



CID  
COMPETENCIAS EN INFORMACIÓN DIGITAL

# CERTIFICADOS DIGITALES



**Reconocimiento – NoComercial-CompartirIgual (By-ns-sa):** No se permite un uso comercial de la obra original ni de las posibles obras derivadas, la distribución de las cuales se debe hacer con una licencia igual a la que regula la obra original.

# CERTIFICADOS DIGITALES



## Objetivos

- Conocer el significado de certificado digital y conocer los elementos que lo forman.
- Saber cómo se obtiene, cómo se renueva y cómo se revoca.
- Aprender a usar los certificados digitales en el ordenador y en los navegadores.
- Conocer que se puede hacer en la Universidad con los certificados digitales.

## PARA EMPEZAR



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 o propietaria 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 una persona concreta. Esa es la razón por la que los certificados están firmados, a su vez, por la Autoridad de Certificación.

## CLAVE DIGITAL



En un certificado, las claves digitales son los elementos esenciales para la firma e identificación de la persona 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 de la persona firmante. En cambio, la **clave pública** se puede repartir o enviar a otras personas.

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).

## OBTENCIÓN DEL 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 de la persona responsable o persona usuaria del certificado, lo cual requiere que ésta 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/a crea las claves. Pero, en el certificado de tarjeta, quien crea e introduce las claves es el proveedor de certificación.

---

### Obtención del certificado en tarjeta (DNIe)

---

Los certificados contenidos en tarjetas deben ser entregados directamente a la persona.

En el caso concreto del DNIe, hay que personarse en las oficinas de la Dirección General de Policía, que es la autoridad certificadora.

---

### Solicitud del certificado software

---

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

Puedes consultar las principales autoridades de certificación españolas que emiten certificados electrónicos de persona física en este [enlace](#).



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



Una autoridad de certificación es una entidad de confianza, responsable de emitir y revocar los certificados digitales o electrónicos, utilizados en la firma electrónica. Jurídicamente es un caso particular de Prestador de Servicios de Certificación.

## RENOVACIÓN DEL CERTIFICADO



Los **certificados electrónicos** tienen un periodo de validez, pasado éste 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.

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.

Aquí encontrarás más información sobre [cómo renovar los certificados de tu DNIe](#).



Ten en cuenta que, 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](#) del Ministerio de Hacienda y Administraciones Públicas. También puedes comprobarlo directamente en tu navegador, en el menú de opciones o herramientas.

## REVOCACIÓN DEL 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 de la persona suscriptora.
- ◆ Pérdida o daños en el soporte del Certificado.
- ◆ Fallecimiento de la persona suscriptora o de su representado, incapacidad sobrevinida, total o parcial, de cualquiera de ellos.
- ◆ Finalización de la representación o extinción de la entidad representada.
- ◆ Inexactitudes en los datos aportados por la persona suscriptora para la obtención del certificado.
- ◆ Que se detecte que las claves de la persona suscriptora 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.



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

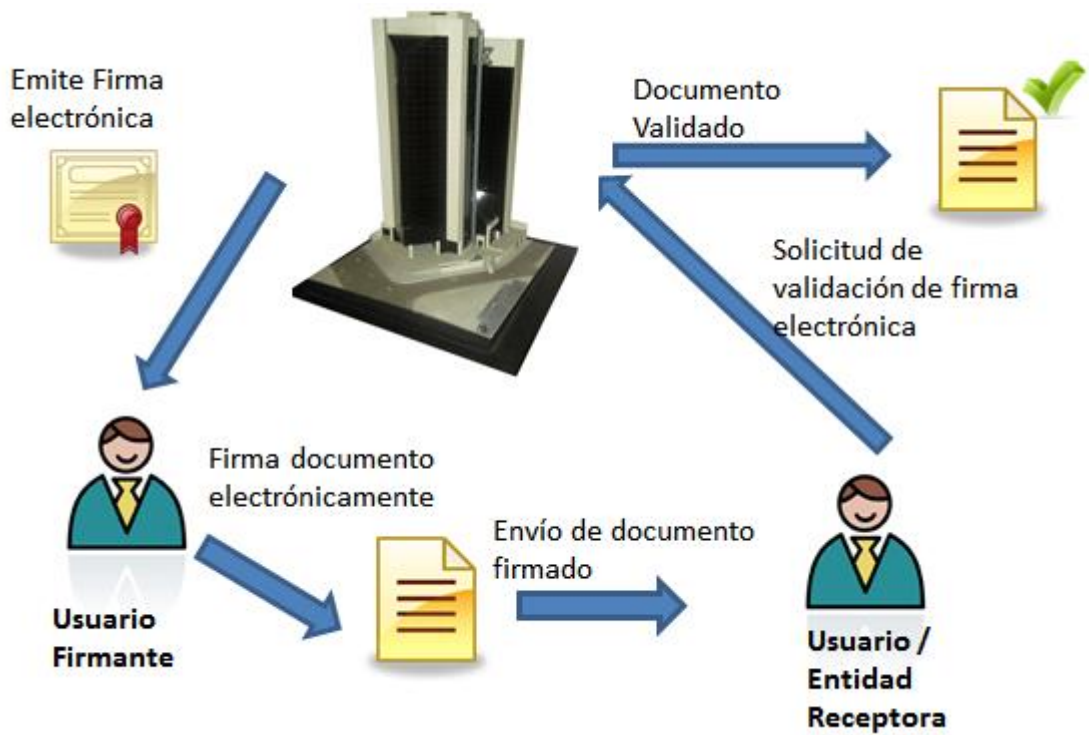


En el caso del DNIE, debes presentarte en cualquier Oficina de Expedición del DNIE para revocar el Certificado. La revocación es inmediata a la tramitación de cada solicitud verificada como válida.

## TRABAJAR CON CERTIFICADOS DIGITALES EN EL NAVEGADOR Y ORDENADOR



## El almacén de certificados







Siempre que vayamos a realizar un proceso de firma electrónica o identificación digital basadas en certificados, será necesario que esos certificados estén disponibles en el ordenador para la aplicación que va a realizar la firma.

Los certificados se guardan en el "**Almacén de Certificados**".

- ◆ Para los certificados contenidos en una **tarjeta digital**, como el **DNI electrónico**, la **propia tarjeta** es el almacén.
- ◆ **Los certificados software** se guardan en un almacén que puede estar ubicado en el sistema operativo o en el propio ordenador. Para poder usarlo primero es necesario importar o cargar el certificado en ese almacén.

## Importar y exportar certificados



### Importar certificados

La **importación de certificados** es el proceso que permite cargar el certificado en el ordenador o en el navegador para su uso posterior en la firma o identificación.



Al importar un certificado es importante que contenga la clave privada, ya que sin ella no vamos a poder firmar. Por tanto, asegúrate de que el fichero del certificado que importas tenga alguna de estas extensiones .pfx .p12 ó .pem.

---

## Exportar certificados

---

La **exportación de certificados** es el proceso que permite obtener una copia del certificado instalado en el ordenador o en el navegador para su uso posterior en otro ordenador o proceso.

En ocasiones es necesario **extraer del almacén un certificado** para lo siguiente:

- ◆ Hacer un backup o copia de seguridad del certificado.
- ◆ Instalarlo en otro ordenador.
- ◆ Enviar la parte pública a otra persona.

En el proceso de exportación se nos solicitará o se podrá marcar una casilla que indique que queremos exportar la clave privada.

- ◆ Marca la casilla si quieres que el certificado exportado se pueda utilizar para firmar. En este caso, el archivo generado se guardará con una extensión .p12, .pfx o .pem. Recuerda que este certificado no se puede distribuir y que hay que mantenerlo en un lugar seguro.
- ◆ No marques la casilla si quieres que el certificado sea público y enviar el certificado a otra persona. En este caso, el archivo generado se guardará con una extensión .cer o .der



La exportación se debe hacer desde el almacén en el que está instalado el certificado.

## Instalar certificados en Windows



El almacén de certificados de Windows es utilizado por navegadores como Internet Explorer y Chrome y por otras aplicaciones como Office y Adobe Reader.

La importación de certificados en este almacén se puede realizar desde cualquiera de los dos navegadores mencionados. La forma de acceder al almacén y a las herramientas de importación es la siguiente:

### **En Internet Explorer:**

- ◆ Opciones de Internet > Contenido > Certificados.

### **En Google Chrome:**

- ◆ Opciones > Avanzada > HTTP/SSL > Gestionar Certificados.

### **En Firefox**

Firefox dispone de su propio almacén de certificados independiente del almacén del sistema operativo. Por tanto, si quieres firmar documentos desde Firefox debes realizar previamente la importación de certificados desde el mismo navegador.

La forma de acceder a la gestión del almacén de Firefox es la siguiente:

- ◆ Opciones > Avanzado > Cifrado > Ver Certificados.

## ¿Qué puedo hacer en la UA con los certificados digitales?



La oficina central del Registro General de la Universidad de Alicante es punto de registro de usuario (PRU) de firma digital de la Agencia de Tecnología y Certificación Electrónica de la Comunidad Valenciana, de acuerdo con el [convenio](#) firmado con la Generalitat Valenciana.

La firma digital expedida en la oficina central del Registro General se puede utilizar para:

- ◆ Recepción y envío de documentos a las Administraciones Central, Autonómica y Local (certificados de vida laboral, declaración de la Renta, o trámites con SUMA, entre otros).
- ◆ Firmar y cifrar los mensajes de correos electrónicos evitando el SPAM.
- ◆ Firmar facturas electrónicas.



Para solicitar un certificado digital es necesario personarse en la oficina central del Registro General con el DNI, NIE, carnet de conducir en formato tarjeta o pasaporte español en vigor.

Con el fin de agilizar los trámites, sugerimos que utilices este servicio entre las 9:00 y las 10:00 horas de la mañana.



## PARA SABER MÁS

### Enlaces:

<https://www.sede.fnmt.gob.es/certificados/persona-fisica>

<https://www.sede.fnmt.gob.es/certificados>

<http://firmaelectronica.gob.es/Home/Ciudadanos/Certificados-Electronicos.html>

<https://sede.dgt.gob.es/es/contenidos/donde-obtener-certificado.shtml>

[https://es.wikipedia.org/wiki/Certificado\\_digital](https://es.wikipedia.org/wiki/Certificado_digital)

<https://www.accv.es/ayuda/instalar-el-certificado-digital-en-fichero/>

### Tutoriales:

<https://www.youtube.com/watch?v=p19J0TOpIks>

<https://www.youtube.com/watch?v=98NXoYUoffo>

<https://www.youtube.com/watch?v=8ab88NLomY8>

<https://www.youtube.com/watch?v=p19J0TOpIks&t=7s>