Esquema para autenticación y validación de documentos electrónicos mediante una autoridad certificadora

Scheme for authentication and validation of electronic documents through a certification authority

Yair Alejandro Ponciano Santiago [1], Rogelio Enrique Telona Torres[2], Juan Rafael González Cadena2*,
1Ingeniería Informática(estudiante), TecNM campus San Andrés Tuxtla, Carretera Costera del Golfo Km 140+100, Matacapan, San Andrés Tuxtla, Veracruz, México, C.P. 95804
2División de Ingeniería Informática, TecNM campus San Andrés Tuxtla, Carretera Costera del Golfo Km 140+100, Matacapan, San Andrés Tuxtla, Veracruz, México, C.P. 95804
*jrgcadena@hotmail.com

Yair Alejandro Ponciano Santiago yair2764@gmail.com
Rogelio Enrique Telona Torres retelona19@hotmail.com
Juan Rafael González Cadena jrgcadena@hotmail.com

Área de participación: *Tecnologías de Información*

PALABRAS CLAVE:

Documento electrónico, autoridad certificadora, certificado digital.

RESUMEN

Hoy en día los medios digitales son susceptibles de substitución, modificación, y replicación, a menos que estén explícitamente protegidos con el objetivo de que se pueda confiar en este medio de comunicación.
En este contexto en el TecNM campus San Andrés Tuxtla es necesario la implementación de un esquema para la validación y autenticación de documentos con la finalidad de: a) la disminución del consumo del papel, b) agilizar el proceso para emisión-recepción y c) la autenticidad de los documentos creados.
El presente trabajo describe cómo implementar una Autoridad Certificadora que permite crear y controlar los certificados emitidos por la misma, así como la firma de los documentos del instituto.

KEYWORDS:

electronic document, certifying authority, digital certificate.

ABSTRACT

Today's digital media are susceptible to substitution, modification, and replication, unless they are explicitly protected in order to be trusted.
In this context, at the TecNM campus San Andrés Tuxtla, it is necessary to implement a scheme for the validation and authentication of documents in order to: a) reduce paper consumption, b) speed up the process for emission-reception, and c) ensure the authenticity of the documents created.
This paper describes how to implement a Certification Authority that allows the creation and control of the certificates issued by it, as well as the signing of the institute's documents.

Recibido: 12 de julio de 2021 • **Aceptado:** 11 de septiembre de 2021 • **Publicado en línea:** 15 de febrero de 2022

1 INTRODUCCIÓN

Con la evolución de las nuevas tecnologías de la información a la que nos enfrentamos día con día estamos expuesto al continuo crecimiento por parte de la expedición de documentos válidos, Derivado de esto, surge la necesidad de desarrollar una autoridad certificadora propia, que permita una gestión adecuada de documentos que faciliten verificar la seguridad y legitimidad de los derechos de autoría. Evitando la falsificación de los documentos emitidos.
De esta manera el instituto estará tomando un rumbo adecuado en su búsqueda por aumentar la calidad de sus procesos y procedimientos con el fin de lograr mejores rendimientos.

La diversidad de documentos que se generan y pasan de escritorio en escritorio en cada departamento de división de las carreras, es continuo. Por tan sencillo que esto parezca se debe mantener control de los documentos, así como la disposición del uso de estos dentro y fuera de la institución, además, el instituto cuenta con la certificación ISO 14001:2015 (Sistema de Gestión Ambiental), por lo cual este proyecto se sumaría a la estrategia "Cero Papel" la cual busca reducir costos y eficiencia en tiempos, además, contribuye a borrar la "huella medioambiental", con la reducción del uso de papel y otros recursos que producen contaminantes.

Por lo anterior, se tomó la decisión de definir un esquema para la emisión de certificados digitales teniendo como objetivo contar con una Autoridad Certificadora mediante la cual se pueda expedir certificados y mantener la información del estado de esta.

Para ello fue necesario la instalación de herramientas *open-source* la cual permite la creación de la autoridad certificadora, y esta a su vez la emisión de certificados digitales que permitan firmar los documentos emitidos en el área académica de la institución donde se realizaron las pruebas.

2 ESTADO DEL ARTE

La creación de una Autoridad Certificadora que emita certificados digitales en México está regida por la Ley de Firma Electrónica Avanzada en sus Artículos 23 y 24:

*"**Artículo 23**. La Secretaría, la Secretaría de Economía y el Servicio de Administración Tributaria son consideradas autoridades certificadoras para emitir certificados digitales en términos de esta Ley.*

***Artículo 24**. Las dependencias y entidades, distintas a las mencionadas en el artículo anterior, así como los prestadores de servicios de certificación que estén interesados en tener el carácter de autoridad certificadora en términos de la presente Ley, deberán:*

> *I. Contar con el dictamen favorable de la Secretaría, y*
>
> *II. Cumplir con los demás requisitos que se establezcan en las disposiciones generales que se emitan en los términos de esta Ley.*

Adicionalmente, los notarios y corredores públicos y las personas morales de carácter privado deberán presentar el documento emitido por la Secretaría de Economía que los acredite como prestadores de servicios de certificación, en virtud de haber cumplido con los requisitos establecidos en el Código de Comercio y su Reglamento" [1].

En este orden de ideas, hay que entender que, por esa razón, en todos los ordenamientos en comento, se define también los datos y dispositivos de creación y verificación de firma; así como los conceptos relacionados con la prestación de servicios de certificación; existentes sólo en el caso de que se trate de una firma de claves asimétricas. Señala el código de comercio:

- *Datos de Creación de Firma Electrónica:* son los datos únicos, como códigos o claves criptográficas privadas, que el Firmante genera de manera secreta y utiliza para crear su Firma Electrónica, a fin de lograr el vínculo entre dicha Firma Electrónica y el Firmante.
- *Prestador de Servicios de Certificación:* la persona o institución pública que preste servicios relacionados con Firmas Electrónicas y que expide los Certificados, en su caso. Conforme al código de comercio pueden ser prestadores de servicios de certificación los notarios públicos y corredores públicos; las personas morales de carácter privado, y las instituciones públicas, conforme a las leyes que les son aplicables.

De acuerdo al código fiscal de la federación es el S.A.T. para personas jurídicas y el Banco de México, para personas físicas. En Guanajuato la secretaría de finanzas y administración, el poder legislativo; el poder judicial; los organismos autónomos; y los ayuntamientos. En Jalisco Hidalgo los notarios públicos, las personas físicas y jurídicas habilitadas para tal efecto; y las entidades públicas federales, estatales o municipales. En Sonora no se señala expresamente sólo habla de la dependencia, unidad administrativa u órgano designado por cada ente público sujeto a la ley (poder ejecutivo, legislativo, judicial, organismos constitucional o legalmente autónomos y ayuntamientos). En Chiapas los agentes certificadores designados por la secretaría de administración. La facultad de expedir certificados no conlleva fe pública por sí misma, así los notarios y corredores públicos podrán llevar a cabo certificaciones que impliquen o no la fe pública, en documentos en papel, archivos electrónicos, o en cualquier otro medio o sustancia en el que pueda incluirse información. [2]

Debido a que el costo del servicio que brindan las Autoridades Certificadoras es alto y la acreditación como prestador de servicios de certificación para la emisión de certificados digitales por parte de la Secretaria de Economía tiene un costo de $258,028.00 [3], y que el uso de los certificados y firmas digitales solo serán de uso interno en el Instituto, se optó por implementar una Autoridad Certificadora utilizando herramientas informáticas de software libre (*open source*).

Tomando como referencia algunos trabajos realizados anteriormente, a continuación de enlistan:

Implementación De Firma Digital En Una Plataforma De Comercio Electrónico [4]

Autor: Walter Augusto García Rojas

Ciudad: Lima, Perú, 2008

Objetivo: El objetivo de la tesis fue desarrollar un esquema de Firma Digital para una plataforma Web de comercio electrónico haciendo uso de la infraestructura adecuada que permita firmar documentos y contratos con cien por ciento de valor legal y que sean cien por ciento confiables.

Resultados: Módulo de obtención de datos a partir de documentos firmados. Esquema de firma de documentos electrónicos en PDF. Esquema de firma de contratos en PDF. Validación de firmas digitales en documentos PDF. Inclusión del sello de tiempo en la firma de documentos y contratos.

Conclusión: La obtención de datos de la firma digital incrustada en los documentos PDF se ha aplicado sólo para documentos que se firman con la plataforma en el proceso de registro o modificación de datos en el mismo momento que esto ocurre, descartándose la posibilidad de obtener los datos de un documento ya firmado con cualquier otra herramienta, ya que no existe la certeza de que corresponda con la persona que realiza el registro o modificación de los datos.

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.

Modelo De Implementación De Mecanismos De Firma Digital [5]

Autor: Patricia Víquez Víquez, Marlis Montes Morales

Ciudad: Heredia, Costa Rica, 2013

Objetivo: Crear un modelo para el adecuado desarrollo de soluciones de software con mecanismos de firma digital, con el fin de mejorar el conocimiento y potenciar el desarrollo de nuevas implementaciones en el país.

Resultados: Se generó un modelo de implementación de mecanismos de firma digital, el cual incluye una guía interactiva que indica los pasos técnicos y legales que deben considerarse para el proceso de implementación de la firma digital, así como los flujos de los procesos de la firma digital, con el fin de que los usuarios y las organizaciones puedan entenderlo de forma más clara.

Conclusión: A través de la investigación, se documentaron las mejores prácticas de diversos países con respecto al funcionamiento y la implementación de los mecanismos de firma digital [5].

El modelo propuesto de implementación de mecanismos de firma digital contempla aspectos técnicos y legales en un mismo documento, y de esta manera, permite guiar tanto a los usuarios como a las organizaciones en la implementación de la firma digital. De acuerdo con la investigación

realizada no se encontró ningún modelo similar en otros países [5].

3 METODOLOGÍA

La investigación surge del estudio sobre la situación actual del firmado de documentos electrónicos en el TecNM campus San Andrés Tuxtla con el fin de conocer las formas en que se realiza este proceso administrativo. Además de la indagación de funcionalidad y operatividad de los procesos, así como en el aspecto jurídico.

En este trabajo la selección de la población se consideró únicamente el Área Académica del instituto.
Se empleó un muestreo por conveniencia, considerando a los jefes de cada carrera y al encargado de la maestría de la institución para su estudio, la cual consta de 9 personas.

La metodología aplicada fue la del método *GRAY WATCH* [6] la cual tiene como objetivo describir los procesos técnicos, de gestión y de soporte que deben de emplear los equipos de trabajo para desarrollo.

Etapa I Estudio del Negocio.
En esta etapa se llevó a cabo las primeras fases de la metodología (Fase I, Gestión y Fase II Soporte) la cual está enfocada en los procesos realizados durante toda la investigación, asegurando de la calidad del producto. Se realizó un estudio sobre el manejo de la firma electrónico.

De la misma forma se realizó la investigación de las instituciones que se encuentran en uso de esta herramienta (firma electrónica), además de los beneficios que esta le trae al ser incorporadas en sus operaciones administrativas.

Etapa II Requisitos del Modelo.
Etapa donde se desarrolló la tercera fase de la metodología (Análisis), lo primero que se realizo fue definir las funciones y procesos que involucra el generar la firma, así como los componentes necesarios para generar el modelo.

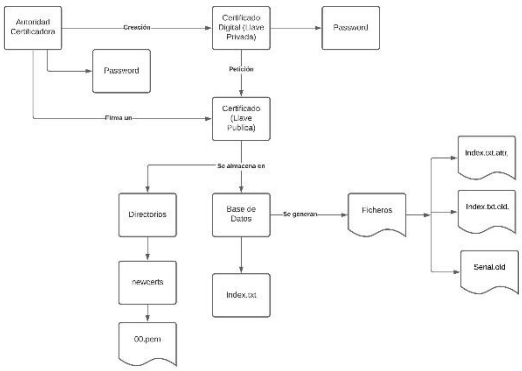

Figura 1 firmado de Certificados

Etapa III Diseño del Modelo
Esta fase permitió completar la tercera fase, donde fueron definidos e integrados los componentes y procesos que fueron necesarios para realizar la configuración de la autoridad certificadora.

Elementos del documento firmado
Los documentos firmados digitalmente constan de 4 elementos en la firma, seleccionados para garantizar la autenticidad del documento. Estos elementos son:

Cadena original:

Es la secuencia de datos formada con la información contenida dentro del documento electrónico.
La secuencia de formación está conformada por los siguientes datos y en el orden en que estas se encuentran:

- Código del documento.
- Sello digital.
- Fecha de emisión del documento.

Toda cadena original es sellada digitalmente, para eso se aplica el algoritmo de encriptación de base de 64 y está compuesto por:

- Folio del documento.
- Propietario del certificado emisor.
- Propietario del certificado receptor.

Sello digital

Toda cadena original es sellada digitalmente, para eso se aplica el algoritmo de encriptación de base de 64 y está compuesto por:

- Folio del documento.
- Propietario del certificado emisor.

- Propietario del certificado receptor.

Sello institucional

Es la secuencia de caracteres que identifica a la institución donde se emiten los certificados y está compuesta por:

- Propietario del certificado de la autoridad certificadora.

Código QR

Código de barras bidimensional que contiene información encriptado en una serie de cuadros y que es decodificada por un lector de códigos QR y contiene:

- Sello digital.

Requerimientos de *hardware y software*:
Servidor Linux (Centos 7), Apache, y OpenSSL

4 RESULTADO Y DISCUSIÓN

Configuración de la autoridad certificadora
Para la configuración de la autoridad certificadora en el servidor es necesario tener creados los siguientes directorios: *certs, csr, crl, newcerts, private*. A demás de tener los siguientes ficheros con el nombre de serial, *crlnumber* y por último un archivo de texto *index*.txt.

A continuación, se describe cada uno de los directorios y archivos.

- *newcerts*: directorio para contener los nuevos certificados emitidos.
- *private*: directorio que contiene el fichero *cakey.key*.
- *serial:* fichero que contiene el número de serie de certificados.
- *crlnumber*: fichero que contiene el número de serie de certificados revocados.
- *certs*: directorio para contener certificados.
- *csr*: directorio para contener los archivos de solicitud de certificados.
- *crl:* directorio para contener certificados revocados.
- *index.txt:* fichero con el índice de certificados firmados.

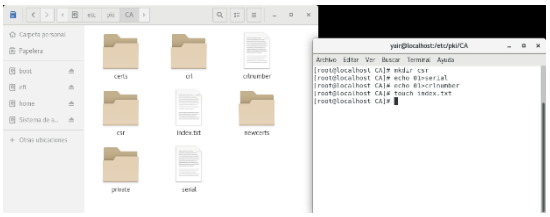

Figura 2 Creación de los directorios y ficheros de la AC

Creación de la autoridad certificadora [7]

Para la creación de una Autoridad Certificadora se debe crear una llave privada y un certificado firmado por la misma llave. Una Autoridad Certificadora firma cada uno de los certificados que son generados y asignados a los diversos departamentos o usuarios que conforman una empresa, estos certificados son firmados por la misma autoridad y hacen que tengan una validez mientras estos no expiren o sean revocados.

Comando para la creación de la autoridad certificadora.

openssl req -config openssl.cnf -new -x509 -extensions v3_ca -keyout private/ca.key -out certs/ca.crt -days 3650
Password: ********

Para este ejemplo, el certificado durara 10 años, y una vez que expire el certificado raíz todos los certificados firmados por la Autoridad Certificadora Raíz no serán válidos.

Creación de certificados digitales (Jefe de la División Ingeniería en Informática) [8]

Lo primero es generar la llave privada del certificado, la cual servirá para descifrar el contenido del certificado a generar [9].

openssl genrsa -des3 -out private/Zetina.key 1024
password: ********

Se debe realizar la petición del certificado usando la llave que se ha creado anteriormente.

openssl req -new -key private/Zetina.key -out csr/Zetina.csr [10]
Password: ********

Petición de un certificado usando la llave de la misma.

En la generación de la solicitud del certificado se especifica la llave con la cual está asociada, así como el nombre de la solicitud, si solo se desea ocupar por un determinado tiempo de vida del certificado solo es necesario agregar el comando –*days* seguido del número de días, debido a que el certificado tiene un determinado número de días que por default este se genera que es de 365.

La solicitud consta de datos importantes que corresponden al solicitante; el código del país al que pertenece, el nombre del estado, la ciudad a la que pertenece, el nombre de la compañía u organización, el nombre del departamento o área que solicita el certificado, el nombre del servidor si es que se cuenta disponible una red o bien el nombre del encargado del departamento o área y un correo electrónico de ese mismo departamento.

Firmado de una solicitud de un certificado

Por último, la Autoridad Certificadora debe firmar la solicitud realizada por algún cliente que requiere de un certificado digital para su correspondiente firmado de documentos.

openssl ca -config openssl.cnf -in csr/Zetina.csr

En este paso pedirá la contraseña que se asignó a la autoridad certificadora *ca.key*

Para el firmado de la solicitud únicamente es usado el archivo de solicitud y se accede al archivo de configuración de *OpenSSL* ya que en él se encuentran guardados la ubicación y el nombre tanto de la llave privada como del certificado de la Autoridad Certificadora. Al preguntar si se desea firmar la respuesta debe ser sí.

A manera de corroborar que el certificado ha sido creado es necesario ingresar al directorio *newcerts*, en ella se encuentra el archivo con el número de serial y la extensión. pem.

Se almacenan los certificados en una base de datos, para comprobar que se ha creado es necesario revisar el archivo index.txt en él se muestran los datos de todos los certificados que se han creado especificando si es aún es válido, expirado o revocado.

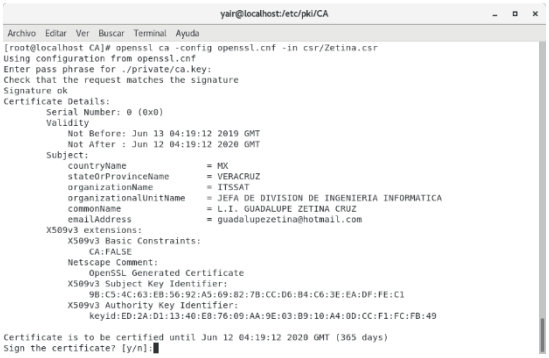

Figura 3 Firmado de una solicitud de certificado

Los certificados que recién han sido generados estos deberán ser enviados a sus usuarios que harán uso de ellos, para ello se entrega la llave privada y su correspondiente certificado. Los certificados deberán ser renombrados con nombre fácil de identificar al igual que los directorios en que se guardan, además de cambiar al formato .crt ya que es la extensión más usada en la mayoría de los navegadores cuando se requiere la instalación del certificado.

Instalación de los certificados digitales

Para realizar el sellado electrónico es necesaria la instalación del certificado digital en el equipo de cómputo del encargado de emitir los documentos. El certificado emitido es recomendable instalarlo en formato p12, ya que él contiene tanto la llave privada con la que se firman los documentos como la llave pública con la cual firma los datos del certificado.

Generar el sello de la institución.

Para que un área o departamento pueda emitir un documento firmado digitalmente, la Autoridad Certificadora debe generar los sellos según el número de peticiones que solicite la entidad emisora.

Un documento digital firmado debe contener una cadena original, un sello digital, y el sello de la institución. La cadena original se compone del código del documento, el sello digital y la fecha de emisión del documento.

El sello digital está compuesto por el número de folio de cada documento, el cual es asignado por la misma Autoridad Certificadora, los datos del emisor y los datos del receptor. El sello de la institución se conforma de los datos propios de la Autoridad Certificadora.

Una vez que el archivo SelloITSSAT cuenta con la información, se aplica un método de encriptación basado en md5, este permite cifrar la información a código binario, al finalizar este genera un archivo de texto distinto con el código generado.

openssl dgst -md5 -sign private/ca.key -out firmas/SelloITSSATmd5.txt firmas/SelloITSSAT.txt

Para mejorar la seguridad de la información que se va a presentar en los documentos firmados, al archivo encriptado con md5 se le aplica otro método de cifrado como lo es base64.

Para este proceso se requiere del archivo de texto que contiene el cifrado md5 así como el archivo de texto de salida que contiene el cifrado final en formato base64.

openssl base64 -in firmas/SelloITSSATmd5.txt -out firmas/Sello64ITSSAT.txt

Generar el sello digital y la cadena original.

Para crear un sello digital se tiene que realizar la consulta de los propietarios tanto de emisor como de receptor y copiarlos dentro de un archivo de texto anexando el número de folio asignado por la misma Autoridad Certificadora.

openssl x509 -in certs/Zetina.crt -noout -subject
openssl x509 -in certs/Telona.crt -noout –subject

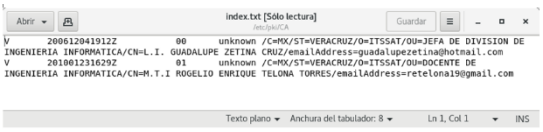

Figura 4 BD certificados generados

Mediante la implementación de la Autoridad Certificadora, todos los documentos generados se firmarán digitalmente, esto se logra en base a una aplicación web denominada eSigna desarrollada específicamente para esta actividad. La aplicación permite crear un documento, firmarlo y validarlo, esto trae consigo diversas ventajas entre las que destaca tener la certeza total de la autoría del documento. A continuación, se muestra el resultado de la combinación de los certificados generados por la AC y la aplicación eSigna.

Figura 5 Documento generado y firmado

Esto permitirá la disminución de papel en las diferentes divisiones del área académica del instituto, a su vez el almacenamiento de los documentos se hará de manera digital, logrando así agilizar este proceso.

Con la implementación de la Autoridad Certificadora se logró:

- Reducir el tiempo empleado en el proceso de emisión-recepción de los documentos.
- Asignar a cada jefe de carrera un certificado con el cual firmaran los documentos.
- Digitalización de los archivos generados.
- Agilizar el proceso de firma de los documentos, los cuales consumían tiempo para la firma y digitalización de la misma, sobre todo cuando era necesario realizar modificaciones por cuestiones de errores o simplemente por cambios, estos requerían reimpresión y digitalización de los archivos.

Uno de los beneficios que la puesta en marcha de la AC en combinación con la aplicación eSigna [11], será la disminución de papel que se genera en

las diferentes divisiones del Área Académica del instituto.

5 TRABAJOS A FUTURO

A partir de la implementación de la Autoridad Certificadora dentro de las instalaciones del instituto, en específico el Área Académica, se plantea expandir a toda la institución el uso de la firma de documentos mediante Certificados digitales. A la par de este proyecto se ha desarrollado un prototipo de Aplicación web que ayudará a gestionar la emisión, firma y validación de documentos electrónicos.

6 CONCLUSIONES

Con la implementación de la Autoridad Certificadora en el instituto, todos aquellos documentos que sean generados serán firmados de manera digital, garantizado la validez del mismo, esto permitirá un flujo adecuado de los documentos digitales creados por las diferentes áreas, además de todo esto traerá consigo mismo un impacto muy importante a nivel ambiental.

A continuación, se describen una estimación basada en el consumo de papel realizada únicamente por los docentes.

Número de docentes	Paquetes de hojas semestral (por docente)	Contenido de hojas por paquete	Hojas consumidas al semestre por los docentes	Hojas consumidas al año por los docentes
91	1	500	45500	91000

Un árbol con una edad entre 30 y 40 años produce alrededor de 20 kilos de papel, aunque no todo es de buena calidad [12], en promedio un paquete hojas pesa 2.5 kilos, en el instituto se consumen aproximadamente, 182 paquetes de hojas al año, lo que hace un total 455 kilos lo que equivale a 22 árboles en promedio por año (455/20). Además, consideremos que cerca del 40% de toda la madera tallada para usos industriales en el mundo se destina a la producción de papel [13] .

Para que un árbol se considere apropiado para su explotación debe de crecer durante 30 años, durante ese periodo se habrán consumido las hojas producidas por 660 árboles (22x33). Considerando que en una hectárea se siembran un aproximado entre 350 y 400, siendo esto equivalente a la desforestación de aproximadamente 2 hectáreas.

Fabricar mil kilos de papel blanco implica un consumo de 100,000 litros de agua. De ellos, un 10% altamente contaminado se vierte a los ríos. Ya que la alta toxicidad de sus métodos industriales se debe, fundamentalmente, al proceso de blanqueo con Cloro [14].

Además, hay que agregar el alto consumo de consumibles de impresión.

REFERENCIAS

[1] I. M. d. P. Industrial, «Portal de Acceso a Servicios Electrónicos,» 11 Enero 2012. [En línea]. Available: https://eservicios.impi.gob.mx/seimpi/ayudaSEIMPI/LFEA.pdf. [Último acceso: 27 Septiembre 2019].

[2] D. A. G. Ávalos, «https://dialnet.unirioja.es/,» 2010. [En línea]. Available: https://dialnet.unirioja.es/descarga/articulo/3438233.pdf. [Último acceso: 14 Enero 2020].

[3] S. d. Economía, «Gobierno de México,» Gobierno de México, 06 Junio 2017. [En línea]. Available: https://www.gob.mx/tramites/ficha/acreditacion-como-prestador-de-servicios-de-certificacion-en-la-emision-de-certificados-digitales-de-firma-electronica-avanzada/SE2402. [Último acceso: 14 Enero 2020].

[4] W. A. G. Rojas, «IMPLEMENTACIÓN DE FIRMA DIGITAL EN UNA,» Tesis PUCP, Lima, Peru, 2008.

[5] P. V. V. y. M. M. Morales, «Modelo de implementación de mecanismos de firma digital,» Universidad Nacional, Heredia, Costa Rica, 2013.

[6] J. . C. Montilva, J. . A. Barrios y M. Riv, «GRAY WATCH METODO DE DESARROLLO DE SOFTWARE PARA APLICACIONES EMPRESARIALES,» NOVIEMBRE 2008. [En línea]. Available: https://luiscastellanos.files.wordpress.com/2016/04/gray-watch.pdf. [Último acceso: 17 ABRIL 2020].

[7] M. A. Jiménez, «OpenSSL (Parte 2). Creación de una Autoridad Certificadora Raíz, 'rootCA'.,» LinuxArena , 6 ENERO 2007. [En línea]. Available: https://www.linuxarena.net/2017/01/06/openssl-parte-2-creacion-de-una-autoridad-certificadora/. [Último acceso: 15 ABRIL 2020].

[8] J. Orovengua, «Configuración OpenSSL y creación de Certificados digitales,» 01 Junio 2018. [En línea]. Available: https://www.linuxparty.es/57-seguridad/9626-configuracion-openssl-y-creacion-de-certificados-digitales. [Último acceso: 17 Abril 2020].

[9] E. V. B. Esteban, «Creación y administración de certificados de seguridad,» [En línea]. Available: http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/Certificados.pdf. [Último acceso: 15 abril 2020].

[10] J. Gamarra, «CÓMO CREAR UN CERTIFICADO DE UNA AUTORIDAD CERTIFICADORA Y EMITIR CERTIFICADOS SSL/TLS,» 29 Enero 2018. [En línea]. Available: https://jorge.gd/2018/01/29/crear-certificado-de-una-autoridad-certificadora-y-emitir-certificados-ssl-tls/. [Último acceso: 18 Abril 2020].

[11] E. M. R. Casanova, «Prototipo de software para la firma y validación de documentos electrónicos,» San Andrés Tuxtla, 2019.

[12] «Packsys Academy,» Packsys Academy, [En línea]. Available: http://www.packsys.com/blog/cuanto-papel-se-puede-fabricar/. [Último acceso: 25 Enero 2020].

[13] Greenpeace, «El papel. Cómo reducir el consumo y optimizar el uso y reciclaje de papel,» Greenpeace, Madrid, 2004.

[14] T. O. N. Site, «Consciencia-Global,» The Omar Nahúm Site, 16 Febrero 2010. [En línea]. Available: http://consciencia-global.blogspot.com/2010/02/papel-uso-indebido-proceso.html. [Último acceso: 8 enero 2020].

Acerca de los autores

Yair Alejandro Ponciano Santiago, Ingeniero en Informática. Estudiante de la maestría en Ingeniería por el Instituto Tecnológico Superior de San Andrés Tuxtla. Ha participado en Business Hackathon Coatzacoalcos, en la III Olimpiada de informática realizado en las instalaciones del Tecnológico de San Andrés Tuxtla, ponente en Festival Latinoamericano de Instalación de Software Libre sede San Andrés Tuxtla, Ponente en el Consejo Zacatecano De Ciencia, Tecnología e Innovación en la ciudad de Zacatecas. Ha participado en Taller de Fibra Óptica impartido por el Centro Regional de Optimización y Desarrollo de Equipo de Orizaba

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.