



**Junta de
Castilla y León**

Delegación Territorial de León
Dirección Provincial de Educación

La Administración Electrónica. La identificación digital. La firma digital.

**20, 21 y 22
septiembre 2021**



Licencia de Creative Commons

La administración Electrónica, Certificado Electrónico y Firma Digital. by Emilio Fernández Delgado is licensed under a Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License.

This work is licensed under the Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License. To

view a copy of this license, visit

<http://creativecommons.org/licenses/by-nc-nd/4.0/>.



**Junta de
Castilla y León**

Delegación Territorial de León
Dirección Provincial de Educación

La Administración Electrónica. La identificación digital. La firma digital.

**20, 21 y 22
septiembre 2021**



Licencia de Creative Commons

La administración Electrónica, Certificado Electrónico y Firma Digital. by Emilio Fernández Delgado is licensed under a Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License.

This work is licensed under the Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License. To view a copy of this license, visit

<http://creativecommons.org/licenses/by-nc-nd/4.0/>.



**Junta de
Castilla y León**

Delegación Territorial de León
Dirección Provincial de Educación

La Administración Electrónica. La identificación digital. La firma digital.

**20, 21 y 22
septiembre 2021**



Licencia de Creative Commons

La administración Electrónica, Certificado Electrónico y Firma Digital. by Emilio Fernández Delgado is licensed under a Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License.

This work is licensed under the Creative Commons Reconocimiento-NoComercial-SinObraDerivada 4.0 Internacional License. To

view a copy of this license, visit

<http://creativecommons.org/licenses/by-nc-nd/4.0/>.

La legislación vigente relacionada con la administración electrónica.

La administración electrónica se comienza a gestar desde cuando se plantea en la administración la integración de los medios informáticos en su gestión.

En la década de los '70 del siglo pasado se desarrolló la primera de una inagotable sucesión de leyes, reglamentos y normas para regular la integración, en aquel momento, de las nuevas máquinas, los ordenadores.

La legislación vigente relacionada con la administración electrónica.

En los años siguientes los diferentes gobiernos han ido desarrollando una serie de leyes para regular el desarrollo de la administración electrónica adaptándose y adaptando los medios y procedimientos.

Estas Leyes, reglamentos y normas regulan el funcionamiento de la propia administración en su relación con el ciudadano, pero del mismo modo marcan las pautas que el ciudadano deberá seguir y respetar en su relación con la administración electrónica.

La legislación vigente relacionada con la administración electrónica.

Las Leyes y normas jurídicas constituyen la base del desarrollo de la administración electrónica dotando a ésta del respaldo necesario para su implantación y normal funcionamiento.

En la página web del portal de la administración electrónica podemos encontrar actualizada y organizada la documentación correspondiente a la legislación básica de la administración electrónica. [Pincha aquí](#) para acceder a ella.

Aquí encontraréis la legislación vigente en cada uno de los ámbitos nacional, autonómico y de la Unión Europea.

La legislación vigente relacionada con la administración electrónica.

A continuación encontramos algunas de las mas relevantes.

El siguiente reglamento desarrolla la ley 39/2015, de 1 de octubre y la 40/2015, de 1 de octubre, Procedimiento Administrativo común de las Administraciones Públicas y Régimen Jurídico del Sector Público respectivamente. Éste se desarrolla la actuación y el funcionamiento electrónico del sector público.

[Real Decreto 203/2021, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos.](#)

La Administración Electrónica
La identificación digital
La firma digital

20, 21 y 22
septiembre
2021



Junta de
Castilla y León

Delegación Territorial de León
Dirección Provincial de Educación



Ayuda

Pasos para la
Tramitación Electrónica

La legislación vigente relacionada con la administración electrónica.

En las web de las diferentes administraciones que intervienen en la gestión y desarrollo de la Administración Electrónica (e-administración) se puede tener acceso a normas y reglamentos específicos de cada una de ellas.



La identificación digital

Nuestra identidad digital regulada en esa gran cantidad de normas, leyes y reglamentos se sustenta sobre tres sistemas o soportes.

Dos de ellos son elementos físicos:

El DNI-e y el Certificado Digital

Estos dos sistemas nos serán útiles a la hora de identificarnos y realizar tramites con las administraciones y otras entidades.

Y un tercero virtual:

El sistema CL@VE.

Este es un sistema de identificación para las relaciones con las administraciones públicas.

20, 21 y 22
septiembre
2021



El DNI-e

La primera versión del DNI electrónico es una tarjeta de un material plástico, que incorpora un chip con información digital y que tiene unas dimensiones idénticas a las del DNI tradicional, por tanto, coincide con las dimensiones de las tarjetas de crédito comúnmente utilizadas.

Descripción física del DNI electrónico

El nuevo Documento Nacional de Identidad dispondrá de un Chip electrónico en el que se registrarán los datos del titular:

- Datos de filiación del titular
- Imagen digitalizada de la fotografía
- Imagen digitalizada de la firma manuscrita
- Plantilla de la impresión dactilar
- Certificado reconocido de autenticación y de firma
- Certificado electrónico de la autoridad emisora
- Par de claves de cada certificado electrónico

El Documento Nacional de Identidad recogerá gráficamente los siguientes datos:

- Apellidos y nombre
- Fecha de nacimiento
- Sexo
- Nacionalidad

Número de serie del soporte

Kinegrama

Posee una fotografía blanco y negro con un holograma en la

Relieves

Firma manuscrita del

Equipo de expedición

Caracteres OCR-B de lectura automática

Imagen cambiante grabada en láser

Número personal de Documento Nacional de Identidad y carácter de verificación

Datos de filiación del titular:

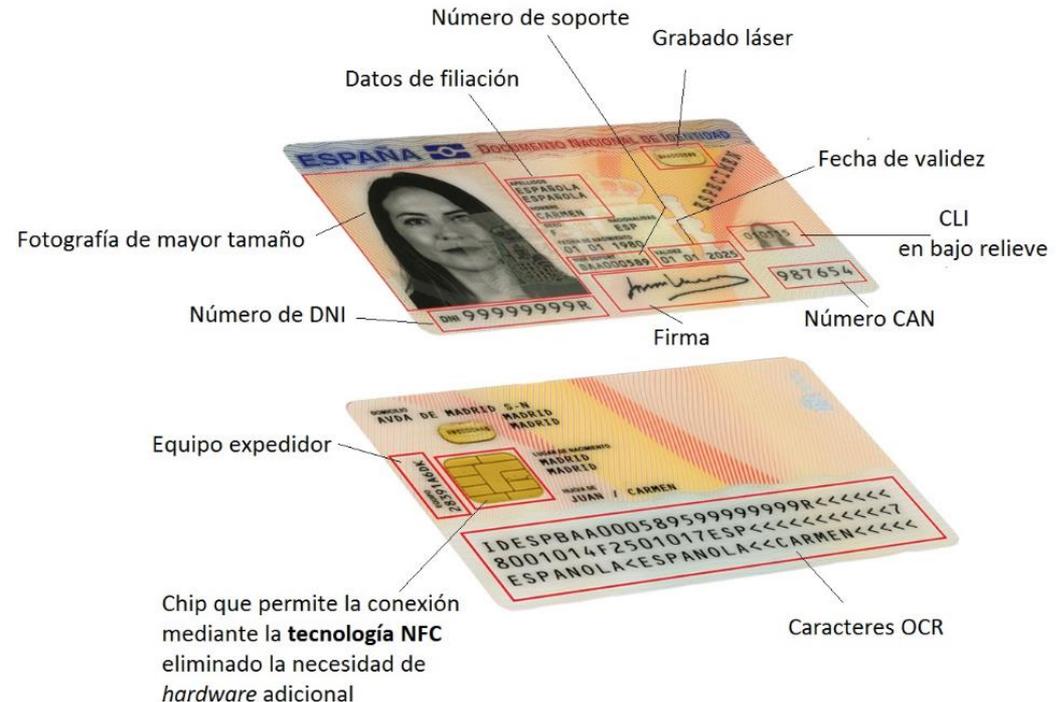
- Lugar de nacimiento (localidad)
- Provincia (si ha nacido en España) o Nación (si ha nacido en el extranjero)
- Nombre de los padres
- Domicilio
- Provincia
- Nación

El DNI 3.0

El DNI 3.0, que desde diciembre de 2015, es el único documento que se expide en todas las Oficinas de Expedición del territorio nacional, es como su antecesor, una tarjeta de un material plástico con un chip digital y de idénticas dimensiones.



El **DNIe 3.0** incorpora un chip *dual interface*, que permite la conexión mediante contacto o de forma inalámbrica mediante tecnología NFC.



DNI-e <> DNI 3.0

El primer DNLe, expedido desde 2006 hasta finales de 2015 incorporaba, a diferencia de su predecesor, un chip en el anverso con información digital y se presentaba por primera vez en una tarjeta de policarbonato con las mismas medidas que una tarjeta de crédito convencional.

Los avances tecnológicos recogidos en el chip permiten al ciudadano conectar con la Administración de forma digital, hacer uso de su identidad electrónica, firmar documentos digitalmente y de forma remota.

Para ello, el ciudadano ha de disponer de un dispositivo hardware que permita la lectura de los certificados contenidos en el chip, y posibilite la conexión a los distintos servicios digitales, así como instalar los diferentes drivers necesarios para el funcionamiento del hardware.

DNI-e <> DNI 3.0

Los cambios en la sociedad de la información requieren la constante actualización del DNI. Conscientes de la necesidad no sólo de implementar un instrumento de elevada seguridad, sino también de mejorar y acercar a los ciudadanos su usabilidad, la Dirección General de la Policía lanzó en 2015 el DNI 3.0. La principal novedad frente a su antecesor es la presencia de un chip con interfaz dual que permite la conexión mediante hardware, pero también de forma inalámbrica a través de la tecnología NFC (Near Field Communication)

La tecnología NFC está presente en la mayoría de los smartphones y tablets del mercado y su funcionamiento se basa en la creación de un campo electromagnético en el que, mediante inducción, se genera un intercambio de datos entre dispositivos.

DNI-e <> DNI 3.0

Para utilizar la funcionalidad inalámbrica del DNI 3.0 únicamente será necesario disponer de:

- Un teléfono Smartphone o tablet con tecnología NFC.
- App del servicio al que nos queremos conectar.
- El ciudadano no tendrá por tanto, que descargarse ningún certificado o driver, sino que la conexión se iniciará simplemente con acercar el DNI 3.0 a la antena NFC del dispositivo, (a una distancia no superior a 1 cm).

DNI-e <> DNI 3.0

En ambos casos es necesaria la adecuada configuración de los equipos a utilizar. Para el DNI-e se requiere...

Elementos hardware

Requiere el siguiente equipamiento físico:

Un Ordenador personal (Intel -a partir de Pentium III- o tecnología similar).

Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816.

Para elegir un lector que sean compatible con el DNI 3.0, verifique que, al menos:

Cumpla el estándar ISO 7816 (1, 2 y 3).

Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1).

Soporta velocidades de comunicación mínimas de 9.600 bps.

Soporta los estándares API PC/SC (Personal Computer/Smart Card)

Elementos software

Sistemas operativos: El DNIe puede operar en diversos entornos (Windows 7 y superiores
GNU/Linux, MAC, Unix)

Navegadores: El DNI 3.0 es compatible con todos los navegadores, como Microsoft Internet Explorer, Google Chrome, Mozilla Firefox

DNI-e <> DNI 3.0

Controlador del Lector:

Para operar con un lector de tarjetas inteligentes, será necesario instalar un driver que, normalmente, se distribuye con el propio lector.

Controladores / Módulos criptográficos de la tarjeta DNI 3.0

Para poder interaccionar adecuadamente con las tarjetas criptográficas en general y con el DNI 3.0 en particular, el equipo ha de tener instalados unas "piezas" de software denominadas módulos criptográficos. En un entorno Microsoft Windows, el equipo debe tener instalado driver denominado Minidriver o CardModule y PKCS#11. En los entornos UNIX / Linux o MAC podemos utilizar el DNI 3.0 a través de un módulo criptográfico denominado PKCS#11.

Instalación automática CardModule:

Para aplicativos Microsoft como Internet Explorer o para Google Chrome basta con tener el equipo conectado a Internet e insertar la tarjeta en el lector. El servicio Windows Update buscará automáticamente el driver de la tarjeta y lo instalará al tratarse de un dispositivo Plug & Play. Instalación Automática CardModule Explorer y Chrome; Instalación Automática CardModule Mozilla Firefox.

DNI-e <> DNI 3.0

Instalación manual CardModule:

Si por cualquier razón no se puede realizar la instalación automática, hay disponible un instalable para realizar la instalación de modo manual.

Instalación PCKS11:

Para instalar el módulo criptográfico PKCS11 se deben seguir las recomendaciones contenidas en Instalación Módulos PKCS#11

Para el DNI 3,0 se requiere...

La tecnología NFC se basa en la proximidad entre dispositivos. Una antena interna de radiofrecuencia conecta directamente el smartphone o tablet con el DNI 3.0 permitiendo el acceso a los distintos servicios telemáticos. Bastará con situar el DNI 3.0 en la parte posterior de su teléfono o tablet para que la antena NFC del dispositivo energice la antena contenida dentro del chip de la tarjeta y se establezca la comunicación. Por motivos de seguridad y conectividad, la distancia entre ambos ha de ser menor a 1 cm ya que si no, la conexión se interrumpiría impidiendo el acceso a cualquier dato o autenticación.

DNI-e <> DNI 3.0

Elementos hardware

Un dispositivo con NFC que cumpla el estándar ISO 14443, tipo A o B, ya que el DNI 3.0 es compatible con ambas implementaciones del estándar ISO 14443. Éste puede ser un Smartphone, una tablet o un lector NFC. Para elegir un dispositivo compatible con el DNI 3.0, verifique que cumple "ISO 14443 - Partes 1/2/3/4. Protocolo de transmisión T=CL"

Elementos software

APP que utilice el DNI 3.0 para identificar al usuario y acceder a un servicio específico o para firmar electrónicamente un documento con igualdad jurídica que la firma manuscrita.

Para elegir un lector que sean compatible con el DNI 3.0, verifique que, al menos:

Cumpla el estándar ISO 7816 (1, 2 y 3).

Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1).

Soporta velocidades de comunicación mínimas de 9.600 bps.

Soporta los estándares:

API PC/SC (Personal Computer/Smart Card)

CSP (Cryptographic Service Provider, Microsoft)

API PKCS#11

DNI-e y DNI 3.0

En la página web www.dnielectronico.es se encuentran una serie de posibles soluciones a los problemas de hardware y software que nos encontramos a la hora de utilizar este dispositivo.

Podemos encontrar información de ayuda para la obtención del DNI, ahora ya únicamente el DNI 3.0.

El certificado digital

La FNMT-RCM, como Proveedor de Servicios de Certificación a través de CERES, ha implementado una serie de aplicaciones que permiten a la **Administración, a los ciudadanos y a las empresas españolas** realizar sus trámites a través de Internet de forma totalmente segura. Las nuevas soluciones de certificación y autenticación de identidad digital que ofrece la FNMT-RCM proporcionan **validez y seguridad a las transacciones electrónicas**.

El certificado digital es el documento digital que contiene los datos identificativos de su propietario.

El certificado digital

Pueden poseer certificado digital emitido por la FNMT:

- Las personas físicas.
- Las personas jurídicas. (representante)
- En las administraciones públicas:
- Certificados de firma electrónica del personal al servicio del sector público.
- Certificado de sede electrónica en el ámbito de la administración.
- Certificado de sello electrónico en el ámbito de la administración.
- Autoridad de Certificación RAIZ.
- Autoridad de certificación subordinada
- Certificados de componentes

El certificado digital

Para la obtención del certificado digital de la FNMT es necesario comprobar que contamos con la configuración previa necesaria.

Debemos comprobar que tenemos instalado el generador de claves, configurador FNMT-RCM.

Instalaremos el configurador y la aplicación Autofirma.

Se debe de realizar todo el proceso de obtención desde el mismo equipo y mismo usuario (anteriormente era necesario incluso hacerlo desde el mismo navegador).

En la actualidad los navegadores compatibles se corresponden con aquellos más comunes: Mozilla Firefox, Google Chrome, Microsoft Edge, Opera y Safari.

El certificado digital. La configuración

En el siguiente enlace se encuentran las indicaciones necesarias para la configuración adecuada de nuestro equipo.

<https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software/configuracion-previa>



Sede Electrónica

Real Casa de la Moneda
Fábrica Nacional
de Moneda y Timbre

Obtener Certificados Electrónicos | Trámites

Inicio > Obtener Certificados Electrónicos > Persona Física > Obtener Certificado Software > Configuración Previa

Persona Física

Obtener Certificado Software

Configuración Previa

Solicitar Certificado

Acreditar Identidad

Descargar Certificado

Obtener Certificado con DNle

Configuración

Solicitud

Acreditación

Descarga



2

3

4

1. Configuración previa

Antes de comenzar con el proceso de solicitud de su Certificado, deberá asegurarse de que su equipo tiene instalado el **software necesario para la generación de claves. CONFIGURADOR FNMT-RCM**

Por favor, lea y siga atentamente las siguientes instrucciones para evitar posibles errores durante el proceso de obtención de su certificado:

El certificado digital. La solicitud.

Una vez configurado nuestro ordenador iniciaremos la solicitud del certificado.

Aquí nos identificaremos con nuestro DNI rellenando con 0 a la izquierda hasta completar los 9 dígitos.

Con nuestro primer apellido tal y como aparece en el DNI.

Y el correo-e, imprescindible para recibir el código de solicitud que será imprescindible para autenticarnos.

Persona Física

- Obtener Certificado Software
- Configuración Previa
- Solicitar Certificado**
- Acreditar Identidad
- Descargar Certificado
- Obtener Certificado con DNIe
- Obtener Certificado con Android
- Verificar estado
- Renovar
- Anular

Certificado de Representante

Configuración Solicitud Acreditación Descarga

1 2 3 4

NOTA: Antes de realizar este paso es necesario instalar el software del paso 1 Configuración.

2. Solicitar Certificado

SOLICITUD DE CERTIFICADO FNMT DE PERSONA FÍSICA

Para tramitar la solicitud de su Certificado FNMT de Persona Física, por favor introduzca la información requerida:

Nº DEL DOCUMENTO DE IDENTIFICACIÓN

PRIMER APELLIDO(tal y como aparece en su documento de identificación)

CORREO ELECTRÓNICO

Confirme aquí su CORREO ELECTRÓNICO

El certificado digital. La acreditación

La acreditación de nuestra identidad la realizaremos en el registro de la Delegación o Subdelegación del gobierno, la Agencia Tributaria, Seguridad Social o delegación de Hacienda.

Una vez acreditada nuestra identidad en alguna de estas oficinas podremos volver al mismo ordenador y en el mismo usuario y con el mismo navegador que lo solicitamos proceder a la descarga.

Persona Física
Obtener Certificado Software
Configuración Previa
Solicitar Certificado
Acreditar Identidad
Descargar Certificado
Obtener Certificado con DNIe
Obtener Certificado con Android
Verificar estado
Renovar
Anular
Certificado de Representante
Cartera Pública

Configuración Solicitud **Acreditación** Descarga



3. Acreditar Identidad

AVISO: Ante la situación actual de la evolución del COVID 19 no todas las oficinas de acreditación están prestando servicio de forma habitual, por este motivo y para evitar desplazamientos innecesarios, es recomendable que antes de acudir se pongan en contacto con el organismo en cuestión para verificar que sigue prestando este servicio. Disculpen las molestias.

Tras haber realizado la [configuración previa \(paso 1\)](#) y haber completado la [solicitud de su certificado \(paso 2\)](#), ya estará en posesión de su Código de Solicitud. Para continuar el solicitante y futuro titular del certificado deberá acudir personalmente a una Oficina de Acreditación de Identidad para acreditar su propia identidad.

Si por cualquier circunstancia no pudiera hacerlo personalmente, podrá ir una tercera persona en su nombre, pero se le exigirá la previa legitimación de su firma del contrato ante notario.

[Más información sobre la legitimación de firma ante notario](#)

[¿Se puede solicitar un certificado de representación de personas físicas?](#)

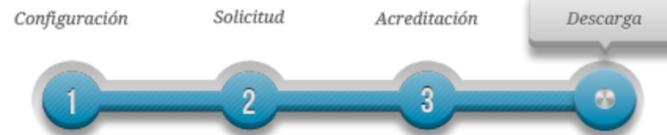
NOTA: Cuando acredite su identidad en una oficina de acreditación de identidad tendrá inmediatamente disponible la descarga de su certificado por lo que le recomendamos descargarlo lo antes posible.

Documentación necesaria para acreditar identidad:

El certificado digital. La descarga

Ya en nuestro ordenador iremos a la opción de descarga y cumplimentando los datos requeridos: DNI, primer apellido y código de solicitud, procedemos a la descarga.

Persona Física
Obtener Certificado Software
Configuración Previa
Solicitar Certificado
Acreditar Identidad
Descargar Certificado
Obtener Certificado con DNle
Obtener Certificado con Android
Verificar estado
Renovar
Anular
Certificado de Representante
Sector Público



4. Descargar Certificado

Para descargar el certificado debe usar el mismo ordenador y el mismo usuario con el que realizó la Solicitud e introducir los datos requeridos exactamente tal y como los introdujo entonces.

DESCARGAR CERTIFICADO FNMT DE PERSONA FÍSICA

Para descargar e instalar su certificado introduzca la siguiente información:

Nº DEL DOCUMENTO DE IDENTIFICACIÓN

PRIMER APELLIDO

CÓDIGO DE SOLICITUD

[Pulse aquí para consultar y aceptar las condiciones de uso del certificado](#)

[Descargar Términos y Condiciones](#)

[Descargar Certificado](#)

El certificado digital. La descarga

Ya en nuestro ordenador iremos a la opción de descarga y cumplimentando los datos requeridos: DNI, primer apellido y código de solicitud, procedemos a la descarga.

Al iniciar la descarga nos preguntará si queremos hacer una copia de seguridad de nuestro certificado. Esto consiste en la descarga directa en una carpeta.

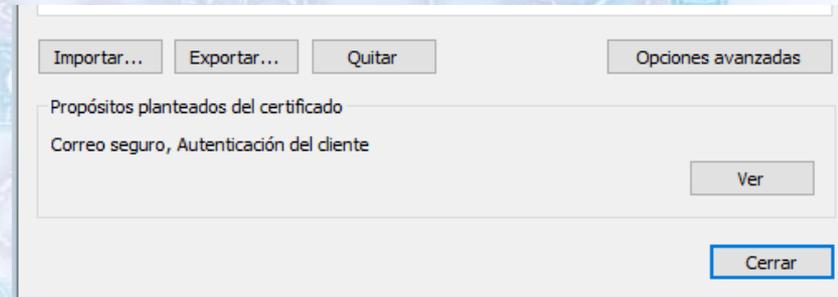
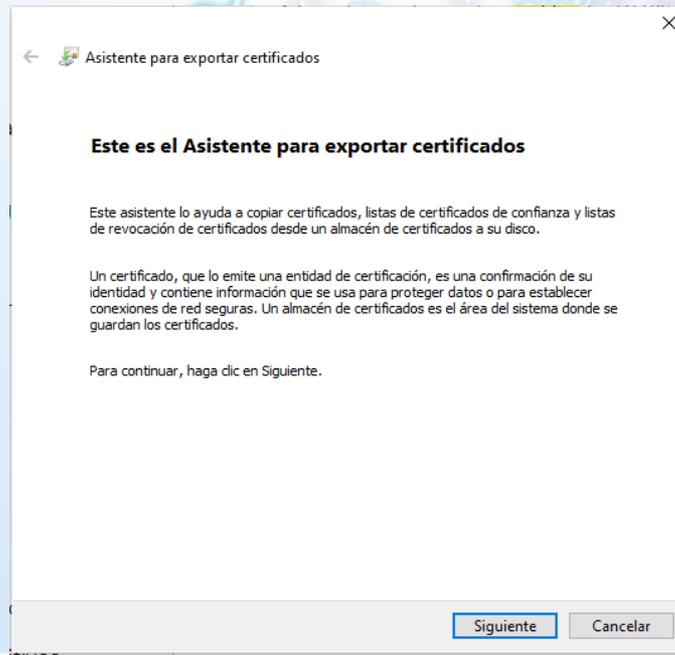
En este proceso nos pedirá que le asignemos una clave al certificado para poder instalarlo en otro ordenador.

Podemos no hacerla ahora y hacerla más adelante ya que el proceso de descarga consiste, realmente, en la instalación en nuestro ordenador del certificado.

El certificado digital. Exportación, Eliminación e instalación.

Seleccionando el certificado podremos exportarlo o quitarlo.

En primer lugar una vez descargado, lo más aconsejable si no lo hemos hecho previamente, es hacer una copia de nuestro certificado. Para esto utilizaremos la opción “Exportar”.



Una vez seleccionemos el Certificado y hagamos click en el botón exportar se abrirá el asistente para exportar certificados.

El certificado digital. Exportación, Eliminación e instalación.

En la siguiente ventana nos pregunta si queremos exportar la clave privada o no.

Si lo hacemos sin clave privada, únicamente podremos autenticarnos en los trámites que sea necesario pero no podremos firmar ningún documento.

Es aconsejable cuando hacemos nuestra primera copia de seguridad del certificado que contenga todas las partes del mismo y así poder instalarlo completo si fuera necesario.

El certificado es lo que utiliza para autenticarnos.

La clave privada es lo que utiliza para firmar digitalmente.

← Asistente para exportar certificados

Exportar la clave privada
Puede elegir la exportación de la clave privada con el certificado.

Las claves privadas se protegen con contraseñas. Si desea exportar la clave privada con el certificado, debe escribir una contraseña en una página posterior.

¿Desea exportar la clave privada con el certificado?

Exportar la clave privada

No exportar la clave privada

Nota: la clave privada asociada está marcada como no exportable. Solamente puede exportarse el certificado.

Siguiente Cancelar

El certificado digital. Exportación, Eliminación e instalación.

Cuando una clave privada no es exportable únicamente se habilitarán las opciones de formato.

Aquí seleccionaremos las opciones necesarias para nuestro certificado.

Estas opciones se habilitan cuando exportamos nuestro certificado sin clave privada exportable.

Incluye los certificados necesarios para la exportación.

Esta opción dejará el ordenador en el que estaba instalado sin la opción de firmar digitalmente.

Habilitamos todas las características del certificado.

← Asistente para exportar certificados

Formato de archivo de exportación
Los certificados pueden ser exportados en diversos formatos de archivo.

Seleccione el formato que desea usar:

- DER binario codificado X.509 (.CER)
- X.509 codificado base 64 (.CER)
- Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
 - Incluir todos los certificados en la ruta de certificación (si es posible)
- Intercambio de información personal: PKCS #12 (.PFX)
 - Incluir todos los certificados en la ruta de certificación (si es posible)
 - Eliminar la clave privada si la exportación es correcta
 - Exportar todas las propiedades extendidas
 - Habilitar privacidad de certificado
 - Almacén de certificados en serie de Microsoft (.SST)

Siguiente Cancelar

El certificado digital. Exportación, Eliminación e instalación.

Ahora es el momento de mantener nuestro certificado lo más seguro posible. Para ello el sistema nos pedirá que le asignemos a nuestro certificado un contraseña para protegerlo de usos fraudulentos o accidentales.

Empresas u organizaciones dedicadas a prestar servicios de seguridad informática.

Seleccionamos contraseña

Introducimos nuestra contraseña. No se marcan exigencias en cuanto a la contraseña aunque deberíamos cumplir unos mínimos.

Repetimos la contraseña.

Una vez introducida la contraseña se activará el botón siguiente.

El certificado digital. Exportación, Eliminación e instalación.

Decidiremos en que lugar guardaremos nuestra copia del certificado y con que nombre.

Podemos asignar un nombre al certificado que nos ayude a la hora de buscarlo.

Podemos hacer una copia directamente en una unidad usb.

← Asistente para exportar certificados

Archivo que se va a exportar
Especifique el nombre del archivo que desea exportar

Nombre de archivo:

Examinar...

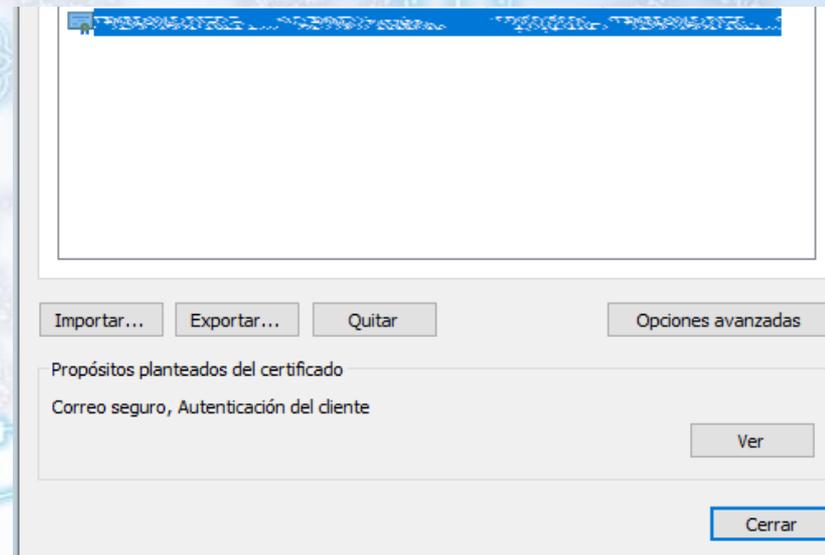
Siguiente Cancelar

El certificado digital. Exportación, Eliminación e instalación.

Supongamos que hemos hecho la solicitud en el ordenador del trabajo o en el del aula, una vez descargado y hecha la copia de seguridad lo deberíamos eliminar, o cuando estamos utilizando un ordenador que no es el nuestro y en el que no queremos que nuestro certificado quede ahí instalado debemos QUITAR del ordenador nuestro certificado.

Para ello seleccionamos el certificado que queremos eliminar y hacemos click en el botón “Quitar”

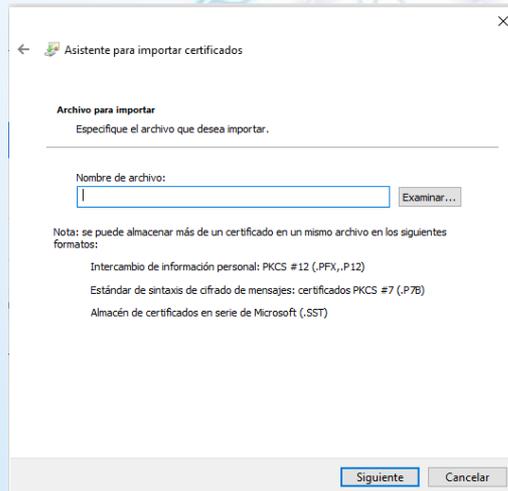
El certificado desaparecerá del administrador y nadie lo podrá utilizar sin nuestro consentimiento.



El certificado digital. Exportación, Eliminación e instalación.

La instalación es el proceso junto con la eliminación que en más ocasiones repetiremos.

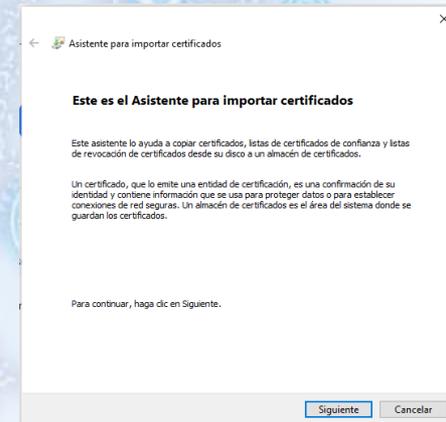
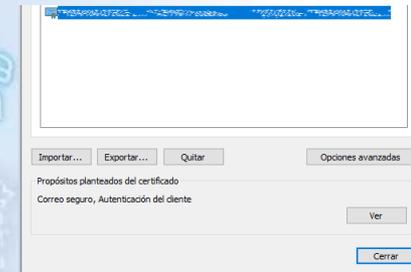
Para instalar nuestro certificado desde una unidad USB o desde el disco duro del ordenador hacemos click en Importar y se nos abre una nueva ventana.



Pulsamos “siguiente” y se abre una nueva ventana.

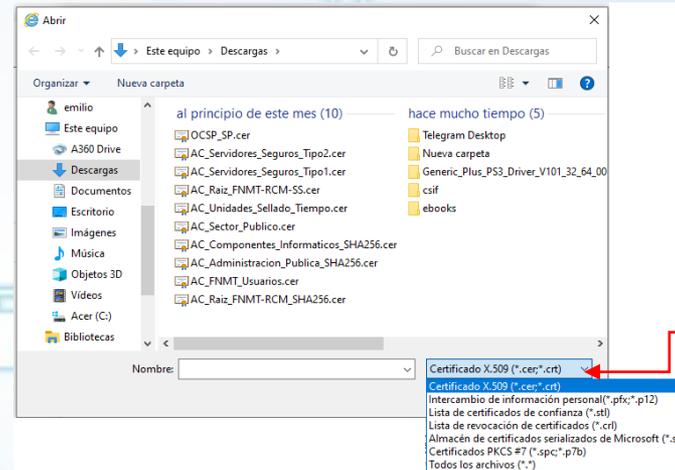
Hacemos click en examinar

lo que nos abre una ventana para buscar nuestro certificado en la carpeta en la que lo tengamos almacenado.



El certificado digital.

Exportación, Eliminación e instalación.



Tipo de documento

En esta ventana debemos seleccionar en tipo “*,*” ya que existen varios tipos diferentes de documentos para los certificados.

Con este asistente podemos importar certificados personales, de empresas o de entidades de certificación.

Seleccionamos en la ubicación en que tengamos almacenado nuestro certificado, lo seleccionamos y hacemos click en abrir.

El certificado digital. Exportación, Eliminación e instalación.

Hacemos click en siguiente y nos pedirá la contraseña que le hemos asignado cuando hemos hecho nuestra copia de seguridad o la hemos exportado con clave privada exportable.

← Asistente para importar certificados

Protección de clave privada
Para mantener la seguridad, la clave privada se protege con una contraseña.

Escriba la contraseña para la clave privada.

Contraseña:

 Mostrar contraseña

Opciones de importación:

Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.

Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.

Proteger la clave privada mediante security(Non-exportable) basada en virtualizado

Incluir todas las propiedades extendidas.

Siguiente Cancelar

Contraseña

Cuando un programa o una web hace uso de nuestro certificado nos aparecerá una ventana emergente de alerta.

Incluimos la condición de exportable a nuestra clave privada, lo que nos permite poder hacer una copia de seguridad desde este ordenador.

La seguridad basada en virtualización (VBS) usa el módulo TPM para almacenar claves. Se puede acceder a la clave desde el sistema operativo, pero no estará disponible si se cambia el sistema operativo.

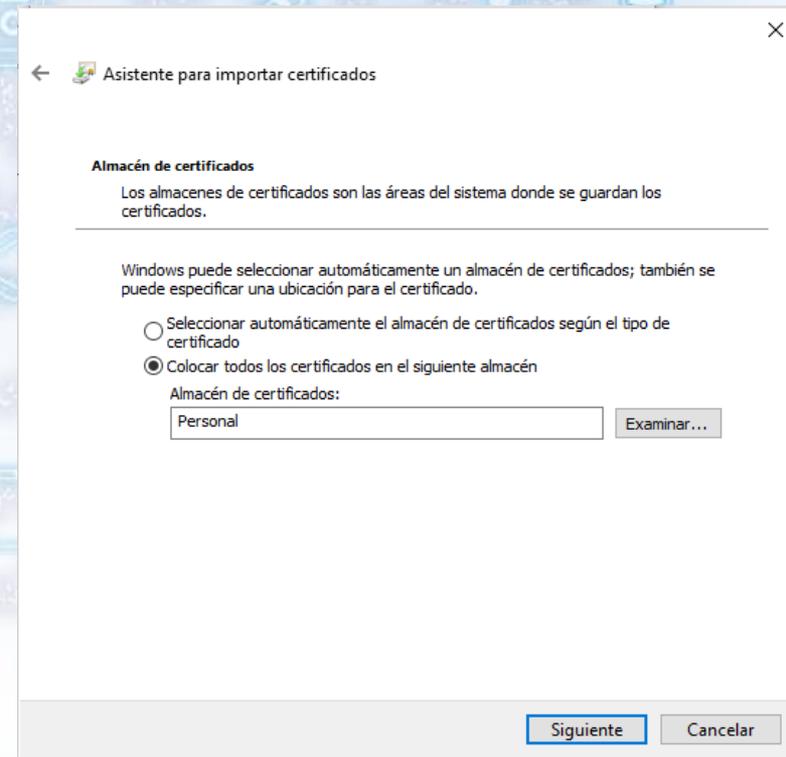
[Para más información haz click aquí](#)

El certificado digital. Exportación, Eliminación e instalación.

El asistente nos preguntará dónde queremos guardar nuestro certificado.

El administrador de certificados tiene una distribución predeterminada y por defecto nos propone una ubicación.

Será conveniente mantener esta ubicación para que a la hora de localizar los certificados cuando sea necesario no tengamos complicaciones innecesarias.

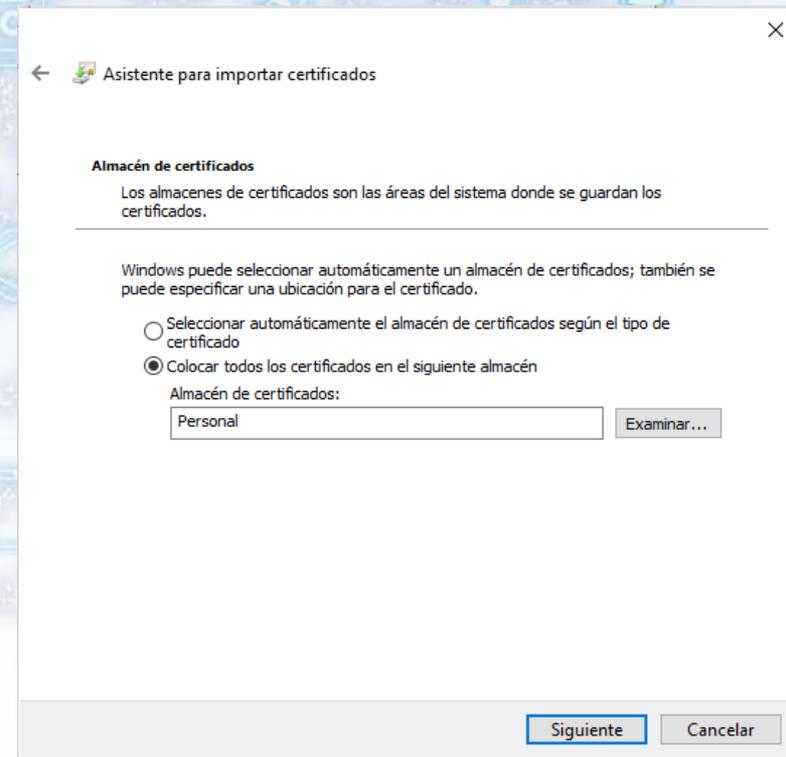


El certificado digital. Exportación, Eliminación e instalación.

El asistente nos preguntará dónde queremos guardar nuestro certificado.

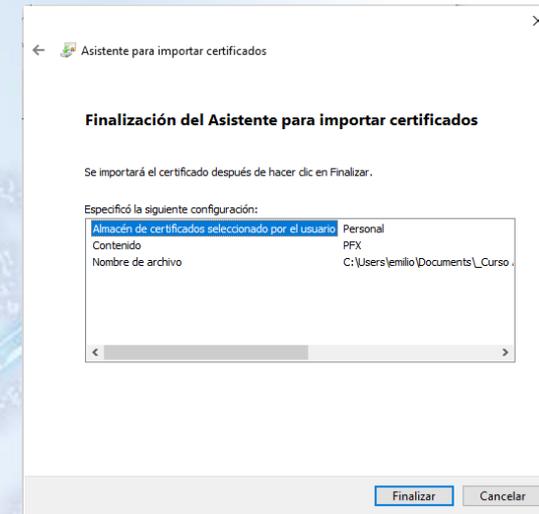
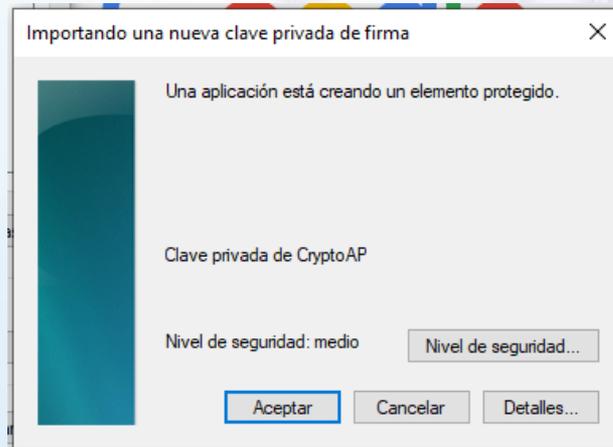
El administrador de certificados tiene una distribución predeterminada y por defecto nos propone una ubicación.

Será conveniente mantener esta ubicación para que a la hora de localizar los certificados cuando sea necesario no tengamos complicaciones innecesarias.



El certificado digital. Exportación, Eliminación e instalación.

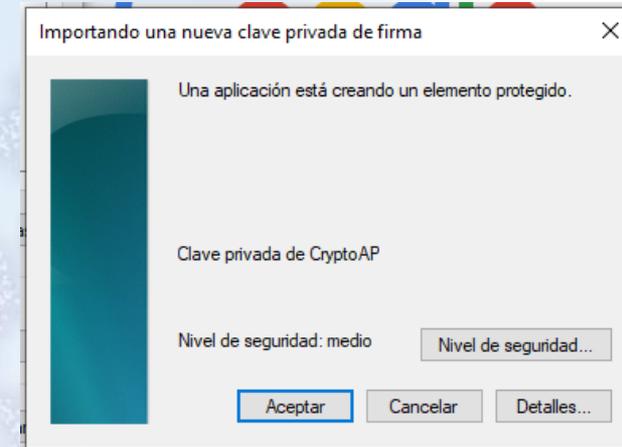
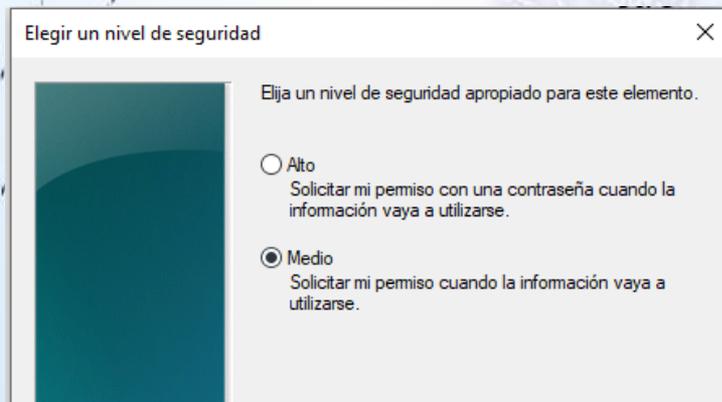
Para finalizar la instalación el asistente nos pide confirmación para importar el certificado.
Una vez hacemos click en finalizar nuestro certificado estará instalado en el equipo.



Cuando instalamos un nuevo certificado nuestro sistema operativo nos pedirá que confirmemos el nivel de seguridad que queremos aplicar a nuestro certificado[^]. Por defecto estará en nivel medio.

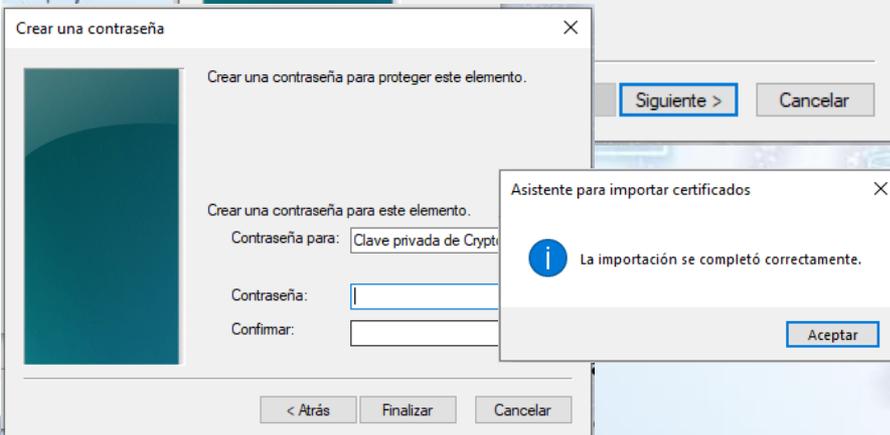
El certificado digital. Exportación, Eliminación e instalación.

Hacemos click en el botón “nivel de seguridad” y podremos cambiar las opciones.



Es aconsejable utilizar un nivel alto de seguridad para prevenir el uso fraudulento o accidental del certificado para la firma de documentos.

Le asignaremos una contraseña que se nos pedirá cada vez que se use nuestro certificado.



Cl@ve.

Identidad electrónica para las Administraciones

El sistema cl@ve es un sistema de identificación frente a los trámite que hacemos ante la administración pública.



Este sistema de identificación tiene tres opciones de uso.

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Cl@ve PIN

Es una forma de realizar trámites por Internet con una validez limitada en el tiempo y que se puede renovar cada vez que necesitemos. Este sistema de identificación electrónica está basado en el uso de un código elegido por el usuario y un PIN comunicado al teléfono mediante la app Cl@ve PIN o con un mensaje SMS

Cl@ve.

Identidad electrónica para las Administraciones

Este sistema de identificación tiene tres opciones de uso.

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Cl@ve PERMANENTE

Es un sistema de autenticación diseñado para personas que necesitan acceder frecuentemente a los servicios electrónicos de la Administración.

Se basa en el uso de un código de usuario, su DNI o NIE, y de una contraseña que se establece en el proceso de activación y que sólo debe ser conocida por ti.

Para los servicios de administración electrónica que requieran un nivel de seguridad elevado, el sistema refuerza la autenticación con la solicitud de introducción de un código numérico de un solo uso (One Time Password, OTP) que se envía previamente por mensaje SMS a tu teléfono móvil.

Cl@ve.

Identidad electrónica para las Administraciones

Este sistema de identificación tiene tres opciones de uso.

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Cl@ve FIRMA

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.

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.

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.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Requisito común para las tres opciones :

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.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – **Cl@ve PERMANENTE** – Cl@ve FIRMA

Requisito necesario para Cl@ve PERMANENTE y Cl@ve FIRMA:

- 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.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Requisito necesario para Cl@ve FIRMA:

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.

La expedición del Certificado irá asociada al soporte físico del documento que haya sido utilizado para el registro en Cl@ve y que será, en el caso de ciudadanos españoles el Documento Nacional de Identidad.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

[Para acceder al proceso de registro hacer click aquí.](#)

Accederemos haciendo click sobre el texto “Regístrate en Cl@ve”.

Si tenemos alguna duda en el proceso podemos hacer click en Ayuda.

The screenshot shows the top navigation bar of the Agencia Tributaria website. It includes the logos of the Spanish Government, the Ministry of Finance and Public Administration, and the Agencia Tributaria. A button for 'Sede Electrónica' is visible, with the tagline 'Todos los trámites on line'. Below the navigation bar, a breadcrumb trail reads: 'Sede Electrónica - Agencia Tributaria Inicio > Todos los trámites > Otros servicios > Registro Cl@ve > Registro Cl@ve'. The main content area is titled 'Procedimiento Registro Cl@ve'. Under the heading 'Trámites', there are two sub-sections: 'Trámites de registro' and 'Otros trámites'. Each sub-section contains a list of actions with corresponding 'Ayuda' (Help) buttons.

GOBIERNO DE ESPAÑA
MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

Agencia Tributaria Sede Electrónica
Todos los trámites on line

Sede Electrónica - Agencia Tributaria Inicio > Todos los trámites > Otros servicios > Registro Cl@ve > Registro Cl@ve

Procedimiento
Registro Cl@ve

▶ Trámites

▶ Trámites de registro

- ▶ Registrarse en Cl@ve [Ayuda](#)
- ▶ Registrarse en Cl@ve con certificado o DNI electrónico [Ayuda](#)
- ▶ Renunciar a Cl@ve [Ayuda](#)

▶ Otros trámites

- ▶ Regenerar Código de Activación de Cl@ve Permanente [Ayuda](#)
- ▶ Modificar el teléfono con certificado o DNI electrónico [Ayuda](#)
- ▶ Modificar el número de teléfono asociado a Cl@ve por VideoLlamada [Ayuda](#)
- ▶ Modificar el correo electrónico [Ayuda](#)
- ▶ Obtener un nivel de seguridad superior en Cl@ve con certificado o DNI electrónico [Ayuda](#)
- ▶ Revocar el certificado de Cl@ve Firma [Ayuda](#)
- ▶ Gestionar mi dispositivo activo con la aplicación móvil Cl@ve PIN [Ayuda](#)

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

El proceso de autenticación para el registro lo podremos llevar a cabo mediante tres procedimientos:

- Mediante carta al domicilio fiscal con un código de autenticación.
- Por videollamada.
- Con certificado digital o DNI-e

Los dos primeros requieren la identificación física del usuario. La tercera suplente la identificación física por la autenticación mediante medios digitales.

Al hacer click sobre el registro nos preguntará que procedimiento queremos utilizar.

GOBIERNO DE ESPAÑA MINISTERIO DE HACIENDA Y FUNCIONES PÚBLICAS Agencia Tributaria Sede Electrónica Todos los trámites on line

Registro en Cl@ve

DNI: 09768336Y

Puede registrarse en Cl@ve mediante una carta de invitación:

¿Quiere que le enviemos una carta de invitación a Cl@ve a su domicilio fiscal?

[También puede registrarse por VideoLlamada](#)

Regístrese en Cl@ve

cl@ve PIN

Usted no está registrado en Cl@ve.

Para poder activar el dispositivo debe estar registrado en Cl@ve.

¿Cómo desea registrarse en CL@ve?

MEDIANTE CARTA AL DOMICILIO FISCAL

POR VIDEOLLAMADA

CON CERTIFICADO O DNIE(WEB)

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Si utilizamos nuestro certificado digital o DNI-e haremos click sobre esta opción donde nos pedirá el dato de nuestro nº del DNI y la fecha de validez del DNI y que seleccionemos el certificado o DNI-e a utilizar.

Seguidamente nos pedirá un número de teléfono y un correo-e.

Alta en el sistema de identificación y firma cl@ve realizada correctamente.

DNI: ~~XXXXXXXXXX~~ Nombre y apellidos: ~~XXXXXXXXXX~~

Nº de Teléfono Móvil: ~~XXXXXXXXXX~~

Correo electrónico: ~~XXXXXXXXXX~~

Código Activación: ~~XXXXXXXXXX~~

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Una vez registrados tenemos que obtener un Cl@ve PIN para acceder a los trámites.

Por tu seguridad, el PIN que vas a recibir sólo puede ser utilizado una vez.

Puedes obtener tu PIN de dos formas, aunque te recomendamos utilizar la aplicación Cl@ve PIN para dispositivos móviles.

Una vez activada la app siguiendo los pasos indicados por ella podremos ver el PIN obtenido desde la web en la app.

Para obtener el PIN debemos seguir estos pasos.

1º paso introducir el DNI.



GOBIERNO
DE ESPAÑA



IDENTIDAD
ELECTRÓNICA PARA
LAS ADMINISTRACIONES



Autenticación

Introduzca su DNI o NIE

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

2º. Seleccionaremos la opción que deseemos:

Logo GOBIERNO DE ESPAÑA, cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES, cl@ve PIN, Agencia Tributaria.

Autenticación

Introduzca su DNI o NIE

Seleccione una opción

- Utilizar la App Cl@ve PIN para obtener el PIN (**recomendado**) ✓
- Usar el navegador para obtener el PIN y recibir un SMS
- No estoy registrado en Cl@ve

3º. Será necesario introducir un dato de contraste, Fecha de validez del DNI, fecha de expedición o número de soporte para NIE.

Logo GOBIERNO DE ESPAÑA, cl@ve IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES, cl@ve PIN, Agencia Tributaria.

Obtención de PIN

Rellene los siguientes datos para obtener el pin

DN/NIE

Fecha Introduzca la Fecha de Validez del DNI (dd-mm-aaaa) o la Fecha de Expedición (dd-mm-aaaa) si es un DNI permanente. Consulte la ayuda para localizar dicha fecha en su DNI.

Deseo personalizar la generación del PIN

¿Cómo obtener la fecha de validez de su DNI?
¿Cómo obtener la fecha de expedición de su DNI?

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

4º. Ya podemos obtener el PIN o personalizar la generación para indicar nosotros mismos el código de 4 caracteres necesario para autenticarnos.

Obtención de PIN

Rellene los siguientes datos para obtener el pin

DNI/NIE

Fecha 12-06-2029

Código personalizado ABCD - Puede modificar este código por 4 caracteres de su elección que deberá utilizar con el PIN que recibirá en su dispositivo móvil

[¿Cómo obtener la fecha de validez de su DNI?](#)

[¿Cómo obtener la fecha de expedición de su DNI?](#)

Obtención de PIN

Rellene los siguientes datos para obtener el pin

DNI/NIE

Fecha 12-06-2029

Deseo personalizar la generación del PIN

[¿Cómo obtener la fecha de validez de su DNI?](#)

[¿Cómo obtener la fecha de expedición de su DNI?](#)

5º La página nos indica que el PIN ha sido generado y nos pide nuestro DNI, Código y el PIN. En la app tendremos el PIN con indicación del tiempo de validez .

Lo introducimos y estaremos autenticados.

9:41 40% CEB

cl@ve
PIN

Tiempo de caducidad del PIN

08:58

PIN

RXB

COPIAR

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Podemos recibir el PIN mediante el envío de un sms.

Tendremos que facilitar el dato de contraste y a continuación podremos personalizar la generación de PIN o recibirlo directamente.

5º La página nos indica que el PIN ha sido generado y nos pide nuestro DNI, Código y el PIN. En nuestro dispositivo móvil tendremos un sms con el PIN. El tiempo de vida de este PIN es muy limitado. Lo introducimos y estaremos autenticados.

Autenticación

Introduzca su DNI o NIE

Seleccione una opción

- Utilizar la App Cl@ve PIN para obtener el PIN (recomendado)
- Usar el navegador para obtener el PIN y recibir un SMS ✓
- No estoy registrado en Cl@ve

En su dispositivo móvil utilice la APP Cl@ve PIN para solicitar un PIN.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – Cl@ve FIRMA

Cl@ve Permanente

¿Qué es?

¿Cómo funciona?

Procedimientos

Seguridad

Preguntas frecuentes (FAQs)

Procedimientos

Describimos a continuación los procedimientos relacionados con la activación, uso y gestión personal de Cl@ve Permanente

Activación de usuario

Mediante este servicio puedes activar tu usuario de Cl@ve Permanente y crear tu propia contraseña de acceso.

Para la activación de tu usuario de Cl@ve Permanente debes acceder al servicio de activación donde se te pedirá que introduzcas tu usuario (tu DNI o NIE), tu dirección de correo electrónico (como dato adicional de contraste) y el código de activación que te suministraron en el acto de registro.

[Accede al servicio](#)

Si son correctos, el sistema te enviará un SMS con un código numérico de un solo uso (One Time Password, OTP) que deberás teclear en el campo del formulario correspondiente. Si es correcto, el sistema te permitirá establecer la contraseña que prefieras, siempre que cumpla con unas características mínimas de seguridad. Esta contraseña será la que deberás utilizar de ahora en adelante cada vez que un servicio de administración electrónica te la solicite.

Si introduces erróneamente el código de activación más de 5 veces, el sistema te informará y acto seguido bloqueará el código de activación. En este caso será necesario generar un nuevo código de activación, para lo cual deberás realizar de nuevo el acto de registro en Cl@ve.

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – **Cl@ve PERMANENTE** – Cl@ve FIRMA

Gestión de la contraseña

Si has olvidado tu contraseña o simplemente deseas cambiarla, puedes volver a establecerla de nuevo en cualquier momento con uno de los siguientes procedimientos:

- Cambio de Contraseña

Por motivos de caducidad o seguridad, puedes desear cambiar la contraseña. Para ello accede al servicio de cambio de contraseña y sigue los pasos que allí se describen.

[Accede al servicio con usuario y contraseña](#) 

[Accede al servicio con certificado digital](#) 

- Olvido de Contraseña

En caso de olvido de la contraseña o de que ésta quede bloqueada por superarse el número máximo de 5 intentos fallidos, se podrá establecer una nueva contraseña siempre que hayas conservado el código de activación. Para ello deberás acceder al servicio de activación de contraseña y seguir los pasos allí indicados.

[Accede al servicio](#) 

- Pérdida del Código de activación

Si no has conservado el código de activación, puedes obtener un nuevo código de activación realizando de nuevo el acto de registro en Cl@ve.

- Regenerar el Código de Activación de Cl@ve permanente.

Si ya estás registrado en Cl@ve y lo necesitas, puedes regenerar el Código de Activación de Cl@ve permanente

[Accede al servicio](#)

20, 21 y 22
septiembre
2021



Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – **Cl@ve FIRMA**

Una vez tenemos nuestra Cl@ve permanente podemos crear nuestra Cl@ve FIRMA.

Nuestra cl@ve firma se creará en el momento de la primera firma.

En este proceso se nos redirigirá a la página de la policía nacional que son quienes se encargan de la gestión y custodia de éstos certificados.

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR DIRECCIÓN GENERAL DE LA POLICÍA POLICÍA NACIONAL cl@ve firma

Emisión de tu certificado de firma centralizado

¡Información!
A continuación debes indicar tu contraseña Cl@ve para comenzar con el proceso de emisión de tu certificado de firma centralizado.
Para más información sobre el certificado de firma centralizada y sus condiciones de uso, pulsa el siguiente enlace [DPC](#)

Contraseña:

[Emitir](#) [Cancelar](#)

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR DIRECCIÓN GENERAL DE LA POLICÍA POLICÍA NACIONAL cl@ve firma

Emisión de tu certificado de firma centralizado

¡Información!
Ya estamos terminando. En unos instantes recibirás un código en tu teléfono móvil. Escríbelo a continuación exactamente igual que lo has recibido y el proceso se completará automáticamente.
Vamos a emitir el certificado para que puedas firmar. Puedes consultar la declaración de políticas de certificación (DPC) en http://www.dnielectronica.es/PCFs/politicas_de_certificacion.pdf
Si estás de acuerdo pulsa "Aceptar"

Aceptar

Código recibidor:

Solicitud del certificado centralizado

Vas a generar tu certificado de firma centralizado. Este certificado podrás utilizarlo igual que el actual certificado digital, pero sin necesidad de tenerlo instalado en el dispositivo con el que estás accediendo a internet. Para más información, puedes consultar en la web de Cl@ve.gob.es

[Solicitar Certificado](#) [Cancelar](#)

Cl@ve.

Identidad electrónica para las Administraciones

Cl@ve PIN – Cl@ve PERMANENTE – **Cl@ve FIRMA**

Una vez creada nuestra Cl@ve FIRMA se terminará el proceso solicitándonos nuestros datos de acceso y el código de firma enviado a nuestro móvil.

Firma

Para solicitar este trámite, es necesario que lo firmes mediante tu certificado de firma centralizado. De esta forma, tendrá la misma validez legal que si lo presentas presencialmente o utilizando certificado digital.

Para firmar, a continuación introduce tu contraseña y el código que te hemos enviado a tu móvil.

USUARIO FIRMANTE
06308687V

CONTRASEÑA

CÓDIGO RECIBIDO
111111 x

Continuar **Cancelar**

MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL

SECRETARÍA DE ESTADO DE LA SEGURIDAD SOCIAL

TU SEGURIDAD SOCIAL

COMPROBANTE DE REGISTRO ELECTRÓNICO

DATOS DE REGISTRO 1 / 1

Solicitud de ALTA DE BENEFICIARIO DE ASISTENCIA SANITARIA
Nº registro: 2015000000000014267
Fecha y hora del registro: 11/12/2015 08:18:46:00

Esta solicitud ha sido aprobada de forma automática.

SOLICITANTE:

Nombre y Apellidos: USUARIO1 USUARIO1 USUARIO1
DNI: 06308687V

BENEFICIARIO:

Nombre y Apellidos: CTRESPO STAR WARS
Fecha Nacimiento: 11/12/2015
Sexo: VARON
País de nacionalidad: ESPAÑA

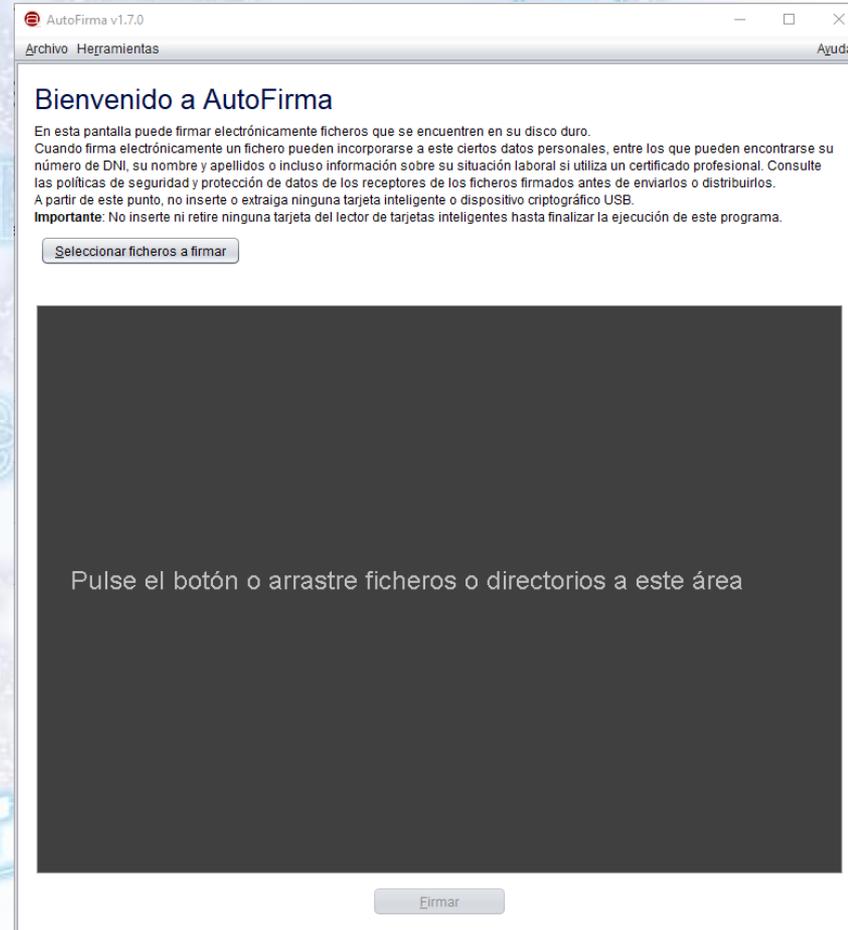
DECLARO, bajo mi responsabilidad, que son ciertos los datos que consigno en la presente solicitud.

Los datos aportados con esta solicitud podrán ser comprobados por el Instituto Nacional de la Seguridad Social para verificar que se cumplen los requisitos para reconocer el alta del beneficiario, de acuerdo con el artículo 3 bis de la Ley 16/2003 de 28 de mayo, de cohesión y calidad del Sistema Nacional de Salud y el artículo 94 ter de la ley 29/2006, de 26 de julio, de garantías y uso racional de los medicamentos y productos sanitarios.

Autofirma

Aplicación de firma digital de documentos.

Al iniciar el programa nos pedirá que le indiquemos con que vamos a firmar con un DNI-e o con certificado. Le indicaremos lo que corresponda.



Nos aparecerá un ventana en la que colocaremos lo documentos a firmar arrastrándolos al recuadro gris o mediante el botón de selección de archivos a firmar.

Autofirma

Aplicación de firma digital de documentos.

Una vez colocado el documento nos preguntará si queremos hacer visible la firma y si queremos insertar una marca visible dentro del documento.

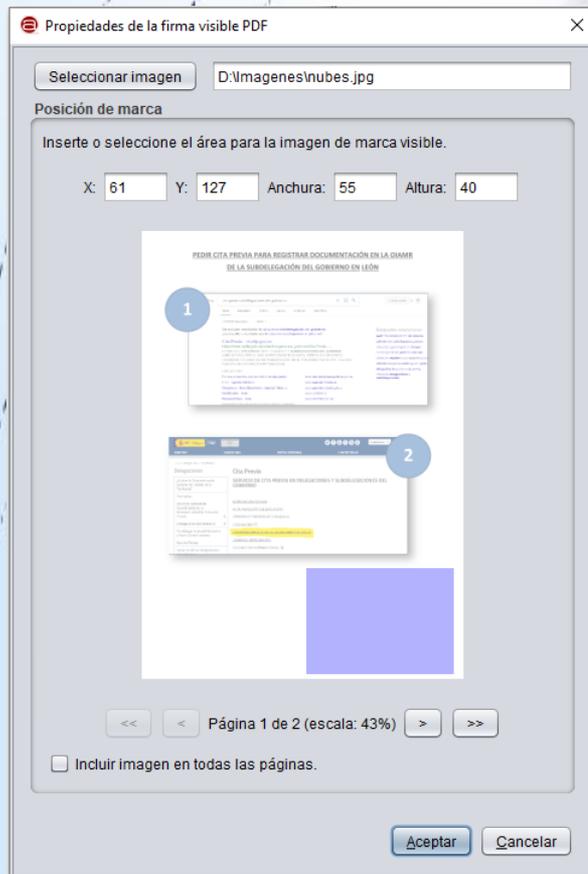


Si decidimos hacer visible la firma nos preguntará dónde la queremos colocar y nos dará la opción de redactar el texto de firma e incluso insertar una imagen de nuestra firma.

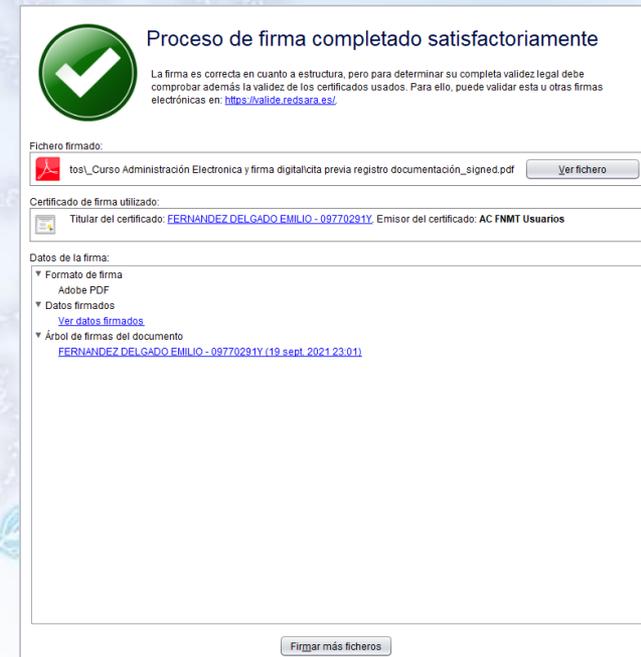
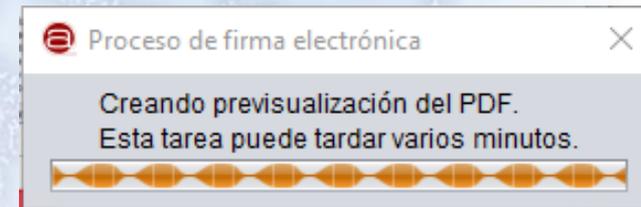
Autofirma

Aplicación de firma digital de documentos.

Si además le hemos indicado que queremos insertar una marca visible nos pedirá una imagen para insertar.



Ahora procedemos a acto de la firma y nos pedirá seleccionar el certificado con el que firmar y procederá a la firma.



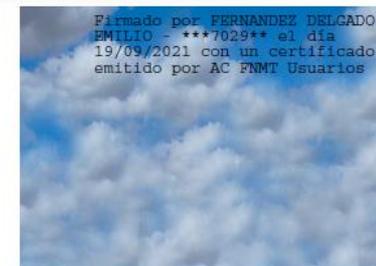
Autofirma

Aplicación de firma digital de documentos.

Este es el resultado final del proceso de firma de un documento con autofirma.

La firma digital de un documento únicamente tiene validez en un mundo digital. La impresión de un documento firmado digitalmente no tiene valor ninguno ya que una firma digital es una huella digital que no es posible reproducción de forma material.

PEDIR CITA PREVIA PARA REGISTRAR DOCUMENTACIÓN EN LA OIAMR DE LA SUBDELEGACIÓN DEL GOBIERNO EN LEÓN



gob.es VALIDE

Aplicación de VALIdación de firma y certificados Online y Demostrador de servicios de @firma.



Determina la validez de firmas y certificados digitales.

VALIDE tiene un acceso libre para todos los usuarios. Podrá validar un certificado, una firma y una sede electrónica además de realizar una firma digital en formatos básicos.

Si desea elegir el tipo de formato al realizar una firma necesitará descargar e instalar en su ordenador la aplicación de firma.

gob.es VALIDE

Aplicación de VALIdación de firma y certificados Online y
Demostrador de servicios de @firma.



Contactar
Bienvenido | Benvingut | Ongi etorri | Benvido | Welcome



Validar Certificado

Si dispones de un certificado digital emitido por cualquier entidad de servicio de certificación reconocida, puedes comprobar en línea su validez.

[Validar Certificado](#)

Preguntas Frecuentes

Consulta nuestras preguntas frecuentes si tienes alguna duda.

¿Qué significa VALIDE?

¿Qué servicios ofrece VALIDE?

¿Qué certificados son reconocidos por la plataforma?

¿Cuáles son los tipos de certificados admitidos por las Administraciones?

¿Cuáles son los formatos admitidos para firma electrónica?

¿Qué debo hacer para usar los servicios de VALIDE?

¿Qué tipos de documentos se pueden firmar con VALIDE?

¿Pueden firmar un documento varias personas?

[Ver más](#)

Realizar Firma

Firma un documento con tu DNI electrónico o cualquier otro certificado reconocido con las máximas garantías de integridad y autenticidad.

[Realizar firma](#)

Validar Firma

Consulta la validez de un documento firmado electrónicamente con múltiples formatos y tipos de certificados, como facturas electrónicas, contratos, etc.

[Validar Firma](#)

Visualizar Firma

Podrás generar informes en los que se mostrará información de la firma o firmas asociadas al documento.

[Visualizar Firma](#)

Validar Sede Electrónica

Podrás comprobar las URLs de sede electrónicas, verificando la validez del certificado que contienen.

[Validar Sede Electrónica](#)

Portal de
Firma electrónica