LA SEGURIDAD DEL DOCUMENTO ELECTRÓNICO: RETO JURÍDICO DEL PRESENTE

Alicia Rendón López

SÍNTESIS

La seguridad del documento electrónico: reto jurídico del presente, pretende exponer de manera general la problemática *real* que aqueja a los documentos electrónicos en su camino por el *ciberespacio*, sobre todo en lo referente a su confidencialidad y autenticidad, así como la forma en que la criptografía ha mitigado sus efectos

No obstante, los juristas tenemos como reto del presente, y dentro de una investigación interdisciplinaria, el crear nuevas formas, modelos, instrumentos o directrices, que permitan salvaguardar y garantizar la confidencialidad y autenticidad de los documentos electrónicos, así como para detectar al *agente* u *operador informático* que accese sin autorización o haga uso indebido de la información contenida en los mismos.

SUMARIO:

I. *Nota Introductoria.* II. *Nociones sobre los documentos electrónicos.* III. *La inseguridad jurídica en los documentos electrónicos.* IV. *El uso de la criptografía en los documentos electrónicos.* V. *Conclusiones.* VI. *Bibliografía.*

I. NOTA INTRODUCTORIA

Actualmente existen nuevas y novedosas oportunidades para el intercambio de información a través de las tecnologías de la información y comunicación, correlativo a ello, también han surgido nuevos riesgos a la seguridad de la misma y, en consecuencia, se han creado mecanismos que garanticen la confidencialidad y autenticidad de la información y los documentos electrónicos que la contienen y se utilizan para transmitirla.

En el presente trabajo se pretende exponer de manera general la problemática *real* que aqueja a los documentos electrónicos en su camino por el *ciberespacio*, sobre todo en lo referente a su confidencialidad y autenticidad, así como la forma en que la criptografía ha mitigado sus efectos. Esto se hará a la luz de los métodos de investigación documental, comparativo y hermenéutico.

Por ello es importante mencionar, que la disciplina matemática que aborda este tema de la seguridad informática, en general, y el de los documentos

electrónicos, en particular, es la criptografía, cuyas ventajas y desventajas, ofrecen un nuevo reto a los juristas: la creación de otros mecanismos jurídico-tecno-lógicos (técnicos y lógicos) para lograr la seguridad de éstos.

Debemos partir del criterio de que la seguridad jurídica se ocupa de la protección de los bienes, que en materia informática serían el hardware, software y los datos o información.

El desarrollo de criptosistemas de clave privada y pública y los sistemas de firma digital y no repudio en la transmisión de datos, son modelos teóricos que se han implementado en aras de la seguridad de la información y los documentos electrónicos que la contienen.

Aún cuando en nuestro país, se ha procurado la orientación sobre el uso adecuado de la información en las tecnologías existentes para evitar su uso indebido e ilegal, queda mucho por hacer para salvaguardar y garantizar la confidencialidad y autenticidad de los documentos electrónicos.

II. NOCIONES SOBRE LOS DOCUMENTOS ELECTRÓNICOS

Dentro de lo que conocemos como informática jurídica, encontramos a la metadocumentaria o decisional:

> la cual se caracteriza por conformarse por una base de conocimientos jurídicos y el uso de la tecnología, que trascienden más allá del contenido del documento, como lo es la toma de decisiones al proveer una información depurada al usuario y en la utilización de programas de inteligencia artificial y sistemas jurídicos expertos que ofrecen soluciones.[1]

Un ejemplo de ello, es el documento electrónico.

Para poder entender el significado del documento electrónico, es pertinente iniciar con la definición de documento, que para Escobar de la Riva, el documento, en sentido estricto, es "una exteriorización del pensamiento perceptible con la vista".[2]

Para el Dr. Julio Téllez Valdés, documento es en sentido amplio "toda representación material destinada e idónea

---

[1] MALDONADO OTERO, Claudia Gabriela, *Presentación de Microsoft Office Power Point 97-2003: Informática Jurídica metadocumentaria o Decisional*, 2009.

[2] ESCOBAR DE LA RIVA, Eloy, *Tratado de Derecho Notarial*, Editorial Marfil, Barcelona, España, 1957, p. 252.

para reproducir una cierta manifestación del pensamiento."[3]

Asimismo, para Téllez Valdés, **el documento electrónico es "toda representación electrónica que da testimonio de un hecho, una imagen o una idea. Requiere soporte material."[4]** y como "aquel instrumento que contiene un escrito–mensaje, destinado a durar en el tiempo, en lenguaje convencional (bits), sobre soporte, que podría ser cinta, disco. En otras palabras, es aquel documento que provenga de cualquier medio de informática o que también sea formado o realizado por esta."[5]

En un *sentido amplio*, nos dice que los documentos electrónicos "son aquéllos que se caracterizan por la posibilidad de ser percibidos y leídos directamente por el hombre sin necesidad de la intervención de máquinas como sería el caso del comprobante que emite un cajero automático o un correo electrónico impreso."[6]

Y **señala, que en *sentido estricto***:

> es la representación material destinada e idónea para reproducir una cierta manifestación de voluntad materializada a través de las tecnologías de la información sobre soportes magnéticos, como un disquete, un cd-rom, una tarjeta inteligente u otro, y que consisten en mensajes digitalizados que requieren de máquinas traductoras para ser percibidos y comprendidos por el hombre.[7]

La Asociación Nacional del Notariado Mexicano, A.C, entiende por documento electrónico, en sentido amplio, a "todos aquellos documentos que se producen con la intervención de la computadora". [8]

Mario Guibour, nos dice que los documentos electrónicos, *en sentido estricto*, son:

> los documentos formados por la computadora misma. En este caso la computadora no sólo es un auxiliar para la realización de una voluntad o decisión humana, sino que en este

[3] TÉLLEZ VALDES, Julio, *Derecho Informático*, ed. 2ª, Ed. McGraww-Hill, México, 2004, p.117.
[4] TÉLLEZ VALDES, Julio, *Seminario Taller Validez de los documentos electrónicos*, diapositiva 9 en presentación de Microsoft Office Power Point -2, Guayaquil, 15 de agosto de 2007. En http://www.cetid.abogados.ec/archivos/37.pdf consultada el 15 de septiembre de 2009.
[5] *Ibidem*, diapositiva 10.
[6] *Ibidem*, diapositiva 15.
[7] *Ibidem* diapositiva 16.
[8] *Revista de Derecho Notarial*, Asociación Nacional del Notariado Mexicano, A.C. Número 110, México, abril 1997, p. 75.

> documento la computadora determina el contenido de la voluntad, siendo aquí que, el documento se conforma como resultado de una serie de datos y parámetros electrónicos, o sea software o programa, el cual es muy parecido a un formato para ser llenado por el usuario de acuerdo a los parámetros que va indicando el mismo documento, es decir, el negocio jurídico nace del interior de la computadora.[9]

De acuerdo con este último autor, los documentos electrónicos, *en sentido amplio*, se pueden distinguir, entre otros, por la manera en cómo se formulan, ya sea que se introduzcan a la memoria de la computadora *por medio de una intervención humana*, mediante el teclado a modo de máquina de escribir; o bien, que se introduzcan a la memoria de la computadora *por medio de un periférico electrónico* el cual podría ser, un lector óptico o un fax de un correo electrónico. Los documentos en estos casos, no se forman por la computadora, pero se crean, memorizan y se reproducen independientemente de que tengan soporte en papel o permanezcan únicamente en soporte electrónico, sin que jamás sean impresos en papel.

Por documento electrónico, también se entiende al elaborado por un medio electrónico, como puede ser una computadora, la cual no se limita a "materializar una voluntad, una decisión, una regulación de intereses ya formados, sino que, conforme a una serie de datos y parámetros y a un adecuado programa, decide, en el caso concreto, el contenido de la regulación de intereses."[10]

Es importante, señalar desde ahora, que los documentos electrónicos, son sólo una especie de ***documentos informáticos***, los cuáles son definidos como:

> Aquéllos en los cuales la computadora sólo es el medio, instrumento o auxiliar para realizar o documentar la voluntad jurídica de las personas, nacida fuera de la computadora; i. e., en esta noción la computadora es considerada sólo como una

[9] GUIBOURG, Mario, et al; *Manual de Informática Jurídica*, Editorial de Alfredo y Ricardo Depalma, Buenos Aires, Argentina, 1996, p.103.

[10] DEL CASTILLO NEGRETE ILLANES, María de las Mercedes, *Tesis de Maestría*, División de Estudios de Posgrado de la Facultad de Derecho de la UNAM, México, 2006, p. 45.

LA SEGURIDAD DEL DOCUMENTO ELECTRÓNICO: RETO JURÍDICO DEL PRESENTE

Alicia Rendón López

> herramienta para documentar y comprobar con mayor eficacia la voluntad de las personas. [11]

Entre los documentos informáticos, podemos considerar a los siguientes:

> 1.-Mensajes de datos
> 2.-Correos electrónicos personales
> 3.-Documentos electrónicos
> 4.-Contratos electrónicos
> Todos ellos identificados a través de una clave o firma electrónica y no deberán ser obtenidos de manera ilícita o violando garantías constitucionales o procesales[12]

Vicente María de la Prada Gaita, notario madrileño, en su ponencia "*El Documento Informático y la Seguridad Jurídica*" en el XX Congreso Internacional del Notario Latino en Cartagena de Indias, en 1992, dice:

> 1. Se distingue tres tipos de documentos informáticos que son los más notables que se utilizan en las empresas: a) Los documentos relativos a transacciones, es decir, contratos, confirmaciones, instrucciones de pago, etcétera; b) Los documentos de tipo cronológico, tales como el libro diario o un libro de entradas y salidas, y c) Los documentos resumen, que facilitan determinar el estado de un negocio…la naturaleza física de los documentos informáticos es: Los documentos sobre soporte papel y los documentos en soporte electrónico, distinguiendo entre éstos a) El telégrafo y el télex; b) los documentos en soporte papel preparados en computadoras; y, c) Los documentos transmitidos de computadora a computadora…[13]

En virtud de lo anterior, **se puede concluir que son *documentos informáticos*** todos aquellos creados o almacenados en la memoria de la computadora (en el disco duro o sus

[11] *Idem*.
[12] TÉLLEZ VALDES, Julio, *Op. cit.,* diapositiva 21.
[13] DELGADO DE MIGUEL, Juan Francisco, *Deontologías Notarial*, Junta de Decanos de los Colegios Notariales de España, Consejo General del Notariado, Imprenta Firma Mieres, Madrid, 1993, p. 146.

periféricos), que documentan la voluntad de las personas nacidas fuera de ésta. Se incluyen en este concepto, los documentos impresos en soporte de papel y los documentos por imprimir y que no constan aún (o nunca) en soporte papel, i. e., que sólo se soportan en la memoria de la computadora.

Y por *documentos electrónicos*, entendemos a todos aquéllos que no solo reproducen, sino también materializan una cierta manifestación de voluntad para ser percibidos y comprendidos por el hombre, a través de las tecnologías de comunicación e información, mediante mensajes digitalizados y sistemas inteligentes o expertos.

Dentro de los documentos electrónicos existen los denominados *documentos electrónicos puros o en sentido estricto*, cuyo contenido y proceso de voluntad se forman por algún *programa de inteligencia artificial o experto* convenido. Generalmente se trata de textos en lenguajes cifrados por seguridad, que para entenderse deben traducirse mediante el uso de claves previamente convenidas.

El problema real, desde un espectro jurídico, del documento electrónico es su validez y la solución de los problemas de seguridad jurídica en las contrataciones mercantiles, por ejemplo, en donde se pueden llegar a manejar
operaciones muy cuantiosas, celebradas mediante la comunicación o trasmisión de textos y voluntades exclusivamente por vía electrónica, y en las que se requiere certeza sobre la autenticidad y confidencialidad de la información y los documentos que las contienen.

III. LA INSEGURIDAD JURÍDICA EN LOS DOCUMENTOS ELECTRÓNICOS

Se dice que la computadora ha sustituido en muchos casos a la pistola o la pluma como el arma preferida de los delincuentes llamados "de cuello blanco". El fraude, es la forma más común de los delitos cometidos vía computadora. Generalmente, se defrauda a un proveedor, haciéndose pasar por un cliente interesado mediante engaños, quien finalmente entrega una mercancía y normalmente tarda mucho tiempo en descubrir el fraude.

Algunos de los cibercompradores en la internet, se han inconformado por contrataciones celebradas vía electrónica, ya que en muchos casos, cuando una persona compra en alguna empresa que se anuncia en la línea, digita su número de tarjeta de crédito para hacer el pago y sólo espera a que le envíen el artículo que en teoría adquirió, sin que éste nunca llegue, porque la empresa en donde virtualmente adquirió el producto, nunca existió, pero ¡el cargo a la tarjeta sí se llevó a cabo!, a este tipo de situaciones comúnmente se le denomina operaciones con empresas fantasmas. En ese sentido, Francisco Ceballos, Director de la Asociación Mexicana de Internet (AMIPCI, mencionó: "Hace falta avanzar en el tema de la seguridad de la navegación, el combate de los crímenes en el ciber espacio y la normatividad vigente."[14]

Otro gran problema en la seguridad informática, lo encontramos con las acciones de sabotaje al hardware (estructura interna de sus componentes físicos) o al software (estructuras de sus componentes lógicos que permiten procesar la información, también llamados programas) de la computadora.

Los programas saboteadores más comunes son:

a) ***Caballos de Troya***: Son programas que se ocultan dentro de un programa de software atractivo, que ordena

[14] P. Sandoval Zamora, Hugo, "México, un buen mercado para internet", *El Universal*, jueves 28 de diciembre de 2006.

realizar acciones destructivas del software. Generalmente se encuentra en los juegos bajados desde la internet o en las reproducciones de programas no autorizadas (piratas).

b) ***Los virus***: Actúan como si fueran verdaderos virus biológicos, ya que su característica es que se reproducen de manera incontrolada invadiendo el espacio de otro programa que se distorsiona, i. e., enloquece. Los virus contagian a los otros discos y se extienden como una *epidemia* o *pandemia* biológica. Hay virus de varios tipos, los más inocentes sólo dejan leyendas; otros borran datos; otros hacen lenta la computadora; otros dañan seriamente el software o el hardware. Los virus se combaten con "vacunas antivirus", que pueden actualizarse gratuitamente desde la internet.

c) ***Los gusanos*** *(tapeworms)*: Son programas que entran directamente al software y comen como los gusanos en una manzana, desde dentro e imperceptiblemente al software de la computadora. Los gusanos viajan independientes por las redes y son muy difíciles de localizar y eliminar.

d) ***Las bombas lógicas****:* Son programas que entran en acción después de cierta secuencia o de realizado un acontecimiento determinado.

Normalmente, y dada nuestra impericia y analfabetismo informático, en muchísimas ocasiones no alcanzamos a distinguir entre estos distintos saboteadores y a todos les llamamos "virus".

Otro fenómeno que ataca a la seguridad informática, son los llamados ***"hackers"***, que son los invasores electrónicos que accesan sin autorización en las computadoras corporativas, gubernamentales y privadas, para delinquir o sólo para curiosear, a fin de obtener información clasificada, utilizando contraseñas sustraídas o robadas. Hay varias maneras de combatir a los hackers, una de ellas, es a través de las restricciones de acceso físico, que consiste en asegurarse que sólo el personal autorizado tenga acceso al equipo de cómputo. Entre las principales maneras de restringir el acceso, están las siguientes:

a) Utilizar una tarjeta de identificación inteligente.
b) Uso de una contraseña, un número de identificación, datos personales, etc.
c) La manera o forma de escribir o la velocidad para teclear, etc.
d) Alguna característica biológica del usuario, como su voz, sus huellas dactilares, la lectura de su retina, etc.
e) El borrado interno (el programa de acuerdo con un reloj interno deja de funcionar en determinado tiempo).

Una de las maneras más utilizadas para proteger la información al transmitirse, es mediante la utilización de un ***software cifrado***, i. e., el emisor tiene que "codificar" o traducir el documento a un lenguaje en clave secreta, llamado "clave de cifrado" y así lo envía. Cuando se recibe el mensaje, a los ojos de los demás se trata de un conjunto de caracteres sin sentido, mismos que el receptor informático tiene que "decodificar" utilizando otra "clave de cifrado", que al aplicarse, traduce el texto del documento, revelando su significado en el lenguaje propio de la computadora.

Estas claves de cifrado se clasifican en: a) lenguaje de alto nivel, que son los que utilizan palabras muy parecidas al lenguaje del hombre, como el "Pascal" o el "Basic"; y b) lenguaje de bajo nivel, que son los que entiende la computadora directamente sin necesidad de utilizar traductor.

Este tipo de cifrado informático, es el estudiado por la criptografía.

IV. EL USO DE LA CRIPTOGRAFÍA EN LOS DOCUMENTOS ELECTRÓNICOS

La criptografía "es la ciencia que estudia la ocultación, disimulación o cifrado de la informática, así como el diseño de sistemas que realicen dichas funciones",[15] ha sido utilizada tradicionalmente en los ámbitos militar, diplomático, comercial, espionaje internacional, NASA, CIA, KGB, etcétera.

[15] VILLALOBOS PEREZ, Jesús, "La Nulidad de los Instrumentos Notariales", *Revista del Colegio de Notarios de Jalisco*, Primer Semestre, Gráfica Nueva, Guadalajara Jalisco, 1990, p. 88, Número 119, México, agosto 1998, p.130.

LA SEGURIDAD DEL DOCUMENTO ELECTRÓNICO: RETO JURÍDICO DEL PRESENTE

Alicia Rendón López

Esta disciplina es tan antigua como las civilizaciones del mundo, pues ya desde el siglo V a.C. se utilizaba la técnica del cifrado para proteger información real. Durante la segunda guerra mundial se dieron grandes avances, ya que los países en conflicto desarrollaron técnicas para romper los mensajes cifrados de los teletipos, a través de los sistemas de sustitución (un carácter se sustituye por otro) y transposición o permutación (los caracteres del mensaje se redistribuyen sin modificarlos, de acuerdo con determinadas reglas, dentro del criptograma) de caracteres.

> Entendemos por Criptografía (*Kriptos* = ocultar, *Graphos*=escritura) la técnica de transformar un mensaje inteligible, denominado **texto en claro**, en otro que sólo puedan entender las personas autorizadas a ello, que llamaremos **criptograma** o texto cifrado. El método o sistema empleado para cifrar el texto en claro se denomina **algoritmo de encriptación**.[16]

Toda criptografía se encuentra basada en un algoritmo, la función de este algoritmo es básicamente codificar la información para que sea indescifrable a simple vista, de manera que una letra "A" pueda equivaler a: "2x4AeaA", así el trabajo del algoritmo es precisamente determinar cómo será transformada la información de su estado original a otro que sea muy difícil de descifrar. Hoy en día los algoritmos de criptografía son ampliamente conocidos, es por esto que para prevenir a otro usuario "no autorizado" descifrar información cifrada, el algoritmo utiliza lo que es denominado llave "key", para controlar el cifrar y descifrar la información.

Un ejemplo de ello, es la gran cantidad de grupos financieros e instituciones bancarias que han utilizado este medio por muchos años para el manejo de transferencias de fondos o giros de dinero de una localidad a otra; o como el caso del Banco Nacional de México, Sociedad Anónima, que lleva un sistema de criptografía en sus sistemas de operaciones bancarias en las sucursales de todo el país, así como sus corresponsales en otros

16 http://www.galeon.com/analisisdealgoritmos/enlaces628082.html. Consultada: 1 de octubre de 2009.

países del mundo; en ambos casos, la clave de cifrado solo es del conocimiento del personal autorizado.

Sin embargo, aún ahora, una gran cantidad de documentos informáticos, que circulan por la red, no tienen cifrado alguno y por tanto, la seguridad con la que cuentan los correos y documentos electrónicos es realmente nula, ya que un correo electrónico normal, en esas condiciones, es como *una postal sin sobre*, que puede ser leída por todo el que tenga interés en su contenido. Por eso es sugerible, que para preservar la intimidad en los mensajes de correo y documentos electrónicos, se recurra a la criptografía, pues por medio de potentes técnicas criptográficas, el contenido del mensaje puede ser enviado ***cifrado***, permitiendo así que sólo el destinario legítimo del correo sea capaz de leerlo. Con este mecanismo se garantiza, aún cuando sólo sea parcialmente, la confidencialidad y autenticidad de los mismos.

Razón por la cual, los modernos sistemas de seguridad del correo, como PGP (Pretty Good Privacity) y otros, no se limitan a cifrar el contenido de los mensajes intercambiados, sino que también añaden otros servicios, como el de *la integridad*, que garantiza que el contenido del mensaje no ha sido alterado por el camino; *la autenticación*, que asegura la identidad del remitente del correo, de manera que podemos estar seguros de que fue escrito por quien lo envió y no ha sido falsificado; y el *no repudio*, que nos protege ante situaciones en donde el que envío el correo (o lo recibió) alegue posteriormente no haberlo enviado (o recibido). Estos últimos servicios se prestan mediante firmas digitales.

Se distinguen dos métodos generales de cifrado:

1. **Cifrado simétrico**

Cuando se emplea la misma clave en las operaciones de cifrado y descifrado, se dice que el criptosistema es simétrico o de clave secreta. Estos sistemas son muchos más rápidos que los de clave pública y resultan apropiados para el cifrado de grandes volúmenes de datos. Para ello se emplean algoritmos (estructuras lógicas que

denotan una instrucción u orden) como IDEA (International Data Encription Algorithm), RC5, DES (Data Encription Standart), TRIPLE, PGP (Pretty Good Privacity), etc.[17]

2. **Cifrado asimétrico**

Cuando se utiliza una pareja de claves para separar los procesos de cifrado y descifrado, se dice que el criptosistema es asimétrico o de clave pública. Una clave, se mantiene secreta, mientras que la segunda clave, la pública, es conocida por todos. De forma general, las claves públicas se utilizan para cifrar y las privadas para descifrar. El sistema posee la propiedad de que a partir del conocimiento de la clave pública no es posible determinar la clave privada, ni

descifrar el texto con ella cifrado. Los criptosistemas de clave pública, aunque más lentos que los simétricos, resultan adecuados para los servicios de autenticación, distribución de claves de sesión y firmas digitales. Se utilizan los algoritmos de Diffie-Hellman (1976), RSA (actualmente), etc.[18]

En general, el cifrado asimétrico se emplea en *claves de sesión* para información y documentos públicos. De modo que pueda ser transmitida sin peligro a través de la red junto con el documento cifrado. La clave de sesión se cifra como pública y normalmente aparecerá en una libreta de claves públicas. Un ejemplo de ello es el One Time Password (contraseña de un solo uso) o clave de sesión.

El cifrado asimétrico se emplea también para firmar documentos y autenticar entidades, como se describe a continuación.

Para obtener una firma digital segura, es necesario cifrar un documento con la clave privada, que solo tiene el poseedor de la misma. Posteriormente, cualquier persona utilizando la clave pública podrá decifrarlo, verificándose así la identidad del firmante.

> En la práctica, debido a que los algoritmos de clave pública son muy ineficaces a la hora de

[17] http://www.alfa-redi.org/rdi-articulo.shtml?x=950 Consultada: 1 de octubre de 2009.

[18] *Idem*.

LA SEGURIDAD DEL DOCUMENTO ELECTRÓNICO: RETO JURÍDICO DEL PRESENTE

Alicia Rendón López

cifrar documentos, los protocolos de firma digital se implementan junto con funciones unidireccionales de resumen, de manera que en vez de firmar un documento, se firma un resumen del mismo. Este mecanismo implica el cifrado mediante la clave privada del emisor del resumen de los datos, que serán transferidos junto con el mensaje. Este se procesa una vez en el receptor, para verificar su integridad. Por lo tanto, los pasos del protocolo son (v. figura):

1. (A) Genera un resumen del documento.
2. (A) Cifra el resumen con su clave privada.
3. (A) Envía el documento junto con el resumen firmado a (B).
4. (B) Genera un resumen del documento recibido de (A), usando la misma función unidireccional de resumen. Después descifra con la clave pública de (A) el resumen firmado, si coincide con el resumen que (B) ha generado, la firma es válida

De esta forma se ofrecen conjuntamente los servicios de no repudio, ya que nadie excepto (A) podría haber firmado el documento, y de autenticación, ya que si el documento viene firmado por (A), podemos estar seguros de su identidad, dado que sólo él ha podido firmarlo. En último lugar, mediante la firma digital se garantiza asimismo la integridad del documento, ya que en caso de ser modificado, resultaría imposible hacerlo de forma tal que se generase la misma función de resumen que había sido firmada.[19]

El PGP (Pretty Good Privacity)

[19] http://www.iec.csic.es/CRIPTONOMICON/correo/firma.html Consultada: 1 de octubre de 2009.

También conocido comúnmente por sus siglas PGP, es una aplicación informática de criptografía de alta seguridad. PGP permite enviar mensajes con intimidad y autenticación. Entendiendo por intimidad, que sólo el destinatario podrá leer el mensaje y, por autenticación, que se podrá identificar al remitente del mensaje con seguridad.

Este programa permite que la información por vía electrónica que nos es enviada no sea leída por nadie más que el destinatario, o poder advertir si fue alterada la información durante su envío.

El PGP utiliza la criptografía de clave pública. Esto quiere decir que todo el que lo utiliza tiene que tener las claves, una pública y otra secreta o privada.

3. Claves privadas y públicas en el documento electrónico

La firma electrónica está compuesta por una llave privada y una llave pública, en pro de la seguridad que autentifique y proteja contra violaciones.

Estas claves son un par de números matemáticamente relacionados entre sí, mediante el uso de un programa de cómputo que se conceptualiza como un archivo binario o una cadena de *bits* o *bytes* y que pueden ser utilizadas para que un sujeto determinado manifieste su voluntad al reconocer el contenido de un documento electrónico o la autoría del mismo.

Generalmente, la clave privada es usada para el procedimiento de firmado de un documento electrónico y, la clave pública para el procedimiento de autenticación de dicho documento.

La clave pública sirve para que el resto del mundo pueda enviar mensajes cifrados. Normalmente la clave pública se deja en algún servidor de claves para que los demás puedan buscarla a través de internet.

Así mismo la clave pública tiene otra utilidad, sirve para comprobar la identidad de un mensaje firmado.

4. Clave secreta

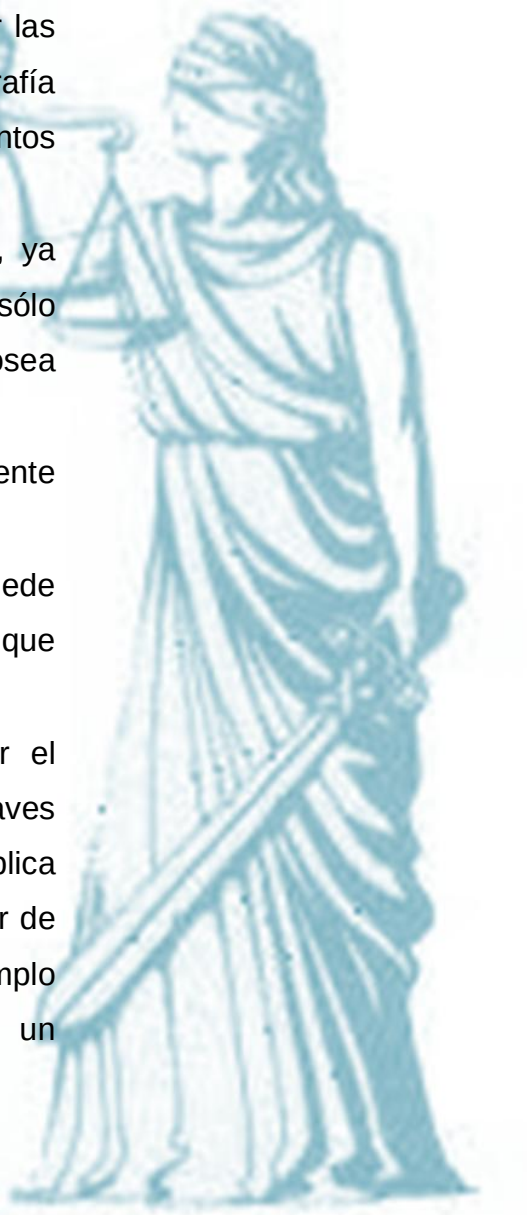
La clave secreta sirve para desencriptar los mensajes que se reciban. Como el remitente ha cifrado el mensaje con la llave pública sólo el destinatario puede descifrarla. La

llave privada o secreta también es necesaria para firmar un mensaje.

Coincido con los operadores informáticos, en que podemos encontrar las siguientes ventajas del uso de la criptografía de clave pública en los documentos electrónicos:

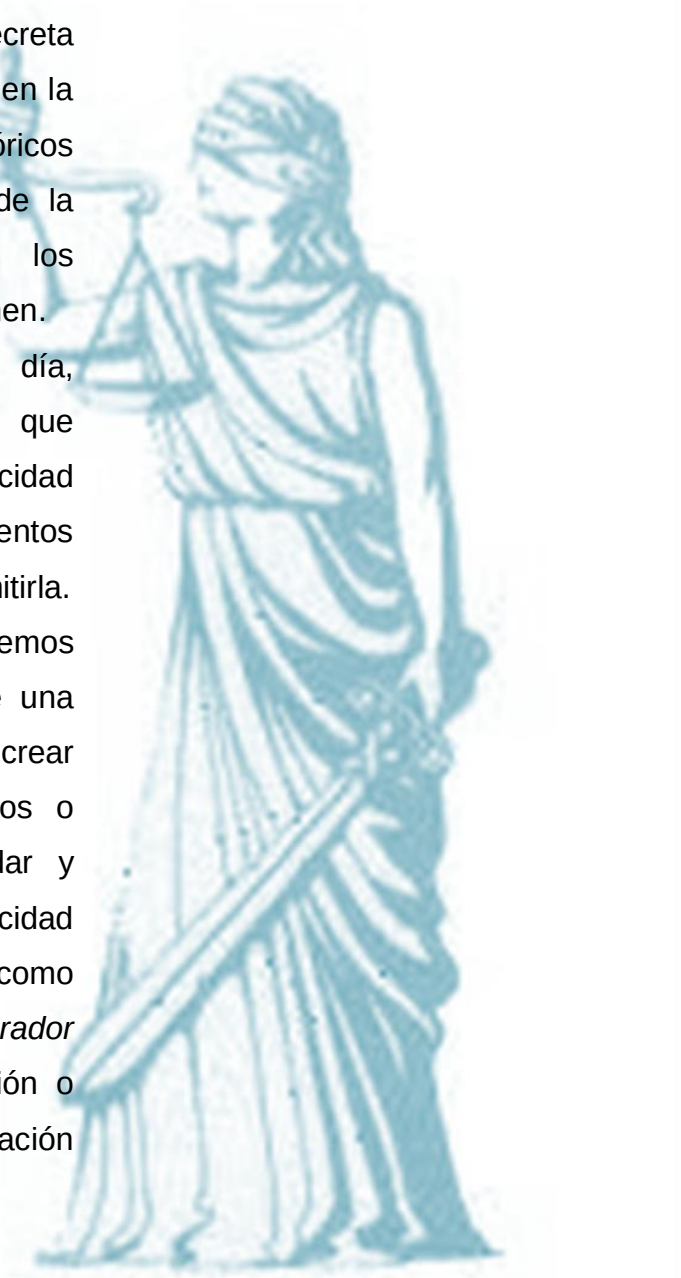
- No se necesita un canal seguro, ya que el mensaje (información) sólo podrá se descifrado por quien posea la clave privada o secreta.
- Permite verificar al remitente unívocamente mediante su firma.
- Mediante la clave pública no se puede deducir la clave secreta, por lo que asegura la intimidad.
- Lo primero que tiene que hacer el usuario, es crear un juego de llaves personal y distribuir su clave pública por e-mail o mediante un "servidor de claves (LISTSERV) como por ejemplo el Rediris que sólo supone un mensaje".[20]

No todo está dicho en esta materia, pero hasta hoy la criptografía continúa aportando elementos de seguridad a los documentos electrónicos.



20 http://www.rediris.es/difusion/publicaciones/boletin/33/enfoque2.html Consultada: 1 de octubre de 2009.

V. CONCLUSIONES



Los criptosistemas de clave privada, secreta y pública, de firma digital y no repudio en la transmisión de datos, son modelos teóricos que se han implementado en aras de la seguridad de la información y los documentos electrónicos que la contienen.

Tales sistemas, supone hoy en día, una posibilidad real y concreta que garantizan la confidencialidad y autenticidad de la información y los documentos electrónicos que se utilizan para transmitirla.

No obstante, los juristas tenemos como reto del presente, y dentro de una investigación interdisciplinaria, el crear nuevas formas, modelos, instrumentos o directrices, que permitan salvaguardar y garantizar la confidencialidad y autenticidad de los documentos electrónicos, así como para detectar al *agente* u *operador informático* que accese sin autorización o haga uso indebido de la información contenida en los mismos.

VI. BIBLIOGRAFIA

DELGADO DE MIGUEL, Juan Francisco, *Deontologías Notarial*, Junta de Decanos de los Colegios Notariales de España, Consejo General del Notariado, Imprenta Firma Mieres, Madrid, 1993.

DEL CASTILLO NEGRETE ILLANES, María de las Mercedes, Tesis de Maestría, División de Estudios de Posgrado de la Facultad de Derecho de la UNAM, México, 2006.

ESCOBAR DE LA RIVA, Eloy, *Tratado de Derecho Notarial*, Editorial Marfil, Barcelona, España, 1957.

GUIBOURG, Mario, et al; *Manual de Informática Jurídica*, Editorial de Alfredo y Ricardo Depalma, Buenos Aires, Argentina, 1996.

MALDONADO OTERO, Claudia Gabriela, *Presentación de Microsoft Office Power* Point 97-2003: Informática Jurídica metadocumentaria o Decisional, 2009.

P. SANDOVAL ZAMORA, HUGO, "México, un buen mercado para internet", *El Universal*, jueves 28 de diciembre de 2006.

REVISTA DE DERECHO NOTARIAL, ASOCIACIÓN NACIONAL DEL NOTARIADO MEXICANO, A.C. Número 110, México, abril 1997.

TÉLLEZ VALDES, Julio, *Derecho Informático*, ed. 2ª, Ed. McGraww-Hill, México, 2004.

TÉLLEZ VALDES, Julio, *Seminario Taller Validez de los documentos electrónicos*, diapositiva 9 en presentación de Microsoft Office Power Point -2, Guayaquil, 15 de agosto de 2007.

VILLALOBOS PEREZ, Jesús, *La Nulidad de los Instrumentos Notariales*, Revista del Colegio de Notarios de Jalisco, Primer Semestre, Gráfica Nueva, Guadalajara Jalisco, 1990, p. 88, Número 119, México, agosto 1998.

Páginas electrónicas

http://www.cetid.abogados.ec/archivos/37.pdf Consultada el 15 de septiembre de 2009.

http://www.galeon.com/analisisdealgoritmos/enlaces628082.html Consultada: 1 de octubre de 2009.

http://www.alfa-redi.org/rdi-articulo.shtml?x=950 Consultada: 1 de octubre de 2009.

http://www.iec.csic.es/CRIPTONOMICON/correo/firma.html. Consultada: 1 de octubre de 2009.

http://www.rediris.es/difusion/publicaciones/boletin/33/enfoque2.html Consultada: 1 de octubre de 2009.