

GUÍA PRÁCTICA CERTIFICADOS ELECTRÓNICOS

¿QUÉ ES UN CERTIFICADO DIGITAL Y LA FIRMA ELECTRÓNICA?

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, según se contempla en el artículo 6.1. de la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En términos sencillos un certificado digital es un documento que se instala en el navegador (Internet Explorer, Firefox, Chrome, Safari, etc) del ordenador con el que habitualmente nos conectamos a internet. La función principal del certificado digital es identificarnos en la gestión online que queramos realizar. El certificado digital es la firma en Internet que demuestra que realmente somos quien decimos ser a la hora de realizar cualquier gestión.

Asimismo, el artículo 3 de la Ley 59/2003, de 19 de diciembre, de firma electrónica define la firma electrónica como 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. Considerándose firma electrónica reconocida 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.

Cualquier ciudadano puede solicitar un certificado digital para realizar trámites con la Administración a través de Internet. La obtención del certificado digital es gratuita.

La utilización de un certificado digital es un medio válido para utilizarlo ante cualquier administración, entidades públicas o privadas que lo admita, como la Agencia Tributaria, Seguridad Social, las Comunidades Autónomas, los Ayuntamientos, Tráfico, etc.

¿CÓMO SE OBTIENE UN CERTIFICADO DIGITAL?

La obtención de un certificado digital depende de si el certificado está contenido en una tarjeta, como el DNle, o de si el certificado se guarda en un fichero software.

En ambos procesos siempre 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.

Certificado en tarjeta (DNle)

Los certificados contenidos en tarjetas deben ser entregados directamente al usuario. En el caso concreto del DNle, hay que personarse en las oficinas de la Dirección General de Policía, que es la Autoridad de Certificación. La utilización del DNle requiere contar con determinados elementos hardware y software que permitan el acceso al chip de la tarjeta y, por tanto, la utilización de los certificados contenidos en él.

Certificado software.

La solicitud y descarga del Certificado se realizan desde el navegador. Hay que personarse en la oficina de la Autoridad de Certificación para acreditar la identidad.

Principales Autoridades de Certificación (AC)¹

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.

A continuación, se indican las principales Autoridades de Certificación españolas que emiten certificados digitales:

- [Fábrica Nacional de Moneda y Timbre \(FNMT\).](#)
- [Agència Catalana de Certificació \(CATCert\).](#)
- [Agencia Notarial de Certificación \(ANCERT\).](#)
- [ANF Autoridad de Certificación \(ANF AC\).](#)
- [Autoridad de Certificación de la Abogacía \(ACA\).](#)
- [Autoritat de Certificació de la Comunitat Valenciana \(ACCV\).](#)
- [Banco de España.](#)
- [Banco de Santander.](#)
- [Camerfirma.](#)
- [EDICOM.](#)
- [Consejo General de Colegios Oficiales de Médicos \(CGCOM\).](#)
- [Cuerpo Nacional de Policía.](#)
- [Coloriuris \(CIPSC\).](#)
- [ESCB.](#)
- [ESFIRMA \(AULOCE\).](#)
- [FirmaProfesional.](#)
- [Gerencia de Informática de la Seguridad Social \(GISS\).](#)
- [IZENPE.](#)
- [Ministerio de Defensa.](#)
- [Ministerio de Trabajo e Inmigración.](#)
- [Servicio de Certificación de los Registradores \(SCR\).](#)
- [Servicio de Salud de Castilla La Mancha \(SESCAM\).](#)
- [SIA.](#)
- [SIGNE.](#)
- [UANATACA.](#)

¹ Información extraída de <http://firmaelectronica.gob.es/Home/Ciudadanos/Principales-Autoridades-Certificacion.html>

- [VINTEGRIS](#).

En cada una de páginas web de las Autoridades de Certificación indicadas se pueden consultar los trámites necesarios a realizar para la obtención del certificado digital.

Respecto al certificado en tarjeta (DNIe), la Dirección General de Policía tiene a disposición de los ciudadanos toda la información relativa a su obtención y funcionamiento en: <https://www.dnielectronico.es/PortalDNIe/>

¿CÓMO FIRMAR UN DOCUMENTO CON CERTIFICADO DIGITAL?

La firma de un documento electrónico con certificado digital requiere los siguientes pasos:

1. El documento debe estar en un formato con extensión .pdf.
2. Dentro del programa Adobe Acrobat Reader seleccionar el botón “firmar”.
3. Colocar el recuadro de firma dónde se quiera que figure la firma que posteriormente se va a insertar.
4. Seleccionar el certificado electrónico con el cual se quiere firmar el documento.

