IX Jornada Nacional de Derecho Contable. Consejo Profesional de Códoba, Córdoba, 2016.

Análisis de las implicancias legales en el uso de Firma Digital, Firma Electrónica o Función de Hash en contratos y documentos comerciales.

Diego Sebastian Escobar.

Cita:

Diego Sebastian Escobar (2016). *Análisis de las implicancias legales en el uso de Firma Digital, Firma Electrónica o Función de Hash en contratos y documentos comerciales. IX Jornada Nacional de Derecho Contable. Consejo Profesional de Códoba, Córdoba.*

Dirección estable: https://www.aacademica.org/escobards/27

ARK: https://n2t.net/ark:/13683/ptuD/zFb

Esta obra está bajo una licencia de Creative Commons.
Para ver una copia de esta licencia, visite
https://creativecommons.org/licenses/by-nc-nd/4.0/deed.es.

Acta Académica es un proyecto académico sin fines de lucro enmarcado en la iniciativa de acceso abierto*. Acta Académica fue creado para facilitar a investigadores de todo el mundo el compartir su producción académica. Para crear un perfil gratuitamente o acceder a otros trabajos visite: https://www.aacademica.org*.

IX Jornada Nacional de Derecho Contable

11 y 12 de agosto de 2016

Ciudad de Córdoba

Presentación de Ponencias

Tema de referencia:

IV Registros Pericias

Título:

Análisis de las implicancias legales en el uso de Firma Digital, Firma Electrónica o Función de Hash en contratos y documentos comerciales.

Diego Sebastián Escobar

Contador Público (UBA)

Licenciado en Administración (UBA)

Especialista en Seguridad Informática (UBA)

Maestrando en Seguridad Informática (UBA)

Análisis de las implicancias legales en el uso de Firma Digital, Firma Electrónica o Función de Hash en contratos y documentos comerciales.

Resumen

Debido a los innumerables cambios en el procesamiento, tratamiento y resguardo de la información producto del avance de las nuevas tecnologías, han surgido herramientas y estándares que pueden ser aplicados en los sistemas de registros contables.

Acompañando la innovación tecnológica, han surgido normas legales reglamentando y formalizando herramientas para su uso y administración en los ámbitos públicos y privados de la Nación.

En el marco de la IX Jornada Nacional de Derecho Contable, el autor propone someter al análisis de todos los asistentes las implicancias en el uso de las herramientas: Hash, Firma Digital o Firma electrónica, en el tratamiento de documentación contable y contratos.

El presente trabajo tiene por objetivo analizar las principales características y las implicancias legales que posee la utilización de las citadas herramientas digitales en el ámbito de la República Argentina.

Palabras Clave: Hash, Firma Digital, Firma Electrónica, Documentación Contable.

Índice temático

Análisis de las implicancias legales en el uso de la Firma Digital, Firma Electrónica o Hash en contratos y documentos comerciales.

1. Introducción

Debido a los innumerables cambios en el procesamiento, tratamiento y resguardo de la información producto del avance de las nuevas tecnologías, han surgido herramientas y estándares que pueden ser aplicados en los sistemas de registros contables.

Acompañando la innovación tecnológica, han surgido normas legales reglamentando y formalizando herramientas para su uso y administración en los ámbitos públicos y privados de la Nación.

En el marco de la IX Jornada Nacional de Derecho Contable, el autor propone someter al análisis de todos los asistentes las implicancias en el uso de las herramientas: Hash, Firma Digital o Firma electrónica, en el tratamiento de documentación contable y contratos.

El presente trabajo tiene la intención de difundir los siguientes objetivos:

- Definir el marco legal de la firma digital y electrónica en la República Argentina.
- Analizar el uso de la función de Hash.
- Definir los conocimientos fundamentales de ambos conceptos y establecer las principales diferencias.
- Analizar la seguridad brindada de estas herramientas en el uso de documentación digital empresarial.

2. Características de la Firma Digital, Electrónica y función de Hash

2.1. Firma electrónica y digital

Existe mucha controversia con la definición de firma digital. En el imaginario colectivo, se asocia este concepto con el escaneo o imagen de una firma manuscrita y su utilización en documentos digitales; pero no corresponde con las herramientas utilizadas en la actualidad.

Tecnológicamente la firma digital es definida como un conjunto de datos asociados a un "*mensaje digital e incorporados a éste por un programa de computación desarrollado al efecto, que permite garantizar la identidad del firmante y la integridad del documento firmado."*[1]

Resulta importante destacar, que la misma equivale a la firma manuscrita, pero no es una copia de la misma. Este concepto es definido por la ley de Firma Digital ya que establece lo siguiente:

" *No es la imagen escaneada de la firma manuscrita.*

 Equivalente a la firma manuscrita.

 Es la encriptación (criptografía) de un documento con la llave privada del hash (huella).

 Existe una diferente para cada documento."

2.2. Función de Hash

La definición teórica de una función de hash es un cálculo matemático en donde se obtiene como resultado un código. Siempre y cuando en ese documento electrónico no se haya modificado ningún carácter, el cálculo del hash arrojará el mismo código resultante.

---

[1] Natalino, Fernando, (2015), Firma Digital, Accedido desde http://www.cs.uns.edu.ar/~prf/teaching/APS11/downloads/Trabajos%20Legislacion/Firma%20Electronica.pdf

Con esta herramienta, podemos garantizar la integridad del documento o archivo que estoy analizando.

3. La utilización de las herramientas de la función de Hash, Firma Digital o Electrónica.

Existe mucha controversia con la utilización de cualquiera de las tres herramientas presentadas en la gestión documental de archivos digitales. Algunos consideran que el uso de un Hash es necesario y suficiente para firmar contratos en formato digital; pero si bien el cálculo de un Hash garantiza la integridad de la información, pero no podemos garantizar la autoría del mismo, por lo tanto, no permite reconocer quienes han firmado el acuerdo, volviéndolo repudiable entre las partes.

Independientemente de lo establecido en la unificación de Códigos Civil y Comercial de la Nación, la Ley N° 25.506, plantea la diferencia entre la firma digital y electrónica, y establece el principio de "No repudio" para un contrato firmado con firma digital. En la siguiente sección se analiza el valor probatorio del mismo.

3.1. Valor Probatorio de un documento firmado digitalmente

En el artículo N° 2 de la Ley N° 25.506, se define a la firma digital como "*el resultado de aplicar a un documento digital un procedimiento matemático que requiere información de exclusivo conocimiento del firmante, encontrándose ésta bajo su absoluto control*."[2] Asimismo, indica que la misma debe ser susceptible de verificación por terceras partes, tal que dicha verificación simultáneamente permita identificar al firmante y detectar cualquier alteración del documento digital posterior a su firma.

Pero la denominación utilizada equivalente al término "Firma Electrónica Avanzada" que se utiliza en la Unión Europea, o "Firma Electrónica" empleado en otros países como Brasil o Chile. Por lo tanto hay que diferenciar con el término de "Firma Electrónica" ya que su significado no es el mismo.

[2] Ley de Firma Digital N° 25.506, Artículo N° 2, Honorable Congreso de la Nación Argentina.

La firma electrónica es definida en la ley como "*al 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*."[3]

Por lo tanto, régimen vigente los términos "Firma Digital" y "Firma Electrónica" al no poseer el mismo significado, no poseen el mismo valor probatorio. En el caso de un documento firmado digitalmente existe una presunción "iuris tantum" en su favor; "*esto significa que si un documento firmado digitalmente es automáticamente verificado como correcta y se presume salvo prueba en contrario por parte del demandante que proviene del suscriptor del certificado asociado y que no fue modificado.*"[4] Por lo tanto, ese documento adquiere características de documento público, a pesar de ser privado.

En el caso de un documento firmado electrónicamente, se invierte la carga probatoria; o sea que en caso de ser desconocida la firma, corresponde a quien invoca su autenticidad acreditar su validez.

Por ejemplo, si entre dos partes que celebran un contrato firmado digitalmente (no electrónicamente) y una de ellas alegase la invalidez de alguna de las dos firmas, le corresponde a ésta demostrar ante la ley la invalidez de la misma.

Si en lugar de ello, "*las partes firmasen el contrato con firma electrónica, ante el mero alegato de una de ellas sobre la invalidez de alguna de las firmas, corresponde a la parte que clama por su validez demostrar ante la ley la autenticidad de la misma.*" En caso de no tener la capacidad de demostrarlo, para la ley argentina esa firma electrónica no es válida.

Por otra parte, para reconocer que un documento ha sido firmado digitalmente se requiere un certificado digital del firmante que haya sido emitido por un certificador licenciado en el

---

[3] Ley de Firma Digital N° 25.506, Artículo N° 5, Honorable Congreso de la Nación Argentina.
[4] Por José Luis González. (2012). Firma Digital en la República Argentina, Publicación electrónica-Dirección de Informática del Ministerio de Economía. Accedida desde www.dime.gov.ar

marco de la Ley de Firma Digital (o sea que cuente con la aprobación del Ente Licenciante).

Es por esto que, si bien entendemos que en los ambientes técnicos se emplea habitualmente el término Firma Digital para hacer referencia al instrumento tecnológico, independientemente de su relevancia jurídica, es conveniente que todos los proveedores de servicios de certificación, divulgadores de tecnología, consultores, etc. que empleen la denominación correcta según sea el caso, a fin de no generar confusión respecto a las características de la firma en cuestión.

Seguridad de un documento firmado digitalmente

La Ley N° 25.506 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 informáticas.

Como se ha mencionado anteriormente, la estructura nivel internacional conocida es conocida cono *Public Key Infraestructure*[5] o las siglas PKI, para emitir y administrar los certificados digitales.

Muchas personas consideran desde el desconocimiento que la utilización de la Firma Digital para documentos, es insegura, vulnerable y riesgosa en su utilización. Pero indiscutibles científicos han demostrado la utilización de la firma digital tomado los recaudos de implementación adecuados resulta prácticamente inquebrable.

Al utilizar encriptación asimétrica para firmar digitalmente, una clave pública y otra privada (secreta), existen experimentos que con el conocimiento de una, deducir la otra es computacionalmente irrealizable, "*aun disponiendo de recursos extremos se presume que se requieren 30.000.000 de años de una computadora que opere a razón de (1MFlop =*

[5] Traducción: Infraestructura de Clave Pública.

1.000.000 de multiplicaciones y divisiones por segundo con números de 309 dígitos decimales) para deducir una sola clave privada RSA 1024-bits a partir de la pública, usando el algoritmo más eficiente conocido."[6]

A modo de ejemplo, en el siguiente cuadro se presentan la extensión de las claves utilizadas en este tipo de tecnología:

Ejemplo Clave Pública – Privada de un Certificado Digital
*** * CLAVE PRIVADA 2048 ** ***   **c:**   **82342721541517954099666074805716550776922051657926121901018270059717241767089468844828384959328640438745141742243987353763275273392835038328296133142873165239265704459136145078709636812680613394839653603216283933495761074915656012792759079334935105916117193099131855197781713404632150746937864066148 1**   **n:**   **82223242875921704475559193702869501278469798044602758231702468294574820334975613947661417172981299830405899629126493932925984621766296883222575348746329932959391084160830697038884796428328295467675928311974971201456274324631386769979787396877157698632033308851385814013369770788584877346667268323607665353712917014476610762907214735713298823344405183658483284902324053031377343454153628963105260968030088061476657167082531611977118907751867547309709010452453203299881762041695007155887814097072539204465776551613909291412159815564724271793419540334984022996276649765104102675450881316875043613609478499666131831695926 87**   *** * * CLAVE PUBLICA 2048 * * ***   **d:**   **12167430486751325478840018935696667364447799156361730169410293702662007333616872344434546064797275042964489677015814181178516588814413853994586692695716061264601377293606033603651889273891211980722089257399359150778518889290755981155174863593597695919064653933185479321364359359314588260874244163406268325456077887843693325528748357334446825249627487325012603130228646483011482923013144445983142948605363194497334801899114909785069317908876480058872818980447526492535777807452089378487604081815032588860844998564380274510522479522627359321037164964331105313649887744129291221620677531920227815008568681496206593415216 41**
Fuente: Hugo Scolnik – Universidad de Buenos Aires

[6] Hugo Scolnik, (2010) Criptografía Asimétrica. Maestría en Seguridad Informática, UBA.

La robustez de esta tecnología es lo que le permite garantizar la integridad de los documentos firmados y la confiabilidad recibida con otro status jurídico y tecnológico que la utilización de una simple función de hash.

4. Conclusiones

Como se indicó en la introducción, el presente trabajo tiene por objetivo analizar las principales características y las implicancias legales que posee la utilización de las citadas herramientas digitales en el ámbito de la República Argentina.

Teniendo en cuenta las características de la función de hash, la firma digital y electrónica en el uso privado, se puede observar que la legislación en la República Argentina, utiliza el término de "firma digital" de la misma forma en que se emplea la "firma electrónica avanzada", diferenciándola claramente de la "firma electrónica" y una simple "función de Hash".

Actualmente la firma electrónica y digital se emplean indistintamente en ámbitos organizacionales pero no poseen el mismo valor probatorio en un litigio. En el caso de la firma digital, existe una presunción "**iuris tantum**" en su favor; esto significa que si un documento firmado digitalmente es automáticamente verificado como correcta se "presume salvo prueba en contrario por parte del demandante que proviene del suscriptor del certificado asociado y que no fue modificado."

Por lo tanto, la firma digital adquiere las características de un "documento público", al contrario de la utilización de una función de hash o la firma electrónica, ya que en un litigio se invierte la carga probatoria.

Por todo lo expuesto, la firma digital se convierte en la herramienta más recomendable para ser utilizada en la gestión de múltiples documentos e instrumentos electrónicos, como por ejemplo, la firma de recibos de sueldos, contratos, papeles de trabajo, mails, facturas, hasta dictámenes de auditores si los consejos profesionales tuvieran la capacidad de ser autoridades certificantes homologadas.

Por último, el autor del presente trabajo destaca la necesidad de difundir estas herramientas con eminente seguridad ante diferentes profesiones para poder elevar el valor probatorio de los instrumentos e incrementar la eficiencia de los procesos administrativos.

5. Bibliografía

Congreso de la Nación Argentina. Ley de Firma Digital N° 25.506, Artículo N° 2.

Congreso de la Nación Argentina. Ley de Firma Digital N° 25.506, Artículo N° 5.

Fernando Natalino, (2010), Firma Digital, Accedido desde http://www.cs.uns.edu.ar/~prf/teaching/PS11/downloads/Trabajos%20Legislacion/Firma%20Electronica.pdf

José Luis González. (2012). Firma Digital en la República Argentina, Publicación electrónica- Dirección de Informática del Ministerio de Economía. Accedida desde www.dime.gov.ar

Hugo Scolnik, (2010) Criptografía Asimétrica. Maestría en Seguridad Informática, UBA.

Poder Ejecutivo Nacional, Decreto 512/2009, JEFATURA DE GABINETE DE MINISTROS, "Créase el Grupo de Trabajo Multisectorial, que tendrá por finalidad concertar e impulsar la "Estrategia de Agenda Digital de la República Argentina".

Poder Ejecutivo Nacional, Decreto N° 2628/2002 PODER EJECUTIVO NACIONAL (P.E.N.) FIRMA DIGITAL LEY N° 25506 – REGLAMENTACION.

Poder Ejecutivo Nacional, Decreto N° 283/2003 PODER EJECUTIVO NACIONAL (P.E.N.) FIRMA DIGITAL EMISION DE CERTIFICADOS DIGITALES.

Poder Ejecutivo Nacional, Decreto N° 1028/2003 PODER EJECUTIVO NACIONAL (P.E.N.) ENTE ADMINISTRADOR FIRMA DIGITAL-DISOLUCION.