**Firma Electrónica**

|  |
| --- |
| **Enlaces** |
| [**https://firmaelectronica.gob.es/**](https://firmaelectronica.gob.es/)  Enlace 2  Enlace 3 |
| **Videos** |
| Video 1  Video 2  Video 3 |
| **Apuntes** |
| La Firma Electrónica.Base legal de la Firma Electrónica.Los Certificados Electrónicos. Conclusiones |

# La Firma Electrónica.

## Definición.

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 el no repudio del documento firmado. Los datos que utiliza el firmante para realizar la firma son únicos y exclusivos y, por tanto, posteriormente, no puede decir que no ha firmado el documento

La base legal de la Firma electrónica está recogida en la Ley 59/2003 de Firma Electrónica y se desarrolla en más profundidad en la sección [Base legal de las Firmas](https://firmaelectronica.gob.es/Home/Ciudadanos/Base-Legal.html). La sección también explora, bajo qué circunstancias la ley equipara la firma electrónica a la firma manuscrita, añade notas respecto a la normativa europea y hace distintas referencias legales a firmas con sellos de tiempo y avanzadas.

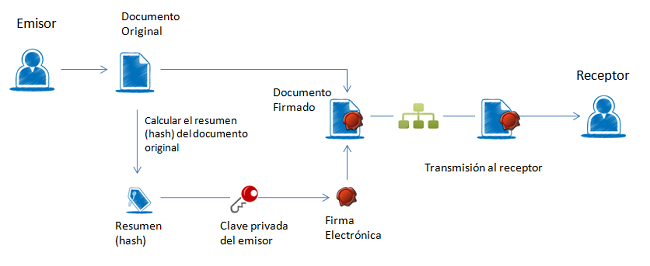
## El Certificado Electrónico, base de la firma electrónica.

Para firmar un documento es necesario disponer de un certificado digital o de un DNI electrónico.

El certificado electrónico o el DNI electrónico contiene unas claves criptográficas que son los elementos necesarios para firmar. Los certificados electrónicos tienen el objetivo de identificar inequívocamente a su poseedor y son emitidos por Proveedores de Servicios de Certificación.

Puedes saber más sobre certificados en la sección [Certificados Electrónicos](https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html).

## El 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 (una hoja de cálculo, un pdf, una imagen, incluso un formulario en una página web) y de un certificado que le pertenece y le identifica.
* La aplicación o dispositivo digital utilizados para la firma realiza un resumen del documento. El resumen de un documento de gran tamaño puede llegar a ser tan solo de unas líneas. Este resumen es único y cualquier modificación del documento implica también una modificación del resumen.
* La aplicación utiliza la clave privada 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.

**Recuerda:**

La firma electrónica es el archivo o **documento electrónico resultante**. Este es el documento válido a efectos legales y el que **debes conservar**. Cualquier impresión o representación gráfica que se haga de él solo es válido en los términos que determine el destinatario de la firma. En general, en este caso, la firma impresa debará contener un CSV o Código Seguro de Verificación que permite contrastar la copia impresa con la original electrónica.

## ¿Cómo firmo un documento?

Algunas de las preguntas que pueden surgir en el proceso anterior son:

* ¿Qué herramienta debo utilizar para firmar?
* ¿Necesito instalar algo en mi ordenador?
* Y cuando firmo un formulario en internet ¿Debo instalar algo o mi navegador ya lo hace todo automáticamente?
* ¿Cómo uso el DNI electrónico desde mi ordenador? ¿Cómo instalo el lector de DNI?

Puesto que estamos hablando de firma electrónica, la firma debe realizarse obligatoriamente por medios electrónicos y la podrás realizar de dos formas:

* Descargando una aplicación en tu PC: En este caso utilizas para firmar la aplicación que instalas en tu ordenador y no necesitas estar conectado a internet. La aplicación a usar es AutoFirma, del Ministerio de Hacienda y Administraciones Públicas. Puedes ver más información sobre esta, y descargarla en la sección [Aplicaciones de firma](https://firmaelectronica.gob.es/Home/Ciudadanos/Aplicaciones-Firma.html).
* Firmar directamente en internet: Esta opción es usada sobre todo cuando firmas formularios o solicitudes, por ejemplo, en la relación con la Administración Pública. Pero también puedes firmar tus propios documentos en internet utilizando el servicio ofrecido por VALIDe. Para firmar debe descargarse una componente que funciona sobre el mismo navegador.

En ambos casos necesitas disponer de un certificado electrónico. En la sección [Navegadores y Ordenador](https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html)podrás encontrar indicaciones sobre cómo instalar tu certificado. Y en la página del [DNIe Electrónico](http://www.dnielectronico.es/)encontrarás un apartado sobre la instalación del lector del DNIe y su uso.

## ¿Qué utilidad práctica tiene la firma electrónica?.

Aporta tres características en la comunicación por Internet: identificación del firmante, integridad de los datos y no repudio.

Pero a parte de eso, las aplicaciones prácticas de la misma son muchas y variadas.

En general están orientadas a realizar operaciones por Internet que en la vida cotidiana requieren de una firma para validarlas.

Algunos ejemplos de operaciones que se pueden realizar actualmente haciendo uso de la firma digital son:

* Realización de la Declaración de la Renta a través de Internet.
* Solicitudes en los registros electrónicos administrativos
* Petición de la vida laboral.
* Recepción de notificaciones electrónicas.
* Firma de correos electrónicos.
* Firma de facturas electrónicas.

## ¿Cómo puedo verificar un documento firmado?

Si recibimos un documento firmado nos interesa validar la firma, es decir, comprobar que los datos firmados se corresponden con los originales, que el certificado con el que se ha firmado es válido y que la estructura del fichero es correcta.

¿Como sabemos si una firma es válida?

Podemos comprobar la validez de la firma de un documento, ver quien es el firmante y el documento firmado en VALIDe.

# Base legal de la Firma Electrónica.

## Legislación aplicable

La firma electrónica se regula en nuestro ordenamiento jurídico mediante la aplicación de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza y el Reglamento (UE) Nº 910/2014 del Parlamento Europeo y del Consejo, de 23 de julio de 2014 (eIDAS), relativo a la identificación electrónica y los servicios de confianza en las transacciones electrónicas en el mercado interior y por el que se deroga la Directiva 1999/93/CE.

Debemos destacar que la reciente Ley 6/2020 ha derogado la Ley 59/2003, de 19 de diciembre, de firma electrónica, y con ella aquellos preceptos incompatibles con el Reglamento eIDAS que es de aplicación directa, evitando así la existencia de vacíos normativos susceptibles de dar lugar a situaciones de inseguridad jurídica en la prestación de servicios electrónicos de confianza.

## La Firma Electrónica Cualificada

Establece el artículo 3 del Reglamento eIDAS sobre definiciones que:

12) «firma electrónica cualificada», una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica;

La firma electrónica cualificada es aquella que se realiza con un certificado cualificado que es definido por el Reglamento como:

 un certificado de firma electrónica, que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I;

La firma electrónica cualificada **comparte todas las características de la firma electrónica avanzada**, al estar vinculada al firmante de forma única e intransferible y ligada al documento de tal manera que no pueda alterarse posteriormente, pero se diferencia en que esta tiene que ser creada por un certificado electrónico que valida la identificación del firmante de forma inequívoca y que debe ser expedido por una Autoridad de certificación, lo que repercute en que sea un método muy seguro y completo.

Firma electrónica avanzada

Recoge el artículo 3 del Reglamento eIDAS sobre definiciones que:

11) «firma electrónica avanzada», la firma electrónica que cumple los requisitos contemplados en el artículo 26;

​Los requisitos para este tipo de firma según el artículo 26 del reglamento serían:

* a) estar vinculada al firmante de manera única;
* b) permitir la identificación del firmante;
* c) haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo,
* d) estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.

La firma electrónica avanzada presenta un mayor nivel de seguridad, ya que, permite identificar al firmante de forma única con el documento electrónico, y el posterior registro de firma y aceptación por parte del mismo, con el fin de evitar cualquier modificación posterior sobre el documento.

Firma electrónica Simple

El reglamente EIDAS en su artículo 3 establece:

10) «firma electrónica», los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firma.

Es decir, la firma electrónica simple es aquella que permite identificar digitalmente al firmante con sus datos, pero ofrece un**escaso nivel de seguridad.**

## Política de Firma

Cuando se firman datos, el firmante indica la aceptación de unas condiciones generales y unas condiciones particulares aplicables a aquella firma electrónica mediante la inclusión de un campo firmado, dentro de la firma, que específica una política explícita o implícita.

Si el campo correspondiente a la normativa de firma electrónica está ausente y no se identifica ninguna normativa como aplicable, entonces se puede asumir que la firma ha sido generada o verificada sin ninguna restricción normativa, y en consecuencia, que no se le ha asignado ningún significado concreto legal o contractual. Se trataría de una firma que no especifica de forma expresa ninguna semántica o significación concreta y, por lo tanto, hará falta derivar el significado de la firma a partir del contexto (y especialmente, de la semántica del documento firmado).

La finalidad de una política de firma es reforzar la confianza en las transacciones electrónicas a través de una serie de condiciones para un contexto dado, el cual puede ser una transacción determinada, un régimen legal o un rol que asuma la parte firmante.

Por ejemplo, la [Política de Firma de la Administración General del Estado (AGE)](http://administracionelectronica.gob.es/es/ctt/politicafirma) especifica las condiciones generales aplicables a la firma electrónica para su validación, en la relación electrónica de la Administración General del Estado con los ciudadanos y entre los órganos y entidades de la AGE.

Según el artículo 24 del Real Decreto 1671/2009 por el que se desarrolla parcialmente la Ley 11/2007 de Acceso Electrónico de los Ciudadanos a los Servicios Públicos, la política de firma electrónica y certificados en el ámbito de la Administración General del Estado y de sus organismos públicos, está constituída por las directrices y normas técnicas aplicables a la utilización de certificados y firma electrónica dentro de su ámbito de aplicación.

## Esquema Nacional de Interoperabilidad (ENI)

La política de firma tiene una misión importante ya que define las reglas y obligaciones de todos los actores involucrados en el proceso de firma en determinados contextos (contractual, jurídico, legal,…).

El Real Decreto 4/2010 por el que se regula el Esquema Nacional de Interoperabilidad establece que la política de firma electrónica y de certificados de la Administración General del Estado, servirá de marco general de interoperabilidad para la autenticación y el reconocimiento mutuo de firmas electrónicas dentro de su ámbito de actuación. También establece que dicha política podrá ser utilizada como referencia por otras Administraciones Públicas para definir las políticas de certificados y firmas a reconocer dentro de sus ámbitos competenciales.

## Esquema Nacional de Seguridad (ENS)

El Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, tiene por objeto el establecimiento de los principios y requisitos de una **política de seguridad** protección de la información.

Pues bien, el decreto, en su artículo 33 también relega a la Política de Firma toda la función de concretar los procesos de generación, validación y conservación de firmas electrónicas, así como las características y requisitos exigibles a los sistemas de firma electrónica, los certificados, los servicios de sellado de tiempo, y otros elementos de soporte de las firmas.

Por otra parte, el RD en su anexo II punto 5.7.4 es muy específico sobre los tipos de firma que deben aplicarse en función del nivel de la información que debe protegerse.

* Nivel BAJO

Se puede emplear cualquier medio de firma electrónica de los previstos en la legislación vigente.

* Nivel MEDIO

Los medios utilizados en la firma electrónica serán proporcionados a la calificación de la información tratada. En todo caso:

Se emplearán algoritmos acreditados por el Centro Criptológico Nacional.

* + Se emplearán, preferentemente, certificados reconocidos.
  + Se emplearán dispositivos seguros de firma.

Se garantizará la **verificación y validación** de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, sin perjuicio de que se pueda ampliar este período de acuerdo con lo que establezca la política de firma electrónica y de certificados que sea de aplicación. Para tal fin:

* + Se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación.
  + Se protegerán la firma y la información mencionada en el apartado anterior con un **sello de tiempo**.
  + El organismo que recabe documentos firmados por el administrado verificará y validará la firma recibida en el momento de la recepción, anexando o referenciando sin ambigüedad la información descrita en los epígrafes a) y b).
  + La firma electrónica de documentos por parte de la Administración anexará o referenciará sin ambigüedad la información descrita en los epígrafes a) y b).
* Nivel ALTO

Se aplicarán las medidas de seguridad referentes a firma electrónica exigibles en el nivel Medio, además de las siguientes:

* + Se usarán certificados reconocidos.
  + Se usarán dispositivos seguros de creación de firma.
  + Se emplearán, preferentemente, productos certificados [op.pl.5].

La norma CCN-STIC-807 del Centro Criptológico Nacional establece en el punto 5.7 cuáles son los mecanismos y algoritmos que se pueden utilizar para firmar en función del nivel de la información.

## Notas Normativas Adicionales

* Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza
* El reglamento europeo 910/2014, de 23 de julio, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior y por la que se deroga la Directiva 1999/93/CE, establece la obligación de validar certificados electrónicos emitidos por cualquier Prestador de Servicios de Confianza europeo.
* La normativa de desarrollo del reglamento eIDAS, Decisión de Ejecución (UE) 2015/1506 de la Comisión de 8 de septiembre de 2015 por la que se establecen las especificaciones relativas a los formatos de las firmas electrónicas avanzadas y los sellos avanzados que deben reconocer los organismos del sector público de conformidad con los artículos 27, apartado 5, y 37, apartado 5, del Reglamento 910/2014, establece que los Estados miembros deben fijar los medios técnicos necesarios que les permitan procesar los documentos firmados electrónicamente que son necesarios cuando se utiliza un servicio en línea ofrecido por, o en nombre de, un organismo del sector público. Para ello define una serie de formatos de firma electrónica avanzada que deben admitir técnicamente los Estados miembros cuando se necesiten firmas electrónicas avanzadas para un procedimiento administrativo en línea.
* Por otro lado, el Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica expone en su artículo 22.4 que los aspectos relativos a la firma electrónica en la conservación del documento electrónico se establecerán en la Política de firma electrónica y de certificados, y a través del uso de formatos de firma longeva que preserven la conservación de las firmas a lo largo del tiempo.
* La preservación de las firmas longevas a lo largo del tiempo se concreta en la Resolución de 19 de julio de 2011, de la Secretaría de Estado para la Función Pública, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma Electrónica y de certificados de la Administración, en el apartado II.7 relativo al Archivado y custodia, que establece que para garantizar la fiabilidad de una firma electrónica a lo largo del tiempo, se podrán utilizar: Firmas longevas mediante las que se añadirá información del estado del certificado asociado, incorporando un sello de tiempo, así como los certificados que conforman la cadena de confianza.
* El sello de tiempo es una parte indispensable de la firma electrónica, sobre todo en el caso de las firmas longevas, que necesiten ser validadas mucho tiempo después de su generación.
* Así mismo el Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en ANEXO II de Medidas de seguridad, en el apartado 5.7.4 relativo a la firma electrónica, especifica que para los sistemas clasificados de nivel medio en las dimensiones de integridad y autenticidad, se garantizará la verificación y validación de la firma electrónica durante el tiempo requerido por la actividad administrativa que aquélla soporte, para lo cual se adjuntará a la firma, o se referenciará, toda la información pertinente para su verificación y validación, y se protegerán la firma y la información mencionada en el apartado anterior con un sello de tiempo.

# Los Certificados Electrónicos.

## Un Certificado Electrónico…

* Es un documento electrónico expedido por una **Autoridad de Certificación e identifica a una persona**(física o jurídica) con un **par de claves**.
* Tiene como misión **validar y certificar**que una firma electrónica se corresponde con una persona o entidad concreta.
* Contiene la información necesaria para firmar electrónicamente e **identificar**a su propietario con sus datos: **nombre, NIF, algoritmo y claves de firma, fecha de expiración y organismo que lo expide**.
* La **Autoridad de Certificación da fe** de que la firma electrónica se corresponde con un **usuario concreto**. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación.

## Las claves digitales.

En un Certificado, las claves digitales son los **elementos esenciales para la firma e identificación**del firmante. Existen dos claves, la **clave privada**y **clave pública**, y trabajan de forma complementaria. Lo que cifra o codifica una clave sólo lo puede descifrar o decodificar la otra.

La diferencia entre ellas es que la clave privada está pensada para que nunca salga del certificado y esté siempre bajo el control del firmante. En cambio, la clave pública se puede repartir o enviar a otros usuarios.

En ocasiones, se habla de **Certificado Privado**para referirse al certificado que contiene la clave privada y la pública y del **Certificado Público**para referirse al certificado que sólo contiene la clave pública.

**Importante**: Si envías tu certificado a un tercero, asegúrate de que es el certificado público (que contiene sólo la clave pública). Para más información sobre cómo exportar un certificado, ve a la sección [Navegadores y Ordenador.](https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html)

## Obtención del Certificado.

|  |  |
| --- | --- |
| Prestadores | Lista de PSC donde puedes obtener el certificado |

Obtener el Certificado Digital depende de si el certificado está contenido en una tarjeta, como el DNIe, o de si el certificado se guarda en un fichero software.

En ambos procesos hay un paso que es la identificación del responsable o usuario del certificado, lo cual requiere que éste se persone en las oficinas de una Autoridad de Registro. Estas oficinas corroboran la identidad.

En el caso de los certificados software, el propio navegador del usuario crea las claves. Pero, en el Certificado de tarjeta, quien crea e introduce las claves es el Proveedor de Certificación.

* Obtención de Certificado en tarjeta (DNIe)

Los certificados contenidos en tarjetas deben ser entregados directamente al usuario.

En el caso concreto del DNIe, hay que personarse en las oficinas de la Dirección General de Policía, que es la Autoridad Certificadora. En la sección del DNI Electrónico puedes ver los pasos concretos para su obtención.

* Solicitud de certificado software.

La solicitud y descarga del Certificado se realizan desde el navegador.

Se puede encontrar un listado de Prestadores de Certificación en esta [página](https://sedeaplicaciones.minetur.gob.es/Prestadores/).

**Nota Importante:**Debes utilizar el **mismo navegador**durante todo el proceso, desde la solicitud hasta la descarga final del certificado.

## Renovación del Certificado.

Los Certificados electrónicos tienen un periodo de validez pasado el cual no sirven para firmar ni tampoco para identificarse.

Cada Proveedor de Certificación establece unos plazos antes de que el certificado caduque para poder renovarlo sin necesidad de otra identificación. En el caso de los certificados de la FNMT, tienen una validez de **36 meses** y se puede renovar durante los 2 meses anteriores a su caducidad.

**Nota importante:**  
Todo el **proceso de renovación de un certificado**, desde la solicitud de renovación hasta la descarga final, se ha de realizar desde el mismo **navegador** en el que está instalado.

Los Certificados incluidos en la tarjeta de **DNIe** tienen una validez de **30 meses** (aunque la tarjeta del DNIe puede tener una validez de hasta 10 años dependiendo de la edad de la persona). Aquí encontrarás más información sobre [cómo renovar los Certificados de tu DNIe.](https://firmaelectronica.gob.es/Home/Ciudadanos/DNI-Electronico.html)

Si el Certificado caduca hay que volver a realizar todo el proceso de solicitud del certificado. Sin embargo, un certificado se puede renovar antes de que caduque y el proceso no requiere una solicitud nueva.

Puedes ver si tu certificado está caducado utilizando el servicio [VALIDe](http://valide.redsara.es/" \t "_blank) del Ministerio de Hacienda y Administraciones Públicas.  
También puedes comprobarlo directamente en tu navegador, en el menú de opciones o herramientas. En la sección de la web [Navegadores y ordenador](https://firmaelectronica.gob.es/Home/Ciudadanos/Navegadores-Ordenador.html) te contamos cómo.

## Revocación de un Certificado.

Puedes **invalidar tu Certificado**antes de que caduque por razones de seguridad.

Estas son las principales causas de revocación de un Certificado:

* Solicitud voluntaria del Suscriptor.
* Pérdida o daños en el soporte del Certificado.
* Fallecimiento del suscriptor o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
* Finalización de la representación o extinción de la entidad representada.
* Inexactitudes en los datos aportados por el suscriptor para la obtención del certificado.
* Que se detecte que las claves del Suscriptor o de la Autoridad de Certificación han sido comprometidas.
* Una vez revocado, el certificado ya no puede ser reactivado y es necesario volver a iniciar todo el [proceso de solicitud](https://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html#obtencion_certificado).

Para revocar los Certificados, deberá ser la propia Autoridad de Certificación la que proporcione el procedimiento, que normalmente está publicado en su página web.

Por ejemplo, la revocación de un certificado emitido por la Fábrica Nacional de Moneda y Timbre (FNMT) puede realizarse de tres formas:

* A través de **Internet**: si el titular del certificado o su representante, en caso de entidades, están en posesión del mismo.
* En la **Oficina de Acreditación**: si el titular del certificado o representante no disponen del mismo por extravío, pérdida o robo, deberá personarse en una de estas Oficinas de Acreditación para, una vez identificado, firmar el modelo de solicitud de revocación del certificado. Las Oficinas de Acreditación transmiten diariamente los registros tramitados a la FNMT para que ésta proceda a la revocación del certificado.
* **Por teléfono: 902 200 616**. Esta opción únicamente deberá utilizarse en aquellos casos en que no pudieras desplazarte a una Oficina de Acreditación o no fuera posible revocar el certificado de manera online.

En el caso del **DNIe**, debes presentarte en cualquier **Oficina de Expedición**del DNIe para revocar el Certificado. La revocación es **inmediata**a la tramitación de cada solicitud verificada como válida.

# Aplicaciones de Firma.

## Las Aplicaciones de Firma.

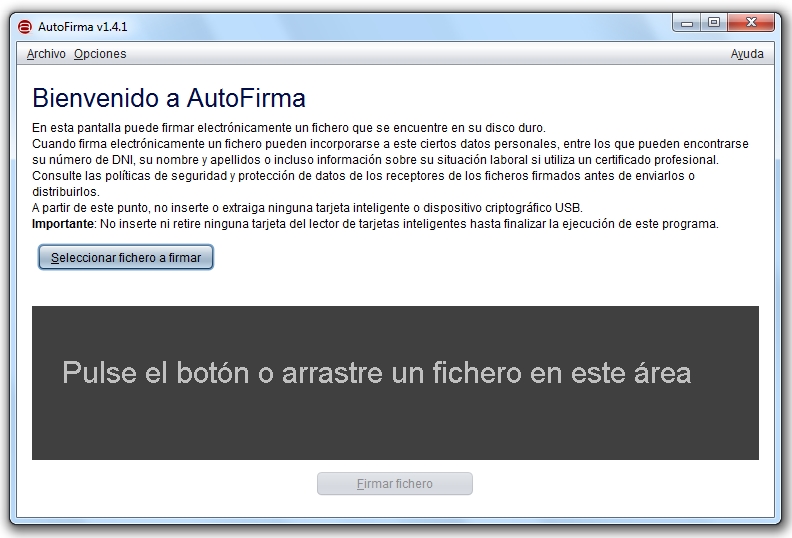
Las aplicaciones de Firma son los programas que permiten firmar un documento electrónico.

* Existen algunos programas de uso cotidiano, por ejemplo, Adobe Acrobat o Microsoft Word, que permiten firmar el mismo documento que se genera. Sin embargo, este tipo de firma tiene dos inconvenientes:
  + No todos los programas que generan documentos son capaces también de firmarlos.
  + En general, el destinatario del documento firmado deberá tener la misma aplicación para ser capaz de verificar la firma.
* Las herramientas o aplicaciones específicas de firma electrónica son capaces de firmar cualquier tipo de documento electrónico y ayudan a superar los inconvenientes anteriores. Además se pueden descargar gratuitamente.

La aplicación AutoFirma, ofrecida por la Administración Pública, te ayudará a firmar documentos.

## AutoFirma

Autofirma es una aplicación de firma realizada por el Ministerio de Hacienda y Administraciones Públicas. Su principal objetivo es ofrecer al usuario un sistema de firma en el que éste pueda firmar cualquier tipo de documento de manera sencilla. El usuario indica qué fichero quiere firmar y la **aplicación escoge automáticamente el formato de firma qué debe aplicar**, liberando así, al usuario de cualquier duda técnica.



Descargar[Descarga AutoFirma](http://firmaelectronica.gob.es/Home/Descargas.html)

## VALIDe

VALIDe (Aplicación de Validación de firma y certificados Online de @firma) es la plataforma de validación que la Administración General del Estado pone a disposición de las Administraciones y de los ciudadanos para la validación de certificados y, además, ofrece los siguientes servicios:

* Validación de firmas electrónicas
* Generación de firmas electrónicas en múltiples formatos
* Visualización de firmas con la ayuda del Visor

