2ª JORNADA NACIONAL DE DERECHO CONTABLE

COMISIÓN II – TECNOLOGÍAS INFORMÁTICAS Y SEGURIDAD JURÍDICA

Autor:

Dr. Guillermo A. Besana	Pedro I Rivera 4471 Of 2 CP 1430 - CABA	011-4522-9578	besana@arnet.com.ar gbesana@consejo.org.ar

PROCEDIMIENTO GENERAL PARA LA EMISIÓN, CONVERSIÓN Y CONSERVACIÓN DE LA DOCUMENTACIÓN RESPALDATORIA EN LOS SISTEMAS DE REGISTROS CONTABLES
- TECNICAS APLICABLES -

PONENCIA

Consideraciones tecnológicas y sociales, aclaraciones, y respuestas sobre los aspectos más comunes a tener en cuenta en el basamento tecnológico de un procedimiento de digitalización de documentación contable de respaldo en papel. A efectos de favorecer su redacción e interpretación se busco la forma de respuestas a preguntas y respuestas que van guiando al lector desde lo más elemental a lo más complejo.

CONTENIDO

DESARROLLO

Que es un Hash?

Son los algoritmos de verificación de integridad que consisten en una fórmula matemática que aplicada a una cadena de caracteres que permite relacionar el valor de cada caracter 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.

Que es Encriptación?

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

El procedimiento de encriptado seria el siguiente:

- Emisor y receptor se ponen de acuerdo en usar una clave.
- El emisor crea el mensaje a enviar, mediante un algoritmo que utiliza la clave acordada lo transforma en ilegible.
- 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.

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 caracter 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. Quiere decir 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 y que están vinculados entre si 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 cual es la clave privada.

El mecanismo de encriptación se llama de clave asimétrica y tiene como característica que un mensaje, una vez cifrado con la clave privada, no puede accederse 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 el mensaje puede ser accedido por cualquier persona que conozca la clave pública.

Entonces, encriptar es poner en clave un mensaje. Su autor puede desconocer su autoría, a menos utilice clave asimétrica. En este caso, el emisor no puede desconocer su mensaje, pues sólo quien conoce la clave privada pudo haberlo firmado. Sin embargo, no es confidencial.

Que 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.

- Un archivo con el mensaje original que puede estar encriptado o no.
- Un archivo con la clave pública del emisor (certificado digital).
- Un archivo con la firma digital que es el hash del archivo original ya encriptado con la clave privada.

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.

En Argentina la diferencia entre firma digital y electrónica esta establecida en la Ley de Firma Digital y esta relacionada con el ente que otorga el certificado digital

Si lo otorga un ente licenciado el procedimiento se llama "Firma Digital" en caso contrario se la denomina "Firma Electrónica".

Que es tecnología PKI?

Se dice que se utiliza tecnología PKI (Public Key Infrastructure) cuando la clave pública del emisor es firmada digitalmente por una persona llamada Entidad de Certificación, la cual es merecedora de confianza por parte de la comunidad y que da fe de que el emisor es la persona física que dice ser, pues se aseguró que es el titular que accede a la clave privada que la vincula.

Que es un certificado digital?

Son los archivos que contienen en su interior:

- La claves públicas del emisor
- La firma digital de la clave pública por la entidad de certificación
- La clave pública de la entidad de certificación.
- La entidad de certificación también puede estar avalada por una entidad de nivel superior por lo que esta cadena de certificaciones puede ser tan larga como certificadores intervengan en el proceso.

  En algunos casos la clave privada del emisor puede estar incluida en el certificado digital, pero ese archivo no viaja con el mensaje, sino que es creado al sólo efecto de ser transportado por el emisor desde un computador a otro o ser instalado en algún dispositivo criptográfico."

Que son los símbolos para reconocimiento automático de datos?

Si bien existen programas de reconocimiento óptico de caracteres mas conocidos por la sigla OCR en ingles que permiten interpretar la escritura, incluso la manual tradicional, desde un medio no digitalizado por ejemplo el papel, el nivel de errores aun es muy alto y esos programas utilizan un alto nivel de procesamiento lo que los hace, en cierta medida, lentos. Los procedimientos mas rápidos y eficientes consisten en insertar en el soporte físico símbolos que puedan ser interpretados por la computadora en forma directa y para ello se recurrió a varios sistemas.

Se insertaron cintas magnéticas que contenían los datos en formato digital (tarjetas de crédito)

También se utilizaron tintas magnéticas con oxido de hierro, se impregnaba el papel y permitían la lectura de los caracteres por medio de lectores magnéticos mientras que los caracteres eran similares a los caracteres alfanuméricos que usamos los humanos. (Chequeras)
La posibilidad de poder interpretar con el sentido de la vista parecería ser una ventaja aunque tal vez no sea así, ya que si no tenemos el control del proceso de grabado podríamos ser fácilmente engañados ya que tendríamos ante nuestros ojos un carácter reconocible pero los datos magnéticos podrían estar diciendo otra cosa.
Los símbolos que hoy todos conocemos como códigos de barras fueron una opción bien económica a la lectura rápida de datos, pero su estructura es lineal y la cantidad de datos que puede representar es limitada, es muy eficiente para procesos en donde se requiere el ingreso de una pequeña cantidad de dígitos como por ejemplo para identificar un producto o algunos pocos datos contenidos en una factura, pero no para un textos mas extensos.
Los lectores de códigos de barras conocidos con el nombre de scanners permiten interpretar cada uno de los caracteres del código de barras y los ingresan a la computadora como si fueran tecleados muy rápidamente desde el teclado.
Como alternativa al código de barras surgen también las etiquetas RFID que permiten hacer lo mismo pero en lugar de caracteres ópticos emiten señales de radiofrecuencia y el lector es un receptor de radio que rápidamente las recibe e ingresa los datos este sistema gana en rapidez pero también está limitado a un número reducido de caracteres.
Como alternativa grafica al ingreso de una considerable cantidad de datos aparecen los códigos de barras de dos dimensiones o códigos de manchas el mas conocido es el PDF 417 cuya estructura permite grabar datos en fila y columnas incluyendo caracteres de control que validan la información ingresada. Tienen la particularidad de ser muy económico pues utiliza tintas comunes y poder guardar datos en un espacio reducido aunque nunca comparable con lo que puede alojar por ejemplo un DVD, además gracias a la utilización de los caracteres de control, permiten ser leídos hasta con hasta un 40% de superficie destruida.
Esta breve descripción de los medios de ingreso nos permite conocer las posibilidades que hoy nos brinda la tecnología, pero su evolución es tan rápida que tal vez ya estén en desarrollo alternativas que hagan obsoletos estos medios.
Lo que me gustaría dejar bien en claro en esta ponencia es que ante el análisis de la utilización de estos medios debemos tener en cuenta nuestro objetivo para su inclusión y como lo vamos a controlar.
Por ejemplo en los códigos de barras siempre podemos distinguir en caracteres alfanuméricos tradicionales el numero del artículo que representa, pero al igual que los caracteres magnéticos podemos percibir con la vista una cosa y la computadora leer otra además también requeriríamos de mayor información, como por ejemplo un listado de productos para saber si ese código esta adherido al verdadero producto que identifica. El consumidor nunca va a confiar en el numero impreso debajo en el código pues no tiene el control del proceso de grabación y no sabe que dato interpretara la maquina, de la misma manera la cajera de un supermercado no podrá confiar en los datos leídos por el scanner porque no sabe si el consumidor cambio la etiqueta por una de menor precio. Esos controles se hacen **después** de que la computadora lee el código y lo representa en una pantalla o lo imprime bajo nuestro control.
Como consecuencia de estar acostumbrados a una cultura basada en representar en medios materiales lo que queremos comunicar, tratamos de llevar a papel la información digitalizada y eso genera peligrosas confusiones.
Por ejemplo, es muy común que cuando vean un PDF 417 tengamos el texto en caracteres tradicionales y el código de manchas en la misma hoja de papel. Si nosotros firmamos ese papel con nuestra firma hológrafa dando conformidad a que se la damos realmente, a los datos alfanuméricos?, al código de manchas?, o a ambos.
Tiene sentido que estén juntos? No sería lo mismo tener un papel con los textos alfanuméricos y un diskette o cd o DVD o pendrive o una dirección de internet donde poder verificar esos datos?
La respuesta a estas preguntas está dada por el objetivo práctico de lo que queremos sistematizar.
Cuando firmamos una hoja de papel validamos la información que nuestros sentidos de la vista y el tacto perciben, si firmamos digitalmente un documento digital validamos la integridad de los datos contenidos

en ese archivo con un procedimiento matemático mucho más completo y preciso pero que nuestros sentidos no pueden percibir pues es abstracto.

Cuando se cambia de medio entonces las características de control se pierden.

El PDF 417 tiene dos vías diferentes de validación aunque estén en la misma hoja de papel.

Es fácil comprender que al escanear un contrato con firma hológrafa esa firma no valida el archivo resultante del proceso de escaneo, para el caso de la firma digital el criterio es idéntico, la firma digital no valida el documento impreso, aunque tal vez tengamos la tendencia muy fuerte a confiar en la impresión cuando llevamos a papel un documento electrónico firmado digitalmente, sin reparar que nuestro sentido de la vista y el tacto no nos permiten verificar una firma digital, necesariamente debemos utilizar una computadora para ello.

Siempre constituyen dos elementos separados el texto del contenido y el código de manchas con su firma digital.

El código de manchas siempre requerirá tener a disposición un scanner de características especiales para poder leerlo y validarlo, aparato este no tan difundido y que requerirá un seguimiento constante sobre su fabricación y obsolescencia.

La inclusión de un código de manchas no es un elemento que por su sola inclusión asegure la inalterabilidad del medio y su contenido como podrían ser los caracteres de control que tiene un billete de papel moneda.

Hay documentos electrónicos hoy vigentes en Argentina?

Los primeros documentos electrónicos de uso masivo, entendiéndose por tales a los archivos que generan relaciones de carácter legal entre las partes, aparecen cuando AFIP lanza sus aplicativos para la confección de las Declaraciones Juradas impositivas. Esos aplicativos generaban un archivo que generaba un código de manchas.

El procedimiento de firma fue originalmente hológrafa en el papel que contenía el código de manchas, es de destacar que el contribuyente no sabía que estaba informando en ese código de manchas.

Luego con la aparición del SIAP los aplicativos generan un archivo de texto que es encriptado y en su momento eran grabado en un diskette y presentado en el banco para su información y/o pago y hoy es presentado vía internet.

Originalmente se firmaba en forma hológrafa una declaración jurada en papel y se transmitía el documento digital con contenido desconocido por el contribuyente referenciado en el documento en papel con un código de control o hash formulado por AFIP.

Hoy se transmite por internet el archivo encriptado y se utiliza un sistema de clave fiscal que obliga al contribuyente a declarar bajo juramento que ingreso datos correctos en los aplicativos de AFIP y que utilizó los aplicativos de AFIP para generar el documento que transmite.

No utiliza firma digital.

Un segundo paso lo marco en el año 2002 la RG 1361 que establece dos tipos de documentos digitales, en su Titulo I redacta las características que deben contener los duplicados de las facturas de ventas con la opción de poder archivarlos en forma electrónica y poder prescindir o no generar documentación en papel y en su Titulo II lo que conocemos como registro de libro de IVA

Los originales de las facturas debían seguir haciéndose en papel hasta que en el año 2008 aparece la RG 2485 que permite y luego obliga a la generación de las facturas electrónicas originales.

En la transferencia de las facturas por el sistema de web servicie se utiliza tecnología PKI pero los certificados no validan a una persona sino a una computadora que interactúa con los servidores de AFIP.

No se utiliza firma digital.

Las facturas electrónicas con la sola implementación de las especificaciones de AFIP son un documento tributario que no tiene asegurada su integridad, en especial en lo referido al detalle de lo facturado. Para lograrlo es necesario calcular su hash o mejor aun, firmarlo electrónicamente o digitalmente cuando sea posible.

Si bien las criticas expuestas en forma tacita o explicita pueden resultar muy duras, las mismas surge a la luz como consecuencia de los avances tecnológicos y de la necesidad de actualización permanente a la que estamos obligados. En el momento en que las normas fueron sancionadas fueron normas de

vanguardia, creando modelos adoptados por otros países y sus responsables fueron y son reconocidos y premiados por diferentes y prestigiosas organizaciones.
Otro gran grupo de documentos digitales y que se utilizan desde hace varios años son las transferencias bancarias, a través de ellas pasan de dueño millones de pesos diarios utilizando tecnología PKI.
El sistema es implementado y está bajo el control del sistema financiero mientras que emisor y receptor puede que ni siquiera lo noten. Los sistemas generan certificados digitales que validan la integridad del proceso, y pueden permitir o no validar a la persona que efectúa la transferencia, quiere decir que pueden operar con clave simétrica o asimétrica siempre bajo la responsabilidad y riesgo del operador. En general el documento digital que genera la transferencia y su firma electrónica constituyen respaldo en las operaciones de las instituciones financieras que las realizan pero no de los titulares intervinientes. Para ellas estas operaciones son asientos contables millonarios que tienen tanto respaldo como las notas de débito y crédito que se realizan en cuenta, a lo sumo el extracto bancario.
Otro gran grupo de documentos digitales pero que no es respaldo de documentación contable de entes privados es la presentación de Balances a la IGJ porteña.
El aplicativo utiliza tecnología PKI con un certificado digital embebido en el mismo programa el cual no valida al firmante sino al software utilizado para la generación del documento digital. Es mucho mas actualizado que los aplicativos de AFIP y tal vez lo más cercano a la utilización de firma digital en forma masiva.

Como se verifica una firma digital?
La respuesta a esta pregunta es tal vez el aporte mas importante que los profesionales debemos dar a la comunidad.
El procedimiento es mediante la ejecución de un software que tiene que ser de carácter público en el sentido que tiene que ser de acceso libre a cualquier persona y permitir verificar cualquier firma digital.
El procedimiento es sencillo hay que ingresar dos datos:
el archivo a verificar por un lado y su firma por el otro si tenemos la firma digital por separado o uno solo si los archivos están unidos.
Tomara los datos contenidos en el certificado digital y validara la clave publica del firmante en función de la firma digital de la entidad de certificación.
Luego con esa clave publica desencriptará los datos para obtener el hash del archivo.
Luego calculara el hash del archivo y lo comparara con el hash desencriptado en el punto anterior
Si los datos son idénticos entonces la firma es válida.
El procedimiento es sumamente complejo pero es aplicable para la validación de cualquier firma.
Con la simple validación de diferentes podemos confiar en el, un soft que solo valide las firmas efectuadas con un determinado certificado no es confiable.

Que es Digitalización Certificada?
Es el procedimiento por el cual le damos valor a un documento digital.
En el mundo del papel si nosotros tenemos un documento que obliga a una persona a pagar $100 y sacamos una fotocopia, esa fotocopia tendrá un valor legal casi nulo, sin embargo si en el proceso interviene un profesional que pueda dar fe se le puede adosar a ese documento una certificación
El profesional interviniente obviamente no puede certificar que el firmante sea quien realmente ha suscripto el documento.
Pero su intervención si permitiría en probar que el documento original existió y que la fotocopia representa su copia fiel dando además una fecha cierta a la copia.
En la práctica si se lleva al profesional un lote de 1000 comprobantes para certificar seguramente designara a un empleado de su confianza para que realice las fotocopias que luego el certificara. Nunca certificará fotocopias ya impresas.
El procedimiento tiene algunas particularidades, imaginemos el tiempo y los costos que puede demandar el proceso agregando que en general no queda ninguna constancia sobre la intervención del empleado, la fotocopia puede sufrir alteraciones con el transcurso del tiempo y también la fotocopia puede ser alterada

o reemplazada intencionalmente sin que el profesional pueda notarlo ya que descansara en la confianza hacia su dependiente.
Si en lugar de generar una copia en papel se genera un archivo digital estamos hablando de digitalización, si además agregamos firma digital a la copia estamos hablando de digitalización certificada. Las ventajas del procedimiento además de la rapidez y el bajo costo permitiría asegurar la inalterabilidad del documento durante todo el proceso ya que es posible técnicamente generar u procedimiento por el cual solo haya intervención humana para colocar el documento original en el scanner quedando constancias de las personas intervinientes mediante su firma digital y también puede contener la co-firma de un profesional actuante y los momentos en que dicho proceso fue realizado.
Con respecto a las incumbencias profesionales tendríamos que analizar en qué momento se realiza el proceso de copia y certificación, si es antes de su registración contable debería ser un escribano quien de fe del original digitalizado, si es después de su registración un Contador Público podría avalar que ese documento digital se corresponde con un registro contable.
Esta tecnología permite la creación de un sistema que, a diferencia de una fotocopia, genera un documento digital inalterable pues es firmado digitalmente en el momento de su generación, para conocer hasta donde llega la responsabilidad del firmante será necesario el análisis de la política de certificación de la entidad emisora del certificado. Aquí no intervienen profesionales salvo para validar la integridad del sistema y verificar si se cumplen las condiciones pre establecidas para su utilización efectiva y confiable.
Este procedimiento ya está vigente en algunos países como por ejemplo en España para los comprobantes tributarios con gran éxito desde Noviembre de 2007 permitiendo eliminar definitivamente el respaldo en papel sin requerir intervención profesional.
El sistema debe asegurar la legibilidad de la digitalización obtenida y ello se consigue fijando un mínimo de pixeles o puntos por superficie. Se considera que un mínimo de 200 puntos por pulgada cuadrada aseguran una correcta interpretación de un original.
También es condición necesaria la utilización de estándares de uso público, para permitir que los archivos puedan ser leídos en el futuro sin necesidad de autorizaciones o software específicos que podrían inhabilitarse en el futuro. Es de notar que en ningún momento se pone atención en el medio en el cual se almacenara el documento, ya que ese proceso es independiente del lugar físico en donde ese archivo este residiendo, pero si debe asegurarse su acceso en cualquier momento sin restricciones ni obsolescencias.