UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO

INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA

“FIRMA DIGITAL”

M O N O G R A F Í A
QUE PARA OBTENER TÍTULO DE
LICENCIADO EN COMPUTACIÓN
P R E S E N T A:
A B E L A L F A R O N E R I A

ASESOR: LIC. EN COMP. LUIS ISLAS HERNÁNDEZ

PACHUCA DE SOTO, HIDALGO JUNIO 2006

UNIVERSIDAD AUTÓNOMA DEL ESTADO DE HIDALGO
INSTITUTO DE CIENCIAS BÁSICAS E INGENIERÍA
SISTEMAS COMPUTACIONALES

P.D.L.C. ABEL ALFARO NERIA
P R E S E N T E

Por este conducto les comunico que el Jurado que les fue asignado a su trabajo de titulación denominado **"FIRMA DIGITAL"** y que después de revisarlo en reunión de sinodales han decidido autorizar la impresión del mismo, hechas las correcciones que fueron acordadas.

A continuación se anotan las firmas de conformidad de los integrantes del Jurado:

PRESIDENTE:	L.C. ISAIAS PÉREZ PÉREZ
PRIMER VOCAL:	L. C. LUIS ISLAS HERNANDEZ
SEGUNDO VOCAL:	LIC. MARIA ELENA TORRES CUEVAS
TERCER VOCAL:	ING. LETICIA JUÁREZ VARGAS
SECRETARIO:	L.C. THEIRA IRASEMA SAMPERIO MONROY
PRIMER SUPLENTE:	ING. TOMAS RIOS MUÑOZ
SEGUNDO SUPLENTE:	L.C. ISMAEL DOMINGUEZ JIMÉNEZ

Sin otro particular, reitero a usted la seguridad de mi atenta consideración.

ATENTAMENTE
"AMOR, ÓRDEN Y PROGRESO"
Pachuca de soto, Hgo., a 19 de junio de 2006

Lic. Luis Islas Hernandez
Coordinador adjunto de la Lic. en Sistemas Computacionales

Ciudad Universitaria Carretera Pachuca – Tulancingo Km. 4.5 C.P. 42184
Col. Carboneras, Mineral de la Reforma, Hgo.
Tel. 017717172000 Ext. 6301, 6302 Fax ext. 6318
castillo@uaeh.reduaeh.mx

A G R A D E Z C O :

A las personas que influyeron en este trabajo y en mi vida sin dejar de mencionar algunas pero a quienes están siempre en mi corazón y mente pero sobre todo a dios.

Mi esposa May por los tiempos difíciles y mas por los mejores momentos en los cuales nos conocimos y queremos para nuestra vida, Monse, hija gracias por tus alegrías, inocencia y fuerza para terminar este trabajo.

Padres por su amor y compresión infinita, madre por tus rezos y cuidados, padre por tu ejemplo de trabajo y responsabilidad, espero ser padre como Ustedes fueron conmigo.

Y para Pepe y Mike por que sin Ustedes que aburrido seria este mundo, sin quien jugar y hasta pelear pero sobre todo el que estén conmigo

Finalmente y no por ello los menos, a mi familia en Mixquiahuala, Toluca y Cancún: tíos y primos, si se pudo! Y mi familia adoptiva en Cd. Sahagún gracias por su ayuda y paciencia se cumplió esta meta.

CONTENIDO

Tema **Pagina**

INTRODUCCIÓN

Cuando a final de la carrera, se dijo que podría realizar un trabajo monográfico donde cada uno podía elegir su propio tema, se me ocurrió recurrir a un trabajo que había escuchado con una nueva tarjeta bancaria y es el titulo de esta monografía.

Este trabajo, tenia como tema o mejor dicho objeto de estudio a la firma digital, terminología que resultaba nueva para mi, en ese entonces. Pero gracias a la investigación y materia tratadas durante la carrera pude emparentarme con esta terminología y descubrí, detrás de ella, todo un nuevo mundo, que hizo, me interesara cada vez más, y es por eso, que hoy, lo escogí como tema para este trabajo detallado.

Creo, que a esta altura, es bueno aclarar al lector, que este va a ser un trabajo, más bien, descriptivo e informativo, ya que tan solo me voy a avocar a describir, en primer término, todo lo relativo a la transmisión segura de información, definiendo y explicando ciertos conceptos que hacen a la materia, desarrollando las ventajas que ofrece la firma digital, los aspectos técnicos de la misma.

Este es un tema que, a la hora de su análisis, es en realidad bastante simple, porque no se han presentado, en torno a él, posturas encontradas, que pudieran significar un verdadero inconveniente para nuestro derecho; tan solo se podría citar, como uno, la concepción que el código civil tiene de la firma ológrafa o bien servir para usos mas convenientes como voto a distancia, manejo de recursos monetarios con seguridad y fidelidad con socios.

Con todo lo anterior, no queda más que decir que, este es un trabajo que tan solo busca brindar, a aquellas personas que, como yo en un principio, no conocen nada acerca de la firma digital y todo lo que ella significa, una visión general de la misma para que puedan comprender que es lo que ella significa y lo provechoso de su uso, como así también todo lo relativo a su uso en nuestro país, que al momento de realizar esta investigación no estuvieron disponibles o por lo menos no estaban publicadas.

JUSTIFICACIÓN

A lo largo de la historia de la humanidad, ha existido un enorme interés en el desarrollo de métodos que permiten garantizar la confidencialidad de la información y comunicación.

Actualmente vivimos en un mundo en constante cambio en el que siempre se esta persiguiendo la excelencia y la mejora; se busca al igual que en tiempos remotos, los mejores métodos que logren mantener a salvo nuestra información y comunicación. Una de las maneras de lograrla confidencialidad es la firma digital.

Como licenciados en Computación y personas dedicadas o enfocadas a la tecnología de la computación es imperante tener conocimiento de los avances que en dicha materia se realicen así como de las oportunidades que estos proporcionan en diversas áreas y su amplia aplicación.

Al analizar el tema de la firma digital se adquirió y ampliara el conocimiento que permita, a quienes estén de una u otra forma relacionados con esta tecnología, comprender lo relacionado con este tema y las ventajas que puede aportar en diferentes usos, como sufragar un voto a distancia, obtener un certificado o titulo de propiedad sin la necesidad de estar presente u obtener transacciones seguras en compra venta de cualquier cosa.

OBJETIVO GENERAL

Brindar una visión general de la firma digital para lograr la compresión de su significado y proporcionar información sobre su amplia utilización en diversos países así como el seguimiento e implementación para futuros proyectos.

OBJETIVOS PARTICULARES (ESPECÍFICOS)

- Describir lo relativo a la transmisión segura de la información
- Analizar las ventajas y desventajas que giran en torno a la firma digital junto con sus aspectos técnicos.
- Analizar la situación actual en cuanto a su uso en los países, incluyendo a México.

CAPÍTULO I

Criptografía para Todos

En esta sección preparamos una serie de conceptos muy básicos, pero sin perder el rigor del concepto de criptografía. Posibles de ser comprendidos por personas no especialistas.

1.1. ANTECEDENTES

Del Antiguo Egipto a la era digital, los mensajes cifrados han jugado un papel destacado en la Historia. Arma de militares, diplomáticos y espías, son la mejor defensa de las comunicaciones y datos que viajan por Internet.

Esclavos con textos grabados en su cuero cabelludo, alfabetos de extraños símbolos, escritos de tinta simpática, secuencias interminables de números... Desde la Antigüedad, el hombre ha hecho gala de su ingenio para garantizar la confidencialidad de sus comunicaciones. La criptografía (del griego kryptos, "escondido", y graphein, "escribir"), el arte de enmascarar los mensajes con signos convencionales, que sólo cobran sentido a la luz de una clave secreta, nació con la escritura. Su rastro se encuentra ya en las tablas cuneiformes, y los papiros demuestran que los primeros egipcios, hebreos, babilonios y asirios conocieron y aplicaron sus inescrutables técnicas, que alcanzan hoy su máxima expresión gracias al desarrollo de los sistemas informáticos y de las redes mundiales de comunicación.

Entre el Antiguo Egipto e Internet, los criptogramas han protagonizado buena parte de los grandes episodios históricos y un sinfín de anécdotas. Existen mensajes cifrados entre los 64 artículos del Kamasutra, el manual erótico hindú del Vatsyayana, abundan en los textos diplomáticos, pueblan las órdenes militares en tiempos de guerra y, por supuesto, son la esencia de la actividad de los espías.

Los espartanos utilizaron, en el 400 a.c. la Scitala, que puede considerarse el primer sistema de criptografía por transposición, es decir, que se caracteriza por enmascarar el significado real de un texto alterando el orden de los signos que lo conforman. Los militares de la ciudad griega escribían sus mensajes sobre una tela que envolvía una vara. El mensaje sólo podía leerse cuando se enrollaba sobre un bastón del mismo grosor, que poseía el destinatario lícito.

El método de la Scitala era extremadamente sencillo, como también lo era el que instituyó Julio César, basado en la sustitución de cada letra por la que ocupa tres puestos más allá en el alfabeto. En los escritos medievales sorprenden términos como Xilef o Thfpfklbctxx. Para esconder sus nombres, los copistas empleaban el alfabeto zodiacal, formaban anagramas alterando el orden de las letras (es el caso de Xilef, anagrama de Félix) o recurrían a un método denominado fuga de vocales, en el que éstas se sustituían por puntos o por consonantes arbitrarias (Thfpfklbctxx por Theoflactus)

La criptografía resurgió en la Europa de la Edad Media, impulsada por las intrigas del papado y las ciudades-estado italianas. Fue un servidor del Papa Clemente VII, Grabiele de Lavinde, quien escribió el primer manual sobre la materia en el viejo continente. En 1466, León Battista Alberti, músico, pintor, escritor y arquitecto, concibió el sistema polialfabético que emplea varios abecedarios, saltando de uno a otro cada tres o cuatro palabras. El emisor y el destinatario han de ponerse de acuerdo para fijar la posición relativa de dos círculos concéntricos, que determinará la correspondencia de los signos.

Un siglo después, Giovan Battista Belaso de Brescia instituyó una nueva técnica. La clave, formada por una palabra o una frase, debe transcribirse letra a letra sobre el texto original. Cada letra del texto se cambia por la correspondiente en el alfabeto que comienza en la letra clave. Pero los métodos clásicos distan mucho de ser seguros. En algunos casos, basta hacer un simple cálculo para desentrañar los mensajes ocultos. Si se confronta la frecuencia habitual de las letras en el lenguaje común con la de los signos del criptograma, puede resultar relativamente sencillo descifrarlo. Factores como la longitud del texto, el uso de más de una clave o la extensión de esta juegan un papel muy importante, así como la intuición, un arma esencial para todo criptoanalista.

La historia de la criptografía está llena de anécdotas y personajes pintorescos. David Kahn narra en "The Codebreakers" (MacMillan 1967), entre otras, la historia deThomas Jefferson Beale, un aventurero que en 1821, emprendió un arriesgado viaje. Antes de partir, dejó a Robert Morris su huésped, dos documentos cifrados para que los

abriese si él desaparecía. Morris se decidió a hacerlo al cabo de 20 años. Con la ayuda de unos amigos, descifró el segundo texto: era una sucesión de números comprendidos entre el 1 y el 1322, que correspondía a la Declaración de Independencia. Sustituyendo cada número por las iniciales de las palabras de la Declaración, se obtenía la descripción de un tesoro de una tonelada y media de oro, dos y media de plata y gran cantidad de joyas. El lugar en que se encontraba enterrado estaba indicado con precisión en el primer texto. Es una secuencia de 520 números comprendidos entre el 1 y el 2906, pero nadie ha descubierto en base a qué documento están numeradas las palabras, lo que permitiría descifrar el mensaje. Durante un siglo y medio se ha intentado relacionarlo con la Constitución estadounidense y con la Biblia, entre otros textos, y se han realizado costosos análisis por ordenador, sin resultados.

1.2. CONCEPTOS BÁSICOS:

1.2.1. Criptografía:

Es el área del conocimiento que nos proporciona los métodos y algoritmos para transmitir con seguridad la información entre dos puntos. La criptografía se define en la época moderna como aquella que resuelve los problemas de confidencialidad, integridad, autenticidad, no rechazo, etc. La criptografía se divide en dos áreas principales: la criptografía simétrica y la criptografía asimétrica.

1.2.2. Criptografía Simétrica.

Es la parte de la criptografía que resuelve los problemas de confidencialidad e integridad, lo hace principalmente con un algoritmo simétrico (la simetría se refiere a que la clave es la misma en los dos puntos)

1.2.3. Criptografía Asimétrica.

Es la parte de la criptografía que resuelve los problemas de autenticidad y no rechazo, lo hace principalmente con un algoritmo de clave pública(o asimétrico, la asimetría se refiere a que la clave de cifrado es diferente a la clave de descifrado)

1.2.4. Firma Digital.

La firma digital es un procedimiento que se aplica a un archivo por una entidad, y sigue el mismo objetivo de la firma convencional, es decir, con la firma se da fe de la autoría del archivo, del compromiso obtenido bajo lo escrito en ese archivo, etc. La firma digital consiste de dos partes, una del procedimiento de firma y la otra del procedimiento de la verificación de la firma. Si la firma es autentica se acepta la firma, de lo contrario se rechaza la firma.

1.2.5. Intercambio de Claves.

El procedimiento de intercambio de claves es un esquema que usa clave pública para intercambiar la clave simétrica, de esta manera en las aplicaciones seguras la criptografía simétrica siempre se usa conjuntamente con la criptografía asimétrica, con la primera se cifra el archivo, con la segunda se intercambia la clave simétrica.

1.2.6. Sesiones seguras.

Las aplicaciones que usan criptografía resuelven los problemas básicos de seguridad y usan criptografía simétrica y asimétrica, como SSL/TLS, PGP, IPse, WTLS, VoIP, etc.

1.3. CRIPTOGRAFÍA SIMÉTRICA Y ASIMÉTRICA (2000-2005):

Actualmente, la criptografía se puede entender como el conjunto de técnicas que resuelven principalmente los siguientes problemas de seguridad de la información: la autenticidad, la integridad, la confidencialidad y el no rechazo. Desde este punto de vista, la criptografía se divide en dos grandes ramas: la criptografía simétrica y la asimétrica. Esencialmente, con la primera se resuelven los problemas de confidencialidad e integridad, mientras que con la segunda se resuelven los de autenticidad y no rechazo.
En general, el proceso criptográfico se aplica a un mensaje de entrada (al que se le puede llamar mensaje original), y da como resultado el mensaje cifrado. Este mensaje cifrado sólo se puede descifrar (para conocer su contenido) con la clave correspondiente.

La principal diferencia entre la criptografía simétrica y asimétrica, es que en la simétrica la clave de cifrar y descifrar es la misma, mientras que en la asimétrica se tiene una clave para cifrar y otra diferente para descifrar. Otra importante diferencia es que la criptografía simétrica es muy rápida respecto a la asimétrica, por lo tanto la primera se usa para cifrar grandes cantidades de información, mientras que la segunda se usa para intercambiar información secreta pero muy corta. Sin embargo ambos tipos de criptografía se usan conjuntamente en casi todas las aplicaciones. A la criptografía simétrica pertenecen los cifradores de bloques, los cifradores de flujo y las funciones 'hash'. De los cifradores de bloques (se llaman así porque cifran de bloque en bloque de, digamos, 64 bits), podemos citar al famoso DES ('Data Encryption Standar, *Encriptador de Datos Estándar*'); actualmente, se usa una versión más robusta, denominada Triple-DES (consistente en aplicar tres veces DES)A lo largo de los años se han propuesto una cantidad considerable de algoritmos, entre éstos, podemos citar IDEA, LOKI, RC2 ó SKIPJACK.

Entre los cifradores de flujo (se denominan así porque cifran bit por bit o byte por byte), se encuentran RC4 y Seal como los más conocidos. De las funciones 'hash', las más usadas son MD5, SHA-1, SHA-256 y RIPEMD-160.

En septiembre del año 1997 se convocó un concurso de algoritmos, cuyo ganador se denomina AES ('Advanced Encryption Standar, Encriptador Estándar Avanzado'), se espera sea el nuevo estándar de la criptografía simétrica de los próximos 20 años. Este algoritmo, con alguna modificación, puede ser usado como un cifrador de bloque, como uno de flujo o como una función 'hash', además de como generador de cadenas pseudoaleatorias. En octubre del año 2001 se anunció que el ganador es el algoritmo Rijndael, y es publicado en el documento Federal Information Processing Standard *Procesamiento Estándar de Información* (FIPS) 197, El algoritmo se denomina AES con 128 bits de longitud de clave.

En cuanto a la criptografía asimétrica, ésta se clasifica en tres familias principales de algoritmos: la primera basa la seguridad de sus algoritmos en el problema de la

factorización entera, e incluye el sistema RSA, o 'Rivest Shamir Adleman', y el RW, o 'Robin-Williams'.

En la segunda familia se encuentran los sistemas DSA ('Digital Signature Algorithm, *Algoritmo de Firma Digital*'), DH ('Diffie-Hellman'), ElGamal y Nyberg-Rueppel, los cuales basan su seguridad en el problema del logaritmo discreto del grupo multiplicativo de un campo finito. La última familia de criptografía asimétrica basa su seguridad también en el problema del logaritmo discreto elíptico, sobre el grupo de puntos racionales de una curva elíptica sobre un campo finito. Se trata de los mismos algoritmos que en el caso de la segunda familia, pero en versión elíptica. La criptografía asimétrica está dedicada principalmente a resolver el problema de autenticidad y no rechazo, y esto se logra con la firma digital. También es utilizada para el intercambio de claves simétricas.

En la criptografía simétrica hay dos claves, una pública y otra privada. La privada no se puede obtener a partir de la pública, a menos que sé factorice el parámetro 'n', un número entero grande; esto significa que 'n' debe de ser al menos de 768 bits. Se sugiere que 'n' tenga entre 1024 bits (308 dígitos) y 2048 bits (616 dígitos) para proporcionar una alta seguridad. Las claves son muy parecidas en tamaño tanto en los algoritmos basados en la factorización entera como en los basados en el logaritmo discreto. Se estima que este tipo de claves (DE 1024 bits) se puede considerar seguras al menos hasta el año 2015. Entre ellas se encuentra el algoritmo RSA, el más usado en la criptografía asimétrica.

Sin embargo, a causa de la magnitud de la clave, estos sistemas tienen la desventaja de no ser eficientes en dispositivos con recursos reducidos de memoria, de procesamiento y de transmisión. En este caso de recursos limitados, las claves de 163 bits de la criptografía elíptica proporciona la misma seguridad que las de 1024 de RSA; asimismo, las claves de 210 con curvas elípticas proporcionan el mismo nivel de seguridad de las de 2048 de RSA. Por lo tanto para aplicaciones con recursos limitados son preferibles los esquemas con curvas elípticas.

Al presente (2 de Noviembre, 2005), el número más grande que se ha factorizado es de 640 bits (193 dígitos), y (Abril 2004) el logaritmo discreto elíptico mayor que se ha calculado es de 109 bits (32 dígitos)

Recientemente, se han propuesto otros sistemas criptográficos que prometen solventar las deficiencias de sus predecesores, es decir, ser eficientes con pocos recursos proporcionando buena seguridad. Entre éstos se encuentra el sistema NTRU ('Number Theory Research Unit, *Unidad Investigadora de Teoría los Números'*), que basa su seguridad en la elección de la base de una retícula. Los inventores de este sistema lo promocionan como el sistema criptográfico más rápido del mundo (de 20 a 400 veces más rápido que las alternativas existentes)

Otro sistema propuesto es el XTR (ECSTR, 'Efficient and Compaq Subgroup Trace Representation, *Representación Grafica De Subgrupo Eficiente y Compacto'*), que hasta la fecha parece buena opción. Se trata de un sistema muy nuevo, tan sencillo como RSA y tan eficiente como los que usan curvas elípticas. Se basa en una nueva representación de los elementos de un subgrupo del grupo multiplicativo de un campo finito. Es tanto el optimismo de sus inventores que a ECSTR lo llaman también 'Elliptic Curves Soon to Retire, *Curvas Elípticas Rápidas para Acumular* '.

Otro tipo de criptografía de clave pública se debe al uso de un mapeo bilineal, y ha resultado muy buena alternativa, desde el año 2000, han aparecido una gran cantidad de esquemas que se basan en la evaluación del mapeo bilineal (particularmente el mapeo de Tate) Una de las aplicaciones de la criptografía bilineal es la creación de la criptografía basada en la identidad, es decir, que la clave pública puede ser cualquier cadena de caracteres, por ejemplo el nombre, la dirección de correo electrónico, el número de identidad, etc.

Es también conocida la criptografía de clave pública basada en ecuaciones de muchas variables, este tipo de criptografía tiene la ventaja de reducir al máximo la longitud de las variables involucradas.

En la práctica, la criptografía simétrica y asimétrica se unen para poder dar seguridad a una gran parte de aplicaciones donde la transmisión de los datos se realiza por una línea considerada insegura. Por ejemplo, esto ocurre en el protocolo más usado en comercio electrónico, SSL ('Secure Sockets Layer, *Conexión de Capa Segura*'), que utiliza criptografía; también en el protocolo de conexión IPsec y en la aplicación de éste a VPNs ('Virtual Private Networks, *Redes Privadas Virtuales*') Ambos son dos de los protocolos de conexión más seguros que existen, al asumir técnicas criptográficas. Estos Se emplean en redes locales, en Internet, teléfonos, etc., es decir, en casi todas las aplicaciones que utilicen una línea de transmisión de datos.

1.4. LA COMPUTACIÓN CUÁNTICA Y SUS CONSECUENCIAS EN LA CRIPTOGRAFÍA ACTUAL(2000):

En el año de 1982 aparecen las primeras ideas de lo que hoy se conoce como computación cuántica, Feyman observa que ciertos efectos de la mecánica cuántica (leyes de la física a nivel de partículas elementales) no pueden ser simulados por una computadora digital, e insinúa que la computación en general puede ser eficientemente mejorada aprovechando esos efectos de la mecánica cuántica. No es hasta 1985 cuando Deutsch describe un modelo de una computadora cuántica, de alguna manera similar como en 1936 fue propuesto el modelo de la máquina de Turing que sirvió como preámbulo de las actuales computadoras. Un principio de la máquina de Turing es afirmar que puede simular cualquier dispositivo físico, cosa que parece no ser cierta cuando se considera fenómenos de la física cuántica. Sin embargo los modelos de computación cuántica que se han propuesto debe de tener como un caso particular el modelo de la computación actual. Una computadora cuántica es hipotéticamente una máquina que usa los principios de la mecánica cuántica para realizar sus operaciones básicas.

A partir de Deutsch ha existido una gran cantidad de aportaciones a sus ideas, una nueva aportación que puede aparecer en la computación cuántica es una forma diferente de realizar los algoritmos como lo muestra el propuesto por Shor en 1994 para resolver el problema del Logaritmo Discreto y el Problema de Factorización.

En términos básicos la computación tradicional se basa en el manejo de bits, es decir la unidad de información más básica con lo que construye los puentes lógicos y así un lenguaje formal con lo que operan todas las computadoras, en el caso de la computación cuántica se considera el *qubits* que se basa en una propiedad cuántica de la superposición, es decir que un mismo registro almacena al mismo tiempo el valor binario 0 y el 1. Esto permite que un registro de 2 *qubits* almacena los valores 00, 01, 10 y 11, así también un registro con 3 *qubits* almacena entonces los valores 000, 001, 010, 011, 100, 101, 110 y 111, en general un registro de n *qubits* almacena al mismo tiempo 2n valores. Esto quiere decir de forma general que las operaciones que requieren tiempo exponencial se pueden reducir a un tiempo completamente lineal n, lo que naturalmente tendría un impacto en la criptografía actual como lo mostró Shor.

Una forma de construir un qupuente es usar la transformada de Hadamard, se puede ver que las entradas a la transformada de Hadamard (|0>, | 0>,... |0>) de un registro de un *n-qubits* se transforman en cualquier estado del tipo (|a1>, |a2>,..., |an>) donde la |ai> es cualquier suposición del 0 o 1, esto constituye una *qu-función* booleana y así poder construir el *qu-XOR*, *qu-AND*, etc., lo que permitiría efectuar al menos las mismas operaciones de una computadora digital.

En 1997 se ha mostrado que la Resonancia Magnética Nuclear puede ser adaptada para lograr los requerimientos de una computadora cuántica.
En agosto pasado se dio la noticia que en los laboratorios de la IBM se había podido construir una computadora cuántica con 3 *qubits*, sin embargo es necesario primero construir computadoras de cientos o miles de qubits para que se considere una buena computadora cuántica además de resolver las dificultades de poder construirla.
Recientemente el equipo de Chaung ha podido construir una computadora cuántica de 5 *qubits*, generalizando el algoritmo de Shor para generar el orden de una permutación, el corazón de esto es usar la transformada de Furier cuántica que permite determinar más eficientemente la periodicidad desconocida de una función que no se sabe nada de ella.

En el experimento se usa una molécula con 5 spins sujeto a un campo magnético estático, que funciona como un *qubits*. Estos *qubits* fueron manipulados usando resonancia magnética nuclear. En este caso se resolvió el problema de "orden-finding" que simplemente significa encontrar un número mínimo de aplicaciones de una función f, hasta regresar a su estado inicial, algo similar a encontrar el orden de un elemento en un grupo finito. Cuando se colocan en un campo magnético estático cada spin tiene dos valores propios de energía discreta spin-up |0> y spin-down |1>, descritos por un Hamiltoniano. Todo esto constituye un *5-qubits* en donde se pudo construir el puente lógico que efectúa eficientemente el algoritmo que resuelve el problema de "orden-finding" controlando en este caso el problema de "coherent" o de múltiple correspondencia, que es uno de los problemas más complicados para poder construir computadoras cuánticas de varios *qubits*.

Obviamente existen tanto tendencias pesimistas que afirman que las computadoras cuánticas nunca se podrán construir, como afirmaciones, que predicen que es solo cuestión de años, es naturalmente difícil predecir cuándo se podrá tener una computadora cuántica, pero conforme pasa el tiempo se ve más claramente cual es el siguiente escalón en el desarrollo de la tecnología, desde el proceso manual, el mecánico, el electrónico, el digital y ahora el cuántico. Quizá sean entre 20 y 30 años los que tengan que pasar para ver materializada una computadora cuántica.[1]

1.5. FIRMA DIGITAL Y CERTIFICADOS DIGITALES (2002):

Tenemos ahora como propósito tratar de explicar y discutir un poco el concepto de firma digital, que nos llevará al de certificado digital.

Primero consideremos que existe la necesidad de comunicación entre dos entes, por ejemplo dos personas que están en dos países diferentes, por lo tanto una de las mejores formas de comunicación es por Internet. Uno de los problemas más sentidos es ¿cómo saber que efectivamente la persona con quien me estoy comunicando es precisamente la que dice ser?. Este problema lo llamaremos el problema de verificación de Identidad o la autenticación.

Veamos como se ha resuelto este problema en la práctica. Por ejemplo, si dos personas se ven en la calle y éstas ya se conocen anteriormente, simplemente se saludan con sus nombres, esto es cada una de ellas verifica la identidad de la otra visualmente y aceptan que es la persona que ya conocen. La práctica dice que es muy improbable que haya equivocación, salvo casos muy raros, cómo que haya dos personas muy parecidas, que tenga la misma apariencia, en fin, casos que en general no ocurren. Ahora por ejemplo hay dos personas que si se conocen pero que no se ven, por ejemplo que esta una del lado de una puerta y la otra del otro lado, ¿cómo pueden reconocerse? Por ejemplo una de ellas puede preguntar por el nombre de otra y reconocer su voz, quizá preguntarle por algo de su familia que sólo ellos conocen, una vez que estos quedan satisfechos por las respuestas aceptan que la identidad de la otra persona es quien dice ser.

Un caso más complicado es por ejemplo cuando dos personas tienen que validar la identidad pero no se conocen anteriormente. Por ejemplo si una persona va a recoger un boleto de avión a una agencia de viajes y tiene que acreditar si identidad, digamos que el boleto esta a nombre de Jesús Ángel, el empleado de la agencia de viajes acepta la identidad de quien dice ser Jesús Ángel si cumple ciertos requisitos, por ejemplo si le muestra una identificación oficialmente válida (el pasaporte por ejemplo para casi todo el mundo), el empleado compara la foto de la identificación con la apariencia del portador y decide si acepta que quien es portador es realmente Jesús Ángel si la foto es parecida al portador.

Los anteriores ejemplos son muy frecuentes en la vida diaria, de esa manera se pueden aceptar o rechazar la identidad de una persona. Por ejemplo en una escuela al hacer un examen, en el aeropuerto al documentar el viaje, al solicitar un tramite oficial, en fin.

Existe otra circunstancia donde es necesario verificar la identidad, en este casi en general es necesario quedarse con un comprobante de tal verificación, es el caso por ejemplo sí quiero cobrar un cheque, el cajero del banco generalmente pide la

identificación oficial y posteriormente una vez comprobada la identidad visual, pide que este cheque este “firmado”. Este proceso entendido por todos ha sido una forma tradicional de tener un comprobante legalmente aceptado para comprobar a posteriori que yo efectúe esa transacción.

La firma tradicional o de cualquier otro nombre que se le conozca tiene varias características, la principal de ellas es que es aceptada legalmente, esto quiere decir que si alguna persona firmó un documento adquiere tanto los derechos como las obligaciones que de él deriven, y si estas obligaciones no son acatadas el portador del documento tiene el derecho de reclamación mediante un litigio. La autoridad competente acepta las responsabilidades adquiridas con sólo calificar a la firma como válida.

Como en las situaciones donde es necesario verificar la identidad son análogas al último escenario. Nos dedicaremos a estudiar a la “firma” como elemento que sirve para demostrar la identidad.

Podemos resumir que existen dos procedimientos importantes, el primero el proceso de firma, que es el acto cuando una persona “firma” manualmente un documento. Y el proceso de verificación de la firma, que es el acto que determina si una firma es válida o no.

Por otro es importante hacer notar que la firma comprueba la identidad de una persona, de tal modo que así se sabe quién es la persona quien firmó, y que esta persona no puede negar las responsabilidades que adquiere en un documento firmado.

1.5.1. Proceso de Firma:

Este proceso es muy simple y consiste sólo en tomar un bolígrafo y estampar, dibujar o escribir garabatos en un papel. En general este garabato debe ser el mismo y es elegido a gusto de la persona. Se usa como una marca personal. Es importante mencionar que por una lado lo que identifica a la persona quien firma (quien hace el

garabato) es la forma misma de la firma, pero también características de escritura, como la velocidad de escritura, la presión que se aplica al bolígrafo, etc.

1.5.2. Proceso de verificación:

Existen en general dos métodos de verificación de la firma, uno es el más usado y simple, que es el visual, esté método lo aplica cualquier cajero al pagar un cheque, o al efectuar un pago con tarjeta de crédito. En muchos casos la firma es rechazada por no pasar este método, sin embargo legalmente no es suficiente el método visual. El método legalmente definitivo es el peritaje de la firma en laboratorio, que consiste en verificar a la firma independientemente de la forma, tomando en cuenta otras características como la presión de escritura, la velocidad de escritura, etc. El conjunto de estas propiedades son propias de cada país y sus leyes. Recalcamos que el resultado es tomado como definitivo, legalmente.

Por otra parte hacemos notar que con la firma queda resuelto legalmente el problema de la autenticidad o el de comprobar la identidad de una persona.
Y de la misma manera el problema que podría aparecer sí una persona rechaza ser el autor de una firma es también resuelto con los métodos anteriores, al menos legalmente.

Es importante hacer notar que la firma frecuentemente se encuentra asentada en un documento de identidad oficialmente válido, como el pasaporte, la credencial de identidad, el permiso de conducir un automóvil, y otros.

Antes de continuar es bueno mencionar algunos conceptos necesarios para explicar lo que sigue. Particularmente sobre la criptografía. La criptografía como ciencia, estudia los problemas básicos de la seguridad en la transmisión de la información por un canal inseguro. La criptografía se divide en criptografía simétrica y criptografía asimétrica. La criptografía simétrica resuelve el problema de la confidencialidad y usa algoritmos como TDES y AES para transmitir información cifrada, y que sólo con una única clave simétrica puede leer el contenido de la información. Esta clave la llamaremos “clave simétrica” y tiene una en general una longitud de 128 bits. El problema aquí es que antes

de realizar la conexión segura es necesario que ambos lados tengan la misma clave simétrica. La criptografía asimétrica consiste en algoritmos basados en problemas de un solo sentido, es decir que por un lado sea muy fácil realizarlo, pero la inversa sea “difícil” de realizarlo, como es problema de la factorización entera, es fácil realizar el producto de dos números pero es “difícil” factorizar un número producto de dos números primos grandes. En este caso tenemos dos claves en cada caso que se le asocian a una entidad, un usuario por ejemplo. Una clave pública que sirve para cifrar información y solo quien tiene la clave privada asociada a esta clave pública puede descifrar el mensaje. Esto es usado para intercambiar claves simétricas. Por otra parte con la clave privada se firman documentos y se verifica la firma con la clave pública.

Es claro que la clave pública puede ser conocida por cualquier persona, sin embargo la clave privada es solo conocida por el dueño a quien se le asociaron el par de claves. La
clave privada debe de guardarse de manera confidencial, ya sea en su computadora personal, en su PDA, en un Smart Card o algún dispositivo personal.

En la práctica la criptografía simétrica y asimétrica se usan conjuntamente. La simétrica para intercambiar grandes volúmenes de información por su rapidez. Y la asimétrica para el intercambio de las claves simétricas y la firma digital.
Con todo lo anterior ya es muy fácil definir los conceptos de firma digital y de certificado digital.

1.5.3. Propiedades de la Firma digital:

Es un número natural, de mas o menos 300 dígitos si se usa el sistema RSA, que tiene las mismas propiedades que la firma convencional. Es decir es posible asociar un número único a cada persona o entidad, existe un método de firma y un método de verificación de la firma. Esta firma digital resuelve satisfactoriamente el problema de autenticación y no rechazo.

1.5.4. Certificado Digital:

Es un archivo de aproximadamente 1k de tamaño que contiene, primero los datos del propietario, después su clave pública y la firma digital de una autoridad competente. Cuando una persona solicita un certificado digital, se generan su par de claves, la pública y la privada. La clave pública viene en el certificado digital explícitamente. La clave privada queda en custodia del propietario del certificado. El tercer elemento importante que tiene el certificado digital es la firma digital de una autoridad certificadora quien esta como aval de que los datos corresponden al propietario. El certificado digital queda muy parecido entonces a un documento oficial de identificación como un pasaporte o una licencia de conducir.

Otra importante característica del certificado digital es que contiene además de lo ya mencionado, el nombre de los algoritmos que se usan para la firma digital.

La firma convencional es usada cuando la comunicación es personal, si esta comunicación fuese por ejemplo por teléfono no es posible usar la firma convencional.
La firma digital esta precisamente diseñada para poder ser usada a grandes distancias, y principalmente cuando esta comunicación esta hecha por dos computadoras e Internet, además puede ser usada por muchos dispositivos electrónicos.

Cabe también mencionar que aunque la firma convencional puede ser enviada vía fax o por un documento que copie el garabato, ésta no es válida legalmente. Esta firma convencional se usa solo por conveniencia de alguna corporación o institución, por ejemplo al usar un sello que estampa la firma de algún ejecutivo, es usada sólo por la rapidez que representa usarla, pero legalmente no es válida. Sólo es válida aquella que es derivada del puño y letra de la persona. Por su parte la firma digital garantiza ser mejor que la convencional y sería de gran beneficio si esta tuviese validez legal.
Quizá la mayor diferencia entre la firma convencional y la firma digital es que la primera en su método de verificación existe una gran probabilidad de error, según algunos hasta del 20%, y en el caso de la firma digital, este error es inapreciable. Es una fuerte razón para que la firma digital tenga valor legal.

El método más usado para firmar digitalmente es el conocido como RSA, lo importante de este método es que es el más usado actualmente y por lo tanto es conveniente usarlo para poder ser compatible. Para que sea seguro la longitud de sus claves (una pública y otra privada) debe de ser de 1024 bits, es decir un número de un poco más de 300 dígitos.

Otro método reconocido para firma digital es el llamado como DSA que es oficialmente aceptado para las transacciones oficiales en el gobierno de USA. Este método usa

también claves del mismo tamaño que RSA, pero esta basado en otra técnica. Aún así, sea podido mostrar que es casi equivalente en seguridad a RSA

Una tercera opción es el método que usa curvas elípticas, este método tiene la ventaja a los dos anteriores a reducir hasta en 160 bits, es decir como 45 dígitos las claves, manteniendo la misma seguridad. Por lo que es más propio para ser usado donde existen recursos reducidos como en Smart Cards *Tarjetas Inteligentes*, PDAs, etc. Actualmente este método se ha integrado como el reemplazo oficial de DSA para el gobierno de USA.

Entre los posibles ataques a los anteriores métodos esta la posible remota construcción de una computadora cuántica, esta podría efectuar una cantidad tan grande de cálculos al mismo tiempo que podría romper los sistemas anteriores, incluso ya existen estos algoritmos que romperían los sistemas. Sin embargo ya existe otro método de forma que aún con la computación cuántica no existe aún algoritmo que pueda romperlos. Este sistema es que esta basado en lattices (*retículas*), se conoce como NTRU (Number Theory Research Unit, *Unidad Investigadora De La Teoría De Los Números*) y entre otras cualidades es más eficiente que RSA.

Existen aún más métodos para firmar, incluso algunos métodos derivados de las anteriores técnicas, sin embargo no han podido tener el impacto de las anteriores, de hecho puede crearse un método de firma para un caso particular.

En la actualidad tenemos un formato (estándar) que se ha extendido casi para todas las aplicaciones, este es el llamado X.509. Este formato contiene los datos del poseedor del certificado, la clave pública del propietario, y la firma de una autoridad certificadora. La mejor propiedad del formato X.509 es que contiene el mínimo necesario de información para poder realizar muchas transacciones, principalmente comerciales y financieras. Sin embargo para otras aplicaciones puede ser un poco robusto.

Un certificado digital, es un archivo que contiene una clave pública y su poseedor una clave privada, con la clave privada podemos firmar cualquier documento, con la clave pública es posible verificar la firma e intercambiar información de forma confidencial, particularmente una clave simétrica.

Para poder obtener un certificado digital es necesario tener un software que genere estos certificados y que nos proporcione ya en formato X.509, para ser compatible. Podemos ver un certificado digital, por ejemplo, si nos conectamos a un sitio por Internet por ejemplo con los populares navegadores Netscape o Explorer y hacer clic en el icono del candado, a partir de ahí podemos llegar a ver el certificado, siempre y cuando este candado este cerrado. La comunicación de un navegador con un servidos se lleva a cabo por medio del protocolo SSL que puede funcionar con al menos un certificado digital.

Como siguiente paso para entender lo que es un certificado digital y la firma digital pueden por ejemplo revisar el artículo “Compras Seguras por Internet” que no es más que un ejemplo de SSL usando un certificado digital.

1.6. LA FIRMA DIGITAL, LAS NUEVAS TECNOLOGÍAS Y SUS CONSECUENCIAS DENTRO DE LOS MARCOS JURÍDICOS ACTUALES(2003):

No hay duda que en la convivencia entre diferentes individuos, las leyes tratan de equilibrar aquellas acciones que no pueden ser superadas por los propios individuos. De tal forma que si alguien tiene alguna diferencia de alguna acción de otra persona o institución puede someter su denuncia a un tercero (un juez), que en este caso mediante

un procedimiento acordado previamente y su interpretación de las leyes, finalmente da una resolución a favor o en contra de lo solicitado. Estamos considerando que en la actualidad este procedimiento es el más aceptado para dirimir diferencias. Sin embargo cabe mencionar que no existe sistema jurídico perfecto, por lo que existe la posibilidad de que este falle incorrectamente. La decisión de un Juez se basa en evidencias que han sido tomadas a lo largo del proceso y que en general se desea que se acercaran a un proceso científico para su sustento.

Particularmente dentro de los procesos jurídicos uno de las decisiones mas acudidas es demostrar la identidad de una persona. Este procedimiento puede encontrarse en verificación de la autoría de documentos. Por ejemplo para saber si un documento fue emitido por un individuo, la relación que existe entre el documento y el individuo legalmente se establece en la firma autógrafa.

Por décadas la firma autógrafa ha servido para identificar la autoría de documentos, sin embargo esta firma desde su invención ha acarreado imperfecciones. Unas de estas son la falsificación y el procedimiento de verificación de la firma. A pesar de esto la firma autógrafa ha servido como el método más aceptado para verificar la identidad de una persona.

La firma en si, tiene dos acciones, la acción de firmar y la acción de verificación de la firma. Para la primera solo basta que un individuo pueda escribir su nombre (rubrica), o algún conjunto de caracteres y líneas particulares. Esta firma no es autorizada por nadie en general, aparece en los documentos de identidad como el pasaporte de la persona que quiere identificarse con esa firma y tal firma tiene validez legal en todo el mundo. La acción de la verificación de la firma, es más complicada sin embargo, en la práctica se lleva a cabo sin mucho cuidado. Podemos ver todos los días este procedimiento al cambiar un cheque o al comprar con una tarjeta de crédito. El proceso de verificación de la firma en general se realiza de forma visual, es decir, el cajero de un banco solo compara la firma del cheque con otra que esta en alguna identificación o que se realice ahí mismo, y de esta manera acepta o rechaza la firma, es decir, acepta o rechaza la identidad del firmante del cheque.

Para casos más difíciles, una firma se puede someter a un procedimiento de verificación, en un litigio. Esta verificación es ordenada por un juez y quiere decir que el procedimiento visual no basta para poder declarar a la firma cono aceptada o rechazada. Este procedimiento lo lleva acabo un perito (un experto) en verificación de firmas. Aunque no existe una norma mundial para determinar con precisión que la firma es autentica, el procedimiento se basa en una serie de pruebas que chequean las características propias de las líneas y que están asociadas a cada individuo. Tales características son por ejemplo: el grueso de la línea, la inclinación de los caracteres usados, la terminación de los caracteres, la curvatura de las líneas, etc. Se considera a la firma autógrafa una biometría, es decir, una característica física propia de cada individuo y que deja marcada estas característica en la firma. Según lo documentado, conque más del 75% de las pruebas sean positivas, entonces un perito puede declarar a una firma como aceptada. De la misma forma el número de pruebas a que se somete una firma es determinado por el perito y depende de su experiencia en el ramo. Estos métodos se han ido refinado al pasar el tiempo, sin embargo, muchos de ellos no corresponden a procedimientos determinísticos y dependen mucho de la experiencia del perito. Los mismos grupos de expertos reconocen que estos procedimientos pueden contar con una probabilidad de error que puede alcanzar el 20%. De tal forma que contamos con un procedimiento de verificación de firma autógrafa con probabilidad de error.

Es también prudente mencionar que este tipo de métodos, han sido usados por muchos años y por lo tanto es complicado y naturalmente difícil pensar que otro tipo de tecnología pueda reemplazar a esta en poco tiempo.

Precisamente nuestro tema principal es mencionar la nueva tecnología que puede reemplazar a la firma autógrafa y que se ha denominado firma digital. En al año de 1976 dos investigadores norteamericanos descubren lo que se denomina la criptografía de clave pública y, como consecuencia de esta, la firma digital.

En 1978, R. Rivest, A Shamir, y L. Adleman, del MIT, proponen él hasta hoy mas usado método de firma digital, denominado RSA. Este método en principio obedece a los mismos principios que la firma autógrafa, es decir, tiene una acción de firma y otra de

verificación de la firma. Antes de entrar a detallar el método podemos adelantar que en este caso el proceso de verificación de la firma es exacto y es prácticamente imposible que haya falsificaciones.

1.6.1 Ventajas de la Firma Digital*:*

Por lo anterior, la primera y principal ventaja de la firma digital en comparación de la firma autógrafa, es que el procedimiento de verificación es exacto y que es imposible en la práctica su falsificación.

Otra ventaja de la firma digital es su portabilidad, es decir, la firma digital puede ser realizada en diferentes puntos del mundo, de forma simultánea y sin necesidad de testigos. Una tercera ventaja que ofrece la firma digital es que esta puede ser compatible con los dispositivos electrónicos actuales. Es decir, el proceso de firma y de verificación son programas que pueden estar almacenados en cualquier procesador contenido en un Smart Card, en un PDA, en una Note Book, en un PC, etc.

1.6.2. Desventajas de la Firma Digital:

Quizá la más notable desventaja actual de la firma digital en contra de la firma autógrafa, es que la primera no es valida legalmente aun en muchos países. Parece ser que esto obedece a una transición natural de esta nueva tecnología, que por lo tanto existe un rechazo en su aceptación a pesar de los grandes beneficios que proporciona.

Otra desventaja visible de la firma digital es que su seguridad depende de la clave privada, es decir, que si la clave privada se compromete por alguna causa, entonces se compromete la seguridad de la firma digital, esto quiere decir que puede ser usada por individuos y eventos no autorizados. Una desventaja más es que la firma digital esta cambiando conforme la tecnología avanza y esto hace que ciertos documentos puedan ser comprometidos.

Por lo que hay que crear métodos que permitan evitar esto. Finalmente damos una conclusión al respecto. Tratando de ser lo más positivos en el caso y tomando en cuenta

la mayoría de opiniones que han aparecido al respecto, podemos mencionar que la firma digital tendrá una aceptación gradual en los procesos financieros y comerciales principalmente.

En esta transición tanto la firma digital como la autógrafa convivirán por un periodo considerable. Respecto al uso de una u otra firma, lo más prudente es considerar que la tecnología debe de ser usada y aprovechada, por lo tanto, se debe de considerar a la firma digital como la alternativa más viable, así ir asumiendo esta tecnología para los nuevos procedimientos que en general hacen uso de las computadoras. Dejar solo para los casos legalmente impedidos a la firma autógrafa.

Por otro lado cabe mencionar que no solo la firma digital ha aparecido en estos últimos 25 años de tecnología digital, así mismo tenemos que temas relacionados con procesos jurídicos, tenemos a Notarios Digitales, que dan fe de la creación de documentos o hechos con tecnología muy parecida a la firma digital. Asimismo, un Análisis Forense a las computadoras involucradas en delitos y la investigación de crímenes usando computadoras.

1.7. SOBRE LA LONGITUD DE LAS LLAVES(2003):

En la mayoría de los sistemas, desde un PC hasta una compleja red de computadoras, existen diferentes llaves de acceso. Estas nos permiten entrar a un sistema y de su seguridad depende que nadie más que los autorizados tengan acceso al sistema.

Las primeras llaves de acceso de las que hablaremos son los PINs (Personal Identification Number), estos son muy usados por ejemplo en un ATM (Automatic Teller Machine) o cajero automático, en las cajas de seguridad de un hotel, en el control de acceso de una puerta electrónica, etc.

Aunque un PIN puede tener hasta 64bits de longitud, es más común usarlo con 4 dígitos numéricos. Es obvio que esta longitud es muy insegura, ya que solo pueden

usarse 104 diferentes PINs y estos pueden recorrerse en menos de un segundo con cualquier PC actual. Sin embargo estos aún se siguen usando. La respuesta ha esto es que un PIN debe de usarse en un ambiente “seguro”, es decir que físicamente no exista riesgo de que alguien pueda ver el PIN o que el dispositivo donde se usa, esté resguardado por otros controles de acceso. Lo que hará entonces difícil que un ataque a fuerza bruta (recorrer todo es espacio posible de llaves) o de inspección visual.

Otro tipo de llaves de acceso son los “Passwords”, un password es usado principalmente en cuentas de e-mail, o acceso a una PC. Este consiste usualmente de entre 6 y 10 caracteres, es decir, desde 48 hasta 80 bits. Un password debe de garantizar la seguridad de acceso a un sistema y al menos debe de resistir dos tipos de ataques comunes, como lo son el ataque de diccionario y el ataque a fuerza bruta. Un ataque de diccionario consiste en recorrer todos los passwords más posiblemente usados, es decir, las palabras que dependiendo del lenguaje usado se piensa pueden usar mas elegidos como passwords, como los nombres propios, combinación de nombres propios y números, etc., según los diseñadores de software que rompen claves de esta manera afirman que mas de la mitad de los passwords usados están formados de esta manera, si son susceptibles a un ataque de diccionario.

Para evitar el primer ataque, el del diccionario, el password debe de ser lo más aleatorio posible, sin embargo este tipo de password, los aleatorios, no son usados ya que no son prácticos. Un password debe ser aprendido y recordado cuando es usado, por lo que en la práctica son más usados passwords fáciles de recordar. No existe un método que sea él mas adecuado, sin embargo la misma practica sugiere uno como el siguiente: en lugar de una palabra fácil de recordar se puede elegir una frase larga pero fácil de recordar, por ejemplo, “Entre los individuos como entre las naciones el respeto al derecho ajeno es la paz”, luego entonces se construye la password tomando la primera letra de la primera palabra y después la segunda de la segunda, la primera de la tercera, la segunda de la cuarta y así sucesivamente, entonces nuestro password queda como “eoioeanlrldjeap”.

Por otra parte un password no debe de ser muy corto ya que esto permitiría ser atacado por fuerza bruta. Respecto a la longitud adecuada de un password lo comentaremos al último. Finalmente otro tipo de llaves de acceso son las conocidas últimamente como claves criptográficas simétricas, este tipo de llaves son usadas para establecer una conexión segura a través de un canal inseguro como Internet o cualquier otro medio de comunicación insegura.

Las claves simétricas deben de ser completamente aleatorias y su generación debe de ser garantizada por un buen software o hardware que genere bits aleatorios. En la actualidad estas claves son de sesión, es decir se generan cada ves que se efectúa una conexión. Estas claves son generadas por un software que en general ya viene incluido en el navegador o en el software que garantiza la conexión, estos procesos son invisibles para el usuario.

Sin embargo para aplicaciones de alta prioridad es recomendable chequear los generadores para estar seguros que las claves son aleatorias. Esto se hace usando un buen algoritmo que se haya probado su calidad, o si no se conoce el algoritmo entonces, se puede someter al generador a algunas pruebas que garantizan la aleatoriedad de sus salidas, como por ejemplo las recomendadas en NIST (National Institute of Standards and Technology, Institución Nacional de Normas y Tecnología)

Finalmente veamos con números, qué longitud de los password o claves es más adecuada, para esto damos los siguientes pasos:

Partimos de un experimento real que se realizó en enero de 1999, donde se rompió a fuerza bruta DES-56, se llevo a cabo con una supercomputadora diseñada explícitamente para el caso, conjuntamente con 100 000 computadoras conectadas por Internet, todo esto logro un poder de cómputo de 245 billones de pruebas por segundo, es decir, 245000000000 de claves se ensayaron cada segundo. DES fue roto en menos de 23 horas, recorriendo un poco más del 25% del espacio de claves.

Tomemos como base ese poder de cómputo, que incluso hoy en día es una buena referencia. Además de suponer que al recorrer al menos el 50% del espacio de claves existe gran seguridad de encontrar la clave. Para el caso de claves de 40 bits, tendríamos un espacio de claves de 240 =1099511627776. Con el poder de computo arriba mencionado, para recorrer el 50% del total es necesario solo 2.2 seg., que se obtiene dividiendo 240/245 billones y después entre dos. Esto es son claves muy inseguras. Para claves de 48 bits, necesitamos 574 seg. = 9.5 minutos, que por lo tanto también consideramos inseguras. El caso de las claves de 56 bits, tendríamos un tiempo de 40 horas. Lo que también determinamos como inseguras. Siguiendo el mismo procedimiento para las claves de 64 bits necesitamos un tiempo de 1.2 años. Que declaramos también como inseguras. Para el caso de 80 bits, el tiempo crece hasta 78234 años.

En estos momentos estamos en posición de determinar si este tiempo es seguro o no, aunque para los más estrictos no lo es, podemos recordar que solo la existencia de la civilización como la conocemos tiene 2000 años, entonces tendrían que pasar más de 30 de estas para llegar a los 70 mil años, con este pequeño razonamiento poder determinar a este tiempo como seguro actualmente. Para 90 bits, el tiempo necesario seria de un poco más de 80 millones de años. Que en este caso las declaramos a las claves como seguras sin duda alguna. Finalmente para las claves de longitud 128 bits, necesitamos un tiempo explícito de 22020985858787784059 años, es decir, 2.2 x 10^19 años, que definitivamente es seguro para nuestros días.

Por lo tanto, respecto a los passwords podemos sugerir que se construyan de una forma fácil de recordar y tengan una longitud de al menos 10 caracteres. Para probar que estos son de buena calidad lo podemos someter a un software comercial que nos garantice que es resistente a un ataque de diccionario.

Respecto a las claves simétricas, la razón de tener 128 bits es más de implementación, ya que las computadoras trabajan con bloques de memoria múltiplos de 32 bits, sin embargo podemos con toda seguridad usar claves simétricas desde 90 bits y que sean generadas aleatoriamente.

Las estimaciones más optimistas predicen que las claves de 80 serán rotas hasta el 2010, las de 112 hasta el 2030 y las de 128 hasta los años posteriores a 2030.
Otro tipo de claves en uso, son las de la criptografía de clave pública muy usadas en el protocolo SSL, en este tipo de claves las más usadas son las del algoritmo RSA, un último comparativo se dice que las claves de 1024 actualmente usadas como seguras, tienen la misma seguridad de las de 80 bits, las de 2048 usadas para autoridades certificadoras tienen la misma seguridad de las de 112, y las de 3072 tienen la misma seguridad de las de 128 bits.

1.8. CRIPTOGRAMAS EN LA RED

Alertado por las posibilidades que las innovaciones tecnológicas abrían, el Gobierno estadounidense intentó, en los años cincuenta, introducir el DES (Data Encryption Standard), un sistema desarrollado por la NSA (National Security Agency, Agencia Nacional de Seguridad) El objetivo era que todos los mensajes cifrados utilizaran el DES; un intento de control que pocos aceptaron.

No ha sido el único. Philip Zimmermann, un criptógrafo aficionado, levantó hace unos años la ira del Gobierno estadounidense. Su delito fue idear un sistema de codificación aparentemente inviolable, el PGP (Pretty Good Privacy, Privacidad Buena Bonita), y distribuirlo por las redes de comunicación para que cualquiera pudiera utilizarlo. Algo que no podía agradar a quienes ven en la criptografía un arma de doble filo, útil para los gobiernos y funesta en manos de terroristas y delincuentes.

Con la expansión de la red se ha acelerado el desarrollo de las técnicas de ocultación, ya que, al mismo ritmo que crece la libertad de comunicarse, se multiplican los riesgos para la privacidad. La Agencia de Protección de Datos, máximo órgano español para velar por la intimidad personal frente al abuso de las nuevas tecnologías, ha advertido de que, a no ser que se utilice un mecanismo de cifrado, debe asumirse que el correo electrónico no es seguro. Métodos como el asimétrico de clave pública defienden la confidencialidad del correo electrónico, fácilmente violable sin ellos, o la necesaria seguridad de las compras por Internet. Sin embargo, la duda persiste. ¿Son capaces las

complejas claves actuales de garantizar el secreto? Muchas de las técnicas que se han considerado infalibles a lo largo de la Historia han mostrado sus puntos débiles ante la habilidad de los criptoanalistas, desde los misterios de Enigma, que cayeron en poder del enemigo, hasta el DES, desechado por el propio Gobierno estadounidense por poco fiable.

Pero a pesar de los muchos rumores que hablan de la poca seguridad que garantizan las transmisiones vía Internet, es muy improbable que un estafador pueda interceptar los datos reservados de una transacción, por ejemplo, el número de una tarjeta de crédito, porque los formularios que hay que rellenar han sido diseñados con programas que cifran los datos. Los hay tan simples como el Ro13, que sustituye cada letra por la situada 13 puestos más adelante, o extremadamente complicados.

En palabras de un apasionado de la criptografía, Edgar Allan Poe, "es dudoso que el género humano logre crear un enigma que el mismo ingenio humano no resuelva".

CAPÍTULO II

Aplicaciones

La firma digital es definida como una secuencia de datos electrónicos,.esto es empleado en varios ámbitos para un desarrollo tecnológico, comercial y hasta electoral.

2.1. DESCRIPCIÓN:

El concepto de firma digital nació como una oferta tecnológica para acercar la operatoria social usual de la firma ológrafa (manuscrita) al marco de lo que se ha dado en llamar el ciberespacio o el trabajo en redes.

Consiste en la transformación de un mensaje utilizando un sistema de cifrado asimétrico de manera que la persona que posee el mensaje original y la clave pública del firmante, pueda establecer de forma segura, que dicha transformación se efectuó utilizando la clave privada correspondiente a la pública del firmante, y si el mensaje es el original o fue alterado desde su concepción.

Las transacciones comerciales y el hecho de tener que interactuar masiva y habitualmente por intermedio de redes de computadoras le dio lugar al concepto. Pero, sólo después que los especialistas en seguridad y los juristas comenzaran a depurarlo alcanzó un marco de situación como para ocupar un lugar en las actuaciones entre personas, ya sea jurídicas o reales.

El fin, de la firma digital, es el mismo de la firma ológrafa: dar asentimiento y compromiso con el documento firmado; y es por eso que a través de la legislación, se intenta acercarla, exigiéndose ciertos requisitos de validez. El papel es el medio de almacenamiento, y el mecanismo es alguno de los tipos de impresión posibles (tinta, láser, manuscrito, etc.) Esta cualidad física le da entidad al documento, contiene sus términos, conceptos y sentidos de una manera perdurable, y al ser un elemento físico cualquier alteración dejará "señales" identificables.

Pero, los papeles ocupan lugar y pesan demasiado, resulta complejo y molesto buscar información en ellos (requiriendo de la acción humana ya sea al archivarlos y/o al rescatarlos), y el compartir los documentos también resulta inconveniente, lo que se podría evitar con un sistema de computación.

La firma digital se puede aplicar en las siguientes situaciones:

- ✓ E-mail
- ✓ Contratos electrónicos
- ✓ Procesos de aplicaciones electrónicos
- ✓ Formas de procesamiento automatizado
- ✓ Transacciones realizadas desde entidades financieras alejadas
- ✓ Transferencia en sistemas electrónicos, por ejemplo si se quiere enviar un mensaje para transferir $100,000 de una cuenta a otra. Si el mensaje se quiere pasar sobre una red no protegida, es muy posible que algún adversario quiera alterar el mensaje tratando de cambiar los $100,000 por $1,000,000, con esta información adicional no se podrá verificar la firma lo cual indicará que ha sido alterada y por lo tanto se denegará la transacción

En aplicaciones de negocios, un ejemplo es el Electronic Data Interchange (EDI) intercambio electrónico de datos de computadora a computadora intercambiando mensajes que representan documentos de negocios. En sistemas legislativos, es a menudo necesario poner un grupo fecha / hora a un documento para indicar la fecha y la hora en las cuales el documento fue ejecutado o llegó a ser eficaz. Un grupo fecha / hora electrónico se podría poner a los documentos en forma electrónica y entonces firmado usando al DSA o al RSA. Aplicando cualquiera de los dos algoritmos al documento protegería y verificaría la integridad del documento y de su grupo fecha / hora.

A diferencia de la firma manuscrita, que es un trazo sobre un papel, la firma digital consiste en el agregado de un apéndice al texto original, siendo este apéndice, en definitiva, la firma digital; al conjunto formado por el documento original más la firma digital se lo denominará mensaje.

Este apéndice o firma digital es el resultado de un cálculo que se realiza sobre la cadena binaria del texto original.

En este cálculo están involucrados el documento mismo y una clave privada (que, generalmente, pertenece al sistema de clave pública-privada o sistema asimétrico) la cual es conocida sólo por el emisor o autor del mensaje, lo que da como resultado que para cada mensaje se obtenga una firma distinta, es decir, a diferencia de la firma tradicional, la firma digital cambia cada vez con cada mensaje, porque la cadena binaria de cada documento será distinta de acuerdo a su contenido.

A través de este sistema podemos garantizar completamente las siguientes propiedades de la firma tradicional:

Quien firma reconoce el contenido del documento, que no puede modificarse con posterioridad (integridad)

Quien lo recibe verifica con certeza que el documento procede del firmante. No es posible modificar la firma (autenticidad)

El documento firmado tiene fuerza legal. Nadie puede desconocer haber firmado un documento ante la evidencia de la firma (no repudio)

El concepto de criptografía de clave pública fue introducido por Whitfield Diffie y Martin Hellman a fin de solucionar la distribución de claves secretas de los sistemas tradicionales, mediante un canal inseguro. Este sistema utiliza dos claves diferentes: una para cifrar y otra para descifrar. Una es la clave pública, que efectivamente se publica y puede ser conocida por cualquier persona; otra, denominada clave privada, se mantiene en absoluto secreto ya que no existe motivo para que nadie más que el autor necesite conocerla y aquí es donde reside la seguridad del sistema.

Ambas claves son generadas al mismo tiempo con un algoritmo matemático y guardan una relación tal entre ellas que algo que es encriptado con la privada, solo puede ser desencriptado por la clave pública. Resumiendo, la clave privada es imprescindible para descifrar criptogramas y para firmar digitalmente, mientras que la clave pública debe

usarse para encriptar mensajes dirigidos al propietario de la clave privada y para verificar su firma.

Si bien no se trata de un tema estrictamente técnico, es conveniente aclarar que en tiempo de generación de cada par de claves, pública y privada, podría intervenir otra clave que es la de la Autoridad Certificante, que provee la garantía de autenticidad del par de claves generadas, así como también, su pertenencia a la persona cuya propiedad se atribuye. Este esquema se utiliza en intercambios entre entidades cuando se trata de transferencias electrónicas de dinero, órdenes de pago, etc. donde es indispensable que las transacciones cumplan con los requisitos de seguridad enunciados anteriormente (integridad, autenticidad, no repudio del origen, imposibilidad de suplantación, auditabilidad y acuerdo de claves secretas), pero no se satisface el concepto de confidencialidad de la información (secreto)

El proceso de firma digital de un mensaje electrónico comprende en realidad dos procesos sucesivos: la firma del mensaje por el emisor del mismo y la verificación de la firma por el receptor del mensaje. Esos dos procesos tienen lugar de la manera que se expresa a continuación, en la que el emisor del mensaje es designado como *Ángel* y el receptor del mensaje es designado como *Blanca*:

2.2. FIRMA DIGITAL DE UN MENSAJE ELECTRÓNICO.

Ángel (emisor) crea o redacta un mensaje electrónico determinado (por ejemplo, una propuesta comercial)

El emisor (*Ángel*) aplica a ese mensaje electrónico una función hash (algoritmo), mediante la cual obtiene un resumen de ese mensaje.

El emisor (*Ángel*) cifra ese mensaje-resumen utilizando su clave privada.

Ángel envía a *Blanca* (receptor) un correo electrónico que contiene los siguientes elementos:

- El cuerpo del mensaje, que es el mensaje en claro (es decir, sin cifrar). Si se desea mantener la confidencialidad del mensaje, éste se cifra también pero utilizando la clave pública de *Blanca* (receptor).
- La firma del mensaje, que a su vez se compone de dos elementos:
- El hash o mensaje-resumen cifrado con la clave privada de Ángel.
- El certificado digital de Ángel, que contiene sus datos personales y su clave pública, y que está cifrado con la clave privada del Prestador de Servicios de Certificación.

2.3. VERIFICACIÓN POR EL RECEPTOR DE LA FIRMA DIGITAL DEL MENSAJE.

1. *Blanca* (receptor) recibe el correo electrónico que contiene todos los elementos mencionados anteriormente.
2. *Blanca* en primer lugar descifra el certificado digital de Ángel, incluido en el correo electrónico, utilizando para ello la clave pública del Prestador de Servicios de Certificación que ha expedido dicho certificado. Esa clave pública la tomará *Blanca*, por ejemplo, de la página web del Prestador de Servicios de Certificación en la que existirá depositada dicha clave pública a disposición de todos los interesados.
3. *Una* vez descifrado el certificado, *Blanca* podrá acceder a la clave pública de *Ángel*, que era uno de los elementos contenidos en dicho certificado. Además podrá saber a quién corresponde dicha clave pública, dado que los datos personales del titular de la clave (*Ángel*) constan también en el certificado.
4. *Blanca* utilizará la clave pública del emisor (*Ángel*) obtenida del certificado digital para descifrar el hash o mensaje-resumen creado por *Ángel*.
5. *Blanca* aplicará al cuerpo del mensaje, que aparece en claro o no cifrado, que también figura en el correo electrónico recibido, la misma función hash que utilizó *Ángel* con anterioridad, obteniendo igualmente *Blanca* un mensaje-resumen. Si el cuerpo del mensaje también ha sido cifrado para garantizar la confidencialidad del mismo, previamente *Blanca* deberá descifrarlo utilizando

para ello su propia clave privada (recordemos que el cuerpo del mensaje había sido cifrado con la clave pública de *Blanca*)

6. *Blanca* comparará el mensaje-resumen o hash recibido de *Ángel* con el mensaje-resumen o hash obtenido por ella misma. Si ambos mensajes-resumen o hash coinciden totalmente significa lo siguiente:

El mensaje no ha sufrido alteración durante su transmisión, es decir, es íntegro o auténtico.

El mensaje-resumen descifrado por *Blanca* con la clave pública de *Ángel* ha sido necesariamente cifrado con la clave privada de *Ángel* y, por tanto, proviene necesariamente de *Ángel*.

Como el certificado digital nos dice quién es *Ángel*, podemos concluir que el mensaje ha sido firmado digitalmente por *Ángel*, siendo *Ángel* una persona con identidad determinada y conocida.

Por el contrario, si los mensajes-resumen no coinciden quiere decir que el mensaje ha sido alterado por un tercero durante el proceso de transmisión, y si el mensaje-resumen descifrado por *Blanca* es ininteligible quiere decir que no ha sido cifrado con la clave privada de *Ángel*. En resumen, que el mensaje no es auténtico o que el mensaje no ha sido firmado por *Ángel* sino por otra persona.

Finalmente, hay que tener en cuenta que las distintas fases del proceso de firma y verificación de una firma digital que han sido descritas no se producen de manera manual sino automática e instantánea, por el simple hecho de introducir la correspondiente tarjeta magnética en el lector de tarjetas de nuestro ordenador y activar el procedimiento.

Gracias a la firma digital, los ciudadanos podrán realizar transacciones de comercio electrónico seguras y relacionarse con la Administración con la máxima eficacia jurídica,

abriéndose por fin las puertas a la posibilidad de obtener documentos como la cédula de identidad, licencia de conducir, pasaporte, certificados de nacimiento, o votar en los próximos comicios cómodamente desde su casa.

En la vida cotidiana se presentan muchas situaciones en las que los ciudadanos deben acreditar fehacientemente su identidad, por ejemplo, a la hora de pagar las compras con una tarjeta de crédito en un establecimiento comercial, para votar en los colegios electorales, con el fin de identificarse en el mostrador de una empresa, al firmar documentos notariales, etc.

En estos casos, la identificación se realiza fundamentalmente mediante la presentación de documentos acreditativos como el CURP, la credencial de elector, el pasaporte o la licencia de conducir, que contienen una serie de datos significativos vinculados al individuo que los presenta, como:

- Nombre del titular del documento.
- Número de serie que identifica el documento.
- Período de validez: fecha de expedición y de caducidad del documento, más allá de cuyos límites éste pierde validez.
- Fotografía del titular.
- Firma manuscrita del titular.
- Otros datos demográficos, como sexo, dirección, etc.

En algunos casos en los que la autenticación de la persona resulta importante, como en el pago con tarjeta de crédito, se puede exigir incluso que estampe una firma, que será comparada con la que aparece en la tarjeta y sobre su documento de identificación. En el mundo físico se produce la verificación de la identidad de la persona comparando la fotografía del documento con su propia fisonomía y en casos especialmente delicados incluso comparando su firma manuscrita con la estampada en el documento acreditativo que porta. En otras situaciones, no se requiere el CURP o pasaporte, pero sí la firma, para que el documento goce de la validez legal (cheques, cartas, etc.), ya que ésta vincula al signatario con el documento por él firmado.

Ahora bien, en un contexto electrónico, en el que no existe contacto directo entre las partes, ¿resulta posible que los usuarios de un servicio puedan presentar un documento digital que ofrezca las mismas funcionalidades que los documentos físicos, pero sin perder la seguridad y confianza de que estos últimos están dotados? La respuesta, por fortuna, es afirmativa, ya que el uso de la firma digital va a satisfacer los siguientes aspectos de seguridad:

Integridad de la información: la integridad del documento es una protección contra la modificación de los datos en forma intencional o accidental. El emisor protege el documento, incorporándole a ese un valor de control de integridad, que corresponde a un valor único, calculado a partir del contenido del mensaje al momento de su creación. El receptor deberá efectuar el mismo cálculo sobre el documento recibido y comparar el valor calculado con el enviado por el emisor. De coincidir, se concluye que el documento no ha sido modificado durante la transferencia.

Autenticidad del origen del mensaje: este aspecto de seguridad protege al receptor del documento, garantizándole que dicho mensaje ha sido generado por la parte identificada en el documento como emisor del mismo, no pudiendo alguna otra entidad suplantar a un usuario del sistema. Esto se logra mediante la inclusión en el documento transmitido de un valor de autenticación (MAC, Message autentication code, *Código de Autentificación de Mensajes*) El valor depende tanto del contenido del documento como de la clave secreta en poder del emisor.

No repudio del origen: el no repudio de origen protege al receptor del documento de la negación del emisor de haberlo enviado. Este aspecto de seguridad es más fuerte que los anteriores ya que el emisor no puede negar bajo ninguna circunstancia que ha generado dicho mensaje, transformándose en un medio de prueba inequívoco respecto de la responsabilidad del usuario del sistema.

Imposibilidad de suplantación: el hecho de que la firma haya sido creada por el signatario mediante medios que mantiene bajo su propio control (su clave privada

protegida, por ejemplo, por una contraseña, una tarjeta inteligente, etc.) asegura, además, la imposibilidad de su suplantación por otro individuo.

Auditabilidad: permite identificar y rastrear las operaciones llevadas a cabo por el usuario dentro de un sistema informático cuyo acceso se realiza mediante la presentación de certificados. El acuerdo de claves secretas: garantiza la confidencialidad de la información intercambiada ente las partes, esté firmada o no, como por ejemplo en las transacciones seguras realizadas a través de SSL.

CAPÍTULO III

Situación en otros Países

En nuestra nación se va haciendo mas evidente el termino de Firma Digital, pero en algunos países este tema va con mas progresos, haremos notar esos avances en países desarrollados que puedan servir a nuestros proyectos.

3.1. FIRMA DIGITAL EN NACIONES UNIDAS

En las Naciones Unidas una firma digital o numérica es un valor numérico que se consigna en un mensaje de datos y que, gracias al empleo de un procedimiento matemático conocido y vinculado a la clave criptográfica privada del emisor, logra identificar que dicho valor se ha obtenido exclusivamente con la clave privada de iniciador del mensaje.

El procedimiento matemáticos utilizados para generar firmas numéricas autorizadas, se basan en el cifrado de la clave pública. Estos procedimientos aplicados a un mensaje de datos, operan una transformación del mensaje a fin que el receptor del mensaje y poseedor de la clave pública del originante pueda establecer: Si la transformación se efectuó utilizando la clave criptográfica privada que corresponde a la clave pública que él tiene como válida. Si el mensaje inicial ha sido modificado.

3.2. FIRMA DIGITAL EN E.U.

En los Estados Unidos podemos observar la sanción de diferentes leyes relativas a la firma digital, para la creación de una infraestructura de firma digital que asegure la integridad y autenticidad de las transacciones efectuadas en el ámbito gubernamental y en su relación con el sector privado:

3.2.1 Iniciativa del Gobierno Federal

Proyecto "Gatekeeper": Prevé la creación de una autoridad pública que administre dicha infraestructura y acredite a los certificadores de clave pública. En el área de telecomunicaciones: Régimen voluntario de declaración previa para los certificadores de clave pública;

- Ley de certificadores de clave pública relacionados con la firma digital;
- Proyecto de Ley sobre la utilización de la firma digital en los ámbitos de la seguridad social y la salud pública;

- Ley sobre creación, archivo y utilización de documentos electrónicos;
- Ley sobre intercambio electrónico de datos en la administración y los procedimientos judiciales administrativos;
- Iniciativa sobre la creación de una infraestructura de clave pública para el comercio electrónico;
- Ley que autoriza la utilización de documentación electrónica en la comunicación entre las agencias gubernamentales y los ciudadanos, otorgando a la firma digital igual validez que la firma manuscrita. (Ley Gubernamental de Reducción de la Utilización de Papel - "Government Paperwork Elimination Act");
- Ley que promueve la utilización de documentación electrónica para la remisión de declaraciones del impuesto a las ganancias;
- Proyecto piloto del IRS (Dirección de Rentas - "Internal Revenue Service") para promover la utilización de la firma digital en las declaraciones impositivas;
- Proyecto de Ley de Firma Digital y Autenticación Electrónica para facilitar el uso de tecnologías de autenticación electrónica por instituciones financieras;
- Proyecto de Ley que promueve el reconocimiento de técnicas de autenticación electrónica como alternativa válida en toda comunicación electrónica en el ámbito público o privado;
- Resolución de la Reserva Federal regulando las transferencias electrónicas de fondos;
- Resolución de la FDA (Administración de Alimentos y Medicamentos - "Food and Drug Administration") reconociendo la validez de la utilización de la firma electrónica como equivalente a la firma manuscrita;
- Iniciativa del Departamento de Salud proponiendo la utilización de la firma digital en la transmisión electrónica de datos en su jurisdicción;
- Iniciativa del Departamento del Tesoro aceptando la recepción de solicitudes de compra de bonos del gobierno firmadas digitalmente;

Casi todos los estados tienen legislación, aprobada o en Proyecto, referida a la firma digital. En algunos casos, las regulaciones se extienden a cualquier comunicación

electrónica pública o privada. En otros, se limitan a algunos actos internos de la administración estatal o a algunas comunicaciones con los ciudadanos.

Se destaca la Ley de Firma Digital del Estado de Utah, que fue el primer estado en legislar el uso comercial de la firma digital. Regula la utilización de criptografía asimétrica y fue diseñada para ser compatible con varios estándares internacionales. Prevé la creación de certificadores de clave pública licenciados por el Departamento de Comercio del estado. Además, protege la propiedad exclusiva de la clave privada del suscriptor del certificado, por lo que su uso no autorizado queda sujeto a responsabilidades civiles y criminales.

Proyecto piloto de desarrollo de infraestructura de firma digital;

3.3. FIRMA DIGITAL EN ESPAÑA

Camerfirma es la autoridad de certificación digital de las Cámaras de Comercio españolas además de tener experiencia en servicios de outsourcing de Entidades de Certificación.[10]

Actualmente, Camerfirma está participado por el Consejo Superior de Cámaras, y por tres importantes entidades financieras como son Banesto, Bancaja o Caixa Galicia. Existen algunas otras entidades de certificación de ámbitos más locales y sectoriales, así como administraciones autonómicas

Acercar los conceptos de certificación digital y entorno de firma al ciudadano es un paso necesario para facilitar y extender el uso de este tipo de tecnologías, y desde Microsoft queremos mostrar nuestro compromiso con este objetivo. El éxito de proyectos como el DNI digital o las aplicaciones consumidoras de certificados CERES, así como las exitosas iniciativas del sector privado, está relacionado con el número de usuarios en disposición de aprovechar las evidentes ventajas que estos proyectos presentan a los ciudadanos.

La autoridad de certificación más importante en España es la Casa de la Moneda.

3.3.1. Firma digital: segura, privada y fiable

El 9 de abril de 2003, el Consejo de Ministros aprobó el Anteproyecto de Ley de la Firma Electrónica que tiene como objetivo promover el uso de este tipo de rúbrica, como instrumento para generar confianza en las comunicaciones electrónicas y para agilizar los trámites con la Administración.

En España cada vez son más las empresas y usuarios que optan por la firma digital. Un método fiable y seguro, que sustituye a la rúbrica convencional y que posee la misma validez legal. Vivimos en un mundo informatizado, en el que la mayoría de los ámbitos en el que se desenvuelve el día a día de un ciudadano está perfectamente computerizado. Nuestros datos personales figuran en los ordenadores de la Administración Central, compramos a través de Internet, cada vez mandamos más emails y menos cartas convencionales y los empresarios ya no podrían realizar su actividad sin la informática.

Autentificación y seguridad. En este mundo, en esta Sociedad de la Información, ya han empezado a cobrar gran importancia términos como seguridad y autentificación, que se han hecho imprescindibles para que los usuarios se "atrevan", por ejemplo, a dar sus datos a comercios online o a hacer la Declaración de la Renta a través de Internet. A partir de este panorama tecnológico surge la necesidad de contar con un mecanismo, por el cual se pueda demostrar que quien escribe es quien dice ser, que el contenido de su mensaje es auténtico y con la validez legal de la firma manuscrita. Estamos hablando de la firma digital.

3.3.2. Cronología del desarrollo jurídico

22 de abril de 1999

Aprobado el Proyecto de Directiva del Parlamento Europeo sobre firma electrónica por el Consejo de Ministros de Telecomunicaciones de la Unión Europea.

16 de julio de 1999

Aprobado en España el Anteproyecto de Ley de firma digital para adecuar la legislación interna a las exigencias del Proyecto de Directiva del Parlamento Europeo y del Consejo por la que se establece un marco común para la firma electrónica.

18 de septiembre de 1999

Aprobado el Real Decreto Ley 14/1999 de 17 de septiembre sobre firma digital que regulará la firma digital y la actividad de los prestadores de servicios de certificación en España, siendo una transposición del Proyecto de Directiva Europea de firma digital.

21 de octubre de 1999

El Congreso de los Diputados convalida el Decreto Ley de Firma Electrónica, convirtiendo así a la firma electrónica en una realidad jurídica en España incluso antes de que la Directiva Europea sobre el tema haya sido aprobada.

3.3.3. Firma electrónica avanzada

El mismo texto legal proporciona una segunda definición de lo que denomina "firma electrónica avanzada" y que es más exacta y está más acorde con el propósito para el que se crea el texto legal. La definición es la siguiente: "Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos".

En definitiva, con el Real Decreto y el posterior Anteproyecto de Ley lo que se hace es dotar a la firma electrónica de la misma validez e importancia que a la firma tradicional. Es decir, se otorga a los documentos electrónicos del valor legal y de la responsabilidad civil equivalente a los de la firma sobre papel. De esta manera, se sobreentiende también que el contenido del texto rubricado no puede ser alterado ni modificado de ninguna manera.

El texto legal español regula la firma digital, le atribuye validez jurídica y previene el régimen aplicable a los prestadores de servicios de certificación. Y es más, el mismo texto legal proporciona una segunda definición de lo que denomina "firma electrónica avanzada" y que es más exacta y está más acorde con el propósito para el que se crea el

texto legal. La definición es la siguiente: "Es la firma electrónica que permite la identificación del signatario y ha sido creada por medios que éste mantiene bajo su exclusivo control, de manera que está vinculada únicamente al mismo y a los datos que se refiere, lo que permite que sea detectable cualquier modificación ulterior de estos".

En definitiva, con el Real Decreto y el posterior Anteproyecto de Ley lo que se hace es dotar a la firma electrónica de la misma validez e importancia que a la firma tradicional. Es decir, se otorga a los documentos electrónicos del valor legal y de la responsabilidad civil equivalente a los de la firma sobre papel. De esta manera, se sobreentiende también que el contenido del texto rubricado no puede ser alterado ni modificado de ninguna manera.

Además, el Real Decreto-Ley regula este servicio para garantizar la seguridad de los usuarios. En este sentido, recoge las obligaciones que se exigen a los prestadores de estos servicios, las responsabilidades e incluso una serie de sanciones en forma de multa para proteger a los usuarios ante posibles irregularidades, y responder ante daños y perjuicios. Por una infracción considerada por el Decreto Ley como muy grave una empresa podría llegar a pagar 600.000 euros.

3.3.4. Fecha y hora de certificación

En esta línea de defender los intereses del usuario, el Real Decreto-Ley incorpora una novedad, que aparece recogida entre los requisitos exigibles a los prestadores de servicios de certificación. La novedad consiste en permitir que la certificación pueda recoger la fecha y la hora en la que se produce la actuación certificante. Y es que, en algunas ocasiones, la fecha que figura en un documento puede llegar a ser tan importante como que éste vaya firmado.

3.3.5. Verificación de la rúbrica

La firma digital no se puede entender sin este método de encriptación (de codificación de la información) desarrollado por dos ingenieros electrónicos de la Universidad de Stanford (Estados Unidos), Whitfield Diffie y Martin Hellman, en 1976. Estos estudiosos se

dieron cuenta de que aplicando fórmulas matemáticas era posible autentificar la información digital. La firma digital sirve, como venimos diciendo, para verificar la identidad del firmante, para autentificar que el que rubrica es quién dice ser. Además, es imposible que éste sea suplantado, no como ocurre con la firma tradicional que es fácilmente falsificable.

La suplantación por otro individuo no se puede dar porque además de necesitar del certificado para realizar una comunicación, el usuario dispone de una clave secreta privada, que él sólo conoce, y que está protegida bien por una contraseña, por una tarjeta electrónica o mediante el control biométrico, por ejemplo.

La firma electrónica permite que sea detectada cualquier modificación de los datos que han sido rubricados. También ofrece la certeza de que el autor del texto no puede retractarse en el futuro de lo expresado en él.

En España, según datos facilitados a Terra por la FNMT, son 331.269 las personas que la utilizan, siendo Madrid con 75.583 la que mayor número de solicitudes ha registrado. Además, desde 1999, año de la entrada en vigor del Real Decreto-Ley, ha ido aumentando significativamente el número de personas que confía en la firma digital.

La firma digital se puede convertir en un futuro en un elemento clave en cualquier transacción comercial por la gran seguridad que ofrece. Además, el ciudadano de a pié puede encontrar en ella el fin a las colas y al papeleo burocrático que tanto recelo suscita, ya que no tendrá que moverse de casa para hacer la Declaración de la Renta o para solicitar el informe sobre su vida laboral a la Seguridad Social.

3.3.6. Cómo obtener un certificado digital

Para obtener un certificado, necesita solicitarlo a una autoridad de certificación. En esta demostración, se solicitará a VeriSign, líder mundial en el mercado. Puede realizar los siguientes pasos:

Conéctese al centro de identificadores digitales de VeriSign en digitalid.verisign.com.
Seleccione “Personal IDs”.
Pulse el botón “Enroll Now”.

Selecciones el identificador “Class 1Digital ID”, que le permitirá enviar y recibir correo cifrado. Para seguir adelante necesita contar con una dirección de correo válida, ya que este certificado quedará ligado a ella.

Rellene cuidadosamente los campos del formulario. Si no desea pagar, puede obtener un certificada de 60 días de validez. Observe que la conexión es segura (la dirección está precedida de https://). Puede verificar la identidad del sitio web al que está enviando sus datos personales pinchando en el candado, que en Netscape Communicator aparecerá en la parte izquierda de la barra de estado, mientras que en Internet Explorer aparecerá en el centro de la barra de estado. Cuando haya terminado, pulse el botón “Accept”.

A continuación el navegador generará su pareja de claves pública y privada. En el caso de que esté utilizando Internet Explorer, deberá permitir la ejecución de controles ActiveX.

Cuando el proceso anterior termina, se le conduce a una página donde se le informa que debe comprobar su correo en busca de instrucciones acerca de cómo conseguir su certificado. Esta información consiste en la dirección URL de una página web y un PIN.

Cuando reciba el citado correo, utilice el *mismo ordenador y el mismo navegador* para conectarse a esa URL e introduzca el PIN si es que no se lee automáticamente (dependerá del cliente de correo que utilice).

El navegador le guiará a través del proceso de instalación de su certificado, que podrá verificar en la ventana de Información sobre Seguridad, en el apartado de Certificados-->Propios (para Netscape) o en Herramientas-->Opciones de Internet-->Contenido-->Certificados-->Personal (para Internet Explorer).

No debe preocuparse por el navegador que utiliza, ya que en función de si usa Netscape Communicator o Internet Explorer, VeriSign le guiará automáticamente a unas páginas u otras.

CAPÍTULO IV

Uso de Documentos Digitales en el Ámbito Privado

Dado que se han establecido los conceptos y forma de transmisión en forma segura de los datos, que utilidades le han dado ciertas empresas u organismos en el amibito privado

4.1. PORQUE EL DOCUMENTOS DIGITALES EN EL ÁMBITO PRIVADO?

Las ventajas que brinda este sistema hace que cada vez haya más entidades que se adhieren al mismo, instrumentando los procedimientos necesarios para la operatoria en un marco legal de Derecho Privado (acuerdo entre las partes)

Se utilizan lo que se denominan VAN (Valued Added Networks, Redes de Valor Agregado) que, sin utilizar Internet, permiten establecer un vínculo seguro con la otra u otras partes. Por otro lado, los esquemas de encripción, manejo de claves, etc. se hacen siguiendo estándares internacionalmente aceptados que brindan no solo los aspectos de seguridad ya mencionados al comienzo, sino también confidencialidad mediante el uso de encripción del texto completo del mensaje (EDI – Electronic Data Interchange, Intercambio Electrónico de Datos)

EDI es el intercambio Electrónico de Documentos Comerciales en formato estandarizado entre las aplicaciones informáticas de empresas relacionadas comercialmente.

Este formato responde a un estándar internacional (EDIFACT/EANCOM) desarrollado por Naciones Unidas y actualmente utilizado en todo el mundo. En el ámbito internacional, EDI es el sistema de intercambio de documentos electrónicos estandarizados más difundido. A lo largo de los últimos años ha crecido exponencialmente en los países desarrollados tales como E.U., Japón y países de Europa. En el contorno regional, específicamente en América Latina, recién esta dando sus primeros pasos.

A continuación se detalla una lista de algunos de los Documentos Estándar disponibles para establecer la comunicación entre entidades:

PARTIN: Este documento proporcionará la información de las partes.
PRICAT: Catálogos de artículos.

ORDERS: Ordenes de compra.

ORDRSP: Respuesta a la orden de compra.

DESADV: Aviso de despacho.

RECADV: Aviso de recibo

INVOIC: Factura

PAYMUL: Orden de pago

DEBMUL: Aviso de débito

CREMUL: Aviso de crédito

REMADV: Aviso de remesa

4.1.1. Beneficios que aporta el comunicarse a través de este estándar:

- Información rápida y precisa en el lugar indicado.
- Permite un mejor planeamiento de la recepción y el despacho de mensajes.
- Seguridad en el procesamiento de transacciones, se eliminan los errores por el reingreso de información disminuyendo así los problemas generados en la conciliación de facturas y la subsiguiente confección de débitos y créditos.
- Reducción de costos administrativos.
- Disminuye notablemente la cantidad de documentos impresos.
- Fortalece la relación comercial de los "socios del negocio".
- Comunicación permanente las 24 horas los 365 días del año.
- Mejora notablemente la relación comercial de los "socios del negocio".

4.1.2. Los Componentes De Un Sistema EDI

Los tres componentes o estructuras de un sistema EDI son los mensajes estándares, los programas EDI y las (tele) comunicaciones.

Para que las empresas estén en condiciones de operar utilizando un Sistema EDI deberán estar en condiciones de manejar los componentes que a continuación se detallan.

4.2. MENSAJES ESTÁNDARES

EDI y los mensajes estándares han llegado a ser interdependientes a medida que el EDI ha progresado desde sistemas propietarios, sistemas cerrados en un entorno único, a sistemas abiertos. Las distintas aplicaciones que se comunican entre sí necesitan una lengua común con el fin de comprenderse unas con otras.

Este lenguaje común se encuentra en los mensajes estándares EDI y más concretamente en UN/EDIFACT (United Nations Electronic Data Interchange for Administration Commerce and Transport, Datos Electrónicos de Naciones Unidas para el Intercambio de Comercio, Administración y Transporte), los mensajes estándar internacionales EDI y la guías de implementación de UN/ EDIFACT tales como EANCOM.

4.3. PROGRAMAS QUE SOPORTAN EDI

La función básica de los programas que soportan EDI, generalmente conocidos como los convertidores EDI, consiste en la traducción de los mensajes entrantes desde un mensaje estándar tal como EDIFACT/ EANCOM a un formato interno de archivo de una compañía, y el proceso inverso para mensajes que salen de la misma. Sin embargo, además de la función de convertidor, los paquetes de EDI contienen también otras funciones adicionales, las cuales generalmente incluyen conversión de múltiples mensajes estándares y versiones de mensaje, mantenimiento de perfiles de los socios de negocios, interfaces de aplicación, módulos de comunicaciones para intercambiar información directamente o por medio de una o más redes de valor agregado, información de administración de mensajes salientes y entrantes incluyendo referencias para auditoria; manuales sobre menús referentes a los módulos de recibo de información y seguridad o control de acceso a través de contraseñas.

4.4. COMUNICACIONES Y REDES DE EDI

Una vez que los datos de una aplicación se han convertido desde un archivo con formato interno al formato de mensaje estándar por medio del software de EDI, los datos

deben ser comunicados o físicamente transferidos al receptor del mensaje. Aunque es posible transferir los datos por medios magnéticos tales como cintas o disquetes, las telecomunicaciones son parte esencial del concepto EDI.

Las comunicaciones de datos requieren algunas normas de disciplina para lograr una transferencia ordenada de información; esto se realiza mediante los protocolos de comunicación. Adicionalmente, habrá varias opciones de telecomunicaciones / redes que tendrán la función de ofrecer medios para la comunicación de datos. Algunas de estas opciones son la comunicación privada punto a punto, utilizando líneas arrendadas, el uso de la red telefónica pública de datos empaquetados o red de servicios de valor agregado ofrecidas por compañías especializadas.

4.5. COSTOS DEL PROYECTO EDI

Encarar un proyecto de este estilo en una empresa no es una tarea sencilla por cuanto se deben considerar los costos que implica la adopción de este nuevo estilo de trabajo, no solo por los cambios tecnológicos sino por los cambios culturales que implica.

Entre los aspectos más destacados en cuanto costos resaltamos:

Estratégicos, o aquellos costos que insume el tiempo invertido en el planeamiento de todo lo que tenga que ver con el sistema EDI. Este costo implica el tiempo que se tomará el área Gerencial de la entidad en tomar la decisión de implementar EDI, analizando Políticas de Implementación.

Desarrollo, el estudio Económico y el Impacto que la nueva tecnología tendrá sobre las operaciones que actualmente se realizan, adquisición de programas EDI, desarrollo y programación de las interfaces de aplicación, mejoramiento del software de aplicación interno para aprovechar todas las ventajas de un EDI integral y las pruebas necesarias para la óptima implementación de la nueva tecnología.

Educación, este aspecto incluye tanto el entrenamiento del personal interno para redefinir y asumir nuevas responsabilidades en un ambiente de EDI, como así también la educación de los socios de negocios. Implementación, incluye el costo del personal del área de Sistemas de Información que asegura la compatibilidad de las aplicaciones internas con los sistemas de los nuevos socios de negocios.

Intercambios, son los costos asociados con el envío y recibo de mensajes EDI a través de redes privadas o redes de valor agregado. Este costo incluye tanto el Gasto en comunicaciones, como el mantenimiento de todos los elementos que permitan el óptimo funcionamiento de los programas EDI, ya sea Líneas Telefónicas, Cuentas de Usuario en la VAN, Servicio Técnico mensual de los Equipos, etc.

4.6. BENEFICIOS DEL PROYECTO EDI

Los beneficios de la implementación de EDI se presentan al iniciar el proyecto, y los beneficios son más cualitativos e intangibles que cuantitativos. Los podemos sintetizar en los siguientes puntos:

4.6.1. Beneficios administrativos y de procesamiento

Estos son probablemente los beneficios más tangibles obtenidos al implementar un sistema EDI. Los estimativos deben realizarse en el número de documento / ítem por línea procesados por año para cada documento en particular. Los costos relativos al procesamiento de tal documento deben incluir papelería preimpresa, sobres, estampillas, teléfono, fax y costos de fotocopias.

Los estimativos deben ser hechos contemplando el tiempo que se gasta en consecución y ordenamiento de los datos, entrada de los mismos, mecanografía, fotocopias, archivo, correo y fax y lo más importante, en el control y corrección de errores de cada ítem por línea. El intercambio directo de datos entre una aplicación y otra eliminará los frecuentes y costosos errores que se producen inevitablemente cuando los datos son manejados e intercambiados manualmente.

4.6.2. Beneficios por la reducción del ciclo de los negocios

Un sistema EDI exitoso reducirá substancialmente el tiempo de realización de una transacción, sea del tipo que fuere. EDI no solamente conducirá a un ciclo de negocios más rápido sino además, a una mejor calidad de la información compartida entre los socios de negocios.

4.6.3. Beneficios Estratégicos

A pesar de que EDI tiene algunos costos y beneficios claros, es antes que todo una forma de hacer negocios, siendo los beneficios estratégicos los más importantes. Estos incluyen aspectos tales como mayor satisfacción del cliente, las mejores relaciones entre empresas y fortalecimiento de las relaciones de negocios. Otros beneficios estratégicos pueden incluir incrementos sostenidos en la participación en el mercado y ventajas competitivas.

Los beneficios estratégicos son difíciles de cuantificar pero presentan una respuesta a las necesidades del mercado. Aunque puede ser fácil demostrar que EDI conducirá a un incremento en la participación del mercado y cuantificar el valor de este incremento, será difícil predecir que tanto se incrementará esta participación gracias a un sistema EDI.

4.7. SEGURIDAD DE LA INFORMACIÓN TRANSMITIDA

Como sabemos, en un Sistema de Comunicación de Datos, es de vital importancia asegurar que la Información viaje segura, manteniendo su autenticidad, integridad, confidencialidad y el no repudio de la misma entre otros aspectos. Estas características solo se pueden asegurar utilizando las Técnicas de Firma Digital Encriptada y la Encriptación de Datos. A continuación se realiza un breve comentario sobre métodos de encriptación, para poder encriptar un dato, se pueden utilizar tres procesos matemáticos diferentes: los algoritmos HASH, los simétricos y los asimétricos.

4.7.1. Algoritmo HASH:

Este algoritmo efectúa un cálculo matemático sobre los datos que constituyen el documento y da como resultado un número único llamado MAC. Un mismo documento dará siempre un mismo MAC.

4.7.2. Algoritmos Simétricos:

Utilizan una clave con la cual sé encripta y desencripta el documento. Todo documento encriptado con una clave, deberá desencriptarse, en el proceso inverso, con la misma clave. Es importante destacar que la clave debería viajar con los datos, lo que hace arriesgada la operación, imposible de utilizar en ambientes donde interactúan varios interlocutores.

4.7.3. Algoritmos Asimétricos (Rsa):

Requieren dos Claves, una Privada (única y personal, solo conocida por su dueño) y la otra llamada Pública, ambas relacionadas por una fórmula matemática compleja imposible de reproducir.

El usuario, ingresando su PIN genera la clave Publica y Privada necesarias. La clave Publica podrá ser distribuida sin ningún inconveniente entre todos los interlocutores. La Privada deberá ser celosamente guardada. cuando se requiera verificar la autenticidad de un documento enviado por una persona se utiliza la Clave Publica porque él utilizó su Clave Privada.

A continuación se muestra un listado con los proveedores con quienes actualmente se puede establecer comunicación mediante la utilización de EDI, que integran la VAN del SEA:

- Proxter.
- Quilmes.
- Budweiser.

- Coca Cola.
- Pepsico.

Estas empresas proveen, a través de este sistema, el 75% de los productos que comercializa La Empresa. Obviamente existen muchas otras no enumeradas, que podrían incorporarse a la VAN, pero las mencionadas son las que actualmente pueden implementar, y de hecho, ya lo han hecho, con Cadenas de Supermercados, y están en mejores condiciones técnicas de realizarlo.

En el momento de tomar la decisión, será muy importante seleccionar adecuadamente a los proveedores con quienes se iniciará la Implantación.

4.8. NOTA PUBLICADA EN LA CRÓNICA

CONTRIBUYENTES PODRÁN HACER TRÁMITES CON FIRMA DIGITAL

(Lizbeth Pasillas)

(2004-02-25)

A partir de marzo los contribuyentes podrán solicitar su firma electrónica avanzada, con la cual podrán hacer, desde una computadora, facturas electrónicas y, posteriormente, declaraciones provisionales, anuales, y solicitud de devoluciones.

Este año la utilización de la firma es opcional. Podrán obtenerla las personas que estén registradas en el padrón del Registro Federal de Contribuyentes (RFC), ya sean personas físicas o personas morales.

Certificaciones. El contribuyente creará su propia firma electrónica avanzada a través de una aplicación localizada en el portal del Servicio de Administración Tributaria (SAT) Ahí, el contribuyente podrá crear su propia firma electrónica avanzada; posteriormente debe asistir en forma presencial ante las oficinas del SAT para obtener un certificado digital que lo ostente como dueño de esa firma.

"Actualmente más de dos millones de contribuyentes cuentan con su firma electrónica, también conocida como Clave de Identificación Electrónica Confidencial (CIEC), mecanismo que permite acceder a diferentes servicios electrónicos, sin embargo, al obtener la firma electrónica, la cantidad de servicios y la seguridad al efectuar transacciones será superior", indicó el SAT. La firma tiene soporte jurídico y reconocimiento ante autoridades fiscales y cuenta con infraestructura técnica confiable, informó el SAT.

Igualmente, la firma electrónica avanzada impide que un mensaje original sea modificado, "el autor del mensaje no puede decir que no lo hizo", tiene la misma validez que una firma autógrafa. Sólo puede ser abierta por el receptor en cuestión. La firma electrónica avanzada poco a poco va a sustituir al CIEC, ya que cuenta con una mayor confiabilidad, seguridad y certeza jurídica.

4.9. ORGANISMOS QUE UTILIZAN FIRMA DIGITAL

Martes 28 de septiembre de 2004

Boletín de prensa No. 492

IMPLANTA EL I.M.S.S. LA FIRMA DIGITAL PARA FACILITAR AÚN MÁS LOS TRÁMITES A LAS EMPRESAS DEL PAÍS.

• Este apoyo a la competitividad de las empresas permitirá ampliar y fortalecer a la seguridad social: Levy

• El sector empresarial apoya el esfuerzo del IMSS para tener una relación más fluida y transparente: Padilla

Ante los presidentes nacionales de Concamin, Concanaco y Canacintra, el director general del IMSS, Santiago Levy, puso en marcha hoy un nuevo paso en el proceso de modernización del Instituto: la incorporación de la firma digital al Programa el IMSS Desde su Empresa (IDSE) lo cual facilitará aún más a los patrones los trámites, incluyendo el pago de las cuotas, e implicará una considerable reducción de costos en apoyo a la productividad de las empresas.

El IMSS, dijo, tiene un compromiso central con la competitividad de las empresas de México porque está perfectamente conciente de que una seguridad social exitosa requiere empresas exitosas, pues su futuro depende del futuro de ellas. Al IMSS, subrayó Levy, le conviene ser un factor que permita que haya más inversión y más creación de empleos porque así habrá a su vez más seguridad social.

“Sólo a través de la incorporación de más trabajadores al mercado formal de trabajo, del combate a la informalidad y de la creación de empleos en empresas competitivas y sólidas sentaremos las bases para la seguridad social del siglo XXI que merecen los mexicanos”, expresó.

Raúl Alejandro Padilla Orozco, presidente de la Confederación de Cámaras Nacionales de Comercio, Servicios y Turismo (Concanaco), a nombre del sector empresarial dijo que éste aplaude y respalda los esfuerzos del IMSS para tener una relación más fluida, simplificada y transparente con el sector empresarial.

“Ahora, con la incorporación de la firma electrónica, herramienta que tiene los más altos estándares de seguridad, confiabilidad y autentificación, y que tiene la misma validez legal que la firma autógrafa, podremos cumplir con mayor oportunidad con nuestras obligaciones, favoreciendo con ello una relación de mayor confianza con las áreas de Incorporación y Recaudación del Instituto”.

Añadió que esta nueva oportunidad para realizar desde la empresa cada vez más trámites, “nos permitirá reducir costos y tiempos de respuesta.

Esperamos también, reducir con ello, observaciones y sanciones, todo en ánimo de una mejor competitividad".

Dijo que todas las empresas, grandes, medianas y pequeñas podrán tramitar y recibir su número patronal de identificación electrónica (NPIE) que brindará seguridad en la realización de gestiones y permitirá fortalecer el mercado interno así como una mayor participación empresarial.

Santiago Levy en su intervención reseñó cómo el Presidente Fox desde el inicio de su administración dio instrucciones para que bajo el liderazgo del Consejo Técnico se construyese un Instituto Mexicano del Seguro Social mucho más moderno y eficaz, para servir mejor a los derechohabientes y a las empresas, y que para ello, con el apoyo del Congreso de la Unión se modificó en 2001 la Ley del Seguro Social para contar con un sólido fundamento jurídico que permitiera realizar transacciones por medios electrónicos.

Añadió que con esa base se impulsó un esfuerzo muy importante para la modernización informática del Instituto que cuenta hoy con la segunda red privada de conexión más grande del país, que ya está funcionando y permite tener interconectadas todas sus subdelegaciones, unidades de Medicina Familiar y hospitales. Esto implicó la adquisición de equipos de cómputo, un importante esfuerzo de capacitación del personal, y el establecimiento de un gran centro de cómputo en Monterrey, con una instalación "espejo" en la capital del país.

Santiago Levy agregó que la firma electrónica es un paso fundamental en la estrategia de modernizar al Instituto para que éste facilite a los empresarios el cumplimiento de sus obligaciones, sin necesidad de ir a los bancos ni hacer "colas" en las subdelegaciones.

Todo esto contribuye a una relación en donde los empresarios del país puedan cumplir con tranquilidad sus obligaciones, sin miedo ni preocupación a ser molestados por el Instituto; todo ello coadyuva, de manera conjunta, a combatir la corrupción. "Esa es la visión que tiene el Presidente Fox del IMSS; esa es la visión que tiene el Consejo

Técnico, y hoy con el lanzamiento de la firma electrónica damos un paso más en la dirección de ésta relación constructiva", enfatizó.

José Antonio Alvarado Ramírez, director de Incorporación y Recaudación del IMSS, al inicio del acto hizo la una explicación de los beneficios que ha implicado el uso de medios electrónicos y señaló que ahora la firma digital permite agregar tres nuevas aplicaciones al IDSE: el envío de la Emisión Mensual Anticipada y de la Emisión Bimestral a través de Internet; la posibilidad de llevar a cabo la confronta con el Sistema Unico de Autodeterminación, partiendo de los archivos de las empresas y de las nóminas para ligarlo con este sistema; y la conexión directa con portales bancarios para el pago de las cuotas. Todo esto con completa certeza y seguridad jurídica.[8]

Conclusiones

Se establecen los términos a los cuales esta enfocada esta monografía.

CONCLUSIÓN

La firma digital es, a mi entender, un requerimiento de la actualidad, de esta globalización que se viene dando en el mundo, desde hace ya unos años, que acarrea consigo al comercio y comunicaciones, el cual, a su vez, le exige al área de computo que avance al ritmo de esta; y es por eso que considero, que era necesaria y fue oportuna un tema así.

No cabría la concepción de firma digital y lo que ella significa, ya que esta firma es un conjunto de números y letras encriptadas, donde existe una clave pública y una privada, un concepto muy lejano al que tuvo, que en su época, ni imagino, que podría haber llegado a existir una firma que no fuera la que surge del puño y letra de un ser humano.

Pero, como se demostró en el desarrollo de este trabajo, ya que esta le da a la firma digital la característica de ser manifestación de la voluntad, igualándola, así, a la firma ológrafa y pudiendo así usarla en ámbitos como el sufragio del voto a distancia.

Estoy totalmente de acuerdo con la implementación del sistema de la firma digital como una nueva forma de manifestación de la voluntad, ya que considero que este significa un gran avance, que es en definitiva la materia de este trabajo, sino también por la influencia que esto tiene en la sociedad comercio y seguridad en transmisión de datos, como de ésta para con el mundo, ya que coloca nuestro conjunto de técnicas a la par de otros países del mundo, como son Alemania, EE.UU., entre otros, y se nos permite así mejorar nuestras formas de proteger nuestros datos y seguridad informática con esos países y, en la medida de lo posible, acrecentarlas.

Y ya para concluir quiero decir que, espero este trabajo haya cumplido con su objetivo de informar a todo lector acerca de un tema, que a lo mejor no ha tenido la difusión que merecería tener, y que a través de este trabajo pretendo, en cierta medida, dársela.

Bibliografía

Referencias electrónicas y bibliografías

BIBLIOGRAFÍA

Para la realización de este trabajo se consultaron los siguientes sitios web:

[1] Centro de Investigación y de Estudios avanzados
http://computacion.cs.cinvestav.mx/~jjangel/Pagina_Todos_es.html

[2] Firmas digitales
http://www.enterate.unam.mx/Articulos/dos/septiembre/firmas.htm

[3] Qubit
www.qubit.org.
http://html.rincondelvago.com/firma-digital.html
http://domino.research.ibm.com/comm/pr.nsf/pages/news.20011219_quantum.html
http://www.physics.uq.edu.au/quant_comp_tech/

[4] Transmisión segura de información: La Firma Digital, de Federico Cabrera, Leonardo Blanch y Martín Cafure.
www.monografias.com :

[5] Recopilación de "Ponencias", del XVIII Jornadas Nacionales de Derecho Civil, Comisión N° 7, "Derecho Internacional Privado. La jurisdicción internacional en el comercio electrónico."

[6] Ramos Suárez, Fernando, Feb. 2000. "Cómo aplicar la nueva normativa sobre firma electrónica", Revista electrónica de derecho informático Nº 19.

[7] Ingenieros en Informática, firma Digital
http://ingenieroseninformatica.org/recursos/tutoriales/firmaelectronica/cap3.php

[8] Portal proceso de certificación digital patronal del IMSS
Http://idse.imss.gob.mx/certificacion/

[9] La firma electrónica
¿Qué es la firma electrónica?
Artículos sobre firma electrónica
http://www.microsoft.com/spain/empresas/tecnologia/firma_electronica.mspx

Firma digital en España
http://html.rincondelvago.com/firma-digital.html