Firmando en tiempos del *hash*

Tu firma manuscrita, la que haces "de puño y letra", es única y tiene mucho valor. Pero ahora son tendencia las firmas electrónicas. ¿Ya la usas? ¿Qué sabes sobre ellas?

Tu autógrafo o firma manuscrita es única y te identifica. En la mayoría de los países no hay reglas sobre su aspecto; puede ser larga y muy elaborada, o apenas tus iniciales adornadas con algún "firulete". Pero a partir de la mayoría de edad tiene valor legal y la debes hacer siempre igual a la que figura en tu documento de identidad.

Al hacerla ofreces prueba que eres quien dices ser y al estamparla en un documento afirmas y te comprometes con lo que expresa su contenido. Si firmaste es porque lo aceptas, y no podrás deslindarte de responsabilidad.

Para saber si es verdadera o falsa se estudian características difíciles de imitar (los datos biométricos): el tipo de trazo, la presión al escribir, la forma de ciertas letras, la rúbrica. Hay expertos especializados en estas cuestiones, los peritos calígrafos, a los que se acude ante dudas o reclamos legales. Si comprueban que es auténtica emiten un certificado que lo confirma y la avala.

La tecnología digital nos facilita realizar varios trámites *online*, utilizando dispositivos electrónicos y la internet. Para trámites y documentos que requieren nuestra firma ahora se usan las firmas digitales o electrónicas (que estrictamente no son lo mismo pero se usan con frecuencia como sinónimos). Y con ellas el proceso de firmar es bien distinto al que seguimos para la manuscrita. En algunos casos es tan simple que podemos no ser conscientes que eso que hacemos es firmar.

Es muy probable que aún sin saberlo ya las uses. Por lo tanto, ¡atención! puedes estar asumiendo compromisos legales. Dependerá del caso y lo que establezca el Gobierno de tu país. Aquí te adelantamos asuntos que conviene que sepas y ejemplos de lo que rige en El Salvador, pero te sugerimos investigar en sitios oficiales del tuyo y artículos científicos para saber más sobre el tema.

La nueva forma de firmar

Cuando pones tu nombre de usuario y contraseña para entrar en tus redes sociales favoritas, lo que hiciste fue una firma digital. También lo es cuando "tecleas" tu PIN en un cajero automático o en un POS, el dispositivo por el que pasas tu tarjeta electrónica para pagar algo. Hasta un tilde que aparece al presionar sobre un cuadro de diálogo (por ejemplo, "*Aceptar términos y condiciones*" de un contrato) se puede llegar a considerar como tal.

Por lo general se entiende que una firma electrónica es un conjunto de datos (un bloque de información) que se generan de manera electrónica, se agregan y quedan relacionados de manera lógica a un documento o archivo electrónico. Según el dispositivo y el mecanismo tecnológico que se utilice para hacerla ofrecerá mayor o menor nivel de seguridad y garantías.

Así es. En "el reino de los ceros y los unos" ya no precisamos una lapicera ni hacer esa bella obra de arte que algún día diseñamos con esmero y decidimos que sería nuestra firma personal.

Cada país establece cuáles se aceptan y cuál tendrá valor equivalente a la manuscrita. En El Salvador se usan varias pero la única de mismo valor legal que un autógrafo es la firma electrónica "certificada".

Para hacerla se precisan dos cosas: un "dispositivo seguro de creación de firma" (podrá ser una tarjeta inteligente, un token u otro de similar seguridad) y un "certificado de firma electrónico" que se debe adjuntar al documento firmado al enviarlo. Ambos se obtienen de proveedores autorizados.

En el dispositivo reside una clave que sólo tú puedes usar (la llave privada), por medio de la cual el documento queda firmado de un modo muy difícil de falsificar y que a la vez lo "tranca". El certificado asegura a quien lo recibe que eres quien dices ser, y le ofrece otra clave (la llave pública) con la que puede validar la firma y verificar que el documento no ha sido alterado luego de firmado. O si lo fue, puede detectarlo.

Firmas electrónicas: Cuál es cuál y cuándo usarlas

- **Firma electrónica simple** Se acepta en documentos o procesos que no requieran alta seguridad, porque es fácil de falsificar. Permite identificar al firmante, por ejemplo usuario y contraseña, pero no verificarlo. La foto de tu firma manuscrita insertada en un documento entraría en esta categoría.

- **Firma electrónica certificada:** Es la más segura y la que más garantías ofrece. Se usa cuando una ley o mandato legal la exige. Permite identificar y verificar al firmante, validar la firma y detectar cualquier cambio que se haya hecho en el documento luego de firmado.

  - **Firma de corta duración*:** Para firmar documentos digitales de un trámite (una sola vez)

  - **Firma longeva*:** Firma certificada con validez a lo largo del tiempo

  - **Firma interactiva*:** Para que varias personas firmen un mismo documento digital

  - **Firma automatizada*:** Para firmar rápidamente una gran cantidad de documentos.

  - **Firma biométrica:** El grafo que haces sobre una pantalla táctil o con el mouse de tu PC se llega a considerar firma electrónica avanzada si el sistema captura y guarda más de un dato biométrico (si fuera necesario, un perito calígrafo podría analizarlos)

  - **Firma certificada y con sello de tiempo certificado:** Es la más completa. Agrega y garantiza en qué momento exacto se firmó el documento, basado en la hora mundial.

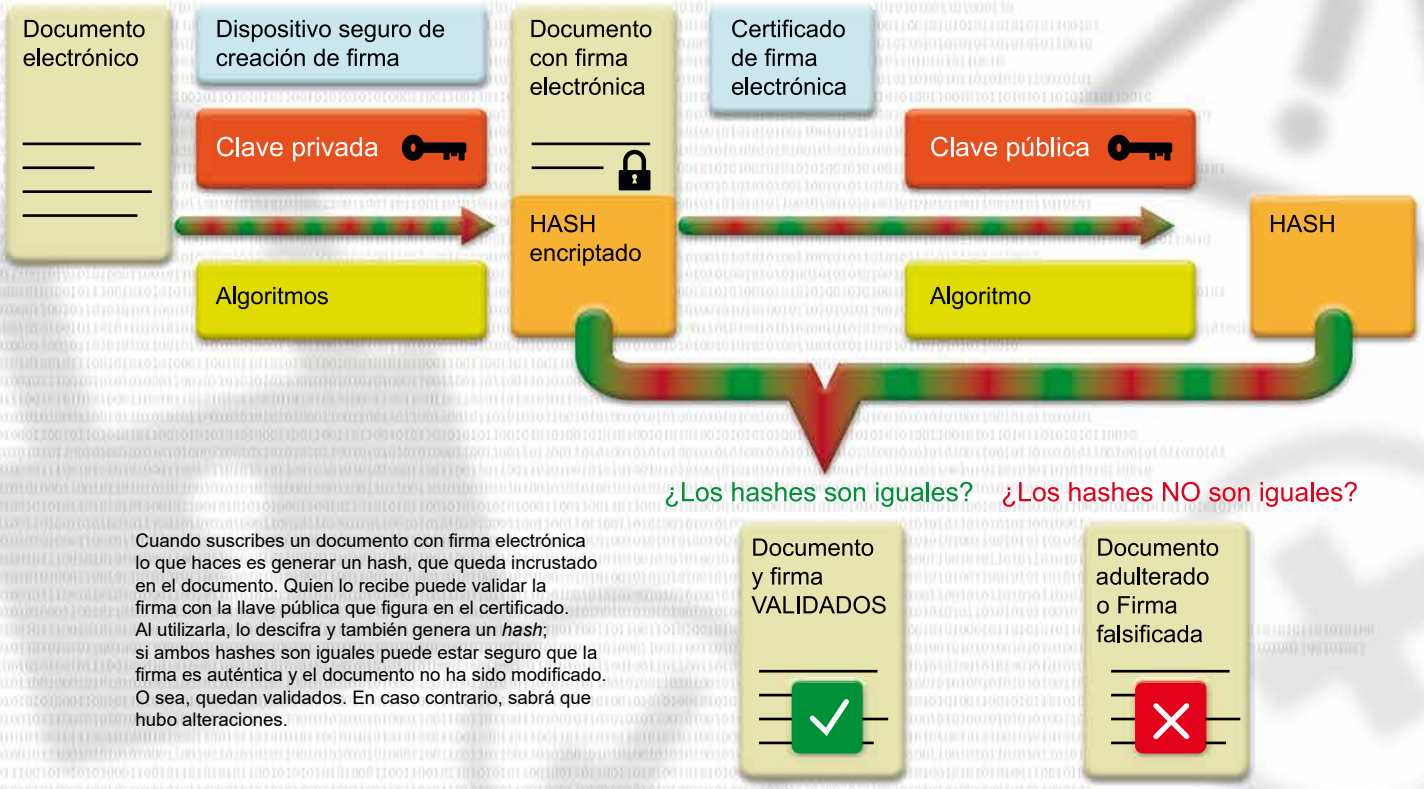
* Datos publicados en *Facebook* por la Secretaría de Prensa de la República de El Salvador (05 de agosto de 2021) https://www.facebook.com/SecPrensaSV/posts/el-gobierno-del-presidente-nayib-bukele-trabaja-por-potencializar-el-clima-de-ne/1006959606789481/

El *backstage* de una firma electrónica

Cualquier conjunto de datos que se tome como dato de entrada se puede transformar en un *hash*, una cadena corta de caracteres alfanuméricos —por ejemplo, ceros y unos— aplicando un algoritmo (la función *hash*). No es posible generar dos hashes idénticos, salvo que también lo sean los datos de entrada.

El *hash* es pieza clave en la firma electrónica certificada. Al hacer esta firma, lo que ocurre en el *backstage* al mismo tiempo, es que has generado y encriptado un hash, aplicando en forma conjunta dos algoritmos que vuelven casi imposible falsificarla o modificar el documento sin que se detecte.

El algoritmo de uso más extendido para las firmas electrónicas es el mismo que hizo posible el desarrollo de *Bitcoin*: el algoritmo SHA-256. Se puede aplicar a cualquier tipo de archivo digital: audios, vídeos, imágenes, textos, etc. Al usarlo en forma conjunta con otro algoritmo (el RSA, por las iniciales de quienes lo formularon) el documento y la firma se vuelven casi imposible de imitar y adulterar.



Cuando suscribes un documento con firma electrónica lo que haces es generar un hash, que queda incrustado en el documento. Quien lo recibe puede validar la firma con la llave pública que figura en el certificado. Al utilizarla, lo descifra y también genera un *hash*; si ambos hashes son iguales puede estar seguro que la firma es auténtica y el documento no ha sido modificado. O sea, quedan validados. En caso contrario, sabrá que hubo alteraciones.

Autores: José Osegueda Miranda (El Salvador) y Silvana Demicheli (Uruguay).

Sello de tiempo

---› El sellado de tiempo es un mecanismo que permite demostrar que un conjunto de datos han existido y no han sido alterados desde un instante específico.

---› ¿Quién registró primero la canción que resultó ser un suceso y se volvió viral? ¿A qué hora pagaste online la compra que tenía plazo límite para hacerlo? Para muchos trámites es importante que quede evidencia del momento exacto en que fue realizado, cuestión que se resuelve agregando un sello de tiempo o *time stamp*, en inglés.

---› Para varios se debe usar un "sello de tiempo cualificado". Lo que incrusta es una marca de hora mundial, y en esto intervienen otros dispositivos electrónicos: los relojes atómicos y los "servidores de tiempo" o servidores NTP.

---› En El Salvador, los servidores NTP que transfieren la Hora Oficial del país vía internet y proporcionan las marcas de tiempo para firma y factura electrónica, operaciones y transacciones bancarias, *secure login*, voto electrónico y visado electrónico los mantiene en operación el Centro de Investigaciones de Metrología (CIM). Permanecen en línea desde finales del año 2017 y se desconectan solo en momentos de mantenimiento.

Ilustraciones: Alberto Parra del Riego.

Fotos: Silvana Demicheli