no puede dar como auténtico el mensaje.
- **Integridad:** El valor del hash cifrado sirve como una huella digital del mensaje. Si el mensaje ha sido alterado, es muy probable que el valor de hash sea diferente ya que es imposible encontrar otro mensaje que tenga el mismo valor de hash. Sin embargo el valor hash criptográfico debe estar protegido, caso contrario un atacante puede modificar el mensaje y regenerar el valor de hash correspondiente. En el proceso de creación de la firma digital, el

valor de cifrado criptográfico se cifra con la clave privada del remitente. Es imposible que un atacante modifique el mensaje y la firma de tal manera que sea válido sin el conocimiento de la clave privada del remitente. Por lo tanto, se conserva la integridad del mensaje.

- **No repudio:** La clave privada y la clave pública están relacionadas matemáticamente. La información cifrada con la clave privada sólo se puede descifrar con la clave pública correspondiente, dado que el remitente firmó el mensaje con la clave privada y se verifica la firma utilizando la clave pública del mismo, de esta manera que el remitente no puede negar haber firmado el mensaje.

Al hacer uso de la firma electrónica, ya no es necesaria la presencia física del firmante en un determinado lugar ni largas esperas para realizar la firma, puesto que el trámite se lo puede hacer de manera remota desde el lugar donde uno se encuentre, siempre y cuando se disponga de un dispositivo y una aplicación que permitan realizar el proceso de firma, lo que sin duda genera una gran variedad de nuevas formas de realización de trámites públicos y privados que pueden realizarse digitalmente y con mayor seguridad y comodidad. A continuación se ilustra proceso de firma electrónica (ver Figura 1) (Paulin, Robledo, & Brusa, 2014).

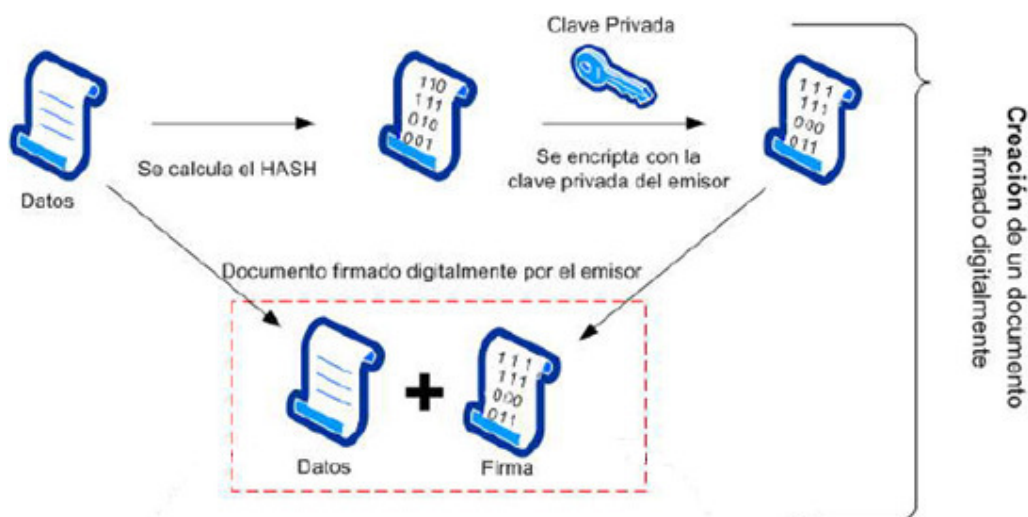


Figura 1 Proceso de firma electrónica

Fuente: (Paulin *et al*, 2014)

En resumen el proceso de firma electrónica es el siguiente:

Primero se debe obtener un resumen hash del archivo a firmar (utilizando cualquier algoritmo estándar como MD5, SHA1, SHA2, etc.), para luego ser cifrado con la clave privada, dando como resultado la firma digital del archivo. De esta manera si uno descifra la firma digital con su clave pública, obtendrá el hash original del archivo, si este hash difiere del hash original el documento ha sido alterado, caso contrario el documento es el original (Vinod Moreshwar , 2012).

En Ecuador el principal uso de las firmas electrónicas se da en el proceso de facturación electrónica impulsado por el SRI, en el cual se generan los siguientes documentos: facturas, notas de crédito, notas de débito, comprobantes de retención y guías de remisión, los mismos que deben ser previamente firmados electrónicamente por los emisores, para su posterior validación y autorización por parte del SRI.

2.1.1 Documentos en los cuales se puede usar una firma electrónica

La firma electrónica puede ser utilizada para firmar de forma electrónica: contratos electrónicos, transacciones electrónicas, correos electrónicos, ofertas del Sistema Nacional de Contratación Pública, facturas electrónicas, trámites tributarios electrónicos u otro tipo de aplicaciones en las cuales sea posible reemplazar la firma manuscrita y se encuentre facultado para hacerlo dentro del ámbito de su actividad o límites de su uso (ECIBCE, 2016).

2.1.2 Formatos de firma

El formato de firma electrónica es la manera en la que es generado el documento de firma y en cómo se almacena o estructura la información de la firma en el documento, la existencia de diferentes formatos de firma se debe a razones históricas, a cómo se ha ido introduciendo la firma en formatos de documentos ya existentes y en cómo se han ido agregando funcionalidades a lo largo del tiempo, entre los principales formatos de firma de acuerdo al tipo de archivo, tenemos los siguientes: CAdES, XAdES y PAdES (PAE, 2016):

- **CAdES** (CMS Advanced Electronic Signatures).

- Consiste en la evolución del primer formato de firma electrónica estandarizado. Su uso es adecuado para firmar archivos de gran tamaño, especialmente si la firma abarca el documento original, ya que optimiza el espacio de la información. Una vez realizada la firma no se podrá ver la información original, ya que está es guardada de forma binaria (PAE, 2016; Hrvoje *et al*, 2013).
- **XAdES** (XML Advanced Electronic Signature).
 - El resultado de este tipo de firma es un archivo de texto XML, en un formato de texto muy similar al HTML que utiliza etiquetas. Los documentos generados suelen ser de mayor tamaño que los generados con CAdES, por esta razón este formato no es adecuado cuando el archivo original es demasiado grande (PAE, 2016; Hrvoje *et al*, 2013).
- **PAdES** (PDF Advanced Electronic Signature).
 - Es en si el formato de firma más adecuado cuando se dispone del documento original en un archivo de tipo pdf, pues se puede verificar de manera fácil la firma y el documento, siendo esta la principal diferencia entre los formatos anteriores (PAE, 2016; Hrvoje *et al*, 2013).
- **OOXML y ODF**
 - Estos son los formatos de firma electrónica usados por Open Office y Microsoft Office, respectivamente (PAE, 2016)

2.1.3 Validez de una firma electrónica

Según la Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos vigente en Ecuador, en su artículo de 15, establece lo siguiente sobre la validez de una firma electrónica: “para su validez, la firma electrónica reunirá los siguientes requisitos, sin perjuicio de los que puedan establecerse por acuerdo entre las partes” (SRI, 2016):

- a) Ser individual y estar vinculada exclusivamente a su titular.
- b) Que permita verificar inequívocamente la autoría e identidad del signatario, mediante dispositivos técnicos de comprobación establecidos por esta ley y sus reglamentos.
- c) Que su método de creación y verificación sea confiable, seguro e inalterable para el propósito para el cual el mensaje fue generado o comunicado.
- d) Que al momento de creación de la firma electrónica, los datos con los que se crease se hallen bajo control exclusivo del signatario, y,
- e) Que la firma sea controlada por la persona a quien pertenece.

2.2 FORMAS DE FIRMA BAJO EL FORMATO XADES

XAdES (XML Advanced Electronic Signatures) es un estándar abierto basado en XMLDSIG, que lo extiende para proporcionar validez a largo plazo y el resto de requisitos necesarios para cumplir con las especificaciones técnicas definidas en el estándar ETSI TS 101 903 V 1.4.2, este estándar específica cuatro formas de firmas avanzadas permitidas bajo XML en el punto 4.4 (ETSI, 2016):

- Firma Electrónica Básica (XAdES-BES)
- Firma Electrónica basada en la Política Explícita (XAdES-EPES)
- Firma Electrónica con Datos de Validación (XAdES-T y XAdES-C)

De acuerdo a la manera en que se relacionan la firma electrónica con el documento, se pueden dar tres tipos de firmas XAdES (Agencia de Tecnología y Certificación Electrónica, 2016):

- Adjunta (attached): a pesar de que la firma y el documento se integran en un único archivo XML, los dos están separados dentro de la estructura del mismo y se firma solamente la parte donde se encuentra el documento.
- Envolvente (enveloped): de la misma manera que en la firma adjunta, los dos elementos están en un mismo archivo, pero en este caso se firma el documento completo.
- Separada (detached): en este tipo de firma XAdES la firma y el documento están en archivos diferentes.

2.2.1 Firma Electrónica Básica (XAdES-BES)

Esta firma cumple los requisitos mínimos de la firma electrónica avanzada, como: identidad del firmante, garantiza que lo firmado no ha sido alterado y que la firma ha sido realizada por medios que únicamente controla el firmante. En XAdES-BES la firma deberá ser construida en base a XMLDSIG, incorporando las propiedades de calificación definidas dentro del documento, es obligatorio proteger el certificado de firma incorporando la propiedad firmada de SigningCertificate o incorporando el certificado desde ds:KeyInfo,

al hacerlo, XAdES-BES puede evitar que el certificado del firmante sea sustituido (Cryptomathic, 2016).

2.2.2 Firma Electrónica basada en la Política Explícita (XAdES-EPES)

La forma de firma electrónica basada en la Política Explícita (XAdES-EPES) amplía la definición de una firma electrónica para ajustarse a la política de firma identificada. Un XAdES-EPES se construye bajo la forma de un XMLDSIG o XAdES-BES mediante la incorporación de un elemento identificador de la política de firma (SignaturePolicyIdentifier). Esta propiedad firmada indica que una política de firma debe ser utilizada para la validación de la firma, pudiendo identificar explícitamente la política de firma (Cryptomathic, 2016).

2.2.3 Firma Electrónica con Datos de Validación XAdES-T

Una firma electrónica XML avanzada con tiempo (XAdES-T) es una firma para la que existe un tiempo de confianza asociado a la misma. El tiempo de confianza puede ser proporcionado por dos medios diferentes (ETSI, 2016):

- La firma de sello de tiempo como una propiedad no firmada, añadida a la firma electrónica;
- Una marca de tiempo de la firma electrónica proporcionada por un proveedor de servicios de confianza.

El sellado de tiempo evita que el firmante pueda alegar que cuando se realizó la firma su certificado estaba revocado.

2.2.4 Firma Electrónica con Datos de Validación XAdES-C

La Firma Electrónica XML Avanzada con referencias de datos de validación completas (XAdES-C) añade al XAdES-T referencias a todos los certificados de la cadena de confianza y referencias a las CRL y/o respuestas OCSP. Tanto los certificados de la cadena de confianza como las CRL/respuestas OCSP son externos a la firma (Cryptomathic, 2016).

2.3 CERTIFICADO DE FIRMA ELECTRÓNICA

Consiste en un documento digital, por medio del cual la autoridad de certificación garantiza la vinculación entre la identidad del usuario, su clave

pública y privada, el certificado es la base de la firma electrónica y contiene lo siguiente (ECIBCE, 2016):

- Identificación de la Autoridad de Certificación
- Los datos del titular del certificado que permitan su ubicación e identificación
- Las fechas de emisión y expiración del certificado
- El número único de serie que identifica el certificado
- Clave pública del titular del certificado
- Puntos de distribución (URL) para verificación de la Lista de Certificado Revocados (CRL).

Un certificado de firma electrónica puede ser usado por personas jurídicas (representante legal y/o perteneciente a empresas), naturales, servidores públicos o funcionarios, de acuerdo a su actividad y conveniencia.

En Ecuador los certificados de firma electrónica pueden ser adquiridos en las siguientes Autoridades de Certificación calificadas:

- Banco Central del Ecuador
- Security Data
- Consejo de la Judicatura

2.3.1 Solicitud de certificado de firma electrónica

A continuación se indica el proceso a seguir para solicitar un certificado de firma electrónica en cada una de las Autoridades de Certificación anteriormente mencionadas, para lo cual se accedió a la información publicada en las respectivas páginas de cada una de las ACs indicadas anteriormente:

- Banco Central del Ecuador: <https://www.eci.bce.ec/>
- Security Data: <https://www.securitydata.net.ec/>
- Consejo de la Judicatura: <https://www.icert.fje.gob.ec/>

2.3.1.1 Proceso de solicitud de certificado de firma electrónica en la AC del Banco Central del Ecuador

Previo a la solicitud de un certificado firma electrónica, el solicitante deberá revisar las normativas correspondientes a cada tipo de certificado en el siguiente enlace: <https://www.eci.bce.ec/web/guest/marco-normativo>, y luego reunir los siguientes requisitos, dependiendo el tipo de persona (natural o jurídica).

Persona Natural

- Copia digitalizada de la cédula o pasaporte a color.
- Copia digitalizada de la papeleta de votación actualizada, (exceptuando a personas mayores a 65 años, las ecuatorianas y ecuatorianos que habitan en el exterior, los integrantes de las Fuerzas Armadas y Policía Nacional y personas con discapacidad)
- Copia digitalizada de la última factura de pago de luz, agua o teléfono

Persona Jurídica

- La empresa debe estar previamente registrada en el sistema, para lo cual debe acceder al siguiente enlace e ingresar los datos solicitados: <https://www.eci.bce.ec/web/guest/registro-empresa-u-organizacion>
- Conocer el número de RUC de la empresa
- Copia digitalizada de la cédula o pasaporte a color
- Copia digitalizada de la papeleta de votación actualizada, (exceptuando a personas mayores a 65 años, las ecuatorianas y ecuatorianos que habitan en el exterior, los integrantes de las Fuerzas Armadas y Policía Nacional y personas con discapacidad)
- Copia digital del nombramiento o certificado laboral firmado por el Representante Legal
- Autorización firmada por el Representante Legal. (En caso de subrogación o delegación, adjuntar el oficio de encargo o delegación)
- **Importante:** Para el día en que se realice el pago, llevar la autorización en formato impreso.

Se recomienda tener los documentos escaneados en formato PDF, con un tamaño menor o igual a 1Mb y que sean claramente legibles.

Con los requisitos anteriormente detallados se deberá llenar la solicitud en el siguiente enlace <https://www.eci.bce.ec/web/guest/solicitud-de-certificado>. Y una vez aprobada la solicitud, se deberá realizar el pago del certificado en

las ventanillas del Banco Central y retirar el certificado de firma electrónica portando la cedula de identidad pasaporte.

Los valores a pagar según el tipo de certificado y el tiempo de vigencia del mismo, se pueden consultar en el siguiente enlace:

<https://www.eci.bce.ec/tarifas>

2.3.1.2 Proceso de solicitud de certificado de firma electrónica en la AC Security Data

Para la solicitud de certificados el solicitante deberá reunir los siguientes requisitos, dependiendo el tipo de persona (natural o jurídica).

Persona Natural

- Ser persona física y mayor de edad.
- Original de la cédula de ciudadanía o pasaporte en casos de extranjeros y papeleta de votación en caso de estar obligado a sufragar. En caso de cédulas enviar mediante correo un escaneado de la cédula actual a color, puesto que se validará la información con el registro civil y esta deberá coincidir.
- RUC electrónico (Solo Para Agentes de Aduana o importadores/exportadores, para personas que vayan usar facturación electrónica, es obligatorio adjuntar el RUC) descargado de la página del SRI el cual se puede descargar en <https://declaraciones.sri.gob.ec> con el usuario y clave en GENERAL>CERTIFICADOS TRIBUTARIOS>REIMPRESIÓN DE RUC.
- Formulario de Persona Natural lleno, el cual puede ser descargado desde el siguiente enlace https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/persona_natural.pdf. (En la primera hoja se encontrara un instructivo para llenar el formulario, no es necesario firmarlo).

Persona Jurídica

Para empresas reguladas por la Superintendencia de Compañías:

- Original de la cédula de ciudadanía o pasaporte en casos de extranjeros y papeleta de votación en caso de que este obligado a sufragar. En caso de cédulas enviar por correo un escaneado de la cédula actual a color, considerando que se validará la información con el registro civil y esta debe coincidir.

- Formulario de Representante Legal Lleno, el cual se puede descargar desde el siguiente enlace https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/representante_legal.pdf (En la primera hoja se encontrará un instructivo para llenar el formulario, no es necesario firmarlo).

Para empresas no reguladas por la Superintendencia de Compañías:

- Original de la cédula de ciudadanía o pasaporte en casos de extranjeros y papeleta de votación en caso de que este obligado a sufragar. En caso de cédulas enviar por correo un escaneado de la cédula actual a color puesto que se validará la información con el registro civil y esta debe coincidir.
- RUC electrónico descargado de la página del SRI el cual se puede descargar de <https://declaraciones.sri.gob.ec> con el usuario y clave en: GENERAL > CERTIFICADOS TRIBUTARIOS > REIMPRESIÓN DE RUC).
- Original o copia notariada y legible del nombramiento del representante legal vigente.
- Original o copia notariada de la constitución de la Empresa solicitante.
- Formulario de Representante Legal Lleno, el cual se puede descargar desde el siguiente enlace https://www.securitydata.net.ec/wp-content/downloads/descargas/Formularios/representante_legal.pdf (En la primera hoja se encontrará un instructivo para llenar el formulario, no es necesario firmarlo).

Los valores a pagar según el tipo de certificado y el tiempo de vigencia del mismo, se pueden consultar en el siguiente enlace:

https://www.securitydata.net.ec/wp-content/downloads/listas/lista_precios.pdf

Los documentos solicitados se podrán enviar a una de las siguientes direcciones de correo electrónico, dependiendo de la ciudad en la que se encuentre el solicitante:

- **Quito:** ventasui@securitydata.net.ec
- **Guayaquil:** ventasgye@securitydata.net.ec
- **Cuenca:** ventascuenca@securitydata.net.ec
- **Manta:** ventasmanta@securitydata.net.ec
- **El Oro:** ventaseloro@securitydata.net.ec
- **Ambato:** ventasambato@securitydata.net.ec
- **Latacunga:** ventaslatacunga@securitydata.net.ec

- **Sucumbíos:** ventassucumbios@securitydata.net.ec
- **Ibarra:** ventasibarra@securitydata.net.ec
- **Riobamba:** ventasriobamba@securitydata.net.ec
- **Azogues:** ventasazogues@securitydata.net.ec
- **Loja:** ventasloja@securitydata.net.ec
- **Tulcán:** ventastulcan@securitydata.net.ec
- **Esmeraldas:** ventasesmeraldas@securitydata.net.ec
- **Santa Elena:** ventassantaelena@securitydata.net.ec
- **Orellana:** ventasorellana@securitydata.net.ec
- **Santo Domingo:** ventasantodomingo@securitydata.net.ec
- **Otras ciudades:** ventasotras@securitydata.net.ec

2.3.1.3 Proceso de solicitud de certificado de firma electrónica en la AC del Consejo de la Judicatura

Para la solicitud de certificados el solicitante deberá reunir los siguientes requisitos, dependiendo el tipo de persona (natural o jurídica).

Persona Natural

- Copia digitalizada en formato PDF de la cédula o pasaporte (extranjeros).
- Copia digitalizada en formato PDF del certificado de votación o documento que justifique el no votar (carnet CONADIS, pasaporte, etc.).
- Copia digitalizada en formato PDF del pago de un servicio básico en el cual se detalle la dirección ingresada en la solicitud. (Para facturación electrónica se deberá llenar el campo de número de RUC en el formulario, caso contrario no podrá facturar electrónicamente).

Persona Jurídica

- Se requiere que la empresa esté registrada previamente.
- Saber el RUC de la misma.

- Copia digitalizada en formato PDF de la cédula o pasaporte (extranjeros).
- Copia digitalizada en formato PDF del certificado de votación o documento que justifique el no votar (carnet CONADIS, pasaporte, etc.).
- Documento digitalizado en formato PDF con la autorización del representante legal o delegado (talento humano, etc.), en el cual se autorice a tener un certificado dentro de la empresa.

Los valores a pagar según el tipo de certificado y el tiempo de vigencia del mismo, pueden ser consultados en el siguiente enlace:

<https://www.icert.fje.gob.ec/tarifas>

Con los requisitos anteriormente detallados se deberá ingresar la solicitud desde el siguiente enlace:

<https://www.icert.fje.gob.ec/solicitud-de-certificado>

2.4 ONLINE CERTIFICATE STATUS PROTOCOL

El Online Certificate Status Protocol (OCSP) permite a las aplicaciones determinar el estado de vigencia de un certificado mediante consulta a los servidores de confianza de la Autoridad de Validación (Galperin, Santesson, Myers, Malpani, & Adams, 2013). Para poder determinar la vigencia de un certificado la Autoridad de Validación puede coincidir o no con la Autoridad de Certificación (CA) que emitió el certificado que se desea validar, la Autoridad de Validación puede atender consultas de certificados emitidos por varias Autoridades de Certificación siempre que esté debidamente autorizada para ello por las propias CAs emisoras de los certificados (ECIBCE, 2016).

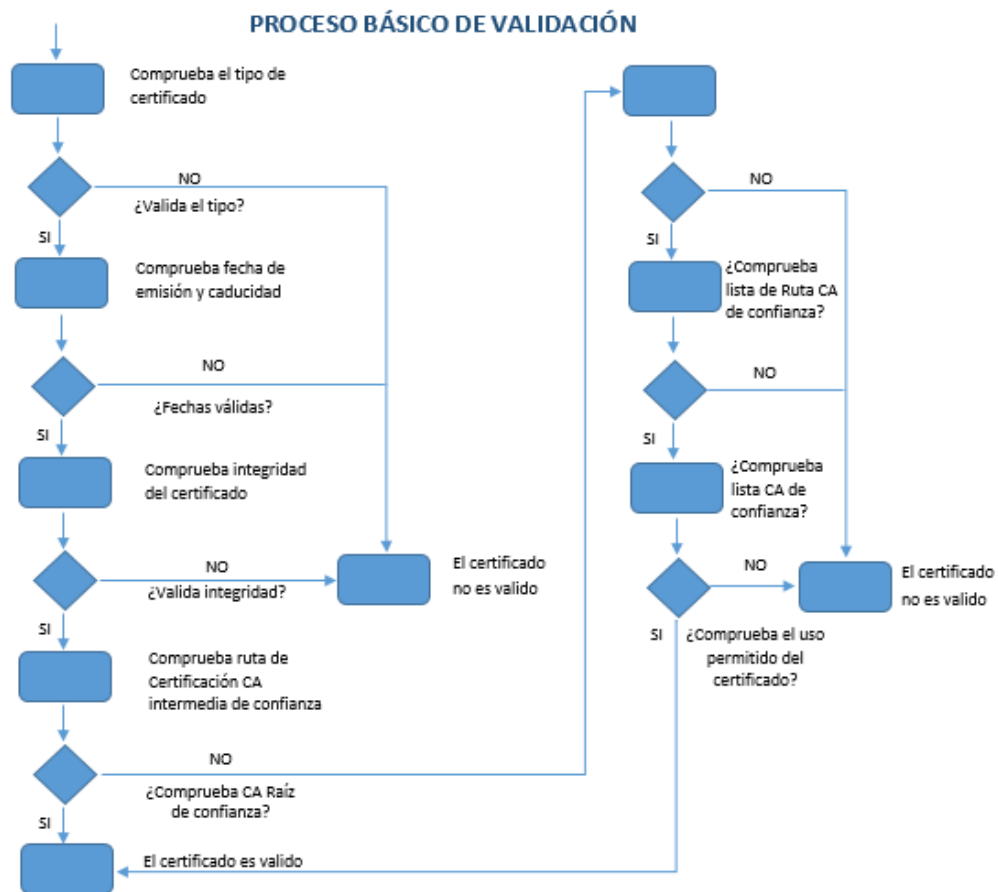


Figura 2 Proceso básico de validación de un certificado

2.5 CERTIFICATE REVOCATION LIST

La Certificate Revocation List (CRL) es una lista, firmada digitalmente por una AC, que contiene los números seriales de los certificados revocados junto con su fecha y razón de revocación. Estas listas son actualizadas periódicamente y publicadas en repositorios de confianza. Para conocer el estado de revocación de un certificado, el verificador debe recuperar la CRL donde se encuentra la información de revocación de dicho certificado y verificar su firma. Luego, debe buscar el número serial del certificado dentro de la lista. Si lo encuentra, el certificado ha sido revocado (Satzábal, Páez, & Forné, 2005).

2.6 AUTORIDAD DE SELLADO DE TIEMPO (TSA)

La Autoridad de sellado de tiempo (del inglés Time Stamping Authority, TSA) es un prestador de servicios de certificación que proporciona certeza

sobre la preexistencia de determinados documentos electrónicos a un momento dado, cuya indicación temporal junto con el hash del documento se firma por la Autoridad de sellado de tiempo (Vigil, Cabarcas, Wiesmaier, & Duchmann, 2012).

Cabe señalar que la entidad con la cual se contrató el servicio de sellado de tiempo para el presente proyecto es la TSA del Banco Central del Ecuador, decisión tomada por la empresa BIGDATA C.A, considerando que es con esta entidad con la cual se ha realizado previamente la adquisición de los certificados de firma electrónica usados en los procesos de facturación a sus clientes.

2.7 SELLADO DE TIEMPO O TIME-STAMPING

El sello de tiempo es un mecanismo que permite garantizar que la información no se ha modificado desde el momento de tiempo en el que se generó el sello (Milinković, Milojković, Spasić, & Lazić, 2012). El servicio de sellado de tiempo se solicita a una Autoridad de Sellado de Tiempo (TSA) mediante un resumen (hash) de la información a sellar.

El Banco Central del Ecuador detalla dos mecanismos de conexión para el consumo de los sellos de tiempo:

- Primer mecanismo.- Sistema de Tarificación de Servicios de Sellado de Tiempo (TTSA).
 - El TTSA sirve de intermediario entre un cliente final, que hace uso de los servicios de sellado de tiempo, y un proveedor de dichos servicios. Al proveedor de los servicios de sellado de tiempo se lo denomina Autoridad de Sellado de Tiempo "TSA".



Figura 3 Primer mecanismo de consumo de sellos de tiempo

Fuente: (ECIBCE, 2016)

- Segundo mecanismo.- Sistema de Sellado de Tiempo (SST)
 - El SST sirve de intermediario entre un cliente final que hace uso de los servicios de sellado de tiempo y un proveedor de dichos servicios. El proveedor de los servicios de sellado de tiempo será llamado Autoridad de sellado de tiempo "TSA", a diferencia del anterior mecanismo el cliente se autentica a través de un usuario y contraseña, sin la necesidad de un certificado digital para la autenticación.



Figura 4 Segundo mecanismo de consumo de sellos de tiempo

Fuente: (ECIBCE, 2016)

2.7.1 Proceso contratación del servicio de sellos de tiempo con la TSA del Banco Central del Ecuador

Como primer paso se consultó en la página Web de la TSA del Banco Central del Ecuador (<https://www.eci.bce.ec/>), acerca del proceso a realizar para contratar el servicio de sellos de tiempo, sin embargo no se encontró información alguna de cómo realizar dicho proceso. Por la razón expresada anteriormente se acudió a las oficinas de la TSA ubicadas en la matriz del Banco en la ciudad de Quito, donde se informó que la página se encontraba en proceso de actualización de la información solicitada, y procedieron a indicar los pasos a seguir para poder contratar el servicio de sellos de tiempo:

- Solicitar a la TSA los formularios para la contratación del servicio de sello de tiempo
- Llenar los formularios solicitados con la información de la empresa solicitante.
- Entregar los formularios llenos al área encargada de la emisión de sellos de tiempo.
- Solicitar que se genere el documento para poder realizar el pago en ventanilla.
- Acercarse a ventanilla y realizar el pago.

Cave especificar que el plan contratado por la Empresa BIGDATA C.A es el plan ilimitado anual, el mismo que tiene un costo de \$. 250 más IVA, dando un valor final de \$. 285.00.

2.8 SELLOS DE TIEMPO Y SU RELACIÓN CON FIRMA ELECTRÓNICA

Cuando se utiliza firmado con Sellos de Tiempo se unen dos procedimientos que coexisten por separado, el procedimiento de firma electrónica y el de Sellado de tiempo. Lo primero que se hace es firmar el documento luego, se adiciona un Sello de tiempo dejando constancia del momento en que se firmó el documento. En este caso, para el proceso de Sellado de Tiempo se tiene como entrada los datos de un documento con una firma digital asociada, emitida por una entidad de confianza. Considerando al documento firmado como cualquier conjunto de datos electrónicos, se trabaja con las pautas del procedimiento explicado anteriormente de Sellado de Tiempo (Paulin, Robledo, & Brusa, 2014).

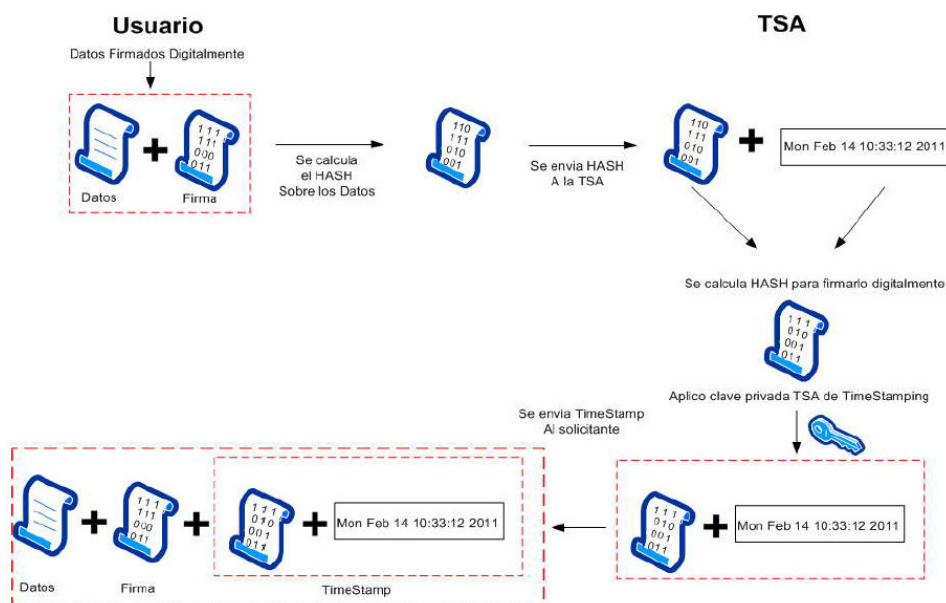


Figura 5 Proceso de firma con Sello de Tiempo

Fuente: (Paulin *et al*, 2014)

2.9 COMPROBANTES ELECTRÓNICOS

Un comprobante electrónico consiste en un documento, el cual cumple con los requisitos legales y reglamentarios exigibles para todos comprobantes de venta, garantizando así la autenticidad de su origen y la integridad de su contenido. El comprobante electrónico tendrá validez legal siempre y cuando contenga una firma electrónica (SRI, 2016).

Beneficios de los comprobantes electrónicos

El SRI destaca los siguientes beneficios de usar comprobantes electrónicos en lugar de los físicos:

- Igual validez que los documentos físicos.
- Reducción los tiempos de envío de los comprobantes.
- Reducción de gastos de papelería física y archivo.
- Contribuye al medio ambiente, dado que se reduce el uso de papel y tintas de impresión.
- Procesos administrativos más rápidos y eficientes.
- Menor probabilidad de falsificación.
- Mayor seguridad en el resguardo de los documentos.

Entre los principales comprobantes electrónicos permitidos por el SRI tenemos los siguientes:

- Facturas
- Notas de crédito
- Notas de débito
- Comprobantes de retención
- Guías de remisión

El formato exigido por el SRI para la generación de comprobantes electrónicos es el formato XML (eXtensible Markup Language), bajo el estándar de firma digital de documentos XML XadES_BES, lo que quiere decir que cada archivo .xml tendrá dentro de su estructura la firma electrónica y constituirá un documento electrónico válido una vez que el SRI proceda con la autorización para la respectiva emisión. (SRI, 2016)

Descripción	Especificación	Documentación técnica relacionada
Estándar de firma	XadES_BES	http://uri.etsi.org/01903/v1.3.2/ts_101903v010302p.pdf
Versión del esquema	1.3.2	http://uri.etsi.org/01903/v1.3.2#
Codificación	UTF-8	
Tipo de firma	ENVELOPED	http://www.w3.org/2000/09/xmldsig#enveloped-signature

Figura 6 Especificaciones técnicas relacionadas al estándar XadES_BES

Fuente: (SRI, 2016)

2.10 XMLDigSig

XML Digital Signature (XMLDigSig) es una forma de firma digital que está optimizada para la firma de datos XML. Lo que diferencia el mecanismo de firma digital XML de las firmas digitales "estándar" es la posibilidad de una firma parcial que permite que la firma digital XML se use sólo en etiquetas específicas en la estructura XML. Esta forma de firma fue desarrollada para solucionar problemas de seguridad específicos relacionados con la seguridad y el control de datos en transacciones electrónicas, y posteriormente en mecanismos de mensajería utilizados en servicios Web. Es mayormente utilizado para resolver problemas como la falsificación, la suplantación y el repudio (Gerić & Vidačić, 2012).

La estructura de una firma bajo XMLDSIG es la siguiente:

```
<ds:Signature ID ?>
  <ds:SignedInfo>
    <ds:CanonicalizationMethod />
    <ds:SignatureMethod />
    <ds:Reference>
      <ds:Transforms />
      <ds:DigestMethod />
      <ds:DigestValue />
    </ds:Reference>
    <ds:Reference /> etc.
  </ds:SignedInfo>
  <ds:SignatureValue />
  <ds:KeyInfo />
  <ds:Object />
</ds:Signature>
```

Tabla 1
Estructura de una firma bajo XMLDSIG

Nº	Etiqueta	Descripción
1	Signature	Encapsula la firma digital
2	SignedInfo	Información sobre lo firmado y como está firmado, contiene la información que se necesita para crear y validar la firma.

Continúa 

3	CanonicalizationMethod	Representa el algoritmo de transformación de SignedInfo previo a la realización de la firma digital.
4	SignatureMethod	Representa el algoritmo usado para calcular el valor de la firma.
5	Reference	Contiene las referencias a los objetos que se van a ser firmados.
6	Transforms (opcional)	Lista ordena de transformaciones aplicadas a los datos antes de hacer el hash, comúnmente usado en firmas envolventes para eliminar el elemento signature antes de calcular la firma
7	DigestMethod	Algoritmo usado para obtener el hash del objeto
8	DigestValue	Es el valor resultante
9	SignatureValue	Contiene el elemento SignedInfo en forma canonizada, resumida y que ha sido encriptado con la clave pública del firmante.
10	KeyInfo (opcional)	Es un elemento opcional, el cual indica la clave que ha de utilizarse para validar la firma.
11	Object (opcional)	Puede incluir cualquier otro dato, como sellos de tiempo, o los datos a firmar en firmas envolventes

Fuente: (W3C España, 2016)

2.11 ALGORITMO RSA

Es un algoritmo de cifrado de clave pública desarrollado por Ron Rivest, Adi Shamir y Len Adlemen en 1997, es el algoritmo criptográfico de clave asimétrica más popular y probado. El algoritmo RSA se basa en el hecho matemático que es fácil encontrar y multiplicar grandes números primos juntos, pero es extremadamente difícil factorizar su producto. Las claves privadas y públicas en RSA se basan en números primos muy grandes formados por 100 o más dígitos, el propio algoritmo es bastante simple a diferencia de los algoritmos criptográficos de clave simétrica (Singh, Sunil K, & Sudesh, 2013).

2.12 FACTORING

El Factoring constituye una herramienta financiera, la cual permite a las empresas obtener recursos líquidos de manera inmediata mediante la venta de sus facturas por cobrar. Estas facturas se venden con un factor de descuento a una empresa dedicada a la actividad del Factoring (Shpresa & Anila, 2015).

Entre las principales ventajas que el Factoring ofrece a las empresas, se encuentran las siguientes (Ivanovic, Baresa, & Sinisa, 2011):

- Ofrece liquidez inmediata sin necesidad de hipotecar sus bienes y sin generar pasivos.
- Permite ampliar los plazos de crédito, mejorando las condiciones de su mercado.
- Ayuda a financiar el capital de trabajo que la empresa necesita
- Incremento en el volumen de sus ventas.
- Fácil acceso a la obtención de este servicio.
- Obtención de descuentos por pronto pago de sus proveedores.
- Adquirir flujo de caja sin necesidad de anticipo por parte de sus clientes.
- Adaptación a las necesidades del cliente.
- Ayuda a planificar de mejor manera su flujo de caja.
- Reducción de dependencia de los bancos.
- La gestión de cobranza es realizada por la compañía de Factoring.

Actores involucrados en un proceso de Factoring

- **Vendedor (empresa emisora de la factura).**- Es el emisor de la factura, quien contacta a una empresa de Factoring para poder vender sus facturas por cobrar.
- **Deudor (empresa deudora de la factura).**- Es el receptor de la factura.
- **Comprador (empresa dedicada al Factoring).**- Es quien compra las facturas al vendedor aplicando un porcentaje de descuento.

2.11.1 Factoring Convencional

En el Factoring convencional se usan facturas físicas autorizadas por el Servicio de Rentas Internas (SRI), como requisito inicial una empresa vendedora debe haber emitido una factura física a una empresa cliente (deudora), para después continuar con el siguiente proceso:

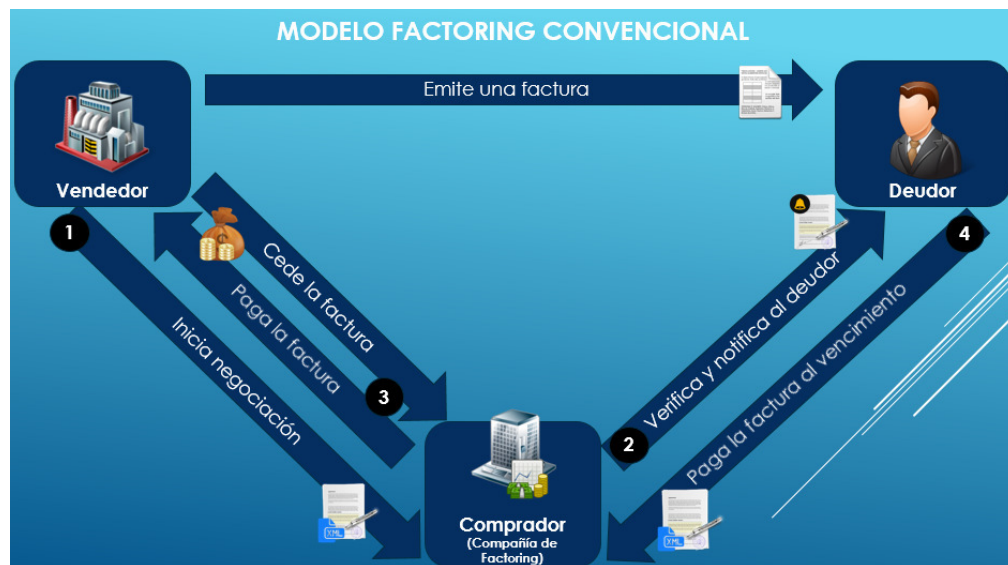


Figura 7 Modelo Factoring convencional

- 1) La empresa vendedora inicia la negociación con una empresa dedicada al Factoring (empresa compradora).
- 2) La empresa compradora verifica la validez de la factura.
- 3) Una vez aceptada y validada la factura, se produce la "cesión" o venta, donde ambas partes (empresa vendedora y compradora) firman un documento donde constan los compromisos adquiridos por las partes, y la empresa compradora procede a hacer el pago la empresa vendedora y notifica a la empresa deudora sobre el traspaso de la factura.
- 4) La empresa deudora cancela su deuda a la empresa comprador en la fecha estipulada en la factura, dando así por finalizado el ciclo del Factoring.

2.11.2 Factoring Electrónico

El Factoring Electrónico es una modalidad del Factoring convencional, en el cual en lugar de facturas físicas se usan facturas electrónicas autorizadas por el SRI, sin usar en ningún momento el papel o algún otro medio físico como soporte, realizando todas las transacciones en un ambiente totalmente electrónico.

Actores involucrados en un proceso de Factoring Electrónico

- **Vendedor (empresa emisora de la factura).**- Sube facturas emitidas a sus clientes en el sistema, para ser vendidas.
- **Confirmador (empresa deudora de la factura).**- Confirma el pago de las facturas que han sido cargadas por el vendedor.
- **Comprador (empresa dedicada al Factoring).**- Compra facturas subidas por el vendedor aplicando un porcentaje de descuento.

2.13 Unified Modelling Language

UML es un lenguaje que permite construir, modelar y documentar los componentes que forman un sistema orientado a objetos, en la actualidad constituye el estándar preferido de la industria. La popularidad de este lenguaje se debe principalmente a que fue desarrollado por los autores de los tres métodos más usados de orientación a objetos: Grady Booch, Ivar Jacobson y Jim Rumbaugh, quienes fueron contratados por la Rational Software Co para crear un notación unificada en la cual poder basar la construcción de sus herramientas CASE (Ferré Grau & Sánchez Segura, 2002; Debasish, Debasis, & Rajib, 2013).

Entre los diagramas que permite construir UML están los siguientes:

- **Diagramas de casos de uso:** describen los casos de usos posibles y las relaciones entre ellos, representando una porción de la funcionalidad del sistema para cada tipo de actor externo (Bustos, 2002).
- **Diagramas de clases:** describen las clases que existen en el sistema y las relaciones entre las mismas (Bustos, 2002).
- **Diagramas de secuencia:** describen la interacción en términos de mensajes ente los objetos de las clases (Bustos, 2002).
- **Diagramas de colaboración:** suelen usarse para representar objetos o clases y la forma en que se transmiten mensajes y colaboran entre ellos para cumplir un objetivo (Bustos, 2002).
- **Diagramas de estados:** describen el comportamiento que exhiben los objetos de una clase, representando cómo evoluciona un sistema a medida que se producen determinadas acciones (Bustos, 2002).

- **Diagramas de actividades:** describen el flujo de trabajo entre actividades, mismas que pueden organizarse de manera secuencial, condicionada y concurrente (Bustos, 2002).

2.14 METODOLOGÍA Y HERRAMIENTAS DE DESARROLLO

2.13.1 UML-based Web Engineering

UML-based Web Engineering (UWE) es una metodología basada en el Proceso Unificado y UML para el desarrollo de aplicaciones Web, fue dada a conocer por Nora Koch de la Universidad de Múnich en Alemania, se caracterizada por ser una metodología orientada a objetos, iterativa e incremental (Granda, Campaña, & Días, 2017). La estrategia de diseño de UWE se basa en modelos que se construyen durante la fase de análisis, principalmente el modelo conceptual y el modelo de procesos, introduciendo clases específicas de proceso como parte de un modelo separado que ofrece una interfaz al modelo de navegación (Rivero, Grigera, Rossi, Robles Luna, & Koch, 2011).

Se escogió esta metodología tomando en cuenta los resultados obtenidos por María Escalona y Nora Koch (Escalona & Koch, 2002) en un estudio comparativo entre metodologías de desarrollo Web como: WSDM, W2000, RNA, NDT, UWA, entre otras, donde UWE destaca principalmente por su enfoque a procesos, obtención de requisitos y soporte con herramientas CASE que brindan apoyo para el tratamiento de los mismos, lo que permite desarrollar aplicaciones de mejor calidad.

UWE utiliza como notación a UML y el método que utiliza consta de cinco modelos principales: Requerimientos, Contenido, Navegación, Presentación y Procesos, donde cada uno de los modelos se desarrolla en un escenario diferente durante el proceso de desarrollo de software (Koch & Kraus, 2002).

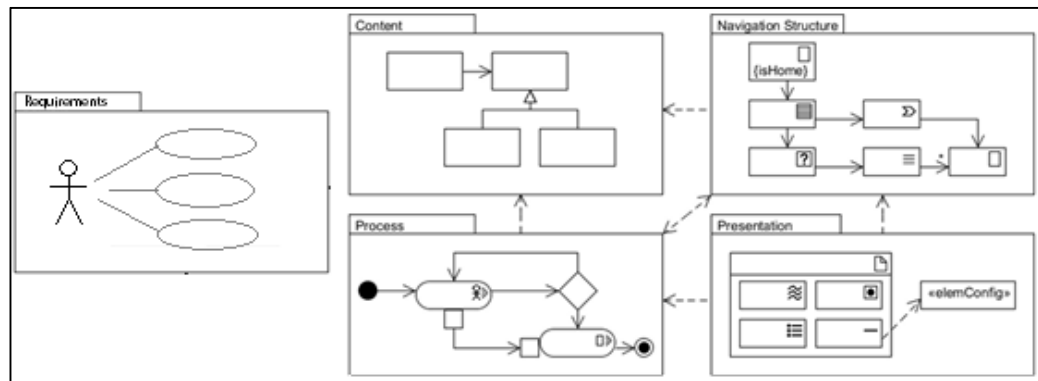


Figura 8 Principales modelos de la metodología UWE

Fuente: (Granda *et al*, 2017)

2.13.2 NetBeans IDE

NetBeans IDE constituye un ambiente de desarrollo en el cual los programadores pueden escribir, compilar, depurar y ejecutar sus programas. Está desarrollado en Java, pero puede servir para otros lenguajes de programación. Cuenta con una gran cantidad de módulos y plugins para extender su funcionalidad (NetBeans, 2017).

2.13.3 Java y Java Enterprise Edition

Java es un lenguaje de programación y una plataforma informática comercializada por primera vez en 1995 por Sun Microsystems. Existen muchas aplicaciones y sitios Web que no funcionarán a menos que tenga Java instalado y cada día se crean más. Java es popular por ser rápido, seguro y fiable. Java está en todas partes, desde computadores hasta centros de datos, desde consolas de juegos hasta súper computadoras, desde teléfonos celulares hasta Internet (Java, 2017).

Java Enterprise Edition es una plataforma de programación que forma parte de la Plataforma Java, sirve para desarrollar y ejecutar software de aplicaciones en el lenguaje de programación Java. Permite utilizar arquitecturas de N capas distribuidas y se apoya ampliamente en componentes de software modulares ejecutándose sobre un servidor de aplicaciones (Oracle, 2017).

2.13.4 Apache Tomcat

Apache Tomcat es una implementación de código abierto de las tecnologías Java Servlet, JavaServer Pages, Java Expression Language y Java WebSocket, que puede ser usado como un contenedor de aplicaciones Web (Apache Tomcat, 2017).

2.13.5 Java Server Faces

JAVA Server Faces (JSF) comúnmente llamado Faces, es un framework JAVA estándar para la construcción de interfaces de usuario y forma parte de la especificación de Java Enterprise Edition (JEE). Una de las ventajas más importantes de JSF es la posibilidad de desarrollar aplicaciones Web de manera rápida a partir de un conjunto de componentes reusables, obteniendo así desarrollos más productivos en un lapso de tiempo menor (Diaz, Queiruga, & Iuliano, 2009).

2.13.6 PrimeFaces

PrimeFaces es una librería de componentes para JSF de código abierto que cuenta con un conjunto de componentes enriquecidos que facilitan la creación de aplicaciones Web. Una de las ventajas de utilizar PrimeFaces, es que permite la integración con otros componentes compatibles con JSF (Egas Clavijo, 2015).

2.13.7 PolygonESL-2.0

PolygonESL-2.0 es un conjunto de librerías de software libre usadas para realizar el proceso de firma, verificación de firmas y sellado de tiempo, estas librerías son facilitadas por la TSA del Banco Central del Ecuador previo a la solicitud y firma de un acuerdo de licencia de usuario final entre la TSA y la empresa contratante (ECIBCE, 2016).

2.13.8 MariaDB

MariaDB Server es un servidor de bases de datos que se desarrolla como un software de código abierto, hecho por los desarrolladores originales de MySQL. MariaDB es un reemplazo mejorado para MySQL, su principal característica es ser rápida, escalable y robusta, con un rico ecosistema de

motores de almacenamiento, comprende una base de datos relacional que proporciona una interfaz SQL para el acceso a los datos (MariaDB Foundation, 2017).

2.13.9 Hibernate

Hibernate es una herramienta de software libre de mapeo objeto-relacional (ORM) y de consulta que permite desarrollar clases persistentes mediante lenguaje orientado a objetos, proporcionando además un lenguaje de consulta llamado HQL (Hibernate Query Language) similar a SQL, con un criterio orientado a objetos (Callejas Cuervo, Peñalosa Parra, & Alarcón Aldana, 2011).

2.13.10 ERS

La especificación de requisitos de software (ERS) es una descripción completa del comportamiento del sistema que se va a desarrollar, la ERS contiene requisitos no funcionales (o complementarios). Los requisitos no funcionales son requisitos que imponen restricciones en el diseño o la implementación, como por ejemplo, restricciones en el diseño o estándares de calidad, está dirigida tanto al cliente como al equipo de desarrollo. El lenguaje utilizado para su redacción debe ser informal, de forma que sea fácilmente comprensible para todas las partes involucradas en el desarrollo (ISTR, 2017).

CAPÍTULO III

PROCESO ACTUAL DE FACTORING ELECTRÓNICO IMPLEMENTADO POR BIGDATA CA, ANÁLISIS Y DISEÑO DE LA APLICACIÓN WEB DE TIME STAMPING

3.1 PROCESO ACTUAL DE FACTORING ELECTRÓNICO IMPLEMENTADO POR BIGDATA CA

El proceso de Factoring Electrónico implementado por BIGDATA C.A está basado en el Factoring convencional, haciendo uso de facturas electrónicas en lugar de físicas, además de ciertas mejoras propuestas por la misma empresa con el fin de brindar mayor seguridad jurídica al proceso y a los documentos generados en el mismo. Entre las mejoras propuestas por la empresa al proceso de Factoring, están (a) la confirmación de pago de la factura por parte del deudor de la misma (donde se detalla el compromiso de pago de la factura en una fecha determinada) y (b) el uso de firmas electrónicas y sellos de tiempo para la firma de los documentos generados (proceso implementado en la aplicación de Time Stamping).

Cabe mencionar que los documentos de confirmación de pago y cesión de la factura se venían realizando en archivos XML generados por el sistema, a partir de los cuales se construían los respectivos documentos en formato PDF, para facilitar la visualización del contenido a los usuarios. Ocasionalmente cuando uno o más de los actores involucrados en un proceso de Factoring, deseaban tener mayor seguridad, se solicitaba la firma física de estos documentos para tener mayor seguridad y respaldo de los compromisos acordados, lo que implicaba mayor tiempo de negociación entre las partes involucradas. El objetivo de las mejoras propuestas por la empresa es evitar que esto siga sucediendo y que el proceso se realice totalmente en línea y en menor tiempo.

La decisión de utilizar el formato de archivo XML para la creación de los documentos (confirmación de pago y cesión de la factura) generados en el proceso de Factoring se dio por las siguientes razones: 1) menor consumo de espacio de almacenamiento en el sistema, 2) mayor facilidad de lectura de los

archivos gracias al uso de etiquetas, 3) mantener un único formato de archivos en el sistema y 4) coincidir con el formato usado por el SRI para la emisión de los comprobantes electrónicos, con el objetivo de reusar los métodos de generación y lectura de archivos que ya han sido desarrollados por la empresa.

A continuación se detalla el proceso de Factoring Electrónico implementado por la empresa BIGDATA C.A (Ver Figura 9):

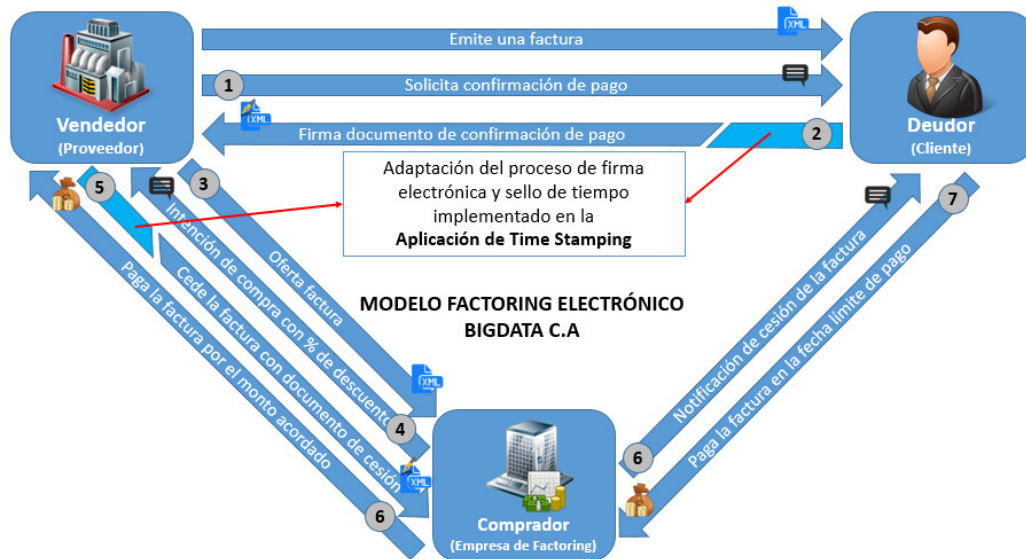


Figura 9 Proceso Factoring Electrónico Empresa BIGDATA C.A

Como requisito inicial para iniciar un proceso de Factoring Electrónico un Vendedor debe haber emitido una factura electrónica a uno de sus clientes (Deudor), para después continuar con el siguiente proceso:

- 1) El Vendedor solicita al Deudor una confirmación de pago de la factura.
- 2) El Deudor da la confirmación de pago de la factura mediante un documento firmado y sellado electrónicamente, en cual consta el compromiso de pago de la factura en una fecha límite.
- 3) Una vez recibida la confirmación de pago, el Vendedor inicia una negociación de la factura a un Comprador registrado previamente en el sistema de Factoring Electrónico.

- 4) El Comprador evalúa la validez de la factura y aplica un valor de descuento sobre la misma en base al valor de la factura y los días restantes para el pago de la misma, e informa la intención de compra al Vendedor con valor de descuento aplicado.
- 5) El Vendedor acepta la intención de compra con el valor descontado por el Comprador y realiza la cesión de la factura a nombre del mismo, mediante un documento firmado y sellado electrónicamente, en el cual se detalla la cesión de la factura y los derechos de cobro del nuevo propietario.
- 6) Una vez recibida la cesión de la factura de parte del Vendedor, el Comprador realiza el pago de la misma al Vendedor y el sistema automáticamente notifica al Deudor sobre la cesión de la factura a nombre del nuevo propietario, a quien deberá cancelar el valor total de la misma en la fecha límite de pago estipulada en el documento de confirmación.
- 7) Finalmente el Deudor cancela el valor total de la factura al Comprador en la fecha límite, dando así por terminado el proceso de Factoring Electrónico.

En el paso 2 y 5 es donde se adaptó el proceso de firma electrónica y sellado de tiempo implementado en la Aplicación de Time Stamping.

La estructura para la creación de los documentos de confirmación de pago y cesión de factura a ser generados por el sistema en formato XML son las siguientes (Ver Tablas 2 y 3):

Tabla 2
Estructura del documento de confirmación de pago creado en el paso 2


Nº	Etiqueta	Descripción
1	<?xml version="1.0" encoding="UTF-8" ?>	Describe el tipo de archivo y la codificación del archivo
2	<confirmacionPago id="confirmacionPago"> </confirmacionPago>	Etiqueta principal, contiene todas las etiquetas relacionadas con la confirmación de pago y es sobre la cual se aplicara la firma electrónica
3	<detalleConfirmacion> </detalleConfirmacion>	Contiene el texto de la confirmación de pago y la información del confirmador

Continúa 

4	<textoCompromiso> </textoCompromiso>	Contiene el texto del compromiso del pago de la factura y las obligaciones adquiridas
5	<razonSocialConfirming> </razonSocialConfirming>	Razón social de la empresa confirmadora o deudora de la factura
6	<numeroRucConfirming> </numeroRucConfirming>	RUC de la empresa confirmadora
7	<ciudadDireccionConfirming> </ciudadDireccionConfirming>	Dirección de la empresa confirmadora
8	<telefonoConfirming> </telefonoConfirming>	Teléfono de la empresa confirmadora
9	<nombreRepresentanteLegalConfirming> </nombreRepresentanteLegalConfirming>	Nombre del representante legal de la empresa confirmadora
10	<cedulaRepresentanteLegalConfirming> </cedulaRepresentanteLegalConfirming>	Cedula del representante legal de la empresa confirmadora
11	<detalleFactura> </detalleFactura>	Contiene las etiquetas relacionadas a la información de la factura
12	<claveAccesoFactura> </claveAccesoFactura>	Contiene la clave de acceso de la factura de la cual se va a dar la confirmación de pago
13	<valorTotalFactura> </valorTotalFactura>	Es el valor total por el cual fue emitida la factura
14	<valorNegociableFactura> </valorNegociableFactura>	Es el valor negociable de la factura, luego de restar impuestos y retenciones aplicadas a la misma
15	<fechaLimitePagoFactura> </fechaLimitePagoFactura>	Es la fecha límite de pago de la factura
16	<checksumFactura> </checksumFactura>	En un hash de la factura original, usado para validar que los valores aquí detallados fueron tomados del comprobante original sin cambios previos

Tabla 3
Estructura del documento de cesión de la factura creado en el paso 5

Nº	Etiqueta	Descripción
1	<?xml version="1.0" encoding="UTF-8" ?>	Describe el tipo de archivo y la codificación del archivo
2	<endosoFactura id="endosoFactura"> </endosoFactura>	Etiqueta principal que contiene todas las etiquetas relacionadas al endoso de la factura, sobre la cual se aplicara la firma electrónica
3	<detalleEndoso> </detalleEndoso>	Contiene el texto del endoso de la factura y la información del endosante
4	<textoEndoso> </textoEndoso>	Contiene el texto del endoso de la factura
5	<empresaEndosante>	Razón social de la empresa endosante

Continúa 

	</empresaEndosante	
6	<numeroRucEmpresaEndosante> </numeroRucEmpresaEndosante>	RUC de la empresa endosante
7	<detalleFactura> </detalleFactura>	Contiene las etiquetas relacionadas a la información de la factura
8	<claveAccesoFactura> </claveAccesoFactura>	Contiene la clave de acceso de la factura de la cual se va a dar la confirmación de pago
9	<valorTotalFactura> </valorTotalFactura>	Es el valor total por el cual fue emitida la factura
10	<valorNegociableFactura> </valorNegociableFactura>	Es el valor negociable de la factura, luego de restar impuestos y retenciones aplicadas a la misma
11	<fechaLimitePagoFactura> </fechaLimitePagoFactura>	Es la fecha límite de pago de la factura
12	<checksumConfirmacionPago> </checksumConfirmacionPago>	En un hash de la confirmación de pago relacionada a la factura original, usado para validar que los valores aquí detallados fueron tomados de la confirmación de pago original sin cambios previos

En las figuras 10 y 11 se muestra un ejemplo de los documentos de confirmación de pago y cesión de la factura generados por el sistema.

```
<?xml version="1.0" encoding="UTF-8"?>
<confirmacionPago id="confirmacionPago">
  <detalleConfirmacion>
    <textoCompromiso>Debo (emos) y pagaré (emos) incondicional e irrevocablemente a 84 días fijos de la fecha de emisión, en esta ciudad de Quito o en el lugar en el que se me reconvenga a la orden de Empresa XYZ, o su endosatario, la suma de $. 196000.00 (CIENTO NOVENTA Y SEIS MIL 00/100 DÓLARES DE LOS ESTADOS UNIDOS DE AMÉRICA). En caso de mora me (nos) obligo (amos) a pagar el máximo interés moratorio vigente a la fecha en que se produzca el vencimiento de la obligación hasta su total cancelación; así como todos los gastos judiciales, extrajudiciales y honorarios profesionales que demande el cobro de esta factura. Sin protesto, Eximo (mimos) al acreedor y al (los) endosatario (s) de la obligación de presentación para el pago y de aviso por falta del mismo.

    Declaro (amos) estar legalmente facultado (s) para firmar y aceptar irrevocablemente la presente factura y de igual manera, declaro (amos) expresamente que he (mos) recibido el (los) bien (es) descritos en esta factura comercial negociable a mi (nuestra) entera y total satisfacción y que estamos de acuerdo en el precio, en los términos de pago, el plazo, forma de pago y montos, y que en caso de controversia la vía sea la Ejecutiva.</textoCompromiso>
    <razonSocialConfirming>Empresa ABC</razonSocialConfirming>
    <numeroRucConfirming>1722547896001</numeroRucConfirming>
    <ciudadDireccionConfirming>Quito, El Inca</ciudadDireccionConfirming>
    <telefonoConfirming>21312312</telefonoConfirming>
    <nombreRepresentanteLegalConfirming>Juan Perez</nombreRepresentanteLegalConfirming>
    <cedulaRepresentanteLegalConfirming>1716063555</cedulaRepresentanteLegalConfirming>
  </detalleConfirmacion>
  <detalleFactura>
    <claveAccesoFactura>0709201601179204998900110010020000000451578492519</claveAccesoFactura>
    <valorTotalFactura>228000.00</valorTotalFactura>
    <valorNegociableFactura>$. 200000.00 menos una retención aplicada a la base imponible de: $. 4000.00 dando un total de: $. 196000.00</valorNegociableFactura>
    <fechaLimitePagoFactura>Wed Nov 30 00:00:00 ECT 2016</fechaLimitePagoFactura>
    <checksumFactura>77a0eac50391041db0faeb33a9f734b9b8f2a98a9cd4ed2a39c44ddaa57126ef</checksumFactura>
  </detalleFactura>
</confirmacionPago>
```

Figura 10 Ejemplo del documento de confirmación de pago, generado en el paso 2

```

<?xml version="1.0" encoding="UTF-8"?>
<endosoFactura id="endosoFactura">
  <detalleEndoso>
    <textoEndoso>Páguese a la orden de Empresa Compradora con RUC 1192100528001 por
valor recibido.</textoEndoso>
    <empresaEndosante>Empresa XYZ</empresaEndosante>
    <numeroRucEmpresaEndosante>1702750984001</numeroRucEmpresaEndosante>
  </detalleEndoso>
  <detalleFactura>
    <claveAccesoFactura>
      0709201601179204998900110010020000000451578492519
    </claveAccesoFactura>
    <valorTotalFactura>228000.00</valorTotalFactura>
    <valorNegociableFactura>200000.00</valorNegociableFactura>
    <fechaLimitePagoFactura>2016-11-30</fechaLimitePagoFactura>
    <checksumConfirmacionPago>
      9ef5d20dda5f7d5c80ce66d6716bb1cb7ec6418eb6e3e62f323bb0a2b5412440
    </checksumConfirmacionPago>
  </detalleFactura>
</endosoFactura>

```

Figura 11 Ejemplo del documento de cesión de la factura, generado en el paso 5

3.2 ANÁLISIS Y DISEÑO DE LA APLICACIÓN WEB DE TIME STAMPING

3.2.1 Análisis de requerimientos

La empresa BIGDATA C.A considera el uso de la firma electrónica en conjunto con los sellos de tiempo como una excelente solución para brindar la seguridad jurídica a documentos electrónicos, con la finalidad de poder probar la integridad y validez de los mismos a las personas interesadas e incluso ante procesos judiciales en caso de ser necesario. Por lo que desea incorporar esta funcionalidad en su sistema de Factoring Electrónico.

A continuación se detallan los requisitos que debe cumplir la aplicación Web de Time Stamping, los mismos que se encuentran especificados en el Anexo 01 y fueron creados en base al estándar IEEE 830 – 1998, el cual establece directrices para elaborar correctamente una ERS.

3.2.1.1 Registro de usuario (RF01)

La aplicación deberá verificar que la información de registro que el usuario haya ingresado sea la correcta, para lo cual deberá realizar las siguientes validaciones para cada dato requerido:

- **Número de cedula de identidad.-** Se deberá usar el algoritmo de validación de número cédula de identidad ecuatoriana según sea el caso, para determinar si es o no un numero correctamente formado.
- **Nombres y apellidos.-** Se validará que estos campos sean llenados correctamente, no se aceptará que estos campos estén vacíos.
- **Certificado de firma electrónica.-** Si el usuario desea, podrá cargar su certificado de firma electrónica a la aplicación en cuyo caso se validará que el archivo posea el formato correcto, aceptando únicamente la extensión de archivos “.p12”, si el usuario no proporciona el certificado de firma, la aplicación solicitará que este sea cargado cada vez que se desee hacer un proceso de firma y sello de tiempo.
- **E-mail.-** Se validará que la dirección de e-mail o correo electrónico este correctamente formada, bajo el siguiente formato “nombreusuario@dominio” ejemplo “usuariojuan@mail.com”, y que no esté siendo usada por ningún otro usuario de la aplicación.
- **Usuario.-** Se validará que el nombre de usuario sea único en la aplicación.
- **Contraseña.-** La contraseña no deberá contener espacios en blanco y deberá contener una mezcla de caracteres alfanuméricos. Para el almacenamiento de la contraseña se deberá usar estándar AES256 para el cifrado de la misma, con una semilla de 32 caracteres alfanuméricos autogenerados por el sistema para cada usuario, con la finalidad de brindar mayor seguridad las contraseñas almacenadas en la base de datos.

Una vez que los datos han sido ingresados correctamente, la aplicación procederá a crear una cuenta para el usuario, con la cual podrá acceder y hacer uso de la aplicación cada vez que desee.

3.2.1.2 Autenticación de usuario (RF02)

La aplicación solamente será accesible a usuarios debidamente autenticados, para lo cual deberán estar previamente registrado. Los datos de acceso a la aplicación serán los siguientes:

- **Usuario.-** Sera el usuario con el cual se registró en la aplicación.
- **Contraseña.-** Sera la contraseña establecida al momento de registrarse en la aplicación.

Una vez proporcionados estos datos, la aplicación procederá a validar los mismos, y de ser correctos permitirá el acceso al usuario, caso contrario mostrara el respectivo mensaje de error.

3.2.1.3 Solicitar nueva contraseña (RF03)

Cuando un usuario no recuerde su contraseña, este podrá solicitar al sistema una nueva, para lo cual deberá seleccionar la opción “Olvido de contraseña” en la pantalla de autenticación, al seleccionar dicha opción la aplicación le solicitará la dirección de correo electrónico o el nombre de usuario con el cual se registró. A continuación se detallará el proceso que la aplicación realizará cuando el usuario proporcione su dirección de correo electrónico o su nombre de usuario:

- Si el usuario proporciona su dirección de correo electrónico, la aplicación validará que la misma está registrada en el sistema y de ser válida procederá a enviar las instrucciones a seguir para crear la nueva contraseña.
- Si el usuario proporciona su nombre de usuario, la aplicación validará que el usuario exista en el sistema, y ser válido, procederá a obtener la dirección de correo electrónico asociada al usuario y procederá a enviar las instrucciones a seguir para crear la nueva contraseña.

3.2.1.4 Recordar nombre de usuario (RF04)

Cuando el usuario no recuerde su nombre de usuario para acceder a la aplicación, podrá seleccionar la opción “Recordar nombre de usuario” en la pantalla de autenticación, al seleccionar dicha opción la aplicación solicitará la dirección de correo electrónico con la cual se registró, y procederá a validar esta exista en el sistema, de ser válida se procederá a enviar el nombre de usuario a la dirección de correo proporcionada.

3.2.1.5 Actualizar información de usuario (RF05)

Una vez que el usuario se ha autenticado en la aplicación, este podrá en cualquier momento actualizar su información permitida de manera parcial o total, los datos que la aplicación permitirá actualizar serán los siguientes: nombres, apellidos, certificado de firma electrónica, dirección de correo electrónico, nombre de usuario del sistema y contraseña de acceso.

3.2.1.6 Firmar y sellar documentos en formato XML (RF06)

Los usuarios podrán aplicar una firma con sello de tiempo a sus documentos XML, para lo cual deberán estar autenticados en la aplicación y

seleccionar la opción “Firmar y sellar”, los datos necesarios para realizar este proceso serán los siguientes:

- **Documento XML sin firma.**- El cual debe estar debidamente formado y contiene la información que se desea firmar electrónicamente y aplicar el sello de tiempo.
- **Certificado de firma electrónica.**- Si el usuario cargo su certificado de firma al momento del registro, este será cargado automáticamente por el sistema, caso contrario deberá cargarlo temporalmente para poder realizar el proceso.
- **PIN del certificado.**- Es el pin del certificado con el cual se va a realizar el proceso de firma.

Una vez proporcionados los datos anteriores el usuario podrá firmar y sellar su documento, y tendrá la opción de descargar el nuevo documento con la firma y sello de tiempo aplicado, una vez firmado el documento este podrá ser descargado por el usuario y almacenado en la base de datos para su posterior descarga.

3.2.1.7 Repositorio de documentos firmados (RF07)

Los usuarios tendrán la opción de consultar, eliminar o descargar los documentos previamente firmados y sellados, para lo cual deberán indicar un rango de fechas de los documentos firmados, los mismos que serán mostrados en una tabla, mostrando únicamente la información básica como: número del documento, nombre del documento y fecha de creación, además de las opciones: ver detalle de firma y sello de tempo y descargar documento firmado.

3.2.1.8 Actualizar parámetros de la aplicación (RF08)

Permite al usuario administrador actualizar los parámetros de la aplicación detallados a continuación:

- **URL de la TSA.**- Es la dirección URL provista por la TSA para realizar el consumo de sellos de tiempo.
- **Nombre de usuario y contraseña.**- Son los datos proporcionados por la TSA al momento de la contratación del servicio de sellado de tiempo, estos datos será usados en la autenticación en la URL de la TSA para la solicitud de un sello de tiempo.

3.2.1.9 Interfaz de la aplicación (RNF01)

La aplicación deberá contar con una interfaz de usuario sencilla y de fácil manejo para los usuarios del sistema.

3.2.1.10 Conexión a internet del dispositivo donde se use la aplicación (RNF02)

El dispositivo debe estar conectado a una red con acceso a internet para poder realizar el proceso de firma, sellado de tiempo y consulta de documentos firmados.

3.2.1.11 Seguridad de la información (RNF03)

Garantizar la seguridad de la aplicación con respecto a la información procesada y almacenada, información como: Datos del usuario, certificado de firma electrónica y documentos firmados.

3.2.1.12 PIN del certificado (RNF04)

La aplicación no guardará en su base de datos ni en ningún otro medio el PIN del certificado de firma electrónica, este deberá ser ingresado por el usuario en cada proceso que requiera hacer uso del mismo.

3.2.1.13 Otros requisitos

La funcionalidad de firma electrónica y sellado de tiempo diseñada para la presente aplicación, deberá ser implementada en el proceso realizado en el sistema de Factoring Electrónico desarrollado por la empresa BIGDATA C.A.

3.2.2 Diseño del proceso de firma electrónica y sellado de tiempo para la aplicación Web de Time Stamping

3.2.2.1 Proceso de la aplicación

Tomando en cuenta el proceso para realizar una firma electrónica, sello de tiempo y los requerimientos de la empresa BIGDATA C.A especificados en el Anexo 01, se diseñó el proceso principal a ser realizado por la Aplicación Web de Time Stamping, el mismo que consiste en aplicar la firma electrónica y el sello de tiempo a un documento en formato XML (ver Figura 12).

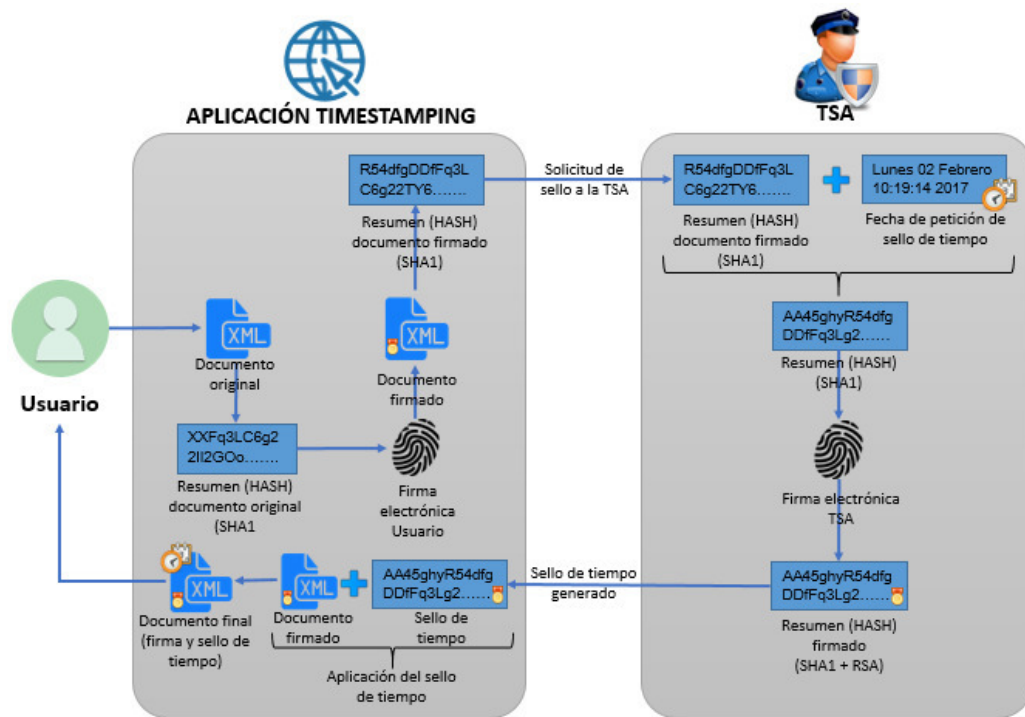


Figura 12 Proceso para la aplicación Web de Time Stamping

3.2.3 Diagramas de Casos de Uso

3.2.3.1 Definición de Actores del Sistema

Previo al desarrollo de la aplicación se procedió a definir los actores involucrados en el sistema: (a) usuario general quien representa a cualquier persona que desee hacer uso de la aplicación de Time Stamping y (b) usuario administrador quien representa a la entidad contratante del servicio de sellado de tiempo con la TSA y se encargará de la administración de la aplicación.

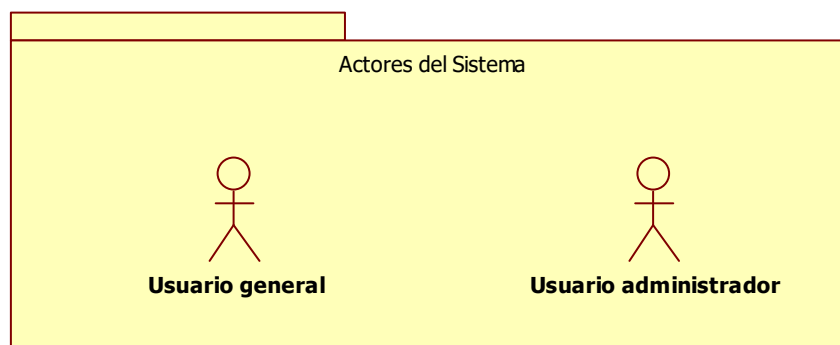


Figura 13 Definición de actores

3.2.3.2 Definición de tareas por actor

Usuario general:

- Registrarse
- Autenticarse para ingresar a la aplicación
- Solicitar nueva contraseña
- Recordar nombre de usuario
- Actualizar información
- Firmar y sellar documentos en formato XML
- Ver repositorio de documentos firmados y sellados
- Visualizar detalle de firma y sello de tiempo de un determinado documento

Usuario administrador:

- Autenticarse para ingresar a la aplicación
- Solicitar nueva contraseña
- Recordar nombre de usuario
- Actualizar información
- Actualizar parámetros del sistema

3.2.3.3 Diagrama de caso de uso general

El objetivo del diagrama de caso de uso general es obtener una idea general de como los usuarios interactuaran con la aplicación, y esta a su vez con la TSA, para realizar el proceso de firma electrónica y sellado de tiempo (ver Figura 14).

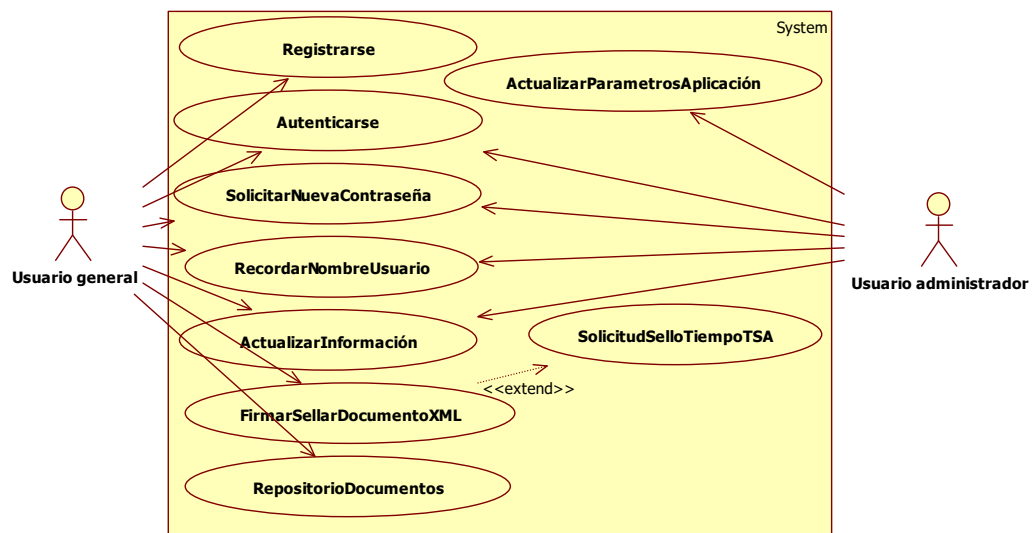


Figura 14 Diagrama de caso de uso general

3.2.4 Descripción de Casos de Uso

3.2.4.1 Caso de uso Registrarse

La descripción se muestra en la Tabla 4.

Tabla 4

Descripción caso de uso “Registrarse”

Caso de uso:	Registrarse (CU_001)
Descripción:	Permite realizar el registro en la aplicación
Actores:	Usuario general
Pre-condiciones:	Ninguna
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario ingresa su número de cedula, apellidos, certificado de firma electrónica (opcional) dirección de correo electrónico, nombre de usuario para la aplicación y contraseña de acceso a la misma. 2. El usuario da clic en el botón “Registrarse”. 3. El sistema verifica que la información ha sido ingresada correctamente. 4. El usuario queda registrado para poder hacer uso de la aplicación.
Escenario alternativo:	<ol style="list-style-type: none"> a. Los datos ingresados por el usuario no están completos o son incorrectos <ol style="list-style-type: none"> 1. El sistema informa que cuales de los datos están incorrectos. 2. El usuario corrige los datos. 3. Continúa con el punto 2 del escenario principal.

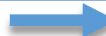
3.2.4.2 Caso de uso Autenticarse

La descripción se muestra en la Tabla 5.

Tabla 5

Descripción caso de uso “Autenticarse”

Caso de uso:	Registrarse (CU_002)
Descripción:	Permite a los usuarios registrados acceder a la aplicación
Actores:	Usuario general y Usuario administrador
Pre-condiciones:	El usuario debe estar registrado en el sistema
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario ingresa su nombre de usuario y contraseña. 2. El usuario da clic en el botón “Ingresar”. 3. El sistema verifica que la información ha sido ingresada correctamente, y que el usuario este previamente registrado en el sistema.

Continúa 

	4. El sistema muestra la pantalla principal de la aplicación, donde se muestran las acciones que el usuario puede realizar.
Escenario alternativo:	<ul style="list-style-type: none"> a. Los datos de ingreso no son correctos <ul style="list-style-type: none"> 1. El sistema muestra mensaje de error de datos incorrectos. 2. El usuario corrige los datos de ingreso. 3. Continúa con el punto 2 del escenario principal.

3.2.4.3 Caso de uso Solicitar nueva contraseña

La descripción se muestra en la Tabla 6.

Tabla 6

Descripción caso de uso “Solicitar nueva contraseña”

Caso de uso:	Solicitar nueva contraseña (CU_003)
Descripción:	Permite a los usuarios solicitar una contraseña para acceder a la aplicación
Actores:	Usuario general y Usuario administrador
Pre-condiciones:	El usuario debe estar registrado en la aplicación
Actividades:	
Escenario principal:	<ul style="list-style-type: none"> a. El usuario ingresa su nombre de acceso al sistema. <ul style="list-style-type: none"> 1. El sistema verifica que el nombre de usuario exista y envía las instrucciones a seguir para crear la nueva contraseña a la dirección de correo electrónico vinculada al usuario. 2. El usuario sigue las instrucciones recibidas en su correo y crea la nueva contraseña. b. El usuario ingresa su dirección de correo electrónico. <ul style="list-style-type: none"> 1. El sistema verifica que la dirección de correo esté vinculada a un usuario del sistema y envía las instrucciones a seguir para crear la nueva contraseña. 2. El usuario sigue las instrucciones recibidas en su correo y crea la nueva contraseña.
Escenario alternativo:	<ul style="list-style-type: none"> a. El nombre de usuario no existe o el correo electrónico no está vinculado a ningún usuario del sistema. <ul style="list-style-type: none"> 1. El sistema muestra mensaje de error de nombre de usuario o correo no existente, según sea el caso. 2. El usuario ingresa el nombre de usuario o correo correcto. 3. Continúa con el punto 2 del escenario principal.

3.2.4.4 Caso de uso Recordar nombre de usuario

La descripción se muestra en la Tabla 7.

Tabla 7

Descripción caso de uso “Recordar nombre de usuario”

Caso de uso:	Recordar nombre de usuario (CU_004)
Descripción:	Permite a los usuarios recordar su nombre de usuario de acceso al sistema
Actores:	Usuario general y Usuario administrador
Pre-condiciones:	El usuario debe estar registrado en el sistema
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario ingresa la dirección de correo electrónico con la cual se registró. 2. El usuario da clic en el botón “Recordar nombre de usuario”. 3. El sistema verifica que la dirección de correo este asociada a un usuario y envía el nombre de este a la dirección de correo proporcionada.
Escenario alternativo:	<ol style="list-style-type: none"> a. La dirección de correo electrónico no está vinculada a ningún usuario del sistema. <ol style="list-style-type: none"> 4. El sistema muestra mensaje de error de correo no asociado a un usuario. 5. El usuario ingresa la dirección de correo correcta. 6. Continúa con el punto 2 del escenario principal.


3.2.4.5 Caso de uso Actualizar información

La descripción se muestra en la Tabla 8.

Tabla 8

Descripción caso de uso “Actualizar información”

Caso de uso:	Actualizar información (CU_005)
Descripción:	Permite a los usuarios actualizar la información con la cual se registró en el sistema
Actores:	Usuario general y Usuario administrador
Pre-condiciones:	El usuario debe estar registrado en el sistema
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario modifica uno o varios de los siguientes datos de registro: nombres, apellidos, certificado de firma electrónica, dirección de correo electrónico, nombre de usuario del sistema y contraseña de acceso. 2. El usuario da clic en el botón “Guardar cambios”. 3. El sistema verifica que la información ingresada este correcta y procede a guardar los cambios realizados por el usuario.

Continúa 

Escenario alternativo:	<ol style="list-style-type: none"> a. Uno o varios de los datos están ingresados incorrectamente. <ol style="list-style-type: none"> 1. El sistema muestra mensaje de error en el ingreso de datos. 2. El usuario corrige los datos ingresados incorrectamente. 3. Continúa con el punto 2 del escenario principal.
------------------------	--

3.2.4.6 Caso de uso Firmar y sellar documento XML

La descripción se muestra en la Tabla 9.

Tabla 9

Descripción caso de uso “Firmar y sellar documento XML”

Caso de uso:	Firmar y sellar documento XML (CU_006)
Descripción:	Permite al usuario firmar y aplicar sellos de tiempo a documentos en formato XML
Actores:	Usuario general
Pre-condiciones:	El usuario debe estar registrado en el sistema y contar con un certificado de firma electrónica.
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario proporciona la siguiente información: documento XML al cual desea firmar y aplicar el sello de tiempo, certificado de firma electrónica (en caso que no lo haya cargado al momento del registro) y el PIN del certificado de firma. 2. El usuario da clic en el botón “Firmar y sellar documento XML”. 3. El sistema verifica que la información ingresada este correcta y que el PIN ingresado permita acceder al certificado de firma. 4. El sistema procede a realizar el proceso de firma electrónica y sello de tiempo. 5. El sistema almacena el documento firmado y da la opción de descargarlo.
Escenario alternativo:	<ol style="list-style-type: none"> a. Uno o varios de los datos ingresados están ingresados incorrectamente. <ol style="list-style-type: none"> 1. El sistema muestra mensaje de error en el ingreso de datos. 2. El usuario corrige los datos ingresados incorrectamente. 3. Continúa con el punto 2 del escenario principal. b. El PIN del certificado no permite acceder al mismo.

Continúa 

1. El sistema muestra el mensaje de error que no se pudo acceder al certificado con el PIN proporcionado.
2. El usuario corrige el PIN ingresado.
3. Continúa con el punto 3 del escenario principal.

3.2.4.7 Caso de uso Repositorio de documentos

La descripción se muestra en la Tabla 10.

Tabla 10

Descripción caso de uso “Repositorio de documentos”

Caso de uso:	Repositorio de documentos (CU_007)
Descripción:	Permite al usuario visualizar todos los documentos a los cuales se han firmado y sellado en el sistema, dando la posibilidad de descargarlo o eliminarlo del sistema.
Actores:	Usuario general
Pre-condiciones:	El usuario debe estar registrado en el sistema y haber firmado y sellado al menos un documento.
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario selecciona el rango de fechas, en el cual desea consultar los documentos firmados y sellados. 2. El usuario da clic en botón “Consultar”. 3. El sistema muestra los documentos firmados en el rango de fechas seleccionado por el usuario. 4. El usuario realiza las acciones de descargar o eliminar uno o varios documentos del sistema. 5. El sistema procede a realizar la acción seleccionada por el usuario, ya sea de descarga o eliminación.
Escenario alternativo:	<ol style="list-style-type: none"> a. No existe ningún documento firmado en el rango de fechas seleccionado por el usuario. <ol style="list-style-type: none"> 1. El sistema muestra mensaje de advertencia que no existen comprobantes firmados y sellados en el rango de fechas seleccionado. 2. El usuario cambia el rango de fechas. 3. Continúa con el punto 2 del escenario principal.

3.2.4.8 Caso de uso Actualizar parámetros de la aplicación

La descripción se muestra en la Tabla 11.

Tabla 11

Descripción caso de uso “Actualizar parámetros de la aplicación”

Caso de uso:	Actualizar parámetros de la aplicación (CU_009)
Descripción:	Permite al usuario actualizar los parámetros de la aplicación, los parámetros a actualizar serán los siguientes: URL de la TSA, nombre de usuario y contraseña proporcionados por la TSA al momento de contratar el servicio de sellos de tiempo.
Actores:	Usuario administrador
Pre-condiciones:	El usuario debe estar registrado en el sistema y ser administrador del mismo.
Actividades:	
Escenario principal:	<ol style="list-style-type: none"> 1. El usuario ingresa los parámetros a actualizar. 2. El usuario da clic en el botón “Probar parámetros de conexión”. 3. El usuario da clic en el botón actualizar parámetros. 4. El sistema actualiza los parámetros de la aplicación.
Escenario alternativo:	<ol style="list-style-type: none"> a. Los parámetros ingresados por el usuario no permiten realizar una conexión exitosa con la TSA. <ol style="list-style-type: none"> 1. El usuario corrige los parámetros 2. Continúa con el punto 2 del escenario principal.

3.2.5 Diagramas de Secuencia

3.2.5.1 Diagrama de secuencia “Registro de usuario”

La Figura 15 muestra el diagrama de secuencia para el caso de uso “Registro de usuario”.

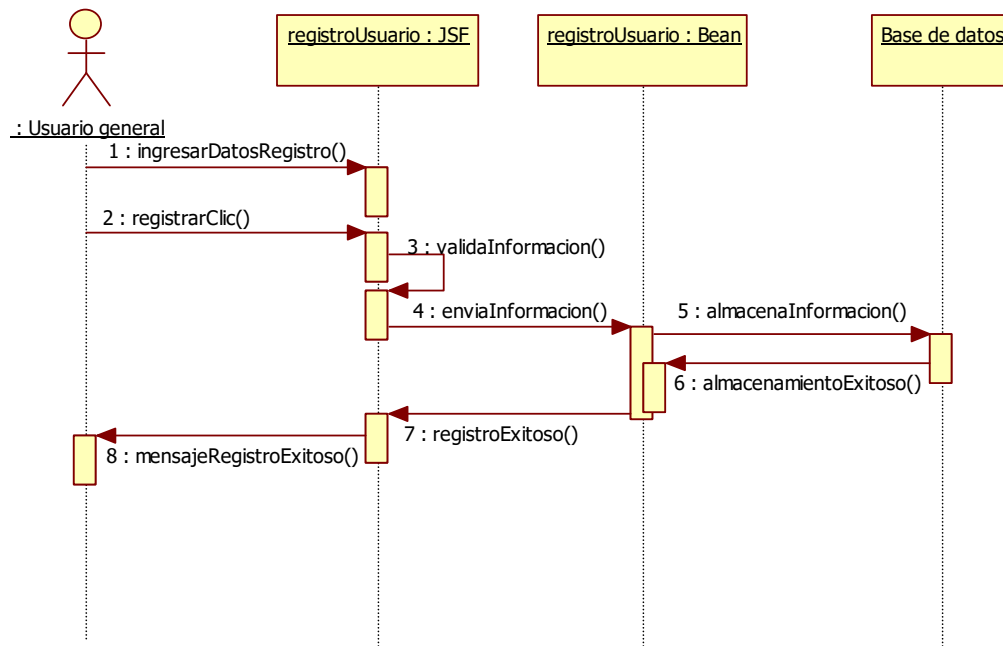


Figura 15 Diagrama de secuencia Registrar usuario

3.2.5.2 Diagrama de secuencia “Autenticación de usuario”

La Figura 16 muestra el diagrama de secuencia para el caso de uso “Autenticación de usuario”.

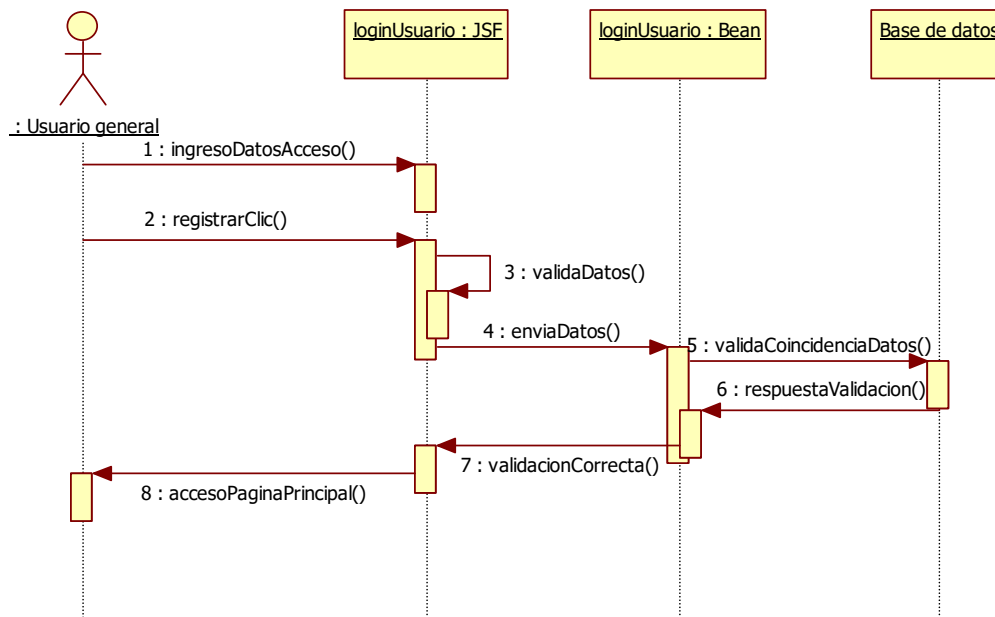


Figura 16 Diagrama de secuencia Autenticar usuario

3.2.5.3 Diagrama de secuencia “Solicitar nueva contraseña”

La Figura 17 muestra el diagrama de secuencia para el caso de uso “Solicitar nueva contraseña”.

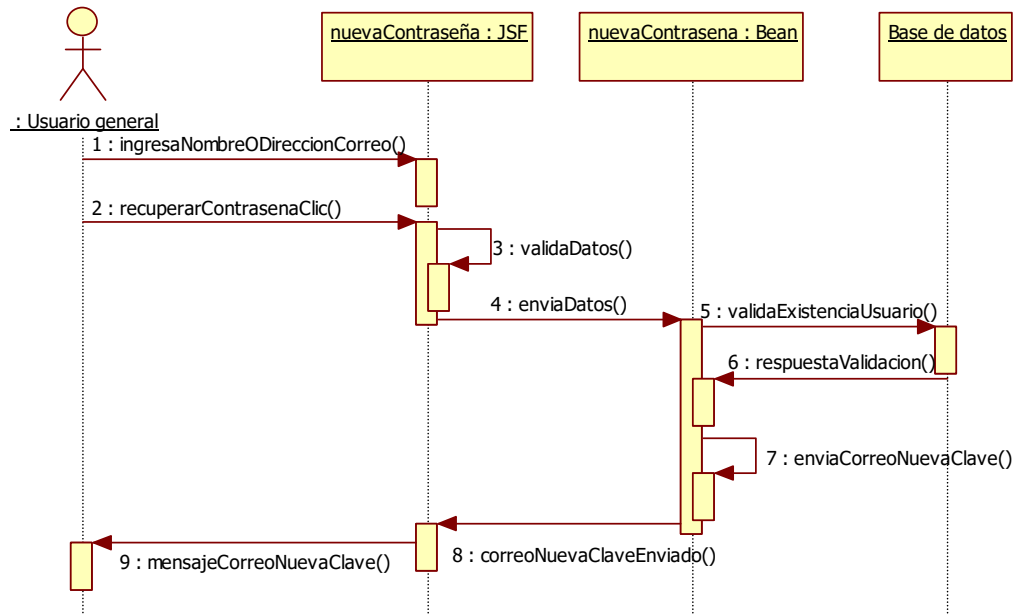


Figura 17 Diagrama de Solicitar nueva contraseña

3.2.5.4 Diagrama de secuencia “Recordar nombre usuario”

La Figura 18 muestra el diagrama de secuencia para el caso de uso “Recordar nombre de usuario”.

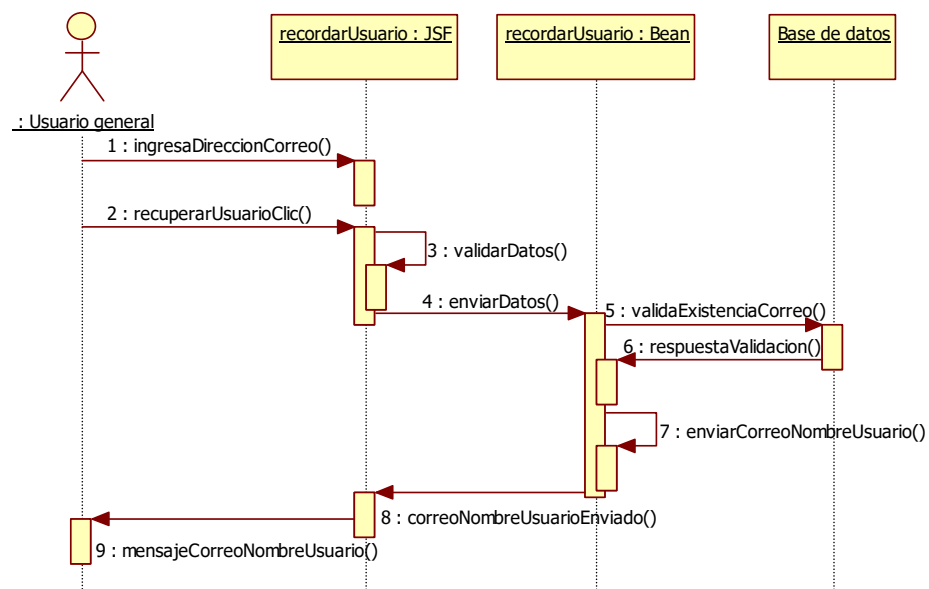


Figura 18 Diagrama de secuencia Recordar nombre usuario

3.2.5.5 Diagrama de secuencia “Actualizar información”

La Figura 19 muestra el diagrama de secuencia para el caso de uso “Actualizar información”.

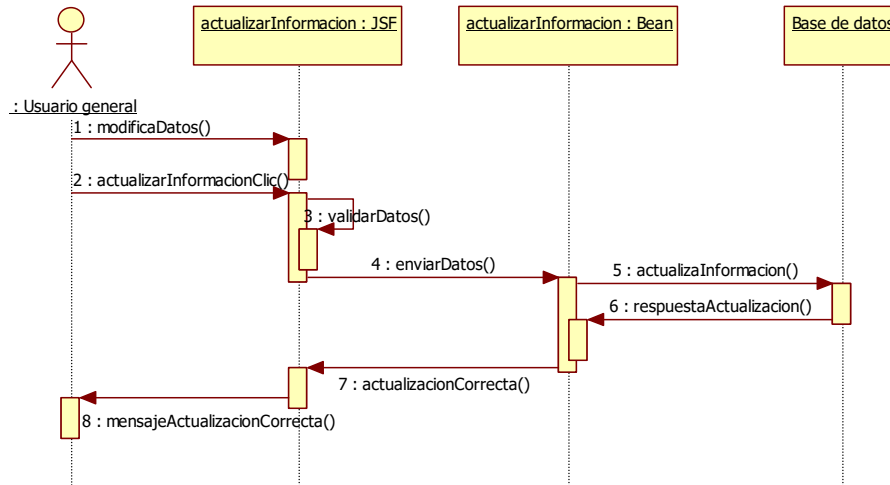


Figura 19 Diagrama de secuencia Actualizar información

3.2.5.6 Diagrama de secuencia “Firmar y sellar documento XML”

La Figura 20 muestra el diagrama de secuencia para el caso de uso “Firmar y sellar documento XML”.

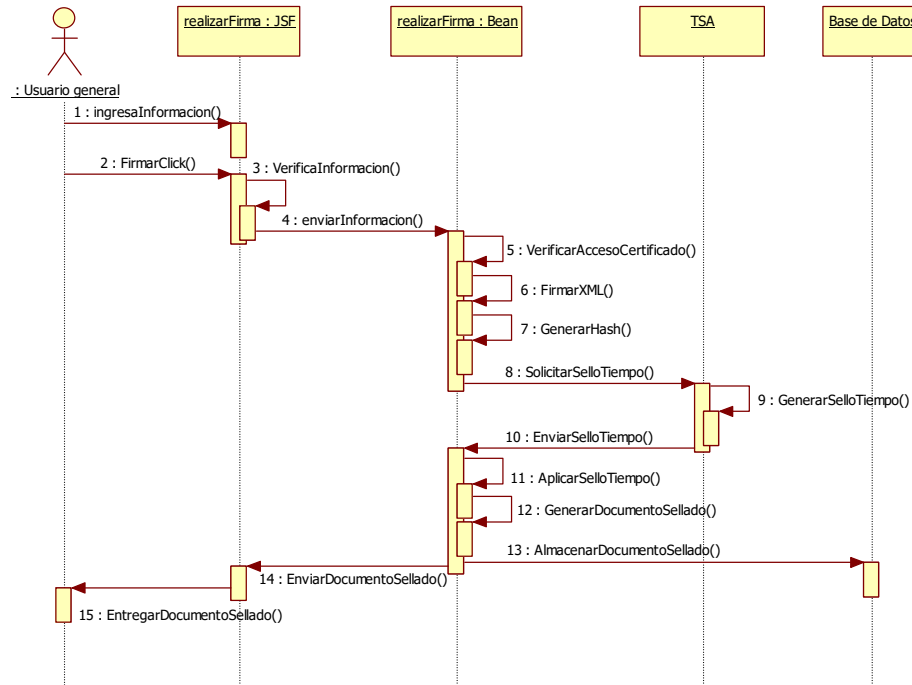


Figura 20 Diagrama de secuencia Firmar y sellar documento XML

3.2.5.7 Diagrama de secuencia “Repositorio Documentos”

La Figura 21 muestra el diagrama de secuencia para el caso de uso “Repositorio documentos”.

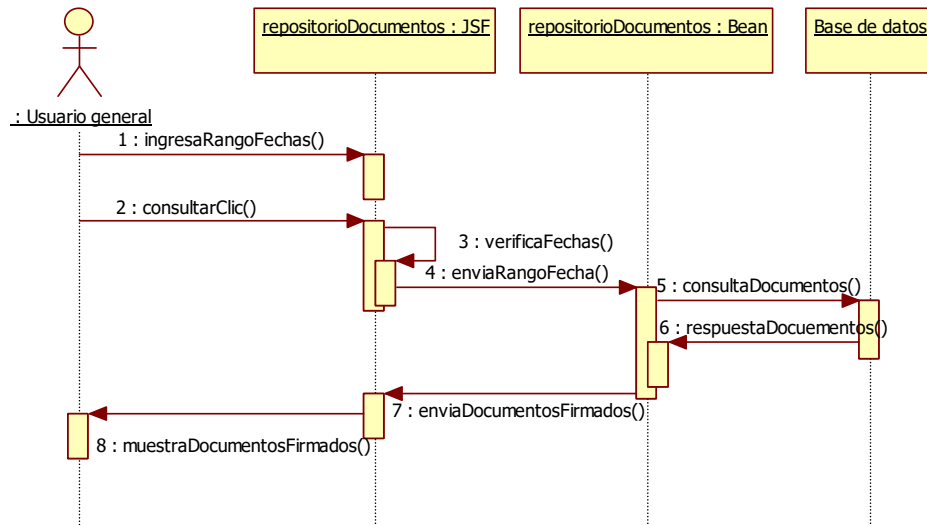


Figura 21 Diagrama de secuencia Repositorio documentos

3.2.5.8 Diagrama de secuencia “Actualizar parámetros de la aplicación”

La Figura 22 muestra el diagrama de secuencia para el caso de uso “Actualizar parámetros de la aplicación”.

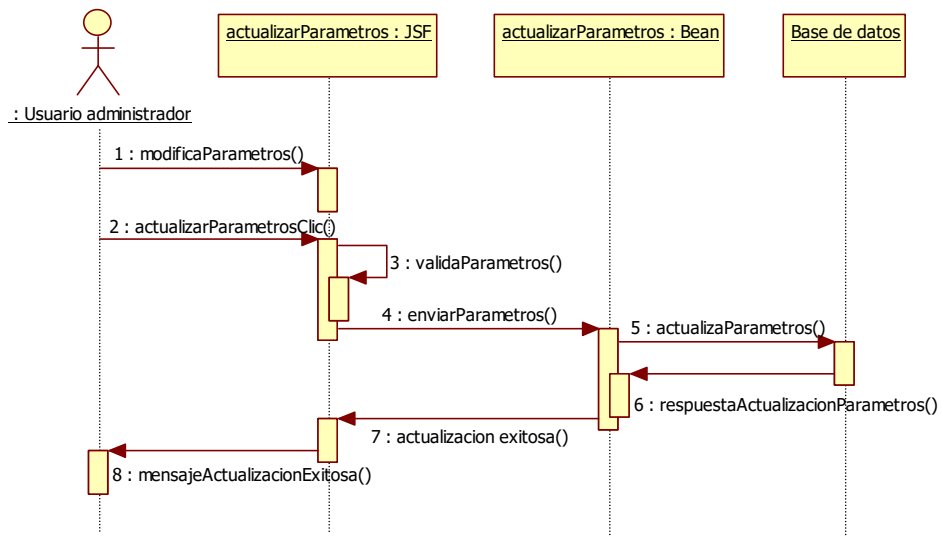


Figura 22 Diagrama de secuencia Actualizar parámetros de la aplicación

3.2.6 Diagramas de Actividades

3.2.6.1 Diagrama de actividad “Registro de usuario”

La Figura 23 muestra el diagrama de actividad para el caso de uso “Registro de usuario”.

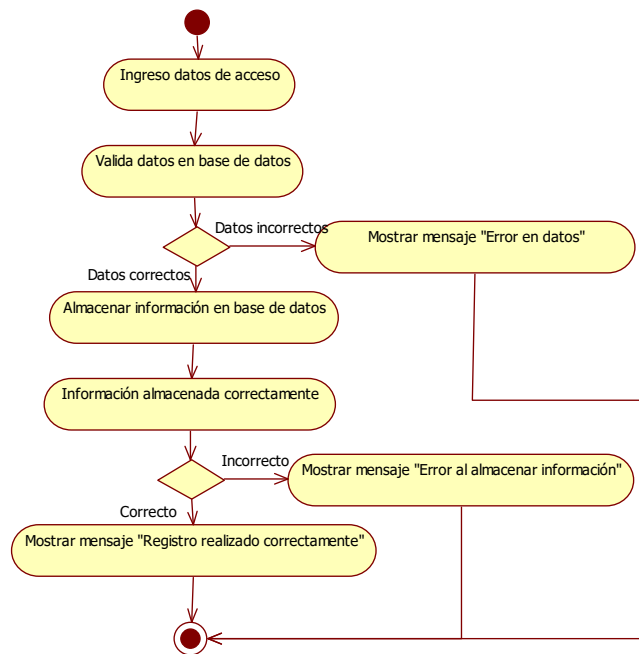


Figura 23 Diagrama de actividad Registro de usuario

3.2.6.2 Diagrama de actividad “Autenticación de usuario”

La Figura 24 muestra el diagrama de actividad para el caso de uso “Autenticación de usuario”.

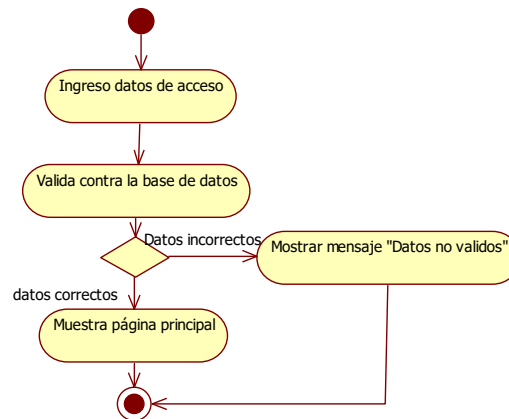


Figura 24 Diagrama de actividad Autenticación de usuario

3.2.6.3 Diagrama de actividad “Solicitar nueva contraseña”

La Figura 25 muestra el diagrama de actividad para el caso de uso “Solicitar nueva contraseña”.

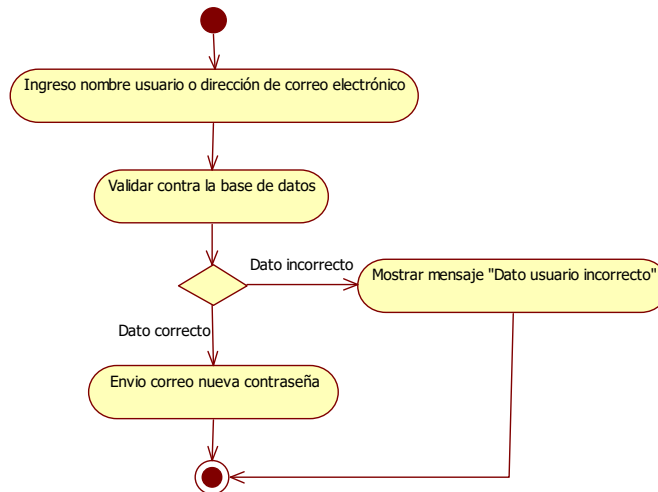


Figura 25 Diagrama de actividad Solicitar nueva contraseña

3.2.6.4 Diagrama de actividad “Recordar nombre de usuario”

La Figura 26 muestra el diagrama de actividad para el caso de uso “Recordar nombre de usuario”.

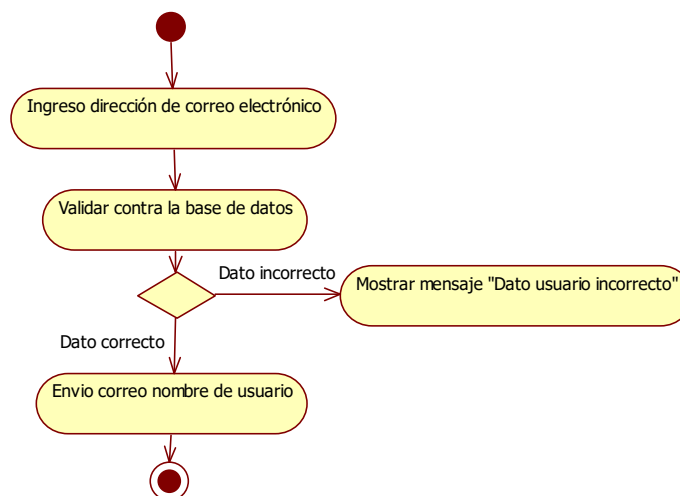


Figura 26 Diagrama de actividad Recordar nombre de usuario

3.2.6.5 Diagrama de actividad “Actualizar información”

La Figura 27 muestra el diagrama de actividad para el caso de uso “Actualizar información”.

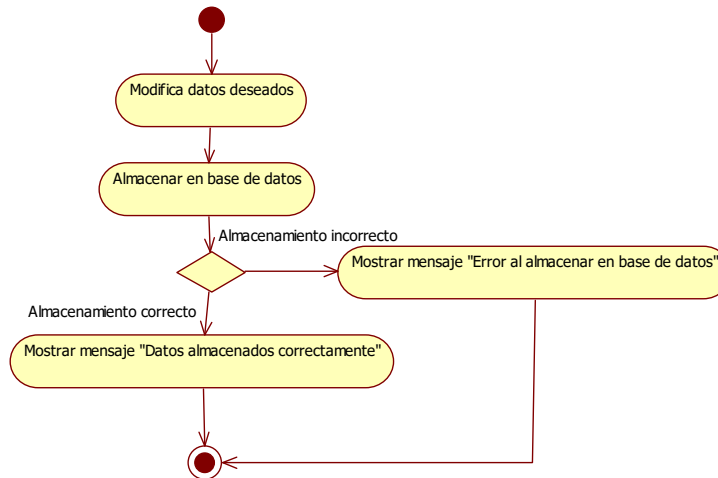


Figura 27 Diagrama de Actualizar información

3.2.6.6 Diagrama de actividad “Firmar y sellar documento XML”

La Figura 28 muestra el diagrama de actividad para el caso de uso “Firmar y sellar documentos XML”.

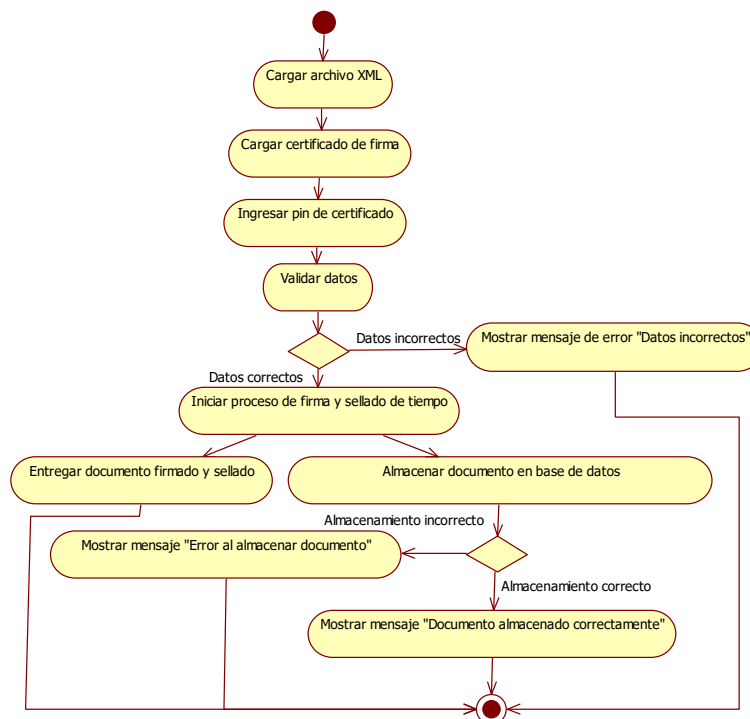


Figura 28 Diagrama de actividad Firmar y sellar documento XML

3.2.6.7 Diagrama de actividad “Repositorio documentos”

La Figura 29 muestra el diagrama de actividad para el caso de uso “Repositorio documentos”.

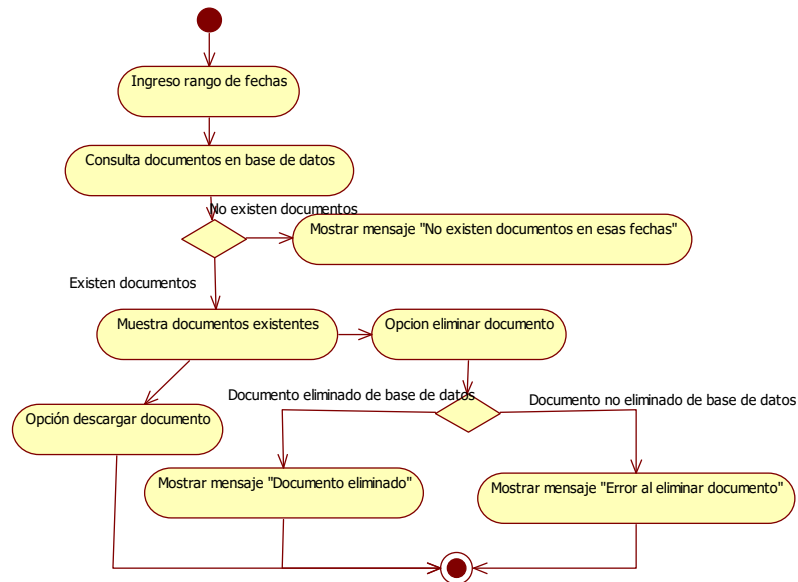


Figura 29 Diagrama de actividad Repositorio documentos

3.2.6.8 Diagrama de actividad “Visualizar detalle de firma y sello de tiempo”

La Figura 30 muestra el diagrama de actividad para el caso de uso “Visualizar detalle de firma y sello de tiempo”.

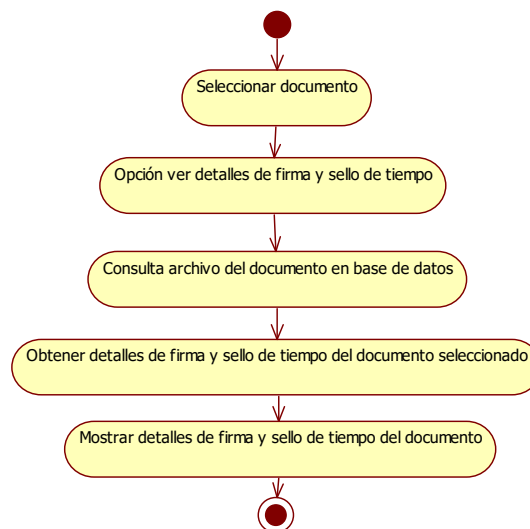


Figura 30 Diagrama de actividad Visualizar detalle de firma y sello de tiempo

3.2.6.9 Diagrama de actividad “Actualizar parámetros de la aplicación”

La Figura 31 muestra el diagrama de actividad para el caso de uso “Actualizar parámetros de la aplicación”.

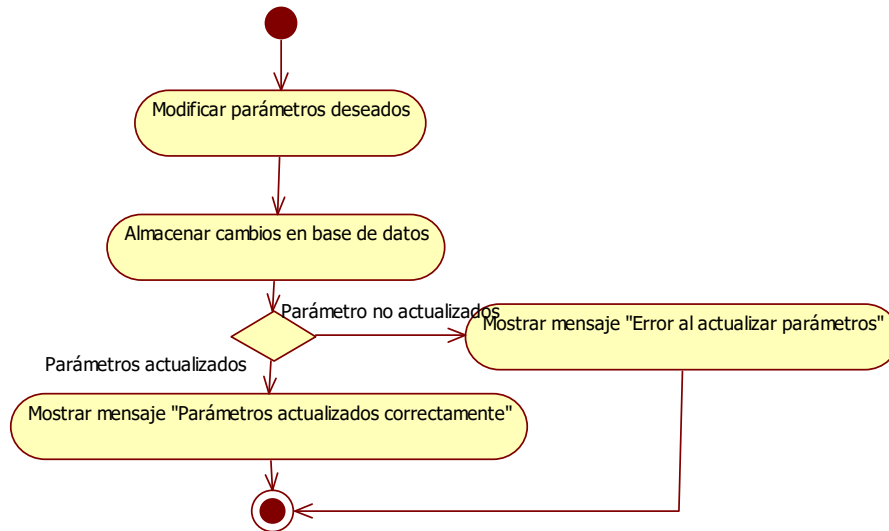


Figura 31 Diagrama de actividad Actualizar parámetros de la aplicación

3.2.7 Diagrama de Despliegue

La Figura 32 muestra la relación entre el cliente, el servidor Web, la TSA y la base de datos, a continuación se describe cada una de las partes involucradas:

- **Cliente.**- usuario que desea realizar el proceso de firma y sellado de tiempo de un documento XML.
- **Servidor Web.**- conformada por la Aplicación Web de Time Stamping y la Interfaz con la TSA donde se utiliza una autenticación “Http” básica para poder hacer la solicitud del servicio de sellado de tiempo.
- **TSA.**- la entidad que atiende las solicitudes de sellos de tiempo realizados por la aplicación.
- **Base de Datos.**- es donde se almacenara la información de los usuarios y los documentos que estos han firmado y sellado en la aplicación.

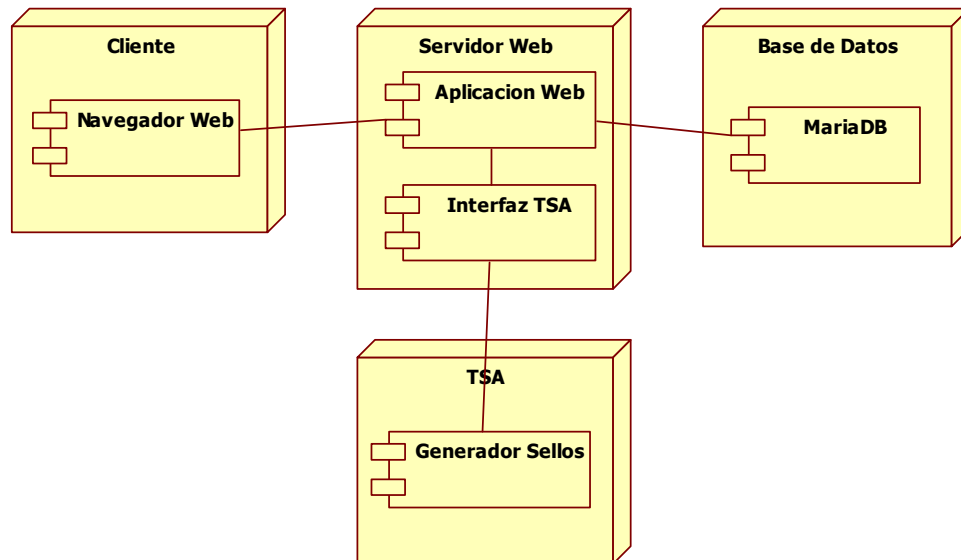


Figura 32 Diagrama de despliegue

3.2.8 Modelo de datos

3.2.8.1 Modelo conceptual de base de datos

A continuación se presenta el modelo conceptual de Base de Datos para aplicación Web de Time Stamping:

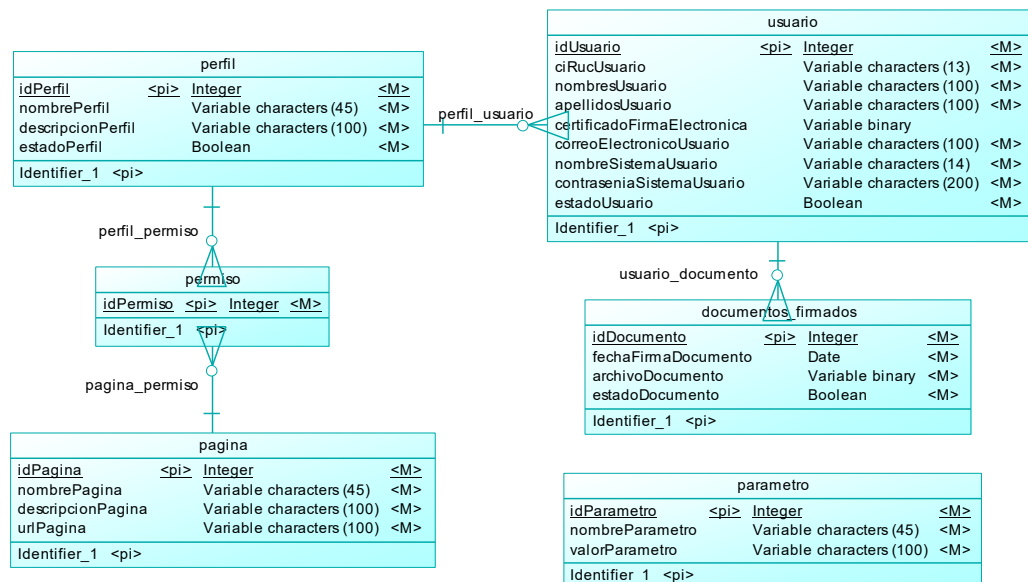


Figura 33 Modelo conceptual de Base Datos

3.2.8.2 Modelo lógico de base de datos

A continuación se presenta el modelo lógico de Base de Datos para aplicación Web de Time Stamping:

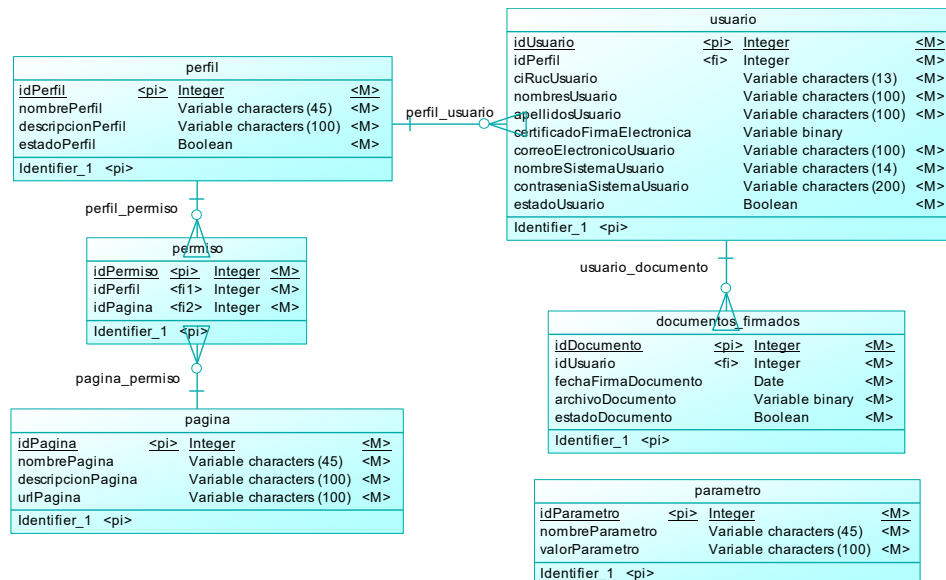


Figura 34 Modelo lógico de Base Datos

3.2.8.3 Modelo físico de base de datos

A continuación se presenta el modelo físico de Base de Datos para aplicación Web de Time Stamping:

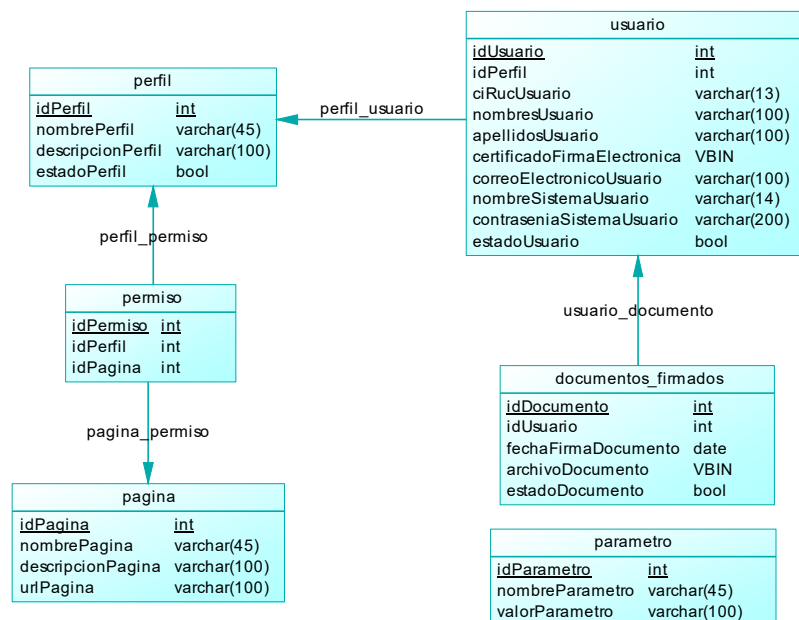


Figura 35 Modelo físico de Base Datos

3.2.9 Diagramas navegación

3.2.9.1 Diagrama de navegación usuario general

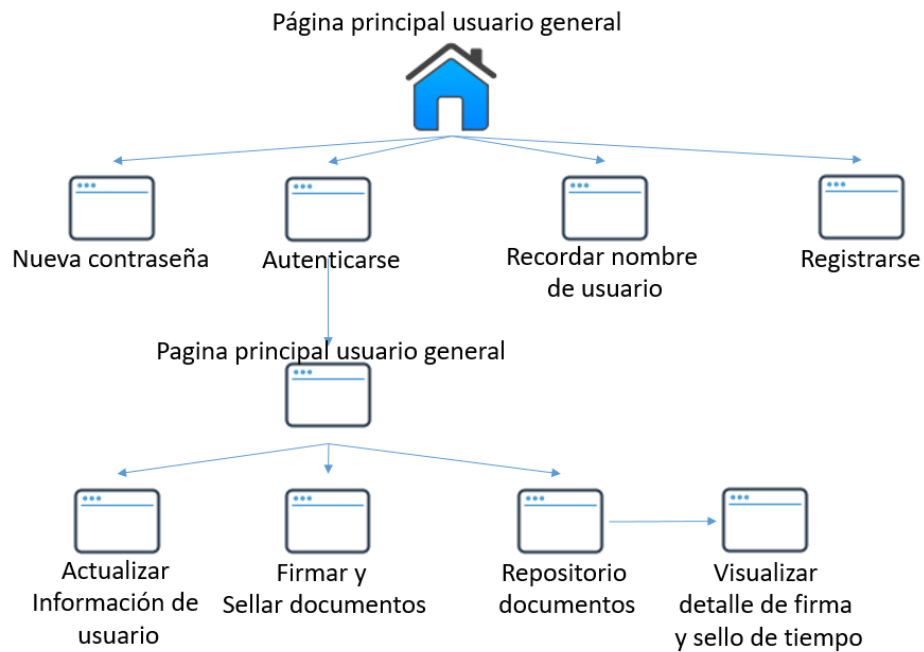


Figura 36 Diagrama de navegación usuario general

3.2.9.2 Diagrama de navegación usuario administrador

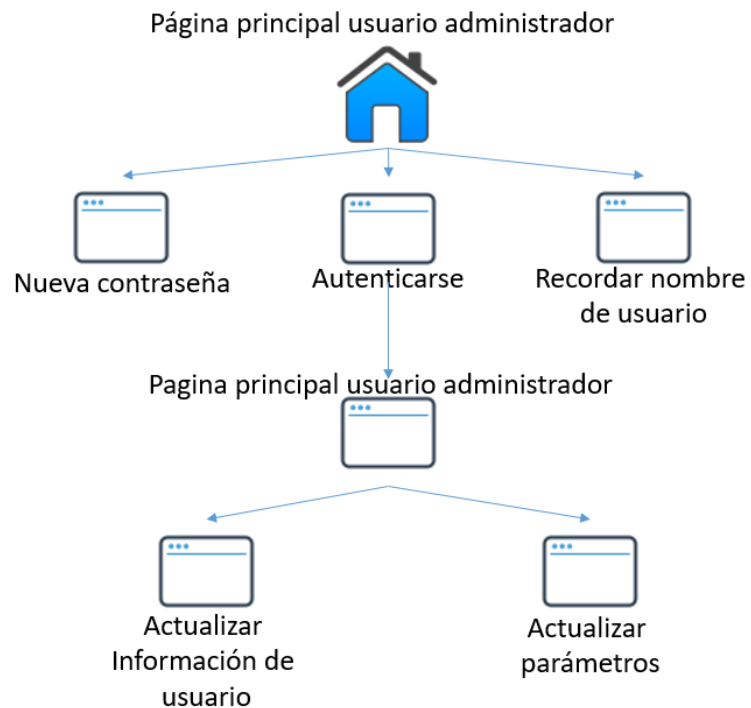


Figura 37 Diagrama de navegación usuario administrador

CAPÍTULO IV

IMPLEMENTACIÓN DE LA APLICACIÓN WEB DE TIME STAMPING Y ADAPTACIÓN DE LA FUNCIONALIDAD DE FIRMA Y SELLADO DE TIEMPO EN EL SISTEMA DE FACTORING ELECTRÓNICO DESARROLLADO POR LA EMPRESA BIGDATA C.A

4.1 IMPLEMENTACIÓN DE LA APLICACIÓN WEB DE TIME STAMPING

4.1.1 Script de base de datos

El script de creación de la base de datos se adjuntó en el Anexo 02.

4.1.2 Paquetes y clases la aplicación

Para la implementación de la Aplicación de Time Stamping se crearon los siguientes paquetes y clases (Ver Figura 38):

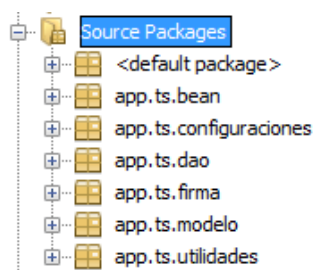


Figura 38 Paquetes creados para la aplicación

A continuación se describirá cada paquete y el contenido del mismo:

Tabla 12
Paquete Bean

Nombre del paquete	app.ts.bean
Descripción	Contiene las clases que manejan las páginas de la aplicación
Clases	FirmarSellarBean.java LoginBean.java MenuBean.java ParametrosBean.java RepositorioBean.java UsuariosBean.java

Tabla 13
Paquete Configuraciones

Nombre del paquete	app.ts.configuraciones
Descripción	Contiene las clases que cargan las configuraciones iniciales para la aplicación.
Clases	CargarParametros.java InicializarAplicacion.java Parametros.java

Tabla 14
Paquete Dao

Nombre del paquete	app.ts.dao
Descripción	Contiene los accesos a los objetos (Data Access Object) correspondientes a las entidades, para interactuar con la base de datos.
Clases	DocumentoDao.java PaginaDao.java ParametroDao.java PefrilDao.java PermisoDao.java UsuarioDao.java

Tabla 15
Paquete Firma

Nombre del paquete	app.ts.firma
Descripción	Contiene las clases necesarias para realizar el proceso de firma y sello de tiempo, estas clases hacen uso de las librerías "PolygonESL-2.0" facilitadas por la TSA
Clases	FirmaArchivo.java SignDocument.java

Tabla 16
Paquete Modelo

Nombre del paquete	app.ts.modelo
--------------------	----------------------

Continúa 

Descripción	Contiene los modelos de las entidades
Clases	DocumentosFirmados.java Pagina.java Parametro.java Perfil.java Permiso.java Usuario.java

Tabla 17
Paquete Utilidades

Nombre del paquete	app.ts.utilidades
Descripción	Contiene clases adicionales que se integran con las librerías “PolygonESL-2.0” para el proceso de firma, además de varios métodos en común con otras clases que ayudan a la reutilización de código.
Clases	ConsolePrivateKeySelector.java PrivateKySelector.java Utilidades.java

4.1.3 Ejecución de la aplicación

A continuación se muestran las capturas obtenidas de las principales secciones de la aplicación:

4.1.3.1 Registro de usuario

La Figura 39 muestra la página para el registro de un nuevo usuario de la aplicación.


 APLICACIÓN TIMESTAMPING

Registro de usuario

Los campos con (*) son obligatorios.

Número de cédula: *	<input type="text"/>	Nombre de usuario: *	<input type="text"/>
Contraseña: *	<input type="text"/>	Repetir contraseña: *	<input type="text"/>
Nombres: *	<input type="text"/>	Apellidos: *	<input type="text"/>
Certificado de firma:**	<input type="button" value="+ Seleccionar"/> <input type="button" value="Cargar"/> <input type="button" value="Cancelar"/>		Certificado actual: Ninguno
Dirección de correo electrónico: *	<input type="text"/>		

** Si proporciona el certificado de firma en este momento, este será cargado automáticamente para cada proceso de firma y sello de tiempo, de no hacerlo deberá ser cargado de manera temporal para cada proceso.

Figura 39 Página de registro para nuevo usuario

4.1.3.2 Inicio de Sesión

La Figura 40 muestra la página de inicio de sesión para acceder a la aplicación y poder hacer uso de la misma.


 APLICACIÓN TIMESTAMPING

Nombre de usuario

Contraseña

Figura 40 Página de inicio de sesión

4.1.3.3 Página principal de la aplicación

La Figura 41 muestra la página principal de la aplicación, una vez que el usuario ha accedido a la misma con su nombre de usuario y contraseña.

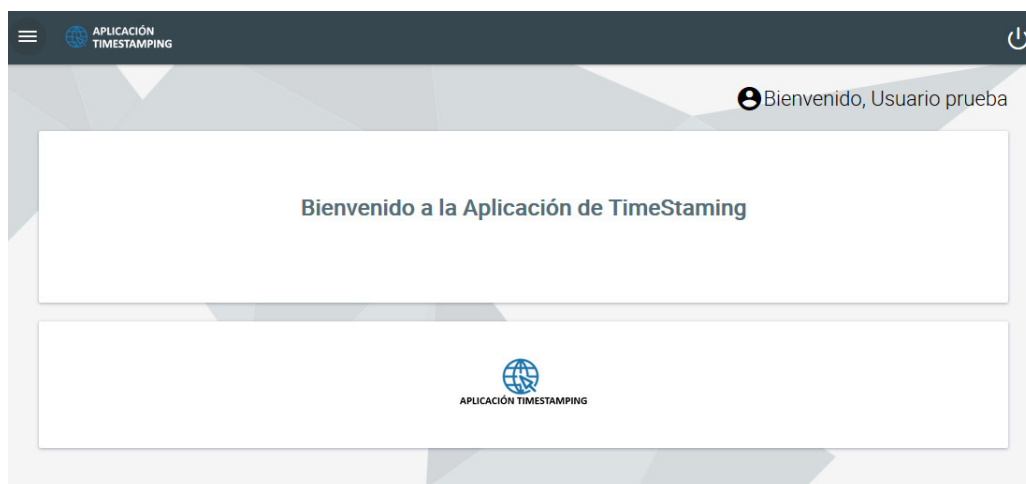


Figura 41 Página principal de la aplicación

4.1.3.4 Página de actualización de parámetros de la aplicación

La Figura 42 muestra la página de actualización de parámetros de la aplicación, dicha opción está disponible únicamente para el administrador de la aplicación, y permite actualizar los parámetros principales de la misma.

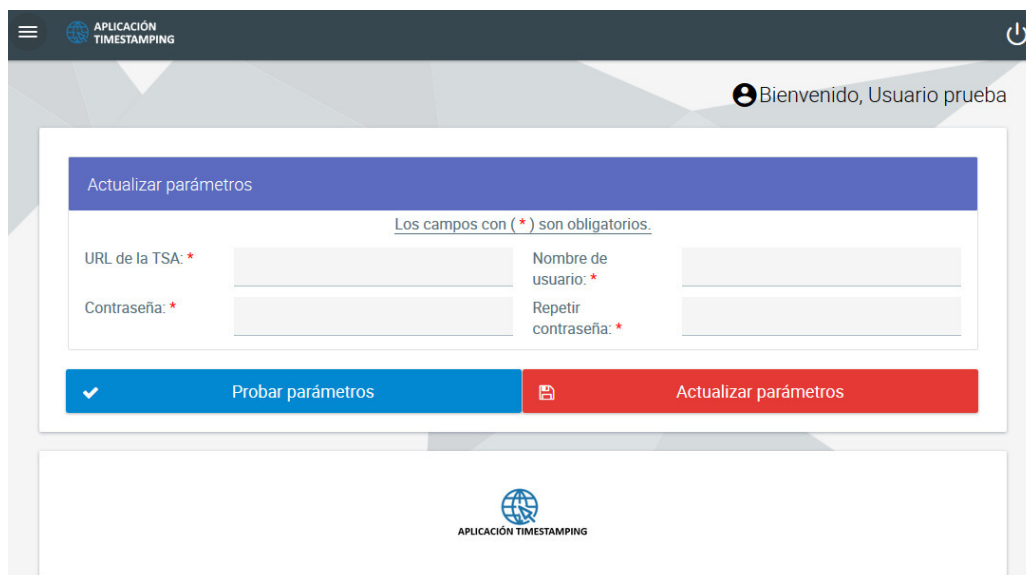


Figura 42 Página de actualización de parámetros

4.1.3.5 Página para la firma y sellado de tiempo de un documento XML

La Figura 43 muestra la página para realizar el proceso de firma y sellado de tiempo de documentos en formato XML.

APLICACIÓN TIMESTAMPING

Bienvenido, Usuario prueba

Carga de archivo XML e información del firmante

Archivo a firmar:

Archivo actual: Ninguno

Certificado de firma:

Certificado actual: Ninguno

Pin del certificado:

Figura 43 Página de firma y sellado de tiempo

4.1.3.6 Página para el repositorio de documentos firmados y sellados

La Figura 44 muestra la página donde se desplegarán todos los documentos que han sido firmados y sellados por el usuario, para poder consultar los mismos, el usuario deberá seleccionar un rango de fechas.

APLICACIÓN TIMESTAMPING

Bienvenido, Usuario prueba

Repositorio documentos

Fecha desde: Fecha hasta:

Nombre documento	Fecha de firma	Detalle de firma	Descargar	Eliminar
No se encontraron comprobantes en las fechas seleccionadas				

(1 of 1) << < > >> 10

APLICACIÓN TIMESTAMPING

Figura 44 Página de repositorio de documentos firmados

4.1.3.7 Página de solicitud de nueva contraseña

La Figura 45 muestra la página de solicitud de nueva contraseña, donde el usuario podrá solicitar una nueva contraseña, ingresando su nombre de usuario o dirección de correo electrónico.


The image shows a web form for requesting a new password. At the top center is a logo of a globe with the text 'APLICACIÓN TIMESTAMPING' below it. Below the logo is a text input field labeled 'Nombre de usuario'. Underneath that is a large 'ó' symbol, indicating an 'or' choice. Below the 'ó' is another text input field labeled 'Dirección de correo electrónico'. At the bottom of the form is a blue button with a white arrow icon and the text 'Solicitar nueva contraseña'. The entire form is centered on a light gray background with a subtle geometric pattern.

Figura 45 Página de repositorio de documentos firmados

4.1.3.8 Página para recordar nombre de usuario

La Figura 46 muestra la página para recuperar el nombre de usuario, para lo cual el usuario deberá ingresar su dirección de correo electrónico.

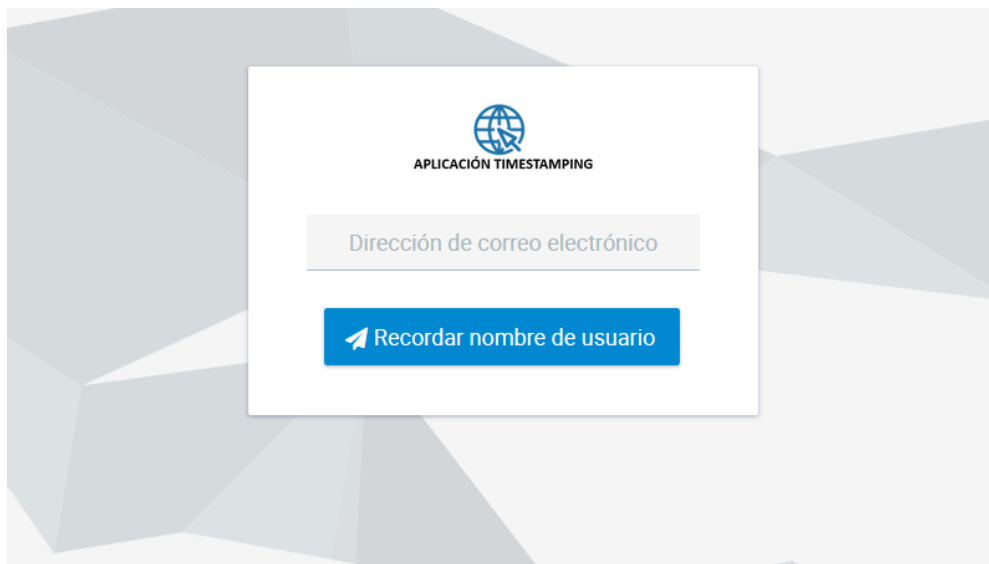
The image shows a web form for remembering a username. At the top center is a logo of a globe with the text 'APLICACIÓN TIMESTAMPING' below it. Below the logo is a text input field labeled 'Dirección de correo electrónico'. At the bottom of the form is a blue button with a white arrow icon and the text 'Recordar nombre de usuario'. The entire form is centered on a light gray background with a subtle geometric pattern.

Figura 46 Página para recordar nombre de usuario

4.1.4 Casos de Pruebas

A continuación se detallan las pruebas realizadas sobre la aplicación Web, las mismas que están basadas cada uno de los casos de uso planteados anteriormente.

4.1.4.1 Caso de Prueba Registro de usuario

La prueba realizada se muestra en la Tabla 18.

Tabla 18

Descripción caso de prueba “Registro de usuario”

Caso de prueba:	Registro de usuario (CP_001)	
Caso de uso asociado:	CU_001	
Funcionalidad a probar	Registro de un nuevo usuario de la aplicación	
Objetivo:	Probar la funcionalidad del caso de uso CU_001	
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de registro de un nuevo usuario en la aplicación de TimeStamping, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.	
Criterios de éxito:	Todos los datos ingresados fueron validados correctamente por la aplicación y almacenados en la base de datos.	
Criterios de falla:	Los datos no fueron validados correctamente y no se almacenaron en la aplicación.	
Pre-condiciones:	Ninguna	
Perfil del usuario:	Usuario general	
Autor:	Jesús Mendoza	
Fecha de creación:	17/02/2017	
Flujo del caso de prueba:	No paso	Usuario del sistema
	1	Ingresa número de cedula
	2	Ingresa nombre de usuario
	3	Ingresa contraseña
	4	Repite contraseña
	5	Ingresa nombre
	6	Ingresa apellidos
	7	Carga certificado de firma electrónica (opcional)
	8	Ingresa dirección de correo electrónico
	9	Clic botón “Registrarse”

Continúa 

Resultados obtenidos:	Usuario registrado exitosamente en la aplicación.
Post condiciones:	Es usuario queda habilitado para poder ingresar al sistema.

4.1.4.2 Caso de Prueba Autenticación de usuario

La prueba realizada se muestra en la Tabla 19.

Tabla 19

Descripción caso de prueba “Autenticación de usuario”

Caso de prueba:	Autenticación de usuario (CP_002)								
Caso de uso asociado:	CU_002								
Funcionalidad a probar	Acceso de usuarios a la aplicación								
Objetivo:	Probar la funcionalidad del caso de uso CU_002								
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de autenticación al sistema a un usuario previamente autenticado, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.								
Criterios de éxito:	Los datos de acceso fueron ingresados y validados correctamente contra la base de datos y permite al usuario ingresar a la aplicación, para hacer uso de la misma.								
Criterios de falla:	Los datos no fueron ingresados o validados correctamente contra la base de datos y no permite el acceso a la aplicación.								
Pre-condiciones:	El usuario debe estar previamente registrado.								
Perfil del usuario:	Usuario general, Usuario administrador								
Autor:	Jesús Mendoza								
Fecha de creación:	17/02/2017								
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Ingresa nombre de usuario</td> </tr> <tr> <td>2</td> <td>Ingresa contraseña</td> </tr> <tr> <td>3</td> <td>Clic botón “Ingresar”</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	Ingresa nombre de usuario	2	Ingresa contraseña	3	Clic botón “Ingresar”
No paso	Usuario del sistema								
1	Ingresa nombre de usuario								
2	Ingresa contraseña								
3	Clic botón “Ingresar”								
Resultados obtenidos:	Usuario accedió exitosamente a la aplicación.								
Post condiciones:	Es usuario puede hacer uso de cada una de las opciones habilitadas de acuerdo a su perfil (usuario general o usuario administrador).								

4.1.4.3 Caso de Prueba Autenticación de usuario

La prueba realizada se muestra en la Tabla 20.

Tabla 20

Descripción caso de prueba “Solicitar nueva contraseña”

Caso de prueba:	Solicitar nueva contraseña (CP_003)						
Caso de uso asociado:	CU_003						
Funcionalidad a probar	Solicitar nueva contraseña						
Objetivo:	Permitir al usuario solicitar una nueva contraseña de acceso a la aplicación, cuando no recuerda la misma.						
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de solicitud de nueva contraseña para acceder a la aplicación, tomando en cuenta los pasos del escenario principal y alternativo descritos en el caso de uso asociado.						
Criterios de éxito:	El dato proporcionado por el usuario (nombre de usuario o correo electrónico) es correcto y la aplicación envía un correo electrónico al usuario indicando el proceso a realizar para generar la nueva contraseña.						
Criterios de falla:	El dato proporcionado por el usuario (nombre de usuario o correo electrónico) es incorrecto y el sistema no envía el correo electrónico.						
Pre-condiciones:	El usuario debe estar previamente registrado.						
Perfil del usuario:	Usuario general, Usuario administrador						
Autor:	Jesús Mendoza						
Fecha de creación:	17/02/2017						
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Ingresa nombre de usuario o dirección de correo electrónico</td> </tr> <tr> <td>2</td> <td>Clic botón “Solicitar nueva contraseña”</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	Ingresa nombre de usuario o dirección de correo electrónico	2	Clic botón “Solicitar nueva contraseña”
No paso	Usuario del sistema						
1	Ingresa nombre de usuario o dirección de correo electrónico						
2	Clic botón “Solicitar nueva contraseña”						
Resultados obtenidos:	Proceso completado correctamente.						
Post condiciones:	Es usuario podrá acceder a aplicación con la nueva contraseña generada.						

4.1.4.4 Caso de Prueba Recordar nombre de usuario

La prueba realizada se muestra en la Tabla 21.

Tabla 21

Descripción caso de prueba “Recordar nombre de usuario”

Caso de prueba:	Recordar nombre de usuario (CP_004)						
Caso de uso asociado:	CU_004						
Funcionalidad a probar	Recordar nombre de usuario						
Objetivo:	Permitir al usuario recordar su nombre de usuario para acceder a la aplicación.						
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de recordar nombre de usuario para acceder a la aplicación, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.						
Criterios de éxito:	La dirección correo electrónico asociado al usuario es correcta y la aplicación envía un correo electrónico al usuario con el nombre de usuario de la aplicación.						
Criterios de falla:	La dirección de correo electrónico asociado al usuario es incorrecta y el sistema no envía el correo con el nombre de usuario.						
Pre-condiciones:	El usuario debe estar previamente registrado.						
Perfil del usuario:	Usuario general, Usuario administrador						
Autor:	Jesús Mendoza						
Fecha de creación:	17/02/2017						
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Ingresa nombre de usuario su dirección de correo electrónico</td> </tr> <tr> <td>2</td> <td>Clic botón “Recordar nombre de usuario”</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	Ingresa nombre de usuario su dirección de correo electrónico	2	Clic botón “Recordar nombre de usuario”
No paso	Usuario del sistema						
1	Ingresa nombre de usuario su dirección de correo electrónico						
2	Clic botón “Recordar nombre de usuario”						
Resultados obtenidos:	Proceso completado correctamente.						
Post condiciones:	Es usuario podrá acceder a aplicación con el nombre de usuario recuperado y su contraseña.						

4.1.4.5 Caso de Prueba Actualizar información de usuario

La prueba realizada se muestra en la Tabla 22.

Tabla 22**Descripción caso de prueba “Actualizar información de usuario”**

Caso de prueba:	Actualizar información de usuario (CP_005)
Caso de uso asociado:	CU_005

Continúa 

Funcionalidad a probar	Actualizar la información de un usuario de la aplicación						
Objetivo:	Permitir al usuario actualizar su información.						
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de actualización de información del usuario, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.						
Criterios de éxito:	Todos los datos modificados por el usuario fueron validados correctamente por la aplicación y actualizados la base de datos.						
Criterios de falla:	Los datos modificados no fueron actualizados correctamente en la base de datos.						
Pre-condiciones:	El usuario debe estar previamente registrado.						
Perfil del usuario:	Usuario general, Usuario administrador						
Autor:	Jesús Mendoza						
Fecha de creación:	17/02/2017						
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>El usuario modifica los datos que desea actualizar, a excepción del número de cédula.</td> </tr> <tr> <td>2</td> <td>Clic botón "Actualizar información"</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	El usuario modifica los datos que desea actualizar, a excepción del número de cédula.	2	Clic botón "Actualizar información"
No paso	Usuario del sistema						
1	El usuario modifica los datos que desea actualizar, a excepción del número de cédula.						
2	Clic botón "Actualizar información"						
Resultados obtenidos:	Los datos fueron actualizados correctamente.						
Post condiciones:	Ninguna						

4.1.4.6 Caso de Prueba Firmar y sellar documentos XML

La prueba realizada se muestra en la Tabla 23.

Tabla 23

Descripción caso de prueba "Firmar y sellar documentos XML"

Caso de prueba:	Firmar y sellar documentos XML (CP_006)
Caso de uso asociado:	CU_006
Funcionalidad a probar	Firma electrónica y sellado de tiempo de documentos XML
Objetivo:	Permitir al usuario realizar el proceso de firma y sellado de tiempo de un documento XML.
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de firma y sellado de tiempo de

Continúa 

	documentos XML, tomando en cuenta los pasos del escenario principal y alternativo descritos en el caso de uso asociado.										
Criterios de éxito:	El documento XML cargado fue firmado y sellado correctamente, y posteriormente almacenado en la base de datos.										
Criterios de falla:	El proceso de firma y sellado de tiempo no pudo ser completado exitosamente.										
Pre-condiciones:	El usuario debe estar previamente registrado.										
Perfil del usuario:	Usuario general										
Autor:	Jesús Mendoza										
Fecha de creación:	17/02/2017										
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>El usuario carga el archivo XML que desea firmar y sellar.</td> </tr> <tr> <td>2</td> <td>El usuario carga su certificado de firma (solamente si no lo cargo al momento de registrarse en la aplicación).</td> </tr> <tr> <td>3</td> <td>El usuario ingresa el PIN del certificado de firma.</td> </tr> <tr> <td>4</td> <td>Clic botón "Aplicar firma y sello de tiempo"</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	El usuario carga el archivo XML que desea firmar y sellar.	2	El usuario carga su certificado de firma (solamente si no lo cargo al momento de registrarse en la aplicación).	3	El usuario ingresa el PIN del certificado de firma.	4	Clic botón "Aplicar firma y sello de tiempo"
No paso	Usuario del sistema										
1	El usuario carga el archivo XML que desea firmar y sellar.										
2	El usuario carga su certificado de firma (solamente si no lo cargo al momento de registrarse en la aplicación).										
3	El usuario ingresa el PIN del certificado de firma.										
4	Clic botón "Aplicar firma y sello de tiempo"										
Resultados obtenidos:	Documento firmado, sellado y almacenado correctamente.										
Post condiciones:	El usuario podrá consultar, descargar o eliminar el documento firmado y ver los detalles de la firma y sello de tiempo del mismo, en la opción "Repositorio de documentos".										


4.1.4.7 Caso de Prueba Repositorio de documentos

La prueba realizada se muestra en la Tabla 24.

Tabla 24

Descripción caso de prueba "Repositorio de documentos"

Caso de prueba:	Repositorio de documentos (CP_007)
Caso de uso asociado:	CU_007
Funcionalidad a probar	Repositorio de documentos firmados y sellados.

Continúa 

Objetivo:	Permitir al usuario consultar los documentos previamente firmados y sellados.										
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad del repositorio de documentos firmados y sellados previamente por el usuario, permitiendo al usuario, consultar, descargar o eliminar sus documentos, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.										
Criterios de éxito:	El usuario pudo consultar sus documentos y gestionar los mismos de manera correcta.										
Criterios de falla:	El usuario no pudo consultar sus documentos.										
Pre-condiciones:	El usuario debe estar previamente registrado, y contar con al menos un documento almacenado en la base de datos de la aplicación.										
Perfil del usuario:	Usuario general										
Autor:	Jesús Mendoza										
Fecha de creación:	17/02/2017										
Flujo del caso de prueba:	<table border="1"> <thead> <tr> <th>No paso</th> <th>Usuario del sistema</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>El usuario ingresa la fecha inicial con la cual desea consultar los documentos.</td> </tr> <tr> <td>2</td> <td>El usuario ingresa la fecha final con la cual desea consultar los documentos.</td> </tr> <tr> <td>3</td> <td>Clic botón "Consultar"</td> </tr> <tr> <td>4</td> <td>Selecciona las opciones disponibles (Descargar o eliminar)</td> </tr> </tbody> </table>	No paso	Usuario del sistema	1	El usuario ingresa la fecha inicial con la cual desea consultar los documentos.	2	El usuario ingresa la fecha final con la cual desea consultar los documentos.	3	Clic botón "Consultar"	4	Selecciona las opciones disponibles (Descargar o eliminar)
No paso	Usuario del sistema										
1	El usuario ingresa la fecha inicial con la cual desea consultar los documentos.										
2	El usuario ingresa la fecha final con la cual desea consultar los documentos.										
3	Clic botón "Consultar"										
4	Selecciona las opciones disponibles (Descargar o eliminar)										
Resultados obtenidos:	Documentos firmados y sellados en el rango de fechas seleccionadas.										
Post condiciones:	Ninguna										

4.1.4.8 Caso de Prueba Actualizar parámetros de la aplicación

La prueba realizada se muestra en la Tabla 25.

Tabla 25

Descripción caso de prueba "Actualizar parámetros de la aplicación"

Caso de prueba:	Actualizar parámetros de la aplicación (CP_008)
Caso de uso asociado:	CU_008

Continúa 

Funcionalidad a probar	Actualización de parámetros de la aplicación.	
Objetivo:	Permitir al usuario administrador actualizar los parámetros de la aplicación.	
Descripción:	El propósito del presente caso de prueba es probar la funcionalidad de la actualización de parámetros de la aplicación, tomando en cuenta los pasos del escenario principal y alterno descritos en el caso de uso asociado.	
Criterios de éxito:	El usuario modifico los parámetros deseados y el sistema actualizó la información en la base de datos correctamente.	
Criterios de falla:	El sistema no logro actualizar los parámetros modificados por el usuario en la base de datos.	
Pre-condiciones:	El usuario debe estar previamente registrado, y tener el perfil de administrador de sistema.	
Perfil del usuario:	Usuario administrador	
Autor:	Jesús Mendoza	
Fecha de creación:	17/02/2017	
Flujo del caso de prueba:	No paso	Usuario del sistema
	1	El usuario modifica los parámetros que desea actualizar.
	2	Clic botón "Probar parámetros"
	3	Clic botón "Actualizar parámetros"
Resultados obtenidos:	Parámetros probados correctamente. Parámetros actualizados correctamente.	
Post condiciones:	Ninguna	

4.1.5 Pruebas adicionales

Si bien la metodología UWE, sugiere la realización de pruebas como parte del proceso de desarrollo de software, esta no especifica el tipo de pruebas que deben realizarse, por este motivo se optó por realizar pruebas adicionales tomando como referencia el proceso de pruebas de aplicaciones Web, sugerido por Roger Pressman en (Presman, 2010) (ver figura 47). Este proceso de pruebas está diseñado en forma piramidal, en el cual el flujo de las pruebas avanza de izquierda a derecha y de arriba abajo, donde los elementos visibles para el usuario del diseño de la aplicación Web, se prueban primero, seguidos por los elementos de diseño de infraestructura.

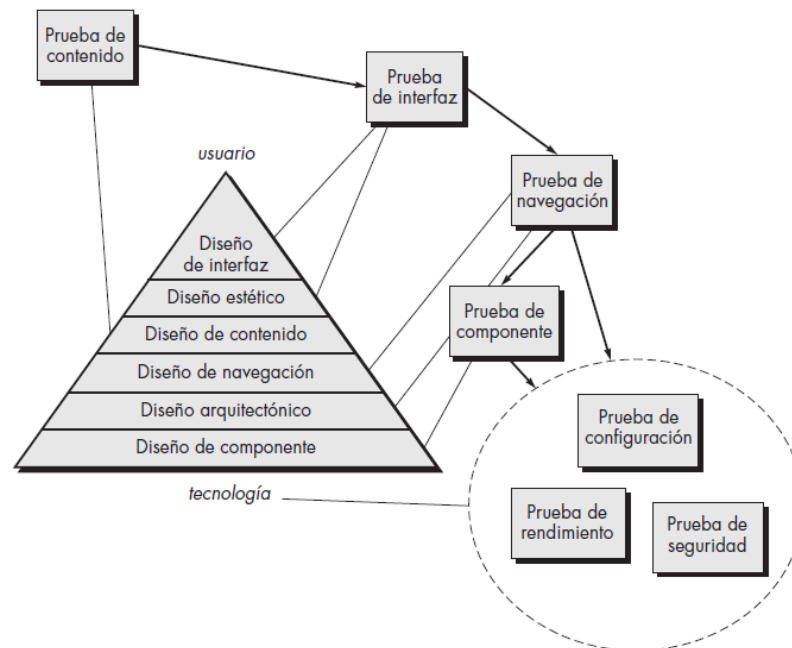


Figura 47 Proceso de pruebas de aplicaciones Web
Fuente: (Presman, 2010)

4.1.5.1 Prueba de contenido

La prueba realizada se muestra en la Tabla 26, donde se indica los errores encontrados con su respectiva solución.

Tabla 26
Prueba de contenido

Tipo de error	Detalle	Solución
Sintáctico	Texto del botón “¿Olvido su contraseña?”, sin tilde en la palabra “Olvido”.	Colocar la tilde en la palabra “Olvido”
	Campo “Nombres”, en la sección de registro sin “:” en la etiqueta.	Colocar los dos putos al final de la etiqueta, de la siguiente manera: “Nombres:”
	Mensaje de error campo “Certificado es obligatorio”, no coincide con ninguna de las etiquetas de información, en la sección “Firmar y sellar documentos”.	Completar el mensaje de error para que coincida con la etiqueta “Certificado de firma:”
Semántico	Ícono del botón “Registrar nuevo usuario” no concuerda con la acción del botón.	Cambiar el ícono del botón por uno más acorde al texto y acción del botón, se eligió un ícono que representa un teclado.

Continúa

Organización o estructura	Al momento de consultar los documentos firmados, el ingreso de las fechas de consulta, no especifica el formato de ingreso de las fechas.	Colocar una sugerencia de formato de fecha en el componente de ingreso de fechas, y usar un componente de selección gráfico para seleccionar las fechas en lugar de digitarlas.
----------------------------------	---	---

4.1.5.2 Prueba de interfaz

La prueba realizada se muestra en la Tabla 27, donde se indica los errores encontrados con su respectiva solución.

Tabla 27
Prueba de interfaz

Tipo de error	Detalle	Solución
Vínculos	No existen.	
Formularios	Al cargar el contenido de los documentos firmados en el componente “Datatable”, no existe un paginador, los que sobre carga la interfaz del usuario y dificulta la búsqueda de los comprobantes.	Usar la opción paginador del componente “Datatable”, permitiendo elegir al usuario los números de elementos que desea mostrar por página.
HTML dinámico	El contenido desplegado en el componente “Datatable” no permite distinguir cuando termina y empieza un nuevo registro.	Aplicar un estilo CSS para sombrear las filas impares del “Datatable”, y mantener el color por defecto de las filas pares.
Cookies	No existen.	
Ventanas pop-up	No existen.	

4.1.5.3 Prueba de navegación

La prueba realizada se muestra en la Tabla 28, donde se indica los errores encontrados con su respectiva solución.

Tabla 28
Prueba de Navegación

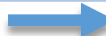
Sección	Detalle	Solución
Solicitud de nueva contraseña	Al seleccionar la opción “Solicitar nueva contraseña”, el botón “Volver”, no direcciona adecuadamente, y muestra mensaje de error “Pagina no existe”.	Escribir correctamente el nombre de la página a re direccionar, cambiando “login.html”, por “login.xhtml”.
Registrar nuevo usuario	Al seleccionar la opción “Registrar nuevo usuario”, en la página de registro no existe un botón para cancelar o regresar a la página anterior.	Colocar un botón “Volver”, para poder regresar a la página principal “login.xhtml”.
Actualizar información de usuario	No se muestra el nombre de la sección u opción seleccionada, lo que no permite al usuario saber en qué lugar del sistema se encuentra.	Ubicar el nombre de la sección del sistema que está haciendo uso del usuario, de manera similar a las otras secciones.

4.1.5.4 Prueba de componentes

La prueba realizada se muestra en la Tabla 29, donde se detallan las pruebas realizadas, y los resultados obtenidos.

Tabla 29
Prueba de componentes

Tipo de prueba	Detalle
Configuración	<ul style="list-style-type: none"> Se verifico que la configuración del sistema permita ser usado desde diferentes navegadores Web (Internet Explorer 10+, Firefox 35+, Google Chrome 35+, Opera 45+ y Safari 5+), sin importar el Sistema Operativo o dispositivo de acceso.
Rendimiento	<ul style="list-style-type: none"> Se realizó esta prueba en diferentes tipos de dispositivos con diferentes tipos de conexión a internet (Wifi, cableado y 4G con paquetes de datos). Se concluyó que el sistema puede ser usado con velocidades de internet desde 256Kb/s o superiores, sin embargo se recomienda contar una velocidad de conexión de al menos 512Kb/s para garantizar un tiempo de respuesta óptimo del sistema.

Continúa 

Seguridad

- Se validó que el sistema sea usado únicamente por usuarios previamente registrados en el sistema, y que cuenten con un certificado de firma electrónica válido.
- Se verificó que el sistema no permita acceder copiando las Url's de las páginas internas de la aplicación, sin antes haber iniciado sesión en el sistema.

4.2 ADAPTACIÓN DE LA FUNCIONALIDAD DE FIRMA Y SELLADO DE TIEMPO EN EL SISTEMA DE FACTORING ELECTRÓNICO DESARROLLADO POR LA EMPRESA BIGDATA C.A

Para la adaptación del proceso de firma y sellado de tiempo en el sistema de Factoring electrónico, se procedió a solicitar a la empresa BIGDATA C.A el acceso al código fuente del mismo, para poder analizar y determinar las clases y métodos en los cuales se debían realizar las modificaciones.

4.2.1 Selección del paquete del sistema de Factoring Electrónico donde se adaptó el proceso de firma y sellado de tiempo de la aplicación de Time Stamping

A continuación se muestra la distribución de paquetes del sistema de Factoring electrónico y el paquete en el cual se procedió a adaptar el proceso de firma y sellado de tiempo de la aplicación de Time Stamping desarrollada (ver Figura 48):

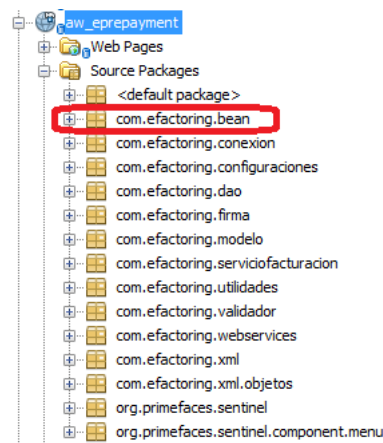


Figura 48 Distribución de paquetes del sistema de Factoring Electrónico

En el paquete “com.efactoring.bean” se encuentran las clases que manejan las páginas del sistema de Factoring Electrónico, en las cuales se generan las peticiones realizadas por el usuario. Para la adaptación del proceso de firma y sellado de tiempo se trabajó con las siguientes clases contenidas en este paquete:

- FacturasConfirmarDeudorBean.java
- ConfirmarVentaFacturasVendedorBean.java

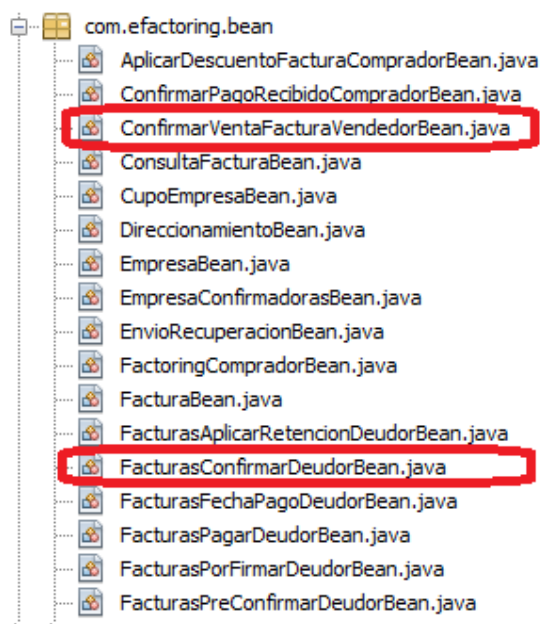


Figura 49 Clases en las cuales se adoptó el proceso de firma y sellado de tiempo para el sistema de Factoring Electrónico

4.2.2 Clase FacturasConfirmarDeudorBean.java

Esta clase contiene los métodos relacionados al actor del sistema de Factoring Electrónico con el rol “Confirmador”, se procedió a identificar en cuál de estos métodos se da la generación del documento XML de confirmación de pago especificado en la Tabla 2 del Capítulo III, una vez identificado dicho método se procedió a adaptar la funcionalidad de firma y sello de tiempo en el mismo.

A continuación se muestra la interfaz en la cual se implementó el proceso de firma y sello de tiempo en el sistema de Factoring Electrónico para el usuario con el rol “Confirmador” (ver Figuras 50 y 51).

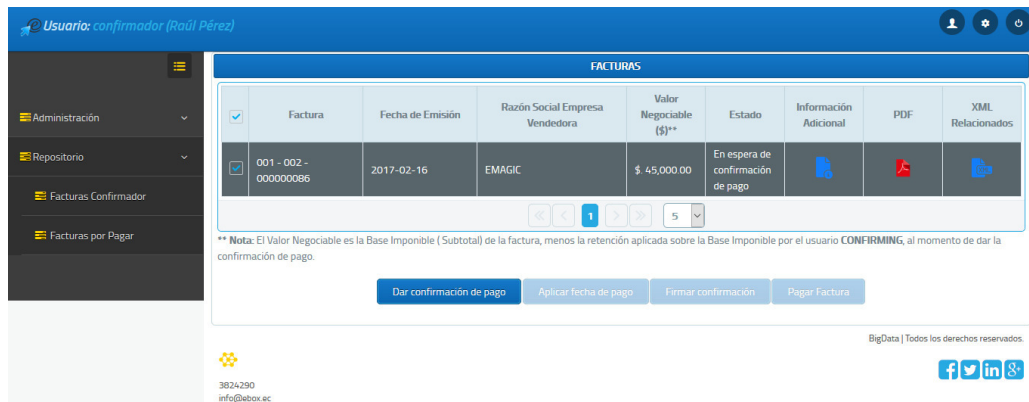


Figura 50 Interfaz de facturas pendientes de confirmación de pago en el sistema de Factoring Electrónico



Figura 51 Interfaz de firma y sellado de tiempo de la confirmación de pago de una factura en el sistema de Factoring Electrónico

4.2.3 Clase ConfirmarVentaFacturaVendedorBean.java

Esta clase contiene los métodos relacionados al actor del sistema de Factoring Electrónico con el rol “Vendedor”, de igual manera se procedió a identificar en cuál de los métodos se da la generación del documento XML de cesión de una factura especificado en la Tabla 3 del Capítulo III, una vez

identificado dicho método se procedió a adaptar la funcionalidad de firma y sello de tiempo en el mismo.

A continuación se muestra la interfaz en la cual se implementó el proceso de firma y sello de tiempo en el sistema de Factoring Electrónico para el usuario con el rol "Vendedor" (ver Figuras 52 y 53).

Factura	Fecha de Emisión	Razón Social Cliente	Valor Total (\$)	Valor Negociable / Subtotal (\$)**	Estado	PDF	XML Relacionados
001 - 002 - 000000082	2016-12-16	BigData C.A.	\$ 28,500.00	\$ 24,500.00	Proceso ePrepayment culminado		
001 - 002 - 000000081	2016-12-16	BigData C.A.	\$ 34,200.00	\$ 29,400.00	En espera de pago		
001 - 002 - 000000080	2016-12-09	BigData C.A.	\$ 68,400.00	\$ 59,400.00	En espera de pago		
001 - 002 - 000000079	2016-12-09	BigData C.A.	\$ 34,200.00	\$ 29,400.00	En espera de confirmación de venta		
001 - 002 - 000000078	2016-12-09	BigData C.A.	\$ 969.00	\$ 850.00	Subida		

** Nota: Si al momento de la confirmación de pago de la factura el usuario CONFIRMING aplica una Retención a la Base Imponible (Subtotal) de la factura, es posible que el valor negociable se vea reducido en base al porcentaje de la Retención aplicada, siendo el valor resultante el nuevo Valor Negociable.

Figura 52 Interfaz de facturas pendientes de confirmación de venta en el sistema de Factoring Electrónico

Factura	Valor Negociable / Subtotal (\$)**	Estado
001 - 002 - 000000082	\$ 24,500.00	Proceso ePrepayment culminado
001 - 002 - 000000081	\$ 29,400.00	En espera de pago
001 - 002 - 000000080	\$ 59,400.00	En espera de pago
001 - 002 - 000000079	\$ 29,400.00	En espera de confirmación de venta
001 - 002 - 000000078	\$ 850.00	Subida

Confirmar Venta

Porcentaje proceso ePrepayment: 3.00%

Valor total de la factura: \$ 34,200.00

Valor Negociable: \$ 29,400.00

Valor descontado por compra: \$ 9,261.00

Valor uso plataforma: \$ 0.00

Valor a recibir: \$ 20,139.00

Días restantes para el pago: 315 días

Contraseña para firma electrónica: (?)*

¿Está seguro de confirmar la venta de la factura?

** Nota: Si al momento de la confirmación de pago de la factura el usuario CONFIRMING aplica una Retención a la Base Imponible (Subtotal) de la factura, es posible que el valor negociable se vea reducido en base al porcentaje de la Retención aplicada, siendo el valor resultante el nuevo Valor Negociable.

Figura 53 Interfaz de firma y sellado de tiempo de la confirmación de venta de una factura en el sistema de Factoring Electrónico

CAPÍTULO V

RESULTADOS OBTENIDOS, CONCLUSIONES Y RECOMENDACIONES

5.1 RESULTADOS OBTENIDOS

La incorporación de firmas electrónicas y sellos de tiempo para la firma de documentos XML, permitió brindar mayor integridad a la información contenida en estos, ya sea para ser usados en proceso judiciales o para evitar la alteración de los mismos, puesto que se tiene la seguridad que la persona firmante es quien dice ser, gracias al certificado de firma electrónica. Por otra parte cualquier alteración, por mínima que sea invalidará el documento y la firma asociada a este, además al contar con el sello de tiempo incorporado a la firma se puede tener absoluta confianza de la fecha de creación de esta última, considerando que dicha fecha ha sido obtenida de una fuente confiable, como lo es la TSA. En la siguiente tabla se muestra una comparación entre el archivo XML sin firma, con firma y con firma en conjunto con sello de tiempo:

Tabla 30
Comparación documentos XML sin firma, con firma y con firma en conjunto son sellos de tiempo

	XML sin firma	XML con firma	XML con firma + sello de tiempo
Integridad de la información	NO	SI	SI
Confianza de la persona firmante	NO	SI	SI
Fecha y hora de firma confiable	NO	NO	SI

Adicionalmente se pudo determinar que el uso firmas electrónicas y sellos de tiempo no se limita únicamente para firmar archivos o documentos en formato XML, también pueden ser usado para firmar otros tipos de archivos como: CMS, OOXML, ODF y PDF, siendo este último uno de los más amigables con el usuario final, en vista que el contenido y la firma asociada se pueden mostrar de manera más simple y directa en cualquier dispositivo que disponga de una aplicación para leer este tipo de archivos. El formato

PDF es recomendado cuando el documento está dirigido a un usuario final, mas no para ser reprocesado por otras aplicaciones, con el objetivo de extraer información específica de los mismos, como suele suceder con los documentos en formato XML, el cual hace uso de etiquetas que facilitan la lectura de la información mediante programación.

Como resultado final de haber implementado el proceso de firma electrónica y sello de tiempo realizado en la aplicación Web de Time Stamping, en el sistema de Factoring Electrónico desarrollado por la empresa BIGDATA C.A, se logró brindar mayor confianza, seguridad y agilidad al proceso de Factoring. La firma electrónica en conjunto con el sello de tiempo permitió que las confirmaciones y cesiones de las facturas negociadas de ahora en adelante sean realizadas totalmente en línea, y ya no de manera manual como se venía realizando cuando una o más de las partes involucradas así lo deseaba, ya que una firma electrónica tiene igual validez que una firma física y con el uso de sellos de tiempo se vuelve incluso más segura que esta última.

5.2 CONCLUSIONES

- En el presente proyecto se cumplieron los objetivos planteados al inicio, se desarrolló una aplicación Web de Time Stamping, usando un formato de firma apropiado que se ajuste al proceso del sistema de Factoring Electrónico y adaptando el proceso de firma y sello de tiempo en el mismo.
- La apertura de la empresa BIGDATA C.A al permitir el acceso al código fuente de su sistema de Factoring Electrónico, facilitó sin duda la integración del proceso de firma y sellado de tiempo desarrollado en la aplicación Web de Time Stamping.
- El uso de las librerías PolygonESL-2.0 proporcionadas por la TSA del Banco Central del Ecuador para el consumo del servicio de sellado de tiempo, permitió reducir considerablemente el tiempo de desarrollo de la aplicación.
- El uso de firmas electrónicas en conjunto con sellos de tiempo permiten mantener intacta la información contenida en los documentos a largo del

tiempo, dando mayor solides y confianza a los mismos, incluso ante procesos judiciales donde se requiera demostrar la integridad de estos.

- Los modelos sugeridos por la metodología UWE permitieron desarrollar la aplicación de manera ágil, centrándose en la parte funcional de la misma, puesto que sus ilustraciones son fáciles de comprender, lo que facilita la comunicación entre el desarrollador y el cliente, permitiendo plasmar de mejor manera los requerimientos previos al desarrollo de la aplicación.
- El no contar con una conexión a Internet estable en el equipo donde se hará uso de la aplicación Web de Time Stamping, puede provocar que esta no funcione adecuadamente al momento de consumir el servicio de sellos de tiempo.

5.3 RECOMENDACIONES

- Se recomienda que el equipo desde el cual se hará uso de la aplicación Web de Time Stamping, cuente con una conexión a Internet, la misma que es necesaria para poder realizar el consumo de sellos de tiempo.
- Sugerir formalmente a las autoridades de la empresa, hacer uso de firmas electrónicas y/o sellos de tiempo en otros procesos, como en la firma de contratos con sus clientes, contratación de personal o cualquier otro documento donde se puedan reemplazar la firma manuscrita por una electrónica, para brindar mayor seguridad y agilidad a sus procesos.
- Sugerir formalmente a empresas de sector público o privado hacer uso de firmas y/o sellos de tiempo en sus procesos, en especial en aquellos que pueden ser realizados en línea y requieran la carga de información firmada por sus clientes, para agilizar así los tramites, evitar la presencia física de las personas y reducir el uso de papel y otros suministros usados en este tipo de trámites.
- Se recomienda tener pendiente la fecha de caducidad de los certificados de firma electrónica y del servicio de sello de tiempo, para poder renovarlos con antelación y así evitar contratiempos, considerando que estos dos elementos son indispensables para el funcionamiento de la aplicación.
- Se recomienda generar una cultura de manejo de la información relacionada al uso del certificado de firma electrónica y el PIN de activación

del mismo, para evitar que personas no autorizadas tengan acceso a estos.

BIBLIOGRAFÍA Y WEBGRAFÍA

BIBLIOGRAFÍA

- Buldas, A., Laud, P., Lipmaa, H., & Villemson, J. (1998). Time-stamping with binary linking schemes. *Annual International Cryptology Conference*, 486-501.
- Bustos, G. (2 de 2002). Integración Informal De Modelos En Uml. *Ingenereare*, 14.
- Callejas Cuervo, M., Peñalosa Parra, D. I., & Alarcón Aldana, A. C. (10 de 02 de 2011). Evaluación y análisis de rendimiento de los frameworks de persistencia Hibernate y Eclipselink. *Ventana Informática - 24*, 9-23.
- Debasish, K., Debasis, S., & Rajib, M. (2013). Automatic code generation from unified modelling language sequence diagrams. *IET Software 7.1*, 12-28.
- Días, J., Macia, N., Molinari, L., Venosa, P., & Sabolansky, A. (05 de 05 de 2010). Importancia de contar con un servicio de sellado digital de tiempo en una PKI. *XII Workshop de Investigadores en Ciencias de la Computación*, 27-31. Obtenido de RedUnci.
- Diaz, J. F., Queiruga, C. A., & Iuliano, P. J. (21 de 09 de 2009). Incorporando seguridad a las componentes de interfaz de usuario del framework JSF (JAVA Server Faces). *XV Congreso Argentino de Ciencias de la Computación*, 1132-1141.
- Egas Clavijo, P. G. (21 de 06 de 2015). PRIMEFACES CRUD GENERADOR PARA NETBEANS. Quito, Pichincha, Ecuador.
- Escalona, M. J., & Koch, N. (01 de 12 de 2002). Ingeniería de Requisitos en Aplicaciones para la Web—Un estudio comparativo.
- Gerić, S., & Vidačić, T. (2012). XML digital signature and its role in information system security. *MIPRO, 2012 Proceedings of the 35th International Convention*, 1520-1525.
- Hrvoje, B., Boris, H., & Hrvoje, S. (2013). Long-term Preservation of Validity of Electronically Signed Records. *INFuture2013: Information Governance.*, 147-158.
- Ivanovic, S., Baresa, S., & Sinisa, B. (2011). Factoring: Alternative model of financing. *UTMS Journal of Economics 2.2*, 189-206.
- Koch, N., & Kraus, A. (24 de 01 de 2002). The expressive power of uml-based web engineering. *Second International Workshop on Web-oriented Software Technology (IWWOST02) (Vol. 16)*.
- Maykin, W., & Pramote, K. (2012). Paper-based document authentication using digital signature and QR code. *2012 4TH International Conference on Computer Engineering and Technology*, 94-98.
- Milinković, S., Milojković, B., Spasić, D., & Lazić, L. (2012). Evaluation of some time-stamping authority software. *6th International Conference on Methodologies, Technologies and Tools enabling e-Government*, 1-10.
- Muñoz Guerrero, D. P. (17 de 01 de 2013). Tributación en comercio electrónico en el Ecuador. Quito.
- Paulin, G. A., Robledo, M. Á., & Brusa, G. M. (2014). Diseño e implementación de Time-Stamping bajo un servidor confiable de fecha y hora. *XLIII Jornadas*

- Argentinas de Informática e Investigación Operativa (43JAIIO)-XVII Concurso de Trabajos Estudiantiles (EST)*, 4-9.
- Rivero, J. M., Grigera, J., Rossi, G., Robles Luna, E., & Koch, N. (2011). Improving Agility in Model-Driven Web Engineering. *CAiSE Forum Vol. 734*.
- Satizábal, C., Páez, R., & Forné, J. (25 de 11 de 2005). ELEGACIÓN PRIVILEGIADA: VALIDACION vs. REVOCACION. *Revista Colombiana de Tecnologías Avanzadas*, 8-14.
- Shpresa, Ç., & Anila, B. (2015). Economic Factoring Role and its Advantages Compared with Debt Collectors and Bank Credit to SMEs in Albania. *International Journal of Management and Business Economics* 4.4, 40-49.
- Singh, S., Sunil K, M., & Sudesh, K. (2013). A Performance Analysis of DES and RSA Cryptography. *International Journal of Emerging Trends & Technology in Computer Science*, 418-423.
- Tinoco Gomez, O., Rosales Lopez, P. P., & Salas Bacalla, J. (2010). Criterios de selección de metodologías de desarrollo de software. *Portal Revistas Peruanas*, 70-74.
- Vigil, M. A., Cabarcas, D., Wiesmaier, A., & Duchmann, J. (2012). Authenticity, Integrity and Proof of Existence for Long-Term Archiving: a Survey. *IACR Cryptology ePrint Archive*, 499.
- Vinod Moreshwar , V. (2012). Digital Signature on-line, One Time Private Key [OTPK]. *International Journal of Scientific & Engineering Research*, 3 (3), 1.
- Presman, R. S. (2010). *Ingeniería de software Un enfoque práctico*. México: MCGRAW-HILL INTERAMERICANA EDITORES, S.A. DE C.V.

WEBGRAFÍA

- Agencia de Tecnologia y Certificacion Electrónica. (20 de 12 de 2016). *Electrónica*. Obtenido de http://www.accv.es/descargas/Setup/arangi/latest/arangi/firma_xades.html
- Apache Tomcat. (23 de 01 de 2017). *Apache Tomcat*. Obtenido de <http://tomcat.apache.org/>
- Camara de comercio de Ambato. (03 de 09 de 2016). *Camara de Comercio de Ambato*. Obtenido de <http://www.cca.org.ec/informativo/blog/160-%C2%BFque-es-el-factoring>
- Cryptomathic. (19 de 02 de 2016). *Cryptomathic*. Obtenido de <https://www.cryptomathic.com/news-events/blog/introduction-into-xades-for-trust-service-providers>
- ECIBCE. (16 de Septiembre de 2016). *Certificación Electrónica Banco Central del Ecuador*. Obtenido de <https://www.eci.bce.ec/preguntas-frecuentes#21>
- ECIBCE. (21 de 10 de 2016). *Entidad de Certificación de Información y Servicios Relacionados*. Obtenido de <https://www.eci.bce.ec/solicitud-de-sellado-de-tiempo-requisitos>
- ECIBCE. (01 de 12 de 2016). *ENTIDAD DE CERTIFICACIÓN DE INFORMACIÓN Y SERVICIOS RELACIONADOS*. Obtenido de <https://www.eci.bce.ec/ocsp>
- ETSI. (24 de 12 de 2016). *European Telecommunications Standards Institute*. Obtenido de

- http://www.etsi.org/deliver/etsi_ts/101900_101999/101903/01.04.02_60/ts_101903v010402p.pdf
- Ferré Grau, X., & Sánchez Segura, M. I. (17 de 01 de 2002). *Universidad Interamericana para el Desarrollo*. Obtenido de http://moodle2.unid.edu.mx/dts_cursos_mdl/lic/IEL/SI/AM/11/UML.pdf
- Galperin, S., Santesson, S., Myers, M., Malpani, A., & Adams, C. (01 de 06 de 2013). *Internet Engineering Task Force (IETF)*. Obtenido de <https://tools.ietf.org/html/rfc6960#section-4.1>
- Granda, M., Campaña, M., & Días, P. (24 de 01 de 2017). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE*. Obtenido de <http://repositorio.espe.edu.ec/bitstream/21000/8432/1/AC-SI-ESPE-048020.pdf>
- ISTR. (04 de 02 de 2017). *ISTR Universidad de Cantabria*. Obtenido de http://www.ctr.unican.es/asignaturas/is1/IEEE830_esp.pdf
- Java. (23 de 01 de 2017). *Java*. Obtenido de https://www.java.com/es/download/faq/whatis_java.xml
- MariaDB Foundation. (20 de 01 de 2017). <https://mariadb.org>. Obtenido de <https://mariadb.org/about/>
- NetBeans. (23 de 01 de 2017). *NetBeans*. Obtenido de https://netbeans.org/index_es.html
- Oracle. (23 de 01 de 2017). *Oracle*. Obtenido de <http://www.oracle.com/technetwork/es/java/javace/overview/index.html>
- PAE. (26 de 11 de 2016). *Portal de administración electrónica*. Obtenido de <http://firmaelectronica.gob.es/Home/Empresas/Firma-Electronica.html>
- PAE. (28 de 11 de 2016). *Portal de Administración Electrónica*. Obtenido de <http://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html>
- Registro Civil. (20 de 11 de 2016). *Registro Civil*. Obtenido de <https://www.registrocivil.gob.ec/?p=4172>
- Security Data. (29 de 11 de 2016). *Security Data*. Obtenido de <https://www.securitydata.net.ec/sellado-tiempo/>
- SRI. (28 de 10 de 2016). *Servicio de Rentas Internas*. Obtenido de SRI: <http://www.sri.gob.ec/web/guest/comprobantes-electronicos1>
- SRI. (29 de 11 de 2016). *Servicio de Rentas Internas*. Obtenido de <http://www.sri.gob.ec/DocumentosAlfrescoPortlet/descargar/df8c03b3-3777-45a0-8349-257a759945e1/LeyComercioElectronico.doc>
- SRI. (16 de 12 de 2016). *Servicio de Rentas Internas*. Obtenido de <http://www.sri.gob.ec/web/guest/base-legal-comprobantes-electronicos>
- W3C España. (30 de 09 de 2016). *W3C España*. Obtenido de <http://www.w3c.es/Divulgacion/GuiasBreves/Seguridad>
- Wallace, C., Pordesch, U., & Brandner, R. (03 de 03 de 2007). *Long-Term Archive Service Requirements*. Obtenido de IETF Tools: <https://tools.ietf.org/pdf/rfc4810.pdf>