UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

FACULTAD DE ESTUDIOS SUPERIORES
A C A T L Á N

"MODELO PARA SISTEMATIZAR LA RECEPCIÓN DE TRAMITES Y DOCUMENTOS EN EL SERVICIO DE ADMINISTRACIÓN TRIBUTARIA, COLABORANDO DE ESTA FORMA EN EL FORTALECIMIENTO DE LA RECAUDACIÓN DE IMPUESTOS"

SEMINARIO TALLER EXTRACURRICULAR

QUE PARA OBTENER EL TÍTULO DE
LICENCIADO EN MATEMÁTICAS APLICADAS Y COMPUTACIÓN

PRESENTA:

ALICIA CRUZ MARTÍNEZ

ASESOR:
M. en C. SARA CAMACHO CANCINO

NOVIEMBRE 2005

AGRADECIMIENTOS

A Saúl mi hijo ... por llegar a mi vida y motivar el inicio y termino de este trabajo.

A Héctor mi esposo ... por su amor y apoyo incondicional y porque con sus aportaciones me ayudó a enriquecer el contenido de este trabajo.

A mis padres ... por que con su cariño, apoyo y ejemplo han sido el pilar de mi vida.

A mis hermanos ... que con sus enseñanzas y ejemplo,
Raquel por su fortaleza y constancia,
Mayra por su valentía y corage,
Marisol por su esfuerzo y dedicación,
Toño por su presencia y mantenerse en el camino,
Leticia por luchar por sus objetivos,
Tania por perseguir sus sueños y
Yessica por no rendirse, me han enseñado que la vida es una historia diferente para cada uno de nosotros pero que también es mucho más hermosa y llevadera si estamos unidos.

A mis sobrinos ... Brenda, Salvador, Erick, Frank, Brandon, Sara, Yair, Emiliano y Camila de quienes he aprendido que la fortaleza y la generosidad no tienen edad y la unión se demuestra también en un juego.

A la familia de mi esposo...	por el cariño que me han brindado durante estos años.
A Sara mi asesora ...	Por la responsabilidad y profesionalismo que respaldan su labor y por las observaciones y aportaciones a este trabajo.
A la UNAM ...	por existir y permitirme ser parte de sus filas.
A mis maestros ...	por los conocimientos y experiencias que me aportaron.
A Dios ...	por darme la vida y permitirme vivir esta experiencia.

A todas aquellas personas... que durante mi vida laboral han dejado enseñanzas y experiencias que me han permitido comprender que la responsabilidad que tengo como egresada de esta universidad, es ser profesional no solo en el ámbito laboral; si no en todos los aspectos de mi vida, porque de esta manera podré extender las riquezas que encontré a mi paso por esta casa de estudios y contribuir así en el desarrollo de mi país.

CONTENIDO

CAPITULO 3

MODELO PARA EL INTERCAMBIO DE DOCUMENTOS

CAPITULO 4

PROCESO DE IMPLEMENTACIÓN

INTRODUCCIÓN

El uso de sistemas de información ha crecido tanto en los últimos años que sobre todo en las grandes ciudades es común encontrar equipos de cómputo en casa, y precisamente por la facilidad con que en la actualidad se tiene acceso a sistemas y equipos de cómputo, las empresas e instituciones han extendido la atención de sus servicios utilizando la red pública. Desafortunadamente la existencia de personas que se dedican a sabotear la información que viaja por las redes de datos ha creado desconfianza en el uso de este medio. Además, la falta de una cultura en seguridad de la información, que incluso las empresas que se dedican al desarrollo de sistemas han dejado de lado, genera una mayor incertidumbre en la veracidad de los procesos que se llevan a cabo por medios electrónicos.

Hablar de seguridad es hablar de un gran número de posibilidades que se pueden considerar para resguardar datos, se podría pensar en asegurar las instalaciones, los equipos, los accesos, todo depende de las necesidades de seguridad que cada quien tenga, y aunque hablando de sistemas, cada una de estas formas de seguridad debe considerarse; el interés que se tiene en el desarrollo de este trabajo es la seguridad de la información que viaja por las redes de datos tanto públicas como privadas.

Afortunadamente el panorama no es tan desalentador como parece, ya que existen mecanismos que se pueden integrar en los sistemas para asegurar el viaje de la información de un punto a otro, aun cuando de punto a punto existan kilómetros de distancia, y además es posible verificar que el documento electrónico que se recibe es el que se envió originalmente.

El presente trabajo pretende dar un panorama al lector sobre los medios que existen actualmente para asegurar información que se encuentra en medios electrónicos, presentar la problemática actual del Servicio de Administración Tributaria (SAT) para la recepción de trámites y documentos usando certificados digitales sin considerar la infraestructura que para esto se requiere, y la presentación del modelo que se propone para resolver la situación, ya que en el corto plazo se espera la integración del total de los contribuyentes al mecanismo de entrega de trámites y documentos por medios electrónicos.

Así mismo es importante mencionar que aún cuando el enfoque de este trabajo se basa en la propuesta de un modelo para resolver un problema en específico, este es

aplicable a cualquier institución que desee asegurar la información que viaja por las redes de información.

El desarrollo de este trabajo esta organizado de la siguiente manera:

En el capítulo uno se mencionan métodos que en la actualidad se utilizan para integrar elementos de seguridad en el intercambio de información, cada uno de estos métodos tiene una función específica y dependerá de las necesidades que cada usuario tenga, decidir cual debe usar para asegurar la información.

En el capítulo dos se plantea la problemática de la institución en estudio, la forma en que se llegó a la situación actual, las necesidades que se tienen para llevar a cabo el intercambio de información de manera segura y en referencia a los métodos planteados en el capítulo uno se establece el que se debe usar para llevar a cabo la recepción de trámites y documentos por medios electrónicos.

En el capítulo tres se plantea el modelo y los procesos que se deben incorporar para que la recepción de documentos por medios electrónicos sea segura y confiable tanto para los usuarios del servicio como para la institución.

En el capítulo cuatro se plantean los procesos mínimos que se deben considerar para llevar a cabo la implementación, en este capítulo se mencionan algunas áreas y actividades que necesariamente deben llevarse a cabo para considerar el proceso completo de la entrega recepción de documentos con las áreas que tienen que estar involucradas durante el desarrollo del sistema.

Se espera que con este trabajo el lector comprenda la importancia de implementar mecanismos de seguridad en los sistemas de información, y si además, su ámbito de trabajo se enfoca en el desarrollo de sistemas, promueva la integración de mecanismos que considere convenientes para elevar la seguridad de los procesos que se llevan acabo en la empresa o institución para la que labora.

CAPÍTULO 1

INTERCAMBIO DE DOCUMENTOS EN MEDIOS ELECTRÓNICOS

Así como en la actualidad realizamos trámites y entrega de documentos ante instituciones, los cuales son aceptados y reconocidos como auténticos por el hecho de que llevan plasmada la firma autógrafa y el trámite se realiza con la presentación de identificaciones oficiales y la presencia física del interesado, de la misma forma se busca que el uso de los medios electrónicos permitan establecer mecanismos que agilicen estos procesos, que no se requiera la presencia física en cada trámite o entrega de documento pero que si se tenga la certeza de que el trámite fue efectuado por la persona indicada. El uso de internet tiende año con año a ser más utilizado, por lo que, sabiendo de ante mano que transmitir información es el principal objetivo de este medio y conociendo de la misma manera que hacerlo sin las medidas de seguridad necesarias deja al descubierto y vulnerable la información que transita, resulta necesario en el mundo digital regular y establecer la forma en que las transacciones digitales deben operar para ser seguras y reconocidas.

En este capítulo hablaremos de la seguridad que regularmente se implementa en el acceso a sistemas de información para llevar a cabo el intercambio de datos, aunque al

hablar de seguridad en el campo de la tecnología de información podría ser muy extenso, el enfoque de este trabajo esta dirigido a la seguridad en los medios electrónicos y específicamente para el intercambio de información. Se espera que al final se cuente con el panorama general de lo que existe actualmente y de que se considere la seguridad como un elemento importante en el desarrollo de sistemas.

En este capítulo se mencionan las técnicas principales de autenticación: contraseñas, identificadores de prenda (tokens) de autenticación, tarjetas inteligentes y biometrías, se señala como la seguridad se involucra en la autenticación y como el grado de la misma se incrementa de acuerdo a las necesidades de seguridad que se requieran, así mismo se describe como se relaciona esta con los certificados digitales, como se generan los certificados digitales y por último se explica como se realiza la recepción de documentos en la institución que se estudia.

En el desarrollo de este trabajo se percibe como no hay una respuesta simple a la pregunta "¿Cuál es la mejor forma de autenticación?". Cada forma puede contar con diferentes niveles de seguridad, distintas características de facilidad de uso, diferentes costos de adquisición y de administración, por ello es importante considerar que se deben tomar en cuenta varios elementos antes de elegir la forma de autenticación adecuada, ya que dependiendo del grado de seguridad que se requiera esta puede ser sencilla o compleja.

1.1 METODOS COMUNES DE INTERCAMBIO

Uso de los medios electrónicos y la seguridad

En las últimas décadas ha aumentado considerablemente el uso de equipos informáticos, y esto en gran parte se debe al beneficio obtenido por el uso de las redes, ya que permiten realizar pagos con tarjetas bancarias, obtener dinero de cajeros automáticos, realizar operaciones monetarias y pagos de servicios vía internet, comprar un boleto de avión o bien adquirir un plan vacacional, tomar clases desde casa, obtener

un historial académico, comprar cualquier clase de artículos, mantener comunicación con familiares o amigos que se encuentran en el extranjero y un sin fin de posibilidades más aún estando a kilómetros de distancia entre los puntos de contacto, y todas estas bondades que nos permiten realizar la redes de datos serían maravillosas a no ser que existen una serie de factores que tienen que considerarse para que los servicios que ofrecen bancos, escuelas, empresas, gobiernos, etc,. sean confiables; este aspecto es sin duda uno de los factores que ha tomado gran importancia en los últimos años y sin embargo todavía en el desarrollo de varios sistemas no es considerado un requerimiento inicial, se trata de la seguridad.

¿Dónde y cuánta seguridad debe integrarse?. Es una de las preguntas que frecuentemente se hacen quienes ante la problemática detectada se ven en la necesidad de integrar procesos de este tipo a sus sistemas, y no hay una respuesta que pueda darse de manera general, ya que dependiendo de la importancia que tenga la información que se maneja, deberá determinarse el grado y tipo de seguridad que se requiere y esta debe ser tal que la operación de las actividades no deben verse afectadas por los candados o procesos de seguridad implementados.

Tipos de Seguridad

Al hablar de seguridad se pueden mencionar varios tipos, por ejemplo la seguridad física de lo equipos, ya que los equipos que almacenan los datos podrían verse afectados por varios factores que pueden ocasionarles daños importantes. Lo mismo puede ocurrir con los medios de almacenamiento físico (discos, cintas, etc.), Por lo tanto es necesario proteger no solo los datos, sino todo tipo de elementos que forman parte del equipo informático. Entre los factores a los que hay que hacer frente se encuentran los atmosféricos (frío, calor, humedad, etc.) que pueden ocasionar desperfectos en los medios de almacenamiento; factores naturales (terremotos, inundaciones, etc.) que pueden causar graves desperfectos; factores humanos (espías, usuarios descontentos, ladrones), que podrían desde robar cualquier componente del

equipo hasta causar todo tipo de destrozos intencionados, y así otros muchos factores más, como incendios, descargas eléctricas, accidentes, virus informáticos, etc.

La seguridad puede verse desde diferentes puntos de vista como los que se acaban de mencionar, los grandes corporativos, instituciones y personas que conocen el valor de lo que sus equipos informáticos manejan prevén el resguardo de equipos y el respaldo de información como medidas de seguridad, sin embargo este tipo de seguridad no será tratada en el desarrollo de este trabajo, ya que el enfoque de la seguridad que se utiliza en el intercambio de información esta relacionada con el comportamiento de los datos y las medidas que existen para proteger el viaje de los mismos de un punto a otro.

Secretos

La autenticación electrónica se basa en secretos. En ocasiones uno mismo y el sistema que trata de autenticarlo conocen el mismo secreto; es decir, para poder acceder a un sistema previamente debió llevarse acabo una actividad a la que comúnmente se le llama "darse de alta en el sistema", y esto no es más que proporcionar un dato denominado "clave de usuario" y contraseñas o formas de acceso. Lo más común es que se conozca un secreto y el sistema que trata de autenticarlo sepa algo derivado del secreto. Existen también formas de acceso en las que además de proporcionar una contraseña se requiere contar con hardware adicional y la combinación de ambos datos permite el acceso a la información.

Contraseñas

Las contraseñas son la forma más común de autenticación. A primera vista, parecería ser la opción de autenticación menos costosa ya que no existe una parte especial de hardware que el usuario deba tener para utilizar una contraseña y no existe un lector especial dentro del cual se deba insertar la contraseña.

Contraseñas en texto claro

En los inicios de la computación, antes de Internet, este tipo sencillo de procesamientos de contraseñas se utilizó para obtener el acceso a muchos sistemas exclusivos. Incluso, en la actualidad, esta técnica se utiliza ampliamente cuando la terminal a la que se está ingresando la clave de usuario y contraseña está directamente conectada al sistema al que se esta tratando de acceder. El hecho de que la contraseña real pase de la terminal de entrada al software de autenticación crea una oportunidad para copiar la contraseña cuando se este transmitiendo.

Aunque este tipo de sistema de contraseñas se ha utilizado con amplitud, se recomienda emplearlo sólo en ambientes que satisfagan criterios como que la base de datos es segura contra robos; la terminal de entrada esta conectada directamente al sistema que realiza la autenticación (no a través de una red).

Una forma de mejorar este tipo de accesos es quitar la necesidad de almacenar la contraseña real en el sistema al que se tiene acceso.

Identificadores de prenda de autenticación

El reemplazo más común para las contraseñas simples es un identificador de prenda (token) de autenticación, que consiste de un dispositivo que, cada vez que se emplea, genera un valor nuevo para la autenticación. Estos dispositivos son pequeños; muchos tienen una apariencia similar a una calculadora pequeña.

Los identificadores de prenda de autenticación tienen un procesador, una pantalla de cristal líquido y una batería. Dependiendo del tipo de identificador de prenda, también pueden contar con un teclado para ingresar información, un reloj en tiempo real y tal vez otras características. En algunos casos las baterías se pueden reemplazar, en otras unidades, la batería dura todo el tiempo de vida de identificador de prenda. Algunos dispositivos arrojan valores numéricos y otros valores hexadecimales.

Cada identificador de prenda está programado con un valor único llamado *semilla*, que garantiza que el dispositivo identificador producirá un conjunto único de códigos de salida.

Los identificadores de prenda generan números pseudoaleatorios llamados *contraseñas de una vez* o *códigos de paso de una vez*. Estos códigos de paso también se llaman pseudoaleatorios porque si se une la serie de números que produce un identificador de prenda y traza la distribución de los números, este trazado tendrá el aspecto de números verdaderamente aleatorios. En otras palabras, los valores estarán distribuidos equitativamente a través del espacio de valores. Sin embargo, los códigos de paso no son verdaderamente aleatorios porque, si se sabe como se calculan, se puede predecir cualquier valor en particular. Esto es importante, debido a que el servidor de autenticación, que verificará el código de paso, podrá estar en capacidad de revisar que un identificador de prenda en particular generó un código de paso en particular.

Cuando se conecta a un recurso, el usuario ingresa su clave de usuario, pero, en lugar de una contraseña, ingresa el código de paso que aparece en la pantalla del identificador de prenda. Una vez que se ha usado un código de paso una vez, no se puede volver a utilizar. En la mayoría de sistemas, el sistema al que se accede no verifica el código de paso suministrado en sí mismo, si no que pedirá a un servidor de autenticación de confianza que lo haga.

El servidor de autenticación debe conocer el valor de la semilla programado dentro de cada identificador de prenda. Como el servidor de autenticación conoce la semilla programada dentro del identificador de prenda que tiene un usuario en particular, dicho servidor verifica que el código de paso suministrado sea el número pseudoaleatorio correcto para ese usuario.

Tarjetas Inteligentes

Básicamente, una tarjeta inteligente es un pequeño microprocesador con memoria incorporada dentro de un trozo de plástico del tamaño de una tarjeta de crédito. Sus niveles de uso van desde el tipo de las tarjetas para llamadas telefónicas sencillas hasta complejos dispositivos que soportan la aceleración criptográfica.

Las tarjetas inteligentes se construyen de acuerdo con un conjunto de estándares, de los cuales el ISO7816 es uno de los más importantes. Este estándar define la forma, el grosor, las posiciones de contacto, las señales eléctricas, los protocolos y algunas funciones del sistema operativo con que deben contar.

Estos dispositivos se reconocen por el hecho de que habitualmente tienen lo que parece un pequeño sello dorado en una de sus caras. En realidad es un grupo de contactos eléctricos de oro que se conectan a la tarjeta inteligente. De hecho bajo estos contactos de oro está oculto un microprocesador. Las tarjetas inteligentes son pequeños procesadores de datos que pueden aceptar datos, procesarlos con programas almacenados en la memoria de la tarjeta y, luego, emitir el resultado procesado a través del puerto de comunicaciones.

En resumen se puede decir que:

- Las tarjetas inteligentes contienen pequeños microprocesadores incorporados dentro de piezas de plástico del tamaño de una tarjeta de crédito.
- Existen tres clases principales de tarjetas inteligentes: de valor almacenado, criptográficas y no criptográficas.
- La mayoría de las tarjetas inteligentes son tarjetas de contacto que se insertan dentro de un dispositivo de lectura, que hace contacto eléctricamente con la tarjeta inteligente. Las tarjetas sin contacto, establecen conexión con el dispositivo de lectura a través de un canal de frecuencias.

- Algunas tarjetas inteligentes tienen partes de contacto y sin contacto, a estas se les conocen como tarjetas combinadas.

- Las tarjetas inteligentes están evolucionando a procesadores de más alto nivel, como los motores RISC de 32 bits, y están evolucionando hacia sistemas operativos abiertos como JavaCard, MULTOS y Windows para tarjetas inteligentes.

Autenticación biométrica

La biometría promete ser uno de los mejores métodos de autenticación, pero si no se utiliza de manera apropiada, puede resultar peor que las contraseñas.

Todos los sistemas biométricos miden alguna característica del usuario. Puede ser su huella dactilar, su voz, el patrón de líneas en el iris de su ojo o algo tan curioso como el perfume corporal.

En todos los sistemas se debe crear una plantilla maestra de la característica biométrica. Cuando se trata de autenticar ante un sistema, se pide presentar el rasgo biométrico. El dispositivo de lectura tomará registro de los datos biométricos y realizará una comparación de los datos biométricos que se encuentran almacenados en la plantilla. Si existe correspondencia, se concede el acceso.

El aspecto de una correspondencia "bastante buena" (pero no exacta) es central para la autenticación biométrica. Todos los sistemas biométricos comparten estos conceptos básicos:

- La biometría mide alguna característica física del usuario.

- Los datos biométricos varían de una presentación a otra.

- Como resultado, la biometría no da correspondencias exactas.

- No se registra el patrón biométrico completo, si no que se archivan las características interesantes de los datos biométricos.

En todos los sistemas biométricos, el usuario debe registrar sus datos biométricos para crear la plantilla maestra, que servirá para las comparaciones posteriores. Los sistemas biométricos tienen un proceso de registro a través del cual se le pide al usuario presentar su biometría en múltiples ocasiones ante el sistema. Después, el sistema promediará las lecturas y creará la plantilla maestra.

La biometría responde con correspondencias aproximadas. En un sistema biométrico el software de correspondencia compara los datos biométricos recién recopilados con la plantilla almacenada previamente, y verifica si la correspondencia es bastante buena. Lo que determina que sea "bastante buena" varía de un sistema a otro, y depende de datos biométricos, lo mismo que de los algoritmos de correspondencia biométrica interna que se utilicen en el sistema. En cualquier caso, todos estos sistemas tienen un parámetro que se puede configurar, denominado coeficiente de aceptación falso FAR o coeficiente de rechazo falso FRR.

FAR y FRR funcionan uno contra el otro. Si se libera el sistema para evitar rechazos inapropiados de un usuario inválido, es probable que se consiga que pueda entrar un usuario inapropiado. Si se ajusta el sistema para hacer menos probable que un usuario inapropiado tenga acceso al mismo, aumentará la probabilidad de que el usuario válido sea rechazado.

1.2 ELEMENTOS DE SEGURIDAD PARA EL INTERCAMBIO DE INFORMACIÓN

El concepto de seguridad se esta volviendo cada vez más sofisticado, ya no solo es limitarse a pensar en barreras de seguridad y enrutadores, ahora se empieza a pensar más en los principios que se deben aplicar a la información y a los servicios que necesitamos proteger y a los cuales se quiere conceder acceso.

La seguridad electrónica se halla en procesos o servicios fundamentales que permiten la construcción de una solución segura para enviar información de negocios y servicios a través de una red. Estos servicios incluyen:

Identificación, autenticación, autorización, integridad, confidencialidad, aceptación.

- La identificación es el proceso de reconocer a un individuo en particular. Se identifica a las personas al reconocer sus rasgos físicos, tales como cara, estatura y contextura física.

- La autenticación es cualquier proceso mediante el cual se comprueba y verifica cierta información.

- La autorización es el proceso de determinar lo que esta permitido hacer. Después de la autenticación (y posiblemente identificación) se permite hacer lo que se tenga permitido.

- La integridad en este contexto, es el proceso de garantizar que la información no cambie. Cuando se firma un mensaje o un documento, no solo es para autenticar el origen del mensaje, si no que también garantiza que el contenido no se podrá modificar.

- La confidencialidad (o privacidad) es simplemente mantener la información en secreto.

- La aceptación es una palabra muy importante que significa que no se puede negar algo que se hizo.

Todos estos servicios se emplean de una u otra forma en la vida diaria. El reto esta en cómo reproducir servicios similares en un mundo electrónico. Las técnicas que se usan para crear análogos electrónicos para estos servicios se basan en la criptografía.

Las aplicaciones iniciales de Internet eran muy débiles en materia de seguridad. De hecho, la mayoría de las aplicaciones, no cuentan con mucha seguridad. Muchas de ellas basan su seguridad en contraseñas. Algunas tienen alguna forma de cifrado, usualmente de la base de datos asociada con la aplicación, pero la mayoría no la tiene. Muy pocas aplicaciones cuentan con opciones de firmas digitales o de aceptación.

En términos generales, el aumento en la seguridad es necesario en la mayoría de las aplicaciones, porque en ellas los datos que se van a procesar tienen algún valor o podría haber algunas repercusiones si la información quedara al descubierto.

Criptografía

La criptografía es la ciencia de aplicar matemáticas complejas para aumentar la seguridad de las transacciones electrónicas. Se basa en problemas matemáticos verdaderamente difíciles. Esta técnica se ha usado desde hace ya varios siglos, actualmente ha tomado gran importancia por la seguridad que integra su uso en los medios electrónicos.

Algoritmos criptográficos

Un algoritmo criptográfico es el conjunto de pasos necesarios para resolver un problema matemático. En el campo de la ciencia de las computadoras, los algoritmos se implementan como partes de un programa que se conoce como una rutina o biblioteca. Algunos, particularmente complejos, se pueden implementar en hardware especializado.

Los algoritmos criptográficos son algoritmos matemáticos y están diseñados de manera que se puedan llamar con diferentes conjuntos de datos para entrar en funcionamiento. Los algoritmos criptográficos son complejos, y en algunos casos, se benefician de un acelerador de hardware para agilizar algunas de las operaciones matemáticas.

En la actualidad la criptografía esta dividida en dos disciplinas: criptología y criptoanálisis.

Los criptólogos son matemáticos e investigadores que se dedican a inventar nuevos algoritmos criptográficos. Después de años de trabajo presentan sus inventos para que la comunidad criptográfica los revise. Es ahí donde aparecen los criptoanalistas; ellos analizan la debilidad del algoritmo y atacan el diseño, en un intento decidido por descifrarlo. Con frecuencia, tienen éxito.

Del resultado de la revisión los criptólogos aprenden algo nuevo sobre como hacer mejores algoritmos y regresan al laboratorio con esta información para crear algoritmos todavía más seguros.

La criptografía se basa en el concepto de que algunos cálculos pueden ser fáciles en un sentido, pero extremadamente difíciles en el sentido contrario.

Además de tener la propiedad de que el cálculo se haga con facilidad en un sentido, pero difícil en el sentido contrario, los algoritmos criptográficos también tienen la propiedad de que son una "trampa". La trampa es una técnica que permite resolver el problema en sentido inverso, en tanto se conozca el secreto.

El cifrado RSA[1] se basa en la factorización de dos números primos. Otros algoritmos criptográficos se basan en problemas matemáticos difíciles y diferentes.

Existen dos clases de algoritmos criptográficos: simétricos y asimétricos. La criptografía simétrica ha existido desde hace mucho tiempo; incluso la usaron los egipcios.

Los algoritmos simétricos y los asimétricos tienen fortalezas y debilidades. Los sistemas criptográficos modernos los usan tratando de explotar la fortaleza de cada uno, sin que hereden los problemas que poseen.

1. Andrew Nash, William Duane, Celia Joseph y Derek Brink, PKI Infraestructura de Claves Públicas página 18.

Las claves son partes importantes de los algoritmos criptográficos, tanto simétricos como asimétricos. Una clave criptográfica es similar a una llave física que se usa para

cerrar o abrir una puerta. Para cada tipo de cerradura existe una llave con una forma específica que se ajusta a aquélla; debe tener una cierta longitud, y unas ranuras para ubicarse en la posición correcta. Por lo general una llave de un fabricante en particular se ajustará a la cerradura de ese tipo, pero solamente si es la llave correcta. La llave apropiada girará y abrirá la cerradura.

Las llaves criptográficas son similares a las llaves físicas de muchas maneras. Cada algoritmo criptográfico necesita una clave con la extensión correcta (en otras palabras, el número correcto de bits). Se puede procesar un algoritmo criptográfico con cualquier clave que tenga la longitud apropiada, pero solo la que tenga el patrón correcto de bits hará que el algoritmo descifre un documento cifrado.

Criptografía simétrica

Los algoritmos criptográficos simétricos toman el texto claro como entrada. Después, usando una clave simétrica, sacan una versión cifrada del texto.

Las claves simétricas son un número aleatorio de la longitud correcta; si el algoritmo simétrico tiene un cifrado simétrico de 40 bits, la clave simétrica tendrá 40 bits de longitud. Si el algoritmo simétrico tiene un cifrado simétrico de 128 bits, la clave simétrica tendrá 128 bits de longitud.

Es muy importante que la clave simétrica se pueda crear con un buen generador numérico aleatorio. El generador numérico aleatorio debería elegir al azar los números distribuidos uniformemente a lo largo del espacio en bits de la longitud de la clave, sin que se presente ninguna desviación hacia o desde determinados valores. Los generadores numéricos aleatorios deficientes tenderán a seleccionar determinados

valores o a descartar otros dentro del espacio de la clave y, como resultado, reducen el número efectivo de bits de la misma. Esto reduce la fortaleza del cifrado.

Los algoritmos simétricos se llaman así porque la misma clave se utiliza para cifrar y para descifrar.

En resumen podemos decir de los algoritmos simétricos que:

- Con la criptografía simétrica, se utiliza la misma clave para cifrar y descifrar.
- El cifrado simétrico es rápido.
- El cifrado simétrico es seguro.
- El texto cifrado que resulta de un cifrado simétrico es compacto.
- Dado que la clave simétrica debe llegar al receptor, el cifrado simétrico está expuesto a ser interceptado.
- La criptografía simétrica requiere una administración compleja de claves.
- La criptografía simétrica no se ajusta a las firmas digitales o a la aceptación.

Criptografía asimétrica

La criptografía asimétrica como la simétrica también requiere de buenos generadores numéricos aleatorios. Cuando se refiere al tamaño de la clave, la situación es más compleja. En general, se requiere de una longitud de clave mayor para lograr el mismo nivel de seguridad que se obtiene con un algoritmo simétrico que utiliza una clave más corta.

Existen pocos algoritmos criptográficos asimétricos y, por lo general, se basan en matemáticas mucho más complejas.

Whitfield Diffie y Martin Hellman fueron los primeros en introducir el concepto de criptografía asimétrica a mediados de la década de 1970. El algoritmo Diffie-Hellman se basa en las matemáticas de logaritmos discretos y, aunque no es tan popular como la criptografía asimétrica RSA, es un algoritmo asimétrico de uso común.

El algoritmo RSA es el algoritmo asimétrico más exitoso; y es el algoritmo asimétrico más estudiado; ha superado muchos ataques a través de su larga vida. La patente fundamental del algoritmo RSA expiró en septiembre del año 2000 y, como resultado, ahora se está incorporando en muchos protocolos como un algoritmo criptográfico asimétrico de carácter obligatorio. En la actualidad, típicamente utiliza claves de 1024 bits y quizá es el algoritmo criptográfico más popular y complejo computacionalmente que se encuentra en uso.

La criptografía de curva elíptica es el siguiente algoritmo asimétrico más reconocido. La ECC[2] ha existido durante un tiempo más corto que el RSA, pero hasta ahora ha resistido los ataques contra el algoritmo. El ECC se encuentra en muchos protocolos como una serie de cifrado opcional y es, tal vez, el algoritmo asimétrico que se debe elegir en aplicaciones que no requieren de gran interoperabilidad. Esto se debe a que el ECC no requiere aceleración criptográfica en la mayoría de las aplicaciones; funciona bien con unidades matemáticas de enteros que se encuentran en todos los procesadores.

Cada algoritmo criptográfico necesita de una clave con un tamaño particular para lograr un cierto nivel de seguridad.

Los algoritmos asimétricos son diferentes a los simétricos en un sentido muy importante. Cuando se genera una clave simétrica, simplemente se escoge un número aleatorio de la longitud apropiada. Al generar claves asimétricas el proceso es más complejo. Los algoritmos asimétricos se llaman asimétricos porque, en lugar de usar

2. Andrew Nash, William Duane, Celia Joseph y Derek Brink, PKI Infraestructura de Claves Públicas página 29.

una sola clave para realizar la codificación y la decodificación, se utilizan dos claves diferentes: una para cifrar, la otra para descifrar. Estas dos claves independientes, pero matemáticamente relacionadas, siempre se generan juntas.

Cuando se completa la generación de una clave asimétrica, hay dos claves: una clave pública y una clave privada. Las claves asimétricas tienen la sorprendente propiedad de que lo que esta cifrado con una sólo se puede descifrar con la otra. Lo interesante de las parejas de claves pública/privada es que una no puede descifrar lo que cifra. Esto permite que cada propietario realice operaciones matemáticas con su clave privada, que nadie más en el mundo pueda realizar. Esta es la base para las firmas digitales y la aceptación.

Sin embargo no todo es bueno, los algoritmos asimétricos son comparativamente lentos, de diez a cien veces más que un algoritmo simétrico con una fortaleza comparable. Esto puede no ser tan grave si se estuviera codificando una receta de cocina, pero si se hablará de un gran proyecto, se convertiría en un gran problema. Otra característica que tienen es que cuando se hacen codificaciones, el tamaño del texto cifrado es mayor que el del texto claro original.

Hashes

Además de la encripción de datos como medida de seguridad para el intercambio de información por medios electrónicos, existe un método que permite corroborar si el documento que se recibe es el que originalmente se envío, y es, la aplicación de un algoritmo hash.

Un algoritmo hash toma la información que se va a enviar y la comprime en lo que se conoce como huella digital o reseña de los datos originales, en si el algoritmo calcula una ecuación con los datos, el resultado es un valor más pequeño que los datos

originales, pero la aplicación de este método tiene la particularidad de que, incluso si se cambia un bit de los datos originales, el valor del hash en el resultado será diferente.

Existen varios algoritmos hash criptográficos. MD2[3] es un hash de RSA que produce una reseña de 128 bits que se optimiza para microprocesadores de baja tecnología de 8 bits. El MD5 también produce una reseña de 128 bits, pero está optimizado para procesadores de 32 bits. El hash SHA-1 también esta optimizado para procesadores de alta tecnología y produce una reseña de 160 bits.

Firmas digitales

Las firmas son algo común: habitualmente firmamos cheques, transacciones con tarjetas de crédito y letras. Una firma digital es la forma electrónica análoga de una firma escrita; identifica al firmante y establece una relación entre éste y los datos firmados. Una firma digital es el resultado de un cálculo matemático con características particulares. Su seguridad se basa en el cifrado asimétrico, en el cual los procesos de cifrado y descifrado usan claves separadas.

El cómputo de una firma digital comienza con el cálculo de un hash de los datos que se firman, después el hash se cifra con la clave privada del firmante; la firma digital evita que el hash sea adulterado. Por consiguiente, una firma digital suministra una prueba sólida de que los datos son los mismos que aparecían cuando se calculó la firma.

3. Andrew Nash, William Duane, Celia Joseph y Derek Brink, PKI Infraestructura de Claves Públicas página 41.

1.3 CERTIFICADOS DIGITALES

En la sección anterior hablamos de las claves públicas y privadas y mencionamos que cuando se lleva a cabo la firma de un documento el remitente hace uso de su clave privada para firmar el documento. Por otro lado, este documento ha sido firmado para ser enviado a alguien y este debe conocer la clave pública que debe usar para tener acceso a la información que le han enviado.

En esencia se puede decir que un certificado digital es la representación digital de lo que en nuestro entorno conocemos como una credencial reconocida cuando menos por la institución que la expide, la cual cuenta con elementos que identifican al poseedor de la misma y la institución que la expide le suministra elementos que garantizan haberla expedido.

Sin embargo para que electrónicamente una identificación sea reconocida, deben existir un conjunto de elementos que avalen la autenticidad, por tal motivo considerando tales elementos se puede decir que un certificado digital es simplemente un documento electrónico que dice "garantizo que esta clave pública está asociada con este usuario en particular". Los certificados presentan en lista quien es el propietario de la clave pública y contienen una copia de la clave pública de ese usuario. Una autoridad de confianza firma la certificación. Se crea un hash para todo el certificado y ese hash queda codificado utilizando la clave privada de la autoridad de confianza.

Para verificar la validez de un certificado digital, todo lo que se necesita hacer es usar la clave pública de la autoridad de confianza para validar la firma del certificado. Si la verificación del certificado es correcta, se puede estar seguro de que la clave pública que está en el certificado pertenece a la persona allí indicada.

Un certificado digital forma una asociación entre una identidad y la pareja de claves pública/privada que posee el propietario de la identidad.

Luego de determinar que una autoridad emisora en particular puede ser de confianza para establecer una identidad, el siguiente paso es producir un documento que se pueda usar para certificar que ha recibido una identidad válida. Un certificado digital es la forma electrónica de este documento. Para uso electrónico, se necesita producir un documento o certificado digital que suministrará suficiente información para permitir que un tercero se sienta con la confianza de que se trata del poseedor correcto de la identidad. Como una analogía de esto podemos mencionar por ejemplo el cobro de un cheque, una persona que cobra un cheque no requiere tener cuenta en el banco para el que se emite, incluso podría no tener cuenta en ningún banco, sin embargo el banco como medida se seguridad debe cerciorarse de que entrega el dinero a la persona que indica el cheque y para esto solicita una "identificación oficial", esto es una identificación que haya sido emitida por una Institución reconocida lo que es similar a la autoridad de confianza, de esta forma el banco realiza la operación solicitada sabiendo que una institución como la Secretaria de Relaciones Exteriores o el Instituto Federal Electoral ha llevado a cabo la autenticación de la personalidad.

A continuación se describe un certificado X.509[4] el cual es un estándar internacional:

Dato	**Descripción del contenido en el certificado digital**
Sujeto	Los nombres y apellidos del individuo o entidad que se van a identificar con el certificado. Se puede incluir información de identificación adicional en el nombre del sujeto o en otros campos específicos del certificado.
Clave Pública	La clave pública corresponde a la clave privada del sujeto.
Expedidor	Identifica la fuente de confianza que generó y firmó el certificado.
Número de Serie	Un número de serie permite que este certificado se identifique como único, incluso si se emite otro certificado con la misma información.
Válido desde	La fecha de iniciación especifica el tiempo desde cuando el certificado se

Dato	Descripción del contenido en el certificado digital
	puede utilizar.
Válido hasta	La fecha final especifica el tiempo máximo hasta cuando el certificado se puede utilizar. Junto con la fecha inicial define el periodo de validez para el certificado.
Uso de clave/ certificado	La información de uso de clave/certificado, describe los usos válidos para la pareja de claves pública/privada del sujeto
Firma digital	La firma digital del expedidor, que se generó utilizando su clave privada, verifica la identidad del sujeto. El valor hash que se utiliza para construir la firma de la Autoridad de Confianza en el certificado permite verificar que el contenido del mismo no haya sido adulterado.

Tabla 1.1 Contenido del certificado X.509

Aunque existen aplicaciones en el mercado que permiten empezar a generar certificados digitales de una manera muy sencilla, la administración de los mismos y las reglas de operación que se establezcan para su uso son finalmente los elementos que permitirán establecer la confianza y credibilidad en los usuarios que se adhieran a los servicios que se proporcionen en la institución que decida utilizarlos. Es por ello que se requiere analizar todo el contexto y lo que involucra una administración de certificados de acuerdo a la cantidad de usuarios y al tipo de operaciones que se desea incorporar a los medios electrónicos, ya que podría resultar contraproducente emitir certificados sin contar con la infraestructura que se requiere para respaldar la operación, y lo único que se conseguiría es afectar el nombre de la institución que los certifica.

4. Andrew Nash, William Duane, Celia Joseph y Derek Brink.PKI Infraestructura de claves públicas. Página 72 y 73

1.4 INFRAESTRUCTURA DE CLAVES PÚBLICAS

Aunque el amplio uso de los mecanismos de tecnología basados en claves públicas es relativamente reciente, la tecnología básica ha estado disponible en diferentes formas durante los últimos 25 años, RSA se desarrolló en 1978 y sigue siendo el algoritmo de clave pública de más amplia difusión y uso en la actualidad.

La criptografía de clave pública suministra las herramientas que permiten operaciones de seguridad, como firmas digitales y distribución de claves. La expansión en el uso de esta tecnología se ha logrado por el conjunto de servicios, interfaces de programación, herramientas administrativas y aplicaciones de usuario que forman una Infraestructura de claves públicas. Aunque la manera de implementar una infraestructura de claves públicas está en evolución, cuenta con una estructura estándar que es reconocible y aceptada.

Inseguridad con el uso de Firmas Digitales

Las firmas digitales son uno de los mecanismos de seguridad más interesantes que se basan en la criptografía de claves públicas, hasta ahora los documentos digitales han carecido de una forma amplia de aceptación que permita certificar el contenido o verificar que este no haya sido modificado durante el viaje. Las firmas digitales soportan este proceso. Una firma digital puede ser empleada solo para efectos de verificación, para revisar que un documento ha sido revisado o firmado y alternativamente para darle a la forma electrónica un estado legal.

El problema es: ¿Cómo saber que la pareja de claves que se usa para cifrar y descifrar realmente pertenece a la persona que se supone firmó el documento?

La creación de una pareja de claves pública/privada es una actividad simple y debido a que los certificados digitales que contiene la clave pública deben estar en un lugar de fácil acceso (por que son públicos) un intruso puede sustituir su clave pública por la clave pública que ya se utilizó para identificar a otra persona y usar la clave privada que

posee para generar una firma. El proceso para verificar la firma dará un resultado correcto y de esta forma se confiará en la firma de manera incorrecta.

Entonces nos damos cuenta de que utilizar simplemente las técnicas criptográficas no es suficiente para permitir el establecimiento de una identidad confiable.

Identidades de confianza

El papel principal de una infraestructura de claves públicas es establecer identidades digitales en las que se pueda confiar y estas se pueden usar con mecanismos criptográficos para prestar un servicio de seguridad como autenticación, autorización o validación de una firma digital, para que los usuarios del servicio puedan tener confianza en que no se les va a engañar.

Encontrar una persona o institución que este preparada para certificar una identidad en la que se pueda confiar, es el problema principal cuando se piensa en la creación de una identidad de confianza. Existen instituciones que aunque no de forma digital realizan procesos de certificación de identidad y entre estas podríamos mencionar a las instituciones que expiden pasaportes, licencias de conducir o tarjetas de crédito, por lo que con esto se puede decir que existen instituciones que tienen la capacidad para establecer identidades y aunque existen algunas expectativas sobre la manera como funcionan las autoridades que expiden identidades, su utilidad estará determinada en base al nivel de confianza que se le otorgue a la autoridad emisora y a la cantidad de pruebas necesarias para establecer dichas identidades. Así mismo se espera que la autoridad emisora de una identidad la expida por un periodo finito y que requiera un proceso de renovación cuando expire su validez.

Autoridades de certificación

La infraestructura de claves públicas es la responsable de certificar identidades y su función no es solo crear certificados digitales y por el hecho de que emite la identidad

se garantiza que esta será usada y se confiará en ella, su labor va más allá, debe desarrollar procesos que verifiquen la identidad de un solicitante que se registra para obtener un certificado y expedir el certificado digital que se puede usar como prueba de esa identidad, ya que estos forman la asociación entre una identidad y la pareja de claves pública/privada. También incluye el personal, los procedimientos de operación, las políticas que definen como se establecen las identidades y cual es la forma de certificado digital que se expide. Una autoridad de certificación esta integrada por varios servicios, los más importantes incluyen un servidor de certificados, una autoridad de registro y un servidor de certificados.

Autoridad de registro

Es la responsable del registro y la autenticación inicial de los solicitantes de certificados digitales y sus servicios pueden incluir también la revocación de certificados. Una Autoridad de registro y sus interfaces se pueden implementar como parte de un servidor de certificados.

Autoridad certificadora

Es el servicio responsable de expedir los certificados con base en la información suministrada en el proceso de registro. La clave pública se combina con otra información de identificación y la estructura del certificado resultante se firma con la clave privada de la autoridad de certificación.

Servidor de certificados

Los certificados y las claves públicas deben estar disponibles para el público antes de que puedan entrar en funcionamiento, por lo que el repositorio será el sitio usual en el que se publiquen los certificados.

Aspectos de la infraestructura de claves públicas

Una Infraestructura de Claves Públicas cuenta con los componentes y servicios que permiten la operación de un sistema que usa certificados digitales. Debe manejar aspectos como:

- Creación segura de buenas claves.
- Validación de identidades iniciales.
- Expedición, renovación y conclusión de certificados.
- Validación del certificado.
- Distribución del certificado.
- Almacenamiento seguro de claves.
- Generación de firmas y registro de hora.
- Establecimiento y administración de relaciones de confianza.

Para tener éxito la infraestructura debe convertirse en un sistema bien integrado a las aplicaciones de las instituciones. Las áreas críticas que se deben abordar incluyen:

a) Facilidad de uso.

b) Transparencia de la estructura para las aplicaciones y los usuarios que confían en sus servicios.

c) Integración con las aplicaciones y una amplia interoperabilidad entre componentes y aplicaciones de la infraestructura.

1.5 DOCUMENTOS EN LA INSTITUCIÓN

Una de las labores indispensables para la existencia del gobierno es sin duda la recaudación de impuestos, ya que todos los recursos económicos que servirán para el desarrollo del país, las obras públicas y los servicios con los que cuenta una sociedad se obtienen de ahí y aunque a nadie le agrada pagar impuestos, estos son necesarios para proveer los servicios que requieren las sociedades.

Con el paso del tiempo, los métodos de recopilación de impuestos han evolucionado. En la actualidad, el apoyo de la tecnología es ya una necesidad para el manejo de la gran cantidad de información que se mueve en las grandes ciudades, y en nuestro país el Servicio de Administración Tributaria que es la institución que se encarga de hacer esta tarea, ha incorporado paulatinamente procesos automáticos para llevar a cabo la recaudación de impuestos y toda la información relacionada con este tema.

Con la tendencia de la tecnología se observa que pasar de los documentos en papel a los documentos electrónicos es un paso inevitable, pero antes de hacerlo es necesario tomar en cuenta una serie de consideraciones que ayudarán a clarificar el proceso, ya que de otra forma se complicaría más que seguirlo haciendo en papel.

Con el propósito de promover una administración tributaria más eficiente que fortalezca la recaudación, impulse la fiscalización, aumente la presencia fiscal, diversifique los controles y amplíe las fuentes de información, se expidió la Ley del Servicio de Administración Tributaria misma que entró en vigor a partir del 1 de julio de 1997 y lo que en un tiempo se llamó "carga fiscal", es ahora una contribución, una colaboración humana para que México cuente con escuelas, hospitales, higiene, comida, habitación, caminos, servicios públicos y fundamentalmente progreso.

Para seguir en este camino se deben tomar decisiones en las que el centro político deberá basar su fortaleza, en la cobranza amplia y generalizada y sobre todo equitativa de impuestos y si el tiempo apremia el apoyo tecnológico resulta necesario.

El Servicio de Administración Tributaria realiza una serie de procesos para poder recaudar impuestos, en primer lugar debe identificar al contribuyente y para esto existe un proceso de alta, en este proceso se identifica el tipo de actividad que se realiza o bien el giro en el que se ubica la actividad y en base a esto y de acuerdo al ingreso obtenido se calculan los impuestos a pagar, así mismo con el alta ante la Secretaría de Hacienda y Crédito Público se expide la denominada cédula fiscal. Con este documento ya se puede llevar a cabo la facturación o bien la expedición de recibos de honorarios. Una de las actividades que los contribuyentes pueden realizar ante los trámites de pagos de impuestos es la deducción de impuestos mediante la presentación de facturas que tengan relación con el tipo de actividad identificado en el alta, explicar todo el proceso sale del alcance de este trabajo, por lo que solo menciono esto para explicar un poco el panorama e identificar parte de las actividades que se llevan a cabo para la emisión de documentos.

Actualmente la emisión de documentos aún se entregan en papel y alternativamente esta opción difícilmente dejará de existir sin embargo se requiere que el papel solo sea utilizado en casos extremos.

Los documentos que se reciben en papel posteriormente son capturados por personal de las Administraciones Locales de Recaudación que se ubican en diferentes puntos de la República Mexicana y este proceso trae como consecuencia errores de captura, por lo que el reto para el SAT es llevar a cabo esta actividad por medios electrónicos, que sea el contribuyente mismo quien capture su información y llegar incluso al proceso de facturación, y para ello la institución tiene que asegurarse de que recibe la información del contribuyente que previamente identificó en sus instalaciones y de quien ya tiene información.

Aunque son muchos los documentos que maneja el SAT, el concepto de incorporarlos a los medios electrónicos será el mismo para todos y es por ello que no resulta importante mencionar cada uno de ellos, si no más bien su manejo en general y los problemas que

están ocasionando, como se van a resolver estos y como se va a asegurar la información, esto es precisamente lo que mencionaremos en el siguiente capítulo.

De esta manera, hasta este momento hemos descrito algunos de los métodos de intercambio de información que actualmente se están utilizando, y como hemos podido darnos cuenta, determinar que tanta seguridad o no debemos considerar en nuestros procesos dependerá más bien de la importancia que tenga la información, por lo que cada caso debe analizarse y definir el mejor método para su protección. En el siguiente capítulo analizaremos la problemática que vive el SAT con el intercambio de documentos y en base a los métodos analizados identificaremos cual de ellos le conviene utilizar, los elementos que deberá considerar para su implementación y el proceso que deberá de seguir.

CAPÍTULO 2

NIVEL DE SEGURIDAD Y PROCESOS REQUERIDOS

Para determinar el nivel de seguridad que se requiere en un sistema de información es necesario analizar las necesidades que se tienen y determinar la importancia que tiene el contar con información integra, confidencial y confiable, solo de esta forma se podrán considerar los elementos necesarios para alcanzar el objetivo deseado al integrar los aspectos de seguridad que se requieren.

En este capítulo se describirá la problemática que se presenta actualmente con los procesos empleados para la recepción de documentos electrónicos, se analizarán los requerimientos que se deben cubrir para llevar a cabo un control adecuado en la recepción de trámites y documentos por medios electrónicos, considerando sobre todo que los procesos deben contar con mecanismos seguros que proporcionen confianza en su uso, y en base a este análisis se identificará el nivel de seguridad que debe implementarse, los procesos a incorporar y los elementos que se deben considerar para su implementación.

2.1 SITUACIÓN ACTUAL

El Servicio de Administración Tributaria desde hace tiempo ha detectado que la tecnología informática es una herramienta que le permite agilizar procesos y se ha beneficiado del control de información con el uso de sistemas, por ello continuamente incorpora procesos automatizados que apoyen y mejoren la atención a los contribuyentes.

Con la finalidad de proporcionar al contribuyente procesos que agilicen la entrega de trámites y que además aseguren el viaje de los datos de un punto a otro, en el año de 1999 se incorpora un proceso que permitiría llevar a cabo intercambio de información por medios electrónicos utilizando certificados digitales, con este proceso además de agilizar los tiempos de entrega, reducir considerablemente el uso de papel e incorporar medidas de seguridad confiables dejaba la responsabilidad del uso de contraseñas en el contribuyente, es decir, el SAT no conservaría en ningún lugar la contraseña del contribuyente.

El arranque del proceso inició con la entrega de declaraciones electrónicas para grandes contribuyentes, al principio solo se consideraron cinco mil grandes contribuyentes y paulatinamente se ha ido incorporando al resto llegando actualmente a ser alrededor de quince mil. Otro proceso que se incorporó bajo este esquema es el de dictámenes fiscales el cual esta dirigido también a grandes contribuyentes. El siguiente paso es incorporar al proceso de entrega de declaraciones electrónicas al total de los contribuyentes los cuales hacienden a más de ocho millones, siendo estos solo los que cuentan con un registro federal de contribuyentes registrado en la institución.

Generación de certificados digitales

Para la emisión de certificados digitales se adquirió un software para el que además de renovar año con año el uso de las licencias se debe pagar una cuota por cada certificado digital generado y aunque actualmente se atiende a quince mil contribuyentes los certificados generados ya rebasan los cien mil, esto debido a que los contribuyentes constantemente olvidan o comprometen la contraseña de su llave privada y requieren nuevos certificados.

La generación de certificados digitales esta a cargo de la institución y las solicitudes se reciben en las Administraciones Locales de Recaudación (ALR) que se encuentran en toda la república mexicana, para recibir una solicitud de generación de un certificado el contribuyente debe acudir a la ALR que le corresponde con documentos que acrediten su personalidad y con el archivo de requerimiento que contiene los datos generales del contribuyente, la cuenta de correo a la que se le deberá enviar el certificado digital y la llave pública. Este archivo es generado utilizando la aplicación monousuario que para este fin el contribuyente puede obtener de la página web de la institución y con la cual también obtendrá la llave privada. Para solicitar la generación del certificado digital, quien atienda al contribuyente deberá:

- Verificar que los documentos estén completos y se presenten en original y copia.
- Acreditar que la foto de la identificación oficial que se presenta corresponde al contribuyente ahí presente.
- Revisar que la información que contiene el archivo de requerimiento concuerda con los datos que tiene registrados la institución.

- Constatar que si el contribuyente desea obtener un certificado a nombre de una empresa, el acta constitutiva que presenta lo mencione como representante legal.

- Obtener la firma del contribuyente en formato libre o en el formato diseñado para ello en el que esta de acuerdo en que el uso del certificado que solicita tiene la validez de una firma autógrafa y que es su responsabilidad el correcto uso del mismo.

- Solicitar la generación del certificado digital, cuando las condiciones anteriores se hayan cumplido e indicar al contribuyente que el certificado digital se lo entregarán en la cuenta de correo que proporcionó en la solicitud en un lapso no mayor a 48 horas.

El proceso de generación de un certificado digital se lleva a cabo de la siguiente manera:

- En la ALR se deposita en la aplicación cliente el archivo de requerimiento que contiene los datos generales del contribuyente y la llave pública.

- Se solicita desde la aplicación cliente la generación del certificado digital, si hay comunicación con el Centro de Procesamiento Nacional (CPN) se transfiere el archivo de requerimiento al directorio del servidor que recibe las solicitudes de las sesenta y seis Administraciones Locales de Recaudación.

- El archivo de requerimiento es renombrado antes de transferirse utilizando el RFC del contribuyente y una contraseña que se genera en el momento de la solicitud.

- Una vez al día se procesan las solicitudes, para esto primero se revisa que las solicitudes no estén duplicadas, posteriormente se verifica que el solicitante no tenga certificados activos y finalmente las solicitudes que hayan

cumplido con las verificaciones se guardan en un disco flexible para su generación.

- Las solicitudes son llevadas en disco flexible al servidor de la Autoridad Certificadora la cual se encuentra fuera de la red, se transfieren los archivos al directorio de proceso y se solicita la generación de los certificados con dos años de vigencia.

- Se extraen de la Autoridad Certificadora los certificados digitales y se colocan en el servidor que se encargará de su publicación y distribución.

- Se solicita la publicación y distribución de certificados digitales. El proceso de publicación se encarga de dejar disponibles los certificados digitales desde la página web del SAT. El proceso de distribución se encarga de enviar vía correo electrónico el certificado digital a los contribuyentes.

Revocación de certificados digitales

Dentro de la administración de los certificados digitales además de la generación se realiza también la revocación de certificados la cual se solicita igualmente en la ALR por el contribuyente para el que se expidió el certificado y tiene como objetivo cancelar el uso de un certificado, el motivo de cancelación puede variar, sin embargo es frecuente una revocación porque no se recuerda la contraseña de la llave privada o esta se encuentra comprometida; es decir, la contraseña es conocida por un tercero, además las empresas que han dejado de tener trato laboral con su representante legal solicitan la revocación.

La solicitud de revocación de certificados digitales se realiza vía correo electrónico y la atención a una solicitud no debe ser mayor a cuarenta y ocho horas, sin embargo este tiempo varía dependiendo de la demanda, la cual se incrementa en las fechas límite de entrega de documentos en las cuales se reciben hasta dos mil solicitudes por día.

La revocación de un certificado digital se lleva a cabo de la siguiente manera:

- El contribuyente entrega en la ALR que le corresponde el documento en el que solicita la revocación e indica el motivo.
- El servidor público que atiende al contribuyente envía correo electrónico a la cuenta establecida para tal fin, solicitando la revocación e indicando claramente el RFC del solicitante, el motivo de la revocación y el número de documento en que sustenta la petición.
- El área encargada de la atención de estas solicitudes revisa constantemente las peticiones y para cada una de ellas verifica que el certificado a revocar este vigente.
- Informa para cada solicitud vía correo electrónico el resultado de la solicitud.

Varias de las actividades que se realizan tanto en el proceso de generación como en el de revocación se realizan de manera manual.

Recepción de documentos electrónicos

Los trámites que actualmente se reciben por medios electrónicos son declaraciones electrónicas y dictámenes fiscales y el proceso que se sigue es el siguiente:

- El contribuyente obtiene de la página de la institución el formato electrónico para el llenado de información correspondiente a cada trámite, el cual se recomienda llenar sin conexión a red.
- El contribuyente incorpora la información que corresponda al formato del trámite que desea realizar.

- El contribuyente obtiene de la página de la institución la aplicación que le permite incorporar el archivo del trámite a enviar y su firma digital.
- El contribuyente envía desde la página de la institución el archivo que contiene su trámite firmado.
- La institución recibe los trámites y los coloca en el servidor de atención a trámites electrónicos.
- El personal del área encargada de verificar los documentos electrónicos realiza procesos manuales para validar la firma e integridad del documento y verificar la vigencia del certificado.
- Si durante el proceso de verificación se detecta alguna anomalía se notifica al contribuyente y se rechaza el documento.

Problemática

La descripción de la situación actual a simple vista parece no presentar graves problemas, desafortunadamente los hay y se prevee que aumenten considerablemente si se pretende incorporar al resto de los contribuyentes bajo este mismo esquema.

A continuación se describirán los problemas que se han detectado en cada uno de los procesos que operan actualmente.

Generación de certificados digitales

- El software con el que se generan los certificados digitales no se apega a los estándares internacionales y esto no permitirá en un futuro integrar la utilidad de un certificado digital con otras instituciones.
- El uso de procesos semi-automatizados retarda la atención de las solicitudes.

- Actualmente la atención a quince mil contribuyentes rebasa la capacidad de atención que tiene el personal asignado a esta actividad, por lo que se prevé un desbordamiento inminente al incorporar a los ocho millones restantes.

- La probabilidad de duplicar una llave pública se incrementa al aumentar la cantidad de certificados generados y no existe manera de detectar en línea esta situación, por lo que una verificación manual no será operable.

- Las fallas de comunicación no las reporta el sistema por lo que aun cuando aparentemente se envía una solicitud, esta no llega ocasionado retraso en los trámites y molestia en los contribuyentes.

Revocación de certificados digitales

- La atención de las solicitudes en fechas límite de entrega rebasa la capacidad de atención, ya que en días normales la respuesta se entrega en un promedio de veinticuatro horas y en esta situación se eleva a siete días hábiles, generando molestia en el contribuyente.

- Recibir las solicitudes vía correo electrónico requiere personal dedicado de tiempo completo y además en fechas límite de entrega las solicitudes se duplican constantemente ocasionando un mayor retraso en la atención.

- La recepción de los datos que se requieren para procesar la solicitud no se apegan a un formato estándar, por lo que quien revisa debe atender una a una cada solicitud.

- La falta de un proceso automatizado además de retrasar la atención propicia la equivocación en el proceso.

- La verificación de la existencia de un certificado activo se lleva a cabo de forma manual.

- El retraso en una solicitud puede ocasionar la recepción de documentos firmados entre el periodo de atención, aún cuando el contribuyente haya solicitado la revocación para evitar precisamente esta situación.

Recepción de documentos electrónicos

- Las operaciones de verificación se realizan de manera manual, por lo que un incremento en la recepción provocará un retraso considerable en la atención y se perderá oportunidad en la atención.

- La falta de oportunidad en los procesos de revocación y recepción de documentos puede ocasionar la aceptación de documentos firmados con certificados que momentos después se encuentren revocados aun cuando la solicitud de revocación se haya recibido primero.

2.2 NECESIDADES DEL SERVICIO

Ante la problemática descrita, es claro que existe un problema en la administración de los certificados digitales y que esto ha traído como consecuencia vulnerabilidad en el proceso de recepción de documentos vía electrónica, ya que aún cuando al contribuyente se le deja la responsabilidad del control de su contraseña y esto permite deslindar a la institución del uso que el contribuyente le da, lo que no puede es olvidar que tiene que proporcionar un servicio de calidad en el que va implícita la seguridad de la información.

Para abordar desde una visión general el objetivo que se pretende alcanzar al permitir que el contribuyente entregue documentos por medios electrónicos, detectar los elementos que requiere para proporcionar la confianza en el uso de este servicio y poder entonces determinar los procesos que se deben incluir, a continuación se describirá cada uno de estos rubros en el orden en que se mencionaron, esperando al

final de esta sección contar con la información necesaria para determinar el nivel de seguridad que se recomienda implementar.

Entrega de documentos por medios electrónicos

El SAT tiene como objetivo fortalecer la recaudación de impuestos, para esto requiere optimizar los procesos que desde los diferentes ámbitos que maneja se llevan a cabo para este fin y además debe controlar toda la información que en torno a esta actividad se genera.

Desde esta perspectiva y viviendo en la era de la información resulta sensato pensar que se puede aprovechar la tecnología informática para recibir trámites por medios electrónicos, pero, ¿porqué y para qué en esta forma?, esto se explica a continuación.

La entrega de documentos por medios electrónicos tiene como objetivo:

- Permitir que el contribuyente use la red pública para entregar sus trámites ante la institución en cualquier momento del día.
- Reducir el uso de papel y la captura de formatos.
- Disminuir errores de captura, al permitir que el contribuyente llene formatos electrónicos con su información.
- Agilizar la integración de los datos del contribuyente en los sistemas de la institución.
- Usar este medio como un mecanismo de entrega con validez legal.
- Integrar el total de trámites en este proceso.
- Compartir en un futuro información con otras instituciones.

- Implementar el proceso con las medidas de seguridad necesarias para garantizar la correspondencia contribuyente/documento.
- Integrar procesos que aseguren la veracidad del documento.

Requerimientos para la entrega de documentos

Además de las necesidades detectadas en la descripción de la problemática, existen una serie de requerimientos que se deben cubrir para cumplir con el objetivo que se persigue y proporcionar la funcionalidad adecuada al sistema, en base a los requerimientos se determinarán los elementos necesarios para su atención y se tendrá una idea clara de la magnitud del proyecto y tomando en cuenta esto se presentará el modelo para resolver la situación.

A continuación se describirán los requerimientos principales que ayudarán a alcanzar el objetivo de utilizar los medios electrónicos para la entrega de trámites y documentos incluyendo en un segundo nivel requerimientos de sistema que deben tomarse en cuenta.

Requerimientos Funcionales

1. Contar con un sistema que administre en línea certificados digitales, que sea de alta disponibilidad y que concentre la información en el Centro de Procesamiento Nacional (CPN).
    - Para la administración en línea se requiere contar con los elementos y procesos necesarios para una infraestructura de clave pública.
    - Para contar con alta disponibilidad es necesario replicar los procesos en línea al Centro de Procesamiento Alterno (CPA).

- La concentración de la información en el CPN, requiere de mecanismos de comunicación confiables con las administraciones locales de recaudación.

2. Autorizar la generación de certificados a los usuarios que estén autenticados ante la institución.

    - Antes de llevar a cabo la generación de un certificado se verificará en el sistema institucional que el contribuyente cuente con la autenticación correspondiente.

3. El certificado digital estará publicado en la página web de la institución.

    - Se creará árbol de directorios en servidor disponible para la red pública para almacenar cronológicamente certificados digitales por contribuyente, dando la posibilidad de obtener una copia de los mismos desde este lugar.

4. Desde la página web de la institución y desde las ventanillas de atención de las administraciones locales de recaudación se contará con la posibilidad de renovar y revocar certificados digitales.

    - Para llevar a cabo el proceso de renovación será necesario firmar digitalmente el archivo de requerimiento con un certificado digital vigente.

    - La verificación de la validez de la firma y vigencia del certificado digital deberá realizarse en línea.

    - Para realizar la revocación de certificados será necesario proporcionar la clave de revocación correspondiente, si no se cuenta con ella se deberá solicitar el trámite por escrito y acreditar la personalidad del solicitante, por lo que el proceso podría llevarse hasta 30 minutos.

5. El certificado digital deberá ser entregado en el momento de la solicitud si por alguna causa esto no fuera posible y el trámite queda pendiente se le dará una respuesta al usuario por correo electrónico.

6. Realizar revocación automática de certificados que han expirado.

    - Desarrollar aplicación que se active periódicamente y que establezca el estado de revocación a los certificados que han vencido su periodo de vigencia.

7. Aceptar desde la página web de la institución documentos firmados que cumplan con la verificación y validación del documento y certificado digital.

    - Verificar mediante la aplicación de algoritmos hash la integridad de la información.

    - Verificar en línea la validez del certificado digital con el que se firma el documento.

    - Determinar con el área responsable del seguimiento al tramite o documento, los criterios mínimos para la aceptación o rechazo del documento.

8. Contar con una aplicación que permita conocer la situación de cada trámite que por alguna causa este pendiente.

    - Desarrollar aplicación administrativa que refleje el seguimiento y la situación actual de los trámites pendientes.

    - Mantener el acceso disponible a esta aplicación desde las administraciones locales de recaudación.

Requerimientos No Funcionales

1. Desarrollar el sistema con personal interno utilizando herramientas institucionales.

    - Una vez definidos los módulos del sistema, establecer el flujo y las prioridades determinarán la cantidad de personas que integrarán el equipo de trabajo para el desarrollo del sistema.

    - El desarrollo se llevará a cabo utilizando como base de datos Infomix y como herramientas de desarrollo, Visual C++, C y Java.

2. Autenticar la personalidad de los usuarios con documentación oficial y complementar la información de los usuarios con datos biométricos.

    - La documentación e identificaciones oficiales, así como los datos biométricos formarán el conjunto de datos que determinarán la autenticación de los contribuyentes.

    - Un agente certificador se encargará de revisar documentos e identificaciones y de tomar los datos biométricos proporcionando su visto bueno en la base de datos institucional para considerar con esto la autenticación del contribuyente.

3. Generar certificados digitales bajo estándares internacionales permitiendo que el usuario tenga el control y la responsabilidad del uso de su contraseña, dando a cada certificado una vigencia de dos años.

    - Utilizar criptografía asimétrica y pedir solo la llave pública al contribuyente para generar el certificado digital.

    - Utilizar el formato X509.v3 para la información que se incluirá en el certificado digital.

4. Los usuarios deberán solicitar el certificado digital la primera vez y las veces que se requiera su presencia física en la Administración Local de Recaudación que le corresponda.

5. El usuario entregará documento firmado en el que acepta hacer uso del certificado digital asumiendo la responsabilidad por el manejo que se le de y aceptando que su uso es equivalente al de una firma autógrafa.

De acuerdo al objetivo que se persigue y a los requerimientos que se deben cubrir para el cumplimiento de los mismos, el panorama deja ver que este es un proyecto en el que se verán involucradas varias áreas, por tal motivo el enfoque en la propuesta se centrará solo a resolver lo que se considera es la esencia del problema, la seguridad y en el capítulo cuatro se mencionarán actividades adicionales que se deben integrar para complementar el ciclo de todo el proceso.

2.3 IDENTIFICACIÓN DEL NIVEL DE SEGURIDAD

Ahora se verán los puntos clave que requiere la institución para asegurar la información, se determinará el nivel de seguridad que requiere y los motivos por los que se propone.

Elementos de seguridad que se requieren:

- Documentos electrónicos que incorporen mecanismos que sustituyan el uso de firma autógrafa.

- Responsabilidad en el uso de contraseñas del lado del contribuyente.

- Generación de certificado digital con entrega del requerimiento que contenga solo la llave pública del contribuyente.

- Verificación de integridad de los documentos que se reciben.

- Identificación de la correspondencia contribuyente/documento.

- Integrar al sistema institucional información que identifique de manera única al contribuyente.

Nivel de seguridad

Considerando los elementos que se acaban de listar y tomando en cuenta la descripción de los elementos que se utilizan para el intercambio de información por medios electrónicos que se citaron en el capítulo uno, se puede ver que el que más se apega a los requerimientos es la implementación de una infraestructura de clave pública, ya que difícilmente se le podría entregar un token (prenda de autenticación) a los contribuyentes ya que el control de un bien aún siendo tan pequeño rebasaría las actividades y capacidades de la institución para su administración, por otro lado la asignación de contraseñas individuales además de dejar vulnerable el trayecto de la información se prestaría a la desconfianza del proceso por el hecho de que hay quienes piensan que personal de la institución puede conocer las claves y manipular la información, así mismo el comparar algún dato biométrico para entregar información además de propiciar la compra masiva de equipo especializado para realizar esta actividad no permitiría verificar que el documento que entrega realmente contiene información del contribuyente, por lo que la opción que más satisface los requerimientos tanto de operación como de seguridad es la implementación de una infraestructura de clave pública.

Motivos de la propuesta

Implementar una infraestructura de clave pública permitirá:

- Dejar en manos del contribuyente la creación del par de llaves, tanto la pública como la privada y lo dejará como responsable del uso que se le de a la contraseña que proporciona para firmar documentos con su llave privada.

- Utilizar certificados digitales con los cuales se podrán firmar documentos electrónicamente y ser el equivalente a una firma autógrafa.
- Incorporar un proceso de autenticación de personalidad que permitirá vincular la correspondencia contribuyente/certificado.
- Controlar la administración de los certificados digitales y evitar el pago a terceros por este servicio.
- Incluir mecanismos que verifiquen la veracidad de los certificados digitales y la de los documentos que se entregan.
- Integrar paulatinamente la entrega de trámites y documentos.
- Llevar a cabo operaciones con otras instituciones.

Parece ser que los motivos además de ser convincentes resuelven los requerimientos planteados y para llegar a cubrir estas características es necesario implementar la infraestructura de tal forma que se cubran los procesos completos de manera automatizada.

2.4 PROCESOS REQUERIDOS

Ahora se describirán los procesos que se deben considerar para implementar la infraestructura de clave pública, estos procesos deben satisfacer los requerimientos y permitir una adecuada operación.

Definición de los elementos que componen la infraestructura

Aunque este es un proceso en el que intervienen tanto elementos de seguridad como decisiones institucionales, se mencionará por la importancia que tiene dentro de la

funcionalidad de la infraestructura y se realizará una propuesta la cual en su momento deberá contar con los ajustes que se consideren necesarios.

Este proceso consiste en definir quien realizará las actividades que cada elemento de la infraestructura llevará a cabo. Para tal fin, se presenta una propuesta en la que se describe quien debe asumir el papel y la razón por la que así se considera.

Elemento	**Función Principal**	**Personalidad**	**Razón**
Autoridad Certificadora	Representa a la autoridad de confianza y es quien certifica los certificados digitales con su firma.	Servicio de Administración Tributaria	Representa a una institución seria y reconocida a nivel nacional con una función clara.
Autoridad Registradora	Autentica electrónicamente a los solicitantes de certificados digitales y administra los procesos que requieren los certificados digitales.	Centro de Procesamiento Nacional	Las funciones que realiza, el equipo con el que cuenta y las características del personal que ahí labora.
Agente Certificador	Autenticar físicamente la personalidad de los solicitantes de certificados digitales,	Personal de las administraciones locales de recaudación.	Es el personal que atenderá directamente a los contribuyentes.

Tabla 2.1 Elementos de la Infraestructura de Clave Pública

Generación del par de llaves

Este proceso consiste en proporcionar al contribuyente una aplicación en la que tenga la posibilidad de generar su llave privada y pública sin necesidad de hacerlo en las oficinas de la institución.

Elementos a considerar:

- La aplicación deberá desarrollarse para ambiente windows.
- Deberá contar con ayuda en línea que guíe la generación.
- Los números de las llaves deberán ser aleatorios.
- La aplicación se ejecutará en modo monousuario.
- Las llaves deberán generarse usando criptografía asimétrica.
- La aplicación deberá indicar claramente la responsabilidad que tiene con su contraseña y le recomendará generar su par de llaves en un equipo seguro y fuera de red.
- La aplicación estará disponible para bajarse desde la página web.

Autenticación de personalidad

La autenticación debe darse en dos etapas, la primera de ellas consiste en verificar la personalidad del contribuyente físicamente, es decir, tendrá que presentarse personalmente ante un agente certificador para que certifique su personalidad y la otra etapa es verificar electrónicamente que la entrega de un trámite o documento lo hace la persona que la institución identificó y a la cual reconoce por medio de una firma digital.

El primer proceso es uno de los más delicados, ya que consiste en avalar que la persona que solicita un certificado digital es quien dice ser y para corroborar esto al solicitante se le pide acuda con documentos oficiales que lo identifiquen y que incluyan fotografía para comparar físicamente el parecido, dentro de los requerimientos solicitados se pide además que se incorporen datos biométricos del solicitante a fin de identificar de manera única a la persona. En este proceso es muy importante contar con personal responsable que realice a conciencia esta actividad.

El segundo proceso tiene que ver con el reconocimiento y correspondencia de información entre el contribuyente que entrega un trámite o documento firmado y el registro de sus datos en el sistema.

Elementos a considerar:

Para verificar que el contribuyente es quien entrega un trámite o documento, lo que se considerará es la firma electrónica, además para todo trámite la institución solicita se proporcione el RFC, lo cual es un elemento más que servirá para verificar la correspondencia, para poder firmar, el contribuyente hará uso de su certificado digital y por consiguiente de su llave privada con la cual tendrá que usar la contraseña que solo el conoce, por lo que, al recibir el documento se deberá llevar a cabo el proceso de obtener el número de serie del certificado y con el verificar que este exista entre la información de los certificados digitales emitidos y que corresponda con el RFC que se indica, al identificar el certificado, extraer la llave pública y compararla con la que se entrega en el documento firmado, si existe correspondencia se puede considerar que el contribuyente correcto esta entregando la información.

Generación de certificado digital

Este proceso consiste en generar el certificado digital certificando la personalidad de quien lo posee y depositando la confianza para operar dentro de las actividades que tiene permitidas en la infraestructura de clave pública.

Elementos a considerar:

- Antes de generar el certificado se debe verificar que el contribuyente cuenta con autenticación física y que se han incluido sus datos biométricos.
- El formato del certificado deberá estar dentro del estándar internacional X.509.
- El proceso de generación deberá llevarse a cabo considerando los elementos de seguridad y disponibilidad necesarios para evitar comprometer la llave privada de la autoridad certificadora.

Administración del certificado digital

Este proceso consiste en llevar a cabo las actividades que le dan vida y utilidad al certificado digital, el control adecuado de las mismas darán la certidumbre al proceso y la confianza a los contribuyentes, sus actividades principales serán las siguientes:

Generar.- consiste en generar el certificado digital considerando vincular unívocamente a un certificado con un contribuyente.

Revocar.- consiste en invalidar el uso de un certificado digital a petición del propietario.

Cancelar.- consiste en invalidar el uso de un certificado a petición de una autoridad por causas que ponen en riesgo la credibilidad en las operaciones.

Publicar.- consiste en hacer públicos los certificados digitales y dejarlos disponibles para el público en general.

Verificar.- consiste en recibir un documento firmado electrónicamente y determinar si procede o no la recepción del mismo, al comprobar la autenticidad del certificado utilizado y la integridad del documento que se envía.

Esta es solo una breve descripción de las actividades básicas que se deben realizar en la administración de certificados digitales, cada autoridad certificadora deberá emitir los

criterios que utilizará para llevar a cabo cada una de ellas y determinar quien, como y donde se podrán llevar a cabo.

Debido a que en la determinación de las reglas de operación deben tomarse en cuenta las necesidades de las áreas que estarán involucradas y en si las necesidades de la institución, es necesario que áreas normativas definan estos puntos y los incluyan como parte de los requerimientos para que sean considerados en los procesos de sistematización.

Recepción de trámites y documentos

Este proceso consiste en llevar a cabo las actividades necesarias para asegurar que el documento que se recibe es el que se envío originalmente, es decir, que no ha sido modificado por alguien en el trayecto, que la persona que lo envía esta reconocida dentro de la infraestructura y que la firma digital la realizó con un certificado válido.

Elementos a considerar

- Debe proporcionarse una aplicación que le permita al contribuyente firmar documentos digitalmente.
- Se deben generar las reglas de operación que proporcionen las restricciones para aceptar o rechazar un documento.

En este capítulo se ha presentado el panorama de una problemática que desafortunadamente es constante en la implementación de sistemas, los análisis de información y más aún el de los requerimientos se hacen al vapor, restándole a esta actividad la importancia que tiene, y los resultados al final son desastrosos, trayendo como consecuencia un mal servicio, el disgusto de los usuarios y el desgaste de las áreas de sistemas y además se proporcionan elementos para que se piense incluso que los sistemas no sirven y todo porque el sistema que tanto se anunció traería grandes beneficios, lo que trajo fueron problemas.

Los sistemas no son el problema, una falta de visión y un entendimiento global de lo mínimo que se debe incorporar en un sistema para que este sea realmente funcional, es lo que, las personas que solicitan servicios de automatización no están acostumbradas a analizar y por lo tanto no lo piden en sus requerimientos, pero es también responsabilidad de quienes coordinan la automatización de los proyectos informar sobre la problemática que se presentará al operar sin considerar procesos necesarios para una correcta funcionalidad y para obtener un real beneficio, y no conformarnos con hacer lo que el cliente pida, porque aunque es quien va a pagar, seguramente pagaría más si se le hace ver que es necesario incluir procesos que probablemente ni siquiera había considerado.

CAPÍTULO 3

MODELO PARA EL INTERCAMBIO DE DOCUMENTOS

Ya que conocemos la problemática que se vive en la institución y se han analizado algunas formas de proteger información usando medios electrónicos, e incluso se ha definido el esquema que resolvería en gran medida la situación, es tiempo de mostrar el modelo y explicar los motivos por los que se propone, así como el detalle de los procesos más relevantes, los productos que deben generarse y la forma en que estos operarán dentro del proceso general.

Es importante recordar que el éxito del modelo depende de la automatización de los procesos y de la implementación de los requerimientos mínimos, ya que de otra forma se estaría cayendo nuevamente en la misma situación de tener procesos semiautomatizados solo que ahora en una mayor escala, lo cual traería como consecuencia un agravamiento de la situación actual.

3.1 PRESENTACIÓN DEL MODELO

De acuerdo a la problemática que vive la institución y a la identificación del proceso que debe implementar como resultado del análisis que se realizó en el capítulo dos, en primer lugar describiremos cada uno de los elementos que forman parte del modelo propuesto y el rol que jugará cada uno de ellos.

Contar con una infraestructura de clave pública, requiere de un conjunto de elementos que darán soporte para una correcta operación, a continuación se señalarán cada uno de los elementos, quien en la institución tomará ese rol y cual será su actividad principal.

Elementos de la Infraestructura de Clave Pública

Elemento	Figura	Actividad Principal
Autoridad Certificadora	Servicio de Administración Tributaria	Generar certificados digitales avalando la correspondencia entre un certificado digital y un contribuyente
Generador del par de llaves	Aplicación	Permitir al contribuyente obtener la llave pública y la llave privada.
Autoridad Registradora	Centro de Procesamiento Nacional	Recibir las solicitudes de generación de certificados digitales, procesar los controles y verificaciones que se requieran antes de solicitar la generación del certificado digital.
Autenticación	Proceso	Revisar, obtener e integrar los elementos que identificarán de manera única la personalidad del contribuyente.

Elemento	**Figura**	**Actividad Principal**
Agente Certificador	Personal de las Administraciones Locales de Recaudación	Llevar a cabo el proceso de autenticación siempre que se emita por primera vez un certificado digital o cuando el proceso lo requiera.
Autoridad Registradora de Aplicaciones	Centro de Procesamiento Nacional	Recibir los documentos firmados que cumplan con los procesos de verificación del certificado y del documento.
Certificado Digital	Archivo	Integrar la información con la que la autoridad certificadora que lo emite lo reconocerá dentro de su infraestructura.

Tabla 3.1 Elementos de la Infraestructura

Proceso general para enviar documentos por medios electrónicos

Para poder llegar a la recepción de documentos por medios electrónicos es necesario dividir el proceso en dos actividades, una es la generación de certificados digitales y otra la recepción de los documentos, aunque el objetivo es el segundo punto este no puede darse sin el primero, o al menos no con el grado de seguridad que se desea, es por ello que en el esquema propuesto necesariamente el primer punto debe existir antes de recibir cualquier documento, por ello a continuación se describe el proceso para alcanzar el objetivo, iniciando primero con la generación de certificados digitales.

Generación de certificados digitales

Actividad	Descripción	Responsabilidad
Generación del par de llaves	Dejar en la página de la institución la aplicación monousuario que le permita al contribuyente obtener su llave privada y su llave pública, considerando su ejecución en plataforma windows.	Institución
	Utilizar para la generación del par de llaves criptografía asimétrica.	Institución
	Guiar al contribuyente para obtener su par de llaves utilizando números aleatorios e indicándole la responsabilidad que adquiere y la importancia del resguardo de su contraseña.	Institución
	Resguardar contraseña y llave privada.	Contribuyente
	Entregar llave pública en disco flexible y sin ningún otro archivo a la institución para solicitar el certificado digital.	Contribuyente
Autenticación de personalidad	Acudir con documentos que acrediten la personalidad del contribuyente, incluyendo identificación oficial con fotografía y si se trata de representantes legales presentar el acta constitutiva de la empresa representada en la que este mencionado como representante legal.	Contribuyente

Actividad	**Descripción**	**Responsabilidad**
	Autenticar la personalidad del contribuyente al verificar la correspondencia entre la documentación presentada, el contribuyente y el registro de información que tiene la institución.	Agente Certificador
	Una vez que se ha autenticado la personalidad del contribuyente realizar la toma de datos biométricos e integrar esta información al registro del contribuyente, quedando de esta forma identificado de manera única.	Agente Certificador
	Obtener el documento firmado por el contribuyente en el que autoriza el uso del certificado digital que solicita como firma autógrafa y afirma estar conciente de la responsabilidad que adquiere con el uso del certificado y del mal uso que se le de al mismo.	Agente Certificador
Solicitud de certificado	Una vez que se ha autenticado al contribuyente, se proporciona el archivo de requerimiento al sistema de certificados digitales y se solicita la generación.	Técnico especializado de la ALR
	Antes de solicitar la generación del certificado debe existir la certeza de que: • El contribuyente no cuenta con certificado activo.	Autoridad Registradora

Actividad	**Descripción**	**Responsabilidad**
	• La llave pública es única. • Existe el registro de datos biométricos. • El contribuyente se encuentra activo ante la institución.	
	Enviar a la Autoridad Certificadora el archivo de requerimiento solicitando la creación del certificado una vez que se hayan cumplido las condiciones establecidas para la generación de certificados.	Autoridad Registradora
	Recibir el archivo de requerimiento, generar el certificado digital, registrar la información de control que relaciona al certificado con el contribuyente y regresar a la Autoridad Registradora el certificado digital generado.	Autoridad Certificadora
	Enviar a la ALR que corresponda el certificado digital solicitado y solicitar la publicación del certificado.	Autoridad Registradora
	Una vez que se ha autenticado al contribuyente, se proporciona el archivo de requerimiento al sistema de certificados digitales y se solicita la generación.	Técnico especializado de la ALR
Entrega del	Recibir el certificado digital desde el sistema de	Técnico

Actividad	**Descripción**	**Responsabilidad**
Certificado Digital	certificados digitales y colocarlo en el disco flexible en el que el contribuyente entregó su archivo de requerimiento.	especializado de la ALR
	Entregar al contribuyente el disco flexible que contiene el certificado digital solicitado, e indicarle que en la página de la institución se encuentra publicado.	Técnico especializado de la ALR

Tabla 3.2 Elementos a considerar para la Generación de Certificados Digitales

Administración de Certificados Digitales

Actividad	**Descripción**	**Responsabilidad**
Renovación de certificado	Recibir solicitud si el contribuyente cuenta con certificado vigente.	Autoridad Registradora
	Generar par de llaves y firmar la solicitud con el certificado vigente.	Contribuyente
	Recibir solicitud desde la página web de la institución.	Institución
	Verificar validez de la firma digital y si procede, revocar certificado vigente y generar el nuevo certificado digital.	Autoridad Registradora/ Autoridad Certificadora

Actividad	**Descripción**	**Responsabilidad**
	Entregar certificado renovado.	Autoridad registradora
Revocación de certificado	Solicitar movimiento usando firma digital del certificado vigente o pedir el movimiento en la ALR que corresponda presentando identificación oficial que acredite la personalidad del solicitante.	Contribuyente
	Validar firma digital	Autoridad registradora
	Revocar certificado	Autoridad certificadora
	Actualizar publicación de certificados digitales	Autoridad registradora
Cancelación de certificado	Determinar los motivos por lo que un certificado digital se cancela.	Áreas normativas
	Crear los procesos que llevarán a cabo esta actividad.	Centro de Procesamiento Nacional
	Cancelar certificado	Autoridad registradora y certificadora
Publicación de	Crear los procesos que permitirán la publicación	Autoridad

Actividad	Descripción	Responsabilidad
certificado	automática de un certificado digital inmediatamente después de su generación.	registradora
	Publicar los certificados y controlar la actualización de las listas publicadas por los movimientos de revocación y cancelación que se presentan.	Autoridad registradora

Tabla 3.3 Elementos a considerar para la Administración de Certificados Digitales

Recepción de documentos por medios electrónicos

Actividad	Descripción	Responsabilidad
Validar firma digital	Obtener llave pública y RFC del documento firmado y verificar su correspondencia con los datos registrados en el sistema de la institución.	Autoridad registradora
	Validad vigencia del certificado digital utilizado para la firma electrónica.	Autoridad registradora
	Aceptar la validez de la firma	Autoridad registradora/ Autoridad certificadora
Verificar integridad del documento	Obtener del envío el documento original.	Autoridad registradora

Actividad	**Descripción**	**Responsabilidad**
	Aplicar algoritmo hash especificado en el envío y comparar resultado con la digestión del documento que incluye el envío.	Autoridad registradora
	Determinar la integridad del documento.	Autoridad registradora
Aceptar o rechazar documento	Obtener las reglas de operación que aplicarán para la recepción de documentos.	Áreas normativas
	Verificar el cumplimiento de las reglas de operación de acuerdo al trámite que se reciba.	Autoridad registradora.
	Determinar la aceptación o rechazo de documentos.	Autoridad registradora.
Aplicación para firmar digitalmente	Proporcionar al contribuyente aplicación en ambiente windows para firmar digitalmente sus documentos.	Centro de Procesamiento Nacional
	Dejar disponible en la página web la aplicación con opción de solo poder bajarla.	Centro de Procesamiento Nacional

Tabla 3.4 Elementos a considerar para la Recepción de Documentos

MODELO PARA OBETENER CERTIFICADOS DIGITALES

Este modelo esta dividido en cuatro procesos los cuales se ilustran y explican a continuación.

OBTENER LLAVE PÚBLICA Y PRIVADA

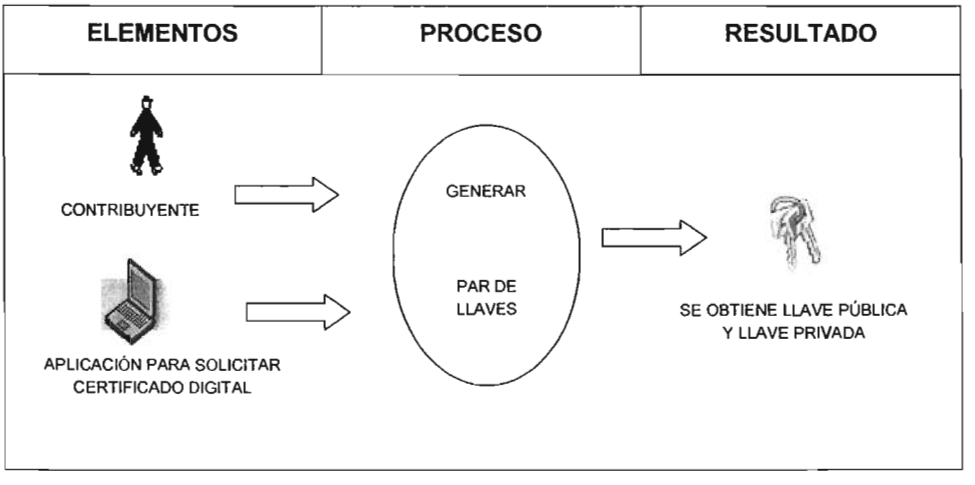

Figura 3.1 Proceso para obtener el par de llaves

La figura anterior representa el primer proceso a realizar con el contribuyente y este consiste en proporcionarle una aplicación en la que incluirá datos que lo identifican y la contraseña con la que podría en caso de obtener su certificado digital firmar documentos y trámites, aún cuando este proceso le proporciona dos archivos conocidos como la llave privada y la llave pública, para generarle un certificado solo se requiere la llave pública.

AUTENTICAR PERSONALIDAD

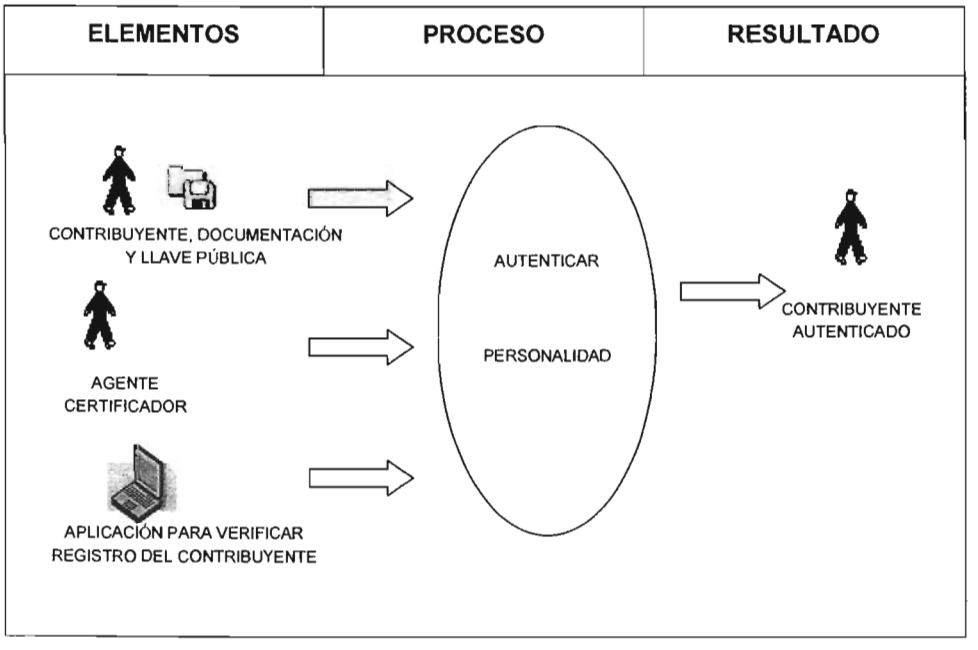

Figura 3.2 Proceso para verificar la personalidad del contribuyente

En la figura 3.2 se presenta el proceso para verificar la personalidad del contribuyente, en este paso interviene la figura del agente certificador, quien en representación de la institución revisará documentos oficiales y cotejará información que la institución ya tiene del contribuyente, de tal forma que su función será aprobar o no la personalidad con el apoyo de documentos y con la observación física del contribuyente.

INTEGRAR INFORMACIÓN BIOMÉTRICA

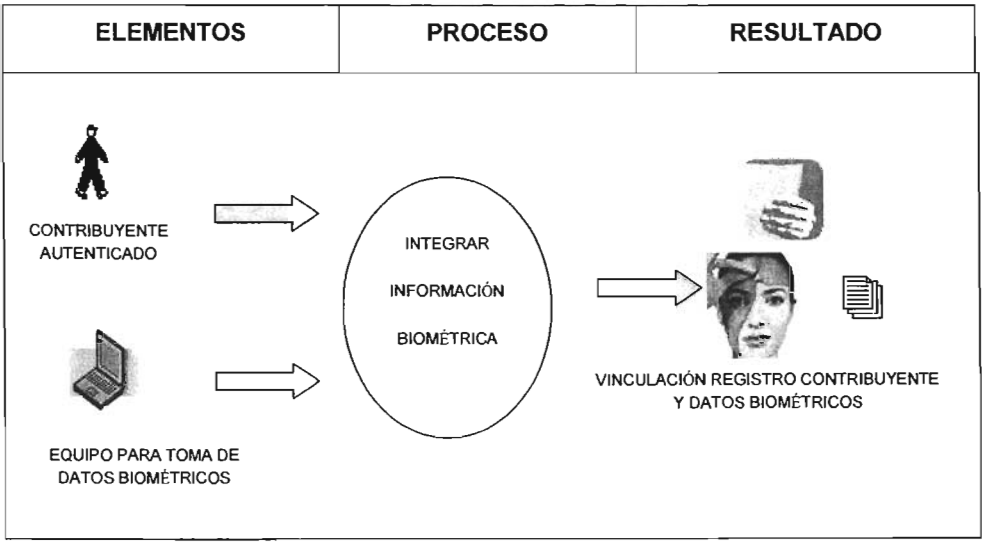

Figura 3.3 Integración de datos biométricos

En la figura 3.3 se presenta el proceso para integrar datos biométricos de un contribuyente autenticado previamente, estos datos permitirán identificar de manera única al contribuyente, lo cual permitirá garantizar que nadie podrá usurpar la personalidad de otro contribuyente, lo cual también asegura generar solo certificado digital a un contribuyente reconocido por la institución.

GENERAR CERTIFICADO DIGITAL

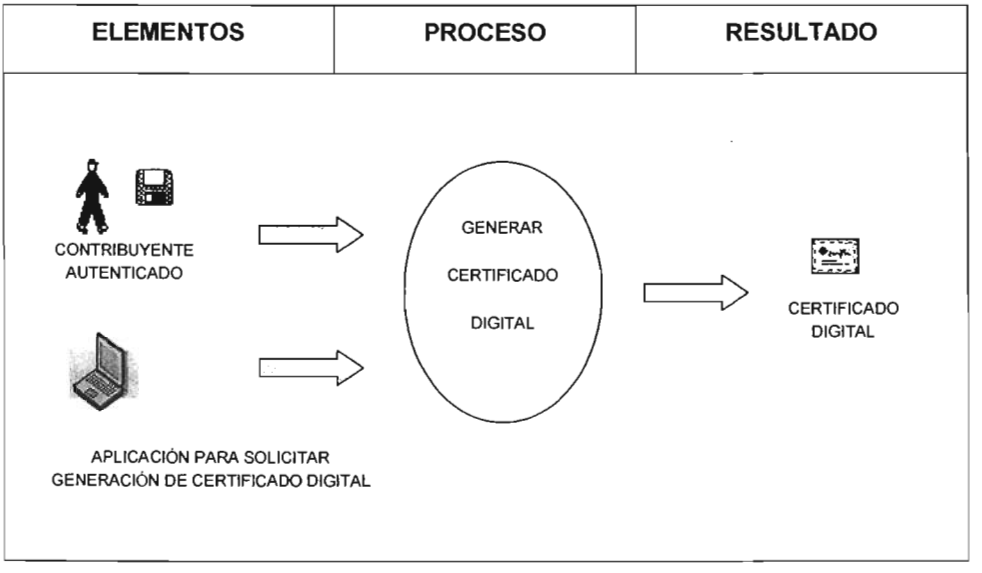

Figura 3.4 Generación del Certificado Digital

En la figura 3.4 se representa la generación del certificado digital, el cual es solicitado para un contribuyente autenticado y de quien se tienen ya datos biométricos, esto se hace a través de una aplicación multiusuario desde alguna oficina autorizada para esta actividad, esta aplicación se comunica con otra que de manera centralizada toma cada una de las solicitudes y realiza una serie de verificaciones antes de generar y enviar al solicitante el certificado.

MODELO PARA LA RECEPCIÓN DE TRÁMITES Y DOCUMENTOS

Este modelo considera que ya se cuenta con un certificado digital, esta dividido en dos procesos que a continuación se ilustran y explican.

FIRMA DE TRÁMITES Y DOCUMENTOS

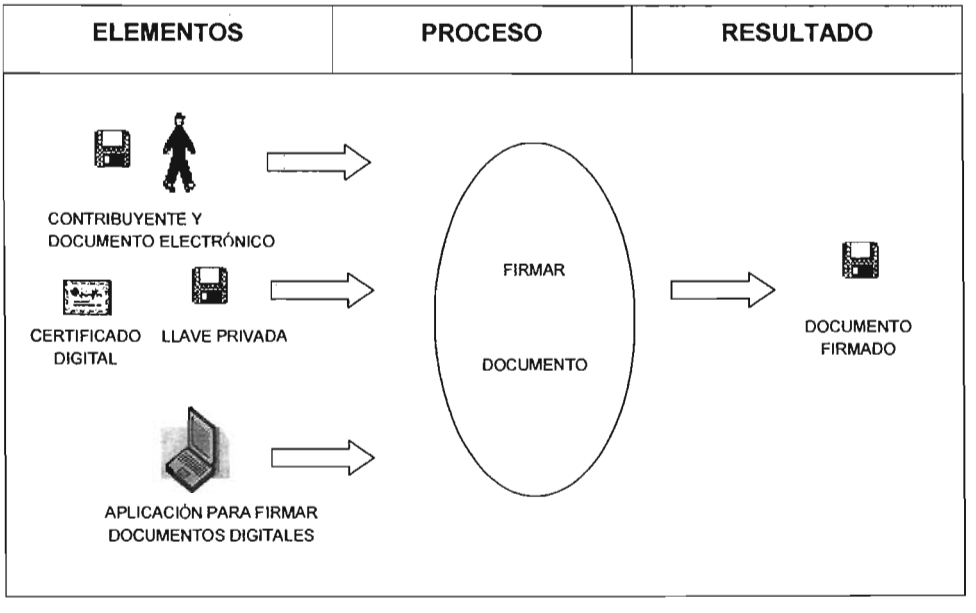

Figura 3.5 Proceso para la firma de trámites y documentos

En la figura 3.5 se muestra el proceso para la firma de trámites y documentos, el cual consiste en que una vez que el contribuyente cuenta con un trámite o documento en formato electrónico que desea enviar a la institución, debe para ello hacer uso de su certificado digital y de la llave privada que resguarda y de la que solo el debe conocer la contraseña, y para esto la institución deberá contar con una aplicación que realizará el proceso de firma y le proporcionará el documento firmado.

VERIFICACIÓN DE DOCUMENTO

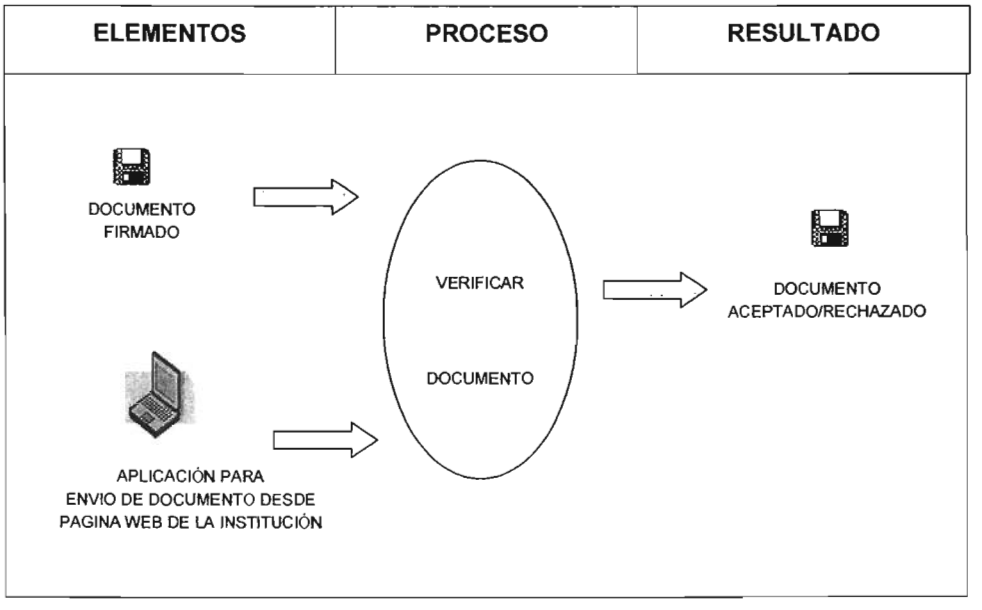

Figura 3.6 Proceso de verificación de trámites y documentos

En la figura 3.6 se muestra el proceso de verificación el cual cuenta con una aplicación que ya sea desde una página web o bien desde una aplicación cliente/servidor podrá recibir documentos firmados, esta aplicación enviará el documento a otra aplicación que de manera centralizada realizará una serie de verificaciones que permitirán decidir si el documento se acepta o se rechaza.

3.2 IDENTIFICACIÓN DE MÓDULOS

Considerando los requerimientos del sistema y visualizando el proceso general en los modelos presentados, se aprecian los siguientes módulos:.

MODULO	DESCRIPCIÓN	RECOMENDACIÓN
I	Aplicación monousuario para la generación del par de llaves y para la firma de documentos, aunque en sí estas aplicaciones no van a integrarse físicamente con el sistema son necesarias para llevar a cabo la operación	Es importante contar en el proceso de análisis con el punto de vista de personal que atiende directamente al contribuyente ya que ante cualquier duda será quien le de orientación y su aportación ayudará a obtener un buen producto.
II	Aplicación para la integración de información de autenticación del contribuyente, desde este módulo deberá integrarse la información biométrica y los documentos que acreditan su personalidad.	Si la institución no cuenta con personal que conozca la forma de tratar y almacenar la información biométrica, se debe acudir al apoyo de personal externo.
III	Aplicación para la atención de solicitudes, movimientos y recepción de documentos, este módulo es el que se instalará en las administraciones locales de recaudación en las cuales se generará el primer certificado de cada contribuyente.	Es importante involucrar en la fase de análisis a personal de las ALR´s.

MODULO	DESCRIPCIÓN	RECOMENDACIÓN
IV	Aplicación para la verificación de las condiciones que se deben cumplir antes de generar, revocar y cancelar un certificado o aceptar un documento, este módulo se encargará de administrar las solicitudes que reciba de las diferentes administraciones locales de recaudación y de llevar a cabo la verificación de firmas digitales, integridad de documentos recibidos y las condiciones que se deban cumplir de acuerdo a la petición antes de llevar a cabo cualquier movimiento en un certificado	Es necesario que en la fase de análisis participe personal del área de redes a fin de estimar el flujo de información esperada y revisar la infraestructura que le dará soporte. Se requiere acordar con personal del área de atención al contribuyente las condiciones que se deben presentar para generar, renovar y cancelar certificados, así como para recibir trámites y documentos.
V	Aplicación para efectuar los movimientos solicitados en los certificados digitales, se encargará de llevar a cabo el movimiento solicitado en el certificado, ya sea generar, revocar o cancelar, el proceso le será solicitado por el módulo que previamente realizó las verificaciones necesarias para determinar la procedencia del movimiento.	Este módulo requiere que en la fase de análisis se considere el impacto en la operación que cada movimiento traerá y establecer el trato que se dará a cada situación.
VI	Aplicación para la publicación y actualización de certificados revocados,	Debe considerarse que si la publicación hace referencia a

MODULO	DESCRIPCIÓN	RECOMENDACIÓN
	este módulo publicará constantemente los certificados que se vayan generando y actualizará las listas de revocación.	un árbol de directorios este debe estar bien organizado a fin de agilizar las búsquedas que se llevarán a cabo.
VII	Aplicación para la consulta y administración de procesos especiales.- este módulo permitirá bajo las restricciones de acceso que se consideren necesarias acceder a la información para consulta de datos, reportes, obtención de estadísticas y llevar a cabo movimientos especiales como la cancelación de un certificado por alguna razón de peso que requiera realizarse de inmediato.	Este módulo será de uso interno, y aunque sin tenerlo automatizado se puede obtener la información no debería omitirse ni aplazarse ya que será de gran apoyo durante la operación.
VIII	Módulo VIII.- Aplicación para la recepción de operaciones que se pueden atender a través de internet, desde la página web de la institución.	Para este módulo es importante incorporar elementos adicionales de seguridad sobre todo en el uso de redes.

Tabla 3.5 Identificación de módulos

3.3 PRODUCTOS ENTREGABLES

De los módulos que se han mencionado y considerando su integración dentro del sistema, se considera deben entregarse los siguientes productos:

Aplicación monousuario para ejecutarse en ambiente windows que permita generar la llave pública y la llave privada del solicitante para solicitar un certificado digital.

Aplicación monousuario para ejecutarse en ambiente windows que permita firmar digitalmente trámites y documentos.

Sistema cliente/servidor para ejecutar aplicación en ambiente windows, utilizando servidor preferentemente en ambiente unix, este sistema deberá llevar el control de la infraestructura de clave pública para atender las solicitudes de generación, revocación y cancelación de certificados, la recepción de documentos electrónicos, la publicación y listas de revocación de los certificados digitales, llevando a cabo antes de cualquier movimiento las verificaciones que cada solicitud requiere de acuerdo a las reglas de operación de la institución y a la funcionalidad misma de la infraestructura de clave pública. Este sistema operará de manera centralizada en las oficinas del Centro de Procesamiento Nacional.

Sistema web para ejecutarse en ambiente windows que permita recibir las solicitudes de movimientos a los certificados que por internet puedan realizarse, este módulo deberá de aprovechar los procesos ya establecidos en el servidor del sistema cliente servidor a fin de evitar la duplicidad de actividades.

La presentación de este modelo pretende dar una visión general de los elementos que deben incluirse en una infraestructura de clave pública, sin embargo para que un sistema sea realmente funcional se deben diseñar sistemas cerrando ciclos y automatizando eficientemente lo que este al alcance y para esto es necesaria la participación de quienes están involucrados en el proceso, se debe tomar en cuenta su

opinión, sin olvidar que quienes están a cargo de la creación de nuevos sistemas tienen la obligación de hacer trabajos realmente profesionales, trabajos en los que la calidad es no solo importante sino necesaria y no debemos esperar a que se tengan los mejores equipos, las versiones más recientes en herramientas de software y los grandes expertos para desarrollar un buen sistema, basta con saber que se tiene y que es lo se puede hacer con esos elementos para perseguir el objetivo y manejar los datos bajo estándares claramente definidos, de tal forma que ante la futura posibilidad de actualizar tecnología estos puedan ser transferidos sin grandes esfuerzos.

CAPÍTULO 4

PROCESO DE IMPLEMENTACIÓN

Ahora que se conocen los procesos y los módulos que requiere el sistema es necesario desarrollar un plan de implementación, para esto se necesita una estrategia que permita generar a cada contribuyente el certificado digital que lo identificará de manera única ante la institución para realizar sus trámites por medios electrónicos, y además emplear mecanismos que lo convenzan y lo obliguen a hacer uso de los medios electrónicos. Invitar al contribuyente a usar su certificado digital y hacerle sentir la confianza de los mecanismos establecidos, no es tarea fácil, por ello antes de iniciar este proceso es importante llevar a cabo la capacitación del personal que operará el sistema y suficientes pruebas que garanticen la correcta operación del mismo, estimando incluso la posible carga de operaciones en periodos de alta demanda en el servicio.

En este capítulo se establecerá el proceso en el que se propone se lleve a cabo la implementación del proyecto, cabe mencionar que solo se considera la generación de certificados digitales y la recepción de documentos, ya que el desarrollo de este trabajo solo plantea la forma en que debe asegurarse la recepción de trámites por medios electrónicos, sin embargo es importante tener en cuenta que para una correcta puesta

en marcha deben considerarse los procesos que integrarán a las áreas que se verán involucradas en todo el ciclo que requiere la operación de esta actividad.

En este capítulo se describen las fases de prueba que se deben realizar para asegurar una correcta operación, se plantea el proceso de instalación para llevar a todas las oficinas de la institución que proporcionarán el servicio las aplicaciones que requieren, se plantea un proceso de capacitación y recomendaciones para la difusión, así mismo se mencionan los procesos que complementarían el ciclo del servicio, además se describe un panorama de la utilidad de este sistema y finalmente se explica la forma en que se podrá realizar una integración con otras instituciones.

Consideraciones Generales

Para la implementación de una infraestructura de este tipo es importante recordar que se encontrarán involucradas las áreas de atención al contribuyente y las de atención a los documentos recibidos y que dependiendo de sus necesidades este proceso podría variar, sin embargo los mecanismos que aseguran la integridad y confidencialidad de la información en la entrega de documentos no se verá afectada, por ello el enfoque de la implementación se ubica considerando sobre todo los elementos para esta función, y para el proceso general se proponen algunos mecanismos que tendrán que ser revisados en su momento por las áreas correspondientes.

Por la experiencia con la operación del sistema que se usa actualmente, se sabe que en promedio cada mes un veinte por ciento de los contribuyentes solicita movimientos en los certificados digitales y que tan solo en la última semana para entrega de trámites lo hace el diez por ciento de ellos, por lo que partiendo de que la atención de este servicio se proporcionará a ocho millones de contribuyentes, se estima entonces que alrededor de un millón seiscientos mil contribuyentes realizará constantes movimientos a sus certificados digitales y que en los días más concurridos se solicitarán movimientos para alrededor de ochocientos mil.

Las solicitudes se recibirán desde las sesenta y seis administraciones locales de recaudación y el equipo de cómputo indispensable para el arranque es el siguiente:

- Un equipo para toma de datos biométricos.
- Una equipo para solicitud de certificados.
- Un escáner para integración digital de documentos.

Las operaciones y el almacenamiento de la información se realizará en el Centro de Procesamiento Nacional y el equipo que requiere es el siguiente:

- Servidor para la Autoridad Registradora.
- Servidor para la Autoridad Certificadora.
- Servidor para la Autoridad Registradora de Aplicaciones.
- Servidor para la publicación de certificados.
- Servidor para respaldos de información.
- Servidor de base de datos para almacenamiento de datos biométricos.

Se estima que la atención de un contribuyente para la entrega por primera vez de un certificado digital será de aproximadamente quince minutos tomando en cuenta lo siguiente:

- Revisión de archivo de requerimiento para identificación de registro ante la institución, dos minutos.
- Autenticación de personalidad contra documentos presentados, cuatro minutos.
- Toma de datos biométricos, cinco minutos.

- Generación y entrega de certificado digital, cuatro minutos.

Por lo tanto se espera que cada administración local de recaudación atienda a cuatro contribuyentes por hora para dar un total de treinta y dos contribuyentes atendidos al día dando un total de dos mil ciento doce contribuyentes atendidos en un día considerando el total de las administraciones locales de recaudación.

Se considera que la atención de movimientos en los certificados no rebasará cinco minutos.

4.1 FASE DE PRUEBAS

Esta etapa solo considera pruebas de funcionalidad especificas para medir la seguridad y rendimiento de las aplicaciones, por tal motivo se asume que previamente se han realizado pruebas de verificación del ciclo completo en un escenario tipo laboratorio en el que además se ha medido la calidad del producto.

En esta sección se describen pruebas para identificar problemas en el rendimiento del sistema, y pruebas para verificar los procesos que aseguran la información, para cada una se describe el escenario, el resultado esperado y si se considera necesario se incluyen observaciones.

Se recomienda realizar tres fases de pruebas durante cuando menos quince días hábiles en cada una y corregir lo que se vaya detectando, este plan debe ir acorde a la instalación de las aplicaciones que requiere cada oficina, en la sección de instalación se menciona la forma en que se propone se lleve a cabo.

PRUEBAS DE SEGURIDAD

Unicidad de llave pública

Escenario.- Solicitar desde dos o más equipos preferentemente al mismo tiempo la solicitud de generación de certificado utilizando el mismo archivo de requerimiento.

Resultado esperado.- Generación del certificado para el archivo de requerimiento que se recibió primero en la Autoridad Registradora y notificación de no procedencia por llave pública duplicada para las solicitudes subsecuentes.

Observaciones.- La probabilidad de que dos archivos de requerimiento generados en diferentes momentos contengan la misma llave pública es casi nula, pero existe. La notificación de no procedencia implica comunicar al contribuyente que debe generar un nuevo para de llaves, este mensaje debe transmitirse correctamente a fin de no transmitirle inseguridad en el proceso.

Existencia de datos biométricos

Escenario.- Solicitar generación de certificado digital para contribuyente que no ha proporcionado datos biométricos y para contribuyente que los tiene incompletos.

Resultado esperado.- Notificación de no procedencia por falta de datos biométricos para el primer caso y notificación de datos biométricos incompletos para el segundo caso.

Estado del certificado digital

Escenario.- Solicitar generación de certificado digital para contribuyente que no tiene certificado digital y para contribuyente que tiene certificado digital activo.

Resultado esperado.- Generación del certificado digital para el primer caso y notificación de no procedencia por certificado activo para el segundo caso.

Observaciones.- Es importante tener en cuenta que el segundo caso se va a presentar sobre todo cuando el contribuyente requiera un nuevo certificado por haber comprometido la contraseña de la llave privada, sin embargo para obtener un nuevo certificado antes debe solicitar la revocación del certificado activo.

Validez del certificado digital

Escenario.- Solicitar verificación de certificado digital para un certificado revocado, otro generado en otra autoridad certificadora y uno vencido.

Resultado esperado.- Notificación de certificado revocado para el primer caso, notificación de certificado no reconocido para el segundo caso y notificación de certificado vencido para el último caso.

Observaciones.- Este tipo de verificación junto con otros procesos será de gran utilidad en la recepción de documentos firmados.

Revocación de certificado digital

Escenario.- Solicitar revocación de certificado digital para un certificado revocado, otro no existente, uno vencido y uno activo.

Resultado esperado.- Notificación de certificado ya revocado para el primer caso, notificación de certificado no reconocido para el segundo caso, notificación de certificado vencido y ya cancelado para el tercer caso y notificación de revocación exitosa para el último caso.

Observaciones.- Los certificados que se denominan como no existentes, deben ser certificados generados con otra autoridad certificadora.

PRUEBAS DE RENDIMIENTO

Solicitud simultánea

Escenario.- Solicitar desde sesenta y seis equipos diferentes en un mismo momento la generación de certificados digitales combinando los escenarios de pruebas de seguridad planteados.

Resultado esperado.- Identificación de los procesos que consumen mayor tiempo y de los que pudieran dejar suspendido algún proceso.

Observaciones.- Este tipo de prueba debe realizarse en diferentes momentos y días a fin de detectar la mayor cantidad de fallas que pudieran existir para corregirlas antes de salir a operación.

Solicitud masiva

Escenario.- Solicitar desde sesenta y seis equipos (preferentemente) la generación constante de certificados digitales combinando los escenarios de pruebas de seguridad planteados.

Resultado esperado.- Identificación del nivel de atención que se dará al contribuyente en situaciones de alta demanda.

Observaciones.- Se aconseja realizar un proceso automático que simule una gran demanda en el servicio, la detección de un nivel de respuesta tardío puede llevar al equipo de trabajo a la revisión de los proceso para su afinación, sin embargo no debe descartarse la posibilidad de que esto se presente por un factor ajeno al proceso de datos como podría ser la red de datos.

4.2 PROCESO DE INSTALACIÓN

La instalación del sistema para la generación de certificados digitales incluye lo siguiente:

- Dejar disponible desde la página web de la institución la aplicación monousuario con la que cada contribuyente generará su llave privada y pública.
- Distribuir a las sesenta y seis administraciones locales de recaudación la aplicación cliente del sistema generador de certificados.
- Instalar en los servidores del centro de procesamiento nacional, la aplicación central y las que requiera cada servidor para la verificación, generación y publicación del certificado digital.

La instalación de los módulos del sistema se recomienda de la siguiente forma:

La aplicación del módulo para la solicitud de certificado digital deberá ubicarse en la sección de la página web que explique todo lo referente a la entrega de tramites por medios electrónicos, y en la cual necesariamente se hará referencia a los certificados digitales y al modo de obtenerlos, deberá contar solo con la opción de guardar en el medio que se indique.

La aplicación cliente del módulo generador de certificados digitales se recomienda instalar en tres etapas:

- Administraciones locales de recaudación que atienden a un número de contribuyentes que se ubica entre los treinta y cuarenta mil, esto a fin de iniciar pruebas en tiempo real en lugares donde existe una afluencia considerable de contribuyentes, de tal forma que sea posible obtener información suficiente sobre la funcionalidad sin necesidad de retrasar la operación de las oficinas ante la detección de fallas.

- En la segunda fase incorporar al proceso a cuando menos cinco administraciones locales con la mayor atención de contribuyentes, estas serán de utilidad para que con procesos ya afinados se realicen pruebas en oficinas que atienden un mayor número de contribuyentes.
- En la tercera fase se distribuye a las administraciones locales de recaudación restantes.

En el siguiente cuadro se muestran las administraciones locales de recaudación y aparecen sombreadas las administraciones candidatas a la instalación de aplicaciones para apoyar la actividad de pruebas en sus diferentes etapas.

No.	ALR's	No.	ALR's	No.	ALR's
1	Acapulco	23	Hermosillo	45	Puerto Vallarta
2	Aguascalientes	24	Iguala	46	Querétaro
3	Campeche	25	Irapuato	47	Reynosa
4	Cancún	26	La Paz	48	Saltillo
5	Cd. Guzmán	27	León	49	San Luis Potosí
6	Cd. Juárez	28	Los Mochis	50	San Pedro Garza
7	Cd. Obregón	29	Matamoros	51	Sur DF
8	Cd. Victoria	30	Mazatlán	52	Tampico
9	Celaya	31	Mérida	53	Tapachula
10	Centro DF	32	Mexicali	54	Tepic
11	Coatzacoalcos	33	Monterrey	55	Tijuana
12	Colima	34	Morelia	56	Tlaxcala
13	Córdoba	35	Naucalpan	57	Toluca
14	Cuernavaca	36	Nogales	58	Torreón
15	Culiacán	37	Norte DF	59	Tuxpan
16	Chetumal	38	Nuevo Laredo	60	Tuxtla Gutiérrez
17	Chihuahua	39	Oaxaca	61	Uruapan
18	Durango	40	Oriente DF	62	Veracruz
19	Ensenada	41	Pachuca	63	Villahermosa
20	Guadalajara	42	Piedras Negras	64	Xalapa
21	Guadalajara Sur	43	Puebla Norte	65	Zacatecas
22	Guadalupe	44	Puebla Sur	66	Zapopan

Tabla 4.2 Administraciones Locales de Recaudación

ALR con registro de contribuyentes entre treinta y cuarenta mil

ALR con más de cien mil contribuyentes registrados

ALR con registro de contribuyentes menor a treinta mil

Es importante recordar que antes de realizar la distribución de la aplicación deben estar integrados en el control de acceso los usuarios que podrán usarlo.

La distribución de las aplicaciones debe hacerse aprovechando la intranet de la institución sin olvidar incorporar los archivos de configuración que se requieran para su correcta operación.

La instalación de las aplicaciones que requieren los servidores deberá estar lista en los equipos correspondientes antes de iniciar la distribución de las aplicaciones que utilizarán los usuarios internos y los contribuyentes, por lo tanto estas deben ser las primeras en quedar listas.

4.3 ESTIMACIÓN DE COSTO EN EL USO DE RECURSOS HUMANOS

Un elemento fundamental en cualquier proyecto de sistemas es el recurso humano, a continuación se presentan los tiempos y costos estimados para cada uno de los módulos que componen el sistema (los cuales se describieron en el capítulo tres), esto debido a que se tiene conocimiento de tiempos aproximados en actividades similareas a las que se llevarán a cabo y los costos están basados en los sueldos que actualmente percibe el personal que opera el sistema de generación de certificados digitales que se usa actualmente, los costos se expresan en pesos, las actividades están divididas en las diferentes estapas del desarrollo de sistemas, así mismo se muestra un cuadro resumen que muestra el total de costos de recursos humanos que se estiman en el proyecto.

Análisis de información

MODULO	PERSONAS	HORAS	COSTO
I	2	80	17,000
II	2	160	33,000

MODULO	PERSONAS	HORAS	COSTO
III	3	90	19,000
IV	4	640	133,000
V	2	320	66,000
VI	2	240	50,000
VII	2	320	66,000
VIII	2	320	66,000
		2170	450,000

Tabla 4.3 Proyección de tiempo y costo para el análisis

Diseño del sistema

MODULO	PERSONAS	HORAS	COSTO
I	2	60	10,000
II	2	120	20,000
III	2	90	15,000
IV	3	480	80,000
V	2	240	40,000
VI	2	240	40,000
VII	2	320	53,000
VIII	2	320	53,000
		1870	311,000

Tabla 4.4 Proyección de tiempo y costo para el diseño

Desarrollo del sistema

MODULO	PERSONAS	HORAS	COSTO
I	2	320	40,000
II	3	360	45,000
III	2	100	12,500
IV	4	640	80,000
V	2	320	40,000
VI	2	320	40,000
VII	2	640	80,000
VIII	2	320	40,000
		3020	377,500

Tabla 4.5 Proyección de tiempo y costo para el desarrollo

Resumen de Costo y Tiempo

ACTIVIDAD	HORAS	COSTO	TIEMPO EN DIAS (HORAS/8)	TIEMPO CON UN EQUIPO DE TRABAJO DE 10 PERSONAS
Análisis	2170	450,000	271	136 (2 personas)
Diseño	1870	311,000	234	117 (2 personas)
Desarrollo	3020	377,500	377	63 (6 personas)
	7060	1,138,500	882	10 meses

Tabla 4.6 Proyección de tiempo y costo Global

Estimar tiempos y costos en un proyecto de desarrollo de software es una de las actividades en la que están involucrados varios factores, desde la contratación del personal, la aprobación de presupuesto, la selección de tecnología a utilizar, la adquisición de equipo, el correcto entendimiento de los requerimientos, la planeación del proyecto, costos administrativos, etc., es por ello que la proyección que se plantea se basa en los elementos del modelo y se asume que se cuenta con un equipo de trabajo, en esencia se puede decir que este proyecto podrá desarrollarse en un tiempo aproximado de diez meses, esto considerando el tiempo del análisis y el del desarrollo, tomando en cuenta que cada mes tiene en promedio veinte días laborales, así mismo el tiempo para llevar a cabo el diseño esta inmerso dentro de este lapso iniciando este a partir de los resultados que vaya generando el análisis y con este material se podrán ir entregando los requerimientos al personal encargado de realizar el desarrollo, y considerando que este último no debería iniciarse antes de tener concluido el análisis y diseño de los primeros cinco módulos.

4.4 CAPACITACIÓN Y DIFUSIÓN

La capacitación para un sistema que opera a nivel nacional sería muy costosa si se lleva a cabo de manera tradicional, es decir explicar cada módulo a todos los usuarios a los que va dirigido, y aunque no se considera necesaria por las facilidades que la misma aplicación debe contener si esta fuera necesaria, tendría que dirigirse a grupos que posteriormente la repliquen al interior de sus centros de trabajo, en lo que respecta a la capacitación de este sistema y hablando específicamente de la generación de certificados digitales, como ya se mencionó no se considera necesaria, ya que en cada módulo se incluirán mensajes que notificarán las omisiones que se cometan, a fin de dejar más clara la funcionalidad, a continuación se menciona cada módulo y los procesos que apoyan el funcionamiento del sistema.

Aplicación para la solicitud de certificado digital

Esta aplicación contará con ayuda en línea para ir guiando al contribuyente sobre el llenado de los datos que le solicita y lo que obtendrá, y además de la aplicación el contribuyente podrá obtener el archivo del manual de usuario con el que puede paso a paso usar la aplicación.

Aplicación para la generación y movimientos del certificado digital

La aplicación cliente estará compuesta de la pantalla de acceso la cual es conocida por los operadores de sistemas de la institución y por lo tanto no requiere ninguna capacitación, la pantalla de solicitud de certificado que pedirá la carga del archivo de requerimiento y recibirá la instrucción de generación y la pantalla de movimientos al certificado desde la cual se podrán llevar a cabo revocaciones y cancelaciones, las pantallas por si mismas explicarán la funcionalidad, por lo que no se requiere capacitación formal, con el manual de usuario disponible en la intranet será suficiente y además para atención de dudas y situaciones que se presenten durante la operación es recomendable dejar a disposición del personal de sistemas de cada administración local de recaudación un número telefónico al que se puedan comunicar para resolverlas.

Aplicaciones para verificar y validar certificados y documentos electrónicos.

Este tipo de aplicaciones no requieren ningún tipo de capacitación ya que serán mantenidas y operadas por el personal responsable de su desarrollo y por lo tanto su operación y mantenimiento requiere de personal especializado, lo que si es importante de verificar es que las funciones, procedimientos, librerías y aplicaciones que componen la operación del sistema estén claramente documentadas.

4.5 DIFUSIÓN

Generalmente quienes lanzan al mercado un nuevo producto no se arriesgan a crear una gran cantidad de este y exponerlo en los aparadores de las tiendas para ver si se vende, por que esto podría llevarlos a la ruina en el primer intento, lo que hacen es realizar estudios de mercado que les permitan evaluar el comportamiento de los consumidores a los que va dirigido el producto y medir el grado de aceptación que tendría y en base a esto decidir si se lanza o no, si la decisión es lanzar al mercado el producto entonces ahora se requiere una campaña publicitaria que impacte en el volumen de ventas al persuadir al consumidor sobre la necesidad que tiene del producto.

Dar a conocer el objetivo del sistema desde el punto de vista de quienes se dedican a la comunicación es fundamental para dar al contribuyente la confianza de participar en el proceso de entrega de documentos por medios electrónicos, es por eso que para este proceso es necesario contar con personal experto en la materia a fin de desarrollar una campaña publicitaria en la que se expliquen las ventajas y se enfatice que la información aun tratada por este medio cuenta con la garantía del secreto fiscal.

Si ya se ha llegado hasta aquí, ya solo es necesario transmitir con las palabras correctas el mensaje que convenza al contribuyente de que use los medios electrónicos, es necesario poner especial cuidado en la forma de transmitir el mensaje, ya que gran parte del éxito del proyecto radica en el convencimiento de los contribuyentes de hacer uso de estos mecanismos.

Aspectos a considerar en la difusión hacia el contribuyente:

No.	Descripción
1	Control del proceso de recepción y aseguramiento de la correspondencia documento/contribuyente.
2	Contraseña solo del contribuyente y en ningún momento le será solicitada.
3	La responsabilidad del uso de la contraseña es del contribuyente.
4	Es importante cancelar los certificados que se sospecha puedan usarse por personas no autorizadas o por mal resguardo de la contraseña.
5	Por seguridad es necesario renovar certificado si el personal que lo usaba ya no labora en la empresa.

Tabla 4.7 Aspectos de la difusión

4.6 PROCESOS COMPLEMENTARIOS

Durante el desarrollo de este trabajo hemos detectado una necesidad y establecido un proceso de seguridad que lo resuelve, la labor se ha enfocado al objetivo principal, el cual se considera es la esencia del problema "la seguridad", sin embargo la operación de un sistema no es solo un proceso, involucra un conjunto de actividades en el que se ven inmersas varias personas o áreas, según el entorno en que se, en esta sección se mencionarán los procesos que complementan la seguridad y correcta operación del ciclo de vida de un certificado digital usado en el proceso de recepción de documentos por medios electrónicos, lo cual es el objetivo que se desea alcanzar, estas actividades deberán estar incluidas durante el desarrollo del sistema, por lo que deberá realizarse un análisis global que amplíe el panorama y permita detectar las variables involucradas, a fin de trabajar en paralelo los procesos para la generación de certificados con las actividades complementarias que se requieren antes de iniciar la operación con los contribuyentes.

Autenticación de personalidad y toma de datos biométricos

Se ha mencionado que el contribuyente acudirá a la administración local que le corresponde a solicitar su certificado digital, pero cuando se trata de ocho millones de contribuyentes debe armarse un plan ya que de otra forma se tendría una gran demanda de este servicio en las fechas límite.

Para la generación de un certificado digital debe tomarse en cuenta que solo será necesaria la presencia física del solicitante la primera vez que lo solicite, y esto debido a que debe pasar por el proceso de autenticación en el cual se hace la revisión de documentos y la toma de datos biométricos..

Emplear un sistema de distribución basado en las primeras letras del apellido paterno, parece ser un mecanismo adecuado para la atención del contribuyente, y tomando en cuenta que la atención por contribuyente se estima en quince minutos y conociendo los contratiempos que se pueden presentar sobre todo si se vive en grandes ciudades agregar al sistema de distribución la posibilidad de que el contribuyente seleccione dentro del periodo que le corresponde el día y la hora en que desea ser atendido creará un mayor control de las actividades y permitirá proporcionar mayor calidad y atención en el servicio.

Para permitir que el contribuyente seleccione el día y la hora en la que desea ser atendido será necesario proporcionar un número telefónico en el que se le atienda para registrar la cita, este mismo servicio podría ser utilizado para realizar una primera verificación de los datos del contribuyente permitiendo detectar casos en los que antes de solicitar el certificado digital requieran una solicitud de actualización de datos.

Una vez que el contribuyente se presenta a la cita para solicitar su certificado deberá pasar por el proceso de autenticación de personalidad, que consiste en verificar documentos y certificar (un agente certificador) que el contribuyente es la persona que se menciona en los documentos solicitados.

Una vez certificada la personalidad del contribuyente se le podrán tomar los datos biométricos, esta actividad debe ser atendida por un técnico con las habilidades y conocimientos necesarios en el manejo del equipo utilizado para esta actividad y con la capacidad de resolver cualquier problema que en su manejo se presente. Además es necesario determinar la cantidad de datos biométricos y las excepciones que se manejarán.

Almacenamiento de documentos

Del proceso de autenticación se desprende una actividad más, el almacenamiento en medios electrónicos de los documentos que le permitieron al contribuyente autenticar su personalidad, y aunque no se verifica su existencia para generar o no un certificado digital, se considera necesaria como documentación probatoria de la transparencia en el proceso, esta actividad además de requerir personal para llevar a cabo la digitalización y almacenamiento en el sistema de los documentos, requiere considerar suficiente espacio de almacenamiento y un proceso que vincule los documentos del contribuyente con el registro de sus datos generales dentro del sistema, ya que de otra forma no serviría de mucho su digitalización.

Certificación de Agentes

El proceso para la certificación de agentes abarca dos situaciones, o se capacita a personal que actualmente labora en las administraciones locales de recaudación para que lleven a cabo la autenticación de personalidad o se contrata personal que ya cumpla con el perfil que la actividad requiere, esta es una decisión que deben tomar las personas que tendrán la responsabilidad de garantizar este proceso, y no hay que olvidar que en manos de estas personas estará una gran parte de la credibilidad en el proceso.

Seguimiento a Trámites

La generación de certificados y el uso de los mismos para la entrega de trámites y documentos por medios electrónicos no garantiza su aceptación, garantiza la recepción, ya que solo es un mecanismo seguro para agilizar el proceso de entrega por medios electrónicos en el que se tiene identificada la correspondencia documento/contribuyente y que dicho documento no ha sido modificado durante el viaje.

Para que el documento sea procesado en el área que corresponde es necesario implementar los procesos que le den continuidad y llevar a cabo su propio ciclo a fin de informar al contribuyente el resultado de su trámite.

Reglas de operación

Una actividad necesaria para establecer el mecanismo que se debe seguir para la generación de certificados digitales e indicar quienes son las personas facultadas para obtenerlos, con que requisitos se debe cumplir, cual será su utilidad y bajo que condiciones operará, es la generación de las reglas de operación, este documento debe ser responsabilidad del área normativa y debe contar con la participación de abogados y personal que aporte los elementos necesarios para elaborar el documento que regirá las formas y modalidades en que podrá obtenerse un certificado digital, bajo que condiciones podrá sufrir movimientos, quienes tienen la facultad para hacerlo y en que lugares se podrán solicitar. Así mismo deberán considerarse excepciones que se pueden presentar y la forma en que se resolverán.

Este documento deberá ser tomado en cuenta durante el desarrollo del sistema, por lo que, aún cuando se considera una actividad complementaria es una de las que debe integrarse rápidamente a fin de tomar en cuenta las restricciones y observaciones que se señalan para la generación y movimientos del certificado digital.

4.7 UTILIDAD DEL SISTEMA

Habrá quien se cuestione sobre la utilidad real de contar con una infraestructura de este tipo si finalmente la operación se esta llevando a cabo en estos momentos y no parece ser necesaria, resulta increíble que incluso personas inmersas en áreas de sistemas lleguen a realizar estos cuestionamientos los cuales solo reflejan una carencia en cultura de seguridad informática.

Los sistemas no hacen milagros, hacen lo que las personas que los analizan y diseñan establecen y verifican que se haga, por lo que, escuchar que alguien comenta que usar certificados digitales es la forma más segura de intercambiar información, es, en terminos generales cierto, pero es cierto si y solo si este se usa adecuadamente.

Usar un certificado digital sin que detrás exista un respaldo de procesos que verifiquen autenticidad, vigencia e identidad del propietario sería tanto como actuar de buena fe, entrar a un proceso de alta vulnerabilidad y al final crear un ambiente de total incertidumbre y desconfianza en los procesos de la institución y si además su uso se enfoca a la firma de documentos que cuentan con información confidencial y delicada al final se enfrentaría una problemática que pondría en entre dicho la credibilidad de los procesos de la institución.

La infraestructura de clave pública que se propone para la institución permitirá:

- Realizar procesos que permitan incorporar datos biométricos del contribuyente e identificarlo con esta información.

- Emitir certificados digitales que se apegan a estándares internacionales.

- Contar con un proceso de autenticación que vincule de manera única a un contribuyente con un certificado.

- Asegurar la autenticidad de certificados digitales.

- Verificar vigencia y situación del certificado digital antes de aceptar cualquier tramite firmado.

- Controlar la contraseña de acceso a la llave privada del contribuyente solo por el, adquiriendo la responsabilidad de su correcto uso.

- Contribuir en el incremento de recepción de trámites por medios electrónicos asegurando la confiabilidad, integridad y confidencialidad de la información.

- Llevar a cabo las actividades antes mencionadas en línea, es decir, en el momento en que se este llevando a cabo la operación.

Con esta infraestructura se verán beneficiados tanto procesos como contribuyentes, ya que además de asegurar la correcta recepción de trámites y optimizar el flujo de su llegada, el contribuyente podrá hacer envíos de información desde la red pública.

4.8 INTEGRACIÓN CON INSTITUCIONES

Actualmente varias instituciones están trabajando constantemente para integrar o actualizar procesos a sistemas de información que les permitan proporcionar una mejor atención al público que atienden, desafortunadamente lo hacen solo para su público.

No contar con mecanismos o normas que regulen a nivel nacional los requerimientos mínimos de información con que debe contar una institución (sobre todo pública) en relación a las personas o instituciones que atiende y el formato en que cada dato debe manejarse, provoca que el intercambio entre dos o más instituciones sea prácticamente nulo o este requiera gran cantidad de horas hombre para, primero ponerse de acuerdo en que información desean compartir, después en que formato deberán transmitirlo, de

tal forma que tanto emisor como receptor lo entiendan, posteriormente elaborar los procesos que manejarán la información y por último incorporar mecanismos seguros para llevar a cabo el intercambio.

Un factor importante que permitirá el intercambio seguro de información con otras instituciones es el uso de certificados digitales generados bajo estándares internacionales.

La generación de certificados digitales bajo la infraestructura que se propone permitirá obtener certificados digitales dentro del formato estándar a nivel internacional.

Para que la integración con otras instituciones se de, es necesario que las instituciones que decidan realizar intercambio de información utilizando certificados digitales con el Servicio de Administración Tributaria se unan a la infraestructura o bien que el SAT se una a la infraestructura de alguna de ellas que utilice el mismo formato en la generación del certificado digital. Una vez que se haya definido quien se unirá a quien la infraestructura dominante determinará a la institución que fungirá como la autoridad certificadora raíz.

La autoridad certificadora raíz tendrá como actividad principal autenticar, acordar o convenir la forma de operar y otorgar la confianza en el nombramiento de autoridad certificadora a las instituciones que se integren a la infraestructura, y siendo autoridades certificadoras podrán realizar las actividades que les competen.

El hecho de que el certificado digital sea reconocido por las instituciones que se integren a la infraestructura es solo el mecanismo que se usará como medio seguro en el intercambio de la información, la utilidad real vendrá con la información que se intercambie y para eso necesariamente hay que trabajar en conjunto entre instituciones o emitir por ley obligaciones de entrega de información promoviendo el uso de este medio.

Ejemplo práctico de integración con instituciones

A manera de ilustrar la utilidad de integrar en una infraestructura de clave pública a varias instituciones, se describirá a continuación la forma en que un proceso para el Servicio de Administración Tributaria resultaría claramente beneficiado.

Uno de los trámites que el Servicio de Administración Tributaria lleva a cabo año con año y que además es conocido bien por todos aquellos que cumplen con su deber ciudadano, es la declaración anual de impuestos, esta es realizada tanto por personas morales (empresas e instituciones) como por personas físicas y básicamente en este trámite le informan al SAT los ingresos y egresos que tuvieron durante el año que declaran y por consiguiente la cantidad de impuestos a pagar o los que resultaron a favor.

La entrega de la declaración de impuestos de una empresa, es acompañada de cifras y datos de proveedores y clientes con quienes por un lado, la empresa realiza compras para llevar a cabo su operación y por el otro hace la venta de sus productos, de esta forma puede hacer deducibles si las compra que realiza tienen que ver con su actividad empresarial y con la venta de sus productos obtiene una ganancia por el bien vendido y de esta venta debe pagar el impuesto que corresponde al gobierno, en este caso al SAT las empresas le informan sobre las compras que hicieron a sus proveedores o sobre los gastos que realizo para la operación de su negocio y sobre las ventas que llevo a cabo con sus clientes, toda esta información es ingresada a los sistemas del SAT para corroborar cifras del documento entregado y hacer algunos comparativos con la información que entregan los proveedores y clientes de la empresa, esta actividad requiere gran cantidad de trabajo humano ya que no existe un proceso que automáticamente realice esta actividad, por lo que en primera instancia el formato se tiene que capturar y aun cuando al personal que realiza esta actividad se le pide no cometer errores finalmente estos se presentan, debido a que el proceso de captura lleva tiempo y el proceso de comparaciones también, en este momento resulta

prácticamente imposible comparar el total de la información, por ello se toman muestras de datos y como una medida para confirmar la veracidad de la información declarada aleatoriamente se llevan a cabo auditorias en las que físicamente se observa la documentación de gastos que tiene la empresa, pero en este proceso existe otro inconveniente ya que para que realmente se tuviera la certeza de que los documentos presentados son reales se tendría que verificar también a cada una de las personas que entregaron una factura a la empresa y las facturas que esta entrego a quienes le compraron, de momento una auditoria es lo que se hace para llevar un control de las declaraciones de impuestos que se informan al SAT.

Usando la infraestructura de clave pública con otras instituciones se tiene que definir un formato de entrega de esta información para que se realice por medios electrónicos, se firma el documento a entregar con el certificado digital y se tiene que sistematizar el proceso de recepción y comparación de datos que proporcione lo siguiente:

- Integración automática de los datos del formato.
- Posibilidad de realizar procesos de comparación.
- Reporte de omisiones o fallas en la declaración.
- Posibilidad de consulta del detalle de los datos que presentan diferencias.

Contar con un proceso seguro que pueda hacer estas actividades sería realmente una gran utilidad en el uso de los certificados digitales.

La entrada de otras instituciones se daría de la siguiente forma:

Si se define un formato para hacer el envío de la declaración de impuestos, también se puede definir otro para el manejo de facturas electrónicas y así como las empresas y establecimientos comerciales envían autorizaciones de crédito para quienes usan tarjetas bancarias para realizar sus pagos, de la misma manera las empresas y

establecimiento comerciales podrían hacer el envío de la factura electrónica en la que notifican al SAT sobre la venta, y debido a que armar toda una infraestructura de comunicación entre empresas y el SAT sería muy costoso, quizá integrar a los bancos a la infraestructura de llave pública del SAT sería lo más conveniente para así aprovechar la infraestructura que tienen y los mecanismos de comunicación que ya existen con el SAT.

Claro que la integración con los bancos y con cualquier institución requiere de establecer acuerdos, compromisos, formas de operar pero sobre todo responsabilidad en ambas partes, y en ocasiones este proceso es más complicado que llevar a cabo las actividades que se requieren para la operación.

Esto es solamente una sugerencia, pero sería el inicio de muchos otros procesos que podrían automatizarse y hacer uso de la infraestructura de clave pública y realizar el intercambio de información por medios electrónicos de una manera más segura.

CONCLUSIONES

Uno de los problemas que comúnmente se presenta en el desarrollo de sistemas, además de no considerar la seguridad como un elemento necesario, es el no visualizarlos e imaginarlos con una funcionalidad y beneficio real en la operación, siempre se esta contra el tiempo y al final se termina invirtiendo más del que seguramente se necesita si se analiza y diseña a conciencia antes de iniciar cualquier actividad de desarrollo.

Como se observa en la problemática planteada en este trabajo, en un intento por tratar de resolver un problema de seguridad se iniciaron operaciones con el uso de certificados digitales sin considerar los procesos automatizados que para la administración de los mismos se requiere y esto ocasionó trabajar con procesos semiautomatizados y parchar sobre la marcha, sin embargo ante la necesidad de incrementar considerablemente la cantidad de usuarios e imaginar la situación inoperable es necesario decidir renovar el sistema o sufrir las consecuencias.

El módelo que se propone considera el uso de un certificado estándar que permitirá incluso considerar en un futuro la integración con otras instituciones y con esto aprovechar las bondades que ofrece el contar con una infraestructura de este tipo, siempre que los procesos que la componen estén realmente automatizados e integrados.

Es importante mencionar que todos los elementos que podamos implementar para hacer más seguros nuestros procesos incrementarán notablemente la seguridad, pero no se debe pensar que una infraestructura de clave pública o el método que se decida utilizar garantizará por completo un proceso, ya que un descuido puede generar vulnerabilidad, con esto finalmente se concluye que ni los métodos, ni las infraestructuras, ni la memoria de quienes acostumbran aprenderse sus contraseñas son infalibles y que la responsabilidad en la implementación de procesos automatizados y el cuidado que los usuarios tengan en el uso de los

mismos es lo que elevará la seguridad en el intercambio de información por medios electrónicos.

El modelo que aquí se propone utiliza procedimientos que garantizan la recepción del documento original y la verificación en la correspondencia de que el documento fue firmado por una persona reconocida dentro de la infraestructura y por ello se consideran procesos seguros, pero hasta que una cultura de la seguridad informática se extienda tanto en los sistemas como en los usuarios se podrá elevar considerablemente la seguridad en el intercambio de documentos por medios electrónicos, ya que aún es común que los usuarios proporcionen sus contraseñas a amigos o compañeros de trabajo o incluso para no olvidarlas las escriben y las pegan al lado del equipo que regularmente utilizan, dejando al descubierto la posibilidad de que otros realicen operaciones en su nombre, por lo que aun cuando una institución haya trabajado en la construcción de una infraestructura capaz de asegurar varios elementos del proceso hay algunos que simplemente rebasan su capacidad.

GLOSARIO

SAT.- Servicio de Administración Tributaria, institución gubernamental que se encarga de la recaudación de impuestos en México.

FAR.- False Accept Ratio, coeficiente de aceptación falso.

FRR.- False Reject Ratio, coeficiente de rechazo falso.

RSA.- es el algoritmo criptográfico más exitoso de clave pública/privada. Fue inventado por Rivest, Shamir y Adleman obteniendo así su nombre.

ECC.- Elliptic Curve Cryptography es después de RSA el siguiente algoritmo criptográfico más reconocido.

ALR.- Administración Local de Recaudación, es la oficina en la que se atiende a los contribuyentes sobre asuntos de recaudación de impuestos.

CPN.- Centro de Procesamiento Nacional, oficina en la que se concentra el personal especializado para realizar la automatización de procesos y el manejo de equipos que apoyan la operación del SAT.

RFC.- Registro Federal de Controbuyentes, clave con la que el SAT identifica a cada uno de los contribuyentes, consta de doce carácteres para personas morales y trece para personas físicas.

CPA.- Centro de Procesamiento Alterno, es un espejo del Centro de Procesamiento Nacional y existe para entrar en operación solo en caso de que el CPN detenga por aguna causa su operación.

BIBLIOGRAFÍA

Andrew Nash, William Duane, Celia Joseph y Derek Brink
PKI Infraestructura de Claves Públicas
Osborne McGraw-Hill 2002, 512 pp.

Rush Housley, Tim Polk
Planning for PKI
Wiley Computer Publishing, USA, 2001, 327 pp.

Bruce Schneier
Applied Cryptography
John Wiley & Sons, Inc, USA, second edition, 1996, 758 pp.

Rolf Oppliger
Sistemas de Autentificación para Seguridad en Redes
Alfaomega 1998, 194 pp.

Stephen Northcutt
Detección de intrusos
Prentice Hall 2001, 445 pp.

Jeff Schmidt
Seguridad en Windows 2000
Prentice Hall 2001, 802 pp.