## LA FIRMA ELECTRÓNICA

JAVIER IGNACIO CAMARGO NASSAR.
NÚMERO 2. FEBRERO 2011.

Como una introducción al estudio de la celebración de actos jurídicos por medios electrónicos, haremos una breve reseña de la firma electrónica. El propósito es comprender cómo la utilización de este instrumento nos permite dar cereza a los actos celebrados por estos medios.

El concepto de la palabra "firma" se define como el nombre y apellido, o signos, que una persona escribe de su propia mano en un documento, para darle autenticidad o para expresar que aprueba su contenido. Proviene del latín *firmare,* que significa afirmar, dar fuerza. Es autógrafa, porque esos signos provienen de la mano de su autor.

A través del concepto tradicional, entendemos que al asentar "su firma" en un documento, o "al firmar un documento", la persona que lo hace, reconoce su contenido y se obliga en los términos en que aparece escrito. Por este medio, consideramos que una persona deja constancia fehaciente de su voluntad para celebrar determinado acto jurídico o reconocer como suyo el contenido de *un documento*. Un documento, según la definición establecida por el Décimo Cuarto Tribunal Colegiado en Materia Civil del Primer Circuito, "… *es toda cosa que sea producto de un acto humano perceptible con los sentidos de la vista y el tacto, que sirve de prueba histórica indirecta y representativa de un hecho cualquiera. Puede ser declarativo-representativo cuando contenga una declaración de quien lo crea u otorga o simplemente lo suscribe, como en el caso de los escritos públicos o privados, pero puede ser solamente representativo (no declarativo), cuando no contenga ninguna declaración, como ocurre en los planos, cuadros o fotografías; de ahí que el documento no es siempre un escrito.…".* Semanario Judicial de la Federación y su Gaceta, Novena Época. Tomo XVI. Pág. 1118.

La implementación de las TIC (Tecnologías de la Información y la Comunicación) ha generado nuevos conceptos que asociados a la palabra "firma" indican de igual forma que una persona da autenticidad o expresa que aprueba el contenido de un documento, que en este ámbito se conocen como *documento electrónico* o *digital y firma electrónica.* Existen distintos tipos de firma, cuyas características propias alcanzan distinto valor legal, a continuación nos referimos a cada una de ellas.

## FIRMA ELECTRÓNICA SIMPLE

La *firma electrónica*, en términos generales, es un conjunto de signos que una persona anexa a un *documento electrónico* para dar autenticidad y reconocer como suyo el contenido de un *mensaje de datos*, es decir, a la información generada, enviada, recibida o archivada por *medios electrónicos*.

El Código de Comercio, siguiendo la Ley Modelo sobre Firmas Electrónicas de la UNICITRAL, define la *firma electrónica* como los datos en forma electrónica consignados en un *mensaje de datos*[1], o adjuntados o lógicamente asociados al mismo por cualquier tecnología, que son utilizados para identificar al firmante en relación con el mensaje de datos e indicar que el firmante aprueba la información contenida en el *mensaje de datos*, y que produce los mismos efectos jurídicos que la firma autógrafa, siendo admisible como prueba en juicio. La *firma electrónica* puede consistir en cualquier signo o cualquier conjunto de caracteres o datos electrónicos adjuntos a otro conjunto de datos consignados en forma electrónica (mensaje de datos), como un nombre, una clave o número de identidad personal, una contraseña o una firma digitalizada, a través de la cual una persona reconoce como suyo el contenido de un *documento electrónico*.

La Ley Modelo para el Comercio Electrónico de la UNICITRAL sugiere que, cuando se requiera la "firma" de un documento -tratándose de *mensajes de datos*- ese requisito quede satisfecho si se utiliza un método para identificar a esa persona y para indicar que aprueba la información que contiene el *mensaje* . Ese método será fiable según lo requieran los fines para los que se generó o se comunicó el mensaje de datos, atendiendo a las circunstancias del caso.

La *firma electrónica simple*, es aquella que no reúne los requisitos a que nos referiremos en el siguiente apartado, es decir, cualquier conjunto de caracteres o datos electrónicos adjuntos a un mensaje de datos, que no es suficiente para vincular en forma inequívoca al autor de ese mensaje de datos, ni asegura su integridad.

[1] El mensaje de datos se define como la información generada, enviada, recibida o archivada por medios electrónicos, ópticos o de cualquier otra tecnología.

**FIRMA ELECTRÓNICA AVANZADA**

La *firma electrónica avanzada* consiste en cualquier símbolo basado en medios electrónicos usado con la intención de vincular, autenticar y garantizar la integridad de un *mensaje de datos*.

La Ley Modelo de la UNCITRAL sobre Firmas Electrónicas dispone que el requisito de la "firma" de un *mensaje de datos*, queda satisfecho si se utiliza una "firma electrónica fiable" apropiada a los fines para los cuales se generó o comunicó la información.

Al respecto, esta Ley Modelo considera "fiable" la firma que cumple con los siguientes requisitos:

- Los datos de creación de la firma, en el contexto en que son utilizados, **corresponden exclusivamente al firmante;**
- Los datos de creación de la firma estaban, en el momento de la firma, **bajo el control exclusivo del firmante;**
- Es posible **detectar cualquier alteración de la *firma electrónica*** hecha después del momento de la firma; y
- Cuando uno de los objetivos del requisito legal de firma consista en dar seguridades en cuanto a la integridad de la información a que corresponde, **es posible detectar cualquier alteración de esa información** hecha después del momento de la firma.

Por lo que se refiere a la *firma electrónica avanzada* o *fiable*, el artículo 97 del Código de Comercio, partiendo de lo que disponen las disposición Internacional antes apuntada, establece que la *firma electrónica* es aquélla que cumple con los siguientes requisitos:

1. Que los datos de creación de la firma, en el contexto en que son utilizados, corresponden exclusivamente al firmante;
2. Que los datos de creación de la firma estaban, en el momento de la firma, bajo el control exclusivo del firmante;
3. Que sea posible detectar cualquier alteración de la *firma electrónica* hecha después del momento de la firma, y
4. Respecto a la integridad de la información de un *mensaje de datos*, es posible detectar cualquier alteración de ésta hecha después del momento de la firma.

Según los requisitos apuntados por el Código de Comercio, podemos definir la *firma electrónica* avanzada como aquélla cuyos datos de creación, en el contexto en que son utilizados, corresponden exclusivamente al firmante y estaban, al momento de la firma, bajo su control exclusivo, siendo posible detectar después del momento de la firma cualquier alteración

de la firma y verificar la integridad de la información contenida en el *mensaje de datos*, es decir que no ha sido alterado.

**FIRMA DIGITAL**

La función de esta firma es asegurar:

- Que el mensaje de datos fue enviado y firmado con la clave privada del titular de la firma digital.
- La integridad del mensaje de datos; y,
- Que el titular de la firma digital no pueda repudiar o desconocer un mensaje de datos que ha sido firmado digitalmente usando su *clave privada*.

La *firma digital* se considera como una especie de la *firma electrónica*. Una *firma digital* es un conjunto de datos asociados a un *mensaje de datos* que permite asegurar la identidad del firmante y la integridad del *mensaje de datos*. Es aquella que utiliza una técnica basada en el uso de una clave privada y una *clave pública* (PKI) -Infraestructura de Clave Pública o *"Public Key Infraestructure* - matemáticamente relacionadas, de tal manera que una no puede operar sin la otra. No debemos confundir esta firma con la firma digitalizada que se trata de una simple representación gráfica de la firma manuscrita obtenida mediante un escáner. No tiene el mismo valor legal que la firma digital, se trata de una firma electrónica simple.

Como veremos más adelante, para crear una *firma digital*, el texto de un *mensaje* debe pasar a través de un algoritmo de "*hashing*", lo que genera un mensaje comprimido o resumen. Este *mensaje* comprimido debe ser "encriptado" empleando la *clave privada* del emisor, transformándolo en una *firma digital*, que sólo puede ser "desencriptada" empleando la *clave pública* de la misma persona. El receptor del mensaje "desencripta" la *firma digital* y mediante un sistema automatizado recalcula el *mensaje* comprimido. El valor calculado de este nuevo *mensaje* comprimido se compara con el valor del *mensaje* comprimido hallado en la firma, si ambos cálculos son iguales, significa que el *mensaje* no ha sido alterado y el receptor puede confiar en su contenido, de lo contrario, debe rechazarlo. Si el documento o la firma son modificados, el procedimiento de autenticación indicará que el documento firmado no es auténtico. A diferencia de la firma autógrafa, todas las firmas digitales generadas por una persona son diferentes entre sí.

## CERTIFICADO DIGITAL

El certificado digital[2] es un *documento electrónico* expedido y firmado en forma electrónica por un *prestador de servicios de certificación*. Es un *documento electrónico* generado y firmado digitalmente por una entidad de certificación, el cual vincula a un par de *claves* con una persona física o moral, confirmando su identidad. Mediante el *certificado digital*, podemos confirmar que el firmante o signatario identificado en un instrumento de esta naturaleza posee, de manera exclusiva, la *clave privada* correspondiente a la ya mencionada *clave pública* de dicho *certificado*. Este instrumento, es emitido por un *prestador de servicios de certificación* al que adelante nos referimos. Para utilizar una *firma digital* es necesario contar con un *certificado digital*. No puede existir una *firma digital* sin el *certificado digital*. El artículo 89 del Código de Comercio define este certificado como todo *mensaje de datos* u otro registro que confirma el vínculo entre un firmante y los datos de creación de una *firma electrónica*. Los datos de creación son únicos, como códigos o claves criptográficas privadas, que el firmante genera de manera secreta y utiliza para crear su *firma electrónica*, a fin de lograr el vínculo entre dicha firma electrónica y el firmante.

Según al artículo 108 del Código de Comercio, estos *certificados* deberán contener:

> I. La indicación de que se expiden como tales;
> II. El código de identificación único del *certificado*;
> III. La identificación del *prestador de servicios de certificación* que expide el *certificado*, razón social, su domicilio, dirección de correo electrónico, en su caso, y los datos de acreditación ante la Secretaría de Economía;
> IV. Nombre del titular del *certificado*;
> V. Periodo de vigencia del *certificado*;
> VI. La fecha y hora de la emisión, suspensión, y renovación del *certificado*;
> VII. La responsabilidad que asume el *prestador de servicios de certificación*, y
> VIII. La tecnología empleada para la creación de la *firma electrónica*.

Según el Código de Comercio, este *certificado* dejará de surtir efectos por expiración de su vigencia, que no podrá exceder de dos años; por revocación; por pérdida o inutilización por daños del dispositivo en el que se contenga; por haberse comprobado que al momento de su expedición, el *certificado* no cumplió con los requisitos establecidos en la ley y por resolución judicial o de autoridad competente que lo ordene.

---

[2] Existen variados formatos para **certificados digitales**. Comúnmente se rigen por el estándar **X.509 UIT-T**. En criptografía, **X.509** es un estándar UIT-T para infraestructuras de claves públicas. El **Sector de Normalización de las Telecomunicaciones de la UIT** (**UIT-T**) es un órgano de la Unión Internacional de Telecomunicaciones (UIT) que estudia aspectos técnicos, y publica normativa sobre los mismos, con vista a la normalización de las telecomunicaciones a nivel mundial

## PROCESO DE COMUNICACIÓN ELECTRÓNICA SEGURO

Para el tema que nos ocupa, debemos determinar cómo pueden confiar las partes que intervienen en este "proceso de comunicación electrónica" que quien envía el *mensaje de datos* es realmente quien dice ser y que el contenido del *mensaje de datos* es precisamente el que envió el remitente. Tanto la autenticidad como la integridad del mensaje se hallan expuestas a su menor o mayor confiabilidad. La repuesta la encontramos en la *firma digital* y el *certificado digital* que se emite a través de una autoridad certificadora, Es un *documento electrónico*, *mensaje de datos* u otro registro que asocia una *clave pública* con la identidad de su propietario, confirmando el vínculo entre éste y los datos de creación de una firma. El *certificado digital* es un *documento electrónico* expedido y firmado en forma electrónica por un *prestador de servicios de certificación* (PSC o AC). El *prestador de servicios de certificación* (PSC), es la persona o institución pública que que expide el mensaje de datos y otros registros que confirman el vínculo entre el firmante y los datos de creación de la firma electrónica.

Dentro del proceso de comunicación segura, la *parte que confía* es la persona que –siendo, o no, el destinatario de un mensaje de datos- actúa en base a un *certificado* o una *firma electrónica*. Así, cuando una persona recibe un *mensaje de datos*, puede actuar con la confianza que le brinda la *autoridad certificadora* que expidió el *certificado*, pues a través de este *documento electrónico* se confirma la identidad del *emisor* y la integridad del *mensaje de datos*, con base en los elementos técnicos que intervienen en este proceso, a los que a continuación nos referimos.

## El proceso de comunicación segura

Dentro del proceso de comunicación segura, intervienen los siguientes elementos:

1. La elaboración y envío del *mensaje de datos*
2. La *firma digital*
3. La *clave* o *llave pública* y *privada*
4. La encriptación
5. La función hash o digesto
6. El *prestador de servicios de certificación*
7.

## 1. La elaboración y envío del *mensaje de datos*

El *mensaje de datos* deber ser generado mediante la utilización de un programa adecuado para el contenido del documento que se pretende elaborar, según sea un procesador de palabras –p.ej., Microsoft Office Word- o algún otro tipo de programa –p.ej., Microsoft Office Excel, Microsoft Office PowerPoint, etc.-. Una vez elaborado el documento -*documento electrónico o digital*- por el *emisor*, deber ser enviado al *destinatario*, utilizando algún *medio electrónico*, *óptico o de cualquier otra tecnología*. En el caso que nos ocupa, el documento es enviado a través de un *medio electrónico* como es *el Internet, mediante un "correo electrónico" que contiene el mensaje de datos. El mensaje de datos* es la información contenida en el *documento electrónico*, que, como antes dijimos, puede ser un texto o una imagen, como un plano o una fotografía de un bien determinado.

## 2. La firma electrónica digital

Para el envío del *mensaje de datos*, el emisor debe "firmar" el *mensaje de datos*, a través de la utilización de la *firma electrónica digital*, que como hemos dichos, es una especie de firma electrónica avanzada, cuyos datos de creación, en el contexto en que son utilizados, corresponden exclusivamente al firmante y estaban, al momento de la *firma*, bajo su control exclusivo, siendo posible detectar –después de su generación- cualquier alteración de la *firma* y verificar la integridad de la información contenida en el *mensaje de datos*. La *firma digital* es una especie de la *firma electrónica* creada utilizando medios que el firmante debe mantener bajo su exclusivo control, vinculada a los datos a que se refiere de modo que cualquier cambio ulterior sea detectable. La *firma digital* es una especie de *firma electrónica* que garantiza la autenticidad e integridad y la posibilidad de detectar cualquier cambio ulterior.[3]

Para utilizar una *firma digital* es necesario contar con un *certificado digital*. No puede existir una firma digital sin el *certificado digital*. El *certificado digital* es un *documento electrónico* expedido y firmado en forma electrónica por un PSC. Es un *documento electrónico* generado y firmado digitalmente por una entidad de certificación el cual vincula a un par de *claves* con una persona física o moral, confirmando su identidad. Mediante el *certificado digital*, podemos confirmar que el firmante o signatario identificado en un *certificado digital* posee, de manera exclusiva, la *clave privada* correspondiente a la *clave pública* de dicho certificado.

[3] Norma Oficial NOM-151-SFCI-2002, "Prácticas que deben observarse para la conservación de mensajes de datos", publicada en el Diario Oficial de la Federación el 4 de junio del 2002.

**3. La clave o llave pública y privada**

Para la utilización de la *firma electrónica avanzada*, es necesario crear dos instrumentos conocidos como *llave pública* y *llave privada*, o *clave pública* y *privada*. Estas *llaves* son creadas mediante un programa informático. La *llave* o *clave privada* es conocida únicamente por el titular, en tanto que la *llave pública*, puede ser del conocimiento general.

Cuando se remite un mensaje, el *emisor* debe "sellar" con su *llave privada* el documento, al que el destinatario tiene acceso únicamente aplicando, mediante un programa informático, la *llave pública* del *emisor*. Los dos instrumentos se encuentra directamente relacionados entre sí, de forma que cuando un documento después de ser elaborado se "firma" o "asegura" con la *llave privada*, el texto "claro" se transforma en una serie de signos ilegibles -texto cifrado-, cuyo contenido únicamente puede ser transformado al mensaje original –descifrado-, mediante la utilización de la *llave pública* del *emisor*.

*La correlación directa entre ambas llaves*, permite asegurar lo siguiente:

1. Si el *destinatario*, *al momento de recibir un documento "firmado" con la llave privada del emisor, aplica la llave pública* de este último, y el texto ilegible se transforma en texto legible, es signo inequívoco de que el *mensaje de datos* fue enviado mediante la utilización de la *llave privada* del *emisor*, pues solamente frente a esta *llave privada* reacciona la llav*e pública* del *emisor*, produciendo este efecto, y los datos que corresponde a la *llave privada* del *emisor* se encuentran bajo su exclusivo control.

2. Si el *destinatario,* al momento de recibir un documento "firmado" con la *llave privada* del *emisor*, aplica la *llave pública* de este último, y el texto ilegible no se transforma en texto legible, ello es signo inequívoco de que el *mensaje de datos* no fue enviado mediante la utilización de la *llave privada* del *emisor*.

Para este efecto, la autoridad certificante, tiene a disposición del público general la *llave pública* de los titulares de los *certificados digitales*, y a través de *medios electrónicos*, el *destinatario* que recibe el *mensaje de datos*, puede confirmar ante la autoridad certificante la autenticidad de la *llave pública* del emisor.

## 4. La encriptación

La criptografía –del griego κρυπτός, "oculto", graphos "escritura"- es el arte de escribir con clave secreta o de un modo enigmático.[4] Técnicamente se conoce como el arte o ciencia de cifrar y descifrar información, utilizando técnicas que hacen posible el intercambio de la información de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Para encriptar el texto de un documento, mediante la utilización de un sistema informático, se aplica al texto legible -texto plano- una función que consiste en una clave o contraseña que convierte al texto ininteligible -texto cifrado o criptograma-. Posteriormente, mediante la aplicación de otra clave -cifrado asimétrico- o la misma -cifrado simétrico-, el texto cifrado se convierte en texto legible. Así es como se completa el proceso de cifrar y descifrar el contenido de un documento. Dentro del proceso de comunicación, el remitente envía el mensaje cifrado y el destinatario puede descifrarlo aplicando el sistema apuntado.

Este proceso permite la confidencialidad del mensaje, pues éste es transmitido de forma que únicamente la persona que conoce la clave para descifrarlo, pueda enterarse de su contenido, y permite además verificar la integridad del mensaje, pues si texto del mensaje es alterado por un tercero, la aplicación de la clave no lo convertirá en texto legible. Existen dos tipos de criptografía: simétrica y asimétrica. La criptografía simétrica utiliza una misma clave para cifrar y para descifrar el contenido de un mensaje. Ambas partes que intervienen en el proceso de comunicación deben conocer *la clave* que van a utilizar para este efecto. Así, el remitente cifra un mensaje con *la clave*, lo envía al destinatario, y éste lo descifra con la misma *clave*. La criptografía asimétrica[5] - de *llave pública* - utiliza un par de *llaves* distintas, una para cifrar el mensaje y otra para descifrarlo. Ambas *claves* pertenecen a la persona que ha enviado el mensaje. Una es pública y puede ser del conocimiento de cualquier persona. La otra *clave* es privada, solamente la conoce el titular, y permanece bajo su control.

En este sistema, el remitente utiliza la *clave pública* del *destinatario*, que es conocida por todos, para cifrar el contenido del mensaje y enviarlo. Una vez cifrado, sólo la *clave privada* del *destinatario* que lo recibe podrá descifrar este mensaje, es decir, convertirlo en texto legible,

[4] Diccionario de la Real Academia de la Lengua Española.

[5] **SSL** es una implementación de la encriptación de clave pública (*Secure Sockets Layer*). Originalmente fue desarrollada por Netscape como protocolo de seguridad para Internet usado por navegadores y servidores Web para transmitir información. SSL se ha convertido en parte de un protocolo de seguridad general llamado TLS (*Transport Layer Security*).

claro o plano. De esta manera, para llevar a cabo el proceso de comunicación segura, es necesario que el remitente conozca la *llave pública* del d*estinatario*. El método de encriptado de datos conocido como algoritmo RSA, por los nombres de sus inventores (Rivest, Shamir y Adleman) es uno de los más usados hoy para la transmisión segura de datos a través de canales inseguros.

Veamos el siguiente ejemplo real de un texto cifrado y después alterado:

1. Texto claro o plano (el mensaje original):

| |
|---|
| Éste es un ejemplo de la forma como se puede encriptar un mensaje. |

2. Contenido del mismo texto cifrado:

| |
|---|
| Qgg*@ofjcxj$**fz-@pnqv-$@pb%^kj@behhfqpz*$@*@oao+s#hxj@^aj^ozgxb . |

3. Resultado de la alteración del texto plano del apartado 1. (La alteración consistió únicamente en cambiar una letra por otra en el texto):

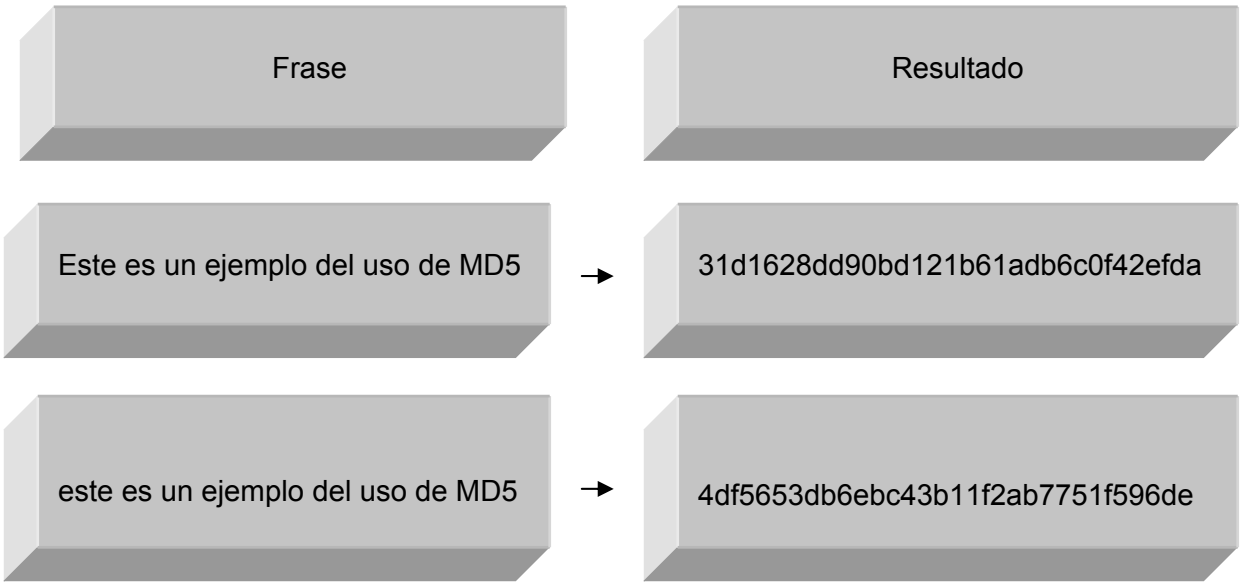
| |
|---|
| 2^*me^&vcdvqwmtfycp%$jyie&#f^@vo#uvx&$pfiqqme^@@+-d&nzek@v^^b^nn. |

**5. La función hash**

La *función hash* –resumen- es una función que asigna un valor determinado a un *mensaje de datos*. Este valor o clave responde únicamente frente al texto del *mensaje de datos*, de manera tal que, si el texto del mensaje varía, en consecuencia, varía también el valor asignado al texto. Esta función de una vía es una forma criptográfica empleada junto con los algoritmos de *clave pública* para encriptación y *firma digital*, que se utiliza para verificar la integridad de un *mensaje de datos*. La *función hash* asigna su entrada a un valor dentro de un grupo finito, que por regla general este grupo es un rango de números naturales. La *firma digital* en un documento es el resultado de aplicar un algoritmo matemático denominado *función hash* a su contenido y en seguida aplicar el algoritmo de firma -clave privada- al resultado de esa operación, generando así la *firma electrónica* o *digital*. Esta función, para que sea útil, debe satisfacer dos condiciones: en primer lugar, deberá ser difícil encontrar dos documentos cuyo

valor para una *función hash* sea el mismo y, en segundo lugar, dado un valor *hash*, deberá ser difícil de recuperar el documento que produjo es valor.

Algunos sistemas como el MD5, son algoritmos[6] que reúnen estas dos cualidades. Al usarlos, un *mensaje de datos* se firma con una *función hash*, y el valor del *hash* es la firma. El *destinatario* puede comprobar la autenticidad de la firma aplicando también una *función hash* al *mensaje de datos* que recibe y comparar el valor *hash* resultante con el del documento original. Si concuerdan, se puede confiar en la integridad del mensaje. Veamos el resultado de este ejemplo en el que se utilizan este algoritmo con una misma frase, cambiando la primera letra por una minúscula:[7]




[6] **MD5** (abreviatura de Message-Digest Algorithm 5, Algoritmo de Resumen del Mensaje 5) es un algoritmo de reducción criptográfico de 128 bits ampliamente usado.

**RSA:** Creado en 1977 por Ron Rivest, Adi Shamir y Len Adleman. El nombre RSA proviene de las iniciales de los apellios de sus inventores. La seguridad de este algoritmo reside en la dificultad que supone la factorización de un número compuesto por factores primos muy grandes.

**HASH o de resumen:** Este algoritmo parte de una información de entrada de longitud indeterminada y obtienen como salida un código, que se puede considerar único para cada entrada. A partir de una misma entrada siempre se obtiene la misma salida. Sin embargo, el interés de estos algoritmos reside en que partiendo de entradas distintas se obtienen salidas distintas.

• **SHA (Secure Hash Algorithm):** Fue sustituido por una versión llamada SHA-1, que se considera más seguro que MD5. Produce un código hash de 160 bits para mensajes de longitud máxima 264 bits. Se considera el mejor algoritmo de esta clase y es el que se aplica en la mayoría de las aplicaciones de firma electrónica. Es habitual aplicar SHA1 seguido de RSA para realizar una firma electrónica de un documento, o bien el algoritmo DSA específico para firma electrónica que también utiliza SHA1 internamente.

• **DSA (Digital Signature Algorithm)**: Es el estándar del Gobierno de los Estados Unidos para firma digital. Es un algoritmo exclusivo de firma electrónica basado en clave pública, pero no vale para comunicaciones confidenciales.

[7] http://www.md5.net/

**6.- El prestador de servicios de certificación**

Entidades encargadas de expedir los *certificados digitales* y confirmar la identidad del usuario, en los términos a que nos hemos referido en este trabajo. Estas instituciones, al momento de expedir un *certificado digital*, verifican la identidad del solicitante y que los datos de creación de la *firma electrónica* se encuentran bajo el exclusivo control del titular. Durante el proceso de comunicación, los usuarios pueden verificar quién es el titular del *certificado*, la *llave pública* del *emisor* y si el *certificado* se encuentra vigente o no.

Recordemos que el Código de Comercio establece la posibilidad de que el notario público formalice actos jurídicos por medios electrónicos y por lo que se refiere al cumplimiento del requisito de forma en los actos celebrados *por medios electrónicos, ópticos o de cualquier otra tecnología,* prescribe que cuando se requiera la forma escrita para la celebración de un acto jurídico, los documentos relativos deben ser firmados por las partes, agregando que tales requisitos [el documento escrito y la firma de las partes] se tendrán por cumplidos mediante la utilización de *medios electrónicos, ópticos o de cualquier otra tecnología*, siempre que la información generada o comunicada en forma íntegra, a través de dichos medios sea (i) atribuible a las personas obligadas y (ii) accesible para su ulterior consulta…", (lo cual como vimos se puede lograr, entre otros medios, con la utilización de un certificado digital), agregando que en los casos en que la ley establezca como requisito que un acto jurídico deba otorgarse en instrumento ante fedatario público, éste y las partes obligadas podrán generar, enviar, recibir, archivar o comunicar la información que contenga los términos exactos en que las partes han decidido obligarse, mediante la utilización de medios electrónicos, ópticos o de cualquier otra tecnología, en cuyo caso el fedatario público, deberá hacer constar en el propio instrumento los elementos a través de los cuales (i) se atribuye dicha información a las partes y (ii) conservar bajo su resguardo una versión íntegra de la misma para su ulterior consulta, otorgando dicho instrumento de conformidad con la legislación aplicable que lo rige."

Debemos entonces establecer los medios a través de los cuales el Notario Público puede cumplir con los requisitos apuntados y además dar forma legal al documento según las disposiciones del derecho común. Esta es una tarea que por ahora queda pendiente.