• Título en mayúsculas del Trabajo:

“ LA INTEGRIDAD, AUTENTICIDAD Y LEGALIDAD DE LOS DOCUMENTOS DIGITALES “

• Nombre del Congreso:

“ 2do CONGRESO METROPOLITANO DE CIENCIAS ECONOMICAS “

• Lugar y fecha de realización del evento:

Ciudad Autónoma de Buenos Aires - 14 AL 16 DE noviembre 2007

• Área y tema al cual pertenece:

Área XII Estudios Societarios

j) Documento digital (del papel al bit). Legislación y normativa aplicable. Experiencia Internacional.

• Nombres y apellidos de los autores.:

Dra Leonor Gladys Guini – Abogada -Procuradora

Dr. Guillermo Besana - Contador Publico

Leonor G. Guini	**Guillermo A. Besana**
Master en Derecho de la Alta Tecnología UCA.	Consultor en temas contables, tributarios e informáticos.
Profesora de grado y postgrado en temas de derecho e informática entre otras en la Universidad de Buenos Aires, CAECE, Belgrano, UTN-Sistemas.	Miembro de la Comisión de Tecnología de la Información y de la Comisión Registros Contables y documentación respaldatoria y de los foros de Internet del CPCECABA.
Fue distinguida por el Dr. Porto como “Alma Mater” en la Universidad de Ingeniería Tecnológica de Belgrano, premio que se otorga a los docentes con mayor puntaje de cada Universidad. (1999).	Miembro asesor de la Comisión de Factura Electrónica y profesor de temas vinculados a la factura electrónica, documentos digitales y firma digital de la Cámara Argentina de Comercio Electrónico.
Asesora Legal de la Oficina Nacional de Tecnologías de Información de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros.	Miembro de la Comisión Asesora en Tecnología de la Información en la FACPCE.
Expositora, autora y coautora de varios ponencias, trabajos profesionales talleres y conferencias en diversos cursos, congresos y videoconferencias del país y del exterior.	Perito de parte en temas informáticos. Desarrollador de software y diversas paginas web. Expositor en diversos congresos y videoconferencias con diversos Consejos del interior del país.

• Título en mayúsculas del Trabajo:

“ LA INTEGRIDAD, AUTENTICIDAD Y LEGALIDAD DE LOS DOCUMENTOS DIGITALES “

• Nombre del Congreso:

“ 2do CONGRESO METROPOLITANO DE CIENCIAS ECONOMICAS “

• Lugar y fecha de realización del evento:

Ciudad Autónoma de Buenos Aires - 14 AL 16 DE noviembre 2007

• Área y tema al cual pertenece:

Área XII Estudios Societarios

j) Documento digital (del papel al bit). Legislación y normativa aplicable. Experiencia Internacional.

Índice

LA INTEGRIDAD, AUTENTICIDAD Y LEGALIDAD DE LOS DOCUMENTOS DIGITALES

INTRODUCCIÓN

Durante más de tres mil años, los humanos vivimos anotando en minerales, maderas, cueros o papel, signos o formas que nos permitieran interpretar en forma más o menos indubitable las ideas o conceptos que quisiéramos comunicar.

Para que esas manifestaciones perduraran en el tiempo fue necesario que el medio utilizado asegurara mediante su alteración (por ejemplo: la escritura, que altera el papel) el reconocimiento de tales signos.

Cuando esos actos debían contener algún tipo de compromiso o acuerdo entre las partes involucradas fue necesario que el medio utilizado tuviere tres características, a saber:

1. Que su duración material fuese superior al tiempo por el que se establecía el acuerdo a efectos de su posterior constatación en caso de dudas.
2. Que permitiere detectar las manifestaciones de su alteración como por ejemplo “borrados” y “agregados” posteriores a la confección del “original”.
3. Que reconociere el “no repudio” o desconocimiento de la conformidad otorgada, lo que se logra con la inclusión de algún elemento que modificando el medio, permitiere identificar sin duda a las personas que hubieran intervenido en el acto mediante la incorporación de su firma o impresión digital.

Con la utilización del papel como medio, surgen los “originales” y las “copias” de los documentos y con el descubrimiento del papel carbónico surgen los

“duplicados”, “triplicados”, etc., todos ellos identificatorios del orden de prelación del papel en el proceso de copia.

En los últimos diez años, la tecnología nos permitió o nos obligó a otras formas de comunicación.

Estas nuevas formas implican nuevas formas de pensar o de comunicarse en forma escrita. Por ello ya no tenemos solamente el papel, sino que podemos comunicarnos a través de otros métodos como por ejemplo mediante la utilización de archivos electrónicos.

Para ello fue necesario el desarrollo de sistemas como el binario donde se piensa cómo escribir a través de un sistema lógico de ceros y unos.

Quiere decir que ya no resulta tan sencillo leer con letras y palabras. Ya no nos habla más el texto de manera directa. Ahora contamos con medios magnéticos que van a ser interpretados con ayuda de la tecnología.

Podemos decir, entonces, que en la historia ha habido tres grandes hitos en lo que a comunicación se refiere: el primero fue oral, cuando no existía la escritura y los juglares y los sabios se ocupaban de trasmitir oralmente tradiciones, historias y cultura.

El segundo sobreviene con la escritura. Gutenberg cambia el mundo y hace que un texto nos hable y que ese texto pudiera llegar a todos De ese modo, aprendimos historia, cultura y tradiciones a través de nuestras familias, nuestros maestros y los libros.

El tercer cambio, el actual, llega con la computadora. Ya no hay medio de comunicación perceptible por nuestros sentidos en forma directa.

Tres milenios de cultura poniendo su foco en el medio y ahora no lo podemos ver ni tocar pues es abstracto. Está en un soporte digital: “ CD”, “disco duro”, “diskette”, “pen driver”, etc.

Esto implica tremendos cambios en la forma de ver estos procesos de comunicación. Quitamos la atención en el medio para centrarla en el contenido semiótico del mensaje a transmitir.

Pasamos de la evolución del medio corpóreo a la simbolización abstracta.

Pasamos de la huella digital al ADN.

Si lleváramos este proceso evolutivo de milenios a términos más comprensibles, como por ejemplo un día, podríamos decir que los humanos durante todo el día estuvimos comunicándonos con elementos materiales, pero en los últimos treinta segundos pasamos a lo inmaterial.

En los sectores vinculados a la informática, las matemáticas, las ciencias exactas, la contabilidad, acostumbrados a manejarse con elementos abstractos y cambios constantes y rápidos, se han creado mecanismos de adaptación y recepción de tales cambios, mientras que en otras actividades dichos cambios producen miedo e inseguridad dificultando su compresión y utilización.

Un ejemplo muy concreto de ello son los algoritmos de verificación de integridad comúnmente denominados “HASH”, que consisten en una fórmula matemática que aplicada a una cadena de caracteres permite relacionar el valor de cada carácter con el orden que ocupa en dicha cadena generando un número de longitud constante, por ejemplo 32 dígitos.

Dicho número es único para cada cadena de caracteres y varía sustancialmente ante el menor cambio en la cadena que le dio origen.

Por ejemplo, en el caso de que esa cadena de caracteres sea un archivo de texto que contenga un contrato, la inclusión o extracción de una coma o un espacio en el texto original genera valores de “hash” absolutamente diferentes y nos indica que el archivo sufrió una alteración por mínima que ella sea.

Si bien existen infinitos valores de “hash” repetidos, el significado que le damos al contenido de la cadena que los alimenta es diferente.

Con el valor de un “hash” no se puede conocer la cadena que le dio origen pues son infinitas, pero cada cadena tiene un valor único de “hash”.

Los algoritmos de “hash” son usados en informática en forma permanente para asegurar integridad de archivos, el uso más común de ellos es asegurar la copia correcta de un archivo de un medio a otro.

Es decir, que un “hash” es un método a través del cuál me aseguro que el documento original no pueda ser alterado. Si lo altero, mi “hash” cambia, por lo tanto, es el”hash” de otro documento, el alterado.

El concepto de “hash” está tremendamente arraigado en las profesiones informáticas; en cambio, en otras, el término es casi desconocido.

Para llevar a cabo el presente trabajo es indispensable tener en cuenta este concepto de “hash”, que es como la antigua prueba del 9 en una división, si no nos da, la división está mal.

INTRODUCCIÓN AL ESTUDIO DE LA CRIPTOGRAFÍA

Uno de los mayores problemas que plantea una red abierta es lograr su seguridad y confidencialidad. Actualmente y debido al incremento de las transacciones comerciales en Internet y a la transmisión de información delicada, es cuando más se requiere garantizar la seguridad.
El medio por excelencia para lograrlo es la criptografía, la cual, si bien fue utilizada en un comienzo para transmitir información diplomática y militar, hoy en día está disponible para todo el mundo.
El único inconveniente que se presenta es que muchas veces se la compara con material bélico y de allí que se prohíba su exportación, pero su uso por excelencia es la posibilidad de crear firmas digitales, autenticar archivos,

verificar su integridad, todo lo cual posibilita y favorece el desarrollo del comercio electrónico.

¿QUE ES ENCRIPTACIÓN?

Es un mecanismo que, mediante la utilización una clave, hace que un mensaje se haga incomprensible para quienes no la conocen.

El procedimiento de “encriptado” seria el siguiente:

1. Emisor y receptor se ponen de acuerdo en usar una clave.
2. El emisor crea el mensaje a enviar mediante un algoritmo que utiliza la clave acordada y lo transforma en ilegible.
3. El receptor aplica el algoritmo usando la clave acordada en sentido contrario y vuelve comprensible el mensaje.

Este mecanismo que utiliza una única clave previamente acordada por las partes se llama “de clave simétrica” y asegura la Confidencialidad del mensaje frente a terceros extraños pero no su autoría.

Por ejemplo, emisor y receptor se ponen de acuerdo en usar como clave el número 4. El emisor crear el mensaje y al enviarlo reemplaza cada carácter por aquel que está cuatro veces más adelante en el orden alfabético (en lugar de “hola” sería “lsoe”).

Este mecanismo no asegura la autoría del mensaje ya que su autor podría desconocer que lo escribió, pues ambas partes, al conocer la clave, pueden acceder al mensaje original y cambiarlo.

Para permitir asegurar la vinculación única y en un solo sentido entre emisor y mensaje existen algoritmos matemáticos que generan 2 claves que son dos números primos sustancialmente grandes que están vinculados entre sí en forma única. Una clave es de conocimiento exclusivo del emisor y se llama

“clave privada”, mientras que la otra es conocida por cualquier persona que acceda al mensaje y se llama “clave pública”.

Obviamente, con la clave pública no puede conocerse cuál es la clave privada.

Este mecanismo de encriptación se llama “de clave asimétrica” y tiene como característica que, una vez cifrado con la clave privada, no puede accederse a un mensaje con esa misma clave, sino que solo puede desencriptarse exclusivamente con la pública, y viceversa.

Este mecanismo asegura el “no repudio” del emisor ya que no puede desconocer su uso en el procedimiento.

Tampoco asegura confidencialidad, pues al mensaje se puede acceder por cualquier persona que conozca la clave pública.

Entonces, encriptar es poner en clave un mensaje. Su autor puede desconocer su autoría, a menos que se utilice clave asimétrica. En caso de utilizarse esta última, el emisor no podría desconocer su mensaje, pues sólo él es quien pudo haberlo firmado dado que la clave privada se encuentra bajo su exclusivo control. Sin embargo, no es confidencial.

¿QUÉ ES CRIPTOGRAFÍA?

Es el estudio, diseño e implementación de algoritmos usados para transformar un mensaje original, llamado texto claro, en otro aparente, ininteligible u oculto llamado criptograma, siendo esto el proceso de encriptado o cifrado. La operación inversa a fin de obtener la información original es el descifrado del mensaje.
Para ser considerados seguros los algoritmos tienen que ser públicos, o sea que se deben exponer a la comunidad científica por un período de tiempo considerable para que se les encuentren fallas o “back doors” intencionales. Por lo que los algoritmos considerados seguros son aquellos en donde para descubrir el mensaje no basta con tener el mensaje encriptado y el algoritmo

que se usó para encriptarlo, ya que no se lo podrá desencriptar si no se cuenta con la clave correspondiente.

¿QUÉ ES CRIPTOANÁLISIS?

Es la ciencia que analiza el sistema criptográfico con el objetivo de quebrar la seguridad del mismo.
La Criptografía es una ciencia antiquísima que existe hace 2000 años pero que a partir de 1970 con la aparición del Sistema Data Encriptation Standard (DES) y los sistemas de criptografía de Clave Pública comienza a tener una importancia clave en la actividad comercial.

EVOLUCIÓN DE LA CRIPTOGRAFÍA

La Criptografía Clásica, desde Julio Cesar en adelante y también durante la primera y Segunda Guerra Mundial, utilizaba técnicas de substitución y transposición (substituye letras del alfabeto por otras ubicadas en otro lugar o bien se envían letras del mensaje mezcladas entre sí).

CRIPTOGRAFÍA MODERNA

SISTEMA DE CLAVE SIMÉTRICA

Utiliza fuertes bases matemáticas y existe un conjunto de algoritmos que se utilizan tanto para el cifrado como para el descifrado con una única clave, por lo que toda la seguridad del sistema depende del secreto de la clave, que debe ser comunicada a todos los posibles receptores, apareciendo así el problema de encontrar un canal seguro de distribución de claves.

SISTEMA DE CLAVE ASIMÉTRICA

Sin embargo, en los sistemas de Clave Pública O ASIMÉTRICA se generan dos claves relacionadas entre asumiendo que la privada nunca va a ser

trasmitida por canal alguno, entendiéndose que lo que hace una clave la otra lo deshace.

EJEMPLO DE UN CRISPOSISTEMA DE CLAVE ASIMÉTRICA.
Texto Plano + Clave Privada + Algoritmo de Encriptación = Criptograma
Criptograma + Clave Publica + Algoritmo de Desencriptado = Texto Plano.

ALGORITMOS DE CIFRADO DE CLAVE SECRETA

Los algoritmos simétricos usan una única clave, por lo tanto el emisor y el receptor se deben haber puesto de acuerdo en que clave usar de antemano y deben hacerlo por un canal seguro. La seguridad se encuentra en la clave la que debe ser mantenida en secreto.
Ejemplos de este tipo de algoritmo es el sistema DES (data encryption Standard) 3DES y AES.

SISTEMAS DE CLAVE PÚBLICA

La Criptografía de clave pública fue desarrollada en 1977 con el nombre de RSA (siglas compuestas de las iniciales de sus inventores, Rivest, Shamir y Adleman); implica el uso de dos claves, una privada y otra pública.
Los algoritmos asimétricos fueron inventados en 1976 por Whitfield Diffie y Martin Hellman. Para operar usan un par de claves, una pública y otra privada, que tienen las siguientes propiedades:
Todo lo que está encriptado por una de ellas solo puede ser desencriptado por la otra.
En estos sistemas las dos claves se generan al mismo tiempo. Cada clave abre el código que produce la otra. Saber la clave pública no sirve para deducir la clave secreta correspondiente. La clave pública puede publicarse y distribuirse ampliamente por una red de comunicaciones.
Cualquiera puede utilizar la clave pública de un destinatario para encriptar un mensaje y él empleará su clave secreta para desencriptarlo. Sólo él lo podrá hacer, ni siquiera la persona que lo encriptó podría descifrarlo.

La autenticación se logra, puesto que la clave secreta del remitente puede emplearse para encriptar el mensaje. Así se genera un valor, que el destinatario puede comprobar descifrándolo con la clave pública del remitente. De esta manera se prueba el verdadero origen del mensaje, ya que solo el remitente posee la clave secreta que ha producido ese valor,

La fortaleza del sistema depende de lo larga que sea la clave ya que a cualquier atacante que no posea la clave privada le costaría años calcular la función inversa.

AUTENTICACIÓN - INTERVENCIÓN DE LA AUTORIDAD CERTIFICANTE.

Por lo tanto, si cada individuo u organización mantiene su clave privada en secreto, y a la vez da a conocer su clave pública, se puede lograr los objetivos de autenticación mediante la utilización de clave asimétrica la que me permite comprobar de quien realmente proviene el documento, o, lo que es lo mismo, la identidad del firmante, la integridad del mensaje lo compruebo con la función hash, ya que me aseguro que llegará a destino íntegro sin alteraciones y finalmente, si quiero confidencialidad utilizo alguna función criptográfica.

Si A quiere mandar un mensaje encriptado a B, lo único que tiene que hacer es encriptarlo con la clave pública de B y por las propiedades asimétricas de estas claves, el único que podrá desencriptar el mensaje es B con su clave privada. Este protocolo tiene un punto débil de seguridad que radica en la acreditación de la titularidad de la claves publicas de los individuos. Supongamos que transcurre la misma situación anterior. A desea mandarle a B un mensaje encriptado. Entonces lo primero que necesita A es la clave pública de B, como A no tiene todas las claves públicas de todos los individuos, debe obtenerla de alguna manera. Si se la pide a B directamente, correrá el riesgo que B la desconozca.

Como esto podría ocurrir siempre, para resolver este problema se parte por asumir la confianza inicial de todos los individuos en una institución, la que nos provee la clave pública de alguna forma segura tradicional. Esta institución es la llamada Autoridad Certificante (C.A), Certification Authority, que autentica a las personas y garantiza la identidad de las mismas y su vinculación con su clave pública mediante la emisión de certificados. El certificado consistirá en un

conjunto de datos básicos del individuo y su clave pública, todo firmado digitalmente por la C.A. En el ejemplo referido, A puede obtener la clave pública de B pidiéndole el certificado emitido por la C.A a B o bien pidiéndoselo directamente a la CA, si verificamos que el certificado fue emitido por la autoridad certificante; dentro del mismo certificado encontraremos la clave pública de B con lo que así podremos dar seguridad al sistema.

FUNCION "HASH"

Es unidireccional, lo que indica que es fácil de calcular hacia un lado pero imposible a la inversa ya que existen infinitas respuestas.
Cuando la función "hash" se aplica a un mensaje de cualquier longitud se obtiene un pequeño resultado de un numero limitado de caracteres por lo que cualquier cambio en el mensaje original modificaría sustancialmente el valor "hash".
Para obtener otro mensaje que iguale al que se quiere falsificar se necesitaría mucho esfuerzo. Este sistema se utilizó primariamente para autenticar programas libres de virus; por ejemplo, al programa se le aplica una determinada fórmula y el receptor verifica el resultado calculando lo mismo sobre el mensaje recibido; si obtiene la misma respuesta, puede estar seguro de su integridad.

FIRMA DIGITAL- CÓMO FUNCIONA

¿Qué es una firma digital?
Cuando el "hash" de un mensaje es encriptado con la clave privada del emisor, entonces estamos frente a una firma digital.
Esto permite al receptor verificar la integridad y autoría de un mensaje, pero no asegura confidencialidad ya que el mensaje viaja sin ser cifrado.
Un sistema de firma digital tiene entonces 3 elementos.

1. Un archivo con el mensaje original que puede estar encriptado o no.
2. Un archivo con la firma digital que es el "hash" del archivo original ya encriptado con la clave privada.

3. Un archivo con la clave pública del emisor (certificado digital).

Cuando el mensaje viaja encriptado con la clave pública del destinatario, se dice que el mensaje tiene “ensobrado digital” asimilándolo a una carta dentro de un sobre. Con esta técnica se logra la más absoluta confidencialidad ya que solo el receptor puede acceder al mensaje con su clave privada. Una vez desencriptado podrá verificar su concordancia con la firma digital.

El programa que utilizamos para firmar digitalmente un documento realiza los siguientes pasos:

1) Procesa el texto que queremos firmar con un programa que se conoce como función “hash” o digesto. Este programa produce un número con una determinada y constante cantidad de caracteres; este número recibe el nombre de “hash”, digesto o huella digital.

El “hash” es una función matemática que se calcula en relación con la ubicación que tiene cada elemento dentro del documento. Si el documento cambió cambia sustancialmente el número de “hash” aunque ese cambio en el original sea mínimo. Estas funciones son unidireccionales; esto quiere decir que a cada documento le corresponde un valor hash, pero con el valor hash no se puede conocer el origen pues son infinitos los orígenes que pueden dar el mismo valor.

2) Una vez obtenido el “hash”, el sistema lo encriptará utilizando la clave privada del emisor. Esto dará lugar a un nuevo número o documento conocido con el nombre de firma digital o valor PKCS#7 donde PKCS es un estándar de criptografía y 7 es el número del estándar que hace referencia a su cálculo.

En resumen la firma digital es la huella digital del documento encriptado con clave privada del firmante

Tenemos que la firma depende del documento al cual se le aplica una función “hash” y del firmante, ya que el “hash” se encripta utilizando su clave privada, lo que implica que existe una vinculación lógica entre firmante, firma y documento.

El circuito se cierra enviando al receptor un paquete que consiste en el mensaje plano, la firma digital y la clave pública del emisor.

PROCESO DE VERIFICACIÓN DE FIRMA

El destinatario, para verificar la firma, deberá proceder de la siguiente manera:

1) Desencriptar la firma digital con la clave pública del emisor recibida obteniendo el número de “hash” original producido por el emisor.
2) Obtener el valor hash del archivo recibido.
3) Compararlos.

Si los números de “hash” coinciden significa que el documento no fue alterado, ya que, si hubiese sido alterado durante su transmisión el “hash” del documento recibido, diferiría el original obtenido como resultado de la desencripción de la firma digital.

De esta manera se corrobora la autoría e integridad del mensaje ya que si nos aseguramos que la clave pública recibida corresponde al emisor del mensaje la única posibilidad es que la firma digital haya sido producida con la única clave privada que se corresponde con dicha clave pública. Caso contrario, los números de “hash” calculados por emisor y receptor no coincidirían.

Este proceso de verificación permite demostrar a un tercero que una persona específica firmó un documento determinado, lo que implica que su autor no podrá repudiar dicha firma.

La única persona capaz de haber producido ese documento es el titular de la clave privada correspondiente ya que el requisito de exclusividad reside en el secreto y posesión de la clave privada.

La manera de saber fehacientemente que una clave pública pertenece al autor del documento es a través de un tercero de confianza o autoridad certificante.

Un certificador da fe de que una clave pública pertenece a una persona determinada a través de la emisión de un certificado de clave pública, lo que significa que certifica que una persona es titular de una clave expidiendo a su favor un documento electrónico llamado “certificado de clave pública”.

El emisor no envía su clave al destinatario sino su certificado de clave pública firmado digitalmente por la autoridad certificante. Esto asegura al destinatario que dicha clave pertenece al emisor y utilizará la clave para verificar el mensaje recibido firmado digitalmente por el emisor.

Lo que necesito para firmar digitalmente es mi clave privada y lo que se necesita para verificar una firma digital es la clave pública del emisor contenida en el certificado de clave pública expedido por un tercero de confianza que da fe respecto de la autenticidad de la información personal contenida en el certificado.

La autoridad certificante asocia los datos de identidad del usuario o suscriptor de un certificado con la clave pública de dicho suscriptor.

Los certificados se encuentran seriados. Incluyen: período nombre, DNI, apellido, período de validez y demás datos que la autoridad quiera certificar y todo ello cerrado y autenticado con firma digital de la autoridad certificante que lo expide.

RECEPCIÓN LEGAL MARCO NORMATIVO APLICABLE

En nuestro país la iniciativa de Firma Digital nace en el seno del Estado Nacional hace aproximadamente una década. Las tareas de investigación, difusión e innovación en esta tecnología se han centralizado en la Secretaría de la Función Pública, después Subsecretaría de la Gestión Pública, específicamente en la Oficina Nacional de Tecnologías de la Información. Desde ese entonces, se han implementando en el Sector Público diversas iniciativas relativas a la digitalización de sus circuitos administrativos y a la utilización de la firma digital para dotar de seguridad a las comunicaciones internas.

En diciembre del año 2001, el proceso se consolida a partir de la promulgación de la Ley Número 25.506 de Firma Digital, que promueve la utilización de esta tecnología en el ámbito interno del Estado y en sus relaciones con los administrados (artículo 47, Capítulo XI, “Disposiciones Complementarias”) y establece un plazo máximo de cinco años para que sea aplicada a la totalidad de las leyes, decretos, decisiones administrativas, resoluciones y sentencias emanadas del Sector Público Nacional, propendiendo a su progresiva despapelización (artículo 48). Estos dos aspectos, que podemos resumir como una conjunción entre aplicaciones y despapelización, son los pilares desde los cuales se estimula la utilidad de la firma digital y el destacable papel que esta

herramienta puede cumplir no sólo en términos de eficacia sino más bien de eficiencia administrativa.

A partir del marco legal, complementado por una serie de decretos reglamentarios y complementarios a la normativa, que establece la organización institucional de todo lo referido a la Firma Digital (infraestructura, autoridad de aplicación, auditoria, comisión asesora) y, define sus diversos componentes (firma, documento y certificado digital, titular del certificado y certificador licenciado) además de la responsabilidad y las sanciones, se sentaron las bases para la implementación y difusión de esta herramienta en el país, comenzando por el sector público -(siguiendo el ejemplo de muchas experiencias internacionales)-; aprobada la Decisión Administrativa 6/2007 el 12 de febrero del corriente año, se está en condiciones de comenzar a otorgar certificados a certificadores licenciados desde una AC (Autoridad de Certificación) Raíz Nacional. La referida Decisión junto con sus ocho anexos contiene las llamadas normas de Licenciamiento, las que describen el proceso técnico y jurídico necesario a fin que los certificadores licenciados otorguen certificados digitales a terceros con validez jurídica; asimismo, instala la AC Raíz Nacional en condiciones de máxima seguridad ya que cualquier tipo de intromisión pondría en peligro el sistema íntegro.

Por último, el Plan Nacional de Gobierno Electrónico (PNGE), implementado a partir del Decreto 387 de abril de 2005 dio un impulso aún mayor a esta tecnología impulsando la digitalización de la documentación pública, en orden a un intercambio más fluido entre el Estado y la ciudadanía, y una mayor y mejor interoperabilidad entre las distintas instancias de la Administración Pública. Dicho decreto alude explícitamente en el Anexo I, a la utilización de Firma Digital asociándola con la tramitación, el documento y el timbrado electrónicos y con la aplicación del Expediente Electrónico para trámites internos del Estado Nacional.

INTRODUCCIÓN A LA TEMÁTICA DE FIRMA Y CERTIFICACIÓN

La firma y la certificación son dos términos simétricos asociados a los modos en que las personas garantizan la autoría de documentos. Firmar implica identificarse y al mismo tiempo aprobar lo escrito en un documento, mientras

que la certificación tiene que ver con la contrapartida, con el momento de dar fe que una firma es válida y que la identidad del firmante se corresponde con la del autor del documento. Hoy en día, cuando las redes abiertas como Internet revisten cada vez mayor importancia para la comunicación mundial se impone la digitalización de muchos procesos asociados a la vida cotidiana, entre ellos la firma y la certificación.

Muchos han sido los sistemas de seguridad que el ser humano ha creado para comprobar en una comunicación la identidad del interlocutor (como la firma o el carnet de identificación), asegurarse de que sólo obtendrá la información el destinatario seleccionado (mediante el correo certificado por ejemplo), que además ésta no podrá ser modificada (ante un escribano) e incluso que ninguna de las dos partes podrá negar el hecho (firmas ante escribanos) ni cuándo se produjo (a través del fechado de documentos). En buena parte de los casos el sistema de seguridad se basa en la identificación física de la persona, información que se contrasta con el documento de identidad (DNI) expedido por la autoridad estatal. Aquí tenemos los tres pilares de una comunicación segura: las dos partes que entran en contacto y un tercero de confianza (en este caso el Estado) que garantiza que las personas que figuran en los documentos son quienes dicen ser.

Ahora bien, como decíamos antes, en la actualidad, cada vez mayor número de actividades se está trasladando al mundo electrónico a través de Internet. Se hace, por lo tanto, necesario trasladar también los sistemas de seguridad a este contexto en el que el principal problema reside en que no existe contacto directo entre las partes implicadas. Necesitamos un documento digital que ofrezca las mismas funcionalidades que los documentos físicos con el plus de ofrecer garantías aún sin presencia física. ¿Cómo se resuelve este problema? Gracias a mecanismos criptográficos siendo los dos elementos fundamentales el certificado y la firma digitales.

En el procedimiento de Firma Digital intervienen los siguientes elementos:

• Una Clave Privada para firmar digitalmente (en poder sólo de su titular)

•La correspondiente Clave Pública para verificar dicha Firma Digital (públicamente disponible).

• El Certificado de Clave Pública que identifica al titular de dichas claves,

Existe acuerdo a nivel mundial de que la firma digital basada en la criptografía de clave pública constituye en la actualidad el único mecanismo que permite resolver las cuestiones de seguridad y certificación en redes abiertas. En este sentido, se coincide en forma casi unánime que el término firma digital debe reservarse para aquel mecanismo que se basa en la criptografía de clave pública. La utilización de la firma digital constituye un avance muy importante en el campo de la seguridad que toda transacción electrónica requiere, sin que esto implique que no existan otros medios para lograr dicha seguridad. La implementación de la firma digital requiere el desarrollo de una compleja infraestructura que permita su correcto funcionamiento. Dicha infraestructura está íntimamente relacionada con el sistema legal imperante en cada país.

CONCEPTO DE DOCUMENTO DIGITAL

El concepto de documento digital surge del artículo 6 de La Ley 25.506, el que lo define como la representación digital de actos o hechos, con independencia del soporte utilizado para su fijación almacenamiento o archivo. Estableciendo que un documento digital satisface también el requerimiento de escritura.

Este principio tomado por nuestra ley de firma digital de La Ley Modelo sobre Comercio Electrónico de la Comisión de las Naciones Unidas para el Derecho Mercantil Internacional establece el principio de equivalencia de los medios electrónicos a los medios en soporte papel en cuanto a su validez y efectos jurídicos como en cuanto a su validez probatoria. De ello se puede colegir que un documento electrónico firmado digitalmente tiene el mismo valor probatorio que un documento escrito.

A fin de reafirmar este concepto, la citada normativa también establece el principio de “no discriminación entre los medios electrónicos”, el que significa que no se puede privar de valor a una firma, documento, acto o contrato por el hecho de constar en un medio electrónico

La Ley 25.506 establece el principio de equivalencia funcional entre la firma ológrafa y la firma digital, principio que surge de su artículo 3 de la citada norma, el cual establece: “Cuando la ley requiera una firma manuscrita, esa exigencia también quedará satisfecha por una firma digital”. Este principio es

aplicable a los casos en que la ley establece la obligación de firmar o prescribe consecuencias para su ausencia".

FIRMA DIGITAL Y FIRMA ELECTRÓNICA

Ley de Firma Digital reconoce dos elementos pasibles de ser utilizados por el signatario como medio de identificación: la firma digital y la firma electrónica.
En dicho marco, se define la firma electrónica en su artículo 5 como "el conjunto de datos electrónicos integrados, ligados o asociados de manera lógica a otros datos electrónicos, utilizado por el signatario como su medio de identificación, que carezca de alguno de los requisitos legales para ser considerada firma digital…".
Se podría decir por esta última acotación que hace la ley en el artículo citado que la firma electrónica no es el género que engloba a la firma digital, sino el complemento que llena el universo, ya que todo lo que no reúne los requisitos legales para ser firma digital es firma electrónica.
Conforme al desarrollo expuesto, nuestra ley de firma digital admite que dentro del concepto de firma electrónica podamos encuadrar otros mecanismos que eventualmente pueden cumplir con las funciones de la firma, como lo son los nuevos mecanismos de identificación automática de la voz, de huellas digitales, de iris, del ADN, que cuenten con una llave biométrica.
A los fines de un mayor entendimiento debemos dejar sentado entonces que el concepto de firma electrónica es sumamente amplio ya que si bien en términos técnicos una firma electrónica realizada con un certificado emitido por un certificador no licenciado sí reuniría los requisitos técnicos de una firma digital, no reuniría dichos requisitos desde el punto de vista legal, no sólo porque el valor probatorio de la firma digital es superior al de la firma electrónica (arts 5 y 7 de La Ley 25.506) sino también porque la firma digital se encuentra soportada por una infraestructura de firma digital (arts 26 a 36 de La Ley 25.506).
Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere que el certificado digital del firmante haya sido emitido por un certificador licenciado, lo que significa que cuente con la aprobación del Ente Licenciante de firma digital, por lo que en el caso de tratarse de un documento

firmado electrónicamente, el certificado asociado a la firma no se encontrará emitido por un certificador licenciado por la autoridad de aplicación de la infraestructura de firma digital (Ley 25.506 y normas complementarias y concordantes).

En síntesis, nuestra ley ha fortalecido notablemente la eficacia de aquellos documentos que cuentan con firma digital basada en un certificado emitido por un certificador licenciado, hasta casi darles un valor probatorio tan alto como el que corresponde a un instrumento privado reconocido, concediendo una presunción *iuris tantum* a la firma digital, ya que cualquier duda sobre su validez podrá ser objeto de comprobación técnica, trasladando la carga de la prueba a quien quiera negar la validez del documento firmado digitalmente.

Obviamente la finalidad de la ley ha sido incrementar la confianza pública en la firma digital emitida por un certificador licenciado, pero ¿cuáles son los riesgos de utilizar un documento digital firmado electrónicamente? La respuesta la encontramos en el mismo artículo 5, que define el concepto de firma electrónica como aquella que carece de alguno de los requisitos para ser considerada firma digital, lo que significa que no existe respecta de este elemento presunción alguna de autenticidad, integridad y no repudio; por lo que en caso de alegarse la invalidez de una firma electrónica corresponderá a la parte que la quiere hacer valer demostrar su validez, invirtiéndose de esta manera la carga probatoria, de tal manera que en caso de no poder demostrarlo, esa firma es inválida.

En síntesis los riesgos de la utilización de firma electrónica se centran fundamentalmente en la deficiencia probatoria que implica su utilización, la que salvo acuerdo de partes quedará supeditada a una cuestión de prueba respecto de su suficiencia técnica y fiabilidad.

INFRAESTRUCTURA DE FIRMA DIGITAL EN ARGENTINA

La definición de Firma Digital que nos brinda el sitio Web de la Infraestructura de Firma Digital de la República Argentina (www.pki.gov.ar) es muy clara: La firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, posibilitando que éstos gocen de una característica que únicamente era propia de los documentos en papel. Una

firma digital es un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje. La firma digital no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma ológráficamente. La firma digital es un instrumento con características técnicas y normativas, lo que significa que existen procedimientos técnicos que permiten la creación y verificación de firmas digitales, y existen documentos normativos que respaldan el valor legal que dichas firmas poseen.

La firma digital debe ser susceptible de verificación por terceras partes (disponibilidad), tal que dicha verificación simultáneamente permita identificar al firmante (autoría) y detectar cualquier alteración del documento digital posterior a su firma (integridad)

Para la legislación argentina los términos "Firma Digital" y "Firma Electrónica" no poseen el mismo significado. La diferencia radica en el valor probatorio atribuido a cada uno de ellos, dado que en el caso de la "Firma Digital" existe una presunción "iuris tantum" en su favor; esto significa que si un documento firmado digitalmente es verificado correctamente, se presume salvo prueba en contrario que proviene del suscriptor del certificado asociado y que no fue modificado. Por el contrario, en el caso de la firma electrónica, de ser desconocida por su titular, corresponde a quien la invoca acreditar su validez.

La legislación argentina emplea el término "Firma Digital" en equivalencia al término "Firma Electrónica Avanzada" utilizado por la Comunidad Europea o "Firma Electrónica" utilizado en otros países como Brasil o Chile.

En nuestro país se denomina "Infraestructura de Firma Digital" al conjunto de leyes, normativa legal complementaria, obligaciones legales, hardware, software, bases de datos, redes, estándares tecnológicos y procedimientos de seguridad que permiten que distintas entidades (individuos u organizaciones) se identifiquen entre sí de manera segura al realizar transacciones en redes (por ej. Internet).

Realmente esta definición es conocida mundialmente con las siglas PKI, que significan “Public Key Infraestructura” o Infraestructura de Clave Pública.

Tenemos entonces que el comercio electrónico se articula en torno a un elemento objetivo (el certificado), a cuyo alrededor, a su vez se interrelacionan

tres elementos subjetivos: la autoridad de certificación, tercera parte de confianza de las otras dos partes (la firmante y la verificadora).

CERTIFICADOS DE CLAVE PÚBLICA O CERTIFICADO DE FIRMA DIGITAL - CONCEPTO

El sistema de certificados de clave pública supone la participación de los siguientes elementos personales: autoridad de certificación, el suscriptor o titular del certificado y el usuario o persona que confía en el certificado.

Los certificados de clave pública emitidos por autoridades de certificación son un elemento esencial para la aplicación de esta tecnología de forma segura.
Cuando una parte desea verificar la firma digital generada por la otra parte, la parte verificadora necesita una copia de la clave pública de la firmante y necesita tener la certeza de la correspondencia entre la clave pública e indirectamente su correspondiente clave privada.
La distribución fiable de las claves y el problema de la autenticación se resuelve mediante certificados de clave pública emitidos por una autoridad de certificación que actúa como tercero de confianza de la parte firmante y de la parte verificadora.

Un certificado es un documento electrónico que contiene información firmada digitalmente por alguna entidad en la cual confía una comunidad de usuarios.
En este tipo de certificados la clave pública se asocia de manera segura a una persona o entidad determinada puesto que se encuentra firmado digitalmente por una autoridad de certificación que ha confirmado la identidad u otros atributos del titular de la clave privada.
Son certificados “identificativos” ya que vinculan un nombre a una clave pública e indirectamente a una clave privada y por último a una firma digital.
“Uncitral” define el certificado como un archivo electrónico que indica que una clave pública junto con el nombre del suscriptor del certificado como el “sujeto” del certificado y confirma que el firmante potencial identificado firmas digitales ha señalado que la función básica de los certificados son: vincular una clave

pública con una persona determinada autenticando la titularidad de la clave pública y comprobar la identidad del firmante

Los certificados de clave pública que son documentos que contienen la clave pública de un tercero, que llevan la firma digital de una autoridad certificante, la cual es de confianza de la persona que necesita verificar la firma digital de un documento.

Las autoridades certificantes que son terceras partes de confianza, que dan fe de la veracidad de la información incluida en los certificados digitales que esa autoridad certificante emite.

El certificado de clave pública es un documento digital firmado digitalmente por una autoridad certificante que vincula la clave pública del suscriptor con sus datos de identidad. Por lo que la AC es una tercera parte confiable que da fe de la verificación de la información incluida en los certificados que emite.

En el sistema de firma digital intervienen cuatro actores principales, el emisor, el receptor, el certificador y la entidad auditante que controla el sistema de firma digital.

Se necesita dentro de la IFD RA una entidad que controle la gestión de las autoridades certificantes (por ejemplo que antes de emitir un certificado de clave pública el certificador realiza todos los procedimientos de verificación de identidad que correspondan o bien que los sistemas del certificador cuentan con la debida seguridad física y lógica.

AUTORIDAD DE CERTIFICACIÓN

La terminología es diversa. Así por ejemplo las ABA Guidelines hablan de autoridad emisora. El grupo de trabajo sobre comercio electrónico de la Uncitral, en su artículo 31, criticó el uso del término “autoridad” y propuso utilizar el de entidad, dejando a cada estado la decisión de someterlas o no a un régimen jurídico de autorización: con ello se quería evitar la posible consecuencia de que las funciones de certificación fueran realizadas necesariamente por autoridades públicas (Comisión de las Naciones Unidas para el Derecho Mercantil Internacional, Informe del grupo de trabajo sobre

comercio electrónico acerca de la labor 31, período de sesiones, Nueva Cork, 18 a 28 de febrero de 1997, A/CN.9/437, 12 de marzo de 1997,párrafo 90).

El reglamento italiano relativo a la formación, archivo y transmisión de documentos con instrumentos informáticos o telemáticos, por otra parte, habla de certificador, definido como el sujeto público o privado, que realiza la certificación, emite el certificado de clave pública, lo publica y actualiza el elenco de certificados suspendidos o revocados.

La Directiva de Comercio Electrónico habla de proveedor de servicios de certificación, definido como aquella entidad o persona física o jurídica que expide certificados o presta otros servicios en relación con la firma electrónica, asimismo, el Real Decreto español utiliza el término “prestador” de servicios de certificación”

La recomendación UIT-T.X509 (1993 S), Pág. 4, habla de autoridad de certificación, definida como aquella autoridad a la cual uno o más usuarios han confiado la creación y asignación de certificados; opcionalmente la autoridad de certificación puede crear las claves de los usuarios.

Cualquiera que sea la forma en que se la denomine, es una entidad dedicada a la emisión de certificados que contienen información sobre algún hecho o circunstancia del sujeto del certificado; en el caso de los certificados de clave pública, vinculan un par de claves con una persona determinada en forma segura, cubriendo la necesidad de servicios de terceras partes de confianza en el comercio electrónico de los tenedores de pares de claves asimétricas.

Cada certificado contiene una clave pública e información que identifica unívocamente al sujeto del certificado. El certificado está firmado digitalmente por la autoridad de certificación, usando la clave privada de firma de la misma.

Sea cual fuere la naturaleza de la autoridad de certificación debe revestir fuerza, seguridad y garantías a la actividad que realizan: la emisión de certificados.

La política de certificación o de actuación de una autoridad de certificación queda plasmada en las llamadas “prácticas de certificación” o “política de certificación”, se refiere básicamente a la política o prácticas que aplica a la emisión, distribución, suspensión, revocación y expiración de sus certificados.

Estas prácticas de certificación como declaraciones unilateralmente elaboradas por la autoridad de certificación son útiles para ayudar a los suscriptores y

terceros a determinar que autoridades de certificación proporcionan certificados más seguros.

Estas declaraciones se incorporan por remisión al certificado ya que un tercero usuario que utiliza un certificado para verificar una firma digital no tiene relación contractual alguna con la autoridad.

Todos los derechos y obligaciones que van surgiendo en las diversas fases del ciclo vital del certificado entre los diversos sujetos implicados se encuentran inmersos en la política o práctica de certificación.

Básicamente, son las obligaciones de la autoridad de certificación derivadas de la emisión de un certificado y contraídas frente a los suscriptores y terceros usuarios, y las obligaciones del suscriptor derivadas de la aceptación del certificado y contraídas frente a la autoridad de certificación y frente a terceros lo que incluye el régimen de responsabilidad de las partes.

JERARQUIA DE AUTORIDADES CERTIFICANTES

Vimos cómo un tercero de confianza da fe de que la clave pública pertenece a una cierta persona y vimos que esto se logra mediante un certificado de clave pública firmado digitalmente por una autoridad certificante

¿Cómo asegurarnos de que la información del certificado es válida y no ha sido alterada? Para esto utilizamos la clave pública de la Autoridad certificante que expidió este certificado a fin de verificar que la firma del certificado fue realizada efectivamente por la titular de dicha clave privada.

Ahora bien, ¿como asegurarme de que dicha clave pública que utilizo para verificar la firma del certificado del usuario es válida? Para asegurarnos de que es auténtica, la tenemos que poner dentro de otro certificado emitido por otra autoridad certificante que da fe de la autenticidad de la clave de la autoridad certificante que firma el certificado del usuario.

De esta manera se genera una cadena de certificación y distintas jerarquías de autoridades certificantes donde una autoridad certificante de mayor nivel certifica a otra de menor nivel, y así sucesivamente.

En algún momento no nos vamos a poder asegurar más de la autenticidad de la clave pública de la AC porque vamos a llegar a la cima de la jerarquía de AC. Llegamos en este punto a la Autoridad certificante raíz, la que no poseerá un certificado emitido por otra autoridad certificante sino un certificado autoemitido con su clave pública y autoafirmado con su clave privada.
La autoridad certificante raíz no necesita ser certificada porque representa al estado y el estado le ha dado dicha potestad sobre la base de su soberanía.

TITULAR DEL CERTIFICADO O SUSCRIPTOR

El sujeto del certificado o suscriptor es la persona o entidad incluida, que acepta el certificado y tiene legítimamente la clave privada correspondiente a la clave pública que contiene el certificado. La Directiva Europea de firma electrónica, al igual que el real decreto 14/1999 español, no establece el concepto de titular de un certificado sino de firmante o signatario como la persona que posee un dispositivo de creación de firma y que actúa en su propio nombre o en el de la entidad o persona física o jurídica a la que representa.

USUARIO DEL CERTIFICADO

El usuario de clave pública es la parte que confía en el certificado; es la persona que obtiene la clave pública del suscriptor a través de una copia del certificado que para ese suscriptor ha emitido una autoridad de certificación, de tal manera que actúa basándose en un certificado y la clave pública que contiene y vincula a su suscriptor.
A diferencia del suscriptor, que realiza un acuerdo con la autoridad de certificación, el tercero usuario tiene una relación no contractual, depende de la autoridad de certificación para su seguridad, ya que la verificación de la firma del mensaje electrónico que ha recibido la realizará basándose y confiando en el certificado emitido por la autoridad.

AUTENTICACIÓN ELECTRÓNICA (e-govermnent)

El vertiginoso avance de Internet y de la telefonía ha derivado en un uso masivo de la tecnología. Cada año aumenta exponencialmente la cantidad de transacciones que pueden realizarse en forma remota, ya sea por Internet o mediante el uso de teléfonos de línea o celulares, desde transferencias bancarias, hasta compras por catálogo, pasando por las compras en el supermercado, reserva de pasajes de avión, declaraciones de impuestos, o pagos de servicios, por citar sólo algunas operaciones que a diario se realizan.-

Tanto las empresas como los gobiernos han ampliado sus mercados mediante la incorporación de estas herramientas en su actividad cotidiana. Usan internet tanto para brindar información a la comunidad como para facilitar a los ciudadanos la realización de trámites, la adquisición de productos, pago de facturas, etc. El gobierno electrónico - e-government, es hoy una práctica concreta, que avanza en pos del objetivo de i-goverment, gobierno inteligente.-

Tanto los ciudadanos como las empresas se benefician cuando pueden acceder fácilmente a los servicios que presta el Estado por internet. Enviar declaraciones de impuestos sin tener que concurrir a las oficinas y hacer largas colas, notificarse de la resolución de un trámite desde el propio domicilio, son sólo algunos ejemplos de los beneficios para la comunidad. También, las empresas amplían sus ganancias al poder ofrecer sus productos por Internet, sin requerir mayores gastos de representación, disponen de una plataforma que los ubica en el mercado global. Internet facilita la difusión de los productos más allá de las fronteras, con sólo disponer de una página web y una plataforma transaccional adecuada.-

Para garantizar la seguridad de estas operaciones electrónicas, las organizaciones tanto públicas como privadas necesitan contar con procedimientos que identifiquen a los usuarios remotos. Este proceso de autenticación electrónica (*e-authentication*) puede ser implementado en forma segura mediante el uso de una gran variedad de técnicas disponibles que brindan un nivel de confianza sobre la identidad del usuario.-

El concepto de “Autenticación” se refiere a la verificación de la autenticidad de las identificaciones realizadas o solicitadas por una persona física o entidad, o sobre los datos tales como un mensaje u otros medios de transmisión electrónica.-

El proceso de autenticación es el segundo de dos etapas que comprenden:

- La presentación de una identificación ante el sistema de seguridad y
- La presentación o generación de información que corrobora la relación entre la entidad y el identificado.

La Guía de Autenticación Electrónica para Agencias Federales del Gobierno de Estados Unidos define a la Autenticación electrónica como “el proceso de establecer confianza en las identidades de los usuarios presentadas electrónicamente ante un sistema de información”. (NIST, Abril 2006) La autenticación electrónica presenta un desafío tecnológico cuando este proceso involucra la autenticación remota de personas individuales sobre una red informática.

Se entiende por Autenticación al proceso mediante el cual se establece un grado de confianza en una afirmación. El Grupo de Trabajo sobre Tecnologías de Seguridad del Nist define Autenticación como “las medidas de seguridad diseñadas para establecer la validez de una transmisión, mensaje o su originador, o un medio de verificar una autorización individual para recibir categorías específicas de información.”

ELEMENTOS: CONFIANZA. ENTORNOS. IDENTIFICACIÓN DE LAS PERSONAS Y TRATAMIENTO DE LA DOCUMENTACIÓN.

Para entender el desafío de la autenticación en línea, es necesario apreciar las fuentes de confianza en las cuales descansa el entorno comercial actual. La gente no realiza negocios con personas en la cuales no confía. Pero esta confianza comercial no es materia de fe, regulación o tecnología, sino que es el resultado de la administración de una relación.-

El marco de seguridad y confianza del nuevo entorno electrónico se compone de distintos aspectos presentes en una situación dada:

- Entorno jurídico seguro y adecuado: que existan leyes reconociendo el valor legal de las transacciones electrónicas. En la región los avances han sido importantes, en procura de reconocer la validez legal de las transacciones realizadas por medios electrónicos.
- Entorno tecnológico seguro y adecuado: que disponga de herramientas que garanticen la seguridad de la información, la confidencialidad de las comunicaciones, la conservación de los documentos electrónicos y la

transmisión integra de documentos digitales. Respecto de los sistemas, se requieren políticas de seguridad informática adecuadas, con manuales de procedimientos, asignación de responsabilidades, y con herramientas que permitan garantizar las condiciones de seguridad necesarias (firewalls, antivirus, dispositivos criptográficos para la identificación de las personas que administran los sistemas, identificación del sitio web mediante certificados digitales de servidor, sesiones seguras de internet, encriptadas para mantener la confidencialidad de la información que circula en dicha sesión, etc)

- Entorno administrativo seguro y adecuado: que permita definir con claridad los procedimientos de autenticación, los procedimientos de verificación de la idoneidad de los participantes, el proceso de la transacción en sí misma, por ejemplo, de una licitación electrónica, y las personas competentes para participar en él, así como también las responsabilidades asociadas al procedimiento.-

Se trata de encontrar cuáles mecanismos pueden utilizarse para hacer más ágiles los procesos de autenticación electrónica sin pérdida de seguridad.-

El proceso de autenticación en los procedimientos administrativos no se limita a verificar la identidad de la persona que inicia el trámite, ya sea en papel o en formato digital.-

Por el contrario, el proceso de autenticación considera múltiples aspectos, tales como el domicilio, la relación parental, los poderes otorgados, la situación impositiva y previsional, etc. La información disponible, si bien en general se encuentra en bases de datos públicas, es solicitada a los usuarios, quienes deben acompañar la documentación que se requiere para acreditar tanto los datos de identidad de la persona como las condiciones que lo habilitan para realizar el trámite. En el actual estado de avance de las administraciones publicas en la región, aún no hay experiencias de ventanilla única en la cual todos los organismos disponen de bases de datos interconectadas, con lo cual se permitiría verificar toda la información de manera automática, por ejemplo, la personería jurídica de una empresa simplemente consultando la base de datos de la dependencia pública que controla a las personas jurídicas.-

En ambos momentos el procedimiento vincula documentación en papel con la persona. En el primer caso, la identidad de la persona que va a interactuar con el sistema.

En el segundo caso, las capacidades de la persona física que interviene en el proceso, la representación que invoca y las capacidades de la persona jurídica a la cual representa.-

FACTORES DE AUTENTICACIÓN

Los mecanismos de autenticación electrónica remota que utilizan los sistemas de información tradicionalmente se describen de acuerdo con los factores de autenticación que usan.-

Los tres factores básicos de autenticación son:

1 Algo que sé (por ejemplo, una palabra clave o password).
2 Algo que tengo (por ejemplo, una credencial o un dispositivo criptográfico o token).
3 Algo que soy (por ejemplo, el reconocimiento de voz, del iris o de la huella digital, u otra medida biométrica).

Los sistemas de autenticación que contemplan los tres factores son los más fuertes en cuanto a seguridad, respecto de los que utilizan uno o dos de los factores descriptos. El sistema puede contemplar los tres factores para identificarse ante él, o bien, combinaciones entre factores para proteger un secreto que debe ser presentado para la verificación de la identidad. Por ejemplo, un sistema que utilice certificados de firma digital para presentar ofertas, puede contemplar el uso de dispositivos criptográficos para albergar la clave privada, a las cuales se puede acceder mediante una password. O bien los sistemas que contemplan el uso de biometría para activar la clave. Aunque este tipo de dispositivos contempla dos factores de autenticación, solamente prueban la posesión de la clave

Métodos de Autenticación según etapa de implementación del sistema
Los gobiernos implementan sistemas de e-gov en forma gradual. Los desarrollos se realizan alrededor de dos ejes:

-Sistemas de información y/o gestión internos – stand alone

-Sistemas de información y/o gestión abiertos – aplicaciones web

Los primeros, en general vinculados con los sistemas de administración financiera, son de acceso exclusivo para funcionarios públicos. Requieren de instalación en cada organismo, y constituyen los primeros avances en e-gov.-
Los segundos, accesibles por Internet en un único portal del gobierno, podrían a su vez clasificarse según las funcionalidades que ofrecen, en las siguientes categorías:
1 Portal de información estática: presencia en internet con información general sobre los organismos. Corresponde con una etapa inicial de difusión de las actividades del gobierno local por Internet.
2 Portal Relacional: portal que recibe información de organismos, la cual publica. Se corresponde con la segunda etapa de implementación de e-Gov, etapa de información, en la cual se construyen bases de datos como sistemas de información sobre distintos componentes de los procesos (en adquisiciones, por ejemplo, catálogo de bienes y servicios, información de oferentes y proveedores, convocatorias, documentos de licitación, etc). Permite el acceso a dicha información, y la carga, actualización y descarga de documentos e información, según el grado de desarrollo de la aplicación.-
El portal relacional a su vez puede ser:
1 Unidireccional: publica información de los procedimientos de compras (convocatorias, ordenes de compras, pliegos, etc) Esta información es suministrada y actualizada por los organismos.-
2 Bidireccional: publica información y documentos de los procedimientos. Permite realizar descargas por parte del público en general. Por ejemplo, publicación y descarga de pliegos por Internet. Inscripción en el Registro de Proveedores. Publicación y descarga de formularios por Internet.
3 Portal Transaccional: Permite realizar transacciones más complejas propias de los distintos procedimientos: presentar ofertas en formato digital, comunicaciones y notificaciones por medios electrónicos, emisión de órdenes de compra, solicitud de partidas, solicitud y adjudicación de vacantes, etc.

Los mecanismos de autenticación no son iguales para todas las etapas, sino que varía según la complejidad y riesgo de la operación específica. El acceso al portal en etapa de difusión con información estática es abierto, no requiere autenticación.

El acceso al portal en etapa relacional es abierto, requiriendo en algunos casos firma electrónica para acceder a las funcionalidades, tales como inscripción en el registro de proveedores.

El acceso al portal en etapa transaccional requiere autenticación basada en firma electrónica, en general, esto es, palabra clave y perfil de autorización.

Las cuestiones relativas a la autenticación fuerte, basada en PKI, surgen en esta etapa. Se observan distintos enfoques en sistemas en operación, y en los proyectos en curso de ejecución.

La idea de los gobiernos debería ser implementar una alternativa de autenticación seguro de tal forma que el trámite con el ciudadano sea totalmente electrónico, ágil, eficiente, seguro y amigable.

Finalmente, el carácter preceptivo del uso de tecnologías de la información y la comunicación debe establecerse con suma prudencia pues, de lo contrario, se genera cierta desconfianza por parte de los usuarios quienes, en definitiva, acaban asumiendo estas nuevas herramientas como una carga instaurada en beneficio de la propia Administración más que una ventaja para la mejor satisfacción de sus derechos y el cumplimiento más flexible de sus obligaciones. En este sentido, más que una estricta aplicación de las habilitaciones legales existentes, resulta más apropiado ofrecer ventajas a quienes las utilicen voluntariamente siempre que no se vulneren los límites del principio de igualdad, así como ofrecer sistemas de comunicación alternativos basados en la colaboración social de los agentes sociales implicados, tal y como se ha previsto en materia tributaria.

El decisivo reto de modernización de las Administraciones Públicas que permite asumir la implantación generalizada de las tecnologías de la información y la comunicación tanto en su actividad interna como en las relaciones con los ciudadanos debe asentarse en una sólida base jurídica. En efecto, no basta con disponer de costosos instrumentos técnicos que aporten una seguridad técnica razonable sino que, además, es necesario llevar a cabo una relevante tarea de adaptación del marco jurídico aplicable a la realidad sobre la que se

proyecta pues, de lo contrario, los ciudadanos perciben que no existe un nivel de protección de sus derechos e intereses equiparable al que proporcionan las relaciones presenciales.

ASPECTOS ESENCIALES A TENER EN CUENTA POR UN PROFESIONAL EN CIENCIAS ECONÓMICAS

Nuestra profesión tan ligada a la documentación en papel va a sufrir tremendos cambios culturales, cambios que de no ser comprendidos pueden ocasionar graves errores y serias responsabilidades.

Un factor que ayudará a no cometerlos es comprender que la seguridad en un documento digital no se encuentra en el medio que lo sostiene sino en el resultado de un procedimiento matemático abstracto, al igual que cuando se verifica el total en el transporte de un libro de contabilidad en el cual no se le da crédito a lo escrito sino al resultado de la suma de la columna.

En un archivo electrónico no hay papel como para poder ver si no esta raspado, si no hay interlineados, si no se agregaron hojas, por lo que podemos sostener que aquí no hay un medio.

Uno de los errores más frecuentes es llevar un documento digital a un medio, por ejemplo imprimirlo, para de esa manera estar seguro de lo que nuestros sentidos captan. Pero el documento digital para que no pierda sus propias características de seguridad no debe ser cambiado de soporte ya que entonces dejaría de ser digital para convertirse en el tradicional documento en papel, perdiendo de este modo sus condiciones de autenticidad, integridad y no repudio propias del documento digital firmado digitalmente.

El otro error gravísimo que se comete es el de confundir un canal seguro con un documento seguro.

Cuando vemos un candadito en una pagina web significa que estamos usando un protocolo de comunicaciones seguro (“https”). Ese protocolo implica un canal de comunicación seguro, como por ejemplo hablar por una línea de teléfonos que no pueda ser interceptada.

El procedimiento de seguridad consiste en encriptar los datos por el navegador de Internet y desencriptarlos con el software receptor de esa pagina web en el destino final, en el servidor.

Que el canal de comunicación sea totalmente seguro no implica que lo sea el documento transmitido por él, ya que podemos transmitir un archivo por un canal seguro y cuando llega entonces alterarlo.
La firma digital da seguridad al documento independientemente del medio por donde este viaje, ya que los datos transferidos son seguros por si mismos.
Estamos en los albores de una nueva cultura, somos quienes sufrirán los cambios y crearemos las bases para su uso racional y eficiente.

NUESTRA MISIÓN

Luego de todo lo expuesto se comprenderá que es muy grande nuestra responsabilidad. Basta solo con pensar en los cambios que esto produce en los procedimientos de auditoria, en los mecanismos para la celebración de contratos, la resolución de conflictos a distancia, las relaciones con el personal con recibos de sueldos digitales, las relaciones con las entidades financieras, con los cheques emitidos digitales, los balances digitales que ya hoy estamos utilizando sin que muchos se den cuenta de ello.
Todo esto no es difícil, pero sí nuevo. Allí radica su dificultad; adaptarse inteligentemente a los cambios y vencer el temor o rechazo que esto produce será la clave de nuestros éxitos laborales en el futuro.
Lo difícil es la respuesta humana, no la tecnológica.
Los autores del presente trabajo esperan que luego de la lectura de las líneas que anteceden hayan podido colocar una semilla para convertir a un posible desocupado del futuro en un verdadero artífice del destino que nuestros hijos se merecen.

BIBLIOGRAFÍA

Subsecretaría de la Gestión Pública http://pki.gov.ar

DIEGO MEDAGLIA, DMEDAGLIA@CIKATO.COM.UY, LICENCIADO EN ANALISIS DE SISTEMAS, Universidad ORT Uruguay, Facultad de Ingeniería

Valor legal de las transacciones digitales: firma digital, firma electrónica y documento electrónico por Por Pablo Fraga y Mercedes Rivolta.

Domingo Laborda, Director General de Modernización Administrativa

del Ministerio de Administraciones Públicas de España

AGIRREAZKUENAGA, Iñaki y CHINCHILLA, Carmen, 2001, "El uso de medios informáticos y telemáticos en el ámbito de las Administraciones Públicas", en *Revista Española de Derecho Administrativo*, núm. 109

BARNÉS VÁZQUEZ, Javier, 2000, "Una reflexión introductoria sobre el Derecho Administrativo y la Administración Pública de la Sociedad de la Información y del Conocimiento", en Administración de Andalucía. *Revista Andaluza de Administración Pública*, núm. 40

CRIADO GRANDE, Ignacio y RAMILO ARAUJO, María del Carmen, 2001, "e-Administración: ¿Un reto o una nueva moda? Problemas y perspectivas de futuro en torno a internet y las tecnologías de la información y la comunicación en las Administraciones públicas del siglo XXI", en *Revista Vasca de Administración Pública*, núm. (61)I

LINARES GIL, Maximino, 2003 "Modificaciones del régimen jurídico administrativo derivadas del empleo masivo de nuevas tecnologías. En particular el caso de la Agencia Estatal de Administración Tributaria", en la obra coordinada por R. MATEU DE ROS y M. LÓPEZ-MONÍS GALLEGO, Derecho de Internet, La Ley de Servicios de la Sociedad de la Información y de Comercio Electrónico, Cizur Menor: Aranzadi

PALOMAR OLMEDA, Alberto, 2003, "Un paso más en la aplicación de la tecnología en el procedimiento administrativo: hacia u procedimiento administrativo común de base tecnológica", en *Revista Aranzadi de Derecho y Nuevas Tecnologías*, núm. 3

SANZ LARRUGA, Francisco Javier, 2002, "Las bases jurídicas de la Administración electrónica en España: el uso de las técnicas informáticas, electrónicas y telemáticas en las Administraciones Públicas", en *Anuario da Facultade de Dereito da Universidade da Coruña*, núm. 6

2004, *El régimen jurídico de la e-Administración*, Granada: Comares

2001, "Los desafíos jurídicos de la Administración Pública electrónica: a propósito del Plan Info XXI", en la obra coordinada por M.A. DAVARA RODRÍGUEZ, *Quince años de encuentros sobre Informática y Derecho*, tomo II, Madrid: Universidad Pontificia de Comillas