INFORME

Llega la firma digital, (pero se toma su tiempo)

Durante siglos, la rúbrica manual ha sido sinónimo de seguridad en la autoría de documentos y compromisos. Pero a pesar de la sencillez del procedimiento, su aceptación se enfrenta con dudas. En la Argentina, algunas empresas y organismos ya la usan.

Por Pablo Raimondi
praimondi@e-mi.com.ar

Los métodos fraudulentos para engañar a la tecnología avanzan día a día. Virus, programas spyware, software para desencriptar claves o el acceso a sitios supuestamente seguros, acechan el terreno de los bits.

Ante esta vulnerabilidad, el usuario se enfrenta a los temores cada vez que realiza el último click. Es que en cualquier transacción o trámite puede perder dinero, ser víctima de robo de datos confiden-ciales, desperdiciar oportunidades de negocios o arriesgarse a la pérdida de confianza por parte de los clientes, quizás la peor cualidad en materia e-business.

Los documentos firmados sobre papel son seguros ya que la tinta es difícil de borrar y la rúbrica manuscrita tiene características propias de cada firmante. Y, por otra parte, es fácil la detección de modificaciones realizadas sobre ella. En cambio, los documentos digitales no poseen esos atributos de seguridad. "Los mensajes que se cursan en sistemas computarizados son simplemente cadenas de dígitos binarios (o bits), ceros y unos que representan información, tal como palabras o números, de una manera codificada", señala Armando Carratalá, gerente de tecnología de Certisur.

Funciona utilizando complejos procedimientos matemáticos que relacionan al documento firmado con información propia del firmante

De los documentos digitales se pueden obtener varias copias con la misma autenticidad una de otra (miles en varios casos), características no compatibles con un documento en papel. Ante el crecimiento del comercio electrónico se hizo necesario contar con una herramienta que garantice seguridad, autenticidad, confidencialidad e integridad de datos: la firma digital.

Ciber-gancho. "Un conjunto de datos asociados a un mensaje digital que permite garantizar la identidad del firmante y la integridad del mensaje". Esta es quizás una de las definiciones más acertadas que se le puede otorgar a la firma digital.

¿Pero cómo se obtiene una firma digital? Para obtener un certificado digital hay que dirigirse a una de las varias entidades certificantes que existen, como la Autoridad Certificante de la Subsecretaría de la Gestión Pública (www.sgp.gov.ar) o Certisur.

Mediante el decreto 1028/03 se disolvió el Ente Administrador de Firma Digital, creado en 2002.

Sus funciones pasaron a estar a cargo de la Oficina Nacional de Tecnologías, dependiente de la Subsecretaría de la Gestión Pública de la Jefatura de Gabinete de Ministros.

Carlos Achiary, director de esta Oficina, comenta a **MI** que "la firma digital es una herramienta tecnológica que permite garantizar la autoría e integridad de los documentos digitales, es decir, saber de quién proviene el documento y tener la certeza de que no ha sido alterado desde el momento en que fue firmado". Y agrega que se trata de un instrumento con características normativas: "existen procedimientos técnicos que permiten la creación y verificación de las firmas digitales, y pronunciamientos normativos que respaldan el valor legal que dichas firmas poseen dentro de la ley". ¿Cuál ley? La 25.506 (*ver recuadro*).

La importancia de la firma digital radica en su utilidad para las transacciones de orden empresarial; en especial, para las pymes. "Las grandes empresas ya tienen sus sistemas de certificación. En cambio, una pequeña o mediana empresa que le exporta a otra vía Internet, como servicios profesionales o transacciones comerciales, utiliza

más esta tecnología para corroborar la veracidad del material que le envían", comenta Pedro del Piero, actual presidente de la Fundación Metropolitana y uno de los precursores en la legislación de la firma digital a principios de 2000.

El directivo ahonda más en el tema al destacar que "en el mercado hogareño abunda más la firma electrónica. El proveedor está registrado y tiene un password, y mediante esta contraseña puede realizar las acciones pertinentes".

Carlos Achiary sostiene que "la firma digital es un sistema considerado internacionalmente como seguro y que está basado en criptografía asimétrica".

De esta forma, según Achiary, se permite que terceras partes puedan reconocer la identidad del firmante y asegurarse que los contenidos del documento no hayan sido modificados.

Una de las grandes ventajas de la firma digital es que un operador comercial puede concretar contratos diariamente con cientos de clientes ubicados en cualquier parte del mundo.

No es lo mismo. A no confundirse: firma digital y firma

El marco normativo

La Ley 25.506 se sancionó en diciembre de 2001, casi al tiempo en que los avatares de la política nacional preanunciaban el colapso económico argentino. Dicha ley establece que una firma digital debe cumplir los siguientes requisitos:

- **Exclusividad:** Debe estar bajo el absoluto y exclusivo control del firmante
- **Autoría:** Que el autor sea claramente identificable
- **Integridad:** Que permita identificar cualquier alteración del documento digital posterior a su firma
- **Vigencia:** Haber sido creada durante el período de vigencia del certificado digital válido del firmante
- **Verificación:** Ser debidamente verificada en referencia a datos indicados en un certificado.
- **Emisión:** Que dicho certificado haya sido emitido o reconocido por un certificador licenciado

El artículo 2 de la ley, indica que la firma digital debe ser susceptible de ser verificada por terceras partes. De esta forma, se permite identificar tanto al firmante, como detectar alteraciones o anomalías de los documentos digitales luego de que éstos fueran rubricados.

electrónica no es lo mismo, aunque al oírlo al paso así lo pareciera. En la rúbrica digital, el emisor puede verificar si la firma ha sido adulterada o no y si tiene las características que él ha pedido a la hora de solicitarla a la autoridad certificante. En el caso de la firma electrónica, si es desconocida por su titular, quien deberá acreditar la veracidad es el receptor de la misma.

Por ejemplo, si entre las dos partes, una de ellas alega invalidez de alguna de las dos firmas (en el terreno digital), le corresponde a ésta demostrar ante la ley su invalidez. En caso de no tener la capacidad de demostrarlo, para la ley argentina esa firma digital es válida**.**

Si en lugar de ello, las partes firmasen el contrato con firma electrónica y surgiera la duda de la validez de la rúbrica, correspondería a la parte que exige su validez demostrar ante la ley la autenticidad de la misma. Y en caso de no tener la capacidad de demostrarlo, para la ley esa firma electrónica no es válida

Posiblemente, la confusión entre estos términos puede atribuirse también a que "Firma Digital" es usada, dentro del marco jurídico, como "Firma Electrónica Avanzada" o "Firma Electrónica Reconocida".

En cuanto al uso de la firma electrónica, es común que se utilice en aplicaciones intraempresariales, comerciales y servicios como simples passwords o claves de identificación. La firma electrónica, a diferencia de la digital, no está avalada legalmente ya que depende de un acuerdo contractual entre las partes, regido por un documento privado. Y, además, es mucho más vulnerable que la holografía digitalizada.

Vale agregar, para no ingresar en un terreno pantanoso, cuáles son las tecnologías que **no** constituyen una firma digital:

- Una firma manuscrita escaneada
- Una password o contraseña
- Un mail encriptado
- Algún procedimiento biométrico que dote a un documento únicamente de autenticidad
- Un documento digital que sólo garantice su integridad y no su autoría

Paso a paso. La firma digital es un dato que acompaña a un mensaje digital. Pero esta firma recién es utilizada luego de que intervengan dos claves: la pública y la privada.

La clave criptográfica pública sirve para verificar una firma digital. Mientras que la clave criptográfica privada sirve para desencriptar la clave pública y a su vez firmar digitalmente. Así, el encriptado es el proceso por el cual la información original se transforma en un contenido inintelegible: el dato cifrado. La otra cara de este proceso es el desencriptado, que se utiliza para darle forma y leer el dato original. Todo esto a través de una clave, es decir, una sucesión aleatoria de caracteres (bits).

Por ejemplo, si una persona (por ejemplo Pedro) desea realizar una transacción con otra, (a la que llamaremos Juan) enviándole un mensaje encriptado mediante un documento digital, el emisor (Pedro) deberá tener tanto una clave pública como otra privada. Si Juan utilizara la clave pública de Pedro para encriptar el mensaje (que en el gráfico figura como documento firmado con el número 628), solamente Pedro podría leerlo. Y eso después de desencriptarlo con su clave privada. (en el cuadro, el valor 987 que figura dentro de una llavecita). Así, el mensaje sería ciento por ciento confidencial. Y al tener el documento con el dato desencriptado, se genera un dato adicional: la firma digital (en el ejemplo, representada con el número 505). De esta manera, Pedro le envía a Juan el mensaje original, adjuntándole la firma digital del mensaje y cuando este último recibe ambos datos emplea la clave pública de Pedro (123) con la cual puede determinar que, efectivamente,

dicha firma coincide con el mensaje recibido.

Regla de oro: siempre el receptor de un mensaje firmado digitalmente deberá tener la clave pública del firmante para verificar la validez de la firma.

¿Con qué se debe contar para poder utilizar esta tecnología? Se debe usar un navegador que soporte el estándar de certificación X509 versión 3.

Entre los navegadores más utilizados que soportan dicha tecnología está el Internet Explorer 4.0x (o superior), el Netscape 4.03 o superior a excepción de la versión 6.2 que no coincide con la firma digital. Y entre los clientes de correo más utilizados: el Outlook 2000 y XP, el Outlook Express 5 o superior y el Netscape Messenger, por citar algunos.

Para tener en cuenta: una firma digital no garantiza la confidencialidad de un documento ni brinda por sí misma una constancia de recibo, es decir que haya sido efectivamente recepcionado por su destinatario.

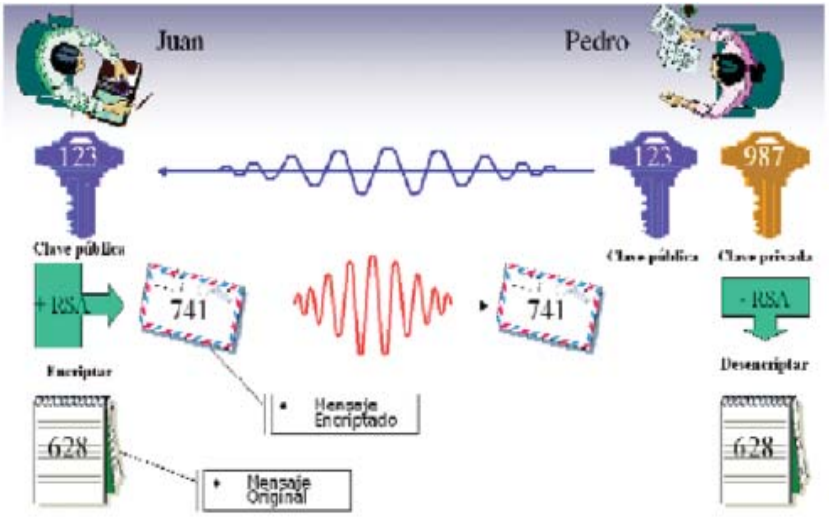
El futuro ya llegó. La firma digital utilizada como mecanismo de autenticación para acceso a datos críticos ya cuenta con varias empresas y organismos que hacen uso de ella en forma asidua. "En Argentina, la Comisión Nacional de Valores (presentación de estados contables) ha sido pionera en el uso de esta tecnología, al igual que la propia Subsecretaría de la Gestión Pública (constancias de retiro voluntario y autenticaciones en sistemas de información). En el sector privado, se destacan las Bolsas de Cereales de Rosario y Buenos Aires, la Caja de Valores y algunos bancos, para sus sistemas de Home Banking", sostiene Achiary.

También es utilizada en el Ministerio de Justicia (certificado de antecedentes penales), la AFIP, el Gobierno de la Provincia de Mendoza, algunos Tribunales Superiores de Justicia provinciales (para trámites internos y experiencias de notificaciones electrónicas) y el BCRA (en comunicaciones con los Bancos).

A nivel mundial la firma digital es utilizada para diversos fines. Achiary da algunos ejemplos: "sistemas de votación electrónica, celebración de contratos, recetas electrónicas, declaraciones juradas impositivas y trámites ante el Estado.

Sustituir la firma de puño y letra por una rúbrica digital, quizás ésa sea la meta a futuro de esta tecnología que gana terreno día a día. Será cuestión de esperar.

CertiSur



www.pki.gov.ar
(Sitio oficial del gobierno argentino sobre firma digital)

"... los documentos firmados sobre papel son seguros, ya que la tinta es difícil de borrar y las características de la rúbrica mantiene el formato de cada firmante (...) En cambio, los documentos digitales no poseen ese atributo de seguridad. "

OPINION

La firma digital: un ejemplo de tensión entre cultura e innovación técnica

Por Horacio Bossio
hbossio@e-mi.com.ar

Los abuelos decían: "Se ha hecho costumbre", cuando un acontecimiento sin razón se insertaba en el comportamiento de la gente. Y lo suscribían con mayúscula, cuando se daba de bruces con la cultura de las personas y las organizaciones.

Los procesos de cambio se idealizaron en la ciencia y en la aplicación de las tecnologías subyacentes. ¿Para qué sirven sino para ayudar a la gente? Bienvenidos fueron y serán los cambios tecnológicos, aun cuando algunos de ellos ofendan normas establecidas. Pués a lo largo de los años se "pegaron" a la estructura generacional del pensamiento y hasta se cristalizaron en refranes. Como por ejemplo "Ponele la firma" .

Un día, la firma reemplazó al apretón de manos, símbolo del honor empeñado, y se convirtió en la estampa gráfica del alma de quien la suscribía. Es que sólo las personas producimos el magnífico acto de superar con su rasgo el simple dibujo que codifica su nombre.

Nos enseñan los grafólogos que la firma conlleva tanto el carácter del individuo, como su condición psicológica.Y modificar este proceso significa cambiar el apretón de manos (o la personalidad del sujeto transcripta en un papel) por la aparente seguridad de certificar que alguien pulsó ciertas teclas de una PC.

La humanidad aceptó estos cambios con un ritmo muy rápido, pero menor al esperado. De hecho, no se vive a principios del siglo XXI como los intelectuales de anticipación lo pronosticaron. Simples artilugios tecnológicos de recolección no se insertan naturalmente, ni siquiera en la operatoria diaria de los potenciales usuarios.

No se trata sólo de seguridad. Si bien puede pensarse que la Seguridad Informática está muy lejos de ser invulnerable, debiéramos aceptar que sus métodos y técnicas son de evolución permanente. Mientras que si nos referimos a la inviolabilidad con mecanismos tradicionales, los encontraremos en un plano descendente.

Pareciera que todas las condiciones están dadas para que un fantástico proyecto sea rápidamente aceptado por la sociedad mundial y se torne en el mayor éxito de la ciencia y la tecnología informática.

La Firma Digital sería socia invalorable de:

* Los contratos en la red.
* La comercialización globalizada; y de
* Todo tipo de negocios y acuerdos.

Pero con semejantes socios, ¿qué es lo que sucede? ¿Por qué el gran proyecto no hace explosión? Analizamos el tema y observamos que otro referente de la tecnología informática, el "voto electrónico", está siendo cuestionado en los Estados Unidos.

Nos hemos relacionado con universidades europeas, principales precursoras del desarrollo de la firma digital y reconocidas por su tarea de investigación . Algunas de ellas, incluso, han constituído agencias y compañías paralelas para su comercialización, sin obtener el éxito esperado. ¿Por qué?

Analicemos algunas variables:

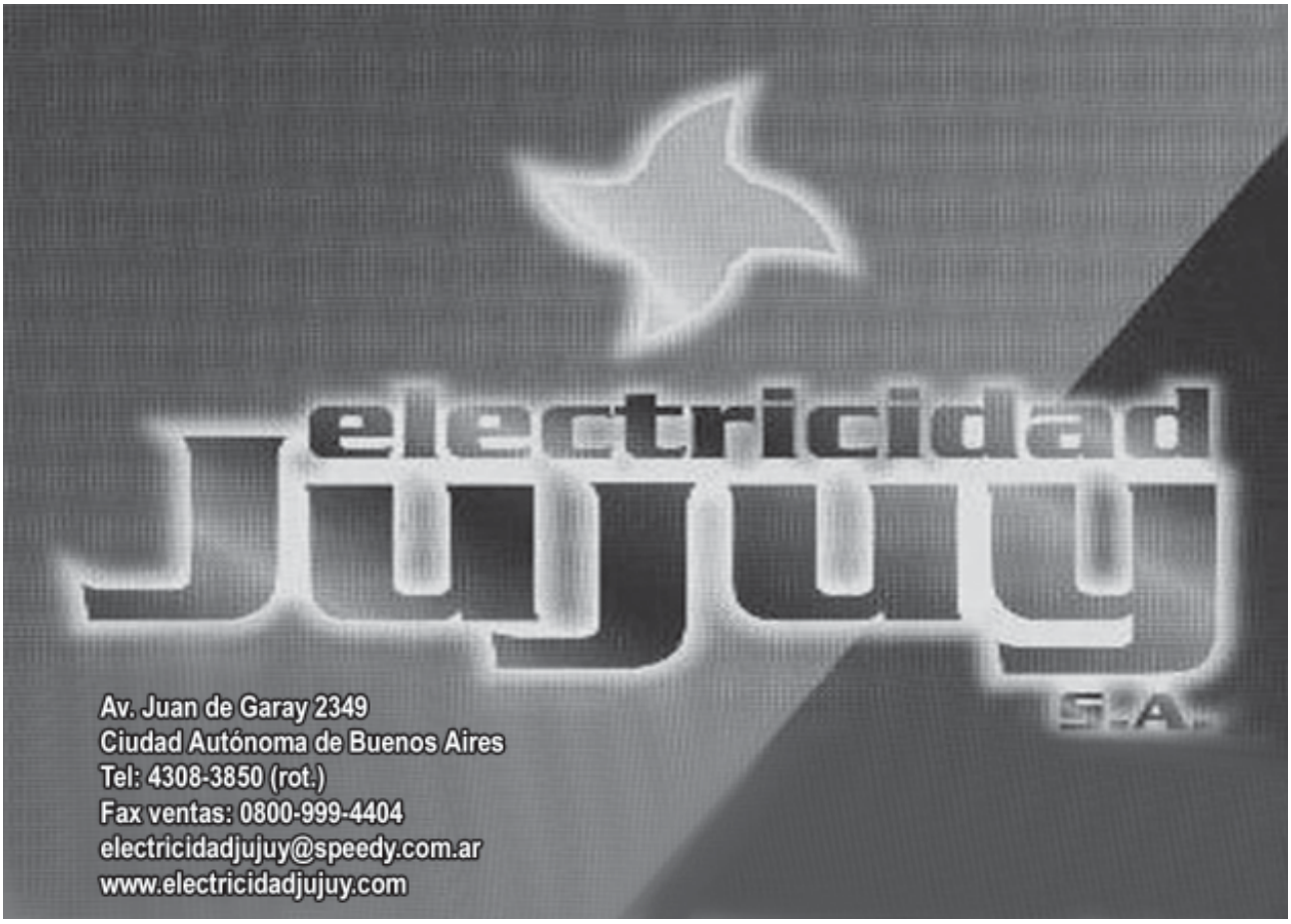
*** Desarrollo tecnológico:** Aceptable, en todos sus aspectos.

*** Normas de aplicación:** Continuamente modificadas, sin alcanzar a lograr la satisfacción de los potenciales usuarios. Es frecuente que los cambios normativos empeoren el estado anterior. El caso más elocuente fue el retroceso en la confianza de los usuarios y la dificultad de aplicación cuando la Unión Europea integró las normas propias de cada país.

*** La aplicación:** El caso que a continuación se describe, es sólo un ejemplo que se repite en otras casas de estudio. Pertenece a la Universitá di

Bologna. Una universidad de primera línea en el desarrollo de tecnología de punta. La integran destacados científicos entrenados en análisis y abstracción, por lo que, se supone, no debieran caer ni en la costumbre ni en el resultado fácil. **El proyecto consistía en desarrollar e implementar la firma digital en el ámbito de la Universidad. Y luego comercializarlo.** El desarrollo tecnológico se resolvió en el tiempo previsto y sin mayores dificultades y su expectativa de mejora y crecimiento fue optimista. La implementación tecnológica, consistente en incorporar la firma digital a todo el proceso de administración y calificación del alumnado demandó siete años. Y aún hoy, el rechazo sigue siendo una constante. Peor aún, se supone que pasarán otros cinco años en ser totalmente utilizada y otros diez en comercializarla extra muros. Es el tiempo estimado de recambio cultural para la inserción de la nueva tecnología. Dentro de la Universidad, la mayor satisfacción recayó en el ahorro de dos millones de euros anuales en gastos de administración. (No logramos saber la opinión de los despedidos).

Después de tanta discusión, debate normativo y de poder de autoridad certificante, parece que el negocio es bueno, pero no sencillo. Todo pareció resolverlo una aplicación tecnológica, pero la cultura de la gente tuvo algo qué decir. ¿Será sólo en este tema?

"Simples artilugios tecnológicos de recolección no se insertan naturalmente, ni siquiera en la operatoria diaria de los potenciales usuarios."

El Disparador espera su opinión en www.e-mi.com.ar/foros.htm