ASESORAMIENTO FIRMA DIGITAL

Sede electrónica municipal para Asociaciones

versia

1 CONCEPTOS GENERALES

¿Qué es un certificado digital?

versia

¿Qué es un certificado electrónico?

Podemos definir el concepto de certificado digital como **un archivo o documento en formato electrónico que se vincula con una determinada persona y sirve para identificarla** de forma fehaciente en el dominio digital.

Los emite una autoridad de certificación.

Puede identificar tanto a una **persona física** como a una **persona jurídica** (en este caso, a través de un representante persona física).

Certificados por nivel de seguridad

Certificados digitales

No es necesaria la identificación de la persona, dispone de un nivel de seguridad bajo y no sirve para firma digital es válido para autentificarnos.
Ejemplo: Bak, Clave pin

Certificados cualificados/reconocido

Certificado electrónico reconocido son los certificados electrónicos que se han expedido cumpliendo requisitos cualificados en lo que se refiere a su contenido, a los procedimientos de comprobación de la identidad del firmante y a la fiabilidad y garantías de la actividad de certificación electrónica.

Ejemplo: Bakq, DNIe, FMNT

Tipos de certificados

- Persona física
- Representante de entidad
- Empleado público
- Profesional corporativo

Todos los certificados digitales reconocidos o cualificados requieren de una identificación de la persona que lo solicita.

En el caso de las **personas físicas** presentarán un documento de identidad, bien sea DNI/NIE/Pasaporte(dependiendo de la entidad emisora)

Los certificados de **representante de entidad** deberán acreditar la capacidad de representación de la empresa por cargo o por poderes otorgados.

Lo de **empleado público y profesional corporativo** acreditarán la pertenencia a una entidad.

Sistemas de firma aceptados

En la mayoría de las administraciones vascas se hace la identificación a través de Giltza (Izenpe) y cada uno decide qué certificados son válidos para subir o firmar documentación.

GIPUZKOA ETORKIZUNA ORAIN

Bizkaia
foru aldundia
diputación foral

2 ENTIDADES CERTIFICADORAS

¿Quiénes las emiten?

versia

Certificados aceptados por Ministerio

La información referente a los prestadores cualificados de servicios de confianza podrá ser objeto de publicación en la dirección de Internet del Ministerio de Asuntos Económicos y Transformación Digital(Abre en nueva ventana) para su difusión y conocimiento, conforme a lo establecido en el artículo 17. 2 de la Ley 6/2020, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza.

Podemos consultar el listado de proveedores y certificados
https://sede.administracion.gob.es/PAG_Sede/dam/jcr:e93f87b6-d3de-4529-bea4-022c6244123a/aFirma-Anexo-PSC.pdf

Buscador de centros de confianza
https://sedeaplicaciones.minetur.gob.es/Prestadores/Inicio.aspx

Entidades emisoras

Nosotros nos vamos a centrar en las 4 entidades emisoras más demandadas y realizaremos casos prácticos:

Izenpe

Izenpe S.A., empresa de certificación y servicios: es una sociedad anónima constituida en 2002 y supone un proyecto impulsado por el Gobierno Vasco y las Diputaciones Forales, constituida a través de sus sociedades informáticas: **EJIE, LANTIK, IZFE y CCASA.**

Izenpe es un prestador de servicios de confianza, es decir, una organización que proporciona servicios de firma electrónica. La firma electrónica se puede definir como un conjunto de procedimientos técnicos y jurídicos que permiten "sustituir" la firma manual convencional con el fin de poder realizar a través de Internet y del teléfono tramites que antes debían hacerse de forma presencial.

Izenpe: persona física

BAKQ: ¿Qué es?

Es un medio de identificación y firma electrónica, para personas mayores de 16 años, que se compone de un identificador y dos factores de autenticación:

- Usuario (DNI/NIE del usuario)
- Contraseña (8 caracteres)

Un juego de coordenadas con 16 posiciones si lo solicitaste antes del 2 de febrero de 2021 o un código enviado por SMS a su teléfono móvil.

Se puede utilizar tanto en ordenadores, como en móviles y tabletas, en cualquier sistema operativo y sin necesidad de instalar nada. Además, la solicitud de una BakQ lleva consigo la posibilidad de usar también Bak por lo que a partir de ese momento podrá utilizar cualquiera de ellas según el caso. La emisión de BakQ lleva implícita la emisión de Bak. Ambos medios de identificación comparten contraseña, datos de contacto y periodo de vigencia. En el caso de BakQ el nivel de seguridad es mayor por lo que da acceso a mayor número de trámites y servicios.

Izenpe: persona física

BAKQ: ¿Cómo se obtiene?

Hay 2 formas diferentes de tener BakQ

- Si tiene un certificado ciudadano de Izenpe (Tarjeta verde) obtenido de manera presencial o un DNIe puede solicitar BakQ desde solicitudes online.

- Si no dispone de ninguna de las soluciones online, debe acudir a algunos de los siguientes puntos de atención presencial para solicitarlo. Puede buscar el punto de solicitud más cercano en el mapa que proponemos (son más de 600) y en el que se muestran las diferentes entidades a las que acudir para solicitar BakQ.
- Puntos de emisión bakq:
  - https://servicios.izenpe.com/solicitud_online/mostrarNewWelcome.do

Izenpe: persona física

BAKQ: Documentación

1. Ciudadanía española: DNI, pasaporte o permiso de conducción.
2. Ciudadanía miembro UE/EEE: pasaporte o documento de identidad de su país de origen junto con Tarjeta de Identificación de Extranjero o certificado emitido por el Registro de Ciudadanos miembros de la Unión o documento oficial de concesión del NIE
3. Ciudadanía extracomunitaria: pasaporte junto con Tarjeta de Identificación de Extranjero o documento oficial de concesión del NIE.

En ningún caso una tercera persona puede tramitar la solicitud de una BakQ en nombre de otra, ni siquiera en casos de representación legal, tutelar o similar.

En esos casos la persona representante deberá solicitar BakQ y ejercer la representación en primera persona ante el servicio correspondiente.

Izenpe: persona física

BAKQ: Validez

Tiene validez de 4 años

Izenpe avisa 30 días antes de la fecha de caducidad de su BakQ por correo electrónico indicando los pasos a seguir para su renovación.

Si llega la fecha de caducidad y no se ha renovado debemos solicitar una BakQ nueva siguiendo los mismos pasos que la primera vez.

En la renovación el segundo factor (juego de coordenadas) será sustituido por un SMS a su teléfono móvil para los usos que haga a futuro. Por ello se solicitará que el número de teléfono utilizado sea de uso exclusivo del titular de la BakQ y no podrá ser compartido con otro usuario.

Coste

Gratuito

Izenpe: persona física

Tarjeta de ciudadano: ¿qué es?

El Certificado Ciudadano de Izenpe permite identificarse y firmar electrónicamente en las relaciones telemáticas con las distintas administraciones públicas locales, forales, autonómicas y estatales.
Se emite en soporte tarjeta y es un que certificado únicamente contiene los datos de identificación de la entidad y de la persona física solicitante: nombre del solicitante y DNI. La tarjeta no contiene ningún otro dato. Si alguno de estos datos cambia, se debe revocar ese certificado y solicitar uno nuevo con los nuevos datos.

Para poder hacer uso de su certificado debe instalarse el software de Izenpe disponible en la web. Además, si su certificado está emitido en tarjeta, debe disponer de un lector para poder acceder al certificado.

Izenpe: persona física

Tarjeta de ciudadano: ¿cómo se obtiene?

La solicitud del Certificado Ciudadano puede realizarse de 2 formas:

•En el caso de contar con su Certificado Ciudadano (tarjeta verde) o DNIe activo y conocer sus claves, podrá tramitarlo de forma completamente on-line y recibirá la tarjeta con el certificado y las claves en la dirección postal indicada:

https://servicios.izenpe.com/solicitud_online/mostrarNewWelcome.do

•En caso contrario, tras cumplimentar la solicitud deberá acudir para su identificación presencial a alguno de los puntos de registro habilitados por Izenpe (Bilbao/Donostia/Gasteiz).

Izenpe: persona física

Tarjeta de ciudadano: documentación

Acreditación de la identidad persona solicitante (original y en vigor):

1. Ciudadanía española: DNI, pasaporte o permiso de conducción.
2. Ciudadanía miembro UE/EEE: pasaporte o documento de identidad de su país de origen junto con Tarjeta de Identificación de Extranjero o certificado emitido por el Registro de Ciudadanos miembros de la Unión o documento oficial de concesión del NIE
3. Ciudadanía extracomunitaria: pasaporte junto con Tarjeta de Identificación de Extranjero o documento oficial de concesión del NIE.

Una tercera persona puede recoger el certificado de firma electrónica en nombre de la persona solicitante siempre que aporte la solicitud de emisión firmada por el solicitante y legitimada ante notario junto con una autorización notarial habilitante legitimada para recoger el certificado en nombre de la persona solicitante y el resto de documentación requerida.

Izenpe: persona física

Tarjeta de ciudadano: validez

Los certificados de persona física de Izenpe caducan a los 4 años de su emisión.

60 días antes de la fecha de caducidad del certificado Izenpe remitirá un correo electrónico a la dirección cedida en el momento de la solicitud para informar del proceso de renovación. En las renovaciones se emitirá un certificado nuevo con fecha de inicio posterior a la de caducidad de su actual certificado para que se puedan usar de forma continua.

Puede comprobar la fecha de caducidad de su certificado impreso en el anverso de la tarjeta al ir a hacer uso de su certificado.

Coste
Su coste es de 20€ IVA incluido

Izenpe: Representante de entidad y entidad sin personalidad jurídica

Representante: ¿qué es?

Un certificado de Representante de Entidad de Izenpe permite relacionarse de forma telemática (autenticarse y firmar) con las distintas administraciones (locales, forales, autonómicas y estatales).

Puede solicitarse en soporte tarjeta, Token USB o formato SOFTWARE. Los soportes tarjeta o Token se emiten de igual manera. La tarjeta criptográfica necesitará de un lector de tarjetas para su uso. El Token se utiliza como cualquier USB directamente al ordenador y sustituye la necesidad de lector.

Izenpe: Representante de entidad y entidad sin personalidad jurídica

Representante: ¿cómo obtenerlo?

•En el caso de contar el solicitante con su Certificado Ciudadano (tarjeta verde), certificado de representante emitido anteriormente de forma presencial o DNIe activo y conocer sus claves, podrá tramitarlo de forma completamente on-line y recibirá la tarjeta con el certificado y las claves en la dirección postal indicada:

https://servicios.izenpe.com/solicitud_online/mostrarNewWelcome.do

•En caso contrario, tras cumplimentar la solicitud deberá acudir para su identificación presencial a alguno de los puntos de registro habilitados por Izenpe (Bilbao/Donostia/Gasteiz).

Izenpe: Representante de entidad y entidad sin personalidad jurídica

Representante: ¿quién pude obtenerlo?

•La persona solicitante podrá ser, o un representante legal o un apoderado/a (general o específico) con facultad de representación ante las administraciones.

•Izenpe asumirá la comprobación de la vigencia de la entidad y de la facultad del solicitante como representante legal o apoderado para representar a la entidad antes las administraciones en el caso de sociedades mercantiles y de aquellas fundaciones, cooperativas, EPSV, centros de educación y federaciones y clubes deportivos que estén inscritas en los correspondientes registros del Gobierno Vasco. El resto de las entidades deberán acreditar la vigencia de la entidad y facultad del solicitante según lo que se indique en la guía de su tipo de entidad.

Izenpe: Solicitud online

Las solicitudes online, siempre que se disponga de un certificado cualificado obtenido presencialmente en el siguiente enlace: https://servicios.izenpe.com/home/mostrarWelcome.do;jsessionid=E8vHdcLzuPIzNBYKeAQbbFTmCPkeArP0VJi8Wrn7s5jsO8HWjNUI!-1735717224!NONE

Izenpe: solicitud online

Certificado Representante Entidad

Es un certificado de firma electrónica cualificado que permite relacionarse de forma telemática (autenticarse y firmar) con las distintas administraciones (locales, forales, autonómicas y estatales) y viene a cubrir el espacio al que antes se accedía con el certificado de persona jurídica o entidad sin personalidad jurídica.

Estos certificados permiten tramitar en representación de un tercero o entidad a aquellas personas que estén habilitadas/autorizadas para ello en los registros de representación voluntaria de las administraciones.

Fábrica Nacional de Moneda y Timbre (FNMT)

La FNMT-RCM como Prestador de Servicios de Certificación pone a su disposición diferentes tipos de certificados electrónicos mediante los cuales podrá identificarse y realizar trámites de forma segura a través de Internet.
En función del destinatario de los mismos, la FNMT-RCM emite los siguientes tipos de certificados digitales que podrá solicitar a través de su SEDE Electrónica:

FNMT: Persona física

¿Qué es y quién lo puede obtener?

El Certificado digital FNMT de Persona Física es la certificación electrónica expedida por la FNMT-RCM que vincula a su suscriptor con unos Datos de verificación de Firma y confirma su identidad.

Este certificado, también conocido como Certificado de Ciudadano o de Usuario, es un documento digital que contiene sus datos identificativos. Le permitirá identificarse en Internet e intercambiar información con otras personas y organismos con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

Cualquier ciudadano español o extranjero, mayor de edad o menor emancipado que esté en posesión de su DNI o NIE, podrá solicitar y obtener su certificado digital de forma gratuita para firmar y acreditar su identidad de forma segura en Internet.

FNMT: Persona física

¿Cómo puedo obtener el certificado?

Existen 2 formas distintas para obtener su Certificado digital de Persona Física como archivo descargable en su ordenador:

- Con acreditación presencial en una oficina. Obtener Certificado software.
- Utilizando su DNIe. Obtener Certificado con DNIe.

FNMT: Representante

Representante de Administrador Único o Solidario: ¿Quién lo puede solicitar?

Este certificado puede ser obtenido por: sociedades anónimas (A) y limitadas (B) si el representante de la sociedad es administrador único o solidario, tenga inscritas sus facultades de Representación en el Registro Mercantil y éstas no hayan sido revocadas. En dicho Registro tiene que constar el NIF actual de la Entidad, el órgano de administración, el NIF o NIE correcto (9 caracteres) del administrador único o solidario, el cargo específico (administrador único o administrador solidario), fecha de nombramiento, duración del cargo (vigente o indefinida), inscripción y fecha de inscripción.

FNMT: Representante

Representante de Administrador Único o Solidario: ¿Cómo puedo obtener el certificado?

El proceso de obtención del certificado de representante para administradores únicos y solidarios se divide en tres pasos, que deben realizarse en el orden señalado:

1. **Configuración previa**. Para solicitar el certificado es necesario instalar el software que se indica en este apartado.

2. **Solicitud vía internet de su Certificado**. Este certificado sólo puede pedirse de forma On Line con un certificado de Persona Física de la FNMT-RCM o DNI electrónico.

3. **Descarga de su Certificado**. Aproximadamente 1 hora después de que haya solicitado su certificado y haciendo uso de su Código de Solicitud, desde aquí podrá descargar e instalar su certificado, así como realizar el pago y realizar una copia de seguridad (RECOMENDADO).

El precio de este certificado es de 24 Euros, impuestos no incluidos, y se emite con un periodo de validez de 2 años.

FNMT: Representante

Representante de persona jurídica: ¿Quién lo puede solicitar?

Las sociedades que tengan como administrador único/solidario a otra sociedad.
A y B: Las sociedades anónimas y limitadas, si el representante de la sociedad es mancomunado, apoderado, socio único, presidente, consejero, consejero delegado solidario, administrador conjunto, liquidador, etc..., y tiene poderes específicos de representación que le permitan obtener este tipo de certificado.
C: Sociedades colectivas.
D: Sociedades comanditarias.
F: Sociedades cooperativas.
G: Asociaciones L.O. 1/2002, fundaciones, partido político, sindicato, asociación de consumidores y usuarios, organización empresarial, federación deportiva, otras asociaciones distintas de las anteriores con personalidad jurídica. Otras asociaciones.
J: Sociedades civiles.
N: Entidades extranjeras con personalidad jurídica, EO procedente EORI, In procedente IVA no establecidos, NR procedente no residentes 210, sociedades anónimas europeas, sociedades cooperativas europeas, corporación, asociación o ente con personalidad jurídica con presencia en España, embajadas, consulados u oficina comercial país extr. en España.
Q: Organismos públicos.
R: Congregaciones e instituciones religiosas.
S: Gobiernos de las CC.AA.
P: Ayuntamientos o diputaciones.
V: Sociedad agraria en transformación, agrupación de interés económico, agrupación europea de interés económico, etc...

FNMT: Representante

Representante de persona jurídica : ¿Cómo puedo obtener el certificado?

El proceso de obtención del certificado de representante de persona jurídica se divide en cuatro pasos, que deben realizarse en el orden señalado:

1. **Configuración previa**. Para solicitar el certificado es necesario instalar el software que se indica en este apartado.
2. **Solicitud vía internet de su Certificado**. Al finalizar el proceso de solicitud, recibirá en su cuenta de correo electrónico un Código de Solicitud que le será requerido en el momento de acreditar su identidad y posteriormente a la hora de descargar su certificado.
3. **Acreditación de la identidad** **Acreditación On Line:** (Recomendada) Sólo para entidades con NIF A, B, C y D.
4. **Acreditación en una Oficina de Acreditación de Identidad:** Compruebe en este apartado la documentación necesaria a aportar. Deberá personarse con su Código de Solicitud en las Oficinas de Acreditación de identidad de la Agencia Tributaria, de la Comisión Nacional del Mercado de Valores, o de la Comunidad Foral de Navarra.
5. **NOTA: En las oficinas de la AEAT se requiere cita previa. La CNMV tiene un procedimiento específico que podrá consultar en este apartado.**
6. **Descarga de su Certificado**. Aproximadamente 1 hora después de que haya acreditado su identidad en una Oficina de Acreditación de Identidad y haciendo uso de su Código de Solicitud, desde aquí podrá descargar e instalar su certificado, así como realizar el pago y realizar una copia de seguridad (**RECOMENDADO**).El precio de este certificado es de 14 Euros, impuestos no incluidos, y se emite con un periodo de validez de 2 años.

FNMT: Representante

Representante de Entidad sin Personalidad Jurídica: ¿Quién lo tiene que solicitar?

E: Las comunidades de bienes, herencias yacentes, titularidad compartida de explotaciones agrarias.
H: Comunidades de propietarios.
N: Corporación o ente independiente pero sin personalidad jurídica con presencia en España, conj. unit. bienes perteneciente a 2 o más personas en común sin personalidad jurídica con presencia en España, entidades en atrib. rentas constituidas en el extranjero sin presencia en España, otras entidades sin personalidad jurídica distintas de las reflejadas en el apartado de representante de persona jurídica.
P: Juntas vecinales, departamento u órgano dependiente de la Administración sin personalidad jurídica.
S: Órganos de la administración central y autonómica, excepto los Gobiernos de las CC.AA.
U: Unión temporal de empresas.
V: Otros tipos sin personalidad jurídica como son: fondo de inversiones, fondo de capital-riesgo, fondo de pensiones, fondo de regulación de mercado hipotecario, fondo de titulización hipotecaria, fondo de titulización de activos, fondo de garantía de inversiones, comunidad titular de montes vecinales en mano común, fondos de activos bancarios, otras entidades sin personalidad jurídica.
W: Entidades no residentes con establecimiento permanente en España.

DNIe: DNI electrónico

¿Qué es?

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita, la identidad, los datos personales que en él aparecen y la nacionalidad española de su titular. Nos puede servir para:

- Acreditar electrónicamente y de forma indubitada la identidad de la persona.
- Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.

Para responder a estas nuevas necesidades, en 2006 se creó el Documento Nacional de Identidad electrónico (DNIe), de policarbonato con los datos de filiación grabados en el cuerpo de la tarjeta y cuya principal novedad es que incorpora un pequeño circuito integrado (chip), capaz de guardar de forma segura información y de procesarla internamente.

En enero de 2015 nace el DNI 3.0. Un documento de alta seguridad que combina las más novedosas medidas de seguridad con la última tecnología aplicada a la identificación de los ciudadanos al disponer de un chip dual-interface que permite su utilización con contacto y también modo contactlesss. La incorporación de la tecnología NFC (Near Field Communication) a los dispositivos móviles de última generación elimina la necesidad de un lector de tarjetas, drivers, etc. facilitando la conexión online y la autenticación del ciudadano. Las Apps creadas hasta ahora, están disponibles en el repositorio oficial de Google Play buscando por el desarrollador: https://play.google.com/store/apps/developer?id=CNP-FNMT&pli=1

DNIe: DNI electrónico

¿Validez?

Sus certificados electrónicos ya que, con independencia de lo que establece el artículo 6.1 sobre la validez del Documento Nacional de Identidad, la vigencia de los certificados electrónicos reconocidos incorporados al mismo no podrá ser superior a cinco años (Real Decreto 414/2015, de 29 de mayo).

Cl@ve

¿Qué es?

Cl@ve es un sistema orientado a unificar y simplificar el acceso electrónico de los ciudadanos a los servicios públicos. Su objetivo principal es que el ciudadano pueda identificarse ante la Administración mediante claves concertadas (usuario más contraseña), sin tener que recordar claves diferentes para acceder a los distintos servicios.

Cl@ve complementa los actuales sistemas de acceso mediante DNI-e y certificado electrónico, y ofrece la posibilidad de realizar firma en la nube con certificados personales custodiados en servidores remotos.

Se trata de una plataforma común para la identificación, autenticación y firma electrónica, un sistema interoperable y horizontal que evita a las Administraciones Públicas tener que implementar y gestionar sus propios sistemas de identificación y firma, y a los ciudadanos tener que utilizar métodos de identificación diferentes para relacionarse electrónicamente con la Administración. Además de posibilitar el acceso a trámites electrónicos a quien no dispone de certificado electrónico, el sistema Cl@ve aporta un uso sencillo, ya sea a través de una contraseña permanente o de un código temporal, y seguro. Es un sistema además que permite la tramitación electrónica en dispositivos móviles que no admitan la firma electrónica con certificados electrónicos.

Cl@ve

¿Cómo solicitarlo?

Cl@ve es una plataforma de verificación de identidades electrónicas para la identificación y autenticación de los ciudadanos en sus trámites con las Administraciones Públicas. Permite la identificación con plenas garantías de seguridad.

El primer paso es registrase en Cl@ve, para lo que existen cuatro modalidades correspondientes a dos niveles de registro:

- Registro Básico

1. A través de Internet por videollamada
2. A través de Internet con carta de invitación

- Registro Avanzado

1. A través de Internet con certificado electrónico o DNIe
2. Presencialmente en una oficina de registro

Cl@ve

¿Dónde puedo usarlo?

Puedes usar los mecanismos de identificación previstos en Cl@ve en todos aquellos servicios de administración electrónica integrados en el sistema. Los servicios integrados se distinguen porque dispondrán, en la pantalla de acceso a los mismos, de un botón similar a la siguiente simbología que te redirigirá al sistema de autenticación Cl@ve:

Actualmente, Cl@ve está disponible para todos los servicios electrónicos de la Administración General de Estado, en todas las Comunidades Autónomas y en la mayoría de las Entidades Locales. Así, con el sistema Cl@ve podrás, por ejemplo, presentar tu declaración de Renta o visualizar tus datos fiscales, consultar tu información clínica, tus puntos de la DGT, descargarte la vida laboral u obtener el certificado digital COVID.

Recuerda que para obtener esos mecanismos de identificación y usarlos en Cl@ve, es necesario haberse registrado previamente con alguno de los procedimientos previstos (puedes ampliar esta información en el apartado de Registro).

Cl@ve firma

¿Qué es?

Cl@ve es un sistema de Identificación, Autenticación y Firma Electrónica para los ciudadanos común a todo el Sector Público Administrativo Estatal, basado en el uso de claves concertadas, conforme a lo previsto en el artículo 13.2.c) de la Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos y conforme al Reglamento Europeo de Identidad y Firma Electrónica 910/2014.

La principal novedad que incorpora el sistema Cl@ve es la posibilidad de realizar firma electrónica mediante certificados electrónicos centralizados, es decir certificados electrónicos almacenados y custodiados por la Administración Pública.
Estos certificados centralizados, o "certificados en la nube" permiten al ciudadano firmar documentos electrónicos desde cualquier dispositivo que tenga conexión a Internet y sin ningún equipamiento adicional.

Cl@ve firma

¿Cómo solicitarlo?

Para utilizar la firma centralizada es necesario haber realizado previamente los siguientes pasos:

- Registro de Nivel Avanzado en el sistema Cl@ve: el ciudadano proporciona sus datos de registro en el sistema, bien de forma presencial en una oficina ante un empleado público habilitado al efecto, o bien de forma telemática, previa autenticación del ciudadano mediante un certificado electrónico reconocido.
- Activación de la Cl@ve Permanente; obtención de credenciales de acceso al sistema mediante identificador de usuario y contraseña, que debe ser custodiada por el ciudadano. La validez de la contraseña está limitada en el tiempo. Adicionalmente, y cuando el tipo de trámite lo requiera, la modalidad de identificación Cl@ve permanente podrá proporcionar un nivel de garantía en la autenticación superior, mediante una verificación de seguridad adicional a través de un código de un solo uso (OTP, "One Time Password") que se envía al dispositivo móvil del usuario. Los requisitos de seguridad de las contraseñas para este sistema se publicarán en el portal Cl@ve(http://www.clave.gob.es)
- Generación del certificado de firma. Esta acción se puede realizar de manera automática en el momento de realizar la primera firma, o en cualquier otro momento a voluntad del usuario.
- Los certificados necesarios para poder realizar firma centralizada, son emitidos y custodiados por la Dirección General de la Policía. Dicha custodia se realiza de manera segura, de tal forma que sólo el propietario del certificado puede tener acceso a los mismos. La Gerencia de Informática de la Seguridad Social (GISS), se constituye en Prestador de Servicios de Confianza, junto con la DGP que además, es Autoridad de Firma. La GISS queda encargada de la custodia de una copia de seguridad de los certificados con el mismo nivel de seguridad que el fichero original.

3 VALIDACIÓN Y FIRMA

La firma de la solicitud

versia

¿Qué es la validación de firma?

La validación de una firma electrónica es el proceso por el que se comprueba:

- La identidad del firmante
- La integridad del documento firmado
- La validez temporal del certificado utilizado

Sabemos que en el proceso de firma, el firmante utiliza su certificado electrónico, en concreto su clave privada, para obtener la firma electrónica.
Pero ¿cómo sabemos si ese certificado es válido?, ¿estaba revocado en el momento de la firma? O ¿si la Autoridad que lo emitió es de confianza?
El proceso de validación de la firma no puede separarse del proceso de validación del certificado usado para la firma. Y por eso, la validación de la firma implica también la validación del certificado.
El certificado electrónico solamente se puede validar mientras esté activo, ya que una vez caducado desaparece de las listas de revocación de la Autoridad de Certificación y ya no se puede comprobar cuál era el estado en el momento de la firma.
Si el certificado no es válido, o está caducado o revocado, la firma no puede ser validade correctamente puesto que no podemos saber cuál era el estado del certificado en el momento de la firma.
Por tanto, las tres validaciones dependen de la capacidad de validar el certificado, para lo cual es necesaria una conexión a internet que permita acceder a una plataforma de validación de certificados

Plataformas de validación

Las plataformas de validación son sistemas online que permiten validar los certificados electrónicos.

La Autoridad de Validación es el componente que suministra información sobre la vigencia de los certificados electrónicos que han sido registrados por una Autoridad de Registro y certificados por la Autoridad de Certificación. En general, la Autoridad de Certificación es también Autoridad de Validación, aunque ambas figuras pueden estar representadas por entidades diferentes.

La información sobre los Certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL) mantenidos por las Autoridades de Validación.
La validación o verificación del estado de un certificado se puede realizar a través de internet accediendo al servicio que proporciona las Autoridad de Validación o de Certificación que ha emitido el certificado.

FMNT

Permite confirmar si su Certificado digital FNMT es Válido o ha sido Revocado.

https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado
https://www.sede.fnmt.gob.es/certificados/certificado-de-representante/verificar-estado

Verificar estado

Ponemos a su disposición un servicio de verificación con el que podrá confirmar si su Certificado digital FNMT es Válido o ha sido Revocado.

Este servicio está disponible para los siguientes tipos de certificados:

- Certificado FNMT de Persona Física (AC FNMT Usuarios)
- Certificado FNMT de Representante (AC Representación)
- Certificado FNMT de Empleado Público y Sello electrónico (Sector Público)
- Certificado FNMT de Sello de entidad (AC Componentes Informáticos)
- DNI electrónico

Para comprobar el estado de su certificado, asegúrese de que éste se encuentra correctamente instalado en el navegador de su equipo, o bien listo para ser usado a través de su dispositivo criptográfico.

SOLICITAR VERIFICACIÓN

Valide

Aplicación de Validación de firma y certificados Online.

https://valide.redsara.es/valide/?

Validación de la firma

Validar firma, consultar la validez de un documento firmado electrónicamente

Izenpe

https://servicios.izenpe.com/herramientasFirma/mostrarWelcome.do

Adobe Reader DC

Cuando se abre un documento PDF con una Firma Digital utilizando la herramienta Adobe Reader DC, esta se encarga de validar las firmas digitales contenidas en el documento. Para verificar que el formato de Firma Digital utilizado garantiza la validez de la firma de ese documento en el tiempo, procedemos de la siguiente forma:

1. Abrimos el documento.
2. Desplegamos el Panel de Firma, pulsando en el botón. 

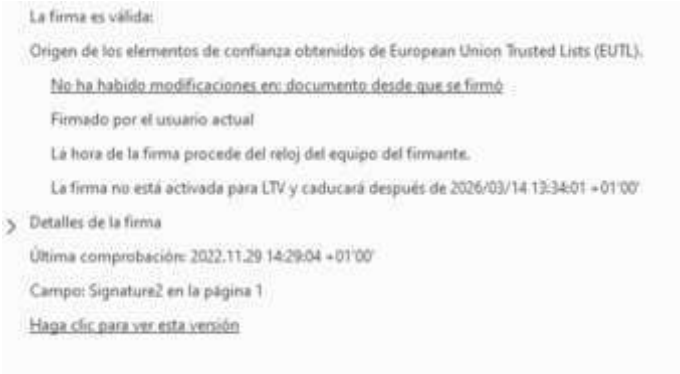
3. Se selecciona la Firma Digital que se desea verificar en el Panel de Firmas y procedemos a abrir el detalle de esa firma dando doble click en el botón. 

Adobe Reader DC

4. Al abrir el detalle de la Firma Digital aparecen una serie de datos que nos confirman que la misma es válida.

   a. Primero Adobe Reader nos indica: “La firma es válida”.
   b. También que No ha habido modificaciones en Documento desde que se firmó.
   c. Nos muestra que el documento ha sido Firmado por el usuario actual.
   d. Se nos indica que el documento cuenta con una estampa de tiempo con el mensaje “La firma incluye una marca de hora incrustada.”

   e. Y lo más importante, el documento indica: La firma está activada para LTV, lo que garantiza que esa Firma Digital se mantenga válida a lo largo del tiempo.



ADOBE READER DC: AGREGAR FIRMA

Los pasos para agregar una Firma Digital a un documento PDF utilizando Adobe Reader DC

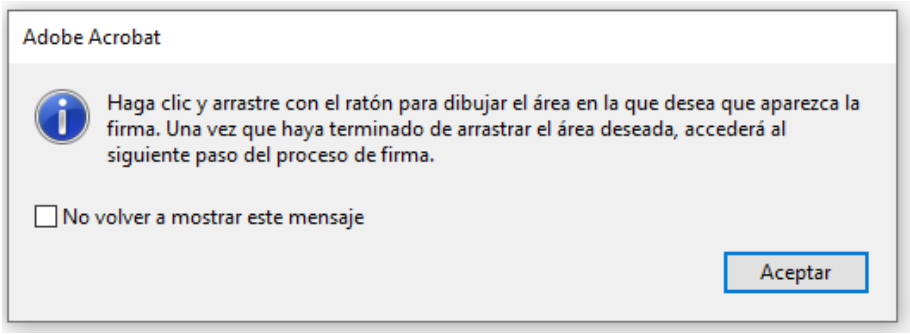
1. Abrimos el documento PDF que se desea firmar digitalmente
2. Elegimos la opción Herramientas ubicada en la parte superior de la aplicación y pulsamos en el icono Certificados, tal como muestra la siguiente imagen:

ADOBE READER DC: AGREGAR FIRMA

3. Seguidamente, debemos pulsar sobre la opción Firmar digitalmente, situada en la parte superior del documento.

ADOBE READER DC: AGREGAR FIRMA

4. En la siguiente ventana que se muestra, Aceptamos y tras ello deberemos de trazar mediante el ratón un rectángulo, un área sobre el lugar donde se desee que aparezca una representación visual de la firma digital.

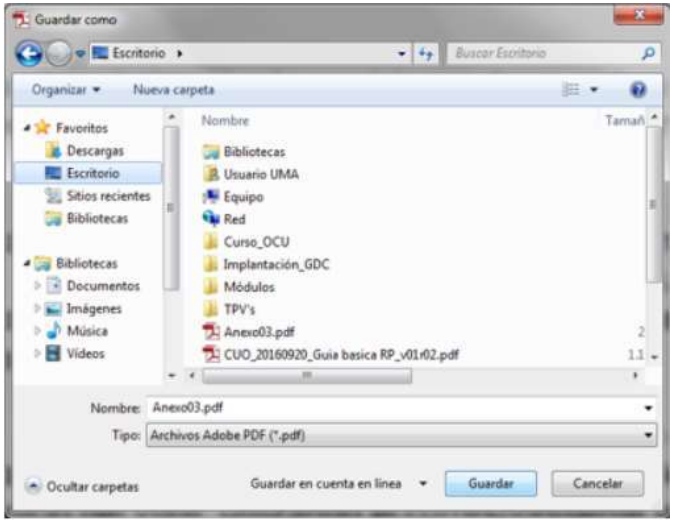


ADOBE READER DC: AGREGAR FIRMA

5. Posteriormente, se abrirá la ventana de Firmar Documento. En el desplegable Firmar como se deberá seleccionar el certificado digital de la persona que va a firmar el documento y presionar el botón Continuar y tras ellos en la nueva ventana que sale Firmar.

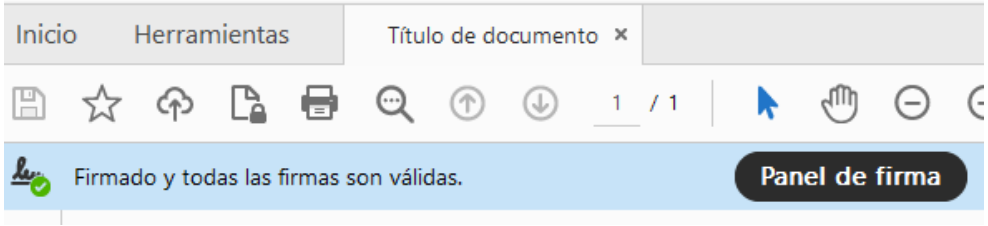
ADOBE READER DC: AGREGAR FIRMA

6. En este punto, la herramienta nos solicitará la dirección donde se va a guardar el documento firmado. Adobe Reader creará un nuevo documento cuando se le agrega la Firma Digital, por lo cual deberá elegir la carpeta donde guardará el documento firmado.



ADOBE READER DC: AGREGAR FIRMA

7. Como resultado final, obtendremos un documento PDF firmado digitalmente, como podemos ver en la siguiente ilustración. En él, se visualiza el mensaje: “Firmado y todas las firmas son válidas”, lo que nos brinda garantía de la validez de la Firma Digital del documento electrónico. También se advierte el Panel de Firma en la parte superior derecha, con el que podemos comprobar las firmas digitales que contiene el documento.



Este panel se despliega en el lado izquierdo y nos revela por quien está firmado el documento y toda la información relacionada con esa Firma Digital

FIRMA CON 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 que debe aplicar, liberando así, al usuario de cualquier duda técnica.

FIRMA CON AUTOFIRMA

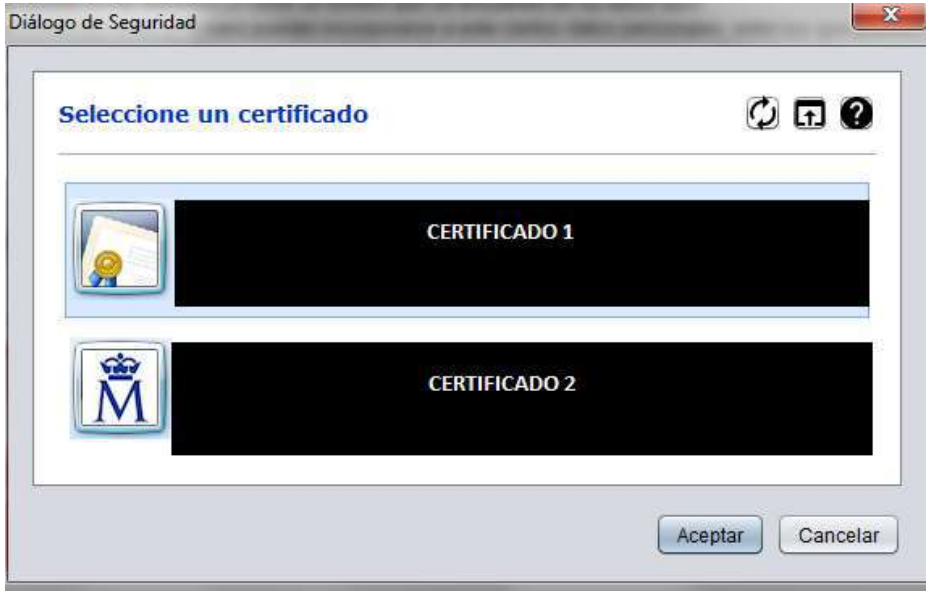
Una vez seleccionado el fichero que vamos a firmar, aparecerá la siguiente pantalla donde tendremos que marcar la opción *"**Hacer la firma visible dentro del PDF**"* y **pulsaremos el botón "Firmar fichero".**

FIRMA CON AUTOFIRMA

1. La siguiente pantalla que aparecerá será la de posición de firma. En ella tendremos que seleccionar el área donde queremos que la firma quede ubicada en el documento y, a continuación, haremos click en Siguiente

FIRMA CON AUTOFIRMA

2. La aplicación ofrecerá el/los certificados/s con el/los cual/es podemos formalizar la firma del documento. Seleccionamos el certificado deseado y hacemos click en . Aceptar



FIRMA CON AUTOFIRMA

3. Una vez firmado el documento, nos aparece una nueva pantalla que nos permite guardar el documento ya firmado mediante certificado digital, proponiéndonos el nombre del archivo. Al hacer click en Guardar hemos finalizado el procedimiento.

4 INCIDENCIAS RECURRENTES

¿Y AHORA QUÉ?

versia

¿Y ahora qué hago?

No me deja firmar (caducado, bloqueado, revocado)

No me deja firmar (instalación de software necesario para la firma)

No me deja firmar (instalación de software necesario para la firma)