 ISSN: 2448-623X

Configuración de un esquema de autentificación y validación de documentos electrónicos mediante una autoridad certificadora

J. R. González-Cadena[1], R. E. Telona-Torres[2], E. Y. Honorato-Rodríguez[3], J. S. Rodríguez-Aguirre[4]

***Resumen*—Hoy en día la mayor parte de la producción de documentos se realiza por medio de herramientas informáticas (procesadores de texto,...), estos pueden ser solo documentos que contengan información general, científica, personal u oficial, así mismo estos documentos pueden ser utilizados de manera discrecional ya que la gran mayoría de ellos no cuentan con las medidas necesarias de seguridad y cualquier persona puede modificar dichos documentos.**

En este contexto en el Instituto Tecnológico Superior de San Andrés Tuxtla (ITSSAT) es necesario implementar un esquema de validación y autentificación de documentos electrónicos con la finalidad de: a) disminuir el consumo de papel en apoyo al sistema de gestión ambiental (norma ISO 14001), b) agilizar la emisión-recepción de documentos y c) la seguridad del documento.

El presente trabajo describe cómo implementar una Autoridad Certificadora que permita emitir y controlar los certificados digitales así como permitir firmar electrónicamente los documentos del ITSSAT.

***Temas clave:* documento digital, autoridad certificadora certificado digital.**

***Abstract*- Today most of the production of documents is performed by means of software tools (word processors, ...), these can be only documents containing general scientific, personal or official information, also these documents can be used in a discretionary manner and that the vast majority of them do not have the necessary security measures and anyone can modify these documents.**

In this context Superior Technological Institute of San Andrés Tuxtla (ITSSAT) is necessary to implement a schema validation and authentication of electronic documents in order to: a) reduce the consumption of paper in support of the environmental management system (ISO 14001 *) b)* expedite the issuance and reception of documents c) document security

This paper describes how to implement a Certificate Authority for the originating, control digital certificates, and allow electronically sign documents ITSSAT.

***Keywords:* digital document certifying authority, digital certificate.**

I. Introducción

Como sabemos, la creciente penetración de las tecnologías de la información en las empresas y en los servicios públicos ha elevado, sustancialmente, el volumen de documentación creada y transmitida por medios electrónicos.

Esta documentación, que ha sido inicialmente creada por vía electrónica, deberá permanecer en este formato durante toda su vida útil. Sucede que, en este momento, las normas de autentificación y archivo, ampliamente usadas y aceptadas para los documentos de papel, no están siendo adaptadas ni normalizadas teniendo en cuenta este nuevo tipo de documentación. Actualmente se corre el riesgo de perder, o de poder quedar inaccesibles, documentos de gran valor para las organizaciones. Es frecuente que documentos de importancia fundamental se destruyan inadvertidamente o se mezclen con una amalgama de otra información sin importancia, perdiéndose su rastro por completo.

Por lo tanto es de gran importancia el establecimiento de buenas prácticas en la gestión de los documentos electrónicos durante todo su ciclo de vida y la aplicación de requerimientos archivísticos en los organismos públicos o privados de información y gestión, tal como ocurre en el Instituto Tecnológico Superior de San Andrés Tuxtla (ITSSAT).

Debido a la gran demanda en la expedición de documentos válidos en el ITSSAT, en materia de fiscalización o verificación irrevocable y autentificación, se ha llegado a la necesidad de desarrollar entidades certificadoras propias, para el uso adecuado de los documentos imprimibles, ligado al control de la seguridad y legitimidad de los derechos de autoría. Evitando así la falsificación de documentos.

Se realizó un esquema para la emisión de certificados digitales y poniendo en evidencia la validación de las Autoridades Certificadoras, a través de llaves privadas y el firmado de los documentos a prueba.

[1] jrgcadena@hotmail.com, Instituto Tecnológico Superior de San Andrés Tuxtla, Carretera Costera del Golfo KM 140+100, San Andrés Tuxtla, C.P. 95804, Veracruz, México.

[2] retelona19@hotmail.com, Instituto Tecnológico Superior de San Andrés Tuxtla, Carretera Costera del Golfo KM 140+100, San Andrés Tuxtla, C.P. 95804, Veracruz, México

[3] eneidayazmin@hotmail.com, Instituto Tecnológico Superior de San Andrés Tuxtla, Carretera Costera del Golfo KM 140+100, San Andrés Tuxtla, C.P. 95804, Veracruz, México

[4] soporte_macrosat@hotmail.com, *Instituto Tecnológico Superior de San Andrés Tuxtla, Carretera Costera del Golfo KM 140+100, San Andrés Tuxtla, C.P. 95804, Veracruz, México*

Para ello se configuraron las herramientas necesarias (OpenSSL y PHP) las cuales servirán para el desarrollo de una aplicación Web sencilla, que consulta la validación y contenido de los certificados digitales de los documentos emitidos solamente en el Área Académica del ITSSAT ya que es el área donde se realizaron las pruebas.

El proceso de certificación de firma trae consigo ciertos procedimientos establecidos por entes encargados de la prestación de este tipo de servicios, enmarcados en requisitos (tecnológicos, económico- financiero, legal y de auditoria) que deberán cumplir las instituciones interesada en la incorporación y utilización de la firma electrónica, abarcando una serie de etapas debidamente estudiadas, que garanticen la total eficiencia del empleo de estas herramientas.

Todo esto da una visión general de que el empleo de este tipo de instrumentos tecnológicos genera ventajas significativas y mejoras a largo plazo en las organizaciones, originando mayor competitividad en sus operaciones, permitiendo la agilización y mejora de sus procesos tanto interno como externo, es decir, que las mismas, a la hora de ser ejecutada aseguren la privacidad de la información.

El ITSSAT forma parte de las organizaciones que se unen a la idea de implementar cambios tecnológicos que contribuyan a mejorar los servicios y garantizar la calidad de los mismos para satisfacer las necesidades de la comunidad tecnológica. De tal manera, que el uso de estas TIC's (Tecnologías de Información y Comunicación) cambiarán la forma en que se gestionan estas transacciones dentro de la institución, originando así, la instauración de una nueva cultura en el manejo de documentación, en cuanto al uso, alcance y efecto de la implementación de estos medios electrónicos en los procesos de gestión administrativas. Formando nuevos escenarios tecnológicos y sociales que constituye una oportunidad única para que la institución impulse múltiples actuaciones a fin de modernizar su actividad de gestión, lo que representa un gran desafío para adaptarse a las enormes posibilidades que ofrece la tecnología a la hora de prestar mejores servicios de una forma más eficaz y eficiente.

II. Parte Técnica del Artículo

- *Metodología.*

La investigación parte del estudio de los hechos sobre la situación actual de firmado de los documentos en el ITSSAT con el fin de determinar las necesidades presentes y conocer la forma en que la misma lleva sus procesos administrativos en sus distintas áreas. Además de la indagación tanto en el aspecto jurídico, técnico, así como de funcionabilidad y operatividad de los procesos de certificación presentes actualmente en materia de certificación electrónica, correspondientes a las instituciones encargadas de promover e impulsar este tipo de herramientas (firma electrónica).

En este trabajo para la selección de la población se consideró solamente al Área Académica del ITSSAT. Para así delimitar el ámbito de la investigación, se tomó como muestra representativa a todos los jefes de carrera del instituto para el estudio, la cual está integrada por 8 personas. Simbolizando una muestra representativa para el análisis.

Para efecto de este proyecto las técnicas empleadas para le recopilación de información basada en el logro del objetivo trazado en esta investigación y siguiendo ciertos esquemas en cuanto a técnicas existentes para la obtención de datos del entorno bajo estudio, fueron: la observación directa, la revisión bibliográfica, la encuesta y la entrevista no estructurada. Todas ellas enfocadas en la obtención de los datos más importantes y fundamentales para la investigación.

La metodología aplicada para el modelo fue la del método *GRAY WATCH* el cual describe los procesos técnicos gerenciales y de soporte que deben emplear los equipos de trabajo, que deberá ser instanciado, es decir, adaptado cada vez que se aplique. El mismo se centró en las etapas de Modelado de Negocios e Ingeniería de Requisitos del cuerpo del Modelo de Proceso Técnicos, así como la generación de los productos asociados al cuerpo del Modelo de Producto y los procesos de gestión, verificación, configuración y calidad del cuerpo del Modelo de Apoyo del respectivo método. A continuación se hace una descripción de las etapas de la metodología operativa utilizada:

Etapa I: Estudio del Negocio.
En esta etapa se llevó acabo las dos primeras fases de la metodología utilizada (**Fase I, Gestión y Fase II, Soporte**), centrada en una serie de procesos que se ejecutaron a todo lo largo de la investigación, gestionando así el aseguramiento de calidad del producto, y el control de los cambios que modifican al mismo. Se realizó un estudio sobre la firma electrónica, con el fin de obtener información necesaria sobre su manejo.

De igual forma se investigó sobre las instituciones que actualmente están al servicio del desarrollo de estas nuevas tecnologías de información, además de determinar los fundamentos que esta herramienta (firma electrónica) ofrece a las organizaciones que deseen incorporarla en sus operaciones administrativas. Así como los beneficios, que la misma pueda generar para quienes la empleen.

Etapa II: Requisitos del Modelo.
Aquí se desarrolló parte de la tercera fase de la metodología, denominada *Análisis*, estructurado de

acuerdo a las interrelaciones y productos que se obtuvieron durante la investigación. Lo primero fue definir los procesos y funciones involucradas para la generación de la firma, así como los componentes físicos necesarios, considerados en cuanto a tecnología, mediante un estudio de las herramientas presentes en el mercado para así poder generar las especificaciones necesarias para la construcción del modelo. Durante esta etapa (requisito del modelo) se evaluaron las características y funcionalidades del modelo en cuanto a la aplicación requerida para la autenticación del documento. Los productos generados se enmarcaron en: Documento de requisito del modelo y unas especificaciones generales donde se describieron las propiedades de la aplicación a utilizar para su futura implementación.

Etapa III: Diseño del Modelo.
En esta etapa se completó la tercera fase de la metodología, donde se definieron e integraron todos los componentes, procesos requeridos para la configuración de la autoridad certificadora de firma digital.

- *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:
La cadena original es la secuencia de datos formada con la información contenida dentro del documento electrónico. Toda la cadena original se encuentra expresada en el formato de codificación UTF-8.

La secuencia de formación está conformada por los siguientes datos y en el orden en el que aparecen: a) Código del documento, b) Sello digital y c) Fecha de emisión del documento.
Sello digital, toda cadena original es sellada digitalmente, para eso se aplica el algoritmo de encriptación de base de 64 y está compuesto por: a) Folio del documento, b) Propietario del certificado emisor y c) 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: a) 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: a) Sello digital.

- *Requerimientos de hardware y software:*

Servidor con Linux, Apache, PHP, Adobe Acrobat, Qrencode y OpenSSL.

B. Configuración de la autoridad certificadora.

Para poder configurar la autoridad certificadora en nuestro directorio necesitamos tener los siguientes directorios: certs, csr, crl, certs y private. Pero también vamos a requerir dos archivos con el nombre de serial, crlnumber y para finalizar un archivo de texto index.txt.

Descripción de directorios y archivos:

- **newcerts**: directorio para contener los nuevos certificados emitidos.
- **private:** directorio que contiene el fichero cakey.key.
- **serial:** archivo que contiene el número de serie de certificados.
- **crlnumber:** archivo 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:** archivo con el índice de certificados firmados.

- *Creación de la autoridad certificadora*.

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 todos 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: auitssat

- *Creación de certificados digitales (ejemplo: División Ingeniería en Informática***)**

Primer paso generar la llave privada del certificado, la cual sirve para descifrar el contenido del certificado a generar:
openssl genrsa -des3 -out private/DivInf.key 1024
password: inf7div

 ISSN: 2448-623X

Después se debe realizar una petición de un certificado usando la llave que se ha creado anteriormente:
openssl req -new -key private/DivInf.key -out csr/DivInf.csr password: inf7div

- *Petición de un certificado usando la llave anterior.*

En la generación de la solicitud del certificado se especifica la llave con la cual se asocia así como el nombre de la solicitud que se envía, si se desea una cantidad específica de días de vida del certificado solo es necesario agregar el comando –days seguido del número de días, ya que el número de días de un certificado por default es de 365.

La solicitud consta de algunos datos que corresponden al solicitante; el código del país al que pertenece el solicitante, el nombre del estado o la provincia, el nombre de la ciudad, el nombre de la compañía, el nombre del departamento o área que está solicitando el certificado, el nombre del servidor en caso de que tenga 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*.

Y en el último paso, 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/DivInf.csr

En este caso va a pedir el password de ca.key que es: auitssat

Para el firmado de la solicitud solamente se usa 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.

Para comprobar que el certificado se ha creado es necesario ingresar a la carpeta *newcerts*, en ella se encuentra el archivo con el número de serial y la extensión *.pem*

Una vez creado los certificados estos deberán ser enviados al personal que va a hacer uso de ellos, para ello se debe entregar la llave privada y su correspondiente certificado. El certificado debe cambiar de ubicación con un nombre que sea fácil de identificar y en formato .crt ya que esta extensión es más usual en algunos navegadores cuando se requiere instalar el certificado.

- *Instalación de los certificados digitales*.

Para el sellado electrónico es necesaria la instalación del certificado digital en el equipo de cómputo del personal 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 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 se cuenta con el archivo SelloITSSAT con la información, se va proceder aplicarle un método de encriptación basado en md5, este permite cifrar la información a código binario, al final se genera otro archivo de texto con el código generado.

openssl dgst -md5 -sign private/ca.key -out firmas/SelloITSSATmd5.txt firmas/SelloITSSAT.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/AreaAca.crt -noout -subject
openssl x509 -in certs/DivInf.crt -noout -subject

- *Creación del código QR.*

El Código QR se usó en el sellado del documento dentro de la institución es con la finalidad de contar con una alternativa más de protección de la información que se envía, atreves de la representación de una imagen en donde incluye el sellado digital.

Para poder realizar el código QR hay que instalar Qrencode y siendo este un software libre, puede distribuirse y /o modificarse bajo los términos de la Licencia Pública General GNU.

 ISSN: 2448-623X

El comando cuenta con parámetros que hace que se genere el código QR, en el caso de *qrencode* se colocara para poder entrar al programa y que pueda reconocer los otros parámetros, el –o (corresponde a output) y se coloca porque es la salida del archivo de ahí va el nombre del archivo con la extensión

- *Proceso de revocación de certificados digitales.*

La revocación de un certificado es cuando este expira la validez de un certificado, esto se puede presentar por varias razones como lo es: el robo de la llave privada, uso incorrecto del certificado, cambio del personal encargado de firmar los documentos en algún departamento, cambio de políticas dentro de la institución o por la actualización de la Autoridad Certificadora.

openssl ca –config openssl.cnf –revoke certs/DeptoSist.crt

Cuando se inserta el comando de revocación del certificado y se ejecuta nos va pedir el *password* de la llave, que en este caso es de la autoridad certificadora, posteriormente nos indica que ha sido revocado el certificado y han bien nos da el número de la serie cuando fue creado.

- *Creación de una lista de revocación.*

La generación de la lista de revocación es muy importante, en ella se va almacenar la información de los certificados que han sido revocados y se actualiza cada vez que un certificado sufre el mismo cambio.

Comando correspondiente para la creación de la lista:

openssl ca –config openssl,cnf –gencerl –out crl/ca.crl

Tenemos que verificar que se ha creado la lista de revocación y principalmente revisar el contenido de esta lista, para ello tenemos que abrir el archivo ca.crl.

Con los procesos que fueron realizados el certificado ya no puede ser usado para firmar los documentos electrónicos, en dado caso que se firmara el software de verificación va mostrar que dicho documento no es válido y que ha sido emitido por una entidad desconocida.

C. Aplicación Web para la consulta y validez del contenido de los certificados.

Una vez realizado la instalación, configuración de la Autoridad Certificadora y se hayan emitido los certificados, sellos digitales y códigos QR, mediante una aplicación Web que estará disponible en el servidor Web del ITSSAT, los usuarios podrán verificar la validez del documento como se muestra en la figura 1.

Figura 1. Aplicación Web

III. APÉNDICE A: BENEFICIOS

La implementación de la Autoridad Certificadora es parte de la investigación denominada "**Gestión de Servicios y Documentos Electrónicos Mediante Estándares de Comunicación",** la cual pretende ser un complemento al sistema de gestión ambiental implantado en el ITSSAT.

Mediante la implementación de esta Autoridad Certificadora, todos los documentos electrónicos que se generen se podrán firmar digitalmente, esto permitirá una disminución sustancial del consumo de papel, así como espacio de almacenamiento de esos documentos, se agilizará el flujo de documentos entre las diferentes divisiones del área académica del ITSSAT que permitirán disminuir el consumo de papel que en estimaciones realizadas, se proyecta a continuación:

A. Consumo estimado de papel en el área académica del ITSSAT.

Esta estimación está basada en el cuerpo de docentes del ITSSAT, en la Tabla 1 se muestra dichas estimaciones.

TABLA 1

Número de docentes	Paquete de hojas semestral (por docente)	Contenido de hojas por paquete	Hojas consumidas por docentes al semestre	Hojas consumidas por docentes al año
70	1	500	35000	70000

- *Consideraciones:*
  - Un árbol con edad entre 10 y 14 años, produce 20 kilos de papel de calidad.
  - En promedio un paquete pesa 2.5 kilos.
  - En el ITSSAT se consumen al año, aproximadamente, 140 paquetes de hojas,

siendo un total de 350 kilos equivalentes a 14 árboles por año.

- Para que un árbol sea considerado "maduro" para explotarlo debe crecer durante 14 años, siendo que en ese periodo se habrían consumido las hojas producidas por 196 árboles.
- En una hectárea se siembran aproximadamente entre 350 y 400 árboles, lo que se contabilizaría en la deforestación de 2.5 hectáreas.

Con la implementación de la Autoridad Certificadora, todos los documentos electrónicos que se generen se firmaran digitalmente, se garantizara la validez del mismo, además se complementaran con el uso de otras herramientas las cuales permitirán la creación de grupos de trabajo colaborativo agilizando el flujo de documentos electrónicos entre las diferentes divisiones del área académica del ITSSAT, así mismo tendrá un impacto importante a nivel ambiental como se puede observar en la Tabla 1.

IV. AGRADECIMIENTOS

Se agradece al Instituto Tecnológico Superior de San Andrés Tuxtla el apoyo brindado para este proyecto de investigación y para la publicación del mismo.

V. REFERENCIAS

[1] HURTADO, J. Metodología de la Investigación Holística, (3ed.), Editorial SYPAL, Caracas, Venezuela.

[2] ARIAS, F. El Proyecto de Investigación, (5ed.), Editorial Episteme, Caracas, Venezuela.

[3] Montilva C., Jonas, Barrios A. Judith y Rivero A. Milagros. Método de Desarrollo de Software para Aplicaciones Empresariales. Edición 2008

[4] ANÓNIMO, "Entidad Emisora de Certificados digitales (CA) for Servidor de Correo Exchange 2003", en http://es.scribd.com/doc/46041116/6/Entidad-Emisora-de-Certificados-digitales-CA,

[5] ANÓNIMO, "Generando Certificado de Firma Electrónica Avanzada", en https://www.comimsa.com.mx/portales/firma-digital/resources/MaterialDeApoyo/GenerandoCertificadoDeFirmaElectronicaAvanzada.pdf

[6] Enrique V. Bonet Esteban, "Creación y administración de certificados de seguridad mediante OpenSSL", http://informatica.uv.es/it3guia/AGR/apuntes/teoria/documentos/Certificados.pdf,

[7] Estaban Saavedra López, Joseph Sandoval Falomici, "Gestión de Certificados Digitales con OpenSSL (2da parte)", en https://speakerd.s3.amazonaws.com/presentations/e038d590245b01307e0222000 a9d06e0/openssl02.pdf

[8] Esteban Saavedra López, Joseph Sandoval Falomici, "Gestión de Certificados Digitales con OpenSSL (1ra Parte)", en https://speakerd.s3.amazonaws.com/presentations/91eafef0245b0130ac9c22000a9d03c4/openssl.pdf.

[9] Toni de la Fuente Díaz, "Usando OpenSSL en el mundo Real", en http://blyx.com/public/docs/security/Usando_OpenSSL_en_el_mundo_real.pdf.

VI. BIOGRAFÍA

Juan Rafael González Cadena, San Andrés Tuxtla, Veracruz, 16 de enero de 1961. Licenciado en Informática por el Instituto Tecnológico Superior de San Andrés Tuxtla, Veracruz, México, 2001. Maestro en Tecnologías de Información por la Universidad Cristóbal Colon, Veracruz, Ver. México, 2008.

El actualmente labora en el Instituto Tecnológico Superior de San Andrés Tuxtla, en Matacapan, Mpio. de San Andrés Tuxtla, Veracruz. Imparte clases en las carreras de Ingeniería Informática, Ingeniería en Sistemas Computacionales, Ingeniería Electromecánica e Ingeniería Mecatrónica. Trabaja actualmente en la línea de investigación: Tecnologías de Información y Comunicaciones.

El M.T.I. González es Perfil Deseable de PRODEP, tiene las siguientes 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.

Publicaciones:

- Sistema de Control Automatizado del Clima, aplicando una Interfaz gráfica de Visual Basic.

Coloquio de Investigación Multidisciplinaria. Evento Internacional CIM-2012.

- Estudio comparativo de herramientas para el trabajo colaborativo

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2014.

Rogelio Enrique Telona Torres, Matacapan, Mpio. de San Andrés Tuxtla, Veracruz, 19 de Abril de 1979. Licenciado en Informática por el Instituto Tecnológico Superior de San Andrés Tuxtla, Veracruz, México, 2004. Maestro en Tecnologías de Información por la Universidad Cristóbal Colon, Veracruz, Ver. México, 2008.

El actualmente labora en el Instituto Tecnológico Superior de San Andrés Tuxtla, en Matacapan, Mpio. de San Andrés Tuxtla, Veracruz. Imparte clases en las carreras de Ingeniería Informática, Ingeniería en Sistemas Computacionales, Ingeniería Electromecánica e Ingeniería Mecatrónica. Trabaja actualmente en la línea de investigación: Tecnologías de Información y Comunicaciones.

El M.T.I. Telona es Perfil Deseable de PRODEP, tiene las siguientes certificaciones: *Certified LabVIEW Associate Developer por National Instruments 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.

Publicaciones:

- Uso de las TIC en la educación con pedagogía Freinet.

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2013.

- USO DE LAS TIC´S EN LA ESCUELA MODERNA.

CONGRESO IBEROAMERICANO DE CALIDAD EDUCATIVA 2013.

- Estudio comparativo de herramientas para el trabajo colaborativo.

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2014.

Eneida Yazmin Honorato Rodríguez, San Andrés Tuxtla, Veracruz, 7 de Octubre de 1974. Ingeniero en Sistemas Computacionales por el Instituto Tecnológico de Veracruz, Veracruz, México, 2004. Maestro en Administración de Sistemas de Información por la Universidad Cristóbal Colon, Veracruz, Ver. México, 2008.

Ella actualmente labora en el Instituto Tecnológico Superior de San Andrés Tuxtla, en Matacapan, Mpio. de San Andrés Tuxtla, Veracruz. Imparte clases en la carrera de Ingeniería en Sistemas Computacionales, Trabaja actualmente en la línea de investigación: Reingeniería de Hardware y Software para la Optimización de Recursos Computacionales en los Sectores Productivo, Empresarial y Educativo de la Región de los Tuxtlas.

La M.A.S.I. Honorato es Perfil Deseable de PRODEP, tiene las siguientes certificaciones: *Certified LabVIEW Associate Developer por National Instruments 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.

Publicaciones:

- Sistema de Control Automatizado del Clima, aplicando una Interfaz gráfica de Visual Basic.

Coloquio de Investigación Multidisciplinaria. Evento Internacional CIM-2012.

- Impacto académico motivacional del aula interactiva en alumnos de Ing. en Sistemas Computacionales del ITSSAT.

Coloquio de Investigación Multidisciplinaria Evento Internacional CIM-2013.

- Estudio comparativo de herramientas para el trabajo colaborativo

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2014.

Juan Salvador Rodríguez Aguirre, Acayucan, Veracruz, 9 de Noviembre de 1979. Licenciado en Informática por el Instituto Tecnológico Superior de San Andrés Tuxtla, Veracruz, México, 2004. Maestro en Tecnologías de Información por la Universidad Cristóbal Colon, Veracruz, Ver. México, 2011.

El actualmente labora en el Instituto Tecnológico Superior de San Andrés Tuxtla, en Matacapan, Mpio. de San Andrés Tuxtla, Veracruz. Imparte clases en las carreras de Ingeniería Informática. Trabaja actualmente en la línea de investigación: Tecnologías de Información y Comunicaciones.

El M.T.I. Rodríguez es Perfil Deseable de PRODEP, tiene las siguientes certificaciones: *Certified LabVIEW Associate Developer por National Instruments y Basic Level Programmer en ROBOTC otorgado por Carnegie Mellon Robotics Academy*.

Publicaciones:

- Uso de las TIC en la educación con pedagogía Freinet.

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2013.

- Estudio comparativo de herramientas para el trabajo colaborativo.

Coloquio de Investigación Multidisciplinaria, evento internacional CIM 2014.