La *firma electrónica avanzada*, también conocida como [firma biométrica](https://es.wikipedia.org/wiki/Firma_biom%C3%A9trica), es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

**Unión Europea**[[editar](https://es.wikipedia.org/w/index.php?title=Firma_electr%C3%B3nica&action=edit&section=3)]

El mercado interior de la [Unión Europea](https://es.wikipedia.org/wiki/Uni%C3%B3n_Europea) implica un espacio sin fronteras interiores en el que está garantizada la libre circulación de mercancías. Deben satisfacerse los requisitos esenciales específicos de los productos de firma electrónica a fin de garantizar la libre circulación en el mercado interior y fomentar la confianza en la firma electrónica.

En ese sentido la Directiva 1999/93/CE sienta un marco común para la firma electrónica que se concretó con la [transposición](https://es.wikipedia.org/wiki/Transposici%C3%B3n_(Derecho_de_la_Uni%C3%B3n_Europea)) de la Directiva a las diferentes legislaciones nacionales de los países miembros.

[**España**](https://es.wikipedia.org/wiki/Espa%C3%B1a)[[editar](https://es.wikipedia.org/w/index.php?title=Firma_electr%C3%B3nica&action=edit&section=4)]

En España existe la Ley 59/2003, de Firma electrónica, que define tres tipos de firma:

* *Firma electrónica*: es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.
* *Firma electrónica avanzada*: es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere, y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
* *Firma electrónica reconocida*: es la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.

La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

**Norteamérica**[[editar](https://es.wikipedia.org/w/index.php?title=Firma_electr%C3%B3nica&action=edit&section=5)]

[**México**](https://es.wikipedia.org/wiki/M%C3%A9xico)[[editar](https://es.wikipedia.org/w/index.php?title=Firma_electr%C3%B3nica&action=edit&section=6)]

En México existe la Ley de Firma Electrónica Avanzada (LFEA) publicada en el diario oficial de la federación el 11 de enero de 2012. La Secretaría de Economía es la encargada de acreditar a los diferentes de servicios de Firma Electrónica Avanzada.

La LFEA establece que la Firma Electrónica Avanzada tiene los mismos efectos jurídicos que la firma autógrafa, garantiza el contenido del documento firmado y no es repudiable.[8](https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica#cite_note-8)​

**Suramérica**

[**Argentina**](https://es.wikipedia.org/wiki/Argentina)[[editar](https://es.wikipedia.org/w/index.php?title=Firma_electr%C3%B3nica&action=edit&section=8)]

La firma digital es legislada en la ley 25506 de la República Argentina. Fue sancionada en noviembre de 2001 y promulgada en el mismo año.[[1]](http://www.derechofacil.gob.ar/leysimple/firma-digital/)

La ley distingue a la *firma digital* de la *firma electrónica*, siendo la primera la de mayor peso jurídico: se establece que la firma digital es equivalente a la firma manuscrita. Esa equivalencia se exceptúa en los siguientes casos:

1. a las disposiciones por causa de muerte;
2. a los actos jurídicos del derecho de familia;
3. a los actos personalismos en general;
4. a los actos que deban ser instrumentados bajo exigencias o formalidades incompatibles con la utilización de la firma digital, ya sea como consecuencia de disposiciones legales o por acuerdo de partes.

A diferencia de la firma electrónica, la firma digital es posible gracias al uso de certificados digitales. Esos certificados contienen datos que identifican al titular de una firma. Los certificados digitales son entregados por Certificadores registrados y autorizados para tal actividad, y pueden ser empresas, registros, u organismos públicos especialmente autorizados.

Son los certificados digitales los que permiten a un tercero establecer la autenticidad de un firmante y detectar la alteración de documentos electrónicos firmados digitalmente.

Por otro lado, la exigencia de establecer la autenticidad del firmante en la firma electrónica recae en el mismo firmante, dado que carece de los requisitos legales para ser considerada firma digital.[9](https://es.wikipedia.org/wiki/Firma_electr%C3%B3nica#cite_note-9)​ En cambio, la autenticidad del firmante en la firma digital se presume, salvo prueba en contrario.

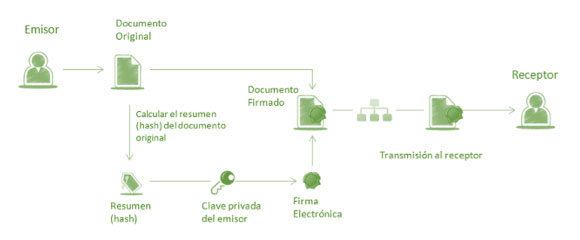
**¿Qué es y para qué sirve la Firma Electrónica?**  
  
La Firma Electrónica es un conjunto de datos electrónicos que acompañan o que están asociados a un documento electrónico y cuyas funciones básicas son:

* • Identificar al firmante de manera inequívoca
* • Asegurar la integridad del documento firmado, asegura que el documento firmado es exactamente el mismo que el original y que no ha sufrido alteración o manipulación
* • Asegurar la integridad del documento firmado, los datos que utiliza el firmante para realizar el firmado son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

El uso de la Firma Electrónica surge de la necesidad de las organizaciones de reducir costos e incrementar la seguridad de sus procesos internos, a través del uso de medios electrónicos que permitan agilizar los procesos, reducir los tiempos y evitar el uso de papel.

**Definición de Firma Electrónica**  
  
De acuerdo a lo publicado en Gaceta Universitaria en los **Lineamientos para el uso de la Firma y Sello Electrónicos, la Firma Electrónica** Electrónica se define como: Conjunto de datos en forma electrónica asociados a un mensaje de datos o documento electrónico, utilizados para acreditar la identidad del emisor con relación al mensaje, que indican que es el autor legítimo de este, por lo que asume como propia la información contenida en él, produciendo los mismo efectos jurídicos que la firma autógrafa. Para poder utilizar la Firma electrónica será necesario haber obtenido previamente un certificado de firma electrónica, el cual es emitido por una Entidad Certificadora [(ver información de Entidades Certificadoras)](http://web.uaemex.mx/fise/2_4_entidades_certificadoras.html). El certificado emitido contiene entre otras cosas la llave pública. El funcionamiento de la firma electrónica se basa en un par de números "la llave pública y la llave privada" con una relación entre ellos. La llave privada se resguarda por parte del firmante en tanto que la clave pública, en cambio, se distribuye junto con el mensaje o documento firmado.  
  
  
**Certificado de Firma Electrónica**  
  
Los certificados son documentos electrónicos que incluyen ciertos datos de su titular y su llave pública, y están validados por una Entidad Certificadora. Este documento permite utilizar la firma electrónica y contiene una serie de datos como son: el Código Único de Identificación, el periodo de validez, los datos del titular del certificado (NOMBRE, RFC), así como la llave pública.  
  
  
**Proceso básico de Firma Electrónica**  
  
El proceso básico que se sigue para la firma electrónica es el siguiente:

* • El usuario dispone de un documento electrónico y de un certificado que le pertenece y le identifica.
* • La aplicación utilizada para firmar electrónicamente realiza un resumen del documento, el cuál es único y cualquier modificación del documento implica también una modificación del resumen.
* • La aplicación utiliza la clave contenida en el certificado para codificar el resumen.
* • La aplicación crea otro documento electrónico que contiene ese resumen codificado. Este nuevo documento es la firma electrónica.



El resultado de todo este proceso es un documento electrónico obtenido a partir del documento original y de las claves del firmante. La firma electrónica, por tanto, es el mismo documento electrónico resultante.

**Entidad Certificadora**  
  
Una Entidad Certificadora es la dependencia universitaria que tiene las facultades de autorizar, revocar, suspender o cancelar los certificados de Firma Electrónica conforme. La Entidad Certificadora tiene como su función más importante verificar la identidad del solicitante de un Certificado antes de su emisión, así como de almacenar y administrar los certificados que emite.  
[(Ver información de Entidades Certificadoras)](http://web.uaemex.mx/fise/2_4_entidades_certificadoras.html).

**Uso de la Firma Electrónica**  
  
La Firma electrónica permite garantizar la identidad de un universitario que realizado una gestión, así como la integridad del contenido de los mensajes que envía. Por este motivo, los universitarios que dispongan de Firma Electrónica podrán consultar información de carácter personal, realizar trámites o acceder a servicios que impliquen una certificación de identidad. Dado que la comprobación de identidad se realiza a través de medios electrónicos, los documentos firmados electrónicamente tienen sustento y validez jurídica únicamente cuando se verifiquen a través de los medios diseñados para dicho efecto.

**Condiciones para considerar un documento electrónico (mensaje de datos) como válido**  
  
El contenido de un documento electrónico o mensaje de datos es lo que se está firmando de común acuerdo entre dos o más involucrados, quienes inicialmente negocian o validan el contenido electrónico y una vez aceptado éste proceden a firmarlo electrónicamente. Los involucrados que aceptaron el contenido del documento electrónico o mensaje de datos y dieron su aceptación utilizando su llave privada para generar su Firma Electrónica son quienes firman el documento o mensaje de datos. El Certificado de Firma Electrónica vincula la identidad de los firmantes con su llave pública, que al encontrarse relacionado con su llave privada permite determinar el autor de una Firma Electrónica. Al ser el Certificado de Firma Electrónica un mensaje firmado electrónicamente, este se puede autentificar y determinar si es integro y que fue emitido por una Entidad Certificadora válida y que éste se encuentra además en su periodo de validez. Una vez que un mensaje ha sido firmado electrónicamente y conociendo sus correspondientes Certificados de Firma Electrónica, es posible determinar si el mensaje no ha sido alterado, que el mensaje firmado por los participantes fue el mismo, que se tienen elementos suficientes para identificar la autoría de las firmas y que un tercero confiable (Entidad Certificadora) verifico la identidad de los firmantes avalando que estos son los poseedores de la llave privada con la que realizaron sus firmas.