GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

Guía para la utilización de la firma electrónica en la empresa

INSTITUTO NACIONAL DE CIBERSEGURIDAD

INDICE

1 Introducción

Hoy en día la actividad de una empresa se desenvuelve cada vez más dentro de un mundo electrónico, al cual se están traspasando actividades que habitualmente se realizaban dentro de un mundo físico. Esta nueva situación afecta a todos los ámbitos de la empresa y son necesarias herramientas tecnológicas, legislativas, normativas u organizativas que hagan posible realizar esas actividades en el mundo electrónico con al menos con las mismas garantías, funcionalidades y seguridad que en el mundo físico.

Ejemplos de actividades son:

- Descarga de documentos electrónicos, impresión, rellenado y posterior entrega a la administración correspondiente.
- Rellenado de un formulario y, a continuación, envío directamente a través de la web.
- Uso del correo electrónico tanto para solicitar como para enviar información o recibirla.
- Envío de información y en paralelo envío de un documento firmado de nuestro puño y letra mediante correo postal o entrega en persona.
- Adquisición de un producto o servicio en la que se nos solicita la firma de un contrato.

Para que esto sea posible es necesaria una herramienta que permita que cualquier trámite pueda ser llevado a cabo de forma completamente electrónica. Esta nueva herramienta es la firma electrónica.

La firma incluye tanto procedimientos técnicos para la realización de una **firma digital** como cuestiones organizativas y un marco legislativo que le da validez jurídica. Su conjunto es lo que llamamos **firma electrónica**.

La realización de trámites electrónicos con seguridad requiere solventar necesidades como:

- Identificar a los firmantes. Poder conocer el origen de una firma.
- Asegurar la integridad de los documentos. Asegurar que los documentos que intervienen en un trámite no han sido modificados, y en caso de que lo hayan sido poder detectarlo.
- No repudio. Asegurar que los participantes en una transacción no puedan negar haberla realizado.
- Confidencialidad en las comunicaciones. Poder comunicarnos con la confianza de que tan sólo participantes legítimos tienen acceso a ellas.
- Identificar a los participantes. Poder identificar a todos los participantes en las comunicaciones.

El presente documento pretende mostrar cómo la firma electrónica permite proporcionar las características necesarias para la tramitación electrónica segura.

2 Definición de firma electrónica

Sin entrar en formalismos una firma electrónica puede ser:

- Firma con un lápiz electrónico al usar una tarjeta de crédito o débito en una tienda.
- Marcar una casilla en una computadora, a máquina o aplicada con el ratón o con el dedo en una pantalla táctil.
- Usar una firma digital (mecanismo criptográfico de firma).
- Usar usuario y contraseña.
- Usar una tarjeta de coordenadas.

Todas ellas tienen su validez dependiendo del ámbito en que se apliquen. Pero si lo que se pretende es obtener una firma con una validez legal equivalente a la firma manuscrita necesitamos una legislación que establezca qué se entiende por firma electrónica y cuáles son los criterios que deberá cumplir dicha firma electrónica.

2.1 Marco legislativo

El 1 de enero de 2010 entró en vigor la Ley 11/2007, de 22 de Junio, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) garantizado a los ciudadanos, al menos desde el punto de vista jurídico, poder realizar todas sus gestiones por medios electrónicos. Esta ley pretende el impulso la Administración Electrónica y da soporte a la firma electrónica junto a otras leyes más específicas como:

- Ley 59/2003, de 19 de Diciembre , de Firma Electrónica.
- Ley 56/2007, de 28 de Diciembre, de Medidas de Impulso de la Sociedad de la Información.
- Directiva 199/93/CE del parlamento europeo por la que se establece un marco comunitario para la firma electrónica.

2.2 Definición

La definición de **firma electrónica** la proporcionala Ley 59/2003, de 13 de diciembre, de firma electrónica.

Primero define lo que se entiende por firma electrónica. Unos datos que nos permiten identificar a un firmante.

> *(Art. 3.1)* ***La 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.*

En el siguiente paso presenta la firma electrónica avanzada. Un tipo concreto de firma que se ha creado de una forma específica y permite detectar si el documento firmado ha sido modificado posteriormente.

> *(Art. 3.2) La* ***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.*

Finalmente presenta la firma electrónica reconocida. Una firma electrónica avanzada creada con determinas medidas de seguridad y usando un tipo de certificado electrónico concreto.

> *(Art. 3.3) Se considera* ***firma electrónica reconocida*** *la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.*

Es a la firma electrónica reconocida a la que se le da el mismo valor que la firma manuscrita.

> *(Art. 3.4) 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.*

Por tanto la firma electrónica reconocida la tiene el soporte legislativo completo que buscamos en nuestras tramitaciones electrónicas. Aun así la ley no elimina la validez jurídica que otros tipos de firma electrónica puedan tener, los cuales son útiles dentro de ámbitos específicos.

3 Necesidades de la tramitación electrónica

La realización de trámites electrónicos con seguridad requiere solventar necesidades que la firma electrónica viene a solucionar.

3.1 Confidencialidad de las comunicaciones

Tener la confianza de que nuestras comunicaciones son confidenciales y sólo tienen a acceso a ellas las personas autorizadas es una propiedad interesante para nuestros trámites electrónicos. En algunos de nuestros trámites no es imprescindible y podemos realizarlos sin preocuparnos si alguien está curioseando en nuestras actividades. Pero en otras ocasiones es vital para nosotros tener la seguridad de que sólo los destinatarios legítimos van a tener acceso a la información.

Para solucionar esta necesidad se hace uso de herramientas como el **cifrado**. El cifrado es un conjunto de algoritmos y herramientas matemáticas que nos permiten ocultar o proteger información que sólo queremos que conozcan aquellos que intervienen en una comunicación.

En concreto se usa **el cifrado simétrico**, en el cual los participantes en la comunicación comparten una única clave. Los poseedores de esta clave son los únicos que pueden cifrar o descifrar la información.

3.2 Identificación

La existencia de las claves de cifrado nos permite identificar a los participantes en un trámite. El hecho de que solamente los poseedores de la clave son capaces de haber realizado el cifrado les identifica como autores.

Pero la existencia de esta clave presenta problemas como:

- Con una sola clave no está resuelta la identificación de los participantes, es necesario una clave diferente para cada par participantes, lo que supone la creación de una gran cantidad de claves.
- El reparto de claves. Las claves se han de repartir a los participantes, este reparto es un momento delicado que puede ser aprovechado para el robo de las claves. Esta situación se agrava cuando hay un gran número de claves que es necesario repartir.

Un nuevo tipo de cifrado, el **cifrado asimétrico**, viene a solventar estos problemas. Cada participante tiene su propio par de claves, una privada que tan solo posee él, y una pública que se deja a disposición de todo el mundo.

Estas claves se caracterizan por:

- Un mensaje codificado con la clave privada tan solo puede ser descifrado con la clave pública.
- Un mensaje codificado con la clave pública tan solo puede ser descifrado con la clave privada.

Por tanto, gracias al cifrado asimétrico:

- Al recibir un mensaje cifrado tenemos garantía de que sólo el poseedor de la clave privada ha podido ser su creador.
- Cualquiera puede realizar esta verificación ya que la clave pública está disponible públicamente.

Este sistema resuelve:

- La identificación de los participantes ya que los poseedores de las claves privadas son identificados de manera única.
- Simplifica el reparto de claves ya que se ha de entregar tan solo un par de claves a cada participante.

Esta herramienta del cifrado asimétrico es la escogida para la creación de firmas electrónicas.

Vemos así que una herramienta matemática como el cifrado nos ayuda a resolver la necesidad de identificación que vemos explícitamente indicada en la ley.

> *(Art. 3.1) La 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****.*

> *(Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite **identificar al firmante** (...) que está vinculada al firmante de manera única y a los datos a que se refiere.*

3.2.1 Certificado electrónico

En el proceso de identificación es necesaria una nueva herramienta, el **certificado electrónico**. Un documento que vincula una clave con una identidad y de esta manera nos ayuda a identificar quien es el poseedor de esa clave.

> *(Art. 6.1) Un **certificado electrónico** es un documento firmado electrónicamente por un **prestador de servicios de certificación** que vincula unos datos de verificación de firma a un firmante y confirma su identidad.*

Vemos que un certificado electrónico es un documento electrónico que incorpora datos relativos a la identidad de un tercero físico (persona) o de una entidad jurídica (empresa, organización, etc.) con estas propiedades:

- El certificado electrónico permite asociar una identidad durante el proceso de firma, de forma que podemos asociar los datos de identidad que incorpora el certificado a la firma electrónica resultante.
- Los certificados electrónicos generalmente son emitidos por un tercero de confianza, una organización acreditada para creación de este tipo de documento.
- Puede incorporar más información que la relativa a la identidad del titular, como su cargo, los poderes que le han sido otorgados para la firma con ese certificado electrónico, etc. Esta información permite personalizar y crear distintos tipos de certificados electrónicos.
- Modificando algunos elementos de la propia estructura del certificado es posible también construir certificados para propósitos específicos.

3.2.2 Tercero de confianza

El proceso de identificación necesita una nueva figura, el **tercero de confianza**, una organización independiente que está acreditada y certificada para emitir **certificados electrónicos.**

A pesar de que el uso de criptografía asimétrica y de los certificados electrónicos asegura la identificación de los participantes, no garantiza que se evite la suplantación de identidades. El que alguien nos haya proporcionado un certificado no nos da la seguridad de que éste corresponda a la persona que dice ser.

Podemos estar seguros de la identidad que asociada a un certificado electrónico tan solo en la medida en que confiamos en la organización que lo ha emitido.

3.2.3 Certificado reconocido

Los certificados reconocidos son certificados emitidos por un tercero de confianza que esté acreditado y certificado para emitir certificados de este tipo. Estas entidades deben cumplir con unos requerimientos muy concretos.

Los prestadores de servicios de certificación que emiten certificados electrónicos en el estado español, los podemos encontrar en el Ministerio de Industria, Energía y Turismo.

Volviendo a la ley de firma electrónica, vemos que para realizar una firma electrónica reconocida ésta debe ser realizada con un certificado electrónico **reconocido**.

> *(Art. 3.3) Se considera firma electrónica **reconocida** la firma electrónica avanzada basada en un **certificado reconocido** (...)*

3.3 Asegurar la integridad de los documentos

La firma de un documento no garantiza su posterior integridad. Existen muchas técnicas, herramientas y mecanismos por los que es posible realizar modificaciones en un documento electrónico sin apenas esfuerzo.

La integridad de los documento se consigue gracias a una herramienta matemática, el generador de resúmenes.

Esta herramienta toma un mensaje y genera un resumen de él, una especie de huella dactilar del documento. El resumen se caracteriza por:

- Tiene una longitud fija.
- No existen dos documentos que generen el mismo resumen, cambiar una simple coma en el documento significa obtener un resumen completamente distinto.

Por tanto, al firmar un documento y adjuntar su resumen estamos garantizando la integridad del documento firmado, ya que cualquier modificación posterior del documento será detectada mediante la validación del resumen adjunto.

> *(Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite (...) detectar cualquier* ***cambio ulterior de los datos***

3.4 Garantizar el no repudio

Otra necesidad en nuestros trámites es la garantía de no repudio. El no repudio, también conocido como irrenunciabilidad, consiste en que el emisor no pueda negar haber participado en la comunicación, es decir, no puede negar que ha enviado el mensaje o que ha firmado un documento electrónico.

Es precisamente la firma electrónica la que garantiza el no repudio. Ésta identifica al firmante unívocamente debido a que una firma sólo la puede haber realizado el poseedor de la clave privada asociada a la clave pública que descifra el mensaje.

El emisor no puede negar el haber realizado la firma y cualquiera puede verificar este hecho ya que la clave pública está disponible públicamente.

4 Creación de la firma electrónica

Una firma electrónica reconocida puede crearse prácticamente desde cualquier dispositivo electrónico. Este dispositivo ha de contener las aplicaciones necesarias y tener acceso al certificado digital.

4.1.1 Dispositivo seguro de creación de firma

El proceso de realización de una firma electrónica debe realizarse con las debidas garantías de seguridad. Es decir, no basta que los distintos elementos que intervienen sean seguros por si solos, sino que, además, hace falta que éstos sean combinados durante el proceso de firma de forma segura.

> *(Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un* ***dispositivo seguro de creación de firma****.*

Es por tanto necesario que el dispositivo que se use para realizar la firma cumpla ciertos requisitos de seguridad.

Como ejemplo de este tipo de dispositivos tenemos el DNI electrónico, que cumple con los requisitos que marca la ley. El DNI electrónico está certificado como dispositivo seguro de creación de firma.

4.1.2 Firma electrónica centralizada

Para algunos usuarios la infraestructura necesaria de un dispositivo seguro de creación de firma puede resultar complicada. Una alternativa que puede ganar impulso en el futuro es la firma electrónica centralizada.

En la actualidad hay empresas ofertando servicios de firma electrónica avanzada con almacenamiento centralizado de claves. Esta modalidad de firma implica que el certificado digital se encuentra en los sistemas de una empresa en la cual el cliente ha confiado la custodia del certificado. Para realizar la firma electrónica el cliente accede al sistema mediante algún tipo de identificación y realiza la firma.

De esta manera el usuario se libera de la custodia del certificado digital y la posesión de los dispositivos necesarios para realizar la firma. Tan sólo necesita tener conectividad a los sistemas de la empresa que ha contratado, que puede ser a través de portátil, móvil, tablet…

En este sentido la Administración del Estado ha creado el proyecto Cl@ve. Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos, permitiendo que estos puedan identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

La funcionalidad de firma centralizada se encuentra en la actualidad en fase de desarrollo, y se prevé que esté disponible para su uso por parte de los ciudadanos a lo largo de 2015. DNI-nb (DNI en la nube) será el sistema dentro de Cl@ve que ofrecerá la posibilidad de realizar firma electrónica centralizada.

Los certificados para la firma serán emitidos por la Dirección General de la Policía y custodiados por la Administración. Para poder firmar con ellos bastará únicamente un dispositivo que permita establecer una conexión a internet, no siendo necesarios el uso de elementos periféricos o la descarga de software adicional para su utilización.

5 Tipos de certificado electrónico

Existen distintas formas de clasificar los certificados electrónicos. Indicamos algunas:

- Según el tipo de identidad que incorporan.
- Según el ámbito de aplicación.
- Según el soporte.

5.1 Según el tipo de identidad que incorporan

- Aquellos que incorporan la identidad de tercero físico o ciudadano. Orientado a ciudadanos, es decir, a terceros físicos y están fundamentalmente pensados para trámites personales aunque, en determinadas circunstancias, pueden ser usados en el ámbito profesional.
- Aquellos que incorporan una identidad jurídica. Están pensados para todo tipo de organizaciones, ya sean empresas, administraciones u otro tipo de organizaciones, todas ellas con una identidad de tipo jurídico.

5.2 Según el ámbito de aplicación

- Certificado de servidor. Diseñados para cumplir dos funciones básicas:
  - Conocer la identidad de un sitio web. Es decir, quién o qué organización es la responsable jurídica de la página en cuestión.
  - Cifrar las comunicaciones de forma que se crea un canal seguro de comunicación entre nuestro navegador y el sitio web al cual nos estamos conectando.
- Certificado de código. Cuyo uso o ámbito de aplicación es la firma electrónica de código. Permite garantizar la procedencia de un programa, aplicación o fichero de código y prevenir su alteración o modificación.
- Certificado de cifrado. Mediante este tipo de certificados es posible llevar a cabo el cifrado de información, bien esté almacenada en un ordenador o servidor, un disco duro, etc. o bien sea información que va a ser enviada a través de una red de comunicaciones.
- Certificado de representante. Es emitido a favor de una persona física representante de una determinada entidad. El titular del certificado se identifica no únicamente como persona física perteneciente a una empresa, sino que añade su cualificación como representante legal o apoderado general de la misma.
- Certificado de empleado público. Para empleados y funcionarios de la Administración Pública.
- Certificado de apoderamiento especial. Emitido a los apoderados especiales de una entidad que pueden actuar en nombre y representación de la misma pero para determinados trámites.
- Certificado de facturación electrónica. Su uso está limitado a la firma de facturas electrónicas.
- Certificado de cifrado de contenidos. Cuyo ámbito de aplicación es la protección de los datos mediante el cifrado de información.
- Certificado de sello de empresa. Normalmente asociado a una máquina, identifica a una empresa. Este tipo de certificado puede ser usado de forma automática desasistida por una aplicación.

5.3 Según el soporte

- Certificados software. Cuando obtenemos el certificado, lo que nos entregan es básicamente un pequeño documento, que se puede guardar en una memoria USB, en un ordenador (en el almacén de certificados), en el disco duro, etc.
- Certificados hardware. Existe la posibilidad de que el certificado esté almacenado en una tarjeta criptográfica, que no es más que una tarjeta similar a una tarjeta de crédito pero que incorpora un chip electrónico. Un ejemplo de tarjeta criptográfica es el DNI electrónico. En estas tarjetas es posible almacenar uno o varios certificados electrónicos.

6 Firma nativa / no nativa

A la hora de realizar una firma, existen dos caminos para llevarla a cabo:

- Firma nativa de documentos electrónicos.
- Firma NO nativa de documentos electrónicos.

6.1 Firma nativa

Consiste en realizar el proceso de firma de un documento electrónico con el mismo programa o aplicación con el que fue creado dicho documento.

Esto quiere decir que si estamos elaborando un documento electrónico con Microsoft Word, una vez terminado el documento lo firmaremos electrónicamente también con Microsoft Word. De forma que al final del proceso de firma obtendremos otro documento Microsoft Word pero que llevará incorporada la firma electrónica del documento.

La firma nativa de los documentos electrónicos facilita la labor a la persona que crea el documento puesto que no hace falta utilizar otra herramienta. Sin embargo, esto tiene varios inconvenientes:

- El programa que usemos para generar el documento ha de soportar la firma electrónica, esto no siempre es así.
- Estamos asociando el proceso de firma a un formato de documento específico. Es decir, firmamos con el programa con el que creamos el documento. Pero, ¿qué ocurre si queremos usar otro formato distinto?
- Una vez firmado un documento electrónico, al enviarlo a otra persona, estamos obligando al receptor del documento a disponer del mismo programa, y posiblemente la misma versión, con el que ha sido firmado.

6.2 Firma NO nativa

Para solucionar los problemas con la firma nativa, podemos recurrir a una solución más universal que consiste en usar herramientas de firma electrónica capaces de firmar cualquier tipo de documento.

En este caso lo que se genera es un documento con un formato especial y específico del programa de firma utilizado, dentro del cual está incorporado el documento original y además la firma electrónica del documento.

Trabajar con la firma NO nativa tiene varias ventajas:

- La firma NO nativa no depende de un formato de documento específico, sino que se usan formatos de documento estándar. Las aplicaciones de firma NO nativa son capaces, en principio, de firmar cualquier tipo de documento electrónico, de manera que son independientes del tipo o formato del documento a firmar.
- Existen herramientas de este tipo, que son gratuitas, como la que ofrece el Ministerio de Industria, Energía y Turismo a través de su página web, donde se puede descargar una aplicación de firma no nativa, eCoFirma.
- No es necesario que la persona a la que enviamos el documento firmado electrónicamente disponga de una herramienta concreta. Puede trabajar con cualquier herramienta que soporte el formato de documento que le hemos enviado.

7 Uso de la firma electrónica

Algunos ejemplos de uso de la firma electrónica.

a) Realización de trámites con las distintas administraciones

Gracias al uso de un certificado digital en el que figura la identidad, es posible acceder de forma sencilla y segura a distintos servicios web donde realizar trámites como declaraciones de IVA, altas y bajas de trabajadores, tramitación de diversos impuestos, etc..

Además, gracias al certificado y a su clave privada se pueden firmar digitalmente documentos electrónicos que luego se envían a través de correo electrónico o de la web.

b) Realización de trámites domésticos

La firma electrónica permite realizar sin salir de casa diversos trámites personales. Algunos ejemplos son:

- Trámites con las administraciones, como obtener su vida laboral, pagar sus impuestos, solicitar documentos o certificados, etc.
- Utilizar la banca on-line.
- Compras de bienes a través de Internet.
- Uso de los distintos servicios on-line.

c) Digitalización de documentos

El escaneo certificado de documentos permite convertir un archivo en papel en un archivo totalmente digital con un conjunto de garantías y opciones de seguridad gracias a la firma electrónica.

Se trata de escanear un conjunto de documentos almacenados en un archivo en papel, en formato digital. Por ejemplo, contratos, facturas, nóminas, albaranes, etc. Son documentos que, una vez emitidos en papel y una vez finalizado cierto periodo, pasan a ser guardados para dejar constancia de operaciones, trámites, etc.

Un documento electrónico puede ser alterado de muchas formas y sin demasiada dificultad. En este caso, digitalizar los documentos no es un problema, puesto que un escáner realiza esa labor sin problema. El problema al que nos enfrentamos es evitar que los documentos, una vez escaneados, puedan ser modificados o alterados. Por otro lado, hay que establecer un mecanismo que nos permita verificar que dicho documento ha sido emitido o generado por la empresa.

En este escenario la firma electrónica nos permite firmar digitalmente todos los documentos electrónicos que genera el escáner a partir del documento en papel.

- Al tener el documento firmado, por ejemplo mediante un certificado digital con los datos de la empresa, podemos verificar que efectivamente dicho documento lo ha generado la empresa y no otra.
- La generación del resumen del documento permite verificar que efectivamente ese documento no ha sido alterado una vez que se encuentra en formato electrónico.

d) Facturación electrónica

Una factura electrónica es básicamente un documento en formato electrónico que, una vez generado y almacenado en un fichero electrónico, es firmado electrónicamente.

Este escenario es muy similar a la digitalización de documentos. En el caso de la factura electrónica se genera una factura directamente en formato electrónico, por ejemplo en formato PDF (Portable Document File). A continuación, se firma digitalmente ese documento PDF, con lo que obtenemos un documento del cual podemos verificar quién lo ha emitido gracias a la firma electrónica y, además,

asegurarnos que no ha sido alterado o modificado, gracias también a la firma electrónica (en concreto gracias al generador de resumen).

La diferencia respecto al escenario anterior es básicamente que aquí ya no se genera un documento en papel que luego se digitaliza sino que el propio documento es generado directamente en formato electrónico.

Aplicando este principio es posible firmar electrónicamente cualquier tipo de documento electrónico, no sólo facturas electrónicas sino también contratos electrónicos, albaranes electrónicos, memorandos electrónicos.

e) Firma de código

Es posible firmar el código de aplicaciones software, esto permite:

- La verificación de la autoría de una aplicación o la procedencia de la misma.
- Verificar que la aplicación no ha sido modificada.

Por tanto, antes de enviar un programa a sus clientes, hay empresas que firman digitalmente sus aplicaciones. De esta forma, los clientes pueden verificar su procedencia y autoría y tienen garantizada la integridad del programa que les llega.

f) Acreditar la existencia de un contenido

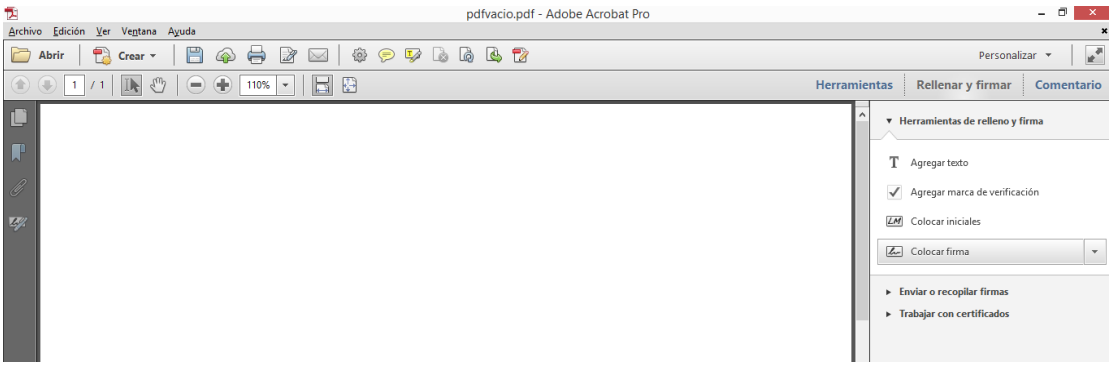
Como ejemplo, el Grupo de Delitos Telemáticos de la Guardia Civil mediante su "Formulario de Información ciudadana" permite informar de forma anónima de una web con contenido ilícito. En el instante que se envía el formulario, mediante la firma electrónica de una organización independiente, se acredita el contenido que en ese momento existía en la web.

8 Casos prácticos de firma de documentos electrónicos

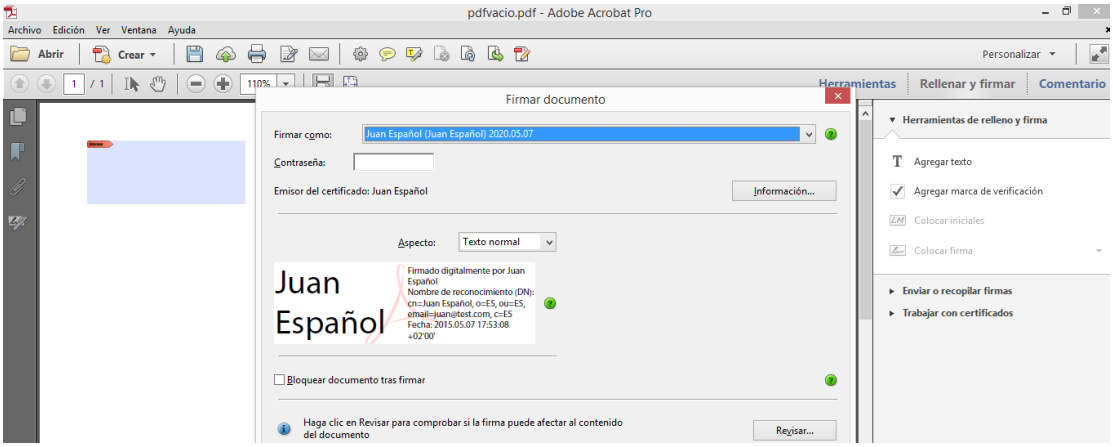
8.1 Firma nativa

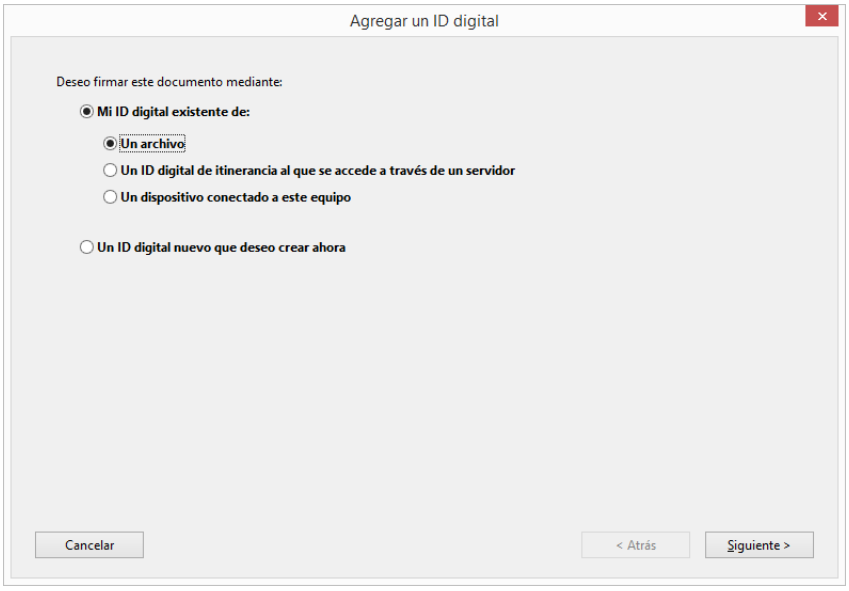
a) Firma de documentos PDF

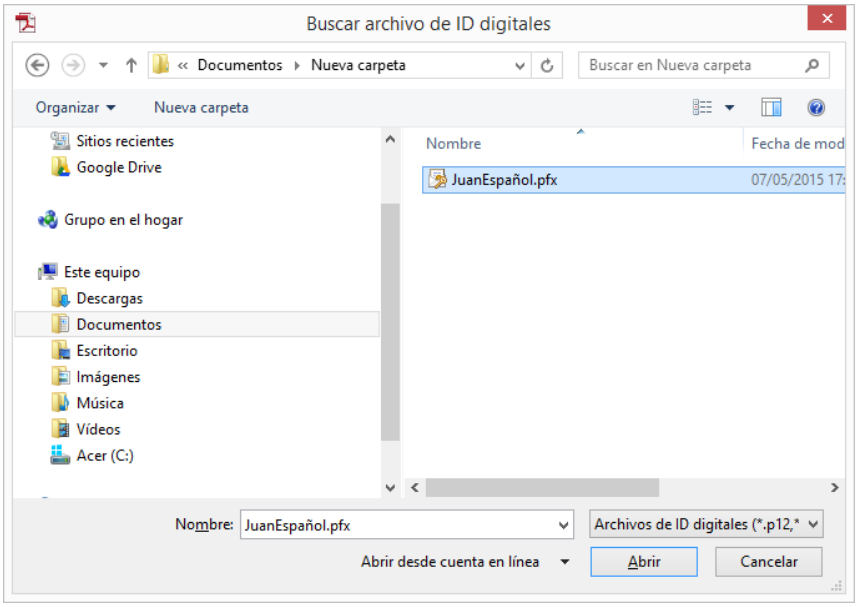
Para firmar un documento PDF necesitamos un editor, por ejemplo Adobe Acrobat. Accedemos a la opción "Colocar firma" en el menú "Rellenar y firmar".



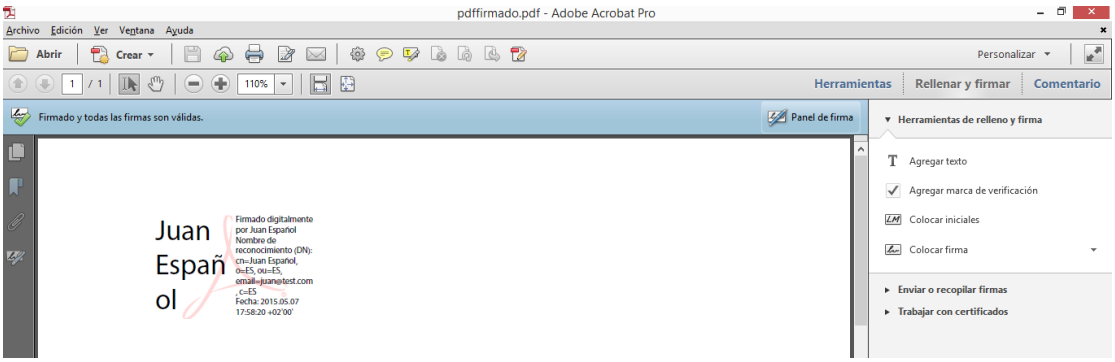
Colocamos el rectángulo de firma sobre el documento, aparece el cuadro de diálogo que nos permite seleccionar el certificado con el que queremos firmar el documento.





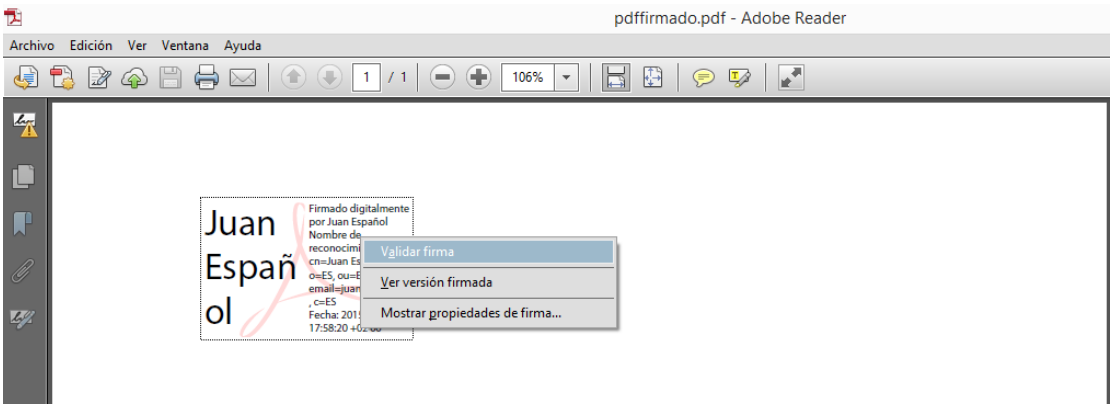


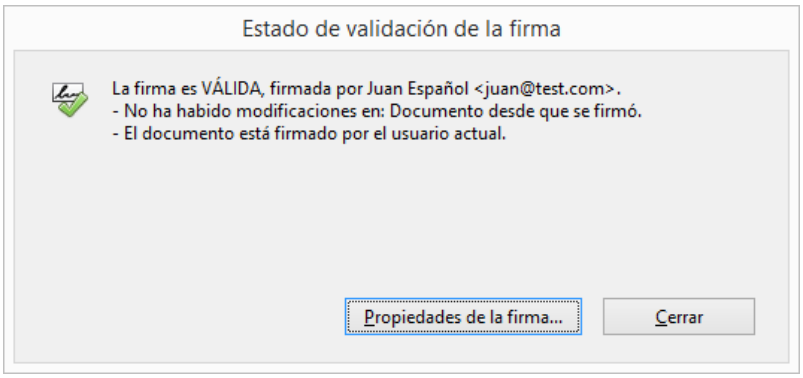
Finalmente obtenemos el documento PDF firmado.



b) Validación de firma de documentos PDF

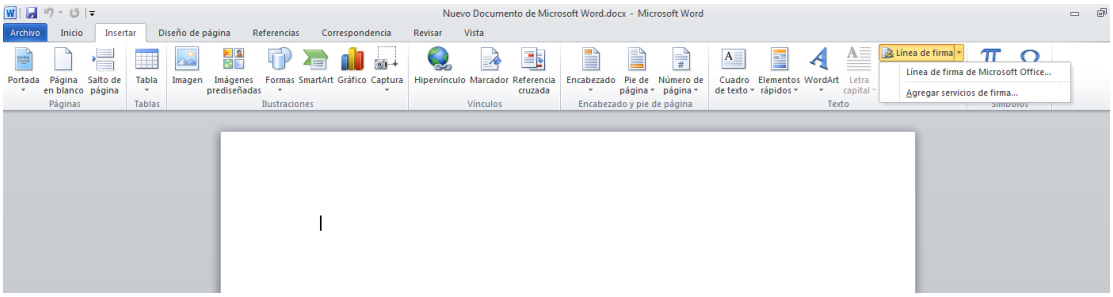
Para leer un documento PDF, típicamente usamos la aplicación Adobe Reader. Esta aplicación permite validar las firmas si el documento ha sido firmado nativamente.



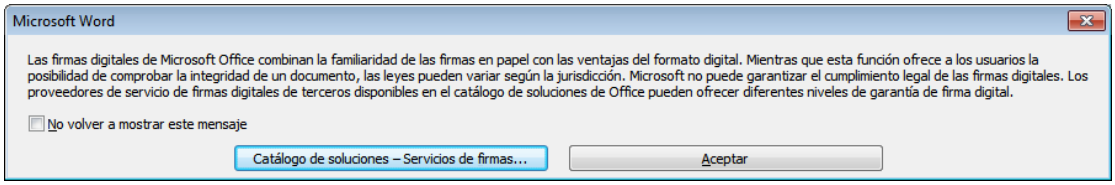


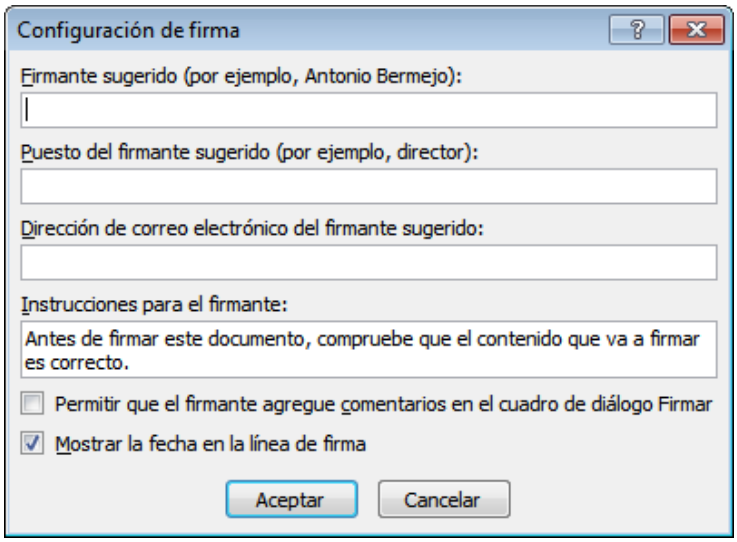
c) Firma de documentos Microsoft Word

Microsoft Word permite firmar digitalmente un documento Word. En la versión 2010 de Word realizamos la firma desde "Línea de firma", dentro de la pestaña "Insertar".

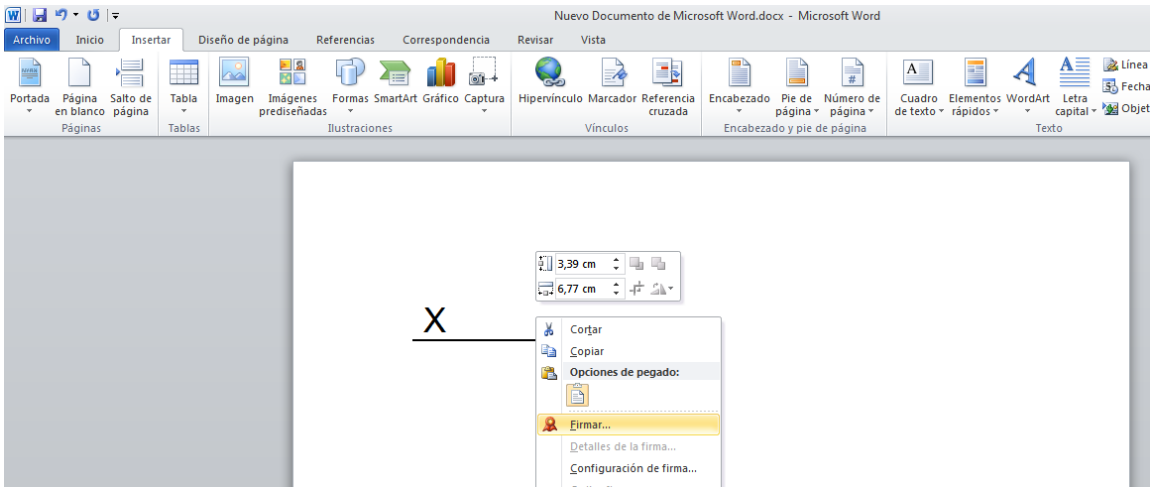


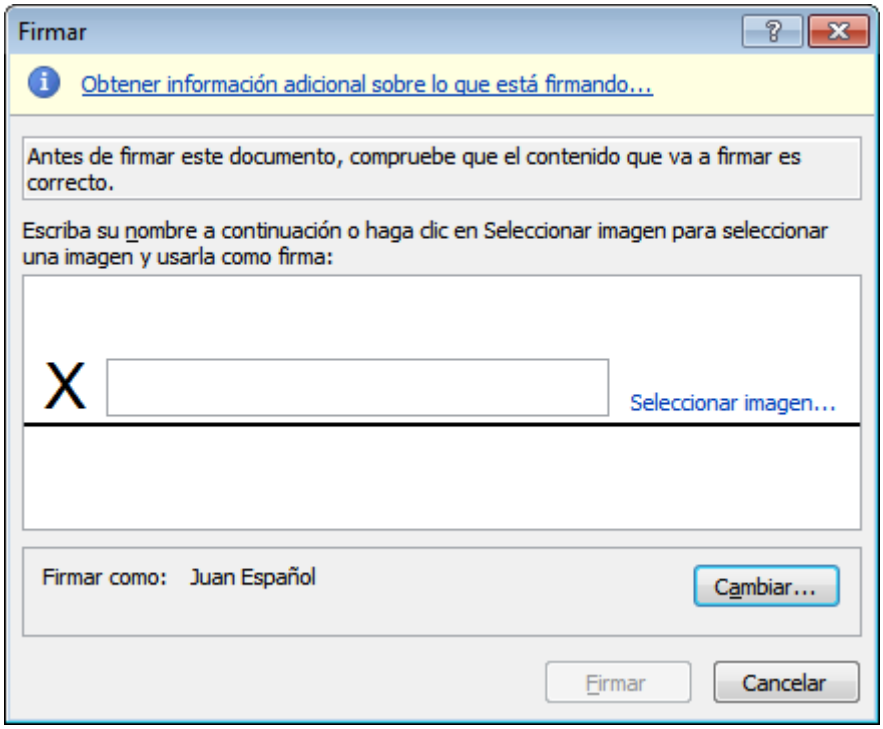
Aparece un mensaje de advertencia sobre las variaciones de la legislación sobre firma electrónica en diferentes países.



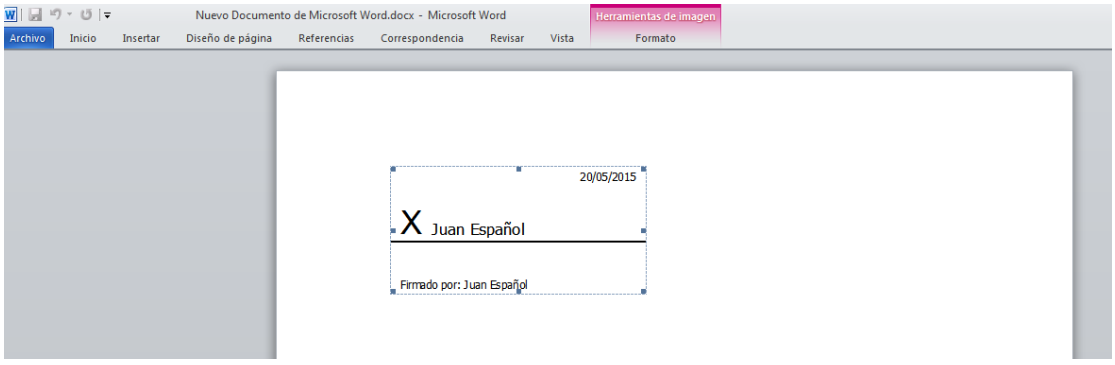


Una vez insertada la línea de firma, la firma se realiza mediante la opción "Firmar".



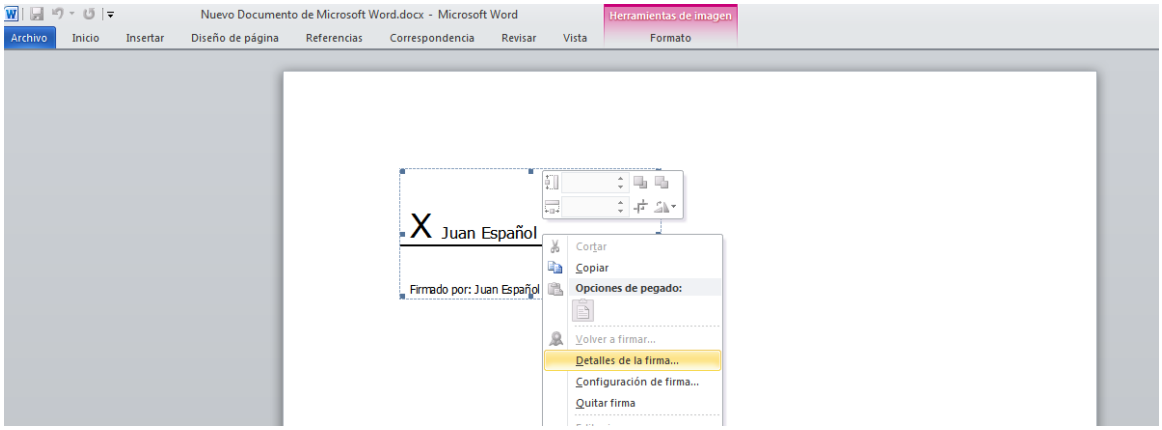


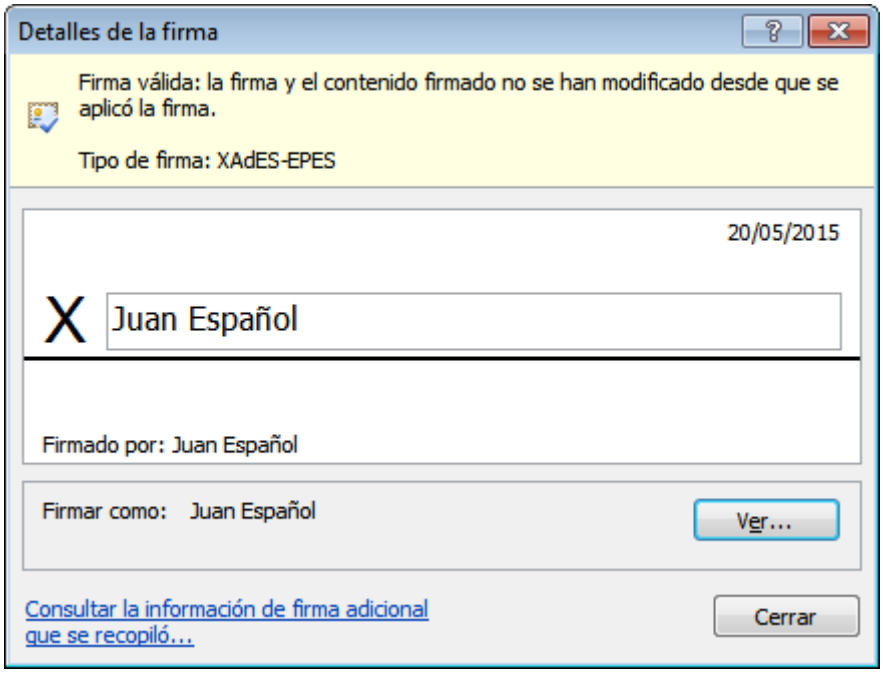
El resultado del proceso de firma aparece dentro del documento.



d) Validación de firma de documentos Microsoft Word

Microsoft Word permite validar la firma del documento mediante la opción "Detalles de firma".





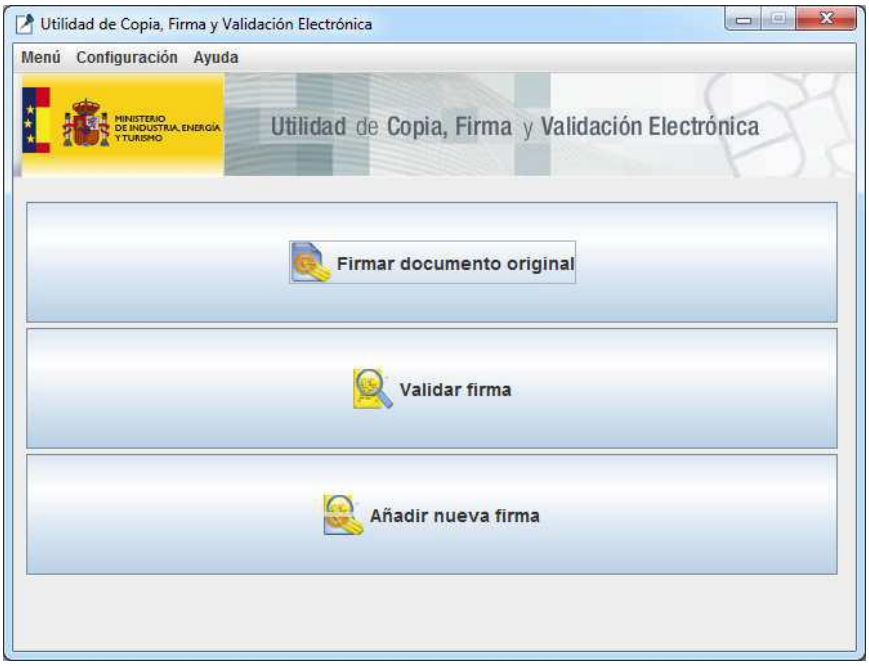
8.2 Firma NO nativa

La Administración del Estado proporciona gratuitamente aplicaciones que permiten firmar un documento con firma NO nativa, como son:

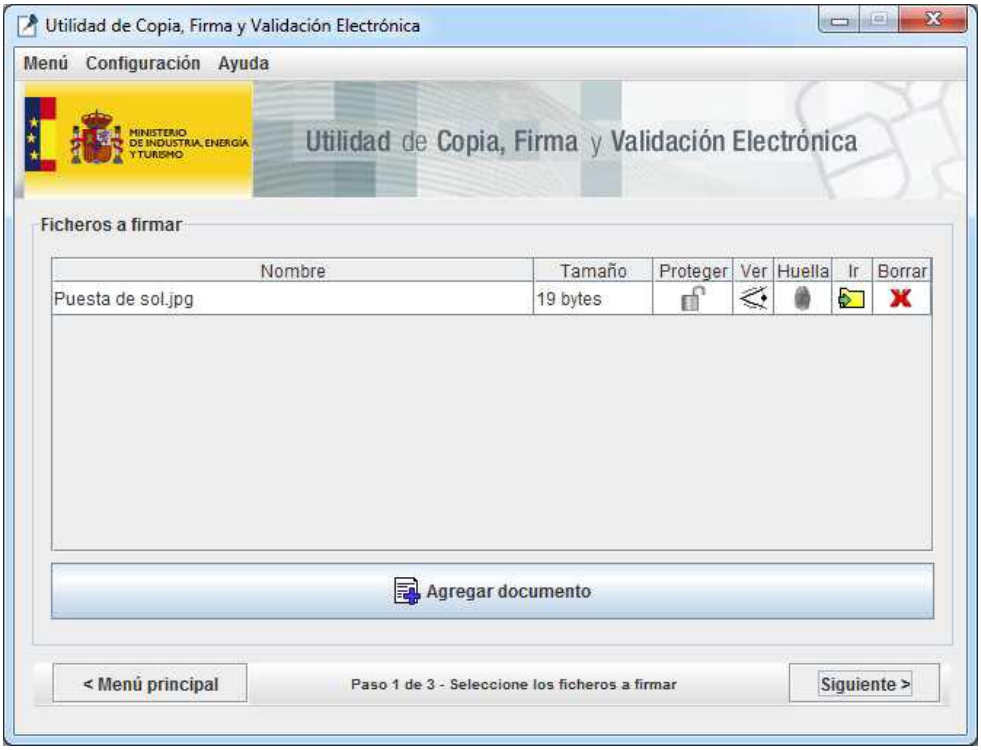
- FirmaFácil.
- @Firma.
- ecoFirma.

Mostramos el uso de ecoFirma, una aplicación creada por el Ministerio de Industria, Energía y Turismo, puesta a disposición de los ciudadanos y de las empresas.

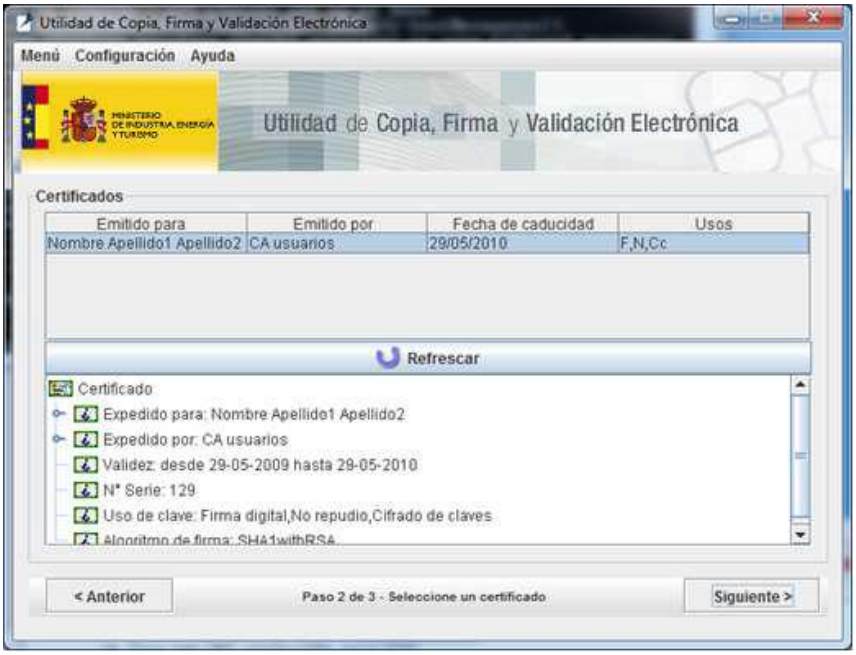
La firma electrónica de un documento se realiza desde el menú principal de la aplicación pulsando en el botón “Firmar documento original”.



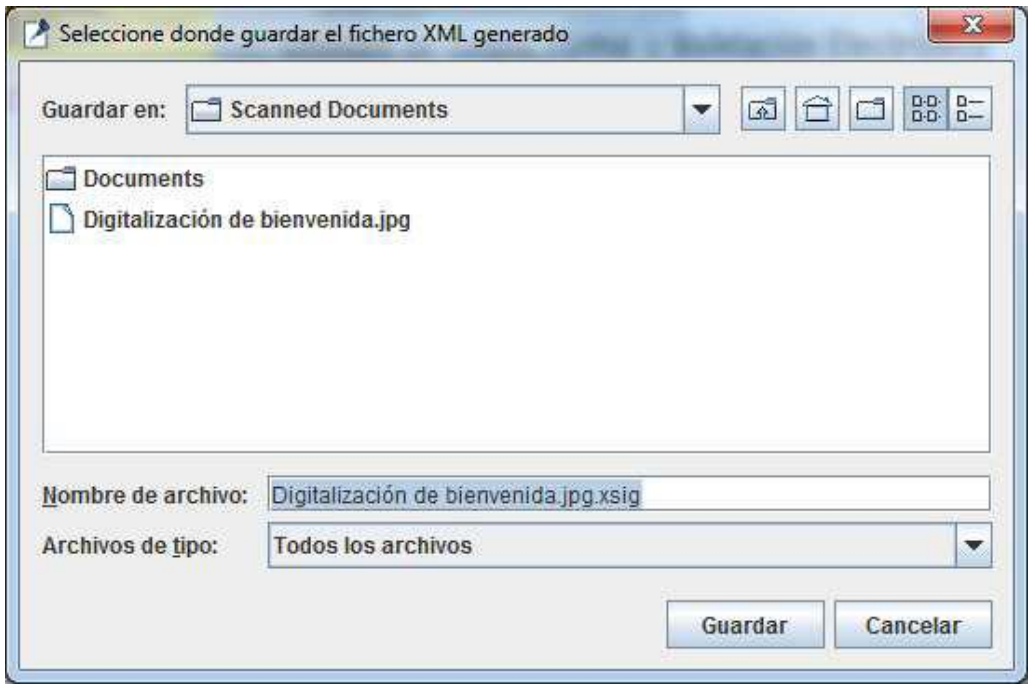
Se selecciona el documento a firmar.



El siguiente paso es seleccionar el certificado con el que vamos a realizar la firma.



Finalmente se indica donde se guardará el documento resultado de la firma.



Una vez finalizada la firma, la aplicación automáticamente presenta una ventana de validación del documento firmado.

El fichero resultante de la firma electrónica, incorpora en su interior dos cosas:

- El documento original.
- La firma electrónica del documento.

9 Conclusiones

En el presente documento se han repasado tanto aspectos teóricos como prácticos de la firma electrónica. Haciendo hincapié en las posibilidades que la firma electrónica abre y las necesidades que viene a solventar.

Hemos visto que tenemos disponibles una infraestructura técnica y legal y una serie de herramientas que tanto empresas privadas como administraciones públicas ponen a nuestra disposición.

La adopción de la firma electrónica no es una cuestión cerrada, nuevas modalidades de firma y la adaptación a la evolución tecnológica mantienen la firma electrónica en evolución. Probablemente la clave de su éxito dependerá de lo bien que sigan solucionando los problemas que diariamente ciudadanos y empresas afrontan en el mundo electrónico.

10 Referencias

1. **Código de Administración Electrónica**. Ministerio de Hacienda y Administraciones Públicas. Dirección de Tecnologías de la Información y las Comunicaciones

   http://www.boe.es/legislacion/codigos/codigo.php?id=029_Codigo_de_Administracion_Electronica

2. **Firma electrónica**. Wikipedia.

   http://es.wikipedia.org/wiki/Firma_electr%C3%B3nica

3. **Firma electrónica.** Portal Administración Electrónica

   http://firmaelectronica.gob.es/

4. **Dni electrónico.** Cuerpo Nacional de Policía

   http://www.dnielectronico.es/PortalDNIe/

5. **CERES.** FNMT

   https://www.sede.fnmt.gob.es/

6. **Cl@ve.** Gobierno de España

   http://clave.gob.es

7. **Factura–e.** Ministerio de Industria, Energía y Turismo. Ministerio de Hacienda y Administraciones Públicas

   http://www.facturae.gob.es/paginas/Index.aspx

8. **FACe.** Gobierno de España

   https://face.gob.es/es/

9. **Plataforma de validación de firma electrónica @firma .** Portal Administración Electrónica

   http://administracionelectronica.gob.es/es/ctt/afirma

10. **eCoFirma.** Ministerio de Industria, Energía y Turismo

    http://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/index.html

11. **Manual de usuario de la utilidad de copia, firma y validación electrónica eCoFirma v 1.4.0**

    https://oficinavirtual.mityc.es/javawebstart/soc_info/ecofirma/ManualUsuarioeCoFirmav1.4.0.pdf

12. **Formulario de Información Ciudadana.** Grupo de Delitos Telemáticos. Unidad Central Operativa

    https://www.gdt.guardiacivil.es/webgdt/colabora.php

13. **Definiciones de clave, cifrado, integridad, identificación.** Wikipedia

    https://es.wikipedia.org

11 Glosario

- **Clave**. Pieza de información que controla la operación de un algoritmo de criptografía. Habitualmente, esta información es una secuencia de números o letras.
- **Cifrado**. Procedimiento que transforma un mensaje de tal forma que sea incomprensible, o, al menos, difícil de comprender a toda persona que no tenga la clave secreta del algoritmo de cifrado.
- **Integridad de un mensaje**. Cuando se envía un mensaje de una persona a otra o bien de una máquina a otra, este mensaje no es modificado, sin que el destinatario pueda comprobarlo.