TECNOLÓGICO NACIONAL DE MÉXICO

Instituto Tecnológico de Tuxtla Gutiérrez

SEP
SECRETARÍA DE EDUCACIÓN PÚBLICA

Ingeniería en sistemas computacionales.

Protocolo de Investigación.

Sistema de Administración de Documentos Digitales Firmados Electrónicamente.

Línea de Investigación:

Tecnologías de la Información y Bases de Datos.

Nombre de la Empresa o Institución:

Grupo de investigación científica y desarrollo tecnológico A. C.

Presentan:

Rincon Trujillo Jessica. 13270272

Espinosa López Adrián Alejandro. 12270727

Asesor:

Dr. Jorge Humberto Ruiz Ovalle

Tuxtla Gutiérrez, Chiapas, México a 16 de mayo de 2016

Índice

Introducción

1.1. Antecedentes

Los inicios de los certificados tal como lo conocemos existen a partir de creación de la firma manuscrita, utilizados como instrumentos (documento, diploma, cedula, personaría jurídica) que afirma la veracidad de un hecho, el cual puede ser la obtención de un bien material, un diploma académico, contratos de trabajo, etc.

El origen de la firma y certificado digital empezó con la creación de la criptografía de clave pública que fue introducido por James Ellis el año de 1969 al tratar de vislumbrar el concepto de criptografía asimétrica. En 1973 el matemático Clifford Cocks plantea la posibilidad de utilizar números primos y la factorización como base del sistema. En 1975 James Ellis, Clifford Cocks y Malcolm Williamson habían descubierto todos los aspectos fundamentales de la criptografía de clave pública incluyendo las técnicas RSA y Diffie-Hellman con algoritmos computacionales. Mientras Whitfield Diffie y Martin Hellman en el año de 1975 a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro, logran redescubrir la Criptografía Asimétrica, el cual fue el principio de las firmas digitales. Este sistema utilizaba dos claves diferentes: una para cifrar y otra para descifrar. En 1978 aparece el algoritmo de criptografía más utilizado y extendido en el mundo, conocido como RSA [1].

Para 1993 se introdujo el concepto de certificados digitales con el fin de entregar a máquinas y a usuarios medios de autentificación a través del Internet y otras redes de comunicación.

Las firmas digitales fueron creadas en 1997 con el objetivo de suministrar al mercado productos eficientes en lo referente a algoritmos criptográficos fuertes generados a partir del concepto de firmas holográficas [1].

En el diario oficial de la federación, el 11 de enero del año 2012 se publicó el decreto por el que se expide la ley de Firma Electrónica Avanzada (FEA). En dicho decreto se menciona (indirectamente) que la firma electrónica estará basada en el uso de certificados digitales por lo que la criptografía de llave pública y el uso de PKIs es requerida [2].

A partir de este decreto, varios estados de la república mexicana han emitido leyes para el uso de la firma Electrónica, así como la ley de firma electrónica avanzada del estado de Chiapas publicada en el Periódico Oficial el miércoles 21 de octubre de 2009 y con su última reforma publicada el 28 de noviembre de 2012 [3].

Uno de los principales problemas que se perciben en la implementación de FEA en México es que actualmente los sistemas de la Administración Pública Federal que utilizan firma electrónica, emplean componentes criptográficos personalizados al 100% con la aplicación, por lo que no pueden ser reutilizados para otros servicios. Las aplicaciones de la FEA han sido principalmente para el gobierno, a nivel municipal, estatal y federal.

Fue el gobierno del estado de Guanajuato la primera administración pública de México en implementar el mecanismo de firma electrónica para la prestación de servicios públicos. En 2008, el estado de México contaba con alrededor de 20 procesos con firma digital [2].

El grupo de investigación científica y desarrollo tecnológico (GICDT) es una Asociación Civil constituida legalmente desde el año 2000. El principal objetivo es fomentar el desarrollo integral en la investigación científica y la tecnología tanto en jóvenes estudiantes como a profesionistas desde un nivel medio superior y hasta el doctorado.

El GICDT satisface las necesidades de la sociedad aplicando la tecnología en la solución de problemas de la vida diaria. Está conformado por un grupo de personas emprendedoras comprometidas con la sociedad, aplicando los conocimientos y desarrollando nuevas tecnologías, enfocadas a la solución de problemas y al bienestar de la sociedad, incluso en el ámbito internacional. La consolidación del grupo fue desde el año 2004 a la fecha, propiciando la idea en difundir fortalezas del grupo de trabajo para contribuir con el desarrollo de Chiapas. Cuenta con una revista tecnológica para la publicación de artículos oficiales, un grupo de investigación, proyectos de investigación, divulgaciones y una bolsa de trabajo. Y gestiona la administración de cursos, talleres, capacitaciones y conferencias, de investigaciones científicas y tecnológicas.

Por los antecedentes citados se hace una necesaria implementación de un sistema de administración de documentos digitales firmados electrónicamente para el GICDT, qué permita gestionar de manera ágil el proceso de firmado de documentos electrónicos con validez oficial, y almacenar los datos necesarios para la autenticación de los documentos generados por dicha firma en una notaría digital.

La inquietud de desarrollar esta investigación es causada por el interés personal de generar un sistema que dé solución a la problemática actual que existe conforme al firmado de documentos y cubra las necesidades de la organización con la implantación de las firmas electrónicas.

1.2. Planteamiento del problema

El grupo de investigación científica y desarrollo tecnológico A. C. consta con una plataforma en la que se otorga un servicio para alumnos y profesores, quienes estén interesados en dar o recibir, cursos, capacitaciones, o simplemente contar con un historial adecuado para diversas organizaciones. Más sin embargo esta organización tiene la problemática de qué la logística para la impresión de constancias y papeles oficiales es muy tardada dado que se requieren las firmas de quien (es) realizaron dicho curso y del director de la organización.

Gestiona la administración de cursos, talleres, capacitaciones y conferencias, de investigaciones científicas y tecnológicas, donde actualmente para la validación de participación se otorgan constancias o diplomas. De igual manera las instituciones u organizaciones como empresas organizadoras de este tipo de eventos tienen la necesidad de emitir un documento de este tipo.

Comúnmente las constancias o diplomas se otorgan en papel y llevan impresos la fecha de emisión, el nombre e información del taller o curso y de la institución u organización, así miso el nombre completo del instructor y del líder de la institución u organización (director o rector, gobernador, etc.) quienes firman caligráficamente (manualmente) y formalmente dicho documento para hacerlo oficial o en su caso legal.

Lo cual implica que se tenga que firmar individualmente cada documentó por la cantidad total de dichos participantes. Lo que conlleva a un tiempo muy tardado para hacer el trámite de los documentos, de hasta 30 días hábiles, siendo así un trabajo muy tedioso dado la recolección de cada firma.

La impresión de documentos para su certificación conlleva a un incremento del consumo de papel. Implicando un aumento en la emisión de residuos e incrementación del consumo de recursos naturales empleados en la fabricación del papel (árboles, agua y energía), afectando con un gran impacto al medio ambiente.

Dada dicha problemática es necesario la implementación de un sistema de Administración de documentos digitales firmados electrónicamente, qué permita gestionar de manera ágil el proceso de validación y autentificación de documentos electrónicos, y almacenar los datos necesarios en una notaría digital.

2. Hipótesis

El desarrollo de un Sistema de Información permitirá mediante metodología “SCRUM” realizar el proceso de certificación de constancias y/o diplomas utilizando firmas electrónicas avanzadas del Grupo de Investigación Científica y Desarrollo Tecnológico concediendo verificar la autenticidad de los documentos generados mediante tecnologías web.

3. Objetivo general y específico

3.1. Objetivo general

Diseñar y desarrollar un software que administre y almacene de una manera ágil documentos autentificados por medio de firmas electrónicas extendidas por la Secretaria de la Función Pública del Estado de Chiapas, verificando la autenticidad del documento en una página web.

3.2. Objetivos específicos

- Diseñar la base de datos que almacene información (constancias, tallares, participantes).
- Implementar una plataforma de almacenamiento.
- Obtener una firma electrónica de la empresa en la Secretaria de la Función Pública del Estado de Chiapas, permitiendo con dicha firma poder realizar la certificación de documentos.
- Realizar y generar el proceso de firmado, agilizándolo con la implementación un sistema encargado de la certificación automática de la documentación de una manera ágil.
- Almacenar la información del proceso de firmado en la base de datos, perdiendo así ya con la implementación en la página web la verificación de la autenticidad de un documento.
- Implementación del sitio web utilizando para su diseño el estándar SCRUM, que permita a los usuarios acceder a él, en el momento que ellos lo necesiten, y realizar los procesos de certificación y verificación de los documentos generados.

4. Justificación

La firma electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuya función básica es identificar de manera única y segura al firmante, asegurando la integridad del documento firmado.

Cero Papel es la iniciativa del Plan Vive Digital que busca hacer más eficiente la gestión administrativa interna en las entidades públicas con el fin de prestar un mejor y más eficiente servicio al ciudadano.

La firma electrónica avanzada permite certificar documentos digitales y eliminar papeles en los trámites. Al certificar documentos electrónicos se evita el plagio de la información y se garantiza que el documento no ha sido modificado, por eso existe la necesidad de implementar un sistema de administración de documentos digitales firmados electrónicamente, que permitirán agilizar y mejorar la gestión de procesos y documentos, como también consultarlos y autenticarlos.

Mediante el desarrollo de un sitio web que administre dichos documentos se logrará la autenticación, validación, recuperación y consulta de forma rápida y las veces que sea necesario mediante la plataforma de internet; esto permitirá agilizar todos los procesos involucrados (institución, instructor, cliente).

5. Estado del arte

Actualmente existe un gran número de aplicaciones que permiten firmar digitalmente documentos de manera independiente, así como también aplicaciones Web. A continuación, se presentarán tesis y artículos que hablan acerca de este tema y como lo han implementado.

5.1. Desarrollo de una Aplicación para Administración de Firmas y Certificados Digitales

El proyecto de grado elaborado por Marcelo Invert Palma Salas (2005) de la escuela militar de ingeniería en la Paz-Bolivia describe la implementación de una aplicación que garantiza la integridad y autenticidad de los mensajes generados, protegiendo la información, equipos y recursos humanos de la Superintendencia de Telecomunicaciones (SITTEL). Evitando la pérdida y modificación de la información [1].

La aplicación de firmas y certificados digitales acorde a la Norma Boliviana ISO-IEC 17799 para los procesos internos de intercambio de información en la SITTEL permitió tener un mayor nivel de confiabilidad y conservo la integridad de la información como también se verifico la autenticidad del origen del mensaje [1].

Aplicando un modelo lineal secuencial para el desarrollo de firmas y certificados digitales, salvaguardando así la integridad y autenticidad de la Información.

Ilustración 1. Interface del Sistema de Administración de Firmas y Certificados Digitales.

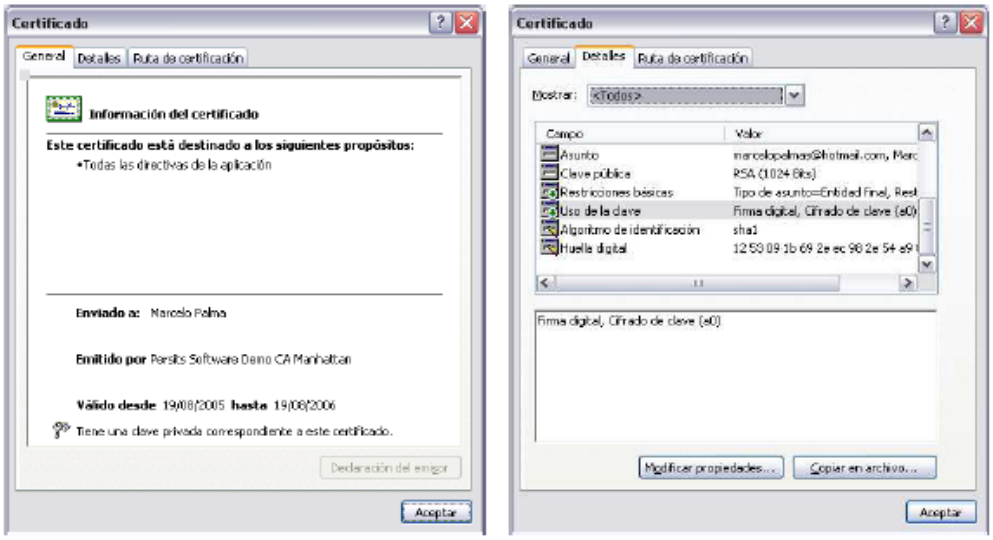

Ilustración 2. Modelo de Certificados Digitales X.509.

5.2. Implementación de firma digital en una plataforma de comercio electrónico

La tesis de licenciatura elaborada por Julio René Santizo Ochoa (2010) de la Universidad de Ingeniería en Ciencias y Sistemas de San Carlos de Guatemala describe la implementación de firma digital para la plataforma de comercio electrónico y construcción del sitio web por medio de la metodología de desarrollo incremental. Permitiéndoles evaluar constantemente los avances y correcciones gracias a dicha metodología [4].

La plataforma de comercio electrónico elimino las barreras idiomáticas y e hiso del comercio entre países, exportaciones e importaciones, una tarea menos complicada y tediosa. Desarrollando un sistema experto que ayuda a las pequeñas y medianas empresas a realizar exportaciones e importaciones sin la necesidad de entender el idioma de la empresa con la cual se negocia, ya que cada empresa verá los documentos en su propio lenguaje. [4]

Dado que dicha documentación (facturas, contratos, etc.) debe de proporcionar una seguridad legal, se optó por implementar la firma digital como un elemento fundamental para dar seguridad legal a dichos documentos.

El esquema de firma de contratos incluye que se generen hasta tres copias por cada contrato: un contrato original sin firmas, un contrato con la firma del vendedor y otro con la firma de ambas partes; esto para tener evidencia de cada etapa del proceso para futuros reclamos legales que puedan suscitarse [4].

Ilustración 3. Sitio web de e-certchile para certificación.

5.3. Experimento Piloto de Firma Digital de Actas Académicas

El artículo de la revista electrónica LATIN AMERICA TRANSACTIONS (IEEE) experimento piloto de firma digital de actas académicas publicado por J. Ferragut Martínez-Vara de Rey, B. Serra Cifre, de la Universidad de les Illes Balears, España trata acerca de la experiencia de firma digital de actas académicas y su implementación y describe la modificación de la página web de ÁGORA para incorporar nuevas funcionalidades de certificación con infraestructura de Clave Pública (PKI) [5].

El mayo de 2002, el Centro de Tecnologías de la Información de la Universidad de las Illes Balears, España (CTI@UIB) comenzó a trabajar en la implementación de la Infraestructura de Clave Pública (PKI) de ámbito universitario [5]:

- Generando conocimiento práctico a través del estudio de la tecnología actual en el mundo de las Infraestructuras de Clave Pública.
- Construyendo una plataforma tecnológica que permitiera la puesta en marcha de futuros servicios basados en certificación y firma digital.

El desarrollo de esta experiencia piloto profundizo en la utilización de la criptografía de clave pública como mecanismo para simplificar al máximo los trámites académicos que supone la firma de actas. Una vez implementado, el nuevo proceso de validación digital se evitó desplazamientos de profesores y agilizo los trámites [5].

La firma digital de actas académicas se apoyó en dos grandes líneas de desarrollo:

a) Una Infraestructura de Clave Pública como elemento generador de confianza y mecanismo de certificación digital al servicio de los colectivos de PAS (Personal de Administración y Servicios) y PDI (Personal Docente e Investigador).
b) Para minimizar el impacto sobre la estructura existente, se diseñó un sistema que permitió a los profesores enviar, de forma segura, las actas firmadas digitalmente al personal de Secretaría Académica.

Ilustración 4. Interface web de la nueva versión de Ágora.

5.4. La mejora de la fiabilidad de las firmas digitales como prueba de no repudio bajo un modelo de amenaza global

La tesis doctoral de López Hernández Ardieta (2011) de la Universidad Carlos III de Madrid describe el diseñó una taxonomía integral de ataques potenciales a la firma digital que permite su clasificación sistemática y rigurosa dadas las amenazas de seguridad que socavan la fiabilidad de las firmas digitales tuvieron que ser formalizadas y categorizadas.

Dicha propuesta robusta y confiable permitirá mejorar la habilidad de las firmas digitales, reforzando así su propiedad de no repudio. Basada en los mecanismos:

- El paradigma de la división del entorno de firma y las políticas extendidas de firma electrónica.
- Diseñado de un nuevo protocolo de intercambio justo donde se integra esta propuesta, demostrando su aplicabilidad en un escenario concreto.

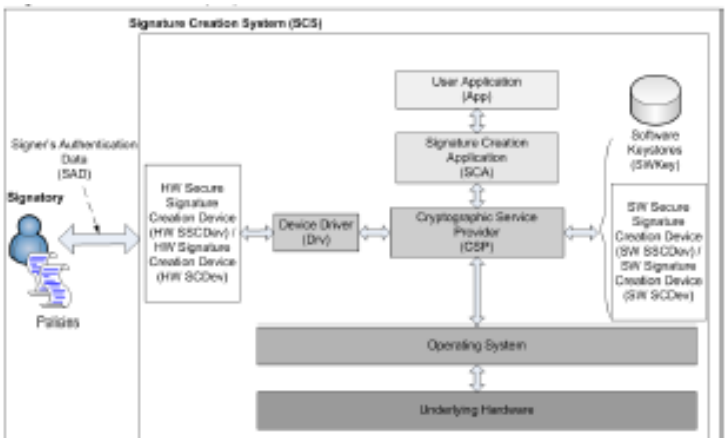

Ilustración 5. Diagrama de modelo funcional.

Tabla comparativa de proyectos		
Proyecto	**Descripción**	**Características**
Desarrollo de una Aplicación para Administración de Firmas y Certificados Digitales	Aplicación de firmas y certificados digitales acorde a la Norma Boliviana ISO-IEC 17799 para los procesos internos de intercambio de información en la Superintendencia de Telecomunicaciones (SITTEL).	• Permite tener un mayor nivel de confiabilidad. • Conserva la integridad de información. • Verifica la autenticidad del origen del mensaje. • Permite salvaguardar la integridad y autenticidad de la Información.
Implementación de firma digital en una Plataforma de comercio electrónico	La plataforma de comercio elimino las barreras idiomáticas. Desarrollando un sistema experto que ayuda a las pequeñas y medianas empresas a realizar exportaciones e importaciones sin la necesidad de entender el idioma de la empresa con la cual se negocia. Implementando firma digital como un elemento fundamental para dar seguridad legal a dichos documentos (facturas, contratos, etc.).	• La plataforma de comercio digital hiso del comercio entre países, exportaciones e importaciones, una tarea menos complicada y tediosa. • Proporciona una seguridad legal. • Genera tres copias por contrato: un contrato original sin firmas, un contrato con la firma del vendedor y otro con la firma de ambas partes • Se obtiene una evidencia de cada etapa del proceso para futuros reclamos legales que puedan suscitarse.
Experiencia Piloto de Firma Digital de Actas Académicas	El Centro de Tecnologías de la Información de la Universidad de las Illes Balears, España (CTI@UIB) trabajo en la implementación de la Infraestructura de Clave Pública (PKI), diseñando un sistema que permite la autentificación de actas académicas por medio de la firma digital.	• Generar conocimiento práctico a través del estudio de la tecnología actual en el mundo de las Infraestructuras de Clave Pública. • Se construyó una plataforma tecnológica, permitiendo futuros servicios basados en certificación y firma digital. • Permitió a los profesores enviar, de forma segura, las actas firmadas digitalmente al personal de Secretaría Académica.

La mejora de la fiabilidad de las firmas digitales como prueba de no repudio bajo un modelo de amenaza global	Se diseñó una taxonomía integral de ataques potenciales a la firma digital. Presentando una propuesta robusta y confiable, basada en: Un paradigma de división del entorno de firma y las políticas extendidas de firma electrónica. Un diseñado de un nuevo protocolo de intercambio justo donde se integra esta propuesta, demostrando su aplicabilidad en un escenario concreto.	• Proporciona un nivel aceptable de confianza para producir evidencias de no repudio fiables basadas en firmas digitales. • Permite la clasificación sistemática y rigurosa de las firmas digitales. • Mejora la habilidad de las firmas digitales, reforzando su propiedad de no repudio.
Sistema de administración de documentos digitales firmados electrónicamente	Implementó de un sistema para la administración de documentos digitales firmados electrónicamente extendidos por la Secretaria de la Función Pública del Estado de Chiapas, para el Grupo de Investigación Científica y de Desarrollo Tecnológico (GICDT). Verificando la autenticidad del documento en una página web.	• Permite gestionar de manera ágil el proceso de validación y autentificación de documentos electrónicos. • Almacena los datos necesarios en una notaría digital. • Se evita un constante uso del papel. • Implementación del sitio web para la validación y autentificación de firmas electrónicas generadas.

Tabla 1. Comparación del proyecto con el Sistema de administración de documentos digitales firmados electrónicamente

6. Propuesta técnica del proyecto

Se aplicara el método ágil Scrum para el desarrollo de un sistema de certificación de documentos digitales firmados electrónicamente y un sistema web que permita verificar la autenticidad de los documentos generados (constancias y/o diplomas) para el GICDT. Permitiendo gestionar de manera ágil el proceso de validación y autentificación de documentos electrónicos, y almacenar los datos necesarios en una notaría digital.

El principal motivo que llevó a la elección de la metodología Scrum es que uno de los métodos de gestión de proyectos más innovadores de los denominados ágiles, destacándose por una gran descentralización como medio para alcanzar la mayor productividad posible. Está basado en un proceso constructivo iterativo e incremental donde las iteraciones tienen duración fija pero corta y el resultado final de cada una de ellas es un producto funcional que contiene un subconjunto de los requerimientos del proyecto.

Se implementara utilizando un proceso de elaboración para páginas web que consiste en planificación, análisis, diseño, construcción y prueba, e implementación, cumpliendo con los principios y valores de las metodologías ágiles aplicando herramientas de ingeniería del software.

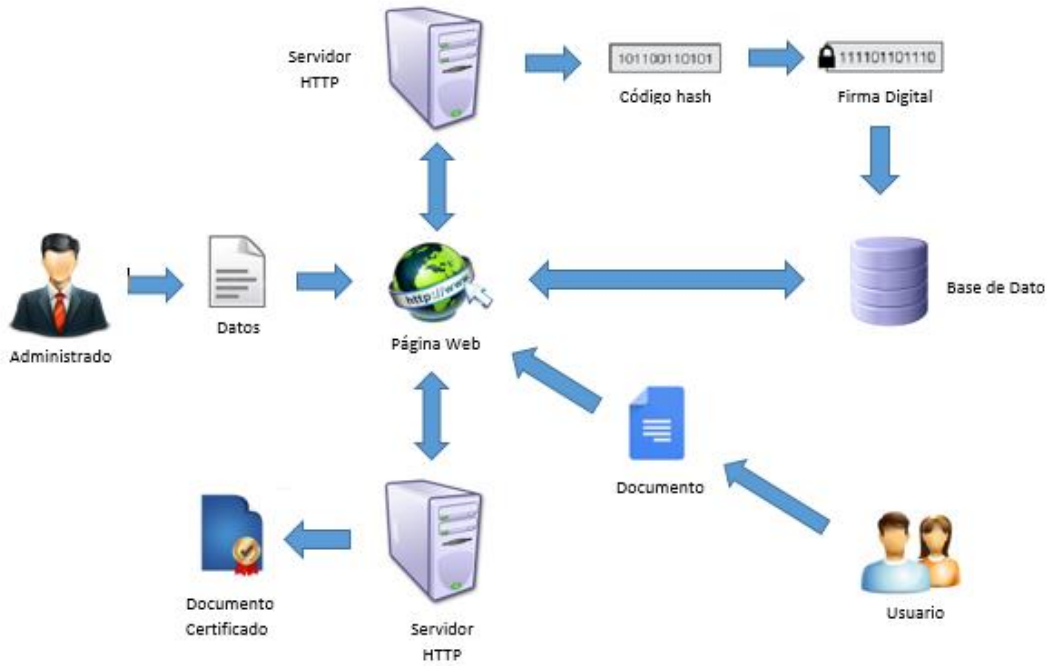

Ilustración 6. Propuesta del sistema para la generación de documentos digitales certificados con firmas electronicas.

Ilustración 6. Propuesta del sistema para la verificación de documentos digitales certificados con firmas electronica.

7. Impacto social o tecnológico

7.1. Impacto social

Al implementar el sistema de administración de documentos digitales firmados electrónicamente para el Grupo de Investigación Científica y de Desarrollo Tecnológico (GICDT) se ahorrará tiempo, dinero y esfuerzo, ya que se lograrán transacciones seguras y con resultados instantáneos.

Así mismo con el desarrollo del sitio web que administre dichos documentos se evitara el plagio de la información y se garantiza que los documentos no han sido modificados. Obteniendo:

- Aumento de la productividad.
- Optimización de los recursos.
- Disminución de los costos asociados a la administración de papel, tales como almacenamiento e insumos.
- Eliminar la duplicidad de documentos.
- Disminuir los tiempos de localización de los archivos.

7.2. Impacto tecnológico

El desarrollar este sistema logrará con el uso de la firma electrónica el incremento sustancial de productividad (disminución de tiempos y costos), lo cual favorecerá con el uso de la tecnología la competitividad en nuestro país. Obteniendo:

- Procesos y servicios más eficaces y eficientes.
- Buenas prácticas en gestión documental.
- Mayor control y seguridad en el manejo de la información.
- Reducir las necesidades de espacio de almacenamiento.
- Protección de la información del individuo.

7.3. Impacto ambiental

- Ahorro de papel.
- Disminución del consumo de recursos naturales empleados en la fabricación del papel: árboles, agua y energía.
- Disminución de la contaminación producida por los productos blanqueadores de papel.
- Disminuir el consumo de energía empleada en imprimir, fotocopiar, etc.
- Reducir los residuos contaminantes como tóner, cartuchos de tinta, etc.

8. Cronograma de actividades

Cronograma de Actividades																						
Actividad	Mes	Enero				Febrero				marzo				Abril				Mayo				
	Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	
Buscar propuesta de proyecto																						
Registrar propuesta de proyecto																						
Entregar propuesta de proyecto																						
Antecedentes																						
Planteamiento del problema																						
Hipótesis																						
Objetivo general																						
Presentar avance para primera revisión																						
Realizar Objetivos específicos																						
Justificación																						
Estado del arte																						
Presentar avance para segunda revisión																						
Elaborar propuesta técnica del proyecto																						
Impacto social o tecnológico																						
Marco teórico																						
Presentar avance para Tercera revisión																						
Entregar protocolo																						

Tabla 2. Cronograma de actividades 7º Semestre (Taller de investigación I)

Cronograma de Actividades																					
Actividad	Mes	Agosto				Septiembre				Octubre				Noviembre				Diciembre			
	Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Definir un backlog completo																					
Trazar los “Paquetes de productos” (objetos) del backlog de la versión elegida.																					
Obtener y analizar los requisitos del sistema																					
Planeación del diseño del sistema																					
Reunión de revisión de diseño																					
Diseñar interfaces del sistema																					
Diseñar y desarrollar la base de datos																					
Corregir errores																					
Conexión de la base de datos con el sistema																					
Presentar avance para cuarta revisión																					
Exponer proyecto en seminario																					

Tabla 3. Cronograma de actividades 8º Semestre (Taller de investigación II)

Cronograma de Actividades																					
Actividad	Mes	Enero				Febrero				marzo				Abril				Mayo			
	Semana	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4	1	2	3	4
Codificar las páginas web																					
Presentar avance para quinta revisión																					
Revisión de operatividad y funcionalidad																					
Corregir errores																					
Implementar el sistema																					
Pruebas de funcionalidad del sistema																					
Montar el servidor																					
Revisión final funcionando																					
Manual de usuario																					
Capacitación a usuarios																					
Entrega final																					
Exponer residencia en seminario																					

Tabla 4. Cronograma de actividades 9º Semestre (Residencia Profesional)

9. Marco Teórico

9.1. Firma electrónica

Una firma electrónica se puede usar para autenticar la identidad de quien envía un mensaje o quien firma un documento electrónico, así como asegurar que el contenido original del mensaje o del documento electrónico que ha sido enviado no ha sido modificado [2].

9.1.1. Firma electrónica simple

El término firma electrónica (o firma electrónica simple) implica el uso de cualquier medio electrónico para firmar un documento. Es este sentido, el simple escaneo de una firma autógrafa y su inserción como imagen en un documento digital puede considerarse como firma electrónica [2].

La firma electrónica hace referencia, a la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje [4].

9.1.2. Firma electrónica avanzada - firma digital

La firma digital o firma electrónica avanzada (FEA) establece que se entiende como tal, aquella firma, que, a través de un certificado digital emitido por una entidad de certificación acreditada, incorpore una serie de datos electrónicos que identifican y autentifican al firmante a través de la asignación de una llave pública y otra privada en base a los parámetros de la criptografía asimétrica (o también conocida como de llave pública). Mediante este proceso, se garantiza que en el caso de sufrir variaciones en la firma y/o gestión de documentación electrónica, la responsabilidad es del usuario, ya que, al tener esta firma bajo su control exclusivo, el usuario es por tanto el responsable último de todos los procesos asociados a la misma [2].

La firma electrónica digital de un documento es el resultado de aplicar cierto algoritmo matemático, denominado función hash, a su contenido y, seguidamente, aplicar el algoritmo de firma (en el que se emplea una clave privada) al resultado de la operación anterior [4].

9.1.2.1. Función de la firma electrónica avanzada

Las firmas digitales son fácilmente transportables y no pueden imitarse. La firma digital puede aplicarse a cualquier tipo de información electrónica, ya sea que se encuentre cifrada o en texto claro [2]. En la tabla 5 se muestra una comparación entre la firma digital y la firma autógrafa.

Propiedad	Firma autógrafa	Firma digital
Se puede aplicar a documentos electrónicos y transacciones	No	Si
El proceso de verificación de firma digital puede automatizarse	No	Si
La firma permite detectar alteraciones en el documento	No	Si
Está reconocida por la ley	Si	Si

Tabla 5. Ventajas de la firma electrónica avanzada (firma digital) frente a la firma autógrafa.

En términos prácticos y desde el punto de vista legal, una firma digital provee una solución viable para contar con documentos electrónicos con validez jurídica.

Con ello, es posible eliminar la necesidad de contar con documentos impresos firmados. Además de los ahorros en consumo de papel, la firma digital permite automatizar los procesos de manipulación de los documentos, tales como su distribución y almacenamiento. La implementación de la firma digital está regulada de acuerdo a las leyes de cada país.

9.2. Metodología ágil Scrum

Scrum es una metodología ágil de gestión de proyectos cuyo objetivo primordial es elevar al máximo la productividad de un equipo. Reduce al máximo la burocracia y actividades no orientadas a producir software que funcione y produce resultados en periodos muy breves de tiempo [7].

Se comienza con la visión general de lo que se desea obtener, y a partir de ella se especifica y da detalle a las partes de mayor prioridad, y que se desean tener cuanto antes.

Cada ciclo de desarrollo o iteración (sprint) finaliza con la entrega de una parte operativa del producto (incremento). La duración de cada sprint puede ser desde una, hasta seis semanas, aunque se recomienda que no excedan de un mes. En scrum, el equipo monitoriza la evolución de cada sprint en reuniones breves diarias donde se revisa en conjunto el trabajo realizado por cada miembro el día anterior, y el previsto para el día en curso. Esta reunión diaria es de tiempo prefijado de 5 a 15 minutos máximo, se realiza de pie junto a un tablero o pizarra con información de las tareas del sprint, y el trabajo pendiente en cada una. Esta reunión se denomina “reunion de pie” o “scrum diario” y si se emplea la terminología inglesa: “stand-up meeting”, también: “daily scrum” o “morning rollcall” [7].

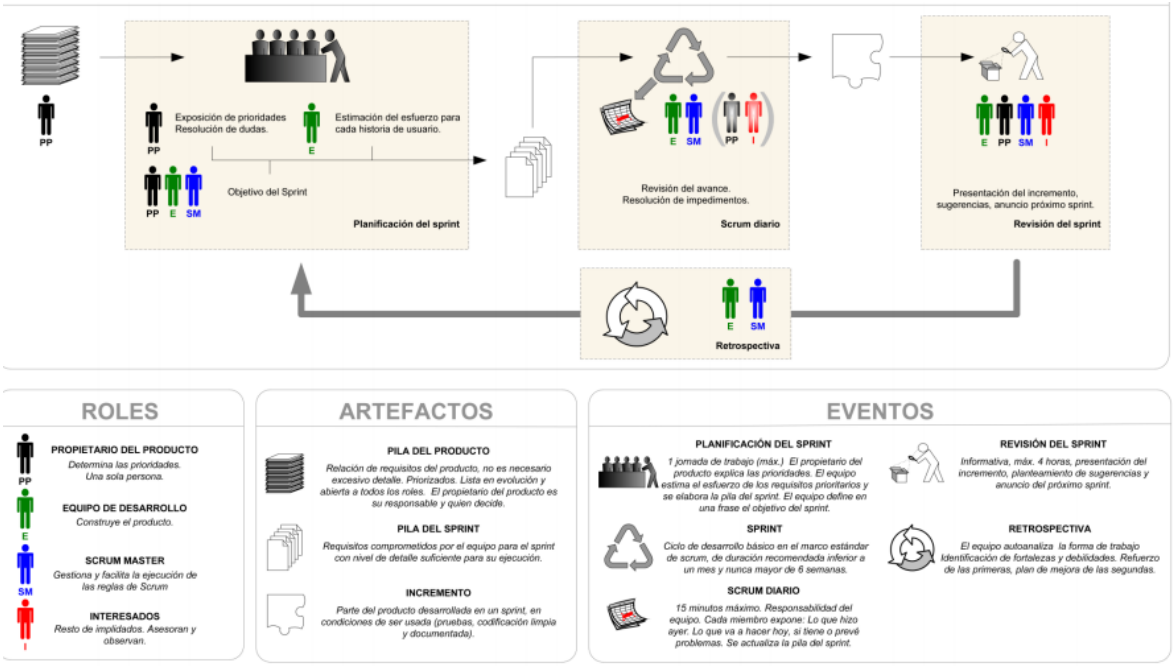

Ilustración 8. Marco Scrum técnico.

9.3. Servidor Web

El servidor de Páginas es el encargado de generar y enviar información a los usuarios finales.

El servidor web responde a las solicitudes de los clientes (por lo general de un navegador Web) y proporciona recursos como documentos. Asocia el URL con un recurso en el servidor (o con un archivo en la red del servidor) y devuelve el recurso solicitado al cliente. Durante esta interacción, el servidor Web y el cliente se comunican mediante una plataforma independiente [8].

9.4. Servidores web

Los Servidores de Páginas Web son Servidores de Aplicaciones ya que se les ha desarrollado alguna funcionalidad especial que les permite realizar, valga la redundancia, aplicaciones de Servidor [9].

Dependiendo de la funcionalidad se trae consigo complejidad al sistema, ya sea en la forma de requerimientos del sistema (memoria, procesadores), carga administrativa (configuración, tiempo de desarrollo) o alguna otra.

Entre los principales Servidores Web podemos encontrar los siguientes:

- Apache
- Nestcape Enterprise 3.0
- Microsoft IIS
- AOLServer
- WebLogic Tengah
- Lotus Domino Go Web Server
- IBM Interner Conecction Server
- Java Web Server

9.4.1. Apache

Apache es uno de los Servidores de páginas más utilizados.

- Es capaz de utilizar otros interpretadores y lenguajes como PhP, Python.
- Puede conectarse directamente a una Base de datos.

Cuando el Servidor de Páginas Web recibe la requisición de un cliente, éste reconoce cuando debe enviar un documento estático o ejecutar algún tipo de aplicación, si se invoca un programa en Perl y este a su vez solicita información a una base de datos, por lo tanto, para llevar a cabo esta operación se inician dos procesos nuevos, y si no se tienen los suficientes recursos en cuanto a memoria y procesadores se refiere, seguramente el servidor será insuficiente [9].

9.5. Servicios web

Un servidor web es una clase que permite que sus métodos sean llamados por otros métodos en otros equipos a través de formatos de datos y protocolos comunes, como XML y HTTP. Se describe así mismo y a las aplicaciones empresariales modulares que exponen la lógica de negocio como servicios sobre Internet a través de interfaces programables y el uso de protocolos de Internet con el propósito de proporcionar formas de buscar, suscribirse e invocar esos servicios [10].

Ejemplos del uso de los servicios web:

- Validaciones de tarjetas de crédito y autorizaciones entre instituciones bancarias.
- Consultas enviando mensajes de texto desde teléfonos celulares.
- Consultas a bases de datos como las que permiten realizan el Registro Nacional de Población (RENAPO) y la Secretaria de Administración Tributaria (SAT).
- Servicios de búsqueda en internet utilizando Google.

9.6. Xml

El lenguaje de marcado extensible (XML) fue desarrollado en 1996 por el Grupo de trabajo de XML del Consorcio World Wide Web (W3C). XML es una tecnología abierta (es decir, tecnología no propietaria) con amplio soporte para describir datos, y se ha convertido en el formato estándar para el intercambio de datos entre aplicaciones a través de Internet [8].

XML permite a los autores de documentos crear marcado (es decir, una notación basada en texto para describir datos) para casi cualquier tipo de información. Esto les permite crear lenguajes de marcado completamente nuevos para describir cualquier tipo de datos, como las fórmulas matemáticas, las instrucciones de configuración de software, las estructuras moleculares químicas, la música, las noticias, las recetas y los reportes financieros. XML describe los datos en una forma que los seres humanos puedan comprender y las computadoras puedan procesar.

9.7. Base de datos (mysql)

9.7.1. Base de datos

Una base de datos es un conjunto de datos almacenados en memoria externa que están organizados mediante una estructura de datos [8]. Cada base de datos ha sido diseñada para satisfacer los requisitos de información de una empresa u otro tipo de organización.

Una base de datos se puede percibir como un gran almacén de datos que se define y se crea una sola vez, y que se utiliza al mismo tiempo por distintos usuarios. En una base de datos todos los datos se integran con una mínima cantidad de duplicidad. De este modo, la base de datos no pertenece a un solo departamento, sino que se comparte por toda la organización. Además, la base de datos no sólo contiene los datos de la organización, también almacena una descripción de dichos datos [11].

9.7.2. Sistema de gestión de bases de datos

El sistema de gestión de la base de datos (SGBD) es una aplicación que permite a los usuarios definir, crear y mantener la base de datos, además de proporcionar un acceso controlado a la misma. Se denomina sistema de bases de datos al conjunto formado por la base de datos, el SGBD y los programas de aplicación que dan servicio a la empresa u organización [11].

La abstracción de datos es el modelo seguido con los sistemas de bases, se da una implementación interna de un objeto y una especificación externa separada, permite cambiar la implementación interna de un objeto sin afectar a sus usuarios ya que la especificación externa no se ve alterada.

9.7.3. Lenguaje SQL

El lenguaje de programación Structured Query Language (SQL), desarrollado por IBM en 1981, es el lenguaje estándar que permite manejar los datos de una base de datos relacional. La mayor parte de los SGBD relacionales implementan este lenguaje y mediante él se realizan todo tipo de accesos a la base de datos.

Una base de datos relacional está formada por un conjunto de relaciones. A las relaciones, en SQL, se las denomina tablas. Cada tabla tiene una serie de columnas (son los atributos). Cada columna tiene un nombre distinto y es de un tipo de datos (entero, real, carácter, fecha, etc.). En las tablas se insertan filas (son las tuplas), que después se pueden consultar, modificar o borrar [11].

9.7.3.1. Mysql

Mysql es un sistema de gestión de bases de datos relacional, licenciado bajo la GPL de la GNU, creada por la empresa sueca MySQL AB. Utiliza el lenguaje de programación SQL.

Características principales:

- Velocidad y robustez.
- Soporta gran cantidad de tipos de datos para las columnas.
- Gran portabilidad entre sistemas, puede trabajar en distintas plataformas y sistemas operativos.
- Cada base de datos cuenta con 3 archivos: Uno de estructura, uno de datos y uno de índice y soporta hasta 32 índices por tabla.
- Aprovecha la potencia de sistemas multiproceso, gracias a su implementación multihilo.
- Flexible sistema de contraseñas (passwords) y gestión de usuarios, con un muy buen nivel de seguridad en los datos.
- El servidor soporta mensajes de error en distintas lenguas.

10. Referencias Bibliográficas

[1] PALMA SALES, M. (2005). *Desarrollo de una aplicación para administración De firmas y certificados digitales, Caso: superintendencia de telecomunicaciones* (Grado). Escuela militar de ingeniería (La paz – Bolivia).

[2] MIGUEL MORALES, A. DÍAZ y L. DOMÍNGUEZ. (junio, 2013). *Firma electrónica: concepto y requerimientos para su puesta en práctica.* IEEE, Centro de Investigación y de Estudios Avanzados Del Instituto Politécnico Nacional, 22.

[3] *Ley de firma electrónica avanzada del estado de Chiapas.* (28, noviembre, 2012).

[4] GARCÍA ROJAS, W. (2008). *Implementación de firma digital en una plataforma de comercio electrónico* (Licenciatura). Pontificia, Universidad Católica del Perú.

[5] J. FERRAGUT MARTÍNEZ-VARA DE REY, B. SERRA CIFRE. (abril, 2005). *Experimento Piloto de Firma Digital de Actas Académicas*. IEEE Latin American Transactions, 2, 15.

[6] LÓPEZ HERNANDEZ-ARDIETA, J. (2011). *Enhancing the reliability of digital signatures as non-repudiation evidence under a holistic threat model* (Doctoral). University Carlos III of Madrid.

[7] PALACIO, J. (2014). *Gestiónde proyectos Scrum Manager*. 2nd ed. Scrum manager, pp.23-37.

[8] D. PAUL, D. HARVEY, & D. ABBEY (2016). *Internet & World Wide Web, como programar* (5th edición, pp. 511-515, 605-611 y 617-634). México: Pearson.

[9] ÁVILA FLORES, J. (2005). *Sistema de Administración de Red (S.A.R.) Versión 1.0* (Licenciatura). Universidad Autónoma del Estado de Hidalgo.

[10] ANAYA LÓPEZ, E. (2016). *Implementación de controles de seguridad en arquitecturas orientadas a servicios (SOA) para servicios web* (Maestría en ciencias con especialidad en informática). Instituto Politécnico Nacional de México.

[11] MARQUÉS, M. (2011). *Bases de datos* (1st ed., pp. 1-5 y 41-49). Castelló de la Plana: Universitat Jaume. Retrieved from http://www.sapientia.uji.es