UNIVERSIDAD AUTÓNOMA DE BAJA CALIFORNIA

FACULTAD DE DERECHO MEXICALI

FIRMA ELECTRÓNICA “FIEL”

Trabajo Terminal para obtener el Diploma de

ESPECIALIDAD EN DERECHO

Presenta:

Marco Herubiel Gómez Cuevas

Asesor:

Mtro. Benjamín Zomora Sánchez Alós

Mexicali, Baja California, México **Enero de 2009.**

INTRODUCCIÓN.

Sin duda la era digital se encuentra sobre nosotros, es por ello que toda la sociedad y en especial el gobierno, tenemos el deber de estar a la altura de las circunstancias de cambio, necesarias en cada época. La firma electrónica aun llamada de otras maneras, siendo simple o avanzada, hace referencia a las acciones que el gobierno, en este caso la Secretaría de Hacienda y Crédito Público a través del Servicio de Administración Tributaria, a efecto de otorgar al contribuyente una serie de herramientas por medio de las cuales facilite el cumplimiento de sus obligaciones ante el fisco, obviamente sin dejar a un lado la simplificación en la recaudación para la autoridad fiscal.

La firma es un signo personal que al plasmarlo denota nuestro compromiso ante determinada obligación o simplemente el conocimiento de alguna situación en particular. Este es un elemento fundamental en la mayor parte de los trámites que realizamos día a día, además, es en algunas ocasiones, esencial en el ejercicio de nuestras actividades dentro de nuestro trabajo. Desafortunadamente en el constante deseo de simplificar nuestras actividades cotidianas, disponemos de mecanismos mediante los cuales nos auxiliamos para la implantación de nuestra firma, pudiendo ser mecánicos o sencillamente que un tercero firme a ruego de nosotros; en este sentido se torna muy importante la seguridad al momento de ser utilizada nuestra firma, ya que nos obliga a situaciones jurídicas, y el uso indebido de esta, acarrea inconvenientes para su propietario. Por ello, el uso eficiente de los recursos y la seguridad del contribuyente, el Servicio de Administración Tributaria creó la Fiel, sin dejar a un lado la olvidada Clave de Identificación Electrónica Confidencial, su predecesora la FEA y la simple Firma Electrónica, no pasa desapercibido que la primera en mención es exactamente lo mismo que la última. Todo este cúmulo de figuras electrónicas tiene la finalidad de que las comunicaciones entre el contribuyente y el fisco federal sean totalmente por vía electrónica y estas estén sujetas a estándares internacionales de seguridad en la trasmisión de datos.

Es por esto que se elabora la presente investigación con el fin de sentar un precedente en el desarrollo de este novedoso tema, tanto en su utilización como por supuesto, en la legislación del país y a su vez hacer un explicación detallada del concepto de firma, de dónde proviene, la seguridad en los documentos electrónicos, la firma electrónica, y el proceso de su obtención ante el Servicio de Administración Tributaria, explicando de manera detallada, concisa, no olvidando los puntos de vista legales que la especialidad de la cual emana el presente, asimismo, agregando un tinte de técnica informática del propio tema.

ÍNDICE.

ANTECEDENTES DEL PROBLEMA:

En dos mil cuatro nace el capítulo “de los medios electrónicos” dentro del Código Fiscal de la Federación, trayendo consigo avances en materia tecnológica en las relaciones fisco-contribuyente, sin embargo, en su corta vida no ha sido obstáculo para causar una serie de inconsistencias en la forma de manejar la política cibernética dentro del Servicio de Administración Tributaria y con ello causar confusión al contribuyente, obligándolo a invertir más tiempo y dificultando las condiciones para cumplir con sus obligaciones tributarias.

METODOLOGÍA.

Requiere de un proceso de investigación de carácter documental, con técnicas encaminadas a documentos hemerográficos, bibliográficos y electrográficos.

CAPITULO 1

FIRMA ELECTRÓNICA, “FIEL”.

1. FIRMA.

Por siglos el ser humano en su afán de comunicación ha buscado distintas formas de expresión desde el conjugar figuras y colores, hasta realizar armoniosas melodías; así llegando a la invención de la escritura, misma que evolucionó hasta los complejos sistemas gramaticales que, en nuestros días, cada idioma conlleva. La creación humana debe ser reconocida a su autor y éste ser identificado de forma fehaciente por la autoría del mismo; es por ello que los creadores de obras de cualquier índole, desde hace siglos, hacen distintiva su autoría mediante un signo que los identifica plenamente.

Por ejemplo, en Roma, no se firmaban los documentos, tampoco era costumbre ni necesario (cód, Just. VII, 6, 1, 1, inst III, 23) aunque existía la *Manufirmatio*, que consistía en una ceremonia, en que leído el documento por su autor o el notario, se colocaba desenrollando y extendido sobre la mesa del escribano y luego de pasar la mano abierta sobre el pergamino en actitud de jurar, pero sin hacerlo, se estampaba el nombre, signo, o una o tres cruces – una por cada persona de la santísima trinidad-, por el autor o el notario en su nombre, haciéndolo seguidamente los testigos. Más que *in requisito*, la *Manufirmatio* era en sí misma parte del espectáculo solemne en que se realizaba el acto. (enciclopedia jurídica mexicana, IV,82).

En la Edad Media, se inscribía una cruz a la que se le añadían diversas letras y rasgos. Estos signos se utilizaban como firma. Debido a que no sabían leer ni escribir, los nobles remplazaron esta práctica con el uso de sellos.

En ese tiempo, pocas eran las personas que sabían leer y escribir, por lo que generalmente los particulares estampaban un signo o firma, en los documentos y en el desenvolvimiento de las transacciones comerciales, haciendo que ésta fuera adquiriendo la importancia y uso que con el transcurso del tiempo fue consagrandola como un símbolo de identificación y de enlace entre el autor de lo escrito o estampado y su persona. (Acosta Romero, Miguel; Nuevo Derecho Mercantil; 539).

La palabra firma significa: Nombre y apellido que una persona pone, con rúbrica o sin ella, al pie de un escrito como señal de autenticidad. A que se pone en una hoja de papel o pliego destinado a ser cubierto posteriormente por determinada persona autorizada por el autor de la suscripción y en los términos convenidos. Autorizar un escrito o documento. Inscripción manuscrita que indica el nombre de una persona que entiende hacer suyas las declaraciones del acto (Nuevo Diccionario Jurídico Mexicano, 2000: 1706-1707). Secuencia de datos utilizada para identificación, tal como un texto que se adjunta a un mensaje de correo electrónico o a un fax. (Diccionario de informática e Internet de Microsoft, 2001: 206).

Según el Diccionario de la Real Academia, la firma es el nombre y apellido, o título, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido.

Se considera a la firma como un conjunto de signos. Se puede decir que su función más importante en el ámbito legal es el hecho de que vincula a la persona con el acto jurídico, esto es, se torna identificadora de la persona, puesto que determina sus derechos y obligaciones sobre el contenido del documento.

Aunque la ley no precisa ni define en qué consiste la firma, esta omisión puede ser suplida acudiendo, no sólo al significado gramatical de la palabra, sino a los usos y costumbres que imperan respecto de la firma. Jurídicamente hablando,

es la afirmación de individualidad, pero sobre todo de voluntariedad. En un primer aspecto, significa que ha sido la persona firmante y no otra quien ha suscrito el documento. En segundo, que se acepta lo que allí se manifiesta. (enciclopedia jurídica mexicana, IV,83).

Así, la firma autógrafa se utiliza para expresar el consentimiento de las partes sobre un contrato en particular, sin embargo la firma como tal no se encuentra regulada en ninguna legislación, aunque su utilización es patente en todos los códigos procesales de este país, considerando a la firma como exteriorización de la declaración de la voluntad de una persona, que es totalmente necesaria en cualquier documento, dejando a un lado la idea de ser un mero formalismo o requisito; precisando una actuación física y corporal del firmante al plasmar su signo como un instrumento de expresión de declaración de su voluntad.

Como en la antigua Roma con la *manufirmatio,* que citamos párrafos atrás, la firma es un signo que contiene una valía o mas bien dicho un significado, el cual en un primer momento se puede decir, es la aceptación o tener conocimiento de una determinada obligación. Sin embargo, al no contar, se insiste, con una teoría sobre la firma, se puede confundir o se confunde con un simple signo, ya que puede ser tan sencilla o complicada como la persona que firma prefiera; llegando al extremo de preguntarnos si una obra de arte está firmada o simplemente el autor insertó un signo distintivo en ella a efecto de ser reconocida su autoría, que en otro aspecto pero que en la misma vía, un documento firmado, obliga al firmante al cumplimiento de lo acordado en el documento o simplemente plasmó un símbolo el cual solo expresa que fue revisado por él mismo, más no se obliga a ello.

La firma, también es considerada como el lazo que une al firmante, entendiendo la como –firmante- a la persona que plasma un conjunto de signos a los cuales les llama firma la cual es insertada en un documento sobre el cual puede expresar su consentimiento u obligación a lo que en el mismo se relata. Este

lazo lo vincula, aunque la firma no exprese legiblemente el nombre de la persona que lo hace, la identificación de esta, ocurre generalmente en el encabezado, en el cuerpo o al final del documento lugar donde se imprime generalmente solo el nombre completo del sujeto a firmar. En otras ocasiones su también se imprime su profesión y/o sus datos generales. El nexo generado, debe ser de la persona con el documento y haber sido plasmada por la misma, sea de manera manuscrita o por cualquier otra grafía que reconozca como signo propio de expresión de su voluntad; incluso ser plasmada por un tercero a ruego de la obligada, siendo aceptable el simple hecho de imprimir la huella digital del individuo, haciendo esta las veces de firma, por citar un ejemplo el Código Federal de Procedimientos Civiles en su artículo 114: *las declaraciones… serán firmadas al pie de la última hoja y al margen de las demás que se contenga…* Si no supieren firmar, pondrán su huella digital, y, si no quisieren hacer lo uno ni lo otro, firmará sólo el tribunal y hará constar esta circunstancia", en el mismo código en su artículo 138 que versa: *"Podrá pedirse el cotejo de firmas, letras o huellas digitales, siempre que se niegue o que se ponga en duda la autenticidad de un documento privado…".*

Por cuestiones de economía y rapidez, se utilizan medios mecánicos para plasmar firmas autógrafas, ejemplo el facsímil, siendo este un medio mecánico utilizado para imprimir réplicas de una grafía. La palabra que proviene de *facsímile*, que de acuerdo a la Real Academia Española es la perfecta imitación o reproducción de una firma, de un escrito o de un dibujo; suscitándose el problema sobre que quien estampa la grafía llamada firma, es una persona distinta a la que dentro del cuerpo de documento señala como responsable u obligada; de esta manera sucede que no tiene conocimiento del contenido del documento en el cual se plasmó la reproducción de su firma, además al ser usando ese medio mecánico, cualquier persona puede utilizar su firma usurpando la identidad del propietario, obligándolo u otorgando su autorización, sin tener conocimiento del documento firmado.

En sintonía a lo escrito por Alfredo Reyes Krafft, dicta que la firma posee las siguientes características:

• Identificativa: Sirve para identificar quién es el autor del documento.

• Declarativa: Significa la asunción del contenido del documento por el autor de la firma. Sobre todo cuando se trata de la conclusión de un contrato, la firma es el signo principal que representa la voluntad de obligarse.

• Probatoria: Permite identificar si el autor de la firma es efectivamente aquél que ha sido identificado como tal en el acto de la propia firma. (Reyes Krafft, Alfredo. La firma electrónica y las entidades de certificación. Ed. Porrúa. México 2004).

Además de los elementos que a continuación se transcriben:

Elementos formales.- Son aquellos elementos materiales de la firma que están en relación con los procedimientos utilizados para firmar y el grafismo mismo de la misma.

La firma como signo personal.- La firma se presenta como un signo distintivo y personal, ya que debe ser puesta de puño y letra del firmante. Esta característica de la firma manuscrita puede ser eliminada y sustituida por otros medios en la firma electrónica.

El *animus signandi*.- Es el elemento intencional o intelectual de la firma. Consiste en la voluntad de asumir el contenido.

Elementos funcionales.- Tomando la noción de firma como el signo o conjunto de signos, podemos distinguir una doble función:

Identificadora. La firma asegura la relación jurídica entre el acto firmado y la persona que lo ha firmado. La identidad de la persona nos determina su personalidad a efecto de atribución de los derechos y obligaciones.

Autenticación. El autor del acto expresa su consentimiento y hace propio el mensaje:

• Operación pasiva que no requiere del consentimiento, ni del conocimiento siquiera del sujeto identificado.
• Proceso activo por el cual alguien se identifica conscientemente en cuanto al contenido suscrito y se adhiere al mismo.

Pugnando Reyes Krafft, en pro de la firma electrónica, al decir que la firma manuscrita expresa la identidad, aceptación y autoría del firmante. No es un método de autenticación totalmente fiable. En el caso de que se reconozca la firma, el documento podría haber sido modificado en cuanto a su contenido -falsificado- y en el caso de que no exista la firma autógrafa puede ser que ya no exista otro modo de autenticación. En caso de duda o negación puede establecerse la correspondiente pericial caligráfica para su esclarecimiento.

La firma es afirmación de individualidad, pero sobre todo de voluntariedad. En un primer aspecto, significa que ha sido la persona firmante y no otra quien ha suscrito el documento. En el segundo, que se acepta lo que allí se manifiesta.

Así, desde el punto de vista jurídico, la firma es el medio que identifica a una persona, utilizada como signo de expresión del consentimiento y permite ejercer la voluntad o asumir el contenido de un documento, para luego ser considerado como una prueba. Aunque en el país no existe una definición legal de firma, lo cierto es que el consentimiento equivale funcionalmente a ella y, por esto, el reto al que se enfrentan en la actualidad los expertos en informática, consiste en migrar a medios electrónicos el reconocimiento y la validez jurídica del contrato celebrado de forma electrónica, darle exigibilidad judicial y buscar el equivalente funcional de la firma a través de la criptografía de clave pública, garantizando atribución, integridad, autenticidad, accesibilidad y confidencialidad.

1.1. Seguridad en Documentos Electrónicos.

La necesidad de garantizar la integridad, la confidencialidad y la autenticidad de los datos que fluyen a través de la Web –palabra en ingles, es el sistema de documentos interconectados por enlaces de hypertexto, que se ejecutan en Internet- se han convertido en un requisito esencial. Por este motivo el área de seguridad en los usuarios de cualquier carácter crece rápidamente, ya que la existencia de información vital de nuestras vidas se encuentra en mayor medida en documentos electrónicos y son, en muchas ocasiones, blanco de ataques por parte de ladrones cibernéticos que obtienen nuestra información con el fin, por ejemplo, de ostentarse como nosotros en transacciones que les acarrean beneficios económicos, afectando además de la esfera jurídica, la privacidad y la economía.

El Documento electrónico, se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

Los documentos son según la real academia española es “el escrito en que constan datos fidedignos o susceptibles de ser empleados como tales para probar algo.
(http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=documento, 10-9-08). En cambio el código tributario, al hablar al respecto de los documentos, menciona en su artículo 17-D, “…éstos deberán ser digitales y contener una firma electrónica avanzada del autor…”, así mismo explica que se entiende por documento digital “…todo mensaje de datos qué contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología…”. Si analizamos la noción tradicional de documento referida al instrumento en el que queda plasmado un hecho que se exterioriza mediante signos materiales y permanentes del lenguaje, vemos como el documento electrónico pretende cumplir con los requisitos del documento en

soporte de papel en el sentido de que contiene un mensaje (texto alfanumérico o diseño gráfico) en lenguaje convencional (el de los bits) sobre soporte (cinta o disco), destinado a durar en el tiempo.

Así la interactividad y la digitalidad del mundo ha cambiado la forma en que se vive. Si se quiere comprobar el saldo de una cuenta bancaria, pagar servicios como la electricidad y el teléfono, se realiza mediante el internet, es suficiente un número de usuario y una clave.

Sin embargo, el sistema de usuario y clave, ha sido ineficaz contra el fraude, pues algunos utilizan un elemento externo tarjetas de identificación, llaves, y claves, en otros casos, es frecuente olvidar una clave de acceso o incluso el usuario, por ello se suele anotar en agendas o cuadernos, con lo que pierden confidencialidad, de esta forma las claves y *passwords* son uno de los puntos más riesgosos y difíciles de sustentar (http://www.microsoft.com/spain/empresas/seguridad/articulos/select_sec_passwords.mspx, 16-4-08). Por ello, y con el desarrollo de las nuevas tecnologías de telecomunicaciones y trasmisión de datos por vía electrónica, se ha generalizando el uso de los sistemas de intercambio electrónico de información en virtud de que permiten mejorar la productividad y reducir costos, además de brindar amplias posibilidades de nuevos servicios en línea. En esta tesitura necesariamente debemos hablar sobre la seguridad en el trafico de información vía internet, considerando los siguientes como aspectos fundamentales:

- La privacidad, tomando en consideración que la información no sea interceptada por un tercero.
- La integridad, que el contenido del mensaje sea recibido tal cual se envió, y,
- La autenticidad, es decir que nos dé la garantía de quién es el autor.

Los sistemas que protegen la seguridad de los documentos electrónicos, son construidos aplicando técnicas basadas en el uso de algoritmos criptográficos

cuya función primordial es transformar un mensaje en un texto no inteligible excepto para el destinatario ya que éste es el único que puede efectuar la transformación inversa y por lo tanto conocer el mensaje original, al texto ininteligible se le conoce como criptograma, dicho de otra manera un mensaje cifrado cuyo significado resulta ininteligible hasta que no es descifrado.

Encripción: es el conjunto de técnicas matemáticas utilizadas en los procesos para ocultar y cifrar -se debe utilizar el término cifrar en vez de encriptar, ya que se trata de un anglicismo de los términos ingleses *encrypt* y *decrypt*- la información.
(http://es.wikipedia.org/wiki/Criptolog%C3%ADa; 16-4-08)

Codificar: significa expresar un mensaje utilizando algún código, pero no necesariamente de forma oculta, secreta o ininteligible.
(http://es.wikipedia.org/wiki/Criptolog%C3%ADa; 16-4-08).

Algoritmo: proviene del latín, *dixit algorithmus* y éste a su vez del matemático persa al Jwarizmi, es una lista bien definida, ordenada y finita de operaciones que permite hallar la solución a un problema. Dado un estado inicial y una entrada, a través de pasos sucesivos y bien definidos se llega a un estado final, obteniendo una solución. Los algoritmos son objeto de estudio de la algoritmia.
(http://es.wikipedia.org/wiki/Algoritmo; 11-11-08).

Criptográfico: proviene del griego κρύπτω *krypto*, -oculto-, y γράφω *graphos*, -escribir-, literalmente -escritura oculta-, es el arte o ciencia de cifrar y descifrar información utilizando técnicas que hagan posible el intercambio de mensajes de manera segura que sólo puedan ser leídos por las personas a quienes van dirigidos.
(http://es.wikipedia.org/wiki/Criptogr%C3%A1fico, 11-11-08).

Con la finalidad de cubrir los aspectos de seguridad que los mensajes electrónicos merecen, nace la llamada Infraestructura de Clave Pública –clave pública y privada -, siendo éste un sistema que permite al usuario firmar de manera digital, basando ésta en una clave pública; misma que resuelve los problemas de seguridad que una simple firma escrita no resuelve, de acuerdo al dicho de los promotores de ésta, es decir la firma electrónica, garantiza que el documento no haya sido modificado después de haber sido firmado y que la su autoría es definida. La finalidad primordial de la mencionada infraestructura, es proporcionar claves y certificados con los que se puedan confiar atendiendo a los aspectos de seguridad mencionados en párrafos precedentes, al momento del intercambio de información por medios electrónicos; como se menciona en www.firma-electronica.unam.mx, logrando la habilitación de la autenticación, la no repudiación –es decir garantizar que el firmante no pueda negar la autoría del mensaje- y la confidencialidad de las claves que la integra.

Habilitar: entendiendo como dar las condiciones necesarias para desempeñar funciones que no son las propias de un sistema.

Autenticación: es decir la acreditación del autor del mensaje.

Repudiación: no aceptar la validez de una clave, o rechazar la acción de un usuario informático.

Así tenemos que en la utilización de un algoritmo simétrico, se garantiza la privacidad de la información, en virtud de que solo el destinatario puede descifrarla, ya que es el único que conoce la clave con la cual el emisor realizó el cifrado de la información. En este caso el destinatario sabe quien generó el mensaje, pero no tiene elementos para demostrar que tal mensaje le es atribuible al emisor.

En el caso de algoritmos criptográficos asimétricos –ejemplo la firma electrónica- cuando el cifrado y descifrado de un mensaje se realiza con base en el par de claves asociado al destinatario, esto es, el emisor utilizando la clave pública del destinatario y este la descifra utilizando su clave privada; garantizando que únicamente el destinatario pueda leer el mensaje, ya que solo el dueño de la clave privada puede descifrar el mensaje, sin embargo el destinatario no puede saber quien genero el mensaje.

Se hace referencia a los aspectos técnicos de la Firma Electrónica con sistemas muy popularizados, que pretenden hacer frente a los problemas de seguridad en los documentos electrónicos, es decir los estándares como XML Encryption y XML Signature, preparados para manejar situaciones en las que partes de un mismo documento necesitan un tratamiento diferente, como ocurren en documentos con diferentes secciones cuyo contenido puede ser visto por unos usuarios pero no por otros. En estos casos la encriptación juega un papel muy importante ya que es lo que va a confirma la integridad del texto. Por otro lado, las firmas digitales permiten la autenticación del remitente. Otro problema añadido surge cuando diferentes personas firman digitalmente un mismo documento XML o cuando es necesario hacerlo conjuntamente codificando ciertas partes de ese documento.

XML *Encryption:* es un lenguaje cuya función principal es asegurar la *confidencialidad* de partes de documentos XML, a través de la encriptación parcial del documento transportado. XML Encryption se puede aplicar a cualquier recurso Web, incluyendo contenido que no es XML-mensajes de datos de cualquier clase-.

XML *Signatura:* asegura la *integridad* de partes de documentos XML transportados. También proporciona la autenticación de mensajes y/o servicios de autenticación de firma para datos de cualquier tipo, tanto si se encuentra en el XML que incluye la firma o en cualquier otra parte.

Puede aplicarse a cualquier contenido digital (objeto de datos), incluyendo XML. Lo que hace principalmente la XML Signature es asociar claves con los datos de consulta. XML Signature representa un sistema que a través de una firma digital permite ofrecer autenticidad de los datos, con la firma digital se confirma la identidad del emisor, la autenticidad del mensaje y su integridad, sin olvidar que los mensajes no serán repudiados.

XML *Key Management:* es un protocolo para distribuir y registrar claves públicas. Lo que hace es ocultar la parte compleja que surge con PKI (Infraestructura de Clave Pública). Está compuesto de dos partes que son: el registro de la clave pública (X-KRSS) y la información de clave pública (X-KISS).

El elemento Signature encapsula la firma digital. Contiene tres subelementos: *SignedInfo, SignatureValue* y *KeyInfo.*

- **SignedInfo:** contiene información sobre qué es lo que se firma y cómo se firma, es decir, contiene la información necesaria para crear y validar la firma. Este elemento contiene dos algoritmos. Por un lado, está el CanonicalizationMethod que es el algoritmo de transformación de SignedInfo antes de realizar la firma digital. Por otro lado, estaría el método de firma SignatureMethod, que sería el algoritmo utilizado para calcular el valor de la firma digital. También se incluye en el elemento SignedInfo las referencias a los objetos que se van a firmar Reference que incluye además DigestMethod y DigestValue. La validación de una firma requiere dos procesos que son la validación de la firma y la validación de los resultados de las referencias.

- **CanonicalizationMethod**: es el encargado de indicar el algoritmo para canonizar el elemento SignedInfo, que tendrá lugar durante la creación de la firma. El SignatureMethod, es el encargado de indicar el algoritmo para

general la firma a partir de la canonización de SignedInfo. El resultado obtenido si indicará en el elemento SignatureValue.

- **Referente:** incluye una referencia al objeto que se firmará. Al mismo tiempo incluye el resultado de DigestValue que es el valor resultante.

- **SignatureValue:** contiene el resultado de la firma digital que se ha aplicado sobre el elemento SignedInfo. El resultado de esta firma está codificado y contiene un atributo que es único con el que se identificará la firma en procesos posteriores de validación.

- **KeyInfo**: se trata de un elemento opcional que indica la clave que ha de utilizarse para validar la firma. El elemento KeyValue, especifica la clave para validar la firma digital.

1.2 Firma Electrónica.

Técnicamente la firma electrónica es un conjunto o bloque de caracteres que viajan junto a un documento, fichero o mensaje y que puede acreditar cuál es el autor o emisor del mismo –lo que se denomina autenticación- y que no ha sido manipulado o modificado el mensaje en el transcurso de la comunicación. Puede definirse también como el conjunto de datos, códigos o claves criptográficas privadas, en forma electrónica, que se asocian inequívocamente a un documento electrónico, que permite identificar a su autor, es decir que es el conjunto de datos, en forma electrónica, anexos u otros datos electrónicos o asociados funcionalmente con ellos, utilizados como medio para identificar formalmente al autor o autores del documento que la recoge. La firma electrónica no implica asegurar la confidencialidad del mensaje. Un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holeográficamente, a diferencia que el documento en papel solo se ve por personas autorizadas. La firma electrónica es un instrumento con características técnicas y normativas; es decir que existen procedimientos técnicos que permite tanto asegurar el acceso solo a personas autorizadas para éste fin, aunque de igual manera personas no autorizadas podrían tener acceso a dicho datos utilizando procedimientos semejantes o incluso, con claves substraídas de forma ilegal sin tener autorización.

Cuando hablamos de firma electrónica o firma digital, la materia es la misma, cambia la acepción de acuerdo a las diferentes regiones geográficas: conceptos que son relacionados con documentos electrónicos, claves criptográficas, certificados digitales, funciones matemáticas, autoridades certificantes e infraestructuras de clave pública. De esta manera exponemos la definición de:

> **Digital:** Relacionado con los dígitos o con el modo en que son representados. En computación, es análogo o binario porque las

computadoras con las que están familiarizadas la mayoría de las personas procesan información codificada como combinaciones de dígitos binarios (bits) (Diccionario de informática e Internet de Microsoft, 2001: 194).

Firma Digital: *Método de identificación personal basado en el cifrado y en códigos secretos de autorización utilizados para "firmar" documentos electrónicos. (Diccionario de informática e Internet de Microsoft, 2001: 206)*

Documentos electrónicos: se concibe como un medio de expresión de la voluntad con efectos de creación, modificación o extinción de derechos y obligaciones por medio de la electrónica, informática y telemática.

Claves criptográficas: es una pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras mediante la cual, en criptografía, se especifica la transformación del texto plano en texto cifrado, o viceversa. (http://es.wikipedia.org/wiki/Clave_(criptograf%C3%ADa), 20-11-08)

Funciones matemáticas: expresión matemática entre dos conjuntos X e Y, "F: X ⟶ Y".

Certificados Digitales: es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad y su clave pública (http://es.wikipedia.org/wiki/Certificado_digital, 11-4-08)**.**

Autoridad Certificadora: es una entidad de confianza, responsable de emitir y revocar los certificados digitales o certificados, utilizados en la firma electrónica, para lo cual se emplea la criptografía de clave pública.

Infraestructura de clave pública: es una combinación de hardware y software, políticas y procedimientos de seguridad que permiten la ejecución con garantías de operaciones criptográficas como el cifrado, la firma digital o el no repudio de transacciones electrónicas.

Protocolo: relación que se reconoce en la comunicación o en la transferencia de información.

La firma electrónica puede ser de dos tipos: simple o avanzada. La primera se refiere a que, a partir de un previo acuerdo entre las partes y tomando en cuenta una presunción establecida en la ley, se le adjudica a alguien el uso de una clave. Asimismo se establece si determinada comunicación partió de un sistema programado por el emisor o en su nombre para operar electrónicamente. Esto alude a las operaciones o transacciones que se llevan a cabo a través de e-mail. La segunda, de acuerdo a lo que la Universidad Autónoma de México publica en la pagina de internet donde fomenta el uso de la Firma Electrónica Avanzada en tramites administrativos, dentro de esa institución: “consiste en datos en forma electrónica asociados a un mensaje de datos, que son utilizados para acreditar la identidad del firmante en relación con el mensaje y que indican que éste asume como propia la información contenida en él, produciendo los mismos efectos jurídicos que la firma autógrafa” (http://www.firma-electronica.unam.mx/, 12-4-08).

El Banco de México, define a la Firma Electrónica como el conjunto de datos que se agrega o adjunta a un documento electrónico y está asociado en forma lógica

al mismo y al signatario, utilizándola para identificar al autor del documento y asegurar que no fue alterado.

Por otro lado, el Servicio de Administración Tributaria en su portal, identifica a la Firma Electrónica como “un conjunto de datos que se adjuntan a un mensaje electrónico, cuyo propósito es identificar al emisor del mensaje como autor legítimo de éste, tal y como si se tratara de una firma autógrafa. (http://www.sat.gob.mx/; 12-4-08).

Para tener acceso a una Firma Electrónica, es necesario obtener un certificado digital el cual se puede definir como un documento digital mediante el cual una autoridad de certificación garantiza la identidad del sujeto o entidad que solicita la Firma Electrónica y su clave pública. Este certificado regularmente contiene el nombre de la entidad certificada, número de serie, fecha de expiración, una copia de la clave pública del titular del certificado (utilizada para la verificación de su Firma Electrónica), y la Firma Electrónica de la autoridad emisora del certificado, de forma que el receptor pueda verificar que esta última ha establecido realmente la asociación.

Para el Servicio de Administración Tributaria -SAT-, el objetivo de la llamada FIEL es permitir a los contribuyentes cumplir con sus obligaciones fiscales a través de Internet, de manera sencilla, gratuita y segura; ya que es una obligación por parte del contribuyente el obtener su Firma Electrónica, de acuerdo al Código Fiscal de la Federación, publicadas en el Diario Oficial de la Federación el 28 de junio y 27 de diciembre de 2006. La citada dependencia liberará gradualmente los trámites y servicios en donde el uso de la FIEL sea obligatorio.

También asegura el SAT que gracias a sus características tecnológicas, la FIEL, es una herramienta que brinda seguridad en las transacciones electrónicas que realicen los contribuyentes con dicho organismo, ya que permite: verificar que

los mensajes recibidos no hayan sido modificados e identificar al autor del mensaje; su diseño se basa en estándares internacionales de infraestructura de claves públicas (o PKI por sus siglas en inglés: *Public Key Infrastructure*) en donde se utilizan dos claves o llaves, matemáticamente relacionadas, para el envío de mensajes: una de las llaves sólo es conocida por el titular de la FIEL y sirve para cifrar - transcribir en guarismos, letras o símbolos, de acuerdo con una clave, un mensaje cuyo contenido se quiere ocultar- datos, de ahí que se le designe con el término "clave privada". La otra llave, denominada "clave pública", está disponible en internet para consulta de todos los usuarios de servicios electrónicos y sirve para descifrar datos. Afirma la citada dependencia que “en términos computacionales es imposible descifrar un mensaje utilizando una llave que no corresponda”.

La firma electrónica funciona utilizando complejos procedimientos matemáticos, mismo que se citan adelante, que relacionan el documento signado con información propia del firmante, y permiten que terceras partes puedan reconocer la identidad del firmante y asegurarse de que los contenidos no han sido modificados. El firmante genera, mediante una función matemática, una huella digital del mensaje, la cual se cifra con la clave privada del firmante. El resultado es lo que se denomina firma digital, que se enviará adjunta al mensaje original. De esta manera el firmante adjuntará al documento una marca que es única para dicho documento y que sólo él, virtualmente, es capaz de producir. Además se dice que el emisor estaría impedido a negar validamente ser el autor del mensaje, toda vez que asume la responsabilidad por el uso de su clave privada al firmar de puño y letra el documento de aceptación de su certificado digital; en tal virtud, los mensajes así cifrados le son atribuibles ya que la firma electrónica difiere de la autógrafa, en que la primera esta vinculada al documento y al signatario, mientras que la segunda solo depende del signatario y es invariable.

La Secretaría de Hacienda y Crédito Público a través del Servicio de Administración Tributaria, ha realizado un gran esfuerzo, asegura, en que la obtención de la FIEL, no sea una carga más al contribuyente para efecto de cumplir con sus obligaciones de tributación, ejemplo de ello es el servicio de citas telefónicas a fin de ahorrar tiempo, pues se brinda la hora exacta en que será atendido sin necesidad de hacer filas y es informado sobre los documentos con los cuales se tiene que hacer acompañar a su cita, los horarios son amplios de lunes a sábado, afirman que la llamada es atendida en menos de un minuto y la cita es asignada ese mismo día hasta treinta días después; además de tener en su portal de internet la relación de requisitos y documentación necesaria, aplicable a cada tipo de contribuyente.

1.3 Sustento Jurídico sobre la creación de la Firma Electrónica.

El cambio tecnológico ha iniciado su proceso en materia fiscal y de una forma radical, este cambio ha sido gradual en todos los ámbitos, inicialmente en materia civil, el 29 de mayo del año 2000, con la modificación del Código Civil Federal, centrándose en el reconocimiento a la celebración de actos jurídicos a través de medios electrónicos, ópticos o de cualquier otra tecnología, añadiéndose los medios tecnológicos como medio idóneo para expresar el consentimiento; del Código Federal de Procedimientos Civiles, reconociendo como prueba, la información contenida en los medios electrónicos, ópticos o en cualquier otra tecnología, dando una serie de reglas para su valoración por parte del juzgador, la fiabilidad del método para generar, comunicar, recibir o archivar la información -que pueda conservarse sin cambio-, su atribución a las personas obligadas y la posibilidad de acceder a ella en ulteriores consultas, del Código de Comercio, definiendo el concepto “Mensaje de Datos” como la información generada, enviada, recibida, archivada o comunicada a través de medios electrónicos, ópticos o cualquier otra tecnología, la obligación a los comerciantes de conservar por un plazo mínimo de 10 años los originales de aquellas cartas, telegramas, mensajes de datos o cualesquiera otros documentos en que se consignen contratos, convenios o compromisos que den nacimiento a derechos y obligaciones, en el caso de mensajes de datos se requerirá que el contenido de la información se haya mantenido íntegra e inalterada a partir del momento en que se generó por primera vez en su forma definitiva y sea accesible para su ulterior consulta, se estableció una presunción en materia mercantil, salvo pacto en contrario, de que el mensaje proviene del emisor -atribución a la persona obligada- si ha sido enviado: Usando medios de identificación, tales como claves o contraseñas de él (para lo que se requerirá de un previo acuerdo entre las partes), o Por un sistema de información programado por el emisor o en su nombre para que opere automáticamente. En materia mercantil el 29 de agosto de 2003, al igual que

en la civil, cuando la ley exija la forma escrita para los contratos y la firma de los documentos relativos, esos supuestos se tendrán por cumplidos tratándose de mensaje de datos siempre que éste sea atribuible a las personas obligadas y accesible para su ulterior consulta, y se reconoce como prueba a los mensajes de datos -para valorar la fuerza probatoria de dichos mensajes, se estimará primordialmente la fiabilidad del método en que haya sido generada, archivada, comunicada o conservada-. La Ley Federal del Consumidor, reconociendo la utilización de medios electrónicos, ópticos o cualquier otra tecnología en la instrumentación de las operaciones que celebren los proveedores con los consumidores, dando las bases sobre las cuales habrán de realizarse dichas operaciones -confidencialidad, certeza, seguridad en la información proporcionada al consumidor-, previendo sanciones administrativas para el caso de que los proveedores no cumplan con dichas disposiciones.

Así llegó el tan deseado cambio al Código Fiscal de la Federación el cual nos trajo el nacimiento de la Firma Electrónica en un primer momento, posteriormente fue Avanzada, comúnmente conocida como FEA, terminando en una simple Firma Electrónica llamada FIEL.

El cinco de enero del dos mil cuatro, fueron publicadas adiciones al Código Fiscal de la Federación, respecto de la presentación de trámites, manifestaciones y demás documentos mediante los llamados medios electrónicos utilizando la novedosa Firma Electrónica Avanzada; siendo opcional su utilización, para los contribuyentes durante dos mil cuatro y obligatoria en dos mil cinco. De esta manera fue adicionada al mencionado código el capítulo denominado "De los Medios Electrónicos" -artículos 17-D a 17-J-, en el cual se establece la obligación a los contribuyentes a que a partir de enero de dos mil cinco, cumplan sus obligaciones fiscales utilizando en forma obligatoria la vía electrónica, -con antelación a esa época existían contribuyentes que presentaban declaraciones mediante sistemas

electrónicos-, para lo cual la autoridad fiscal proporcionó una firma electrónica llamada " Clave de Identificación Electrónica Confidencial " (CIEC) -sistema de identificación basado en el RFC y el NIP (número de identificación personal)-, a fin de ser utilizado en la presentación declaraciones provisionales y declaraciones anuales. Menos de un año después la Firma Electrónica Avanzada, cambio de acepción para ser solamente la Firma Electrónica que todos conocemos.

Esta FIEL -llamada así hasta 2007- es a partir del uno de enero de 2005, el instrumento que todos los contribuyentes obligados, ya sean personas morales o personas físicas, deben utilizar para cumplir con sus obligaciones de carácter fiscal a través de Internet.

Hay que recordar que el Código Fiscal de la Federación fue modificado el cinco de enero de 2004 y uno de los cambios más interesantes fue en materia de Informática Fiscal ya que surge un capítulo llamado de los medios electrónicos, el cual abarca los artículos 17-C al 17-J. Mencionando en el artículo 17-D la obligación del uso de la FEA –llamada de esta manera en esa época, hoy FIEL- en todos los trámites para el cumplimiento de nuestras obligaciones fiscales que necesiten ser en documento digital.

> Artículo 17-D.
>
> "Cuando las disposiciones fiscales obliguen a presentar documentos, éstos deberán ser digitales y contener una firma electrónica avanzada del autor, salvo los casos que establezcan una regla diferente. Las autoridades fiscales, mediante reglas de carácter general, podrán autorizar el uso de otras firmas electrónicas.- Para los efectos mencionados en el párrafo anterior, se deberá contar con un certificado que confirme el vínculo entre un firmante y los datos de creación de una firma electrónica avanzada, expedido por el Servicio de Administración Tributaria cuando se trate de personas morales y

de los sellos digitales previstos en el artículo 29 de este Código, y por un prestador de servicios de certificación autorizado por el Banco de México cuando se trate de personas físicas. El Banco de México publicará en el Diario Oficial de la Federación la denominación de los prestadores de los servicios mencionados que autorice y, en su caso, la revocación correspondiente.- En los documentos digitales, una firma electrónica avanzada amparada por un certificado vigente sustituirá a la firma autógrafa del firmante, garantizará la integridad del documento y producirá los mismos efectos que las leyes otorgan a los documentos con firma autógrafa, teniendo el mismo valor probatorio.- Se entiende por documento digital todo mensaje de datos que contiene información o escritura generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.-Los datos de creación de firmas electrónicas avanzadas podrán ser tramitados por los contribuyentes ante el Servicio de Administración Tributaria o cualquier prestador de servicios de certificación autorizado por el Banco de México.- Cuando los datos de creación de firmas electrónicas avanzadas se tramiten ante un prestador de servicios de certificación diverso al Servicio de Administración Tributaria, se requerirá que el interesado previamente comparezca personalmente ante el Servicio de Administración Tributaria para acreditar su identidad. En ningún caso los prestadores de servicios de certificación autorizados por el Banco de México podrán emitir un certificado sin que previamente cuenten con la comunicación del Servicio de Administración Tributaria de haber acreditado al interesado, de conformidad con las reglas de carácter general que al efecto expida. A su vez, el prestador de servicios deberá informar al Servicio de Administración Tributaria el código de identificación único del certificado asignado al interesado.- La comparecencia de las personas físicas a que se refiere el párrafo anterior, no podrá efectuarse mediante apoderado o representante

legal. Únicamente para los efectos de tramitar la firma electrónica avanzada de las personas morales de conformidad con lo dispuesto en el artículo 19-A de este Código, se requerirá el poder previsto en dicho artículo.- La comparecencia previa a que se refiere este artículo también deberá realizarse cuando el Servicio de Administración Tributaria proporcione a los interesados los certificados, cuando actúe como prestador de servicios de certificación.- Los datos de identidad que el Servicio de Administración Tributaria obtenga con motivo de la comparecencia, formarán parte del sistema integrado de registro de población, de conformidad con lo previsto en la Ley General de Población y su Reglamento, por lo tanto dichos datos no quedarán comprendidos dentro de lo dispuesto por los artículos 69 de este Código y 18 de la Ley Federal de Transparencia y Acceso a la Información Pública Gubernamental.- Para los efectos fiscales, los certificados tendrán una vigencia máxima de dos años, contados a partir de la fecha en que se hayan expedido. Antes de que concluya el período de vigencia de un certificado, su titular podrá solicitar uno nuevo. En el supuesto mencionado el Servicio de Administración Tributaria podrá, mediante reglas de carácter general, relevar a los titulares del certificado de la comparecencia personal ante dicho órgano para acreditar su identidad y, en el caso de las personas morales, la representación legal correspondiente, cuando los contribuyentes cumplan con los requisitos que se establezcan en las propias reglas. Si dicho órgano no emite las reglas de carácter general, se estará a lo dispuesto en los párrafos sexto y séptimo de este artículo.- Para los efectos de este Capítulo, el Servicio de Administración Tributaria aceptará los certificados de firma electrónica avanzada que emita la Secretaría de la Función Pública, de conformidad con las facultades que le confieran las leyes para los servidores públicos, así como los emitidos por los prestadores de servicios de certificación que estén autorizados para ello en los

términos del derecho federal común, siempre que en ambos casos, las personas físicas titulares de los certificados mencionados hayan cumplido con lo previsto en los párrafos sexto y séptimo de este artículo."

Este artículo es clave vital, ya que a partir del 9° párrafo del artículo 29 nace la posibilidad de la Factura Electrónica y con ella una serie de cambios que aceleran muchos procesos de automatización dentro de las empresas *y,* desde luego, la eficiencia *y* la eficacia serían condiciones que tendrían las empresas que utilizaran los documentos digitales. Los artículos 18 y 31 de este mismo ordenamiento nos mencionan la obligatoriedad de la FIEL en diversos trámites.

Artículo 18

"Toda promoción dirigida a las autoridades fiscales, deberá presentarse mediante documento digital que contenga firma electrónica avanzada".

Artículo 31

"Las personas deberán presentar las solicitudes en materia de registro federal de contribuyentes, declaraciones, avisos o informes, en documentos digitales con firma electrónica avanzada a través de los medios y formatos electrónicos que señale el Servicio de Administración Tributaria mediante reglas de carácter general…".

Esta firma, como *se* puede apreciar, es indispensable para todo trámite que se quiera efectuar ante el SAT ya que en ningún momento hace referencia a la clave CIEC –Clave de Identificación Electrónica Confidencial- misma que en dos mil cinco en el nacimiento del capítulo, fue la pieza fundamental del tan esperado cambio que actualmente es el mecanismo por medio del cual el contribuyente

cumple con sus obligaciones a través de Internet.

Desde luego que la obtención de la FEA (FIEL) debía ocurrir durante todo el 2004 para empezar su utilización a partir del 1° de enero del año 2005, esta es la razón por la que muchos contribuyentes estaban esperando la Resolución Miscelánea 2004 para conocer las requisitos y procedimientos para su obtención; sin embargo, esta Resolución no traía los cambios esperados y es hasta la primera modificación a ésta cuando aparecen estas reglas, de las cuales fue la eliminación del término “avanzada”, a la firma electrónica.

El veintisiete de mayo de dos mil ocho, es publicada en el Diario Oficial de la Federación (DOF) la Resolución Miscelánea para el ejercicio 2008, en donde aparece una nueva estructura de las reglas de resolución miscelánea, las correspondientes a la FIEL se identifican con 11.2.20. Medios Electrónicos. Esta regla tiene varias condiciones a cumplir, es importante comentar que el SAT le ha dado a la firma electrónica avanzada el nombre de FIEL así que de aquí en adelante así se conocerá. Sin embargo, en el pasado era conocida como tu firma, y antes de ello fue la poco agraciada FEA.

1.4 Proceso de Obtención de la Firma Electrónica Avanzada

1.4.1 Cita para su obtención.

Se debe obtener una cita para obtener la FIEL. Para la gestión de la FIEL -Firma Electrónica Avanzada-, podrá obtener información sobre este producto, así como agendar una cita para obtenerla o solicitar soporte técnico para el uso de este servicio, a los números telefónicos que el SAT muestra en su portal de internet: El asesor telefónico que le atienda, antes de registrar su cita, validará su situación fiscal. Para validarla, se verificarán los siguientes datos: registro federal de contribuyentes -RFC- , nombre -personas físicas- y/o razón social -personas morales- y el domicilio fiscal.

En caso de mostrar inconsistencias, el asesor telefónico le solicitará que acuda a la Administración Local de Asistencia al Contribuyente que corresponda a su domicilio fiscal, para poder realizar las aclaraciones respectivas. Algunas de esas inconsistencias pueden ser desde el nombre que no coincide con su RFC, hasta estar registrado como un contribuyente no localizado.Posteriormente, se debe comunicar al centro atención telefónica para solicitar nuevamente cita.

Si el resultado de la validación de la situación fiscal es correcto, el asesor telefónico que le atienda registrará la cita en el sistema y le indicará el folio asignado; este número lo debe proporcionar cuando acuda a la oficina del SAT asignada para su cita.

Lo interesante es que se puede acudir a cualquiera de las administraciones aunque no le corresponda a su domicilio, por ejemplo, si se vive en Chihuahua y se encuentra de visita en Monterrey se podrá solicitar una cita para la obtención de la FIEL en las oficinas en dicha ciudad.

1.4.2 Programa para generar la FIEL y la clave correspondiente.

El siguiente paso es obtener el programa para generar la FIEL es acceder al portal del SAT -www.sat.gob.mx-. En la barra de menus se oprime la opcion de menú despelgandose otros distintos, en este último bloque de opciones selecciona firma electrónica avanzada FIEL y se accede al desarrollo de la firma electrónica.

Sin embargo, si se desea ingresar de manera inmediata a esta pantalla, en el menú principal en la parte inferior izquierda existen lo llamados accesos directos, en donde se oprime "firma electrónica avanzada", de inmediato nos lleva a la descarga del programa. En esta zona damos un clic sobre "como se efectua el trámite" para acceder a la zona previa de descarga del programa. En buscamos la zona "descarga aquí el programa SOLCEDI y su respectivo manual de usuario" seleccionamos el link y comenzamos con la descarga. Para esto se debe seleccionar la dirección donde queremos guardar el programa -comúnmente se hace en mis documentos puesto que es la selección que tiene predeterminada la mayor parte de las computadoras-. Una vez que el programa ha sido descargado se localiza con el explorador de windows, al momento selecciona el archivo para descomprimirlo y una vez hecho lo anterior accede a la aplicación llamada SOLCEDI -Solicitud de Certificado Digital-.

Dentro del programa se abre en "sistema", se desplegarán una serie de submenús, donde seleccionamos "requerimiento de FIEL", donde se solicita:

- RFC. Tiene que capturar el RFC con homoclave (13 caracteres en total). Es la clave del registro federal de contribuyente de la persona que solicita la certificación, esta clave debió ser asignada por el SAT, en un trámite anterior; es única e intransferible, está conformada por una combinación de doce caracteres en el caso de personas morales y de trece para personas físicas. La combinación de caracteres sigue el formato: los primeros son letras (tres para

personas morales y cuatro las personas físicas), los siguientes seis son números que representan la fecha, los último tres son la homoclave conformada por letras y números.

En caso de que la información sea incorrecta o incompleta el sistema notificará error.

En caso de que el RFC sea de una persona moral, en el momento de captúralo, se inhabilita la zona del CURP -Clave Única de Registro de Población- , y se vuelve obligatoria la zona que corresponde el CURP representante legal.

- CURP. Es opcional este campo, en caso de que se capture en forma incorrecta o incompleta, señala un error.
- Correo electrónico. Debe proporcionar una dirección de correo electrónico para realizar el trámite. La dirección de correo electrónico con que cuenta el contribuyente y en la cual recibirá las notificaciones que se generen durante el proceso de certificación digital. Es necesario seguir la estructura definida para este dato, es decir, debe contener una arroba -@-, puntos entre los identificadores de dirección y no utilizar caracteres extraños o acentuados.

  En caso de no proporcionarlo, se presenta un error, o con errores en la captura del correo, con caracteres extraños, con una estructura incompleta.
- Incapacidad o inimputabilidad declarada jurídicamente. Al marcar este objeto, la persona que solicita el Certificado declara que tiene alguna capacidad que no le permite llevar a cabo sus trámites ante el SAT, entonces se le concede la alternativa de nombrar un Representante Legal.
    - RFC del Representante Legal. Este campo se habilitará si el requerimiento a generar es para una persona moral. O en el caso de personas físicas menores de edad o que expresen tener alguna Incapacidad o inimputabilidad declarada

judicialmente. Este campo sólo acepta RFC de personas físicas mayores de edad.

- CURP del Representante Legal. Si se presenta algunos de los casos en que se permita capturar al Representante Legal, entonces se activará este campo para ingresar su Clave única de Registro Poblacional.
  Este dato es de carácter opcional.

- Clave de Revocación. Esta clave es necesaria para poder cancelar el certificado, si se llegase a necesitar. Esta clave debe tener cuando menos una combinación de números y letras, no acepta un solo tipo de carácter y cuando menos ocho caracteres y máximo 25. Es una clave ideada por el contribuyente, con la cual podrá realizar, si es necesario, el trámite de revocación de su Certificado Digital. Se considera la diferencia entre minúsculas y mayúsculas, también se cuentan los espacios en blanco. Debe conformarse por una combinación de números y letras; acepta caracteres especiales.
- Confirmar Clave. Como el campo de Clave de revocación no permite visualizar el dato, es necesario proporcionar una confirmación, es decir, volver a introducir la clave, para poder garantizar que no hay error en el dato, la clave de revocación será aceptada hasta que la comparación indique que los campos son iguales, en caso de no ser así nos envía un nuevo “introducir la clave”, para poder garantizar que no hay error.
- Solicitud de Renovación. Esta caja habilita la herramienta que le permita generar archivo de formato “.ren”, después de generar el requerimiento.

Una vez que la información ha sido capturada selecciona “continuar” para entrar a la siguiente opción. Es la de proporcionar la clave de acceso para proteger su

llave privada y elegir la ruta de almacenamiento del archivo de requerimiento -.req- y de la llave privada -.key-. Los datos de captura son:

- Clave de acceso. Esta clave servirá para que el contribuyente pueda utilizar el certificado, aunque se recomienda sea lo más grande posible, entre 8 y 255 caracteres. De preferencia letras, números y caracteres especiales. Debe considerarse que los espacios en blanco cuentan y que esta clave es sensible a mayúsculas y minúsculas. Además, debe conformarse, al menos, por una combinación de números y letras.
- Confirmar clave. Como en el campo de Clave de Acceso no se permite visualizar el dato, es necesario introducir nuevamente la clave para garantizar que no hay errores al escribirla, esta clave se aceptará hasta que la comparación indique que este campo es igual al de clave de acceso. En caso de que la confirmación no sea idéntica a la clave, aparece un mensaje que nos indica que hay inconsistencias entre las dos claves, o cuando el número de caracteres es inferior a 8.
- Ruta para almacenar el archivo de requerimiento. De manera automática se tiene la ruta donde se encuentra el SOLCEDI, para modificarla oprime el botón de -?-, al abrir la ventana se proporciona la nueva ruta, no se recomienda cambiar el nombre del archivo ya que al salir de la ventana se sustituye por el RFC dado en la primer ventana. Es importante no olvidar la ruta donde se deposita el archivo de requerimiento -.req-, ya que este archivo se utilizará para continuar con el proceso de certificación.
- Ruta y nombre para almacenar el archivo de llave privada: se utilizan las mismas instrucciones que en el párrafo anterior solamente la extensión del archivo es -.key-.
- Una vez que las claves se han capturado y son idénticas, damos clic en el botón “generar” debiendo aparecer un mensaje previo a

la generación de las llaves. En dicho mensaje se oprime “si”, ahora se deben generar los números aleatorios.

- Generación de número aleatorios. Para aumentar la seguridad en sus archivos cifrados, es necesario alimentar una serie de número aleatorios, esta pantalla funciona como auxiliar para generarlos, oprimiendo en “continuar” y acto seguido se inicia el proceso de generación.

  Es importante que el cursor se encuentre en movimiento ya que de otra manera el sistema no generará correctamente; por otro lado, es muy importante que la generación de la llave se haga en un sistema operativo windows 95 a posteriores; a pesar de no ejecutarse correctamente en la versión XP de dicho sistema ya que en caso de generar las llaves éstas no se generan, aunado a ello envía mensaje de error, hasta no tener el sistema operativo compatible con el generador.

Las llaves, tanto la pública -archivo con extensión .req- como la privada -archivo con extensión .key-, han sido generadas y se localizan en la ruta que previamente registramos en el momento del inicio del proceso. Este conjunto es la llamada Firma Electrónica siendo responsabilidad del contribuyente el uso de las mismas. Se sugiere guardar una copia de las mismas en algún dispositivo que se considere seguro en el caso de contingencia.

En el caso de la personas morales hay que recordar que además de existir la FIEL de los representantes legales, será conveniente firmar cartas responsivas por su uso indebido aquellos que tengan acceso a su utilización; cuando son personas físicas, el uso personal de ésta se encuentra garantizado, pero en caso de proporcionar a su contador o a la persona que normalmente presenta sus declaraciones, sería conveniente que se haga ante la presencia de un notario para evitar el mal uso.

Es sumamente necesario conservar la llave privada, la clave de acceso para cifrar la clave privada y la clave de revocación.

1.4.3 Archivo a presentar para la obtención de la FIEL

El siguiente paso es guardar en una unidad USB -siglas en ingles de "*Universal Serial Bus"* o Conductor Universal en Serie, es un dispositivo que sirve para guardar información a partir de ser conectado por el puerto del mismo nombre- el archivo con extensión -.req- o la llave pública pues se debe presentar en el momento de la obtención de su certificado.

Antes de su cita, tiene que reunir toda la documentación que indicó el asesor telefónico, así como la contenida en el USB con el archivo antes mencionado. En caso de que algún documento o el archivo falten no se podrá generar la FIEL. El tiempo promedio estimado de duración para la generación de la Firma Electrónica Avanzada es de quince minutos, según los datos de la autoridad, además es necesario llegar por lo menos diez minutos antes de la hora de su cita.

1.4.4 Documentación necesaria para la acreditación.

Tratándose de personas físicas

- Copia certificada -para cotejo- y fotocopia del acta de nacimiento.

  Personas físicas extrajeras:

  - Original y fotocopia simple del documento migratorio vigente que corresponda, emitido por autoridad competente, con la debida autorización para realizar los actos o actividades que manifiesten en su aviso -prórroga o refrendo migratorio, original para cotejo-.

- Fotocopia debidamente certificada, legalizada o apostillada por autoridad competente, del documento con que acrediten su número de identificación fiscal del país en que residen, cuando tengan obligación de contar con éste en dicho país, y se trate de residentes en el extranjero.

Personas mexicanas por naturalización:

- Carta de naturalización expedida por la autoridad competente debidamente certificada o legalizada, según corresponda y fotocopia simple -documento certificado o legalizado para cotejo-.

- Original (para cotejo) y fotocopia de identificación oficial -Credencial para votar del Instituto Federal Electoral, Pasaporte vigente. Cédula Profesional o Cartilla del Servicio Militar Nacional-.

- Original -para cotejo- y fotocopia del comprobante de domicilio fiscal. Se aceptará cualquiera de los siguientes documentos:

    - Estado de cuenta a nombre del contribuyente que proporcionen las instituciones que componen el sistema financiero, con una antigüedad no mayor a dos meses. Recibos de pago:

    - Último pago del impuesto predial; en el caso de pagos parciales el recibo no deberá tener una antigüedad mayor a cuatro meses y tratándose de pago anual, éste deberá corresponder al ejercicio en curso.

    - Último pago de los servicios de luz, teléfono o agua, siempre y cuando dicho recibo no tenga una antigüedad mayor a 4 meses.

- Última liquidación a nombre del contribuyente del Instituto Mexicano del Seguro Social.

- Contratos de:
    - Arrendamiento, acompañado del último recibo de pago de renta vigente que cumpla con los requisitos fiscales o bien, el contrato de subarriendo acompañado del contrato de arrendamiento correspondiente y último recibo de pago de renta vigente que cumpla con los requisitos fiscales.
    - Fideicomiso debidamente protocolizado.
    - Apertura de cuenta bancaria que no tenga una antigüedad mayor a dos meses.
    - Servicios de luz, teléfono o agua, que no tenga una antigüedad mayor a dos meses.
- Carta de radicación o de residencia a nombre del contribuyente expedida por los Gobiernos Estatal, Municipal ó del Distrito Federal o por las Delegaciones conforme a su ámbito territorial, que no tengan una antigüedad mayor a cuatro meses.
- Comprobante de Alineación y Número Oficial emitido por el Gobierno Municipal o su similar en el Distrito Federal. Dicho comprobante deberá contener el domicilio del contribuyente y antigüedad no será mayor a cuatro meses.

- Solicitud de Certificado de Firma Electrónica Avanzada por duplicado, el cual se descargar en la pagina del SAT.
- Dispositivo de almacenamiento con archivo -.req- o clave pública.

Con respecto a las personas morales:

- Original -para cotejo- y fotocopia del poder general para actos de dominio o de administración del representante legal.

- Original -para cotejo- y fotocopia de identificación oficial del representante legal -Credencial para votar del Instituto Federal Electoral, Pasaporte vigente, Cédula Profesional o Cartilla del Servicio Militar Nacional. Tratándose de extranjeros, documento migratorio vigente-.

- Original -para cotejo- y fotocopia del comprobante de domicilio fiscal. Se aceptará cualquiera de los siguientes documentos:

    - Estado de cuenta a nombre del contribuyente que proporcionen las instituciones que componen el sistema financiero con una antigüedad no mayor a dos meses.

    - Recibos de pago:

        - Último pago del impuesto predial; en el caso de pagos parciales, el recibo no deberá tener una antigüedad mayor a cuatro meses y tratándose de pago anual, éste deberá corresponder al ejercicio en curso.

        - Último pago de los servicios de luz, teléfono o agua, siempre y cuando dicho recibo no tenga una antigüedad mayor a cuatro meses.

    - Última liquidación a nombre del contribuyente del Instituto Mexicano del Seguro Social.

    - Contratos de:

        - Arrendamiento, acompañado del último recibo de pago de renta vigente que cumpla con los requisitos fiscales o bien, el contrato de subarriendo acompañado del contrato de arrendamiento correspondiente y último recibo de pago de renta vigente que cumpla con los requisitos fiscales.

        - Fideicomiso debidamente protocolizado.

- Apertura de cuenta bancaria que no tenga una antigüedad mayor a dos meses.

- Servicios de luz, teléfono o agua, que no tenga una antigüedad mayor a dos meses.

- Carta de radicación o de residencia a nombre del contribuyente expedida por los Gobiernos Estatal, Municipal o del Distrito Federal o por las Delegaciones, conforme a su ámbito territorial, que no tengan una antigüedad mayor a cuatro meses.

- Comprobante de Alineación y Número Oficial emitido por el Gobierno Municipal o su similar en el Distrito Federal. Dicho comprobante deberá contener el domicilio del contribuyente, con antigüedad no mayor a cuatro meses.

a) En caso de fideicomisos, el contrato con firma del fideicomitente, del fideicomisario o de sus representantes legales así como del representante legal de la institución fiduciaria. -original para cotejo-.

b) En caso de Sindicatos, Original y fotocopia del Estatuto de la agrupación y de la Resolución de registro emitida por la autoridad laboral competente -original para cotejo-.

c) Las personas morales residentes en el extranjero deberán proporcionar, acta o documento constitutivo debidamente apostillado o certificado, según proceda. Cuando el acta constitutiva conste en idioma distinto al español, deberá presentarse una traducción autorizada, así como documento con que acrediten su número de identificación fiscal del país en que residan debidamente certificado, legalizado o apostillado según corresponda por autoridad competente, cuando tengan obligación de contar con éste en el país de procedencia.

- Acta constitutiva de la sociedad:
    - *Sociedades mercantiles*: Copia certificada -para cotejo- y fotocopia del acta constitutiva.
    - *Personas distintas de sociedades mercantiles:* Copia certificada -para cotejo- y fotocopia del documento constitutivo, o fotocopia de la publicación en el órgano oficial -periódico o gaceta oficial-.
    - *Asociaciones en participación:* Original -para cotejo- y fotocopia del contrato de asociación en participación, con firma autógrafa del asociante y asociados o de sus representantes legales.
- Solicitud de Certificado de Firma Electrónica Avanzada por duplicado, la cual se puede descargar de la página del SAT.
- Dispositivo de almacenamiento con el archivo -.req- o clave pública.

1.4.5 Acudir a la cita.

Una vez en poder de la documentación señalada en los párrafos precedentes, debe acudir el día de su cita. No debe hacer fila, pase directamente al módulo de registro e información de la Administración Local que le corresponda. Ahí verificarán el folio de su cita, que la documentación esté correcta, finalmente indicarán el área a la que debe dirigirse.

Es atendido por un Agente Registrador, a quien le entregará la documentación solicitada; él consultará en el sistema su situación fiscal y revisará su documentación. Digitalizara los documentos, se toma una foto al solicitante, digitaliza la firma autógrafa y ocho huellas dactilares, se exceptúan los dedos pulgares.

Usted podrá descargar su certificado digital dentro de la página electrónica del SAT en la sección de entrega de certificados, sin embargo en una primera fase, el certificado será proporcionado directamente por el Agente Registrador.

Hay que recordar que se debe obtener una cita vía telefónica y proporcionando un número de folio para acudir el día y hora indicadas, además si deseamos confirmar nuestra cita, podemos ingresar a la dirección electrónica del SAT y consultar el status de nuestra cita. Ingresando el RFC y el número de folio que fue proporcionado, podremos encontrar la situación antes de que se obtenga el certificado y después de que el certificado se ha obtenido. Una vez que el procedimiento ha concluido en el SAT, se entrega la clave pública en el dispositivo de almacenamiento proporcionado en el cual se encuentra el certificado digital que es precisamente el archivo con el que vamos a cumplir todas nuestras obligaciones fiscales a través de Internet, en ese acto se entrega una constancia de este hecho.

Con la obtención del certificado concluye este trámite, siempre se espera no pasar por el tan mexicano peregrinar en la obtención de tramite alguno dentro la administración pública.

En estos certificados podemos apreciar varios detalles técnicos y fiscales, bastan seleccionar los iconos de cada uno de ellos, para desplegar una ventana que brinda sus características como a nombre de quien está el certificado y su vigencia.

CONCLUSIÓN.

Es importante hacer la mención en el sentido que la presente investigación es la primera parte de la tesis para la obtención del grado de maestro en derecho con énfasis en el área fisco administrativa, motivo por el cual, además de ser un estudio de naturaleza descriptiva, las conclusiones aquí expresadas no pueden ser definitivas y por ello me constreñiré a hacer opiniones relacionadas al área comprendida en el presente estudio.

La utilización de recursos informáticos en nuestra vida diaria ha sido desde hace algunos años un tema trascendental, ya que en ellos se encuentra la mayor parte de la información más preciada, la cual revela nuestros hábitos y costumbres, en pocas palabras nuestra vida en lo personal, al ser analizada, nuestra privacidad se ve vulnerada tanto en la seguridad de nuestras cuentas bancarias como en la de nosotros mismos como personas, es por ello que dentro de los sistemas de información debe ser prioridad fundamental el aspecto de salvaguarda dicha información del acceso no autorizado de personas, es decir, la seguridad de nuestra información en primer término es responsabilidad de nosotros y en segundo, pero no menos importante, de las instituciones a las que les confiamos dicha información. Aunado a ello el gobierno debe implementar políticas públicas en materia de manejo eficiente y seguro de la información; con la única finalidad de respetar la confidencialidad de nuestra información, además es su deber enriquecer la legislación al respecto, elaborando normatividades adecuadas, que otorguen seguridad jurídica al gobernado y por ende se castigue eficazmente a quien vulnere la mencionada privacidad.

Por otro lado, la implementación de sistemas tendientes a modernizar y eficientar, los sistemas tributarios en nuestro país, es un avance que tardó en llegar. Es positivo utilizar sistemas electrónicos y el internet con el fin de hacer

eficiente al fisco mexicano; contrarios lo es, el implementar un sistema, que a la consideración del autor, a sabiendas de ser una mala copia del utilizado en otro país –España-, donde existe una ley especialmente creada a fin de regular el uso de los medios electrónicos, costando años, el desarrollo de los sistemas adecuados para la población a beneficiar con este sistema y las políticas de recaudación, y no sustentándolo en un capítulo de un código, reglamentado su uso en resoluciones misceláneas, y mucho menos dejando de lado el que para que el contribuyente cumpla con sus obligaciones tributarias, debe disponer de un sistema de cómputo y un conocimiento sobre su utilización, caso que, se concluye, una parte considerable de los mexicanos, en especial los que habitan zonas rurales y en las periferias de las ciudades, sin dejar a un lado las poblaciones de menor tamaño, no cuentan con estos medios, por lo tanto, al contrario de lo dicho por la autoridad tributaria, no facilita en nada las obligaciones fiscales y menos aun, el hacer atractivo al contribuyente hacia el cumplimiento de sus obligaciones tributarias, puesto que no comprende el sistema además de generar una erogación extra para dicho fin.

Es un hecho que nuestra visión del tema central de la tesis “notificaciones vía electrónica” a penas comienza, pero este trabajo es brecha sobre la cual seguiremos nuestra investigación.

Concluyendo, la reforma que trajo consigo la introducción del capítulo de los medios electrónicos dentro del Código Fiscal de la Federación, así como la reforma al Código Federal de Procedimientos Civiles y al Código de Comercio, en materia de medios electrónicos y transferencia de la información, es un paso que se dio al comienzo de este milenio, el cual fue un muy acertado y necesario, pues comparado con Estados Unidos de Norte América y la hoy llamada Unión Europea, dieron este paso inevitable desde la última década del siglo pasado es por demás necesario que el gobierno de muchos más pasos y con mayor firmeza que los mencionados, pues en un país en vías de desarrollo como el nuestro se necesita para lograr el tan anhelado progreso, siempre aportando los mejores métodos para que el ciudadano común tenga acceso a estos adelantos

sin ver mermada un aspecto de su vida. Aunque se tubo que esperar algunos años para concluir el presente, con especial agradecimiento a Dios y a todas las personas que con las que conté y cuento con su incondicional apoyo para dar este paso y completar el caminar de un capítulo más en mi vida, y porque no, también a aquellos que con sus deseos no tan gratos me hicieron, con mayor ahínco, tomar un camino el cual culmina hoy con una etapa colmada de éxitos, a todos ustedes gracias.

BIBLIOGRAFÍA

- Constitución Política de los Estados Unidos Mexicanos.

- Código Fiscal Federal 2005.

- Arrioja Vizcaino, Adolfo.
  Derecho Fiscal. 5ª Ed.
  México, D.F. 1989

- Defensa Jurídica de los particulares frente a la Administración en México
  PJF, TFJFyA.
  México, D.F. 2000.

- Enciclopedia Jurídica Mexicana.
  Editorial Porrúa,
  México, D.F. 2004

- Nuevo Derecho Mercantil.
  Acosta Romero, Miguel;
  Editorial Porrúa.
  México, D.F. 2003.

- Diccionario de informática e internet de Microsoft
  Sánchez González, Carmelo.
  McGraw Hill.
  Madrid, España 2004

- La firma electrónica y las entidades de certificación.
  Reyes Krafft, Alfredo.
  Ed. Porrúa.
  México 2004.

ELECTROGRAFÍA.

- SERVICIO DE ADMINISTRACIÓN TRIBUTARIA.
  www.sat.gob.mx

- SUPREMA CORTE DE JUSTICIA DE LA NACIÓN.
  www.scjn.gob.mx

- CONGRESO DE LA UNIÓN.
  www.hcucdd.gob.mx

- RÉGIMEN JURÍDICO ACTUAL.
  www.ordenjuridico.gob.mx

- INSTITUTO DE CIENCIAS JURÍDICAS DE LA UNIVERSIDAD AUTÓNOMA DE MÉXICO.
  www.ejuridicas.unam.mx

- FISCALIA
  Revista de Especialistas en Materia Fiscal.
  www.fiscali.com

- IMPUESTUM
  Revista especializada en Materia Fiscal.
  www.impuestum.com

- JURÍDICAS.
  Portal de Noticias Jurídicas, España.
  http://www.juridicas.com

- GESTIÓN DIGITAL.
  Portal del Gobierno de Argentina informativo de la firma electrónica.
  http://www.pki.gov.ar/

- UNIVERSIDAD DE GINORA.
  Portal principal de la Universidad de Ginora, España.
  http://www.civil.udg.es/

- INSTITUTO NACIONAL DE ESTADÍSTICA, GEOGRAFÍA E INFORMÁTICA.
  Portal del INEGI del Gobierno Federal de México.
  http://www.inegi.gob.mx

- REAL ACADEMIA DE LA LENGUA.
  Portal de Internet
  www.rae.es

- ENCICLOPEDIA WIKIPEDIA.
  Portal de la enciclopedia de en internet de microsoft.
  www.wikipedia.org