FIRMA DIGITAL EN EL INSTITUTO NACIONAL DE SALUD

Leonardo Rojas Mezarina

Médico especialista en Administración de Salud

¿QUÉ ES LA FIRMA DIGITAL?

La **firma digital** es una modalidad de firma electrónica que utiliza una técnica de criptografía asimétrica y que tiene la finalidad de asegurar la integridad del mensaje de datos a través de un código de verificación, así como la vinculación entre el titular de la firma digital y el mensaje de datos remitido[1].

Es un instrumento con características técnicas y normativas, esto 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 no implica asegurar la confidencialidad del mensaje; un documento firmado digitalmente puede ser visualizado por otras personas, al igual que cuando se firma holográficamente.

Según el artículo 3.º de la Ley de Firmas y Certificados Digitales, Ley 27269, la **firma digital** es aquella firma electrónica que utiliza una técnica de criptografía asimétrica, basada en el uso de un par de claves único; asociadas una clave privada y una clave pública relacionadas matemáticamente entre sí, de tal forma que las personas que conocen la llave pública no pueden derivar de ella la clave privada[2].

En estas definiciones se encuentran varios conceptos conexos: firma electrónica, claves pública y privada. En la ley se define a la **firma electrónica** como cualquier símbolo basado en medios electrónicos utilizado o adoptado por una parte con la intención precisa de vincularse o autenticar un documento cumpliendo todas o algunas de las funciones características de una firma manuscrita. *Siendo la firma digital una especie de la firma electrónica,* consiste en un símbolo basado en medios electrónicos y su función es cumplir las funciones de la firma manuscrita.

En el Perú, la autoridad administrativa competente de la infraestructura oficial de firma electrónica es INDECOPI (Instituto Nacional de Defensa de la Competencia y de la Propiedad Intelectual)[3].

¿CÓMO FUNCIONA LA FIRMA DIGITAL?

Lo particular de la firma digital es el uso de la técnica de la **criptografía asimétrica**, por tanto, no consiste en escanear una firma (en términos estrictos "digitalizar la firma") sino en una técnica especial de encriptación.

La firma digital utiliza las claves asimétricas[4] o "claves públicas" (que son diferentes a las cla-

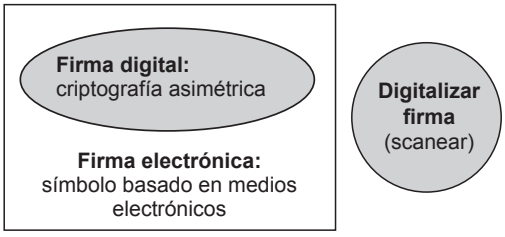

Figura 1. Diferencias entre la firma digital, electrónica y escaneada.
Fuente: Mendoza Luna, Amilcar. (2003). *"Los Artículos 141 y 141-A del Código Civil y la Firma Digital"*. (tesis de maestría). PUCP. Lima.

1 Definición de INDECOPI para firma digital.

2 Ley 27269, Ley de Firmas y Certificados Digitales.

3 El Reglamento de Firmas y Certificados Digitales, aprobado por el Decreto Supremo 019-2002-JUS, designó al INDECOPI como la Autoridad Administrativa Competente de la Infraestructura Oficial de Firma Digital.

4 MARTINEZ NADAL, Apollonia. Comercio Electrónico, Firma Digital y Autoridades de Certificación. Madrid: Civitas. 1998. p.42.

ves simétricas que son conocidas por los usuarios que intervienen). Los usuarios que utilizan las claves públicas no comparten la clave, sino poseen claves complementarias y relacionadas entre si, una de ellas es conocida publicamente y la otra es privada o secreta.

El uso de la criptografía asimétrica permite CONFIDENCIALIDAD incluso a través de redes abiertas como Internet, también proporciona AUTENTICIDAD, INTEGRIDAD Y VINCULACIÓN (O NO REPUDIO), los cuales son características de la firma digital.

El proceso de firma digital se divide en dos subprocesos, la realización de la firma y la comprobación de la firma:

Primer subproceso: realización de la firma

- **1**.- Se tiene un documento original al cual se le aplica una función hash[5] (o MAC) y se obtiene un *hash* o resumen del mismo.

Figura 2. Primer subproceso: realización de la firma digital.
Fuente de imágenes: www.micit.go.cr/docs/Presentacion%203.ppt.

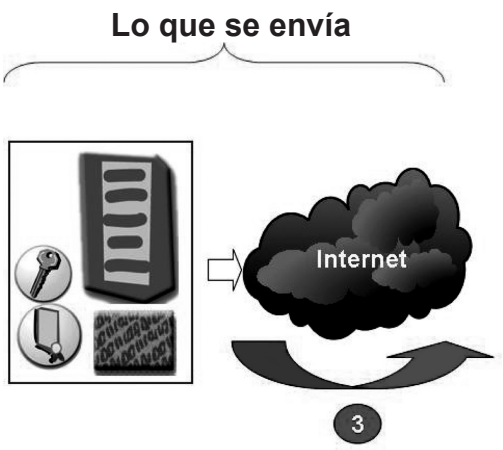

Figura 3. Información que se envía al destinatario luego de la firma en el proceso de firma digital.
Fuente de imágenes: www.micit.go.cr/docs/Presentacion%203.ppt.

- **2**.- El resumen obtenido luego de aplicar la función *hash*, se cifra con la clave privada del titular del certificado.
- **3**.- Se envía al destinatario el conjunto formado por el documento original, el *hash* (o MAC) firmado y el certificado (Figura 2).

Segundo Subproceso: realización de la firma

- El receptor recibe el conjunto formado por el documento original, el *hash* firmado y el certificado.
- **45**.- A partir del certificado se extrae la clave pública del remitente. Con la clave pública desencripta el mensaje que fue cifrado con la clave privada y obtengo el *hash* que se calculó en origen.
- **44**.- Se calcula el *hash* a partir del documento original.
- 4 Comparamos el *hash* del documento y el que se obtuvo con la clave pública, y deben ser idénticos (Integridad).

5 Una función o algoritmo *hash*, en términos informáticos, se refiere a una función o método para generar claves o llaves que identifican de manera casi unívoca a un documento, archivo, registro, etc. Como resultado de la aplicación de esta función o algoritmo a un documento, archivo o registro dado se obtiene, lo que se denomina, un hash (llamado también "resumen").

6 INSTITUTO NACIONAL DE ESTADÍSTICA E INFORMATICA. Seguridad en Internet. Lima: INEI. 1997. p. 50-51.

Figura 4. Segundo subproceso: comprobación de la firma digital.
Fuente de imágenes: www.micit.go.cr/docs/Presentacion%203.ppt.

¿QUÉ CARACTERÍSTICAS TIENE LA FIRMA DIGITAL?

Un aspecto importante sobre la firma digital es que posee cinco propiedades[6]:

1. **Integridad del mensaje:** es decir, que el mensaje esté completo y no sea alterado de manera alguna. Cuando un usuario usa una llave pública de A para descifrar un mensaje, él confirma que fue A y solamente A quien envió el mensaje.

2. **Inviolabilidad**: solamente A conoce su llave secreta.

3. **La firma no es reutilizable**: la firma es una función del documento y no puede ser transferida para otro documento.

4. **Autenticidad**: cuando un usuario usa una llave pública de A para descifrar un mensaje, él confirma que fue A y solamente A quien envió el mensaje. La certidumbre sobre quién manda el mensaje o el documento electrónico. Es uno de los aspectos más fáciles de entender sobre la firma digital, se trata simplemente de verificar la identidad. Según el artículo 4.º del Reglamento de la Ley de Firmas Digitales (D.S. 019-2002-JUS) la autenticación es el proceso técnico que permite determinar la identidad de la persona que firma electrónicamente, en función del mensaje firmado por éste y al cual se le vincula; este proceso no otorga certificación notarial ni fe pública.

5. **No repudio (o vinculación):** que nadie pueda negar que el mensaje ha sido recibido y que lo vincule efectivamente al mismo. El usuario B no precisa de ninguna ayuda de A para reconocer su firma y A no puede negar tener firmado dicho documento.

¿CUÁL ES EL MARCO NORMATIVO DE LA FIRMA DIGITAL?

En el Perú, el marco legal que regula el uso de las firmas y certificados digitales, es el siguiente: Ley 27269, Ley de Firmas y Certificados Digitales y su Reglamento aprobado con Decreto Supremo 052-2008-PCM, que regula la utilización de la firma electrónica, así como, de la firma digital otorgándole la misma validez y eficacia jurídica que el uso de una firma manuscrita.

De acuerdo al artículo 57.º del Reglamento de la Ley de Firmas y Certificados Digitales, aprobado por D.S. 052-2008-PCM, el Instituto Nacional de Defensa de la Competencia y de la Protección de la Propiedad Intelectual (INDECOPI) ha sido designado como autoridad administrativa competente (AAC) teniendo como principal función la implantación y buen funcionamiento de la infraestructura oficial de firma electrónica (IOFE) para lograr eficiencia, eficacia y transparencia en la gestión pública y para promover su uso en el comercio electrónico.

Asimismo, el artículo 28.º del Decreto Legislativo 1033 que aprueba la Ley de Organización y Funciones del INDECOPI, se le asigna a la

Comisión de Normalización y Fiscalización de Barreras Comerciales No Arancelarias (CNB) la función de administrar la infraestructura oficial de firma electrónica, conforme a la normativa de la materia. En base a lo anteriormente dicho, se asegura que con la puesta en funcionamiento de la "plataforma tecnológica para la administración y supervisión de la IOFE", por parte de la AAC, se garanticen transacciones de gobierno electrónico seguras y, de manera general, que los actos jurídicos autenticados con el uso de firmas y certificados digitales tengan plena validez y eficacia jurídica.

Actualmente, el Instituto Nacional de Salud cuenta con un convenio firmado entre el INDECOPI y el INS para el uso de la Firma Digital, dicho convenio establece que el representante legal de la institución es el que registra a los servidores que podrán utilizar dicha herramienta, para ello se ha definido que todos los directores generales y ejecutivos del INS deberán tener y utilizar la firma digital para algunos de los procesos que se llevan a cabo a través del SIGANET. Se espera que para el segundo trimestre del presente año el INS ya cuente con tan importante herramienta que permitirá dinamizar sus procesos de manera más eficiente para satisfacción de los usuarios.

Correspondencia: Leonardo Rojas Mezarina, Calle 30 N.º 111 Dpto. 203, San Borja, Teléfonos: +511 620 8767, +51 997 242 891, leorm98@gmail.com.