Programación Matemática y Software (2020) 12 (3): 49-57. ISSN: 2007-3283

Prototipo de software para la firma y validación de documentos electrónicos

Software prototype for the electronic document's signature and validation

Erick Manuel Ramírez Casanova[1], Rogelio Enrique Telona Torres[2], Juan Rafael González Cadena[2]*

[1] Ingeniería Informática(estudiante), TecNM campus San Andrés Tuxtla,
Carretera Costera del Golfo Km 140+100, Matacapan,
San Andrés Tuxtla, Veracruz, México, C.P. 95804

[2] División de Ingeniería Informática, TecNM campus San Andrés Tuxtla,
Carretera Costera del Golfo Km 140+100, Matacapan, San Andrés Tuxtla, Veracruz, México, C.P. 95804

Correo-e: jrgcadena@hotmail.com

PALABRAS CLAVE:

Firma digital, Software, aplicación web, validación.

RESUMEN

En este artículo se presenta el desarrollo de un prototipo de software empleando las tecnologías web más actualizadas capaz de crear, firmar y validar un documento electrónico a partir de un certificado digital y una llave privada. En la aplicación web el usuario remitente podrá realizar un documento con su firma digital y a su vez generar un hash de validación los cuales se enviarán a un destinatario por algún medio. El destinatario podrá verificar la validez de la firma del remitente usando el documento firmado y hash de verificación.

KEYWORDS:

Digital signature, Software, web application, validation.

ABSTRACT

This article presents the development of a software prototype using the most up-to-date web technologies capable of creating, signing and validating an electronic document from a digital certificate and a private key. In the web application the sending user will be able to create a document with its digital signature and at the same time generate a validation hash which will be sent to a recipient by some means. The recipient will be able to verify the validity of the sender's signature using the signed document and verification hash.

Recibido: 18 de agosto del 2020 • Aceptado: 08 de septiembre del 2020 • Publicado en línea: 30 de octubre de 2020

1 INTRODUCCIÓN

En el mundo tecnológico para poder darle validez y legitimidad a un archivo electrónico se recurre a la firma electrónica avanzada o firma digital que es el conjunto de datos electrónicos para identificar al emisor de un mensaje, al igual que la integridad del mismo. Este modelo de firma es creado bajo una serie de medios que están bajo observación directa del firmante, dicho en otras palabras, es una tecnología de infraestructura de clave pública (PKI), que permite intercambiar información y realizar transacciones de manera ágil y sencilla a través de sistemas en línea y el uso de un certificado digital mediante mecanismos que otorgan certeza y seguridad técnica con los mismos efectos jurídicos que una firma autógrafa. [1] El certificado digital también es un documento electrónico que está firmado por una entidad certificadora que acredita la identidad del titular y asocia dicha entidad con un par de claves, una pública y otra privada. La clave privada la posee únicamente su dueño. También se le llama porción privada y junto con la clave pública (porción pública) conforman un par de claves únicas. Por otro lado, la clave pública es publicada en la web por la autoridad certificadora, después de ser aprobada por esta. [2] Para aprobar un certificado digital, la autoridad de certificación firma con su clave privada la clave pública del certificado digital.

Se propone un prototipo de software que permita la firma y validación de documentos electrónicos en el área académica del TecNM campus San Andrés Tuxtla. La autoridad certificadora otorgará el certificado, la llave pública y privada a cada académico, esta podrá ser utilizada para firmar y validar la legitimidad de los mismos. El prototipo consiste en una aplicación web mediante la cual el usuario académico podrá iniciar sesión y generar automáticamente documentos electrónicos firmados digitalmente para un destinatario, o podrá verificar (mediante un hash generado por el remitente) si el documento que recibe está firmado o este ha perdido su firma, es decir, ha sido modificado.

2 ANTECEDENTES

El inicio de la Firma Electrónica en México

"Tu firma" en el año 2004 fue el primer intento por implementar un mecanismo que permitiera identificar al emisor de un mensaje electrónico como autor legítimo como si se tratara de una firma autógrafa por el Sistema de Administración Tributaria (SAT) implementó como un mecanismo alternativo en su inicio y obligatorio para el 2005, después de una serie de reformas al Código Fiscal de la Federación.

Este primer intento por consolidar las transacciones electrónicas alcanzó casi dos millones de contribuyentes registrados que junto con su Clave de Identificación Electrónica Confidencial (CIEC), iniciaron el camino para la posterior puesta en marcha de la Firma Electrónica Avanzada (FEA).

Cabe destacar que, aunque el SAT es la única entidad del Gobierno Federal que generaba estos certificados electrónicos, el Banco de México (BANXICO) comenzó en este mismo periodo con un proyecto para autorizar el funcionamiento de otros "fedatarios" que desde el sector privado pudieran prestar este servicio de certificación electrónica; sin embargo, el proyecto no tuvo el éxito esperado pues el gobierno federal se reservó la labor de emisión de la Firma Electrónica.

La Firma Electrónica Avanzada

La segunda etapa de la firma electrónica se inicia con el cambio de la CIEC por la denominada Firma Electrónica Avanzada, que inicialmente tenía las mismas funciones que la firma electrónica, y que fue creciendo en funcionalidad.

El Gobierno Federal mexicano define la Firma Electrónica Avanzada, en el sitio de internet de la Secretaría de la Función Pública, como se detalla a continuación:

"La Firma Electrónica Avanzada "Fiel" es un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa".

Por sus características, la FIEL brinda seguridad a las transacciones electrónicas de los contribuyentes, con su uso se puede identificar al autor del mensaje y verificar que no haya sido modificado.

Su diseño se basa en estándares internacionales de infraestructura de claves públicas (o PKI por sus siglas en inglés: *Public Key Infrastructure*) en donde se utilizan dos claves o llaves para el envío de mensajes:

- La "llave o clave privada" que únicamente es conocida por el titular de la Fiel, que sirve para cifrar datos; y
- La "llave o clave pública", disponible en Internet para consulta de todos los usuarios de servicios electrónicos, con la que se descifran datos. En términos computacionales es imposible descifrar un mensaje

utilizando una llave que no corresponda [3].

Aunque en México, se exige que la firma electrónica sea autenticada por un certificado digital, este tipo de firma es utilizada principalmente en transacciones específicas requeridas por el gobierno federal, como por ejemplo la Secretaria de Hacienda y Crédito Público. En el caso del TecNM campus San Andrés Tuxtla se utilizará tanto la firma electrónica como el certificado digital para dar más certeza a la documentación.

La Ley de Firma Electrónica Avanzada que fue publicada en enero de 2012, fundamenta su uso y validez en México. Según dicha ley, cualquier documento generado electrónicamente o mensaje de datos, podrá utilizar este tipo de forma electrónica.

Una de las exigencias más importantes de las firmas electrónicas avanzadas es la existencia de un certificado digital. Esta herramienta establece la posibilidad de una transacción entre una clave pública y una clave privada.

En otras palabras, el certificado es un mensaje de datos encriptados que sólo se puede descifrar si tienes las dos claves. Una la tiene el firmante (clave privada) y otra la tiene el certificado (clave pública).

La Firma Electrónica Avanzada en el Gobierno del Distrito Federal

Es en el Gobierno del Distrito Federal en donde la legislación en esta materia es ya una realidad, ya que el gobierno local cuenta ya con una Ley en materia de firma electrónica la cual fue aprobada en el año 2009. En esta Ley se definió a la firma con las características siguientes:

"La firma electrónica avanzada que es generada con un certificado reconocido legalmente a través de un dispositivo seguro de creación de firma y tiene, en relación a la información firmada, un valor jurídico equivalente al de la firma autógrafa" [4].

Esta Ley de firma electrónica del Distrito Federal, aprobada por la Asamblea Legislativa pretende, específicamente, transparentar la función pública y combatir la corrupción en el ámbito del gobierno local.

Este instrumento cuenta con validez jurídica en documentos oficiales, notariales, administrativos o judiciales, así como aquellos que contengan información digital en formato de audio y video.

Asimismo, con esta Ley se reconoce la validez en documentos oficiales emitidos y firmados mediante esta vía por servidores públicos en ejercicio de sus funciones y los emitidos por particulares, entre otros.

De acuerdo con dicha ley, corresponderá a la Secretaría de Desarrollo Económico del Distrito Federal promover y difundir el uso generalizado de este instrumento tecnológico dentro de los procesos de negocios de las empresas establecidas en el esta entidad federativa.

De igual forma, le corresponderá asesorar a los entes públicos para el funcionamiento de los programas que la utilicen, así como la gestión y obtención de los recursos para su habilitación.

¿Por qué el uso de la firma electrónica no ha tenido en México el desarrollo esperado por el avance tecnológico que ha tenido en otros países?

Uno de los factores nodales para explicar estas interrogantes es el grado de accesibilidad de la población que utiliza los servicios tecnológicos y de comunicaciones digitales. En México, el nivel obtenido en la última década en cuanto a la penetración y el uso de los servicios de TIC´s va en continuo crecimiento, sin embargo, aún no se pueden alcanzar los niveles de países como la India, China, Brasil o la CEE [5].

Pero independientemente del nivel de acceso a los servicios de TIC´s, en México el uso de la firma electrónica ha sido un problema esencialmente de confianza y credibilidad más que un tema de utilidad y accesibilidad de los medios tecnológicos. Es un aspecto cultural de respaldo impreso, o de documentación en papel que acredite lo pactado, lo que ha frenado el uso de este mecanismo de autentificación electrónica.

3 METODOLOGÍA

Para lograr el diseño del prototipo se realizaron una serie de pasos que a continuación se describen:

Identificación de los requisitos funcionales y no funcionales

En el área académica del Instituto TecNM campus San Andrés Tuxtla están establecidos una serie de estándares que se deben seguir para la correcta realización de un documento oficial, siguiendo esta serie de pasos se definirán brevemente los principales conceptos.

Requisitos funcionales: hacen referencia a la descripción de las actividades y servicios que un sistema debe proveer. Normalmente este tipo de requerimientos están vinculados con las entradas, las salidas de los procesos y los datos a almacenar en dicho sistema. Los requerimientos funcionales de un sistema describen lo que el software debe hacer. Los cuales dependen de conjunto de características y necesidades que estas demanden.

Requisitos no funcionales: describen otras prestaciones, características y limitaciones que debe tener el sistema para alcanzar el éxito en su desarrollo. Los requerimientos no

funcionales engloban características como el rendimiento, facilidad de uso, presupuestos, tiempo de entrega, documentación, seguridad y auditorías internas.

En base a las necesidades del área académica se identificaron los siguientes requisitos

Funcionales:

- Generar un documento y firmarlo mediante certificados digitales.
- Verificar la legitimidad del documento y a su vez identificar si este ha sido modificado.
- Capacidad para realizar el contenido desde cualquier dispositivo tecnológico.

No funcionales:

- Utilizar el lenguaje de programación PHP.
- Manejo de librerías de PHP para agilizar el tiempo de programación.
- Uso de frameworks de HTML.
- Manejo de OpenSSL para el tratamiento de certificados digitales.

Modelado

Implementando los requisitos funcionales se desarrollaron diversos diagramas basados en el estándar UML (Lenguaje Unificado de Modelado) para la mejor administración del prototipo de software, generando diagramas de caso de uso, clase, secuencia y estado.

El diagrama de caso de uso, véase figura1, muestra que el usuario al ingresar al sistema podrá tener tanto la función de remitente como destinatario. Por lo que podrá generar y firmar un documento o validar su autenticidad.

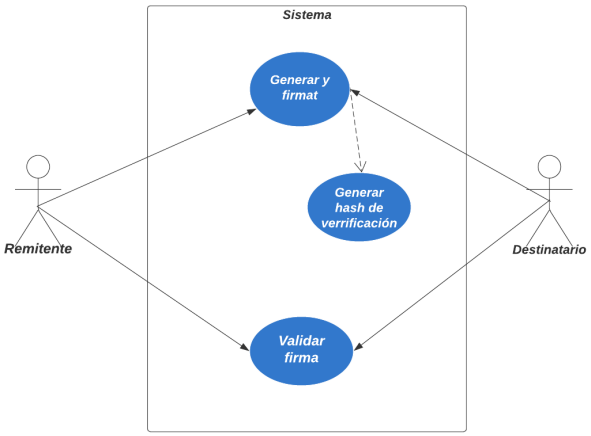

Figura 1 Diagrama de caso de uso

Los diagramas de secuencia, figura 2 y 3, permiten visualizar que el remitente dentro del mismo prototipo podrá generar el documento y firmarlo mediante su llave privada, de esta forma obtendrá el documento firmado electrónicamente, de igual manera generará el hash de verificación. Esto permitirá hacer el envío del documento al destinario que se requiera.

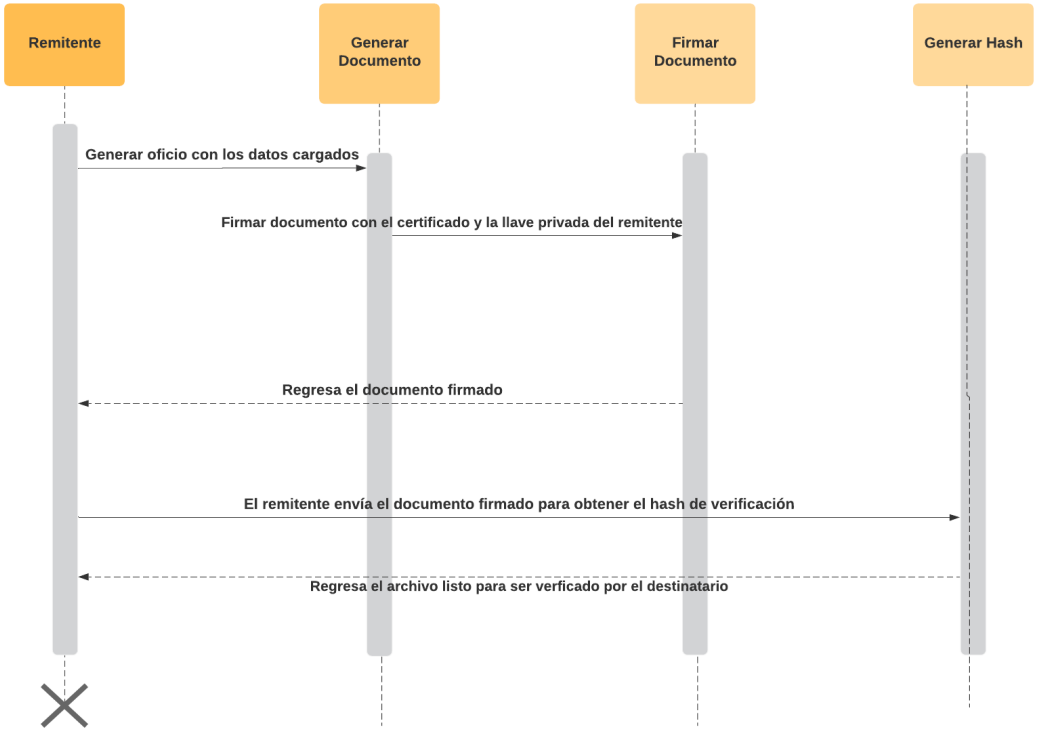

Figura 2 Diagrama Secuencia Remitente

El destinatario, podrá realizar la verificación del documento en el prototipo y este indicará si es válido o no.

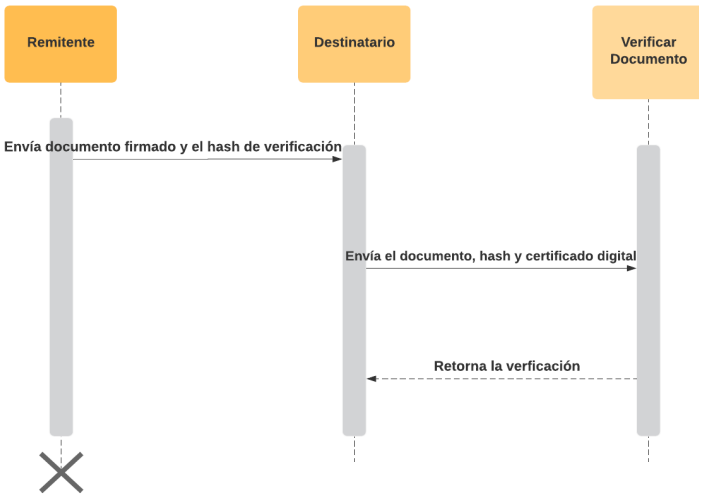

Figura 3 Diagrama Secuencia Destinatario

Diseño del sistema

Esta etapa permite definir el aspecto que tendrá el prototipo y en su caso realizar las modificaciones pertinentes, permitiendo generar una idea clara del diseño antes de construirlo.

4 DESARROLLO Y PRUEBAS

Tecnología empleada

Para el desarrollo del prototipo el uso de tecnología empleada se puede dividir en 2 partes, el lado del servidor, XAMPP el cual incluye PHP, Apache, MariaDB, Perl, OpenSSL y PhpMyAdmin. [6]

Se requirió el uso de librerías de PHP, que permitieron agilizar el proceso de desarrollo, específicamente se implementaron las siguientes tecnologías escritas en el lenguaje PHP:

- TCPDF: Para el tratamiento del PDF y firma digital mediante certificados digitales [7].
- PHPQRCORDE: Para generar códigos QR [8].

En lo que se refiere al lado del cliente se empleó Bootstrap: la cual contiene las siguientes tecnologías web HTML5, CSS y JQUERY [9].

Adicionalmente se utilizó AJAX para hacer validaciones del lado del cliente, esto ayuda mucho a que las peticiones al servidor sean únicamente para generar y firmar el documento electrónico siendo así, una aplicación web más rápida y robusta.

Pruebas

La aplicación fue probada bajo las características señaladas por el estándar ISO-9126 [10], ya que se considera

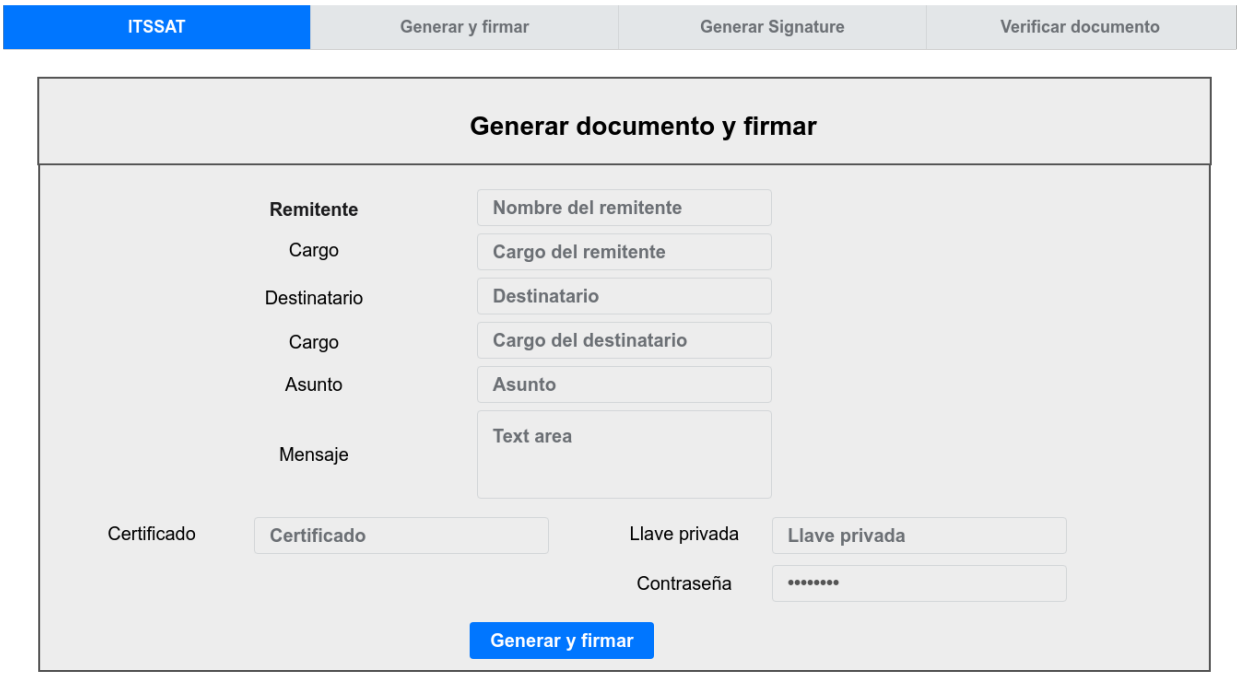

Figura 4 Diseño de la pantalla Generar y firmar

una base útil para realizar mediciones y ofrece una lista de comprobación que permite evaluar la calidad del sistema, los atributos considerados a cumplir por esta aplicación son:

Funcionalidad: permitió verificar que la aplicación cumpliera los requisitos del cliente.

Usabilidad: para cada categoría de usuario, se validó que la aplicación tenga la capacidad de ser comprendida, usada y atractiva para el usuario.

Portabilidad: se validó que la aplicación funcionara correctamente en distintos navegadores y dispositivos.

5 RESULTADOS Y DISCUSIÓN

Basado tanto en los diagramas generados como en el maquetado, se desarrolló el prototipo para firma y validación de documentos electrónicos. El ingreso al sistema se realizara desde la siguiente dirección 194.168.1.149/esigna/ en la cual, el usuario deberá autenticarse como administrador o académico, para poder ingresar al sistema.

Figura 5 Inicio de sesión.

En la sección administrador el usuario con estos privilegios podrá crear y eliminar usuarios de manera rápida:

Figura 6. CFDI impreso

Así mismo, podrá personalizar la plantilla del documento oficial cada vez que se instruya el uso de un nuevo formato, esto se logra modificando los elementos de la plantilla PDF.

Figura 7 Modificación de la plantilla pdf.

El usuario común podrá generar un documento, generar el hash de verificación y posteriormente validar la firma de dicho documento:

Muestra del documento generado y firmado electrónicamente.

6 TRABAJO A FUTURO

La sección Modificar Plantilla, es una mejora que se encuentra en desarrollo, pues ante las constantes variaciones que se tienen de los formatos y logotipos autorizados por las diversas instituciones educativas que rigen a los Tecnológicos, es difícil definir un tipo de documento estándar para el sistema. Es por esto que se trabaja en el desarrollo del módulo en mención de tal manera que cuando se realice un cambio el sistema permita personalizarlo y seguir brindando un funcionamiento óptimo.

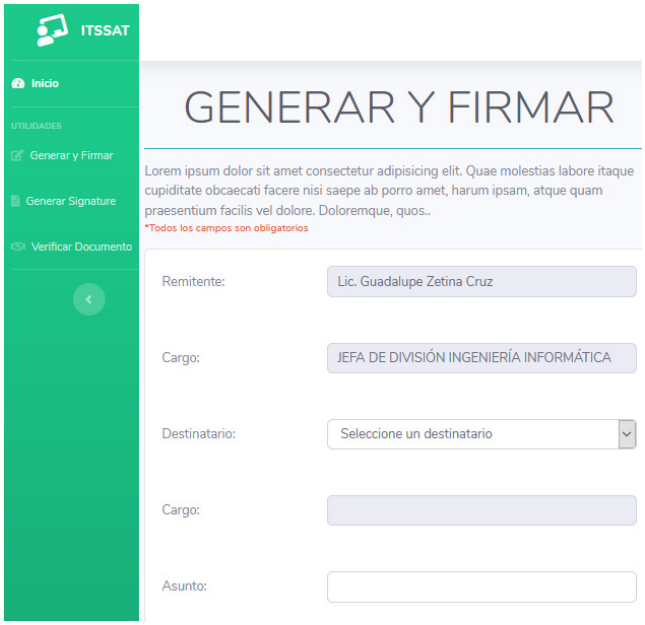

Figura 8 Funciones de un usuario común

7 CONCLUSIONES

El prototipo de software, desarrollado en ambiente web, ayudará a que cada documento generado por el TecNm campus San Andrés Tuxtla pueda ir debidamente firmado y al mismo tiempo se garantiza que dicho documento podrá ser validado o verificado por un destinatario.

Considerando los resultados obtenidos y las actividades desarrolladas el prototipo podrá brindar a los académicos una forma amigable a la hora de gestionar documentos digitales ya que, encontrándose en las últimas etapas de desarrollo, este es capaz de agilizar la elaboración de un oficio y firmarlo de manera automática Aligerando el tiempo empleado en la generación de estos.

Figura 9 Documento generado y firmado

Es importante resaltar que el prototipo es totalmente responsivo, sin embargo, es aconsejable emplearlo usando un ordenador para el proceso de generación y firma del documento ya que el certificado digital de cada académico está instalado de manera directa por la autoridad certificadora [11].

Un aspecto importante a destacar de la aplicación es que deriva del proyecto financiado por TecNm GED, siendo esta una fase que requiere de la generación previa de certificados emitidos por una autoridad certificadora anteriormente configurada, y que en su totalidad forman un sistema que puede ser replicable en cualquier otra institución que requiera una gestión adecuada de documentos digitales.

AGRADECIMIENTOS

Agradezco al área académica del TecNM campus San Andrés Tuxtla, en especial a la división de Ingeniería informática por brindar todas las facilidades para que el prototipo se desarrollara y realizar las pruebas necesarias en esa área.

REFERENCIAS

1. L. A. B. Zúñiga, Evolución de la firma autógrafa a la Firma Electrónica Avanzada., 2011.
2. A. d. S. S. d. l. Reyes, «http://www.ssreyes.org,» [En línea]. Available: http://www.ssreyes.org/es/portal.do?TR=C&IDR=759. [Último acceso: 27 Agosto 2019].
3. S. d. l. F. Pública, «Secretaría de la Función Pública,» Gobierno de México, 09 12 2013. [En línea]. Available: https://www.gob.mx/sfp/documentos/firma-electronica-avanzada-fiel. [Último acceso: 19 04 2019].
4. A. L. D. D. FEDERAL, «Asamblea Legislativa del Distrito Federal,» 04 11 2009. [En línea]. Available: http://aldf.gob.mx/archivo-8a9f98083f8b38fb40fb3cef1b2bf9ce.pdf. [Último acceso: 16 01 2019].
5. I. M. Soumitra Dutta, «The Global Information Technology Report 2010–2011,» World Economic Forum and INSEAD, Geneva, 2011.
6. A. Friends, «Apache Friends,» Xampp, [En línea]. Available: https://www.apachefriends.org/. [Último acceso: 12 Noviembre 2019].
7. TCPDF, «TCPDF,» [En línea]. Available: https://tcpdf.org/. [Último acceso: 09 Enero 2020].
8. K. Fukuchi, «PHP Qr Code,» [En línea]. Available: http://phpqrcode.sourceforge.net/. [Último acceso: 10 Diciembre 2019].
9. Bootstrap, «Bootstrap,» [En línea]. Available: https://getbootstrap.com/. [Último acceso: 18 Noviembre 2019].
10. R. S. Pressman, Ingeniería de Software, Un enfoque practico, México: McGraw-Hill, 2010.
11. Y. A. P. Santiago, «Implementación de un esquema para autenticación y validación de documentos electrónicos mediante una autoridad certificadora,» San Andrés

Acerca de los autores

Juan Rafael González Cadena. Licenciado en Informática. Maestro en Tecnologías de Información por la Universidad Cristóbal Colon. Perfil Deseable de PRODEP desde 2013, certificaciones: Oracle PL/SQL Developer Certified Associate por ORACLE Corporation y Basic Level Programmer en ROBOTC otorgado por Carnegie Mellon Robotics Academy. Miembro Colaborador del Comité de Investigación del Instituto Tecnológico Superior de San Andrés Tuxtla, miembro del Cuerpo Académico "Tecnologías de Información y desarrollo de software", evaluador de Perfil Deseable de PRODEP, miembro del Consejo de Posgrado del Instituto Tecnológico Superior de San Andrés Tuxtla . Ha publicado varios artículos en el área de Tecnologías de Información y Comunicaciones en diferentes revistas, ha participado como ponente y organizador en eventos académicos nacionales.

Rogelio Enrique Telona Torres, Licenciado en Informática. Maestro en Tecnologías de Información por la Universidad Cristóbal Colon. Perfil Deseable de PRODEP desde 2013, certificaciones: Certified LabVIEW Associate Developer por National Instrumentsy Basic Level Programmer en ROBOTC otorgado por Carnegie Mellon Robotics Academy. Miembro Colaborador del Comité de Investigación del Instituto Tecnológico Superior de San Andrés Tuxtla, miembro del Cuerpo Académico "Tecnologías de Información y desarrollo de software", evaluador de Perfil Deseable de PRODEP, miembro del Consejo de Posgrado del Instituto Tecnológico Superior de San Andrés Tuxtla. Ha publicado varios artículos en el área de Tecnologías de Información y Comunicaciones en diferentes revistas, ha participado como ponente y organizador en eventos académicos nacionales.

Erick Manuel Ramírez Casanova. Egresado de la carrera de Ingeniería Informática con especialidad en Tecnologías de la Información y Comunicaciones en el Instituto Tecnológico Superior de San Andrés Tuxtla. Ha participado en varios proyectos de investigación y en el desarrollo de software open source bajo la licencia GPLV3, así como ganador del primero y segundo lugar del concurso de programación en su fase regional y estatal en el 2018 y 2019.