Me @dministro 2.0

La e-Administración para la inserción laboral

GUÍA

IDENTIDAD DIGITAL

Federación Nacional aspaym

Fundación Vodafone España

Guía: La e-Administración para la inserción laboral
Identidad Digital

2018

www.aspaym.org

ÍNDICE

PRÓLOGO FUNDACIÓN VODAFONE ESPAÑA

Vivimos en un mundo digital. El desarrollo de nuestra sociedad no se entiende sin la irrupción de las nuevas tecnologías, un factor clave que sin duda definirá nuestra competitividad y desarrollo futuro.

Oímos hablar del Internet de las Cosas, la inteligencia artificial, el Big Data o las tecnologías en la nube y a veces no nos damos cuenta de que todas estas nuevas tendencias tecnológicas tienen ya un evidente reflejo en nuestra vida diaria. Sus aplicaciones son innumerables, desde la gestión más eficiente de los recursos públicos, hasta la educación de nuestros hijos, la monitorización de los servicios de salud, limpieza o tráfico e incluso la formación de los mayores y el control de los objetos personales.

Siempre hemos estado convencidos de que la adopción de estas nuevas prácticas y procesos digitales debe ser, ante todo, un vehículo para mejorar la calidad de vida de las personas, prestando especial atención a todas aquellas con necesidades especiales. Y es que la inclusión social puede y debe ser potenciada con la innovación tecnológica. Tenemos que entender la tecnología como una herramienta de impulso para lograr una sociedad que realmente ofrezca igualdad de oportunidades, tanto laborales como de disfrute personal.

Empresas, instituciones y administraciones públicas tenemos la responsabilidad de proporcionar respuesta a las necesidades del 10% de la población que tiene alguna discapacidad. Es verdad que todavía queda mucho camino por recorrer, de hecho, según el Observatorio de Administración Electrónica (OBSAE) tan solo el 52 % de ciudadanos realizaron un uso directo de los servicios telemáticos en 2017, pero somos optimistas y creemos firmemente que se están dando los pasos adecuados. Así, según el Observatorio Vodafone de la Empresa 2018, la digitalización sigue siendo el elemento que más preocupa a las Administraciones Públicas y el 79% de considera que la relación con el ciudadano ha mejorado gracias a la implementación de las nuevas tecnologías.

De ahí que esta guía “La e-Administración para la inserción laboral” elaborada conjuntamente con la Federación Nacional ASPAYM, pretenda servir como herramienta de orientación sobre los distintos servicios electrónicos y productos de apoyo disponibles para aquellos que necesitan adaptarse a las nuevas dinámicas laborales y personales que implica una era digital en constante cambio.

Tras los buenos resultados obtenidos con el proyecto “Me @administro” desarrollado en los dos últimos años, el plan de capacitación y formación “Me @dministro 2.0” nace para dinamizar el uso de los servicios telemáticos o electrónicos, promover la inserción laboral, capacitar a personas con discapacidad en el uso de los productos de apoyos tecnológicos y promover la participación.

Además, el proyecto incorpora como gran novedad la implantación de un concurso de videotutoriales de productos de apoyo tecnológicos de bajo coste para promover el conocimiento mutuo e impulsar el trabajo en red y la creación y distribución de nuevos productos de apoyo de bajo coste.

En definitiva, se trata de seguir trabajando para concienciar a empresas y administraciones públicas sobre la necesidad de corregir la brecha digital, facilitando el acceso a programas formativos que les orienten no solo en la aplicación de las nuevas tecnologías a sus procesos de trabajo sino también en sus posibilidades para fomentar la inserción socio-laboral de los colectivos menos favorecidos.

Remedios Orrantia

Patrona Ejecutiva

Fundación Vodafone España

PRÓLOGO FEDERACIÓN NACIONAL ASPAYM

Cada año que sumamos en el siglo XXI, es un paso hacia delante en la Sociedad de la Información. Vivimos en un mundo totalmente tecnológico y en el que las denominadas "Nuevas Tecnologías", ya han pasado a formar parte de nuestra vida diaria.

Esta sociedad, en la que el progreso está unido a los avances en este ámbito, supone una oportunidad para todas las personas para ser más independientes y autónomas en muchas de las acciones cotidianas.

Para que el acceso universal a la información sea una realidad, es necesario capacitar a todas las personas, y las nuevas tecnologías son un gran aliado para conseguir derribar barreras que ayuden a lograr la plena accesibilidad.

Por ello, la e-accesibilidad supone una herramienta fundamental para el beneficio de todas las personas, igualando así las oportunidades a la hora de acceder a los servicios de la sociedad actual.

En la actualidad, se pueden tramitar servicios de forma telemática cuyo conocimiento ahorraría tiempo y desplazamiento a las personas. Este hecho adquiere relevancia entre las personas con movilidad reducida, que necesitan realizar muchos trámites para obtener certificados o ayudas, con la dificultad de movilidad y en ocasiones de imposibilidad que supone.

La Federación Nacional ASPAYM, como entidad representativa estatal de la lesión medular, tiene la responsabilidad de promover la inserción laboral y capacitar a las personas con discapacidad en el uso de las nuevas tecnologías,

Tras los buenos resultados obtenidos con "Me @dministro", y siendo conscientes de la importancia, la accesibilidad y la igualdad de oportunidades que suponen las posibilidades que otorga la e-Administración, colaboramos con la Fundación Vodafone España para lanzar "Me @dministro 2.0".

En esta edición, queremos promover la inserción laboral y capacitar a más personas con discapacidad, personas mayores y otros colectivos de interés, para que la brecha digital y el desconocimiento hacia las nuevas tecnologías y las posibilidades de la e-Administración cada vez sean menores.

Fotografía realizada por Juan Carlos Monroy

José Ramón del Pino

Presidente

Federación Nacional ASPAYM

¡HOLA! SOMOS "ME@DMINISTRO 2.0"

La e-Accesibilidad es algo que nos beneficia a todas y todos por igual.

Con relación a la brecha digital y al desconocimiento de las posibilidades de las Nuevas Tecnologías, es preciso realizar un esfuerzo de información y formación, trasladando una visión positiva de lo que pueden ofrecer las Nuevas Tecnologías a toda la población, y especialmente, a las personas con discapacidad.

Una adecuada formación en el uso de las tecnologías de la información incrementa la percepción de sus beneficios entre los que se encuentra la reducción de los costes.

En cuanto al nivel formativo, éste es clave para la inserción laboral, a medida que se incrementa mejoran las posibilidades de empleo y las condiciones de contratación. Este es un hecho que afecta a toda la población, sin embargo, para el caso de las personas con discapacidad es aún mayor. Sin duda una mejor formación estrecha las diferencias con la población general.

Asimismo, es necesario emprender acciones que minimicen la brecha digital y maximicen la e-accesibilidad de las personas a los servicios telemáticos mejorando su calidad de vida y la del resto de la población.

“Me @dministro 2.0”: La e-Administración para la inserción laboral

“Me @dministro 2.0” es un proyecto de capacitación y formación para dinamizar el uso de los servicios telemáticos o electrónicos, promover la inserción laboral, capacitar a personas con discapacidad en el uso de los productos de apoyos tecnológicos y promover la participación ciudadana a través de los servicios digitales que la propia Administración pone a disposición de la población.

Con la llegada del DNI electrónico, las posibilidades de realizar trámites y gestiones crecen enormemente: las webs de las administraciones ofrecen numerosos servicios on-line, no sólo información.

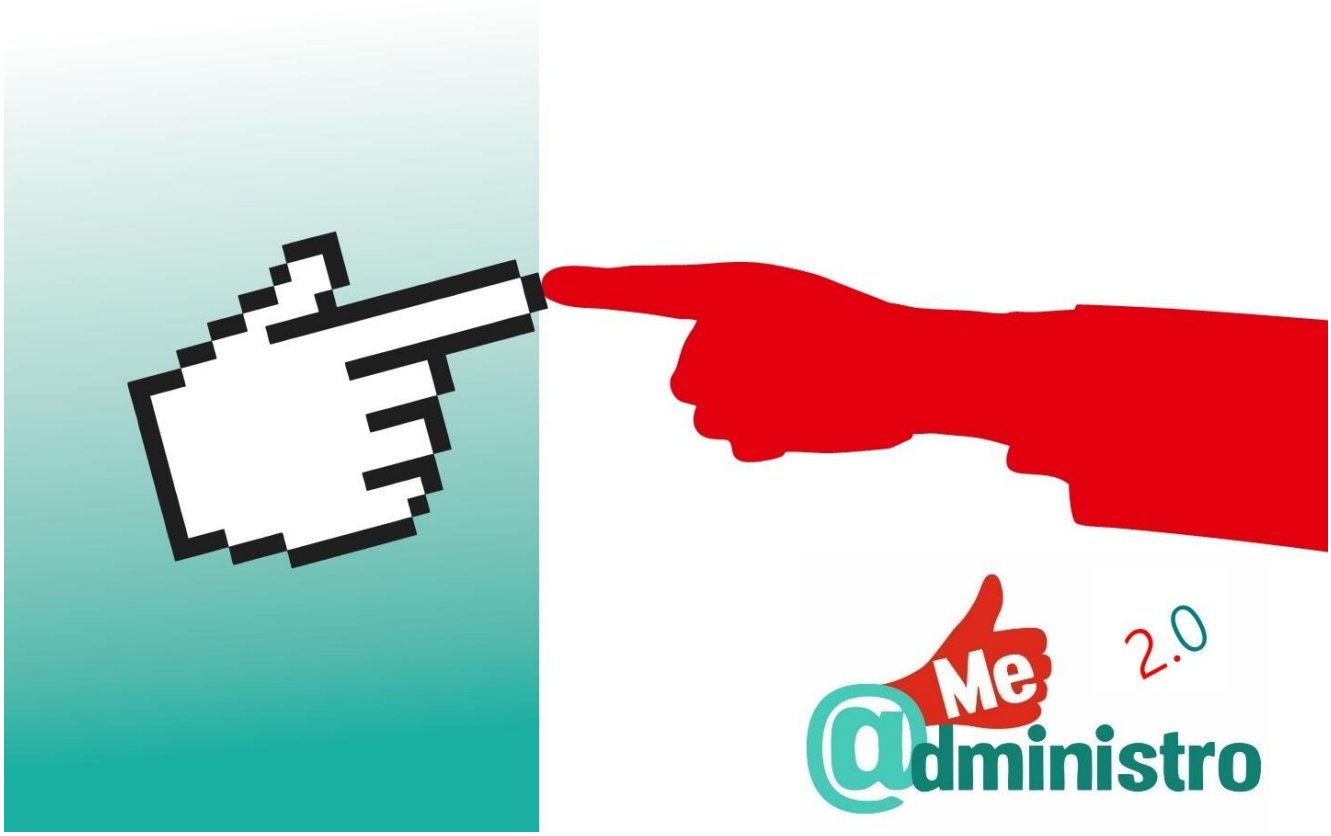
Concretamente, en cuanto a los servicios electrónicos de las Administraciones Públicas, se trata de herramientas fuertemente arraigadas a nuestra realidad cotidiana, en algunos casos de forma prácticamente excluyente: si una persona no puede realizar un determinado trámite de forma electrónica puede perder su autonomía en este ámbito, necesitando a otras personas que lo hagan en su lugar.

Por otra parte, teniendo en cuenta el cumplimiento de la Ley 39/2015, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas en la que se indica la obligatoriedad de tener un certificado digital de personalidad jurídica(empresas, asociaciones….) y de estar dados de alta en el servicio de notificaciones electrónicas, en la nueva edición de las guías que darán soporte a la formación on-line y presencial, se incluirán los contenidos tanto para su obtención, instalación, uso , renovación y revocación.

En este sentido, una adecuada formación en el uso de los productos de apoyo tecnológicos tanto del mercado como de creación propia, permiten desarrollar las actividades en igualdad de condiciones, con eficiencia y maximizando las capacidades de las personas con discapacidad.

“Me @dministro 2.0” es un proyecto realizado por la Federación Nacional ASPAYM en colaboración con Fundación Vodafone España, aprovechando su experiencia en servicios telemáticos accesibles, para la promoción de la autonomía personal y la disminución de la brecha digital a través del apoyo y la formación en Nuevas Tecnologías, tras los buenos resultados obtenidos con el proyecto “Me @dministro” desarrollado en el año 2016-2017.

Maximizar la e-accesibilidad de las personas con discapacidad.



LA IDENTIDAD DIGITAL: EL 'YO' ELECTRÓNICO

A lo largo de la historia la humanidad las personas se han enfrentado a múltiples dilemas para establecer relaciones de confianza entre ellas, ya sea para comerciar, para la guerra, para hacer valer la palabra empeñada o proteger secretos de ojos curiosos.

- ¿Cómo se puede saber que la identidad de una persona es quien dice ser y no está mintiendo?
- ¿Cómo hacer valer la autenticidad de un contrato y obligar a que se cumpla lo que dice?
- ¿Cómo evitar que un mensaje estratégico sea leído por el enemigo?
- ¿Cómo se puede comprobar que un testamento no fue modificado?

Para dar solución a estas interrogantes se han desarrollado infinidad de técnicas:

- Documentos de identidad, pasaportes, tarjetas de identificación, partidas de nacimiento, etc. para garantizar que la identidad que dice tener una persona es de verdad así y no está engañando.
- El correo certificado, las comunicaciones cifradas por criptografía, etc. para asegurar la privacidad de los mensajes y que estos no han sido alterados por nadie ajeno a la comunicación.
- La firma manuscrita, los documentos notariados, el uso de testigos, etc. para evitar que alguna de las partes que llegan a un acuerdo luego lo nieguen o no quieran cumplirlo.

Y así ha sido y sigue siendo hasta ahora.

Hasta ahora los sistemas de identificación se han basado en la identificación física de las personas, al contrastar la identidad de esta con el documento de identidad que le acredita (DNI, NIE, pasaporte). Pero con la llegada de la era de las comunicaciones y los sistemas telemáticos llega el reto de proveer de garantías de identificación a un mundo virtual en el que no existe contacto directo entre las partes implicadas en una comunicación.

Por tanto, se hizo necesario crear documentos digitales de identidad que solucionaran la gran pregunta: ¿Cómo saber con quién se está tratando al otro lado de la pantalla?

LA IDENTIDAD EN UN MUNDO ELECTRÓNICO

La forma como se resolvió el dilema de poder relacionar y garantizar la identidad real de una persona o una entidad con su identidad electrónica, fue con la utilización de mecanismos criptográficos que ofrecen las mismas funcionalidades y garantías que los documentos de identificación físicos.

Para estos mecanismos criptográficos son fundamentalmente los **certificados digitales o electrónicos** y la **firma electrónica**, que juntos constituirán esa identidad digital.

Por lo tanto, por identidad digital podemos entender a todos los "procesos, mecanismos y tecnologías" que permiten a una persona o una organización poder identificarse de forma fiable en los medios electrónicos o digitales, y conocer la identidad real de las otras personas u organizaciones con las que se interactúa.

Esta identidad digital estará certificada por una **tercera parte de confianza** que verifique de forma segura que una identidad digital pertenece a una persona u organización en particular.

La identidad digital no es solo para las personas físicas, también es necesaria y se usa en las empresas y organizaciones para interactuar entre ellas, con los ciudadanos y las administraciones públicas. Lo mismo ocurre con multitud de sistemas, componentes y servicios electrónicos que requieren tener la confianza de saber con quién se está interactuando.

Para comprender mejor estos procesos y antes de ver las aplicaciones prácticas de esta identidad digital hay que conocer un poco las partes que lo hacen posible y que a continuación describimos.

¿QUÉ ES LA CRIPTOGRAFÍA?

Criptografía (del griego kryptós, “oculto” y graphos, “escribir”, “palabra oculta”) significa, según el Diccionario de la Real Academia Española: “Arte de escribir con clave secreta o de un modo enigmático”.

O en términos algo más actuales: la criptografía es el estudio de los principios y mecanismos necesarios para establecer procesos de cifrado y descifrado de datos o mensajes y la generación de las claves necesarias para poder hacerlo.

La criptografía **Cifra** o **Codifica** la comunicación entre dos entes, utilizando **códigos** o **algoritmos matemáticos** para **proteger** su contenido y evitar que pueda ser visto por terceros.

Por tanto, una comunicación está cifrada cuando solo pueden extraer la información del mensaje el emisor y el receptor del mismo, y que para cualquier otra persona ajena a esta comunicación el contenido del mensaje carecerá de todo sentido y no será capaz de comprenderlo.

El cifrado de mensajes para proteger información se ha practicado desde hace milenios, en tiempos modernos la criptografía permite la transmisión o el almacenamiento de información sensible a través de redes inseguras, como por ejemplo Internet, de forma privada y segura.

Los objetivos básicos de la criptografía son:

1. **Garantizar el secreto entre dos entidades (personas o cosas).**
2. **Asegurar que la información es auténtica en los dos sentidos.**
3. **Impedir que el contenido del mensaje enviado sea modificado durante el tránsito o viaje de este.**

Unos ejemplos históricos y sencillos de criptografía los encontramos en la **"escítala"** de los espartanos y el **"cifrado César"** de los romanos.

[1]**La técnica de la escítala:** consiste en el envío de mensajes secretos escritos sobre tiras o cintas estrechas de pergamino o cuero. El **emisor** enrolla una tira sobre una estaca para escribir el mensaje a todo lo largo de esta, de forma que en cada vuelta de la tira quede solamente una letra de la palabra, una vez escrito el mensaje se desenrollaba y se enviaba al **receptor**. El receptor debe enrollar la tira sobre una estaca del mismo diámetro que la usada para escribir el mensaje y así poder ordenar las letras de forma correcta y poder leer el mensaje.

Esta técnica criptográfica es un ejemplo de **"cifrado por transposición"**.

El cifrado César: esta técnica de cifrado debe su nombre al emperador romano Julio César que la utilizó en sus comunicaciones y es un método de cifrado simple, pero efectivo, que consiste en desplazar las letras del alfabeto un número determinado de posiciones. Por ejemplo, si se decidía que un mensaje tenía una **clave criptográfica** basada en seis, cada letra se desplazaba seis posiciones, por lo cual la "A" equivaldría a la "G", la "B" a la "H", la "C" a la "I" y así sucesivamente.

Esta técnica criptográfica es un ejemplo de **"cifrado por sustitución"**.

Ejemplo de cifrado César														
Sin cifrar	A	B	C	D	E	F	G	H	I	J	K	L	M	N
Con cifrado	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S
Sin cifrar	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	
Con cifrado	T	U	V	W	X	Y	Z	A	B	C	D	E	F	

Ambas técnicas de cifrado introducen en los conceptos de **"clave criptográfica"** o **"algoritmo de cifrado"** y de **"clave simétrica"**. Donde la clave criptográfica para codificar los mensajes era el diámetro de la estaca o el número de letras que se desplaza el abecedario. Y es simétrica porque ambas partes utilizan la misma clave para cifrar y descifrar el mensaje.

Los sistemas criptográficos que se utilizan en la actualidad en las telecomunicaciones, Internet y demás redes de comunicación, son muchísimo más complejos que los métodos utilizados por los espartanos o Julio César, aunque la base es la misma: **una clave cifra el mensaje**.

Veamos con más detalle estas claves simétricas y su evolución.

La criptografía de clave simétrica

Como se vio con los métodos de cifrado con la "escítala" y el "cifrado César", una persona o ente (el emisor) toma un mensaje legible y le aplica una clave o algoritmo de cifrado, este proceso genera como resultado un mensaje ilegible (mensaje cifrado) que enviará a otra

[1] CC BY-SA 3.0, https://commons.wikimedia.org/w/index.php?curid=1698345

persona o ente que ya conoce de antemano la clave de cifrado utilizada para que así pueda descifrar el contenido y el mensaje sea legible.

Este proceso es conocido como **criptografía de clave simétrica**, ya que se utiliza una sola clave o algoritmo, conocida tanto por el emisor como por el receptor, para cifrar y descifrar la comunicación.

Veamos con un ejemplo ficticio cómo se puede utilizar una clave simétrica:

- Julieta quiere escribirle mensajes a Romeo sin que su familia ni la de él, ni nadie más, puedan leerlo.
- Para lograrlo Julieta crea un sistema de encriptado que hace que sus cartas al codificarlas sean una mezcla de letras, números y símbolos.
- Julieta le pasa a Romeo en secreto la clave de cifrado de su sistema de encriptado.
- Romeo y Julieta empiezan a dejarse mensajes por toda Verona que, cuando sus familiares y la gente los encuentra, ven que son una locura sin sentido.
- Sus mensajes estarán a salvo siempre que la clave permanezca en secreto.

La criptografía por clave simétrica **es muy rápida**, por lo que es ideal para cifrar grandes cantidades de datos.

El gran problema que presenta es que hay que dar a conocer y distribuir la clave entre todos los participantes en la comunicación y si se logra descubrir esa clave se podrán descifrar todas las comunicaciones secretas inmediatamente.

Para hacer el sistema de encriptación más robusto se desarrollan métodos que no dependan de una clave de cifrado única.

La criptografía de clave asimétrica

Con la criptografía de clave asimétrica los participantes de la comunicación poseen **una pareja de claves** o algoritmos de cifrado complementarios:

- La **“clave privada”**: esta clave solo será conocida por su propietario en secreto absoluto.
- La **“clave pública”**: esta clave puede ser conocida y tenerla cualquier otra persona o ente.

Que la clave privada y la pública sean complementarias significa que **lo que cifra una de ellas solo puede ser descifrada por la otra** y viceversa.

Veamos el proceso de utilización de criptografía de clave asimétrica con un ejemplo ficticio:

- Para Romeo y Julieta el sistema de clave simétrica les resulta muy arriesgado, así que optan por uno más seguro y se pasan a uno de clave asimétrica.
- Tanto Romeo como Julieta consiguen una pareja de claves (la pública y la privada) para cada uno.
- Mantienen en secreto sus respectivas claves privadas, ni siquiera se las dicen entre ellos.

- En cambio, dejan que sus respectivas claves públicas sean conocidas por todo Verona, sobre todo por sus familias.
- Romeo y Julieta empiezan a dejarse mensajes cifrados por toda Verona.
- Ella encripta sus mensajes con la clave pública de Romeo, él hace lo mismo con la clave pública de Julieta.
- Ambos, cuando ya están lejos de miradas curiosas, descifran los mensajes que se han dejado el uno a la otra con sus propias claves privadas.

Este método criptográfico ofrece mayor seguridad ya que evita la vulnerabilidad de utilizar una única clave criptográfica que tiene que ser conocida entre los participantes de una comunicación ya que no necesita distribuir una clave secreta.

Para aumentar aún más la seguridad del par de claves necesarios en la criptografía de clave asimétrica, éstas se obtienen mediante **métodos matemáticos complejos**, realizando cálculos con números primos de gran tamaño que dan como resultados números enormes, que hacen imposible conocer una clave a partir de otra debido a que la capacidad de cómputo de los ordenadores en la actualidad no es suficiente como para poder realizar esa tarea.

El inconveniente de la criptografía de clave asimétrica es que **es un proceso lento**, lentitud que aumenta de forma proporcional a la cantidad de datos a cifrar.

Para solventar este problema se hace el cifrado retomando los métodos de criptografía de clave simétrica junto con la clave pública.

A continuación, veremos en detalle esta combinación de procesos

El cifrado de clave pública

La utilización de claves asimétricas tiene el inconveniente de que el proceso de cifrado es lento, y la forma como se logró solventar inconveniente fue realizando un cifrado de la misma clave pública. Con este procedimiento primero se cifra el mensaje con una clave simétrica que se genera de forma aleatoria, llamada **clave de sesión**, para posteriormente realizar el cifrado con la clave pública del mensaje ya encriptado.

Veamos con un ejemplo ficticio cómo se hace el cifrado de clave pública:

- Romeo y Julieta ya tienen su pareja de claves respectivas, la pública y la privada para encriptar sus mensajes, pero el proceso es lento.
- Para agilizarlo primero cifrarán sus mensajes con criptografía simétrica utilizando una clave de sesión. Es como vimos que hacían en un principio, pero con la gran diferencia de que esta clave de sesión se crea de forma totalmente aleatoria cada vez que cifren un mensaje.
- Ahora con los mensajes encriptados por la clave de sesión los cifrarán de nuevo con sus claves públicas.
- Cuando le llegue a cada uno el mensaje del otro harán el proceso inverso.
- Descifrarán sus claves públicas propias con las privadas que mantienen en secreto.

- Al descifrar la primera fase obtendrán la clave de sesión que encriptó el mensaje con una clave simétrica.
- Finalmente, con la clave de sesión descifrarán el mensaje que han recibido del otro.

Agregando el algoritmo de clave simétrica de la clave sesión al cifrado de la clave pública, se consigue sumar la **confidencialidad** del cifrado que garantiza que solo los participantes legítimos de la comunicación vean el mensaje. Y la **integridad** del mensaje, al garantizar que no podrá ser modificado durante la comunicación.

Pero para conseguir unas comunicaciones telemáticas efectivas y confiables es necesario contar con sistemas que garanticen la **autentificación** y la **garantía de no repudio**, así que para solventar esta carencia fue necesario buscar nuevas soluciones basadas en la criptografía de clave pública…

La firma digital

Con la firma digital se consigue que el receptor de un mensaje firmado digitalmente pueda **autentificar** el emisor del mensaje, verificar la **integridad** de los datos del mensaje, y que estos no han sido modificados desde que se envió, así como obtener del emisor una garantía de **"no repudio"** o de **"no repudio en origen"** que le impida desconocer o rechazar que ha enviado el mensaje o su contenido.

Características de la firma digital

1. **Autentifica al emisor del Mensaje.**
2. **Verifica la integridad de los datos del Mensaje.**
3. **Obtener una Garantía de "No repudio".**

La criptografía de **clave asimétrica con su clave pública** permite desarrollar firmas digitales basándose en la función de que un mensaje cifrado con una clave pública solo puede ser descifrado por su par, la clave privada, pero aplicándola de forma inversa, ya que: **una firma digital es cifrar un mensaje utilizando una clave privada**.

Esta firma digital tiene la misma validez que una firma manuscrita y es imposible de falsificar, siempre y cuando la clave privada del firmante se mantenga en secreto.

Veamos cómo sería la utilización de la firma digital con un ejemplo ficticio:

- Julieta le pide a Romeo que le envíe unos documentos importantes firmados digitalmente, para que así ella pueda verificar que son suyos de una forma indudable, que nadie los ha manipulado para el momento en que ella los reciba y que Romeo acepta lo dicho en esos documentos.
- Romeo obtiene una firma digital y le envía a Julieta el documento original junto a la firma creada.
- Ahora Julieta debe comprobar la validez de la firma digital para verificar la integridad del documento y autentificar que Romeo es el autor.

- Julieta descifra el documento que le ha enviado Romeo utilizando la clave pública de Romeo.

Con la firma digital se consigue la autentificación entre emisor y receptor, equivalente a una firma manuscrita, pero aún más segura. Sumando la firma digital ya se cuentan con todos los elementos necesarios para establecer relaciones de confianza a través de redes telemáticas y conseguir varios de los aspectos fundamentales de la seguridad informática:

- **Autenticación:** poder verificar que un documento ha sido elaborado o pertenece a quien lo envía.
- **Integridad:** asegurar que el mensaje no ha sido modificado durante su tránsito por algún agente ajeno a la comunicación.
- **No repudio:** evitar que la persona que envíe el mensaje niegue haberlo hecho.

Un cuarto pilar que asegura que la comunicación solo es visible para el emisor y el receptor, es la **confidencialidad**. Ésta se consigue a través de la utilización de canales seguros.

LAS CLAVES PÚBLICA Y PRIVADA EN UN CERTIFICADO DIGITAL

En la práctica, la forma en la que se utilizan y distribuyen los códigos o algoritmos matemáticos de las claves pública y privada y la firma digital que utiliza la criptografía asimétrica es a través de un **certificado digital o electrónico**.

> El certificado digital es un documento electrónico en donde una **tercera parte de confianza** asocia una clave pública con la identidad de su propietario.

Estos certificados electrónicos pueden estar contenidos en un dispositivo físico, que es el caso del **"Documento Nacional de Identidad Electrónico"**, o en un software como es el caso del **"Certificado de la Fábrica Nacional de Moneda y Timbre".**

TERCERAS PARTES DE CONFIANZA

El dilema que presentan los certificados digitales o electrónicos cuya clave pública va asociada a una persona determinada es cómo se puede saber si el certificado es auténtico, está vigente y si la persona que dice ser su propietario es realmente quien dice ser.

La única manera de garantizar la validez de un certificado en un entorno de clave pública es recurriendo a una **Tercera Parte de Confianza** (**TPC**), en inglés **Trusted Third Party** (**TTP**), que **certifique y vincule la identidad de la persona propietaria con el certificado digital**. Estableciendo así las bases para una relación de confianza entre las partes involucradas en una comunicación o trámite telemático que les permita intercambiar información cifrada o firmada.

Estas TPC serán además quienes se encarguen de generar, distribuir y gestionar las claves públicas, en forma de certificados digitales, entre los usuarios que confían en esa tercera parte.

Los certificados digitales expedidos por una TPC tendrán la firma digital sobre esta, avalando así la fiabilidad de un certificado firmado por una tercera parte de confianza.

Una TPC, que se encarga de la firma digital de certificados digitales para usuarios de un entorno de clave púbica, se conoce con el nombre de **Autoridad de Certificación** (**AC**).

Infraestructura de clave pública

Al conjunto de servicios, protocolos y estándares que permiten utilizar aplicaciones de criptografía de clave pública gestionados por terceras partes confiables se denominan **Infraestructuras de Clave Pública** (**ICPs**), o en inglés **Public Key Infrastructures** (**PKIs**). Esta infraestructura permite la emisión de los certificados digitales, su gestión, su fiabilidad y su seguridad.

Estas infraestructuras de clave pública están compuestas por terceras partes distintas, que gozan todas de la misma confianza por parte de los usuarios. Estas pueden ser una **Autoridad de Certificación**, una **Autoridad de Registro** y otras, como puede ser una **Autoridad de Fechado Digital.**

Para garantizar la validez de un certificado en un entorno de clave pública se recurre a una **Tercera Parte de Confianza** (**TPC**), que **certifique y vincule la identidad de la persona propietaria con el certificado digital**.

Los sistemas de identificación digital

Con los conocimientos básicos sobre los procesos que hacen posible los sistemas de identificación digital, se cuenta con una visión más integral sobre sus fundamentos, para entender mejor sus aplicaciones prácticas y funcionamiento.

En esta guía vamos a tratar y a trabajar con los principales sistemas de identificación digital para personas físicas y jurídicas utilizados por la **Administración General del Estado**. Estos sistemas son:

- El “Documento Nacional de Identidad Electrónico”,
- El “Certificado electrónico o digital”, en particular el “Certificado de la Fábrica Nacional de Moneda y Timbre”.
- El sistema “Cl@ve: identidad electrónica para las administraciones”.

A continuación, veremos en detalle cada uno de ellos, acompañados de guías prácticas sobre su funcionamiento.


El uso de las nuevas tecnologías me reporta beneficios
Me
2.0
@dministro

DOCUMENTO NACIONAL DE IDENTIDAD ELECTRÓNICO

El **Documento Nacional de Identidad (DNI)** es el documento de identificación personal fundamental de todo ciudadano español, el único de uso universal, reconocido y de plena aceptación en todas las administraciones y ámbitos públicos y privados en España. La presentación de este documento es Obligatorio para la expedición y obtención de otros muchos documentos y trámites, como pueden ser: pasaporte, permiso de conducir, seguridad social, NIF, etc. El **DNI** lo expide el Ministerio del Interior de España, Dirección General de la Policía a través del Cuerpo Nacional de Policía (en adelante CNP).

En este sentido, el **Documento Nacional de Identidad electrónico** (en adelante **DNIe**) es la respuesta a las nuevas necesidades surgidas en la **nueva sociedad de la información y las comunicaciones telemáticas**, proporcionando ahora a los ciudadanos una identidad personal en el mundo digital de una sociedad interconectada.

El DNI Electrónico tiene su página oficial en la dirección www.dnielectronico.es

¿QUÉ HACE EL DNI ELECTRÓNICO?

El DNIe se adapta a esta nueva realidad y suma al documento ya existente herramientas electrónicas para poder realizar una infinidad de gestiones digitales de forma segura. Esto es posible gracias a la incorporación de un pequeño **circuito integrado** (**chip**) que contiene:

- Los **datos digitalizados** que muestra la tarjeta (incluyendo foto, firma y huella dactilar).
- Los **certificados digitales** de identidad, autentificación y firma electrónica.

El DNIe no contiene ningún registro histórico de la persona titular ni datos sanitarios, fiscales, penales, laborales, etc

Este chip puede ser leído por dispositivos electrónicos para acceder y así interactuar con sus **certificados electrónicos** y utilizarlos para la autentificación en un servicio o firma de un documento electrónico de la Administración Pública o de una empresa privada.

El DNIe nos ofrece en un mismo documento las funcionalidades y garantías de identificación necesarias para el mundo moderno.

¿QUÉ GARANTÍAS NOS OFRECE EL DNIE?

Así como el DNI ha sido el documento legal que garantiza nuestra identidad personal y le da validez legal necesaria a nuestra firma manuscrita para utilizarla en cualquier documento, el DNIe da esas mismas garantías en el mundo digital, asegurando tanto tu identidad como tu firma electrónica, otorgándoles la misma validez legal.

Estas garantías en el mundo digital son posibles porque la infraestructura establecida para el DNIe nos permite poder establecer relaciones de confianza necesarias para las comunicaciones electrónicas:

- Autentificación de la identidad personal.
- Certificación de la integridad de los documentos electrónicos, es decir, que no han sido modificados por terceras partes.
- Firma electrónica de documentos y la garantía de que estos documentos no pueden ser luego negados por quien hizo la firma, la llamada garantía de no repudio.

DNIe y DNI 3.0

Como ya comentamos, la evolución de la sociedad ha llevado a que nuestros documentos de identidad cambien adaptándose a los tiempos y a la evolución de la tecnología y la sociedad. Antes del DNIe ya pasó con el DNI por la incorporación de la fotografía o la huella dactilar.

Y al entrar en la era de las comunicaciones y lo digital, con su desarrollo vertiginoso, esa evolución se acelera. El DNIe, que nació en el 2006, se tuvo que adaptar rápidamente a nuevas necesidades y a finales del año 2015 surge el **DNI 3.0** en sustitución del DNIe, siendo esta una versión mejorada que incorpora nuevas tecnologías y características ampliadas.

> El DNIe y el DNI 3.0 coexistirán hasta la paulatina desaparición del DNIe, tal como sucede con el DNI tradicional.

Aunque el DNI 3.0 es el documento que está vigente seguiremos haciendo mención de las siglas DNIe como referencia general al documento de identidad electrónico, por su mayor arraigo y fácil identificación.

La diferencia principal entre estos documentos de identidad es que el DNI 3.0 trae un chip de **interfaz dual** (**dual interfaz**) que permite una conexión inalámbrica entre este y un dispositivo lector a través de tecnología inalámbrica **NFC** (Comunicación de campo cercano), así como la conexión por contacto físico con un **lector de tarjetas inteligentes** tal como hace el DNIe.

Este tipo de conexión permite que se pueda acceder a un servicio electrónico utilizando un **teléfono inteligente** y el DNI 3.0 a través de una **aplicación** y realizar el trámite telemático.

DNI

Firma, foto, huella dactilar

DNIe (2006)

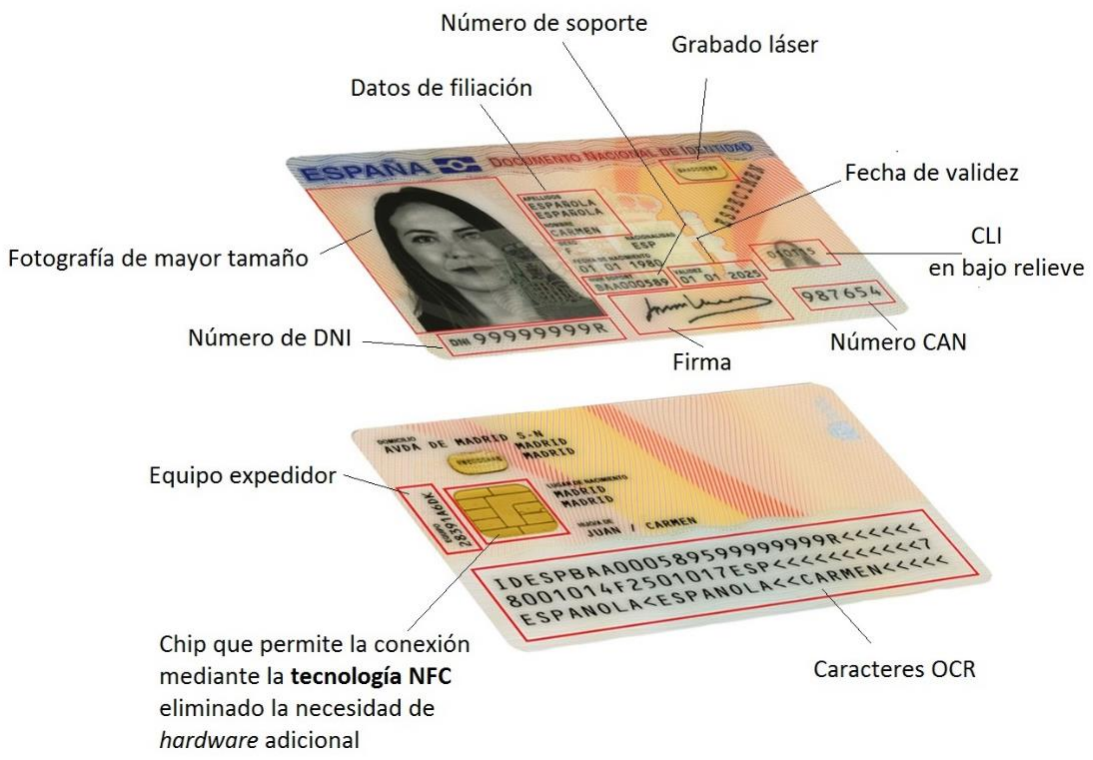
Chip electrónico:

- Certificados digitales

DNI 3.0 (2015)

Conectividad NFC

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



LOS CERTIFICADOS DEL DNIe

Las funciones de identidad, autentificación y firma electrónica que permite realizar el DNIe/3.0 se hacen a través de los llamados **certificados electrónicos o digitales**, que son archivos o documentos digitales que se encuentran en el chip del DNI que contiene las claves criptográficas que nos sirven de **identidad en el mundo digital** y que han sido certificadas por el CNP al momento de expedir el DNI.

Esta identidad digital almacenada en el DNIe la conforman los siguientes certificados:

- Los de **autentificación e identidad**, para acreditar con certeza quiénes somos.
- Los de **firma electrónica**, para firmar digitalmente documentos electrónicos.

> Los certificados digitales del DNIe tienen las mismas funcionalidades que se encuentran en el "Certificado de la Fábrica Nacional de Moneda y Timbre", con la diferencia de que estos están almacenados en el chip del DNIe.

Caducidad de los certificados del DNIe

Los certificados electrónicos del DNIe no tienen una validez indefinida. De hecho, **cada 5 años** hay que acudir personalmente a renovarlos en uno de los "Puntos de Actualización del DNIe" ubicados en cualquier **"Oficina de Expedición del DNI electrónico"**.

Cuando los certificados están a punto de caducar llega una notificación al correo electrónico que se ha indicado cuando se expide el DNI.

La actualización de los certificados digitales del DNIe no es de carácter obligatorio, solo necesitará hacerlo quien utilice el DNIe para gestiones electrónicas.

¿SON COMPLICADOS DE UTILIZAR?

Utilizar el DNIe o el 3.0 nos ofrece ventajas muy evidentes, pero presentan algunas barreras iniciales:

- Su instalación inicial puede resultar complicada.
- Para gestionarlo hay que desplazarse físicamente a una oficina de expedición.

En esta guía aclararemos las dudas que presentan la instalación y la gestión del DNIe/3.0.

¿CÓMO SE OBTIENE?

El Documento Nacional de Identidad en España se obtiene acudiendo **de forma presencial** a una de las **"Oficina de Expedición del DNI electrónico"** dependientes del CNP, que en un único acto administrativo entregarán el DNI el mismo día del trámite.

La expedición o renovación del documento nacional de identidad debe hacerse de forma presencial en las oficinas de expedición del DNI, incluyendo la gestión del DNIe y sus certificados electrónicos. Solo se contempla la opción de **"imposibilidad de**

desplazamiento" si por motivos de salud no se puede acudir a una oficina de expedición. Para más información sobre este procedimiento de "imposibilidad de desplazamiento" puedes visitar el "Portal Oficial del DNI Electrónico":

http://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_481&id_menu=[8

A grandes rasgos se puede indicar que, para **sacar, renovar o restituir un DNIe por pérdida o robo** es necesario lo siguiente:

- Establecer una cita en el servicio de "Cita previa DNIe" del CNP: www.citapreviadnie.es.
- Acudir a la oficina de expedición seleccionada en la cita con todos los requisitos solicitados para el tipo que gestión que se quiere hacer (nuevo documento de identidad o renovación por caducidad o pérdida) y pagar la tasa correspondiente.
- En el caso de la renovación del DNI esta debe hacerse dentro de los últimos 90 días de vigencia o se tendrá que abonar una tasa.

Para más información sobre este procedimiento puedes visitar el "Portal Oficial del DNI Electrónico": www.dnielectronico.es

Con la expedición del nuevo DNIe se da un sobre cerrado que contiene un código PIN (número de identificación personal) que es la clave de seguridad **necesaria** para utilizar el DNIe.

La clave personal de acceso: código PIN

El código PIN es la **contraseña** de seguridad que permite acceder y utilizar las características electrónicas del DNIe para utilizar sus certificados electrónicos en trámites y gestiones telemáticas o para gestionar el mismo DNIe.

El PIN es **secreto, personal e intransferible**, conformado por una combinación de letras, números y caracteres especiales. Hay que conservar este PIN en un lugar **seguro y privado**, en caso de perderlo o que sepas que puede ser conocido por otra persona tendrás que solicitar uno nuevo. **El PIN puede ser cambiado** en cualquier momento y todas las veces que se considere necesario.

NUNCA guardes el PIN apuntado en el mismo sitio en el que tienes tu DNIe, como tu cartera.

Cuando se accede a un servicio electrónico utilizando el DNIe para identificarse, el sistema solicitará el código PIN para asegurar así que el DNIe no está siendo utilizado por otra persona que no sea el titular del documento de identidad.

Si se introduce mal el PIN **tres veces consecutivas** se bloqueará el DNIe. Para desbloquearla tendrás a acudir a una oficina de expedición y renovar la contraseña en un **"Punto de Actualización de DNIe"**.

Validez y renovación del DNIe

La tarjeta del DNIe, el soporte físico, tiene un tiempo determinado de validez que varía en función de la edad de la persona.

Estos períodos de validez van desde los dos años cuando la persona tiene entre 0 y 5 años, cinco años cuando tienen entre los 5 a los 30, diez años entre los 30 y 70 años y, a partir de los 70 años, el documento nacional de identidad pasa a ser permanente.

IMPORTANTE: una vez que el DNIe/3.0 caduca no se pueden utilizar sus certificados electrónicos.

¿Qué hago si lo pierdo o me lo roban?

Si se pierde o es robado el documento de identidad, sea electrónico o no, hay personarse lo más pronto posible en una "Oficina de Expedición del DNI" para denunciar el hecho.

IMPORTANTE: en el caso de que tu DNI fuese electrónico o 3.0 los certificados electrónicos del documento serán revocados de forma inmediata en cuanto verifiquen la validez de tu denuncia.

¿Cómo se usa el DNIe?

Como ya se ha ido comentando a lo largo de esta sección, al acceder a los certificados electrónicos que contiene el chip del DNIe/3.0 se pueden realizar las diversas operaciones de identificación, autentificación y firma electrónica necesarias para utilizar y realizar servicios y trámites electrónicos.

Asimismo, para acceder a los datos del chip se puede hacer de dos formas:

- **Por contacto físico o de hardware:** introduciendo el DNIe o el DNI 3.0 en un dispositivo lector de tarjetas inteligentes, comúnmente conocido como **"lector de DNI electrónico"**.
- **Por conexión inalámbrica:** solo con el DNI 3.0 y un dispositivo que disponga de conexión inalámbrica por **NFC**.

Una vez conectado el DNIe/3.0 de forma física o inalámbrica se puede proceder a identificarse en un servicio electrónico o firmar un documento electrónico.

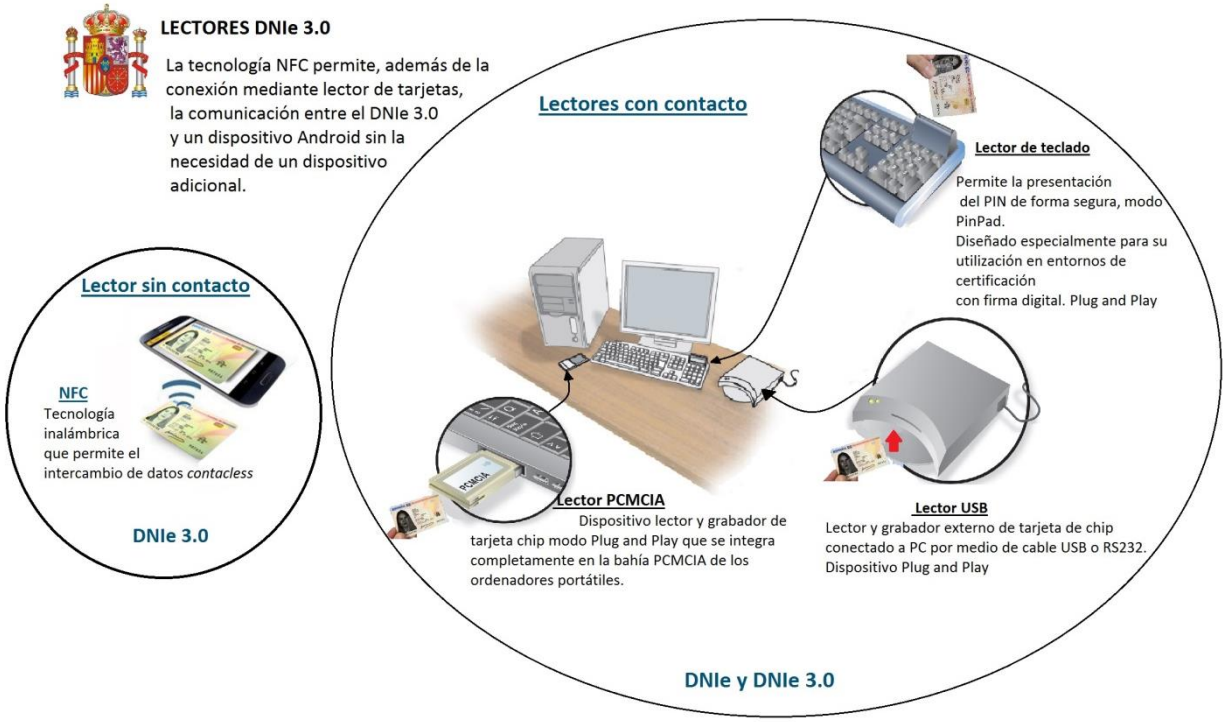
Conexión con lector de DNIe

Para utilizar el DNIe o el 3.0 en un ordenador o incluso un dispositivo móvil se necesita utilizar un lector de tarjetas inteligentes conectado al mismo. En su mayoría, estos lectores son periféricos externos para conectar vía USB. Estos lectores también pueden venir integrados en un teclado.

Antes de poder utilizar el lector es necesario que se haga una instalación previa del dispositivo, que dependiendo del tipo de lector y el sistema operativo que se use, puede requerir de la instalación de algunos componentes de software. La instalación del lector y su óptima puesta en funcionamiento variarán en función del navegador con el que se vaya a trabajar.

Conexión por NFC

Conectar de forma inalámbrica por NFC el DNI 3.0 estará, mayoritariamente, reservado a los dispositivos móviles (smartphones o tablets). Para utilizar NFC hay que activar dicha función en las conexiones inalámbricas del dispositivo móvil y una vez activada solo hay que aproximar el DNI 3.0 a menos de un centímetro del dispositivo para que la antena active el chip y lea su contenido y así utilizarlo con un servicio electrónico.



Gestión del DNIe

Las características y funciones electrónicas del DNIe requieren que se puedan hacer una serie de gestiones para garantizar su funcionamiento, cosas como actualizar los certificados electrónicos o cambiar el PIN o contraseña de nuestro DNIe/3.0.

Todas las gestiones se realizan presencialmente a través de los **"Puntos de Actualización del DNIe"** ubicados en las oficinas de expedición del DNIe.

El "**Punto de Actualización del DNIe**" (PAD) es un terminal informático que, previa identificación, permite acceder a las funciones electrónicas del documento y gestionarlo.

Para acceder a los puntos de actualización hay que identificarse con **el DNI y el código PIN** de este (en el PAD será mencionado como contraseña) o, según lo requiera el caso, con las huellas dactilares (llamadas **impresiones dactilares** o **plantillas biométricas**).

Las gestiones que se pueden realizar en un PAD son:

- Consultar y cambiar algunos datos del DNI.
- Cambiar el PIN.
- Desbloquear el DNI.
- Comprobar y renovar los certificados electrónicos.

Si encuentras problemas con la utilización del DNIe o del PAD debemos pedir ayuda a uno de los funcionarios de la oficina de expedición.

El terminal y su accesibilidad

El PAD es un terminal vertical que dispone de una **pantalla táctil** que permite controlar la mayoría de las opciones. Además, de forma complementaria y alternativa, tiene un teclado completo y un **ratón de bola**. Más arriba y a la izquierda del teclado se encuentra el **"Lector de DNIe"** y a la misma altura en el lado opuesto el **"Lector de huella dactilar"**.

Para personas que no tienen la altura necesaria para utilizar el PAD (por ejemplo, al ir en silla de ruedas), al borde derecho del teclado hay dos botones que permiten subir y bajar el PAD para adaptarlo a la altura de la persona. Todos los elementos del PAD están identificados en Braille y se dispone de un conector para audífonos ubicado debajo del lector de DNIe.

"ME @DMINISTRO 2.0" EN LA PRÁCTICA: DNI ELECTRÓNICO

Esta sección contiene las guías prácticas sobre el "Documento Nacional de Identidad Electrónico".

Instalar el DNIe:

- DNIe: cómo se instala el lector de tarjetas y el DNIe
  - Instalación DNIe: con Internet Explorer y Google Chrome

Gestionar el DNIe:

- DNIe: gestiones en los Puntos de Actualización del DNIe (PAD)
  - DNIe PAD: cómo me identifico
  - DNIe PAD: cómo restaurar la contraseña por olvido o bloqueo
  - DNIe PAD: cómo verificar el estado DNIe
  - DNIe PAD: cómo cambiar el PIN o contraseña
  - DNIe PAD: cómo renovar los certificados
  - DNIe PAD: cómo cambiar el correo electrónico en el DNIe

ADVERTENCIA

Dada la naturaleza cambiante de los servicios electrónicos de la misma Web, en constante actualización y renovación, los contenidos de esta guía pueden variar.

Esta guía debe tomarse como una referencia general que te ayude a completar un objetivo en el que procuramos llegar lo más cerca posible.

DNIE: CÓMO SE INSTALA EL LECTOR DE TARJETAS Y EL DNIE

Estas guías instruyen sobre los procedimientos para instalar el lector de tarjetas inteligentes y del DNIe con **Internet Explorer y Google Chrome** en ordenadores con el **sistema operativo Windows**.

Más información sobre cómo hacer estos procedimientos en otros sistemas operativos (Mac, Linux, etc.) en el "Portal del DNIe": www.dnielectronico.es.

Instalación DNIe: con Internet Explorer y Google Chrome

Para instalar un lector de tarjetas inteligentes en Windows 7, 8 y 10 y utilizar el DNIe con Internet Explorer y Google Chrome hay que seguir los siguientes pasos:

- Conecta el dispositivo en el ordenador. Windows buscará los controladores.
- Una vez instalado el lector de tarjetas inteligentes introduces el DNIe y se descargará e instalará, del servicio de actualización de "Microsoft Windows Update", los controladores (drivers) necesarios para su funcionamiento con Internet Explorer y Chrome.

Nota: si hay una instalación manual hecha previamente tendrás que desinstalarla primero antes de proceder a hacer una instalación automática nueva.

IMPORTANTE: no retires el DNIe del lector de tarjetas hasta que no termine la instalación.

DNIE: GESTIONES EN LOS PUNTOS DE ACTUALIZACIÓN DEL DNIE (PAD)

La pantalla inicial **"PUNTO DE ACTUALIZACIÓN DEL DNIe"** ofrece dos opciones con instrucciones de ayuda para utilizar el terminal:

- **"Cómo acceder"**.
- **"Uso del ratón"**.

IMPORTANTE: Mientras se use el PAD, hay que mantener conectado todo el tiempo el DNIe en el lector de DNIe. Si se retira **se perderá la comunicación** y el procedimiento que se esté haciendo dará error o, en determinados casos, **puede dañar el chip irremediablemente.**

DNIe PAD: cómo me identifico

Para identificarnos y empezar a usar el terminal hay que seguir los siguientes pasos:

- Nos identificamos en el PAD introduciendo el DNI en la ranura del lector con el chip hacia arriba.
- Se activará la pantalla **"DNIe: INICIO DE SESIÓN"**. Utilizando el teclado introducimos la **"contraseña de acceso al DNIe"** (código PIN).

Para ver si estamos escribiendo bien la contraseña podemos pulsar el símbolo en forma de ojo que se encuentra al lado de la casilla de la contraseña del DNIe, esto hará que se visualicen los caracteres en vez de ver los puntos de control.

La contraseña (código PIN) puede tener letras **mayúsculas o minúsculas**, así que es muy importante estar atentos a esto para evitar errores con la contraseña. Asegúrate de que la tecla de "bloquear mayúsculas" del teclado no está activada, para saberlo presiónala y si está en modo mayúsculas saldrá un mensaje en pantalla advirtiéndolo. Y si tienes dudas selecciona el ícono en forma de ojo para cerciorarte.

- Si introducimos correctamente el PIN pasaremos a la pantalla **"DNIe: INFORMACIÓN DE USUARIO"**. Desde aquí accedemos a todas las gestiones que permite el punto de actualización:
  - **"Verificar la identidad"**.
  - **"Cambiar contraseña"**.
  - **"Renovar certificados"**.
  - **"Mostrar información adicional"**: se muestran toda la información personal que contiene el DNI y se puede cambiar el correo electrónico.

DNIe PAD: cómo restaurar la contraseña por olvido o bloqueo

Si no se puede hacer la identificación en el PAD con la contraseña, ya sea por olvido, pérdida o porque se bloqueó el DNIe, al introducir incorrectamente la contraseña tres veces, hay que usar **el DNIe y las huellas dactilares** para identificarse.

Para restituir la contraseña hay que seguir los siguientes pasos:

- En la pantalla inicial **"PUNTO DE ACTUALIZACIÓN DEL DNIe"** seleccionamos "**Comenzar"**.
- Introducimos el DNIe en la ranura del lector con el chip hacia arriba.
- En la pantalla **"DNIe: INICIO DE SESIÓN"** seleccionamos "**He olvidado mi contraseña"**.
- Se mostrará la pantalla **"DNIe: DESBLOQUEO DE CONTRASEÑA"**. Nos indicarán que debemos poner un dedo en el lector de huellas dactilares, el dedo que debemos usar estará destacado con un círculo rojo en el dibujo en las instrucciones de la pantalla. **Ponemos la yema del dedo en el lector**, con firmeza, pero sin ejercer mucha fuerza.

IMPORTANTE: no retiraremos el dedo del lector hasta que un mensaje nos indique que podemos hacerlo. Si retiramos el dedo del lector antes de terminar el proceso de verificación de identidad el proceso se interrumpirá.

- En caso de error se mostrará un mensaje indicando las posibles causas y preguntando si se intenta de nuevo. Para intentarlo de nuevo pulsamos **"Aceptar"**.
- Si la huella capturada es verificada correctamente se mostrará la pantalla **"DNIe: NUEVA CONTRASEÑA DE USUARIO"**. Introduciremos una contraseña nueva.

  IMPORTANTE: no olvides tu nueva contraseña o tendrás que repetir el procedimiento. En la parte inferior de la pantalla te indican las condiciones que debe cumplir la nueva contraseña.
- Al terminar pulsamos **"Aceptar"**.
- Tenemos que confirmar la nueva contraseña escribiéndola de nuevo. Al terminar pulsamos **"Aceptar"**.
- Al introducir correctamente la contraseña un mensaje nos avisará que esta ha sido actualizada. Pulsamos **"Continuar"**.
- Ya de vuelta en la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** podemos acceder a todas las gestiones que permite el punto de actualización o salir del mismo.

DNIe PAD: cómo verificar el estado DNIe

Con esta verificación se comprueba el estado de los certificados electrónicos y las claves de usuario del DNIe. Para comprobar el estado del DNIe hay que seguir los siguientes pasos:

- Desde la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** pulsamos **"Verificar DNI"**.
- Una ventana nos indicará que se comprobará el contenido de DNIe.
- Al terminar la comprobación si todo está correcto un aviso nos indicará que la operación se completó con éxito.
- Pulsamos **"Continuar"**.
- De fallar dirá: **"El DNI no ha superado las comprobaciones necesarias"**. Selecciona **"Reintentar"** para realizar una nueva comprobación.
- De fallar repetidamente seleccionamos **"Cancelar"** y renovamos los certificados digitales del DNIe. Si el problema persiste consulta con el personal de la oficina de expedición.

DNIe PAD: cómo cambiar el PIN o contraseña

En determinadas ocasiones será necesario cambiar la contraseña actual del DNIe por una nueva. Para cambiar la contraseña hay que seguir los siguientes pasos:

Desde la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** seleccionamos **"Cambiar contraseña"**.

- En **"DNIe: NUEVA CONTRASEÑA DE USUARIO"** aquí introduciremos una contraseña nueva.

- Al terminar selecciona **"Aceptar"**.
- Tenemos que confirmar la nueva contraseña escribiéndola de nuevo. Al terminar pulsamos **"Aceptar"**.
- Al introducir correctamente la contraseña un mensaje nos avisará que esta ha sido actualizada. Pulsamos **"Continuar"**.
- Ya de vuelta en la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** podemos acceder a todas las gestiones que permite el punto de actualización o salir del mismo.

DNIe PAD: cómo renovar los certificados

Para renovar los certificados y las claves de usuario del DNIe hay que seguir los siguientes pasos:

- Desde la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** selecciona "**Renovar certificados"**.
- Una ventana nos advertirá que el proceso eliminará todas las claves privadas y certificados de usuario del DNIe para generar unos actualizados. Selecciona **"Aceptar"**.
- Se mostrará la pantalla **"DNIe: RENOVACIÓN DE CERTIFICADOS"**. Nos indicarán que debemos poner un dedo en el lector de huellas dactilares, el dedo que debemos usar estará destacado con un círculo rojo en el dibujo en las instrucciones de la pantalla. **Ponemos la yema del dedo en el lector**, con firmeza, pero sin ejercer mucha fuerza.

> **IMPORTANTE:** No retiraremos el dedo del lector hasta que un mensaje nos indique que podemos hacerlo. Si retiramos el dedo del lector antes de terminar el proceso de verificación de identidad el proceso se interrumpirá.

- Si todo está correcto comenzará la actualización de los certificados. Este procedimiento puede durar varios minutos.

IMPORTANTE: no retires el DNI del lector de tarjetas hasta que termine el proceso porque podría quedar inservible.

- Si todo va bien se mostrará la ventana **"La renovación se ha completado con éxito"**. Seleccionamos **"Continuar"**.
- En esta pantalla se iniciará un proceso para verificar y asegurar el buen funcionamiento de los certificados y claves de usuario nuevos. Seleccionamos **"Aceptar"**.
- Si todo está bien se mostrará la pantalla **"DNIe: VERIFICACIÓN DEL DNI"** con un mensaje confirmando que la operación se ha completado con éxito. Seleccionamos **"Aceptar"**.

DNIe PAD: cómo cambiar el correo electrónico en el DNIe

Se puede cambiar el correo electrónico dado como dato personal al momento de sacar o renovar el DNI y que sirve de referencia para diversas gestiones, como puede ser recibir la notificación de la próxima caducidad de los certificados digitales del DNIe. Esta operación se puede realizar tantas veces como sea necesario.

IMPORTANTE: Al cambiar la dirección de correo electrónico se tendrán que renovar los certificados electrónicos y las claves de usuario.

Para cambiar el correo electrónico utilizado en el DNIe hay que seguir los siguientes pasos:

- Desde la pantalla **"DNIe: INFORMACIÓN DE USUARIO"** seleccionamos **"Mostrar información adicional"** debajo del título **"DNIe: INFORMACIÓN PERSONAL"**.
- En la pantalla **"DNIe: INFORMACIÓN ADICIONAL"** se muestran toda la información personal contiene el DNI. En el último renglón seleccionamos el **icono de edición** ubicado a la derecha de la casilla del correo electrónico.
- Se abrirá la ventana para introducir la nueva dirección de correo electrónico. Indicamos la nueva dirección y al finalizar seleccionamos **"Aceptar"**.
- Se abrirá una ventana solicitando la renovación de los certificados para confirmar el cambio. Selecciona **"Aceptar"**.
- Se abrirá la ventana advirtiendo que el proceso eliminará las claves privadas y certificados de usuario en el DNI para generar otros actualizados. Selecciona **"Aceptar"**.
- Se mostrará la pantalla **"DNIe: RENOVACIÓN DE CERTIFICADOS"**. Nos indicarán que debemos poner un dedo en el lector de huellas dactilares, el dedo que debemos usar estará destacado con un círculo rojo en el dibujo en las instrucciones de la pantalla. **Ponemos la yema del dedo en el lector**, con firmeza, pero sin ejercer mucha fuerza.

IMPORTANTE: no retiraremos el dedo del lector hasta que un mensaje nos indique que podemos hacerlo. Si retiramos el dedo del lector antes de terminar el proceso de verificación de identidad el proceso se interrumpirá.

- Si todo está correcto comenzará la actualización de los certificados. Este procedimiento puede durar varios minutos.

IMPORTANTE: no retires el DNI del lector de tarjetas hasta que termine el proceso porque podría quedar inservible.

- Si todo va bien se mostrará la ventana **"La renovación se ha completado con éxito"**. Seleccionamos **"Continuar"**.
- En esta pantalla se iniciará un proceso para verificar y asegurar el buen funcionamiento de los certificados y claves de usuario nuevos. Seleccionamos **"Aceptar"**.
- Si todo está bien se mostrará la pantalla **"DNIe: VERIFICACIÓN DEL DNI"** con un mensaje confirmando que la operación se ha completado con éxito. Seleccionamos **"Aceptar"**.


Acceso en igualdad de condiciones.
Me
2.0
@dministro

CERTIFICADO ELECTRÓNICO O DIGITAL

El certificado electrónico o digital es un documento digital que contiene **claves criptográficas** que sirven de identidad a una persona física y jurídica en el mundo digital y que está **firmado electrónicamente** por un **prestador de servicios de certificación** que valida y vincula la identidad de dicha persona con las herramientas de identificación, autentificación y firma electrónica que le representarán en el ámbito telemático, electrónico o digital.

Por tanto, el certificado electrónico es un documento o archivo digital, que se instala en el ordenador o en el navegador de Internet que se vaya a utilizar para realizar trámites telemáticos o en **dispositivos criptográficos de seguridad** como puede ser una tarjeta inteligente o una unidad USB, el más conocido de estos dispositivos criptográficas es el "Documento Nacional de Identidad Electrónico".

¿PARA QUÉ SIRVEN?

En definitiva, el certificado digital es un conjunto de datos informáticos que sirven de identidad gracias a que un organismo verificó que la persona física y la que dice ser en el certificado electrónico es la misma. Estos datos a su vez garantizan que sea una identidad única.

Esto es lo mismo que sucede cuando se obtiene o renueva un DNIe: el funcionario de la oficina de expedición verifica la identidad de la persona, toma las huellas dactilares y ve realizar la firma manuscrita, certificando así que todos los datos que aparecen en el DNI son de esa persona y que esa firma tenga validez legal cada vez que la use en un documento de papel, y que posteriormente vinculará a las funciones electrónicas del DNIe.

Estos certificados electrónicos dan las herramientas de identificación, autentificación y firma electrónica necesarias para realizar trámites y gestiones telemáticas, intercambio de información y firmado de documentos digitales de forma segura y con totales garantías legales.

¿Todos son iguales?

Los certificados electrónicos pueden ser para personas físicas o jurídicas (empresas, organizaciones privadas o de carácter público, que vinculan la identidad del organismo o de un representante de estos con el certificado). Incluso los hay para componentes informáticos, como por ejemplo un servidor, que garantiza la identidad del sitio o del servicio a los usuarios que están accediendo a ellos y utilizándolos.

Existen además una multitud de prestadores de servicios de certificación, públicos y privados, que emiten certificados electrónicos y que según el prestador del servicio puede tener un uso más o menos amplio.

En el caso de esta guía hablaremos de los certificados para personas físicas y Jurídicas de la **Fábrica Nacional de Moneda y Timbre**.

¿Qué dificultades presenta?

Los certificados electrónicos tienen ventajas muy evidentes, pero presentan algunas barreras iniciales:

- Para obtener el certificado es necesario desplazarse en persona para que se acredite la identidad del solicitante si no se cuenta con algún sistema de identificación electrónica como el DNIe que reemplace este proceso.
- Su instalación inicial puede resultar complicada.
- Su gestión puede resultar complicada.

En esta guía aclararemos las dudas que presentan el proceso de registro, la instalación y la gestión de un certificado digital.

CERTIFICADOS DE LA FÁBRICA NACIONAL DE MONEDA Y TIMBRE

La **Fábrica Nacional de Moneda y Timbre de la Real Casa de la Moneda** (en adelante **FNMT-RCM)**, emite los **"Certificados FNMT"** a través de su departamento **CERES** (CERtificación ESpañola).

La FNMT-RCM emite varios tipos de certificados digitales, para el caso de nuestra guía vamos a describir los **certificados de persona física y los certificados de Representante de Persona Jurídica** (en adelante certificados de persona jurídica).

Si quieres ver más detalles sobre todos los diferentes tipos de certificados que emite la FNMT-RCM, puedes consultar la url: https://www.sede.fnmt.gob.es/certificados.

Tanto el certificado de las personas físicas como el certificado de las personas jurídicas, es de uso generalizado por los servicios telemáticos de las administraciones públicas en España.

Puedes visitar la sede electrónica de la Fábrica Nacional de Moneda y Timbre de la Real Casa de la Moneda en la siguiente dirección: www.sede.fnmt.gob.es.

¿Cómo se obtiene el certificado electrónico?

El certificado FNMT-RCM se puede solicitar a través de tres vías:

- **Obtener el certificado con acreditación personal**: Con este procedimiento se inicia el trámite solicitando el certificado desde la **sede electrónica** de la FNMT-RCM (www.sede.fnmt.gob.es) que generará un **"código de solicitud"** con el que hay que presentarse en una oficina de registro para que se **acredite la identidad**. Una vez hecho esto se descarga e instala el certificado electrónico en el navegador donde se haya comenzado el proceso.

- **Obtener el certificado con DNI electrónico (en caso de persona física)**: Este proceso es idéntico al anterior con la salvedad de que no hace falta acreditar la identidad en una oficina de registro, será utilizando un DNIe o 3.0 que se garantice la identidad de quien lo solicita.

- **Obtener el certificado para dispositivos Android**: con esta modalidad, la solicitud del certificado electrónico se comienza desde una aplicación para Android de la FNMT-RCM y su descarga se hace al mismo dispositivo móvil una vez validada la identidad en una oficina de registro.

La FNMT-RCM acredita la identidad de las personas solicitantes a través de una red de **"Oficinas de Registro"** ubicadas en oficinas de la Seguridad Social, en Delegaciones y Administraciones de la Agencia Tributaria y en Oficinas Consulares de carrera de España en el extranjero.

IMPORTANTE: Nunca hay que ceder o dejar copiar nuestro certificado electrónico a otras personas, servicios o aplicaciones.

¿Cuánto dura un certificado electrónico?

Los certificados electrónicos, en cualquiera de sus modalidades y formas de obtenerlos, tienen un tiempo predeterminado de validez y vigencia. La duración actual de los Certificados FNMT de persona física es de cuatro años y los certificados expedidos antes del 1 marzo del 2015 tienen una duración de tres años. La duración actual de los Certificados FNMT de persona jurídica es de dos años.

¿Se puede renovar un certificado?

Una vez que el certificado electrónico de la FNMT-RCM caduca hay que hacer de nuevo todo el proceso de obtención, pero 60 días antes de que este caduque se abre un plazo para renovarlo telemáticamente desde la sede electrónica de la FNMT-RCM (www.sede.fnmt.gob.es).

Los certificados electrónicos FNMT de personas físicas, sean los nuevos o los anteriores a marzo del 2015, pueden renovarse telemáticamente solo una vez. Una vez caduque el segundo período de 4 años tendrá que hacerse de nuevo todo el proceso de obtención.

En caso de los certificados electrónicos FNMT de persona Jurídica, es preciso personarse en una oficina de registro para obtener un certificado de representante, con la documentación exigible.

Anular un certificado.

Si por alguna razón es necesario anular un certificado FNMT de Persona Física, Jurídica, o cualquier otro certificado, antes de que este caduque se puede hacer en cualquier momento, ya sea de forma presencial o telemáticamente.

Al solicitar la anulación del certificado electrónico y una vez validada la identidad del titular del certificado, este es anulado de forma inmediata.

IMPORTANTE: Una vez que revocas un certificado electrónico no se puede reactivar, será necesario que comiences de nuevo todo el proceso para solicitar un nuevo certificado.

Entre las razones por las que se puede anular un certificado están:

- Que se pierda o dañe el equipo donde se tenga instalado el certificado y no exista una copia de seguridad.
- Que la persona titular del certificado fallezca o tenga una situación de incapacidad sobrevenida.
- Que se esté utilizando un certificado de representación de una entidad y ya no se pertenezca a ella.
- Que haya errores en los datos personales utilizados para obtener el certificado.
- Que se detecte o sospeche que las claves de acceso al certificado electrónico han sido comprometidas, que ya no son secretas y pueden ser conocidas por otras personas.

Dentro de los dos tipos de certificados que estamos describiendo vemos lo siguiente:

En el caso del "Certificado FNMT de Persona Física" se observa que se han de cumplir dos condiciones:

1. Podrán solicitar la revocación los titulares de los certificados.
2. La solicitud de la revocación podrá efectuarse durante el período de validez del certificado que consta en el mismo.

Mientras que en el caso del "Certificado FNMT de Persona Jurídica", además se añade la necesidad que la persona que solicite la revocación sea hecha por una persona con facultades de representación suficientes.

La revocación de los dos certificados tanto los de persona física como el de persona jurídica puede hacerse de tres formas:

- **Online:** solicitando la anulación desde la **sede electrónica** de la FNMT-RCM (www.sede.fnmt.gob.es).
- **En una oficina de acreditación:** haciendo el trámite de forma presencial en una Oficina de Acreditación, las mismas donde se acredita la identidad cuando se obtiene el certificado.
- **Por teléfono:** con una llamada telefónica al "Servicio de Revocación Telefónica" en el número 902 200 616 / 91 740 6848 / 91 387 83 37. El servicio funciona las 24 horas del día, los 365 días del año.

GESTIONAR LOS CERTIFICADOS ELECTRÓNICOS

Los certificados electrónicos descargados e instalados en el navegador se ubican en el **"Administrador de certificados"** o **"Almacén de certificados"** desde donde se puede ver, importar, exportar y eliminar del navegador cualquier certificado digital que se tenga instalado.

La mayoría de los navegadores de Internet tienen almacén de certificados, que en el caso de Microsoft Internet Explorer y Google Chrome lo comparten entre sí. Microsoft Edge no tiene esta función. En el caso de los certificados electrónicos en dispositivos Android, estos se archivan en el almacén de certificados del mismo dispositivo.

Una de las gestiones más importantes que hay que hacer con el certificado electrónico es crear una **copia de seguridad** o **respaldo** que permita conservar una copia en un lugar seguro o poder utilizar el certificado en otros navegadores y ordenadores.

IMPORTANTE: una vez que descargaste el certificado electrónico durante el proceso de obtención no podrás hacerlo de nuevo. Si se borra no se puede recuperar, por lo cual es muy importante realizar una copia de seguridad. Si no se cuenta con una copia de seguridad y se pierde el certificado instalado implicará tener que realizar de nuevo todo el proceso de obtención.

¿Cómo se hace una copia de seguridad?

Una de las gestiones más importantes que se debe hacer con el certificado electrónico es hacer una copia de seguridad. Preferentemente, se debe hacer la copia de seguridad en un dispositivo externo al ordenador donde ya está instalado, ya sea en una memoria USB, un CD-ROM o en una **tarjeta o USB criptográfico**.

La copia de seguridad se hará a copia del certificado entero, es decir, vas a respaldar tanto la **clave pública** como la **clave privada**. Sólo se exportará la clave pública para utilizarla cuando queramos identificarnos en comunicaciones cifradas.

Esta copia de seguridad también sirve para llevar el certificado digital a otros navegadores, e incluso otros equipos, copiándolo al administrador de certificados de cada navegador en el cual se quiera utilizar para realizar trámites telemáticos.

IMPORTANTE: Nunca debes ceder tu certificado digital con la clave privada a otras personas, servicios o aplicaciones.

¿Qué formato usan los certificados electrónicos?

Los certificados electrónicos vienen en diversos formatos de archivo, estos variarán según el uso que se les va a dar, como por ejemplo el navegador que los va a utilizar o si el certificado contiene la clave privada y la pública o solo la pública.

Entre los formatos más comunes de certificados electrónicos encontramos los siguientes:

- Sin clave privada: archivos “.cer” y “.p7b”.
- Con clave privada: archivos “.p12” y “.pfx”.

Nota: los archivos .P12 y .PFX son de tipo PKCS #12, por lo cual, **si por algún motivo no podemos utilizar nuestro certificado en formato .P12 simplemente ponemos la extensión a .PFX cambiando el nombre y reescribiendo la extensión**.

"ME @DMINISTRO 2.0" EN LA PRÁCTICA: CERTIFICADO FNMT

Esta sección contiene las guías prácticas sobre el "Certificado de la Fábrica Nacional de Moneda y Timbre".

Obtener el Certificado Electrónico de la FNMT-RCM:

- Certificado electrónico: cómo obtener el certificado software
- Certificado electrónico: cómo obtener el certificado con DNIe
- Certificado electrónico: cómo obtener el certificado con Android

Gestionar el Certificado Electrónico:

- Certificado electrónico: cómo comprobar la instalación
- Certificado electrónico: cómo verificar el estado del certificado
  - Verificación en el navegador: datos y caducidad
    - Ver caducidad en Firefox
    - Ver caducidad en Internet Explorer
    - Ver caducidad en Chrome
  - Verificación online: ver datos, validez y caducidad
- Certificado electrónico: cómo hacer una copia de seguridad
- Certificado electrónico: cómo exportar la clave pública
- Certificado electrónico: cómo usar el certificado en otros sitios
  - Cómo importar el certificado electrónico
    - Importar el certificado a Firefox
    - Importar el certificado a Internet Explorer
    - Importar el certificado a Chrome
- Certificado electrónico: cómo renovarlo telemáticamente
- Certificado electrónico: cómo anularlo telemáticamente

IMPORTANTE: los procedimientos explicados en estas guías están hechos en el sistema operativo Windows, en sus versiones 7, 8 y 10. Más información sobre cómo hacer estos procedimientos en otros sistemas operativos (Mac y Linux) en la sede electrónica de la FNMT-RCM: www.sede.fnmt.gob.es.

ADVERTENCIA

Dada la naturaleza cambiante de los servicios electrónicos de la misma Web, en constante actualización y renovación, los contenidos de esta guía pueden variar.

Esta guía debe tomarse como una referencia general que te ayude a completar un objetivo en el que procuramos llegar lo más cerca posible.

CERTIFICADO ELECTRÓNICO: CÓMO OBTENER EL CERTIFICADO SOFTWARE

Como ya se comentó en la sección "¿Cómo se obtiene el certificado electrónico?", del "Certificado de la Fábrica Nacional de Moneda y Timbre", el proceso de obtención del certificado tiene varias etapas, por tanto, para facilitar la explicación de todo el proceso la guía se ha divido en varias fases:

1. **Preparación:** "Consideraciones previas y configuración del navegador"
2. **Solicitud del certificado:** "Solicitud vía internet de su Certificado"
3. **Acreditación de la identidad:** "Acreditación de la identidad en una Oficina de Registro"
4. **Instalación del certificado:** "Descarga de su Certificado de Usuario"

Nota: el procedimiento entero descrito en esta guía está hecho basándose en el navegador **Mozilla Firefox**. Un navegador gratuito, de código libre y disponible para la gran mayoría de sistemas operativos para ordenadores y dispositivos móviles.

Veamos paso a paso cada fase…

1 "Consideraciones previas y configuración del navegador"

Antes de solicitar y descargar el certificado es necesario que el ordenador y el navegador de Internet que se van a utilizar en el procedimiento cumplan ciertos requisitos para poder procesar la solicitud sin problemas. Estos requerimientos variarán según el navegador que se use.

Para realizar todo el procedimiento es muy importante que desde la solicitud del certificado software hasta la descarga del mismo se haga cuidando estos puntos:

- Tiene que hacerse desde el mismo ordenador.
- Si el ordenador tiene más de un "usuario" creado el procedimiento tiene que hacerse en la misma "sesión de usuario".
- Solo se pueden utilizar los siguientes navegadores de internet:
  - Microsoft Internet Explorer.
  - Mozilla Firefox, a partir de su versión 35.
- Todo el procedimiento tiene que hacerse desde el mismo navegador de Internet.
- No se pueden hacer cambios en el ordenador que se está utilizando, cambios como instalar de nuevo el sistema operativo. Y preferentemente hay que evitar las actualizaciones del sistema.

Dependiendo del navegador que se vaya a utilizar para solicitar e instalar el certificado electrónico hay que seguir los siguientes pasos…

IMPORTANTE: Al iniciar el procedimiento de obtención del certificado digital, tiene que hacerse desde el mismo ordenador, mismo navegador y mismo usuario del ordenador. Tampoco se debe formatear el ordenador, ni realizar actualizaciones del sistema operativo, hasta que hayas descargado el certificado

El procedimiento con Microsoft Internet Explorer

Con Internet Explorer es necesario descargar e instalar un configurador automático creado por la FNMT-RCM antes de solicitar y descargar el certificado electrónico. Para hacerlo hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace:
  - https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"Configurador FNMT-RCM"**,
  bajo el título **"Configuración para Internet Explorer"**.
- Descargamos el configurador. El archivo que se descargará tiene la extensión **".exe"**.
- Buscamos el archivo descargado **"Configurador_FNMT_RCM.exe"** y los ejecutamos.
  - Instalamos el configurador siguiendo los pasos del asistente de instalación.
- Una vez terminada la configuración automática de Internet Explorer ya estamos listos para la siguiente etapa: 2 "Solicitud vía internet de su Certificado" …

El procedimiento con Mozilla Firefox

Antes poder solicitar e instalar el certificado electrónico de la FNMT-RCM en Firefox es necesario instalar dos cosas:

- Un complemento (addon) para firmar.

Nota: los complementos o addons (también llamados extensiones o plugins en otros programas) son pequeños añadidos de software que se instalan, en nuestro caso, a un navegador para aumentar o mejorar sus funcionalidades.

- Los certificados raíz de la FNMT-RCM.

Veamos con detalle cada uno de estos pasos…

Instalación del complemento para firmar

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"complemento para firmar"**,
  bajo el título **"Configuración para Mozilla Firefox 35 o superior"**.
- Se abrirá en una pestaña nueva la página del complemento **"signTextJS"** en el sitio web de complementos de Mozilla Firefox.
- Hacemos clic en **"+ Agregar a Firefox"**.
- Una ventana emergente nos advertirá que se está intentando instalar el complemento de Firefox "signTexUS".
- Hacemos clic en **"Instalar"**.
- Una ventana emergente te avisará que el complemento se instaló con éxito.
- Cerramos la pestaña.

Instalación de los certificados raíz

Los certificados raíz son certificados emitidos por una Autoridad de Certificación, en este caso la FNMT-RCM, que contienen la clave pública de dicha autoridad, necesaria para que se compruebe la autenticidad de los certificados emitidos por ella.

Para instalar los certificados raíz de la FNMT-RCM hay que seguir los siguientes pasos:

- De vuelta en la página de **"Consideraciones previas (paso 1)"** hacemos clic en el enlace **"Instalación de los certificados raíces"**, debajo del título **"Configuración para Mozilla Firefox 35 o superior"**.
- Se abrirá en una pestaña nueva la página **"Procedimiento de Obtención de Certificados"** con los enlaces de los certificados raíz de la FNMT-RCM que debemos instalar en el navegador. Hacemos clic sobre cada uno de los seis enlaces para instalarlos o, en su defecto, descargarlos para luego instalarlos:
  - **"Descarga AC Raíz FNMT-RCM"**.
  - **"Descarga certificado FNMT Clase 2 CA"**.
  - **"Descarga certificado AC FNMT Usuarios"**.
  - **"Descarga certificado AC Representación"**.
  - **"Descarga AC Administración Pública"**.
  - **"Descarga AC Componentes Informáticos"**.
- Con cada enlace realizaremos este procedimiento:

- Hacemos clic en el enlace. Se abrirá una ventana emergente.

Nota: si por error hacemos clic de nuevo en un enlace ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **"Aceptar"**.

- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **"Aceptar"**.

- Una vez terminada la instalación de los certificados raíz en Firefox ya estamos listos para la siguiente etapa: 2 "Solicitud vía internet de su Certificado"…

Instalar un certificado descargado

Si los certificados raíz de la FNMT-RCM no se instalan automáticamente hay que descargarlos para posteriormente importarlos a Firefox.

Para instalar los certificados de forma manual hay que seguir los siguientes pasos:

- Descargamos los certificados. Los archivos que se descargarán tienen la extensión **".cer"**.
- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Avanzado"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Autoridades"**.
- Hacemos clic en **"Importar…"**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si por error cargamos un archivo ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **"Aceptar"**.

- Hacemos clic en el botón **"Abrir"**.
- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **"Aceptar"**.
- Repite el procedimiento con los otros certificados.
- Una vez terminada la carga manual de los certificados raíz ya estamos listos para la siguiente etapa: 2 "Solicitud vía internet de su Certificado" …

2 "Solicitud vía internet de su Certificado"

Una vez que se tenga todo preparado según lo especificado en la etapa 1 "Consideraciones previas y configuración del navegador" se puede proceder a realizar la solicitud y posterior descarga del certificado electrónico.

IMPORTANTE: Recuerda que al solicitar un certificado nuevo a la FNMT-RCM se anulará automáticamente cualquier otro certificado del mismo tipo que tengas.

Para comenzar la solicitud para obtener el certificado software hay que seguir los siguientes pasos:

- Conectamos el lector de tarjetas inteligentes e introducimos el DNIe en el lector.
- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **"Solicitud vía internet de su Certificado"**.
- Una ventana emergente nos alertará sobre la importancia de contar con la configuración necesaria para el navegador antes de solicitar el certificado, según vimos en la etapa: 1 "Consideraciones previas y configuración del navegador".
- Hacemos clic en **"Aceptar"**.
- Rellenamos el formulario con los datos solicitados:
  - **"N.º DEL DOCUMENTO DE IDENTIFICACIÓN"**: ya sea el DNI o el NIE.
  - **"PRIMER APELLIDO (tal y como aparece en su documento de identificación)"**.
  - **"CORREO ELECTRÓNICO"**.

IMPORTANTE: Debes utilizar una dirección de correo electrónico que uses de forma habitual ya que allí **enviarán el "código de solicitud" necesario para los siguientes pasos** de la solicitud del certificado. También quedará asociado a la información del certificado y será por donde la FNMT-RCM **enviará notificaciones**, como la proximidad de la fecha de caducidad del certificado

  - **"Confirme aquí su CORREO ELECTRÓNICO"**: repetimos el correo anterior de forma idéntica.
  - Si se solicita una longitud de clave seleccionamos la de grado alto.
- Al terminar hacemos clic en **"Pulse aquí para consultar y aceptar las condiciones de expedición del certificado"**. Esto desplegará las condiciones de expedición.
- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **"Acepto las condiciones de expedición"** para aceptarlas.

- Hacemos clic en **"Enviar petición"**.
- Enviarán un correo electrónico a la dirección que indicamos antes, desde la cuenta "ac.usuarios@fnmt.es" con el asunto **"Notificaciones FNMT AC Usuarios"**.
- En el correo vendrá el **"código de solicitud"**, este código será requisito fundamental para los siguientes pasos.

> **IMPORTANTE**: Debes conservar el **"código de solicitud"**, no borres el correo. Si el código se te pierde y no lo tienes apuntado tendrás que comenzar de nuevo

Con el código de solicitud ya estamos listos para la siguiente etapa: 3 "Acreditación de la identidad en una Oficina de Registro" …

3 "Acreditación de la identidad en una Oficina de Registro"

En esta etapa se acredita la identidad del solicitante presentándose en persona ante un prestador de servicios de identificación, que en el caso de los certificados de la FNMT-RCM será en una "Oficina de Registro". Hay que recordar que la FNMT-RCM tiene oficinas de registro repartidas entre las oficinas de la Seguridad Social y las delegaciones y administraciones de la Agencia Tributaria distribuidas por todo el territorio nacional, y en determinadas oficinas consulares en el extranjero.

Para realizar la acreditación de la identidad es necesario llevar a la oficina de registro lo siguiente:

- Documento de identidad vigente: DNI, pasaporte, carné de conducir, NIE o el "Certificado de Ciudadano de la Unión" donde conste el NIE junto con el pasaporte o un documento de identidad del país de origen.
- En caso de certificado de persona jurídica, la documentación necesaria para justificar la acreditación dependerá de la forma jurídica que tenga la entidad, los detalles de cada una de ellas se puede consultar en la página 28 del siguiente documento

  https://www.sede.fnmt.gob.es/documents/10446703/10515015/re_pr_representantepj_representanteespj.pdf
- El código de solicitud recibido por correo electrónico en el paso: 2 "Solicitud vía internet de su Certificado".

Localizar una oficina de registro

Para localizar una oficina de registro y que acrediten nuestra identidad hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software

(En caso de persona jurídica hay que seguir las instrucciones de este otro enlace https://www.sede.fnmt.gob.es/certificados/certificado-de-representante/persona-juridica/acreditar-identidad)

- Hacemos clic en **"Acreditación de la identidad en una Oficina de Registro"**.
- En la página **"Acreditar Identidad (paso 3)"** bajo el título **"¿Dónde puede acreditar su identidad?"** encontraremos tres enlaces con formas distintas de encontrar una oficina de registro:
  - **"Las oficinas de la Seguridad Social"**: se abrirá una ventana nueva al listado de **"Oficinas de Registro de Certificados Digitales"**.
    - Hacemos clic en la **Comunidad o Ciudad Autónoma** que corresponda, ya sea en el mapa o en el listado.
    - Saldrá un listado de las **provincias según la Comunidad Autónoma**, hacemos clic en la provincia que corresponda.
    - Se mostrará un listado de **"Oficinas de Registro de Certificados Digitales"** a las que podemos personarnos con sus datos. Indicando si se puede certificar la identidad para el "Certificado de Persona Física de la FNMT-RCM" o del sistema "CL@VE, identidad electrónica para las administraciones".

IMPORTANTE: Cada oficina indica si es necesario pedir una cita previa y los términos de la misma.

  - **"Delegaciones y Administraciones de la AEAT"**: se abrirá una ventana nueva con múltiples opciones para encontrar una delegación o una administración de la Agencia Tributaria.

Para la mayoría de los trámites es obligatorio solicitar cita previa. Puedes iniciar el trámite de pedir cita previa haciendo clic en el enlace **"Cita previa"** en la página **"Delegaciones y Administraciones"**.

- Hacemos clic en el nombre de la **Comunidad o Ciudad Autónoma** que corresponda.
- Posteriormente hay que seleccionar la provincia, si corresponde, y en ellas seleccionamos si se desea acudir a una Delegación o una Administración.
- Finalmente se mostrará un listado con los datos y condiciones de las delegaciones o administraciones disponibles.
- También se puede hacer una búsqueda por código postal, haciendo clic **"Búsqueda de Delegaciones y Administraciones por código postal"** en la página **"Delegaciones y Administraciones"**.

- **"Servicio de localización de las OFICINAS MÁS CERCANAS**": se abre una ventana nueva con un mapa mostrando todas las oficinas de registro.
  - En la caja de búsqueda ubicada en la parte superior izquierda podemos buscar por nombre de población, barrio o por una dirección específica y ver las oficinas de registro más cercanas.

  - En el menú ubicado en la parte superior izquierda podemos filtrar el tipo de oficina de registro que queramos, en nuestro caso: **"Personas Físicas"** o **"Personas Físicas y Jurídicas"**.

- Ya ubicada la oficina de registro nos personamos con nuestro documento de identidad y el código de solicitud.

- Una vez que hayan certificado nuestra identidad enviarán un correo electrónico a la dirección que indicamos en el paso 2 "Solicitud vía internet de su Certificado", avisando que se puede proceder a descargar el certificado y los datos que debemos utilizar para hacerlo: código de solicitud, nuestro primer apellido y número de documento de identidad.

- El correo electrónico también indica el **enlace para descargar el certificado**. Hacemos clic en el enlace y ya estamos listos para la siguiente etapa: 4 "Descarga de su Certificado de Usuario"

4 "Descarga de su Certificado de Usuario"

En esta última etapa se procede a descargar e instalar, en un mismo proceso, el certificado electrónico para persona física o Jurídica de la FNMT-RCM que se ha solicitado. A continuación, vamos a ver los pasos a seguir para cada tipo de certificado.

Para descargar el certificado de persona física hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software

- Hacemos clic en **"Descarga de su Certificado de Usuario"**.

- Rellenamos el formulario con la información solicitada:

  - **"N.º DEL DOCUMENTO DE IDENTIFICACIÓN"**.

  - **"PRIMER APELLIDO (tal y como aparece en su documento de identificación)"**.

  - **"CÓDIGO DE SOLICITUD"**: el código ya utilizado en los pasos anteriores.

- Al terminar hacemos clic en **"Pulse aquí para consultar y aceptar las condiciones de expedición del certificado"**. Esto desplegará las condiciones de expedición.

- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **"Acepto las condiciones de expedición"** para aceptarlas.
  Nota: si deseas descargar una copia en formato PDF de las condiciones de expedición haz clic en **"Descargar condiciones"**.

- Hacemos clic en **"Descargar Certificado"** para iniciar la descarga e instalar el certificado.

- Una ventana emergente avisará que vamos a proceder a instalar el certificado y que desde ese momento adquirimos la condición de **"titular"** y que esto quedará registrado en los sistemas de referencia de la FNMT-RCM que hemos aceptado en las condiciones de uso del certificado. Hacemos clic en **"Aceptar"**.

- Si la descarga fue exitosa aparecerá el botón **"Instalar certificado"**. Hacemos clic en el botón.
- Una ventana emergente alertará que el certificado se instaló. Hacemos clic en **"Aceptar"**.

Si se produce algún error en la instalación vuelve a la página anterior e inténtalo de nuevo. Este mensaje también alerta que se debe hacer una copia de seguridad del certificado.

- Nuestro certificado está listo para usar.

Cuando descargamos un certificado de persona jurídica debemos seguir las instrucciones del enlace siguiente:

https://www.sede.fnmt.gob.es/certificados/certificado-de-representante/persona-juridica/descargar-certificado

El procedimiento es muy similar al del certificado de persona física, con la única diferencia que hay que pagar una cantidad (el precio de certificado para persona jurídica a la fecha de publicación de esta guía es de 14 €), dicho pago debe hacerse con tarjetas de tarjetas de crédito/débito Visa o Mastercard.

En caso de necesitar más ayuda a la hora de conseguir tu certificado puedes consultar directamente a la FNMT-RCM en su página web de preguntas frecuentes en www.cert.fnmt.es/preguntas-frecuentes, por correo electrónico al correo representacion.ceres@fnmt.es o por teléfono en el 91 740 67 21 (atención en días laborables de 9 de la mañana a 6 de la tarde).

CERTIFICADO ELECTRÓNICO: CÓMO OBTENER EL CERTIFICADO CON DNIE

Como ya se comentó en la sección "¿Cómo se obtiene el certificado electrónico?", del "Certificado de la Fábrica Nacional de Moneda y Timbre", el proceso de obtención del certificado con DNIe tiene varias etapas, por tanto, para facilitar la explicación de todo el proceso la guía se ha divido en varias partes.

La obtención del certificado con DNIe difiere del proceso visto en "Certificado electrónico: cómo obtener el certificado software" en que no es necesaria la etapa del paso 3 "Acreditación de la identidad en una Oficina de Registro" ya que el DNIe proveerá las garantías necesarias para realizar la acreditación de identidad. Obtener el certificado electrónico con DNIe tiene estas fases:

- **Preparación:** 1 "Consideraciones previas y configuración del navegador"
- **Solicitud del certificado:** 2 "Solicitud con Certificado"
- **Instalación del certificado:** 3 "Descarga de su Certificado de Persona Física"

Nota: el procedimiento entero descrito en esta guía está hecho basándose en el navegador **Mozilla Firefox**. Un navegador gratuito, de código libre y disponible para la gran mayoría de sistemas operativos para ordenadores y dispositivos móviles.

Veamos paso a paso cada fase…

1 "Consideraciones previas y configuración del navegador"

Antes de solicitar y descargar el certificado con DNIe es necesario que el ordenador y el navegador de Internet que se van a utilizar en el procedimiento cumplan ciertos requisitos para poder procesar la solicitud sin problemas. Estos requerimientos variarán según el navegador que se use.

Para realizar todo el procedimiento es muy importante que desde la solicitud del certificado software hasta la descarga del mismo se haga cuidando estos puntos:

- Tiene que hacerse desde el mismo ordenador.
- Si el ordenador tiene más de un "usuario" creado el procedimiento tiene que hacerse en la misma "sesión de usuario".
- Solo se pueden utilizar los siguientes navegadores de internet:
  - Microsoft Internet Explorer.
  - Mozilla Firefox, a partir de su versión 35.
- Todo el procedimiento tiene que hacerse desde el mismo navegador de Internet.
- No se pueden hacer cambios en el ordenador que se está utilizando, cambios como formatearlo e instalar de nuevo el sistema operativo. Y también hay que evitar las actualizaciones del sistema.

Dependiendo del navegador que se vaya a utilizar para solicitar e instalar el certificado electrónico hay que seguir los siguientes pasos…

El procedimiento con Microsoft Internet Explorer

Con Internet Explorer es necesario descargar e instalar un configurador automático creado por la FNMT-RCM antes de solicitar y descargar el certificado electrónico. Para hacerlo hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado con DNIe"** desde este enlace:
  - https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"Configurador FNMT-RCM:"**,
  bajo el título **"Configuración del navegador para Sistemas Winddows"**.
- Descargamos el configurador. El archivo que se descargará tiene la extensión **".exe"**.
- Buscamos el archivo descargado **"Configurador_FNMT_RCM.exe"** y los ejecutamos.
  - Instalamos el configurador siguiendo los pasos del asistente de instalación.
- Una vez terminada la configuración automática de Internet Explorer ya estamos listos para la siguiente etapa: 2 "Solicitud con Certificado" …

El procedimiento con Mozilla Firefox

Antes poder solicitar e instalar el certificado electrónico de la FNMT-RCM en Firefox es necesario instalar dos cosas:

- Un complemento (addon) para firmar.
- Los certificados raíz de la FNMT-RCM.

Veamos con detalle cada uno de estos pasos…

Instalación del complemento para firmar

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado con DNIe"** desde este enlace:
  https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"complemento para firmar"**,
  bajo el título **"Navegadores soportados"**.
- Se abrirá en una pestaña nueva la página del complemento **"signTextJS"** en el sitio web de complementos de Mozilla Firefox.
- Hacemos clic en **"+ Agregar a Firefox"**.

- Una ventana emergente nos advertirá que se está intentando instalar el complemento de Firefox “signTexUS”.
- Hacemos clic en **“Instalar”**.
- Una ventana emergente te avisará que el complemento se instaló con éxito.
- Cerramos la pestaña.

Instalación de los certificados raíz

Los certificados raíz son certificados emitidos por una Autoridad de Certificación, en este caso la FNMT-RCM, que contienen la clave pública de dicha autoridad, necesaria para que se compruebe la autenticidad de los certificados emitidos por ella.

Para instalar los certificados raíz de la FNMT-RCM hay que seguir los siguientes pasos:

- Utilizaremos el procedimiento **“Obtener Certificado software”** para descargar los certificados raíz de la FNMT-RCM con mayor facilidad desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **“Consideraciones previas y configuración del navegador”**.
- De vuelta en la página de **“Consideraciones previas (paso 1)”** hacemos clic en el enlace **“Instalación de los certificados raíces”**, debajo del título **“Configuración para Mozilla Firefox 35 o superior”**.
- Se abrirá en una pestaña nueva la página **“Procedimiento de Obtención de Certificados”** con los enlaces de los certificados raíz de la FNMT-RCM que debemos instalar en el navegador. Hacemos clic sobre cada uno de los seis enlaces para instalarlos o, en su defecto, descargarlos para luego instalarlos:
  - **“Descarga AC Raíz FNMT-RCM”**.
  - **“Descarga certificado FNMT Clase 2 CA”**.
  - **“Descarga certificado AC FNMT Usuarios”**.
  - **“Descarga certificado AC Representación”**.
  - **“Descarga AC Administración Pública”**.
  - **“Descarga AC Componentes Informáticos”**.
- Con cada enlace realizaremos este procedimiento:
  - Hacemos clic en el enlace. Se abrirá una ventana emergente.

  Nota: si por error hacemos clic de nuevo en un enlace ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **“Aceptar”**.
  - En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **“Aceptar”**.

- Una vez terminada la instalación de los certificados raíz en Firefox ya estamos listos para la siguiente etapa: 2 “Solicitud con Certificado” …

Instalar un certificado descargado

Si los certificados raíz de la FNMT-RCM no se instalan automáticamente hay que descargarlos para posteriormente importarlos a Firefox.

Para instalar los certificados de forma manual hay que seguir los siguientes pasos:

- Descargamos los certificados. Los archivos que se descargarán tienen la extensión **“.cer”**.
- En Firefox hacemos clic en botón de **“Abrir menú”** y luego en **“Opciones”**.
- En las opciones hacemos clic en **“Avanzado”** y luego en **“Ver certificados”**.
- Se abrirá la ventana emergente del **“Administrador de certificados”**, hacemos clic en la pestaña **“Autoridades”**.
- Hacemos clic en **“Importar…”**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si por error cargamos un archivo ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **“Aceptar”**.

  - Hacemos clic en el botón **“Abrir”**.
- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **“Aceptar”**.
- Repite el procedimiento con los otros certificados.
- Una vez terminada la carga manual de los certificados raíz ya estamos listos para la siguiente etapa: 2 “Solicitud con Certificado” …

2 “Solicitud con Certificado”

Una vez que se tenga todo preparado según lo especificado en la etapa 1 “Consideraciones previas y configuración del navegador” se puede proceder a realizar la solicitud y posterior descarga del certificado electrónico.

> **IMPORTANTE**: Recuerda que al solicitar un certificado nuevo a la FNMT-RCM se anulará automáticamente cualquier otro certificado del mismo tipo que tengas.

Para comenzar la solicitud para obtener el certificado software hay que seguir los siguientes pasos:

- Conectamos el DNIe al lector de tarjetas.

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado con DNIe"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie
- Hacemos clic en **"Solicitud con Certificado"**.
- Se abrirá la ventana emergente **"Contraseña requerida"** que nos solicitará la contraseña para acceder al DNIe.
- Hacemos clic en **"Aceptar"**.
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente, en este caso solo con el DNIe.
- Hacemos clic en **"Aceptar"**.
- Una ventana emergente nos alertará sobre la importancia de contar con la configuración necesaria para el navegador antes de solicitar el certificado, según vimos en la etapa: 1 "Consideraciones previas y configuración del navegador".
- Hacemos clic en **"Aceptar"**.
- En la pantalla **"PASO 1: PROCESO DE GENERACIÓN DE CLAVES"** iniciaremos el proceso de creación de las claves públicas y privadas asociadas a nuestro certificado. Solo habrá que hacer una selección:
  - Si se solicita una longitud de clave seleccionamos la de grado alto.
- Al terminar hacemos clic en **"Pulse aquí para consultar y aceptar las condiciones de expedición del certificado"**. Esto desplegará las condiciones de expedición.
- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **"Acepto las condiciones de expedición"** para aceptarlas.
- Hacemos clic en **"Siguiente"**.
- En la ventana emergente **"Diálogo de selección de objeto"** seleccionaremos la opción **"Disp. software de seguridad"** en el menú desplegable.
- Hacemos clic en **"Aceptar"**.
- Una ventana emergente nos indicará que se está generando una clave privada.
- En la pantalla **"PASO 2: EMISIÓN DE CERTIFICADO FNMT DE PERSONA FÍSICA"** rellenaremos el formulario con los datos solicitados:

Nota: algunos campos ya estarán rellenados con los datos tomados del DNIe.
IMPORTANTE: los datos marcados con un asterisco (*****) son obligatorios.

  - **"PAÍS"**:
  - **"DIRECCIÓN"**:
  - **"CÓDIGO POSTAL"**:
  - **"LOCALIDAD"**:

  - **“PROVINCIA”**:
  - **“TELÉFONO”**:
  - **“CORREO ELECTRÓNICO”**:
    - **“CONFIRME SU CORREO ELECTRÓNICO”**:
  - Marcaremos la **casilla de selección** de **“Marque esta casilla si se desea incluir la dirección de correo electrónico en el certificado para poder cifrar y firmar emails”**.
- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **“Acepto las condiciones de expedición”** para aceptarlas.
- Hacemos clic en **“Aceptar”**.
- En la pantalla **“PASO 3: FIRMA ELECTRÓNICA DE LA SOLICITUD”** confirmaremos los datos que hemos dado en el formulario anterior.
- Si todo está correcto hacemos clic en **“Firmar”**.
  - Si hay algún error en los datos que hemos suministrado hacemos clic en **“Corregir datos”**.
- La ventana emergente de **“Test Signing Request”** (el texto de la ventana está en inglés) nos pedirá firmar electrónicamente el texto de solicitud **“Solicito la expedición del certificado emitido por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT - RCM)”** con los datos suministrados y la aceptación de las condiciones de uso.
  - Indicaremos nuestra contraseña del DNIe en el formulario de abajo.
  - Hacemos clic en **“OK”**.
- Enviarán un correo electrónico a la dirección que indicamos antes, desde la cuenta “ac.usuarios@fnmt.es” con el asunto **“Notificaciones FNMT AC Usuarios”**.

Nota: no escribas ni respondas a esta dirección.

- En el correo vendrá el **“código de solicitud”**, este código será requisito fundamental para los siguientes pasos.

> **IMPORTANTE**: Debes conservar este código, no borres el correo. Si el código se te pierde y no lo tienes apuntado tendrás que comenzar de nuevo el proceso.

- Con el código de solicitud ya estamos listos para la siguiente etapa: 3 “Descarga de su Certificado de Persona Física” …

3 “Descarga de su Certificado de Persona Física”

En esta última etapa se procede a descargar e instalar, en un mismo proceso, el certificado electrónico para persona física de la FNMT-RCM que se ha solicitado.

Para descargar el certificado hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado con DNIe"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-dnie
- Hacemos clic en **"Descarga de su Certificado de Persona Física"**.
- Rellenamos el formulario con la información solicitada:
  - **"N.º DEL DOCUMENTO DE IDENTIFICACIÓN"**.
  - **"PRIMER APELLIDO (tal y como aparece en su documento de identificación)"**.
  - **"CÓDIGO DE SOLICITUD"**: el código ya utilizado en los pasos anteriores.
- Al terminar hacemos clic en **"Pulse aquí para consultar y aceptar las condiciones de expedición del certificado"**. Esto desplegará las condiciones de expedición.
- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **"Acepto las condiciones de expedición"** para aceptarlas.

Nota: si deseas descargar una copia en formato PDF de las condiciones de expedición haz clic en **"Descargar condiciones"**.

- Hacemos clic en **"Descargar Certificado"** para iniciar la descarga e instalar el certificado.
- Una ventana emergente avisará que vamos a proceder a instalar el certificado y que desde ese momento adquirimos la condición de **"titular"** y que esto quedará registrado en los sistemas de referencia de la FNMT-RCM que hemos aceptado en las condiciones de uso del certificado. Hacemos clic en **"Aceptar"**.
- Si la descarga fue exitosa aparecerá el botón **"Instalar certificado"**. Hacemos clic en el botón.
- Una ventana emergente alertará que el certificado se instaló. Hacemos clic en **"Aceptar"**.

Nota: si se produce algún error en la instalación vuelve a la página anterior e inténtalo de nuevo.
IMPORTANTE: este mensaje también alerta que se debe hacer una copia de seguridad del certificado.

Nuestro certificado está listo para usar. Podemos verificar que está instalado siguiendo los pasos indicados en: "Certificado electrónico: cómo comprobar la instalación".

CERTIFICADO ELECTRÓNICO: CÓMO OBTENER EL CERTIFICADO CON ANDROID

A fecha de realización de esta guía, la FNMT ha retirado de forma temporal la obtención de certificados con Android, para realizar un mantenimiento de la aplicación (no hay fecha prevista para la nueva versión).

En cualquier caso, en el momento que sea operativo se pueden consultar los pasos de obtención en:

www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-con-android

CERTIFICADO ELECTRÓNICO: CÓMO COMPROBAR LA INSTALACIÓN

Una vez instalado el "Certificado FNMT-RCM de Persona Física o de Persona Jurídica" se puede hacer una comprobación en el almacén o administrador de certificados del navegador.

Nota: la guía está hecha en base al navegador Mozilla Firefox, pero el procedimiento es similar en la mayoría de los navegadores.

IMPORTANTE: Todos los pasos pueden variar ligeramente con sucesivas actualizaciones del navegador.

Para hacer una comprobación de la instalación del certificado en el administrador de certificados de Firefox hay que seguir los siguientes pasos:

- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad y Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Sus certificados"**.
- Bajo **"Nombre del certificado"** debe visualizarse el certificado **"FNMT-RCM"**.
  - Si queremos ver los detalles del certificado hacemos clic encima del certificado y luego en el botón **"Ver…"** y se abrirá una ventana con todos los detalles.

CERTIFICADO ELECTRÓNICO: CÓMO VERIFICAR EL ESTADO DEL CERTIFICADO

Una vez instalado el "Certificado FNMT-RCM de Persona Física" se puede hacer una verificación del estado del certificado y saber los datos que contiene, si está valido y su fecha de revocación. Para hacerlo se puede recurrir a dos formas:

- Desde el ordenador: "Verificación en el navegador: datos y caducidad".
- Desde Internet: "Verificación online: ver datos, validez y caducidad".

Veamos cada una…

Verificación en el navegador: datos y caducidad

Ver la fecha de caducidad de un certificado electrónico se hace desde el almacén de certificados del navegador. Se explicará el procedimiento para los navegadores:

- Mozilla Firefox.
- Microsoft Internet Explorer.
- Google Chrome.

Veamos en detalle el procedimiento para cada uno…

Ver caducidad en Firefox

Para ver la fecha de caducidad del certificado electrónico desde Firefox hay que seguir los siguientes pasos:

- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad y Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Sus certificados"**.
- Hacemos doble clic sobre el certificado **"FNMT-RCM"**, debajo de **"Nombre del certificado"**, para desplegar los detalles y luego hacemos clic en ellos para seleccionar el certificado.
- Debajo del campo **"Caduca el"** veremos la fecha de caducidad del certificado.
- Si deseamos ver más detalles sobre el certificado hacemos clic sobre los detalles del certificado y luego al botón **"Ver…"**.
- Se abrirá la ventana **"Visor de certificados"** con los detalles del certificado.

Ver caducidad en Internet Explorer

Para ver la fecha de caducidad del certificado electrónico desde Microsoft Internet Explorer hay que seguir los siguientes pasos:

- En Internet Explorer hacemos clic en botón de **"Herramientas"** y luego en **"Opciones de Internet"**.
- En las **"Opciones de Internet"** hacemos clic en la pestaña **"Contenido"** y luego en **"Certificados"**.
- Se abrirá la ventana emergente **"Certificados"**. Este es el "Almacén de Certificados" digitales de Windows, compartido por Internet Explorer y Chrome.
- En la pestaña **"Personal"** bajo el campo **"Fecha de expiración"** correspondiente a nuestro certificado veremos la fecha de caducidad del mismo.
- Si deseamos ver más detalles sobre el certificado hacemos clic sobre este y luego al botón **"Ver…"**.
- Se abrirá la ventana **"Certificado"** con todos sus detalles.

Ver caducidad en Chrome

Para ver la fecha de caducidad del certificado electrónico desde Google Chrome hay que seguir los siguientes pasos:

- En Chrome hacemos clic en el botón **"Personaliza y controla Google Chrome"** y luego en **"Configuración"**.

- Entramos en **"Mostrar opciones avanzadas"** En el apartado **"Privacidad y seguridad"** entramos en **"Gestionar Certificados"**.
- Hacemos clic en el título llamado **"Administrar configuración y certificados HTTPS/SSL"**
- Se abrirá la ventana emergente **"Certificados"**. Este es el "Almacén de Certificados" digitales de Windows, compartido por Internet Explorer y Chrome.
- Si deseamos ver más detalles sobre el certificado hacemos clic sobre este y luego al botón **"Ver…"**.
- Se abrirá la ventana **"Certificado"** con todos sus detalles.

Verificación online: ver datos, validez y caducidad

A través del servicio "Verificar estado" de la FNMT-RCM se pueden ver los datos del certificado electrónico, su fecha de validez y si está revocado o no.

Para utilizar el servicio hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Verificar estado"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado
- Hacemos clic en **"SOLICITAR VERIFICACIÓN"**.
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En la pantalla **"Solicitar verificación"** nos indicarán:
  - Si nuestro certificado es **"Válido y no revocado"** o "**No válido y revocado**".
  - La **"Información sobre la identidad (valores personales)"**.
  - La **"Información sobre las claves (valores técnicos)"**.

IMPORTANTE: te pedirán que verifiques los datos del certificado para asegurarte de que estos coincidan exactamente con los datos de tu DNI. Si son incorrectos deberás anular el certificado y solicitar uno nuevo, tal como se explica en las secciones:

"Certificado electrónico: cómo anularlo telemáticamente"

"Certificado electrónico: cómo obtener el certificado software"

"Certificado electrónico: cómo obtener el certificado con DNIe"

CERTIFICADO ELECTRÓNICO: CÓMO HACER UNA COPIA DE SEGURIDAD

Una vez instalado el "Certificado FNMT-RCM de Persona Física" se debe hacer una copia de seguridad del mismo desde el almacén o administrador de certificados del navegador.

Nota: la guía está hecha en base al navegador Mozilla Firefox, pero el procedimiento es similar en la mayoría de los navegadores.

Para hacer una copia de seguridad del certificado electrónico desde el administrador de certificados de Firefox hay que seguir los siguientes pasos:

- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad & Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Sus certificados"**.
- Hacemos doble clic sobre el certificado **"FNMT-RCM"**, debajo de **"Nombre del certificado"**, para desplegar los detalles y luego hacemos clic en ellos para seleccionar el certificado.
- Hacemos clic en el botón **"Hacer copia…"** (En Google Chrome y en Microsoft Internet Explorer se utiliza el botón **"Exportar")**
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde queremos almacenar la copia del certificado.
  - Ponemos un nombre a la copia de seguridad del certificado en la casilla **"Nombre"**.

  Nota: al usar Firefox la extensión del archivo será ".P12", que exporta los certificados electrónicos con clave privada. Si necesitas guardar la copia de tu certificado como un archivo ".PFX" haz lo siguiente:
    - En el campo **"Guardar como"** selecciona la opción **"Todos los archivos (*.*)"** en el menú desplegable, escribe el nombre del archivo y a continuación la extensión **".pfx"** (sin comillas).
  - Hacemos clic en el botón **"Guardar"**.
- Se abrirá una nueva ventana para establecer una contraseña de seguridad a la copia de seguridad del certificado. Escribe la contraseña en **"Contraseña de respaldo para el certificado"**.
  - En **"Contraseña de respaldo para el certificado (confirmar)"** repetimos la contraseña anterior de forma idéntica.
- Hacemos clic en **"Aceptar"**.
- Una ventana emergente avisará que la copia de seguridad del certificado se ha realizado con éxito. Hacemos clic en **"Aceptar"**.

- Ya tenemos una copia de seguridad para respaldar nuestro certificado electrónico en el ordenador o un dispositivo externo, ya sea en una memoria USB, un CD-ROM o en una tarjeta o USB criptográfico, o para usarlo en otros navegadores.

CERTIFICADO ELECTRÓNICO: CÓMO EXPORTAR LA CLAVE PÚBLICA

Una vez instalado el "Certificado FNMT-RCM" se puede exportar la clave pública del certificado desde el almacén o administrador de certificados del navegador.

Nota: la guía está hecha en base al navegador Mozilla Firefox, pero el procedimiento es similar en la mayoría de los navegadores.

Para exportar la clave pública del certificado electrónico desde el administrador de certificados de Firefox hay que seguir los siguientes pasos:

- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad & Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Sus certificados"**.
- Hacemos doble clic sobre el certificado **"FNMT-RCM"**, debajo de **"Nombre del certificado"**, para desplegar los detalles y luego hacemos clic en ellos para seleccionar el certificado.
- Hacemos clic en el botón **"Ver…"**.
- Se abrirá la ventana **"Visor de certificados"**. Hacemos clic en la pestaña **"Detalles"** en la parte superior.
- Hacemos clic en **"Exportar…"**.
- Se abrirá una ventana **"Guardar certificado en archivo"**. Selecciona la ubicación donde quieres almacenar la copia del certificado.
    - En la casilla **"Nombre"** ya estará puesto el nombre del certificado digital, si quieres puedes cambiarlo.

Nota: al usar Firefox la extensión del archivo para exporta la clave pública del certificado electrónico será ".CER", con su alternativa ".P7B". O escoge de la lista desplegable la extensión que necesites.

- Hacemos clic en el botón **"Guardar"**.
- Ya tenemos una copia de la clave pública para usar en aplicaciones externas.

CERTIFICADO ELECTRÓNICO: CÓMO USAR EL CERTIFICADO EN OTROS SITIOS

Una vez hecha la copia de seguridad del certificado electrónico completo o solo exportada la clave pública del mismo se pueden utilizar en otros navegadores o en otras aplicaciones. A continuación, ofrecemos algunas posibilidades.

Cómo importar el certificado electrónico

Una vez hecha una copia de seguridad del "Certificado FNMT-RCM" según lo visto en las guías de la sección "Certificado electrónico: cómo hacer una copia de seguridad" se puede utilizar para instalarla en otros navegadores, sea en el mismo dispositivo o en otro.

Importar una copia de seguridad del certificado electrónico se hace desde el almacén de certificados del navegador. Se explicará el procedimiento para los navegadores:

- Mozilla Firefox.
- Microsoft Internet Explorer.
- Google Chrome.

Veamos en detalle el procedimiento para cada navegador…

Importar el certificado a Firefox

Para importar un certificado digital a Mozilla Firefox hay que seguir los siguientes pasos:

- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad & Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Sus certificados"**.
- Hacemos doble clic sobre el certificado **"FNMT-RCM"**, debajo de **"Nombre del certificado"**, para desplegar los detalles y luego hacemos clic en ellos para seleccionar el certificado.
- Hacemos clic en el botón **"Importar…"**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado.
  - Hacemos clic en el botón **"Abrir"**.
- Nos pedirán la contraseña que pusimos a la copia de seguridad.
  - Hacemos clic en **"Aceptar"**.
- Una ventana emergente avisará que la copia de seguridad del certificado se ha restaurado satisfactoriamente.
  - Hacemos clic en **"Aceptar"**.
- Hacemos clic en **"Aceptar"** para cerrar el administrador de certificados.
- Nuestro certificado está listo para usar.

Importar el certificado a Internet Explorer

Para importar un certificado digital a Microsoft Internet Explorer hay que seguir los siguientes pasos:

- En Internet Explorer hacemos clic en botón de **"Herramientas"** y luego en **"Opciones de Internet"**.
- En las **"Opciones de Internet"** hacemos clic en la pestaña **"Contenido"** y luego en **"Certificados"**.
- Se abrirá la ventana emergente **"Certificados"**. Este es el "Almacén de Certificados" digitales de Windows, compartido por Internet Explorer y Chrome.
- En la pestaña **"Personal"** hacemos clic en **"Importar…"**.
- Se abrirá la ventana emergente **"Asistente para importar certificados"**, hacemos clic en **"Siguiente"**.

Nota: desde este asistente puedes importar certificados y listas de revocación de certificados. Se pueden importar desde otros almacenes de certificados, como el de Firefox, o desde una copia de seguridad almacenada en el ordenador o un dispositivo de almacenamiento externo.

- Buscamos el archivo a importar haciendo clic en **"Examinar…"**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si no ves la copia de seguridad de tu certificado electrónico tendrás que cambiar el tipo archivo haciendo clic en el menú desplegable de tipo de archivo y seleccionando el tipo que corresponda al formato de tu copia de seguridad, que para Firefox es ".pfx" y ".p12". Chrome selecciona de forma predeterminada el sistema de archivos ".cer" y ".crt".

- Hacemos clic en el botón **"Abrir"**.
- Hacemos clic en **"Siguiente"**.
- Nos pedirán la contraseña que pusimos a la copia de seguridad.

Nota: si te quieres asegurar de escribir bien la contraseña puedes hacer clic en la casilla de selección de **"Mostrar contraseña"** y así podrás ver qué escribes.

- Hay tres **"Opciones de importación"** para configurar el certificado y su uso, las marcaremos según nuestras necesidades haciendo clic en la **casilla de selección múltiple** de cada opción:
  Nota: si no tienes claras el uso y utilidad de cada opción opta por dejar las selecciones ya hechas de forma predeterminada.
  - **"Habilitar protección segura de clave privada"**: esta opción activa un aviso seguridad cada vez que la clave privada del certificado digital se va a utilizar. Opcional.

  - **“Marcar esta clave como exportable”**: esta opción permite poder exportar el certificado digital que se está importando. Opcional.
  - **“Incluir todas las propiedades extendidas”**: esta opción es necesaria para que funcione bien el certificado. Obligada.

- Hacemos clic en **“Siguiente”**.
- Se nos preguntará dónde preferimos almacenar nuestro certificado, la opción preseleccionada es **“Colocar todos los certificados en el siguiente almacén”** y como almacén de certificados está seleccionado el de **“Personal”**, que para nuestro caso es el más apropiado.
  - Si deseamos seleccionar otro de los almacenes hacemos clic en **“Examinar…”**, se abrirá una nueva ventana para seleccionar el almacén haciendo clic en él y luego en **“Aceptar”**.
  - Si prefieres que Internet Explorer haga la selección según considere sea el más adecuado marca la opción **“Seleccionar automáticamente el almacén de certificados según el tipo de certificado”** haciendo clic en la **casilla de selección simple**.
- Ya seleccionado el almacén de certificados hacemos clic en **“Siguiente”**.
- Esta última ventana nos hace un resumen de las selecciones hechas en el asistente. Si estamos conformes hacemos clic en **“Finalizar”**.
- Una ventana emergente nos confirmará que la importación se ha realizado con éxito, hacemos clic en **“Aceptar”**.
- El certificado aparecerá en la pestaña **“Personal”** de la ventana **“Certificados”**, bajo el campo **“Emitido para”** mostrará nuestro nombre y número del documento de identidad, tal como sucede en Firefox. Si queremos ver los detalles del certificado hacemos clic en el botón **“Ver”** o doble clic sobre el nombre del certificado.
  Nota: si en el **“Asistente para importar certificados”** seleccionaste la opción **“Habilitar protección segura de clave privada”** se abrirá la ventana **“Importación de una nueva clave privada de intercambio”** que advierte que una aplicación está creando un nuevo elemento protegido.
  - Aquí podemos crear un nivel extra de protección a la clave privada de nuestro certificado digital.
  - El nivel de seguridad predeterminado es el nivel **“medio”**, esto lo podemos cambiar haciendo clic en el botón **“Nivel de seguridad…”**.
  - Si seleccionamos el nivel **“Alto”** se abrirá una ventana nueva con un asistente que nos permitirá establecer una contraseña que nos pedirán cada vez que la clave privada vaya a ser utilizada.
  - Una vez establecido el nivel de seguridad que queramos, hacemos clic en **“Aceptar”**.
- Una ventana emergente nos confirmará que la importación se ha realizado con éxito, hacemos clic en **“Aceptar”**.

- Hacemos clic en **"Aceptar"** para cerrar el administrador de certificados.
- Nuestro certificado está listo para usar.

Importar el certificado a Chrome

Para importar un certificado digital a Google Chrome hay que seguir los siguientes pasos:

- En Chrome hacemos clic en el botón **"Personaliza y controla Google Chrome"** y luego en **"Configuración"**.
- Entramos en **"Mostrar opciones avanzadas"** En el apartado **"Privacidad y seguridad"** entramos en **"Gestionar Certificados"**.
- Hacemos clic en el título llamado **"Administrar configuración y certificados HTTPS/SSL"**
- Se abrirá la ventana emergente **"Certificados"**. Este es el "Almacén de Certificados" digitales de Windows, compartido por Internet Explorer y Chrome.
- Si deseamos ver más detalles sobre el certificado hacemos clic sobre este y luego al botón **"Ver…"**.
- Se abrirá la ventana **"Certificado"** con todos sus detalles.
- En la pestaña **"Personal"** hacemos clic en **"Importar…"**.
- Se abrirá la ventana emergente **"Asistente para importar certificados"**, hacemos clic en **"Siguiente"**.

Nota: desde este asistente puedes importar certificados y listas de revocación de certificados. Se pueden importar desde otros almacenes de certificados, como el de Firefox, o desde una copia de seguridad almacenada en el ordenador o un dispositivo de almacenamiento externo.

- Buscamos el archivo a importar haciendo clic en **"Examinar…"**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si no ves la copia de seguridad de tu certificado electrónico tendrás que cambiar el tipo archivo haciendo clic en el menú desplegable de tipo de archivo y seleccionando el tipo que corresponda al formato de tu copia de seguridad, que para Firefox es ".pfx" y ".p12". Chrome selecciona de forma predeterminada el sistema de archivos ".cer" y ".crt".

- Hacemos clic en el botón **"Abrir"**.
- Hacemos clic en **"Siguiente"**.
- Nos pedirán la contraseña que pusimos a la copia de seguridad.

Nota: si te quieres asegurar de escribir bien la contraseña puedes hacer clic en la casilla de selección de **"Mostrar contraseña"** y así podrás ver qué escribes.

- Hay tres **"Opciones de importación"** para configurar el certificado y su uso, las marcaremos según nuestras necesidades haciendo clic en la **casilla de selección múltiple** de cada opción:

Nota: si no tienes claras el uso y utilidad de cada opción opta por dejar las selecciones ya hechas de forma predeterminada.

  - **"Habilitar protección segura de clave privada"**: esta opción activa un aviso seguridad cada vez que la clave privada del certificado digital se va a utilizar. Opcional.
  - **"Marcar esta clave como exportable"**: esta opción permite poder exportar el certificado digital que se está importando. Opcional.
  - **"Incluir todas las propiedades extendidas"**: esta opción es necesaria para que funcione bien el certificado. Obligada.

- Hacemos clic en **"Siguiente"**.
- Se nos preguntará dónde preferimos almacenar nuestro certificado, la opción preseleccionada es **"Colocar todos los certificados en el siguiente almacén"** y como almacén de certificados está seleccionado el de **"Personal"**, que para nuestro caso es el más apropiado.
  - Si deseamos seleccionar otro de los almacenes hacemos clic en **"Examinar…"**, se abrirá una nueva ventana para seleccionar el almacén haciendo clic en él y luego en **"Aceptar"**.
  - Si prefieres que Chrome haga la selección según considere sea el más adecuado marca la opción **"Seleccionar automáticamente el almacén de certificados según el tipo de certificado"** haciendo clic en la **casilla de selección simple**.
- Ya seleccionado el almacén de certificados hacemos clic en **"Siguiente"**.
- Esta última ventana nos hace un resumen de las selecciones hechas en el asistente. Si estamos conformes hacemos clic en **"Finalizar"**.
- Una ventana emergente nos confirmará que la importación se ha realizado con éxito, hacemos clic en **"Aceptar"**.
- El certificado aparecerá en la pestaña **"Personal"** de la ventana **"Certificados"**, bajo el campo **"Emitido para"** mostrará nuestro nombre y número del documento de identidad, tal como sucede en Firefox. Si queremos ver los detalles del certificado hacemos clic en el botón **"Ver"** o doble clic sobre el nombre del certificado.

Nota: si en el **"Asistente para importar certificados"** seleccionaste la opción **"Habilitar protección segura de clave privada"** se abrirá la ventana **"Importación de una nueva clave privada de intercambio"** que advierte que una aplicación está creando un nuevo elemento protegido.

  - Aquí podemos crear un nivel extra de protección a la clave privada de nuestro certificado digital.

  - El nivel de seguridad predeterminado es el nivel **"medio"**, esto lo podemos cambiar haciendo clic en el botón **"Nivel de seguridad…"**.
  - Si seleccionamos el nivel **"Alto"** se abrirá una ventana nueva con un asistente que nos permitirá establecer una contraseña que nos pedirán cada vez que la clave privada vaya a ser utilizada.
  - Una vez establecido el nivel de seguridad que queramos, hacemos clic en **"Aceptar"**.
- Una ventana emergente nos confirmará que la importación se ha realizado con éxito, hacemos clic en **"Aceptar"**.
- Hacemos clic en **"Aceptar"** para cerrar el administrador de certificados.
- Nuestro certificado está listo para usar.

CERTIFICADO ELECTRÓNICO: CÓMO RENOVARLO TELEMÁTICAMENTE

Como ya se comentó en la sección "¿Cuánto dura un certificado electrónico?", del "Certificado de la Fábrica Nacional de Moneda y Timbre", el certificado se puede renovar telemáticamente antes de que caduque. Renovar el certificado electrónico tiene estas fases:

- **Preparación:** 1 "Consideraciones previas y configuración del navegador"
- **Solicitud de renovación:** 2 "Solicitar la renovación"
- **Instalación del certificado:** 3 "Descargar el certificado"

Nota: el procedimiento entero descrito en esta guía está hecho basándose en el navegador **Mozilla Firefox**.

Veamos paso a paso cada fase…

1 "Consideraciones previas y configuración del navegador"

Antes de solicitar la renovación y descargar el certificado en software es necesario que el ordenador y el navegador de Internet que se van a utilizar en el procedimiento cumplan ciertos requisitos para poder procesar la solicitud sin problemas. Estos requerimientos variarán según el navegador que se use.

Para realizar todo el procedimiento es muy importante que desde la solicitud del certificado software hasta la descarga del mismo se haga cuidando estos puntos:

- Tiene que hacerse desde el mismo ordenador.
- Si el ordenador tiene más de un "usuario" creado el procedimiento tiene que hacerse en la misma "sesión de usuario".
- Solo se pueden utilizar los siguientes navegadores de internet:
  - Microsoft Internet Explorer.
  - Mozilla Firefox, a partir de su versión 35.

- Todo el procedimiento tiene que hacerse desde el mismo navegador de Internet.
- No se pueden hacer cambios en el ordenador que se está utilizando, cambios como formatearlo e instalar de nuevo el sistema operativo. Y de preferencia hay que evitar las actualizaciones del sistema.

Nota: esta guía explica el procedimiento basándose en el sistema operativo Windows, en sus versiones 8 y 10. Más información sobre cómo hacer estos procedimientos en otros sistemas operativos (Mac y Linux) en la sede electrónica de la FNMT-RCM: www.sede.fnmt.gob.es.

Dependiendo del navegador que se vaya a utilizar para solicitar e instalar el certificado electrónico hay que seguir los siguientes pasos…

El procedimiento con Microsoft Internet Explorer

Con Internet Explorer es necesario descargar e instalar un configurador automático creado por la FNMT-RCM antes de solicitar y descargar el certificado electrónico. Para hacerlo hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Renovar Certificado"** desde este enlace:
  - https://www.sede.fnmt.gob.es/certificados/persona-fisica/renovar
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"Configurador FNMT-RCM"**,
  bajo el título **"Configuración para Internet Explorer"**.
- Descargamos el configurador. El archivo que se descargará tiene la extensión **".exe"**.
- Buscamos el archivo descargado **"Configurador_FNMT_RCM.exe"** y los ejecutamos.
  - Instalamos el configurador siguiendo los pasos del asistente de instalación.
- Una vez terminada la configuración automática de Internet Explorer ya estamos listos para la siguiente etapa: 2 "Solicitar la renovación" …

El procedimiento con Mozilla Firefox

Antes poder solicitar e instalar el certificado electrónico de la FNMT-RCM en Firefox es necesario instalar dos cosas:

- Un complemento (addon) para firmar.

Nota: los complementos o addons (también llamados extensiones o plugins en otros programas) son pequeños añadidos de software que se instalan, en nuestro caso, a un navegador para aumentar o mejorar sus funcionalidades.

- Los certificados raíz de la FNMT-RCM.

Veamos con detalle cada uno de estos pasos…

Instalación del complemento para firmar

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Renovar Certificado"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/renovar
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"complemento para firmar"**, bajo el título **"Configuración para Mozilla Firefox 35 o superior"**.
- Se abrirá en una pestaña nueva la página del complemento **"signTextJS"** en el sitio web de complementos de Mozilla Firefox.
- Hacemos clic en **"+ Agregar a Firefox"**.
- Una ventana emergente nos advertirá que se está intentando instalar el complemento de Firefox "signTexUS".
- Hacemos clic en **"Instalar"**.
- Una ventana emergente te avisará que el complemento se instaló con éxito.
- Cerramos la pestaña.

Instalación de los certificados raíz

Los certificados raíz son certificados emitidos por una Autoridad de Certificación, en este caso la FNMT-RCM, que contienen la clave pública de dicha autoridad, necesaria para que se compruebe la autenticidad de los certificados emitidos por ella.

Para instalar los certificados raíz de la FNMT-RCM hay que seguir los siguientes pasos:

- De vuelta en la página de **"Consideraciones previas (paso 1)"** hacemos clic en el enlace **"Instalación de los certificados raíces"**, debajo del título **"Configuración para Mozilla Firefox 35 o superior"**.
- Se abrirá en una pestaña nueva la página **"Procedimiento de Obtención de Certificados"** con los enlaces de los certificados raíz de la FNMT-RCM que debemos instalar en el navegador. Hacemos clic sobre cada uno de los seis enlaces para instalarlos o, en su defecto, descargarlos para luego instalarlos:
  - **"Descarga AC Raíz FNMT-RCM"**.
  - **"Descarga certificado FNMT Clase 2 CA"**.
  - **"Descarga certificado AC FNMT Usuarios"**.
  - **"Descarga certificado AC Representación"**.
  - **"Descarga AC Administración Pública"**.
  - **"Descarga AC Componentes Informáticos"**.
- Con cada enlace realizaremos este procedimiento:

- Hacemos clic en el enlace. Se abrirá una ventana emergente.

Nota: si por error hacemos clic de nuevo en un enlace ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **"Aceptar"**.

- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **"Aceptar"**.

Una vez terminada la instalación de los certificados raíz en Firefox ya estamos listos para la siguiente etapa: 2 "Solicitar la renovación" …

Instalar un certificado descargado

Si los certificados raíz de la FNMT-RCM no se instalan automáticamente hay que descargarlos para posteriormente importarlos a Firefox.

Para instalar los certificados de forma manual hay que seguir los siguientes pasos:

- Descargamos los certificados. Los archivos que se descargarán tienen la extensión **".cer"**.
- En Firefox hacemos clic en botón de **"Abrir menú"** y luego en **"Opciones"**.
- En las opciones hacemos clic en **"Privacidad & Seguridad"** y luego en **"Ver certificados"**.
- Se abrirá la ventana emergente del **"Administrador de certificados"**, hacemos clic en la pestaña **"Autoridades"**.
- Hacemos clic en **"Importar…"**.
- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si por error cargamos un archivo ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **"Aceptar"**.

- Hacemos clic en el botón **"Abrir"**.
- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **"Aceptar"**.
- Repite el procedimiento con los otros certificados.
- Una vez terminada la carga manual de los certificados raíz ya estamos listos para la siguiente etapa: 2 "Solicitar la renovación"…

2 “Solicitar la renovación"

Una vez que nos hemos asegurado de cumplir con los requisitos previos procedemos para solicitar la renovación:

Accedemos a la página **“SEDE de la Fábrica Nacional de Moneda y Timbre”** en el apartado **“Renovar Certificado”** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/renovar

- Hacemos clic en **“Solicitar la renovación”**.
- Se abrirá la ventana emergente **“Petición de identificación de usuario”** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **“Elija un certificado para presentarlo como identificación”**.
- Hacemos clic en **“Aceptar”**.
- Una ventana emergente nos alertará sobre la importancia de contar con la configuración necesaria para el navegador antes de solicitar el certificado, según vimos en la etapa: 1 “Consideraciones previas y configuración del navegador”.
- Hacemos clic en **“Aceptar”**.
- Nos aparecerá una pantalla con nuestros datos personales a confirmar, una vez verificados pulsamos **“Continuar”**.
- Enviarán un correo electrónico a la dirección que indicamos antes, desde la cuenta “ac.usuarios@fnmt.es” con el asunto **“Notificaciones FNMT AC Usuarios”**.
- En el correo vendrá el **“código de solicitud”**, este código será requisito fundamental para los siguientes pasos.

> **IMPORTANTE**: Debes conservar este código, no borres el correo. Si el código se te pierde y no lo tienes apuntado tendrás que comenzar de nuevo el proceso.

- Con el código de solicitud ya estamos listos para la siguiente etapa: 3 “Descargar el certificado” …

3 “Descargar el certificado”

En esta última etapa se procede a descargar e instalar, en un mismo proceso, el certificado electrónico para persona física de la FNMT-RCM que se ha renovado.

Para descargar el certificado hay que seguir los siguientes pasos:

- Accedemos a la página **“SEDE de la Fábrica Nacional de Moneda y Timbre”** en el apartado **“Obtener Certificado con DNIe”** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/renovar
- Hacemos clic en **“Descarga el certificado”**.
- Rellenamos el formulario con la información solicitada:

  - **“N.º DEL DOCUMENTO DE IDENTIFICACIÓN”**.
  - **“PRIMER APELLIDO (tal y como aparece en su documento de identificación)”**.
  - **“CÓDIGO DE SOLICITUD”**: el código ya utilizado en los pasos anteriores.
- Al terminar hacemos clic en **“Pulse aquí para consultar y aceptar las condiciones de expedición del certificado”**. Esto desplegará las condiciones de expedición.
- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **“Acepto las condiciones de expedición”** para aceptarlas.
  Nota: si deseas descargar una copia en formato PDF de las condiciones de expedición haz clic en **“Descargar condiciones”**.
- Hacemos clic en **“Descargar Certificado”** para iniciar la descarga e instalar el certificado.
- Una ventana emergente avisará que vamos a proceder a instalar el certificado y que desde ese momento adquirimos la condición de **“titular”** y que esto quedará registrado en los sistemas de referencia de la FNMT-RCM que hemos aceptado en las condiciones de uso del certificado. Hacemos clic en **“Aceptar”**.
- Si la descarga fue exitosa aparecerá el botón **“Instalar certificado”**. Hacemos clic en el botón.
- Una ventana emergente alertará que el certificado se instaló. Hacemos clic en **“Aceptar”**.

Nota: si se produce algún error en la instalación vuelve a la página anterior e inténtalo de nuevo.

Nuestro certificado está listo para usar. Podemos verificar que está instalado siguiendo los pasos indicados en: “Certificado electrónico: cómo comprobar la instalación”.

CERTIFICADO ELECTRÓNICO: CÓMO ANULARLO TELEMÁTICAMENTE

Como ya se comentó en la sección "Anular un certificado", del "Certificado de la Fábrica Nacional de Moneda y Timbre", el certificado se puede anular telemáticamente antes de que caduque. Anular el certificado electrónico tiene estas fases:

- **Preparación:** 1 "Consideraciones previas y configuración del navegador"
- **Solicitud de revocación:** 2 "Anulación online"

IMPORTANTE: Este procedimiento solo se puede realizar con los navegadores permitidos, Internet Explorer y Mozilla Firefox.

Nota: el procedimiento entero descrito en esta guía está hecho basándose en el navegador **Mozilla Firefox**. Un navegador gratuito, de código libre y disponible para la gran mayoría de sistemas operativos para ordenadores y dispositivos móviles.

Veamos paso a paso cada fase…

1 "Consideraciones previas y configuración del navegador"

Antes de solicitar y descargar el certificado en software es necesario que el ordenador y el navegador de Internet que se van a utilizar en el procedimiento cumplan ciertos requisitos para poder procesar la solicitud sin problemas. Estos requerimientos variarán según el navegador que se use.

Nota: esta guía explica el procedimiento basándose en el sistema operativo Windows, en sus versiones 7, 8 y 10. Más información sobre cómo hacer estos procedimientos en otros sistemas operativos (Mac y Linux) en la sede electrónica de la FNMT-RCM: www.sede.fnmt.gob.es.

Dependiendo del navegador que se vaya a utilizar para solicitar e instalar el certificado electrónico hay que seguir los siguientes pasos…

El procedimiento con Microsoft Internet Explorer

Con Internet Explorer es necesario descargar e instalar un configurador automático creado por la FNMT-RCM antes de solicitar y descargar el certificado electrónico. Para hacerlo hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace:
  - https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de "Consideraciones previas (paso 1)" hacemos clic en **"Configurador FNMT-RCM"**,
  bajo el título **"Configuración para Internet Explorer"**.
- Descargamos el configurador. El archivo que se descargará tiene la extensión **".exe"**.

- Buscamos el archivo descargado **"Configurador_FNMT_RCM.exe"** y los ejecutamos.
  - Instalamos el configurador siguiendo los pasos del asistente de instalación.
- Una vez terminada la configuración automática de Internet Explorer ya estamos listos para la siguiente etapa: 2 "Anulación online" …

El procedimiento con Mozilla Firefox

Antes poder solicitar e instalar el certificado electrónico de la FNMT-RCM en Firefox es necesario instalar dos cosas:

- Un complemento (addon) para firmar.

Nota: los complementos o addons (también llamados extensiones o plugins en otros programas) son pequeños añadidos de software que se instalan, en nuestro caso, a un navegador para aumentar o mejorar sus funcionalidades.

- Los certificados raíz de la FNMT-RCM.

Veamos con detalle cada uno de estos pasos…

Instalación del complemento para firmar

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Obtener Certificado software"** desde este enlace:
  - https://www.sede.fnmt.gob.es/certificados/persona-fisica/obtener-certificado-software
- Hacemos clic en **"Consideraciones previas y configuración del navegador"**.
- En la página de **"Consideraciones previas (paso 1)"** hacemos clic en **"complemento para firmar"**,
  bajo el título **"Configuración para Mozilla Firefox 35 o superior"**.
- Se abrirá en una pestaña nueva la página del complemento **"signTextJS"** en el sitio web de complementos de Mozilla Firefox.
- Hacemos clic en **"+ Agregar a Firefox"**.
- Una ventana emergente nos advertirá que se está intentando instalar el complemento de Firefox "signTexUS".
- Hacemos clic en **"Instalar"**.
- Una ventana emergente te avisará que el complemento se instaló con éxito.
- Cerramos la pestaña.

Instalación de los certificados raíz

Los certificados raíz son certificados emitidos por una Autoridad de Certificación, en este caso la FNMT-RCM, que contienen la clave pública de dicha autoridad, necesaria para que se compruebe la autenticidad de los certificados emitidos por ella.

Para instalar los certificados raíz de la FNMT-RCM hay que seguir los siguientes pasos:

- De vuelta en la página de **“Consideraciones previas (paso 1)”** hacemos clic en el enlace **“Instalación de los certificados raíces”**, debajo del título **“Configuración para Mozilla Firefox 35 o superior”**.
- Se abrirá en una pestaña nueva la página **“Procedimiento de Obtención de Certificados”** con los enlaces de los certificados raíz de la FNMT-RCM que debemos instalar en el navegador. Hacemos clic sobre cada uno de los seis enlaces para instalarlos o, en su defecto, descargarlos para luego instalarlos:
  - **“Descarga AC Raíz FNMT-RCM”**.
  - **“Descarga certificado FNMT Clase 2 CA”**.
  - **“Descarga certificado AC FNMT Usuarios”**.
  - **“Descarga certificado AC Representación”**.
  - **“Descarga AC Administración Pública”**.
  - **“Descarga AC Componentes Informáticos”**.
- Con cada enlace realizaremos este procedimiento:
  - Hacemos clic en el enlace. Se abrirá una ventana emergente.

Nota: si por error hacemos clic de nuevo en un enlace ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **“Aceptar”**.

  - En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **“Aceptar”**.
- Una vez terminada la instalación de los certificados raíz en Firefox ya estamos listos para la siguiente etapa: 2 “Anulación online”…

Instalar un certificado descargado

Si los certificados raíz de la FNMT-RCM no se instalan automáticamente hay que descargarlos para posteriormente importarlos a Firefox.

Para instalar los certificados de forma manual hay que seguir los siguientes pasos:

- Descargamos los certificados. Los archivos que se descargarán tienen la extensión **“.cer”**.
- En Firefox hacemos clic en botón de **“Abrir menú”** y luego en **“Opciones”**.
- En las opciones hacemos clic en **“Avanzado”** y luego en **“Ver certificados”**.
- Se abrirá la ventana emergente del **“Administrador de certificados”**, hacemos clic en la pestaña **“Autoridades”**.
- Hacemos clic en **“Importar…”**.

- Se abrirá la ventana emergente del explorador de archivos de Windows. Seleccionamos la ubicación donde está almacenada la copia del certificado y hacemos clic en el certificado.

Nota: si por error cargamos un archivo ya usado saldrá una ventana emergente advirtiendo que ese certificado ya está instalado como una autoridad certificadora. Hacemos clic en **"Aceptar"**.

  - Hacemos clic en el botón **"Abrir"**.

- En la ventana emergente hacemos clic en las tres **casillas de selección múltiple** y luego en **"Aceptar"**.

- Repite el procedimiento con los otros certificados.

- Una vez terminada la carga manual de los certificados raíz ya estamos listos para la siguiente etapa: 2 "Anulación online"…

2 "Anulación online"

Para comenzar el proceso de revocación hay que seguir los siguientes pasos:

- Accedemos a la página **"SEDE de la Fábrica Nacional de Moneda y Timbre"** en el apartado **"Anular o revocar Certificado"** desde este enlace: https://www.sede.fnmt.gob.es/certificados/persona-fisica/anular

- Bajo el título **"Procedimiento"** hacemos clic en **"Anulación online"**.

- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.

- Hacemos clic en **"Aceptar"**.

- Se mostrará un formulario en el cual parte de los campos ya están rellenados por los datos del certificado electrónico. Rellenamos el resto de ellos con la información que solicitan. Los campos marcados con asteriscos (*) son obligatorios, el resto se pueden dejar vacíos si así lo queremos.

- En el campo **"CAUSA DE LA REVOCACIÓN*:"** tenemos que seleccionar una causa en el menú desplegable. Como causas de revocación tenemos:

  - **"Error en los datos personales"**.

  - **"Claves de acceso comprometidas"**.

  - **"Otros"**.

- Al terminar hacemos clic en **"Pulse aquí para consultar y aceptar las condiciones de expedición del certificado"** para desplegar las condiciones de expedición.

- Bajamos hasta el final de la página y hacemos clic en la **casilla de verificación** de **"Acepto las condiciones de revocación"** para aceptarlas.

- Hacemos clic en **“Aceptar”**.
- En la pantalla **“FIRMA ELECTRÓNICA DE SU SOLICITUD DE REVOCACIÓN”** confirmaremos los datos que hemos dado en el formulario anterior.
- Si todo está correcto hacemos clic en **“Firmar”**.
    - Si hay algún error en los datos que hemos suministrado hacemos clic en **“Corregir datos”**.
- La ventana emergente de **“Test Signing Request”** (el texto de la ventana está en inglés) nos pedirá firmar electrónicamente el texto de solicitud **“Solicito la revocación del certificado emitido por la Fábrica Nacional de Moneda y Timbre - Real Casa de la Moneda (FNMT - RCM)”** con los datos suministrados y la aceptación de las condiciones de uso.
    - Indicaremos la contraseña de nuestro certificado digital en el formulario de abajo.
    - Hacemos clic en **“OK”**.

Una ventana emergente alertará que el certificado se anuló. Hacemos clic en **“Aceptar”**.


Capacitación entre iguales.
Me
2.0
@dministro
Me
2.0
@dministro

CL@VE, IDENTIDAD ELECTRÓNICA PARA LAS ADMINISTRACIONES

El **sistema Cl@ve** (Clave) es una plataforma única de **identificación, autentificación y firma electrónica** para utilizar los trámite telemáticos o electrónicos de la Administración General del Estado, cuya principal novedad está en la posibilidad de realizar firmas electrónicas. Esto es posible gracias a la utilización de certificados electrónicos almacenados y custodiados en servidores remotos de la Administración Pública, en lo que comúnmente se denomina: la **nube**.

Cl@ve está pensado para facilitar la interacción entre la ciudadanía y los servicios públicos de la **Administración Electrónica** (**e-Administración**).

En Cl@ve se integrarán, paulatinamente, todos los diferentes órganos y organismos de la Administración General del Estado y sus carteras de servicios y trámites electrónicos. Así también, Cl@ve se irá incorporando y siendo compatible con los sistemas de reconocimiento e identificación transfronterizos presentes en la Unión Europea.

Nota: el Sistema Cl@ve tiene su página oficial en la dirección. www.clave.gob.es

¿CÓMO FUNCIONA?

Al darse de alta como usuario en el sistema Cl@ve este permite identificarse y utilizar los trámites telemáticos de la Administración General del Estado integrados en el sistema desde cualquier ordenador o dispositivo móvil conectado a Internet. Para hacer esto el sistema Cl@ve cuenta con dos modos de uso:

- **Cl@ve ocasional (Cl@ve PIN)**: un sistema de contraseñas temporales, pensada para los usuarios que usan de vez en cuando estos servicios electrónicos.
- **Cl@ve permanente**: un sistema de contraseña permanente, con seguridad reforzada si el tipo de trámite lo requiere. Con esta modalidad se puede acceder a la opción de firmar documentos digitales desde la nube.

Al ser una plataforma de identificación común para todos los servicios electrónicos integrados en el sistema, en cuanto se abre una sesión desde cualquiera de ellos ya se puede acceder a los demás sin tener que identificarse de forma individual en cada uno, a tantos de estos servicios como se necesite mientras que la sesión no se cierre o caduque, ya sea con la modalidad Cl@ve PIN o con Cl@ve Permanente.

Darse de alta en el Sistema Cl@ve para empezar a utilizar cualquiera de estas modalidades se puede hacer de forma telemática o presencial.

¿QUÉ VENTAJAS TIENE CL@VE?

El objetivo principal de Cl@ve es simplificar a la ciudadanía el uso de la e-Administración de la Administración General del Estado. Esto se logra a través del uso de clave de acceso concertadas y aceptadas entre todas las administraciones, es decir, un solo código o contraseña para identifícate en todas ellas de una sola vez, sin tener que recordar claves diferentes.

Y con la utilización de certificados electrónicos en la nube se elimina la necesidad de tener que hacer ningún tipo de instalación ni configuración de componentes de hardware o software en el ordenador o dispositivo móvil desde el que se quiera realizar un trámite telemático, pudiendo realizarlo desde cualquier equipo que disponga de conexión a Internet.

Los certificados electrónicos centralizados de Cl@ve ofrecen las mismas posibilidades y funcionalidades que ofrecen los del "Documento Nacional de Identidad Electrónico" o los del "Certificado de la Fábrica Nacional de Moneda y Timbre".

A estas ventajas para los usuarios de facilidad de uso y comodidad se suman las garantías de seguridad dadas por los organismos y cuerpos de seguridad de la Administración General del Estado involucrados en el sistema.

Y para las administraciones públicas tiene la gran ventaja de poder contar con una plataforma unificada que les evita tener que implementar y gestionar de forma individual sus propios sistemas de identificación, autentificación y firma electrónica para las gestiones y servicios electrónicos que ofrecen.

Cada vez hay más administraciones públicas que lo utilizan, se pueden consultar en el link http://www.clave.gob.es/clave_Home/clave/usabilidad.html

¿Qué desventajas tiene?

Las ventajas de Cl@ve son evidentes, pero aún presenta algunas barreras, entre ellas tenemos:

- Para registrarse en el sistema y acceder a todas sus características es necesario desplazarse en persona para que acrediten la identidad si no se cuenta con algún sistema de identificación electrónica como el DNIe o el certificado digital.
- Su utilización inicial puede ser difícil de entender.
- No está implantado de forma general en los trámites telemáticos de la Administración General del Estado. El sistema Cl@ve fue implantado a finales de año 2014, desde entonces el número de servicios electrónicos que lo utiliza crece poco a poco.
- Por los momentos no se usa en trámites telemáticos de las administraciones públicas autonómicas o municipales.

En esta guía aclararemos las dudas que presenta el proceso de registro en el sistema Cl@ve y su uso.

¿CÓMO DARSE DE ALTA EN EL SISTEMA CL@VE?

Para registrarse en el sistema Cl@ve es necesario que se valide la identidad del solicitante, esto puede hacerse de forma telemática o presencial. Según la forma de validación de la identidad los modos de darse de alta en Cl@ve son los siguientes:

- "A través de Internet: con DNIe o Certificado Digital".
- "A través de Internet: Sin Certificado Digital, con carta de invitación".
- "Presencial: en una oficina de registro".

IMPORTANTE: Al realizar el alta en el sistema Cl@ve se genera (en formato PDF) o entrega impresa (si el alta es presencial) un documento de justificante de alta en el sistema Cl@ve que además contendrá el **código de activación** para poder activar la Cl@ve Permanente.

Una vez registrado en Cl@ve se puede empezar a utilizar la "Cl@ve PIN" inmediatamente. Para utilizar la "Cl@ve Permanente" habrá que crear la contraseña necesaria para este modo de identificación con un código de activación generado en el proceso de alta.

Veamos primero en que consiste cada modo de alta en el sistema Cl@ve…

A través de Internet: Con DNIe o Certificado Digital

El registro online en el sistema Cl@ve utilizando el DNIe/3.0 o certificado electrónico es sencillo, inmediato y totalmente telemático.

Desde la sede electrónica de la Agencia Tributaria se comienza el proceso de registro, validando la identidad con el sistema de identificación digital que se disponga. Una vez validada la identidad el alta será efectiva de forma inmediata.

Nota: para saber sobre estas formas de identificación digital mira las secciones "Documento Nacional de Identidad Electrónico" y "Certificado electrónico o digital".

A través de Internet: Con carta de invitación

De no contar con la posibilidad de hacer el alta en el sistema Cl@ve por medio del DNIe/3.0 o el Certificado FNMT de Persona Física se puede hacer telemáticamente solicitando una carta de invitación a Cl@ve desde la sede electrónica de la Agencia Tributaria. La carta, que a llegará la dirección fiscal de quien solicita el alta, con un **Código Seguro de Verificación** (**CSV**) que se utiliza en la sede electrónica de la Agencia Tributaria para hacer el registro.

Solo se podrá solicitar la carta de invitación si previamente se ha indicado un número de cuenta bancaria a la Agencia Tributaria de la cual el solicitante sea titular, como puede ser haber hecho la declaración del IRPF, y tener establecido un domicilio fiscal ya que estos serán necesarios como datos de identificación de la persona que solicita el alta y para el envío de la carta.

Para utilizar determinados servicios electrónicos o hacer uso de la "Cl@ve Firma" se exige un nivel de seguridad que no proporciona el registro en el sistema Cl@ve por carta de invitación, por lo cual no podrás utilizarlos ya que tu identidad estaría validada de forma inequívoca. Esto no sucede si el alta se hace con DNIe/3.0 o con certificado electrónico o de forma presencial. Cuando esto pueda suceder te lo informarán adecuadamente.

Presencial: en una oficina de registro

Por último, se puede hacer el alta de forma presencial en una de las Oficinas de Registro de Cl@ve y validar allí la identidad en persona. Actualmente funcionan como Oficinas de Registro la red de Oficinas de la Agencia Estatal de Administración Tributaria y otros organismos estatales.

Nota: para saber dónde localizar las oficinas de registro de Cl@ve visita:

http://clave.gob.es/clave_Home/registro/Como-puedo-registrarme.html

A grandes rasgos podemos indicar que, para darse de alta de forma presencial es necesario:

- Pedir cita en la Oficina de Registro donde queramos acudir.
- Tener DNI o NIE, que no esté caducado, y los ciudadanos extranjeros con el pasaporte.
- Un número de teléfono móvil, cuyo número pertenezca a una operadora de telefonía que preste servicios en España.
- Un correo electrónico.

Cl@ve PIN

Con **Cl@ve PIN**, también conocido como **Cl@ve ocasional**, se generan de forma aleatoria un PIN o contraseña con un tiempo de validez muy limitado y de **"un solo uso"** que se envían al teléfono móvil que se indique durante el proceso de alta mediante un **mensaje de texto** o **SMS**. El PIN es un sencillo código de tres caracteres alfanuméricos (letras y/o números) fácil de recordar.

> **IMPORTANTE**: No pueden pasar más de 10 minutos entre que generas el PIN y lo utilizas porque caducará y tendrás que solicitar uno nuevo.

Una vez que se ha utilizado el Cl@ve PIN para identificarse en el sistema Cl@ve se pueden realizar todas las gestiones que se necesiten, y en cualquier trámite telemático que esté integrado en el sistema, sin que sea necesario identificarse de nuevo, dentro del tiempo de validez del PIN, llamada **"sesión de trabajo"**, que estará activa mientras no se cierre el navegador o se esté inactivo durante más de 60 minutos.

Una vez caducada la Cl@ve PIN hay que generar un PIN nuevo. El PIN se puede renovar tantas veces como se necesite, aunque no haya caducado.

¿Cómo obtener y usar el PIN?

Cada vez que se vaya a utilizar el sistema Cl@ve hay que generar un PIN en Cl@ve PIN. Para generar el PIN se puede hacer de dos formas:

- Online desde la web de la Agencia Tributaria.
- Desde un dispositivo móvil con la Veamos con más detalle la aplicación "Cl@ve PIN" …

Generar un PIN con la aplicación "Cl@ve PIN"

Para facilitar el proceso de obtener un PIN está disponible la **aplicación para smartphones Cl@ve PIN**, para dispositivos Android e IOs, que permite generar contraseñas con suma facilidad.

Para Android: https://play.google.com/store/apps/details?id=es.aeat.pin24h&hl=es

Para IOs https://itunes.apple.com/es/app/cl-ve-pin/id842624380?mt=8

IMPORTANTE: La aplicación Cl@ve PIN solo funcionará con el número telefónico que hayas indicado en el proceso de alta en el sistema Cl@ve y que ha quedado registrado en la Agencia Tributaria.

Al instalar la aplicación se realizará una confirmación de seguridad de la identidad del usuario para poder activarla, es decir, se comprobará que es el número de teléfono utilizado para instalar la aplicación es el mismo que está registrado en los datos del alta en el sistema Cl@ve. Esta activación se tendrá que hacer de nuevo si se instala de nuevo la aplicación.

Una vez activada la aplicación se podrá generar la Cl@ve PIN de forma sencilla y, según como se tenga configurado el móvil, sin tener que introducir ningún dato de confirmación o seguridad.

¿Cómo se usa el PIN?

Utilizar Cl@ve PIN es muy sencillo. Al acceder a un trámite telemático de la Administración General del Estado, que esté integrado en el sistema Cl@ve, ofrecerá una opción para identificarse utilizando Cl@ve PIN o Cl@ve Permanente según sea el caso.

Se selecciona la opción disponible para el sistema Cl@ve y en el caso de Cl@ve PIN se hacen dos pasos:

- Generar un código con cualquiera de los métodos mencionados con anterioridad.
- Utilizar el PIN generado para acceder al servicio electrónico y el número de DNI/NIE del usuario.

Hay que recordar que la Cl@ve PIN generada al ser de “un solo uso” (OTP) solo se puede utilizarla en una sesión, que una vez acabada o cerrada habrá que generar un PIN nuevo.

CL@VE PERMANENTE

Cl@ve Permanente ofrece un sistema de identificación y autenticación por contraseña que, si el nivel de seguridad del trámite telemático lo requiere, cuenta además con un nivel de verificación adicional a través de claves OTP vía SMS. Pensado para aquellos usuarios que tienen que hacer un uso más habitual de los servicios telemáticos de la Administración Pública.

Nota: la activación de Cl@ve Permanente permite acceder a la realización de firmas electrónicas en la nube con Cl@ve Firma.

¿Cómo activar la Cl@ve permanente?

Para activar el usuario en Cl@ve Permanente y crear la contraseña se necesita el **código de activación** generado en el documento del justificante de alta en el sistema Cl@ve.

IMPORTANTE: El código de activación también te servirá para recuperar o gestionar la contraseña, cambiar datos o darte de baja en Cl@ve Permanente.

Desde el portal del sistema Cl@ve (www.clave.gob.es) se accede al servicio de activación del usuario de Cl@ve Permanente. Se rellena el formulario de activación y la confirmaremos con un código OTP para poder crear la contraseña que se va a utilizar junto con el número de DNI/NIE del usuario para identificarse con Cl@ve Permanente.

¿Cómo usar Cl@ve Permanente?

Utilizar Cl@ve Permanente es muy sencillo. Al acceder a un trámite telemático de la Administración General del Estado, que esté integrado en el sistema Cl@ve, ofrecerá una opción para identificarse utilizando Cl@ve PIN o Cl@ve Permanente según sea el caso.

Se selecciona la opción disponible para el sistema Cl@ve y en el caso de Cl@ve Permanente se rellena el formulario indicando el DNI/NIE del usuario y la contraseña creada para Cl@ve Permanente.

¿Cómo gestionar la contraseña de Cl@ve Permanente?

Si es necesario cambiar la contraseña por seguridad, por haberla perdido, olvidado o por bloqueado al hacer varios intentos fallidos de identificación de forma consecutiva, se puede hacer, según sea el caso, utilizando el certificado digital o con la propia contraseña de Cl@ve Permanente.

Desde el portal del sistema Cl@ve (www.clave.gob.es) se accede al servicio de gestión de la contraseña de Cl@ve Permanente.

Nota: la contraseña de Cl@ve Permanente caduca a los 2 años, aunque por seguridad es recomendable cambiar de contraseña de forma regular.

¿Se puede desactivar el usuario de Cl@ve Permanente?

Si por alguna circunstancia es necesario dar de baja la Cl@ve Permanente se puede hacer en cualquier momento utilizando el certificado digital o con la contraseña de Cl@ve Permanente.

Desde el portal del sistema Cl@ve (www.clave.gob.es) se accede al servicio de desactivación de Cl@ve Permanente.

CL@VE FIRMA

Completando las funciones de identificación y autentificación del sistema Cl@ve, está la de poder realizar firmas de documentos electrónicos en aquellos trámites telemáticos de la Administración General del Estado que así lo requieran. Que como ya se comentó es la principal novedad que presenta Cl@ve.

Esta función de firma electrónica es posible por la emisión de un **Certificado de Firma Centralizado**, es decir, un certificado electrónico en 'la nube', también denominado **DNI en modo nube** (**DNI-n**). Este certificado centralizado está firmado por la Autoridad de Certificación del DNI Electrónico, que es la Dirección General de la Policía.

La Cl@ve Firma requerirá siempre de un nivel alto de seguridad con autentificación por código OTP.

GESTIONAR EL SISTEMA CL@VE

Una vez hecha el alta en el sistema Cl@ve, y se tenga, o no activado el usuario en Cl@ve Permanente, se pueden gestionar los datos de registro, el código de activación o solicitar la baja en el sistema.

El acceso a estas gestiones dependerá del sistema de identificación que utilicemos:

- Con Cl@ve PIN: cambiar el correo electrónico y fecha de vencimiento del DNI/NIE.
- Con DNIe/3.0 o Certificado Digital: cambiar todos los datos, generar un nuevo código de activación para Cl@ve Permanente y darse de baja en la plataforma Cl@ve.

¿Cómo darse de baja en el sistema Cl@ve?

Si por alguna circunstancia es necesario darse de baja en el sistema Cl@ve se puede hacer en cualquier momento. Al anular o renunciar al sistema Cl@ve se elimina el acceso a todos sus servicios, tanto a Cl@ve Permanente como a Cl@ve PIN. Para poder utilizarlos de nuevo tendrás que realizar un nuevo proceso de alta, según lo descrito en la sección "¿Cómo darse de alta en el Sistema Cl@ve?".

Nota: al fallecer una persona que esté registrada en Cl@ve será dada de baja automáticamente en el momento que haya constancia de su fallecimiento.

IMPORTANTE: también se puede renunciar a Cl@ve personándose en una Oficina de Registro como las mencionadas en la sección "Presencial: en una oficina de registro".

Más información sobre este procedimiento presencial en el enlace:

http://clave.gob.es/clave_Home/registro/Renuncia.html.

"ME @DMINISTRO 2.0" EN LA PRÁCTICA: SISTEMA CL@VE

A continuación, vamos a enumerar las guías prácticas sobre "CL@VE: identidad electrónica para las administraciones".

Registrarse en el Sistema Cl@ve:

- Sistema Cl@ve: registro online con DNIe o Certificado Electrónico
- Sistema Cl@ve: registro con carta de invitación

Usar la Cl@ve PIN:

- Cl@ve PIN: cómo generar un PIN vía web
- Aplicación Cl@ve PIN: cómo usar la aplicación "Cl@ve PIN"
  - Aplicación Cl@ve PIN: activación de la aplicación
  - Aplicación Cl@ve PIN: cómo solicitar un PIN
- Cl@ve PIN: cómo usar el PIN

Usar Cl@ve Permanente:

- Cl@ve Permanente: cómo dar de alta el usuario y crear la contraseña
- Cl@ve permanente: cómo usarla

Gestionar Cl@ve Permanente:

- Cl@ve Permanente: cómo cambiar la contraseña
- Cl@ve Permanente: cómo recuperar la contraseña
- Cl@ve Permanente: cómo darse de baja

Usar Cl@ve Firma:

- Cl@ve Firma: cómo usarla
  - Cl@ve Firma: primer uso, emisión de los certificados para firmar
  - Cl@ve Firma: cómo firmar

Gestionar la cuenta de Sistema Cl@ve:

- Sistema Cl@ve: cómo modificar los datos de registro
- Sistema Cl@ve: cómo generar un código de activación
- Sistema Cl@ve: cómo renunciar al sistema
- Sistema Cl@ve: cómo gestionar los datos de registro con Cl@ve PIN

ADVERTENCIA

Dada la naturaleza cambiante de los servicios electrónicos de la misma Web, en constante actualización y renovación, los contenidos de esta guía pueden variar.

Esta guía debe tomarse como una referencia general que te ayude a completar un objetivo en el que procuramos llegar lo más cerca posible.

SISTEMA CL@VE: REGISTRO ONLINE CON DNIE O CERTIFICADO ELECTRÓNICO

Para utilizar los servicios del Sistema Cl@ve es necesario registrarse en la plataforma, para hacerlo teniendo un DNIe/3.0 o el Certificado Electrónico para personas físicas de la FNMT-RCM hay que seguir los siguientes pasos:

- Accedemos a la página **"Registro y obtención de Cl@ve PIN"** desde este enlace: https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/GC27.shtml
- Hacemos clic en **"Registrarse, renunciar y modificar datos en Cl@ve con certificado o DNI electrónico"**
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En la pantalla **"Registro, renuncia y modificación de datos con certificado"** el formulario tendrá la información necesaria tomada del DNI o certificado, hacemos clic en **"Enviar"**.
- Se desplegará una sección informativa sobre qué es el Sistema Cl@ve, hacemos clic en **"Enviar"**.
- La pantalla mostrará nuestros datos de identificación y la opción **"Alta"** seleccionada.
- Rellenamos el formulario "Datos asociados al Sistema de identificación y firma" con los datos solicitados:
  - **"Teléfono móvil"**: un número de teléfono móvil personal sin el prefijo de país
    - **"Confirme Teléfono móvil"**: repetimos el número anterior de forma idéntica.

> **IMPORTANTE**: El número de teléfono móvil personal es de suma importancia ya que será el medio por el que llegarán los códigos de seguridad generados por el sistema clave Cl@ve mediante SMS.

  - **"Correo electrónico"**.
    - **"Confirme Correo electrónico"**: repetimos el correo anterior de forma idéntica.
- Hacemos clic en la **casilla de selección simple** de la opción que se ajuste a nuestro tipo de documento de identidad:
  - **"Fecha de validez del DNI-TIE"**: indicamos con números la fecha de validez siguiendo el formato dd/mm/aaaa.

  - O **"DNI con validez permanente o 01-01-9999 o con Certificado de Registro de Ciudadano de la Unión"**.

- Hacemos clic en la **casilla de selección** en **"Se han leído y aceptado las condiciones"**.
- Hacemos clic en **"Enviar"**.
- Sucederán dos cosas:
  - Se generará el documento PDF **"Justificante de alta en el sistema de identificación y firma Cl@ve"** que abrirá una nueva pestaña. Con nuestros datos, número de expediente y en el apartado **"Código para activar su contraseña de acceso a servicios electrónicos de la administración general del estado en el sistema de Cl@ve permanente"** el **"Código de Activación"** necesario para activar el servicio de Cl@ve Permanente.
    IMPORTANTE: hay que conservar una copia este documento y su código.
  - Nos enviarán un SMS al número de móvil que dimos, confirmando el alta en el servicio.
- Ya estamos listos para usar el Sistema Cl@ve.

SISTEMA CL@VE: REGISTRO CON CARTA DE INVITACIÓN

Para utilizar los servicios del Sistema Cl@ve es necesario registrarse en la plataforma, para hacerlo con una carta de invitación de la Agencia Tributaria hay que seguir los siguientes pasos:

- Accedemos el servicio **"Solicitud de carta de invitación"** para solicitar la carta de invitación desde este enlace:
  https://www2.agenciatributaria.gob.es/es13/s/pi24pi24040f
- Rellenamos el formulario con los datos solicitados:
  - **"DNI-NIE"**.
  - **"Primer apellido"**.
  - **"Número de cuenta bancaria"**: indicamos los dígitos del bloque **cuarto** y **sexto** del número IBAN de una cuenta bancaria de la que seamos titulares y que hayamos utilizado en algún trámite con la Agencia Tributaria, como, por ejemplo, en la declaración del IRPF.
- Hacemos clic en **"Enviar"**.
- En unos días recibiremos una carta en nuestro domicilio fiscal con el CSV para realizar el alta en Cl@ve Permanente. Al recibirla accedemos al servicio de alta en este enlace:
  https://www2.agenciatributaria.gob.es/es13/s/pi24pi24020f
- En **"Registro con código seguro de verificación"** rellenamos el formulario con los siguientes datos:
  - **"DNI-NIE"**.

  - **“Primer apellido”**.
  - **“Código seguro de verificación (C.S.V.)”**: el código de la carta de invitación.
  - **“Número de cuenta bancaria”**: los dígitos del bloque **cuarto** y **sexto** del número IBAN utilizado para solicitar la carta de invitación.
- Hacemos clic en **“Enviar”**.
- En la pantalla **“Registro, renuncia y modificación de datos con certificado”** el formulario tendrá la información necesaria tomada del DNI o certificado, hacemos clic en **“Enviar”**.
- Se desplegará una sección informativa sobre qué es el Sistema Cl@ve, hacemos clic en **“Enviar”**.
- La pantalla mostrará nuestros datos de identificación y la opción **“Alta”** seleccionada.
- Rellenamos el formulario **“Datos asociados al Sistema de identificación y firma”** con los datos solicitados:
  - **“Teléfono móvil”**: un número de teléfono móvil personal sin el prefijo de país.
    - **“Confirme Teléfono móvil”**: repetimos el número anterior de forma idéntica.

> **IMPORTANTE**: El número de teléfono móvil personal es de suma importancia ya que será el medio por el que llegarán los códigos de seguridad generados por el sistema clave Cl@ve mediante SMS.

  - **“Correo electrónico”**.
    - **“Confirme Correo electrónico”**: repetimos el correo anterior de forma idéntica.
- Hacemos clic en la **casilla de selección simple** de la opción que se ajuste a nuestro tipo de documento de identidad:
  - **“Fecha de validez del DNI-TIE”**: Escribimos con números la fecha de validez siguiendo el formato: dd/mm/aaaa.
  - O **“DNI con validez permanente o 01-01-9999 o con Certificado de Registro de Ciudadano de la Unión”**.
- Hacemos clic en la **casilla de selección** en **“Se han leído y aceptado las condiciones”**.
- Hacemos clic en **“Enviar”**.
- Sucederán dos cosas:
  - Se generará el documento PDF **“Justificante de alta en el sistema de identificación y firma Cl@ve”** que abrirá una nueva pestaña. Con nuestros datos, número de expediente y en el apartado **“Código para activar su contraseña de acceso a servicios electrónicos de la administración general del estado en el**

sistema de Cl@ve permanente" el **"Código de Activación"** necesario para activar el servicio de Cl@ve Permanente.

IMPORTANTE: hay que conservar una copia este documento y su código.

- Nos enviarán un SMS al número de móvil que dimos, confirmando el alta en el servicio.

- Ya estamos listos para usar el Sistema Cl@ve.

CL@VE PIN: CÓMO GENERAR UN PIN VÍA WEB

Para generar una Cl@ve PIN desde la web hay que seguir los siguientes pasos:

- Descargamos en nuestro smartphone la aplicación del generador de Cl@ve PIN de la Agencia Tributaria desde este enlace: https://www2.agenciatributaria.gob.es/es13/h/p24obp01.html

IMPORTANTE: Hay que registrarse previamente para poder utilizar el sistema Cl@ve con la aplicación de Smartphone.

- Rellenamos el formulario con todos los datos solicitados:
  - **"DNI/NIE"**: el número con la letra.
  - **"Fecha de validez DNI/NIE"**: indicamos con números la fecha de validez siguiendo el formato dd/mm/aaaa.
    - **"¿Permanente?"**: si nuestro documento de identidad no tiene fecha de caducidad marcamos la **casilla de selección**.
  - **"Elija su clave de acceso"**: pulsamos e introducimos una clave de acceso de cuatro letras, esta puede ser una palabra que podamos recordar fácilmente. Queda excluida la letra "Ñ" y no importa que sean mayúsculas o minúsculas.

  Nota: algunos servicios solicitarán esta clave de acceso junto con el PIN, memorizarla o apuntarla.

    - **"Confirme su clave de acceso"**: repetimos la clave anterior de forma idéntica.

- Una vez rellenado el formulario hacemos clic en el botón **"Obtener PIN"**.

- Sucederán dos cosas:
  - Una ventana emergente nos confirma que han enviado un SMS con el PIN solicitado a nuestro número de teléfono móvil, hacemos clic en "**Cerrar"**.
  - Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve. En el SMS viene indicado el PIN generado.

IMPORTANTE: El PIN debes utilizarlo en los 10 minutos siguientes a que lo recibas.

- Con el PIN que hemos recibido ya podremos identificarnos en el servicio electrónico.

IMPORTANTE: Cl@ve PIN es una clave de "un solo uso" (OTP) si lo intentas usar de nuevo un mensaje te advertirá que el PIN ya fue usado y que obtengas uno nuevo.

Aplicación Cl@ve PIN: cómo usar la aplicación "Cl@ve PIN"

Con la aplicación Cl@ve PIN se generan códigos PIN de forma muy ágil y cómoda. Después de su descarga y activación estará lista para usarse de forma muy sencilla. Para ello hay que seguir los siguientes pasos:

- Descargamos la aplicación "Cl@ve PIN" adecuada a nuestro dispositivo móvil:
  - Para Android: https://play.google.com/store/apps/details?id=es.aeat.pin24h&hl=es
  - Para IOs (Apple): https://itunes.apple.com/es/app/pin24h/id842624380?mt=8
- Abrimos la aplicación y en la primera vez nos mostrará la pantalla **"Clave PIN. Información inicial"** con instrucciones e información sobre la Cl@ve PIN y la activación de la aplicación. Baja y pulsa en **"Finalizar"**.
- Se mostrará el **"Acuerdo de licencia"**. Al terminar pulsamos en **"Aceptar"**.
- A continuación, tenemos que activar la aplicación antes de empezar a usarla…

Aplicación Cl@ve PIN: activación de la aplicación

Al utilizar la aplicación por primera vez después de descargada hay que realizar un proceso de activación. Para activar la aplicación hay que seguir los siguientes pasos:

- Rellenamos el **"Formulario de activación (paso 1)"** con todos los datos solicitados:
  - **"DNI/NIE"**: pulsamos y escribimos el número con la letra.
  - **"Fecha de validez DNI/NIE"**: pulsamos el botón **"Establecer fecha"**. Se abrirá un selector de fechas, pulsamos sobre el día, mes y año y escribimos la fecha de caducidad del documento de identidad.
    - Si el documento de identidad no tiene fecha de caducidad pulsamos en la **casilla de selección** de **"DNI/NIE Permanente"**. Al marcar la casilla de selección indicamos los dígitos del bloque **cuarto** y **sexto** del número IBAN de una cuenta bancaria de la que seamos titulares y que hayamos utilizado en algún trámite con la Agencia Tributaria, como, por ejemplo, en la declaración del IRPF.
  - **"Clave"**: pulsamos e introducimos una clave de acceso de cuatro letras, esta puede ser una palabra que podamos recordar fácilmente. Queda excluida la letra "Ñ" y no importa que sean mayúsculas o minúsculas.

  IMPORTANTE: esta clave no es una contraseña, es solo una variable de seguridad para generar la Cl@ve PIN, pero será necesario recordarla mientras esté en uso. Si así se quiere se puede cambiar cada vez que generemos un PIN nuevo.

  - Pulsa sobre la **casilla de selección** de **"recordar clave"** para que no se borre al cerrar la aplicación.

- Al terminar de rellenar todos los datos pulsamos en **"Enviar"**.
- Sucederán dos cosas:
  - Un mensaje emergente nos confirma que han enviado un SMS con el PIN solicitado a nuestro número de teléfono móvil para usar en el siguiente formulario. Pulsamos sobre **"Aceptar"**.
    IMPORTANTE: el PIN debes utilizarlo en los 10 minutos siguientes a que lo recibas.
  - Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve. En el SMS viene indicado el PIN generado para la activación de la aplicación.
- En el **"Formulario de activación (paso 2)"** introducimos el código que recibimos por SMS pulsando en **"PIN"**.
- Pulsamos en **"Enviar"**.
- Un mensaje emergente nos avisará que la activación se ha completado con éxito. Pulsamos sobre **"Aceptar"**.
- Ahora la aplicación "Cl@ve PIN" está lista para usar.

Eliminar el usuario de la aplicación

Si se quiere eliminar o cambiar al usuario de la aplicación hay que seguir los siguientes pasos:

- Pulsamos el **icono de papelera**.
- Un mensaje nos advertirá que: **"Borrar DNI/NIE. Se va a proceder al borrado del DNI/NIE en la aplicación ¿Está usted seguro?"**.
- Pulsamos sobre **"Aceptar"** para eliminarlo.
- La aplicación queda lista para utilizar con otro usuario.

Aplicación Cl@ve PIN: cómo solicitar un PIN

Una vez activada la aplicación se puede solicitar una Cl@ve PIN de forma muy sencilla ya que no habrá que introducir datos. Para solicitar un PIN hay que seguir los siguientes pasos:

- En **"Solicitud de la Cl@ve PIN"** indicamos la fecha de validez del DNI/NIE pulsando el botón **"Establecer fecha"**. Se abrirá un selector de fechas, pulsamos sobre el día, mes y año y escribimos la fecha de caducidad del documento de identidad.
  Nota: si disponemos de un dispositivo móvil con Android 4.2 (Jelly Bean) o superior y lo tenemos protegido con un sistema de protección por contraseña, patrón o biometría la fecha se almacenará cuando marquemos la casilla **"recordar fecha"**.
- En **"Clave"** se puede dejar la utilizada durante la activación (si hemos marcado la **casilla de selección** de **"recordar clave"**), usar una nueva o poner una distinta en cada nueva solicitud de PIN.

- Pulsamos sobre **"Enviar"**.
- Se generará el PIN de tres caracteres alfanuméricos que usaremos para conectarte en los servicios telemáticos que estén integrados en la plataforma de Cl@ve.

IMPORTANTE: La Cl@ve PIN no se almacena en la aplicación, se debe memorizar o apuntar mientras se tenga en uso, ya que se puede borrar o perder.

- Si necesitamos generar una nueva Cl@ve PIN simplemente pulsamos en **"Solicitar nuevo PIN"** y se generará un nuevo código de forma inmediata.

CL@VE PIN: CÓMO USAR EL PIN

Una vez generado el código PIN para identificarse con Cl@ve PIN hay que seguir los siguientes pasos:

- Una vez que estemos en el servicio electrónico que queramos utilizar, que esté integrado en el sistema Cl@ve, seleccionamos la opción de usar Cl@ve para identificarnos.
- Se abre una página para autentificarnos en el sistema. Rellenamos el formulario con los datos que solicitan:
  - **- "DNI/NIE"**.
  - **- "Clave del código de acceso"**: en determinados servicios pedirán el código de 4 caracteres que utilizamos para generar el PIN.
  - **- "PIN del código de acceso"**: introducimos el código PIN que generamos vía web o con la aplicación.
- Al terminar hacemos clic en **"Acceder"**.
- Se abrirá de nuevo la página del servicio telemático por el cual hemos empezado el procedimiento para realizar la gestión telemática.

Nota: si aún no tenemos una Cl@ve PIN hacemos clic en **"No tengo PIN"**. O si aún no estamos registrado en el sistema hacemos clic en **"No estoy registrado"** (instrucciones en: "Sistema Cl@ve: registro online con DNIe o Certificado Electrónico" o "Sistema Cl@ve: registro con carta de invitación").

CL@VE PERMANENTE: CÓMO DAR DE ALTA EL USUARIO Y CREAR LA CONTRASEÑA

Para activar el usuario en Cl@ve Permanente y crear la contraseña hay que seguir los siguientes pasos:

- Accedemos a la página **"Procedimientos"** del portal de Cl@ve desde este enlace: http://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html
- Debajo de título **"Activación de usuario"** hacemos clic en el enlace **"Acceder al servicio"**.

- En la pantalla **"Servicios de gestión de contraseña - Cl@ve permanente"** rellenamos el formulario con los datos solicitados:
  - **"Tipo de Documento"**: si es un DNI o un NIE.
  - **"Número de Documento"**.
  - **"Dirección de Correo Electrónico"**: la misma que utilizamos cuando nos registramos en Cl@ve.
  - **"Código de Activación"**: que es el número que viene en el documento PDF **"Justificante de alta en el sistema de identificación y firma Cl@ve"** que está en el apartado **"Código para activar su contraseña de acceso a servicios electrónicos de la administración general del estado en el sistema de Cl@ve permanente"**.
  - El último campo es una verificación de seguridad. Respondemos la pregunta que formulan utilizando alguna de las palabras que dan para seleccionar.
- Al terminar hacemos clic en **"Siguiente"**.
- Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve un código OTP de verificación para continuar el alta.
- Introducimos el código OTP que enviaron, hacemos clic en **"Siguiente"**.
- Crea la contraseña que vas a utilizar con Cl@ve Permanente.

> **IMPORTANTE**: Si la contraseña es de menos de 16 caracteres debe cumplir al menos estas condiciones (mínimo 3): una letra mayúscula, una letra minúscula, un número o un carácter especial.

Repetimos la contraseña de forma idéntica para confirmarla.

- Hacemos clic en **"Emitir"**.
- Una última pantalla **"Registro Finalizado"** confirmará que está activado tu usuario y creada tu contraseña de Cl@ve Permanente. Un texto te informará sobre el uso adecuado de la contraseña y su gestión.

CL@VE PERMANENTE: CÓMO USARLA

Una vez hecha el alta, usar la Cl@ve Permanente en un servicio electrónico que utilice este sistema es muy sencillo. Para utilizarla hay que seguir los siguientes pasos:

- Una vez que estemos en el servicio electrónico que queramos utilizar, que esté integrado en el sistema Cl@ve, seleccionamos la opción de usar Cl@ve Permanente para identificarnos.
- Rellenamos el formulario con los datos que solicitan:
  - **DNI/NIE**.
  - **La contraseña de Cl@ve Permanente**.

- Al terminar hacemos clic en **Autenticar”**.
- Se abrirá de nuevo la página del servicio telemático por el cual hemos empezado el procedimiento para realizar la gestión telemática.

IMPORTANTE: algunos servicios requerirán un nivel de seguridad más elevado, en esos casos será necesario identificarse con un código OTP enviado al móvil por SMS.

CL@VE PERMANENTE: CÓMO CAMBIAR LA CONTRASEÑA

Se puede acceder al servicio de cambiar la contraseña de Cl@ve Permanente con el usuario y la contraseña de Cl@ve Permanente o con nuestro certificado digital.

Para cambiar la contraseña de Cl@ve Permanente hay que seguir los siguientes pasos:

- Accedemos a la página **“Procedimientos”** del portal de Cl@ve desde este enlace: http://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html
- 1. Para identificarnos en el servicio seguimos estos pasos iniciales según sea nuestro caso:
  - **A) Con usuario y contraseña:**
    - Debajo del título **“Gestión de la contraseña”** hacemos clic en **“Accede al servicio con usuario y contraseña”**.
    - Se abrirá la ventana **“Plataforma de Autenticación - Sede Electrónica de la Seguridad Social”**. Rellenamos el formulario con los datos del **“DNI/NIE”** y la **“Contraseña”** de Cl@ve Permanente.
    - Una vez rellenados hacemos clic en **“Autenticar”**.
  - **B) Con certificado digital:**
    - Debajo del título **“Gestión de la contraseña”** hacemos clic en **“Accede al servicio con certificado digital”**.
    - Se abrirá la ventana emergente **“Petición de identificación de usuario”** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **“Elija un certificado para presentarlo como identificación”**.
    - Hacemos clic en **“Aceptar”**.
- 2. Una vez identificados en el servicio rellenamos el formulario con los datos de la contraseña actual y la nueva que deseas:
  - **“Contraseña Actual”**.
  - **“Contraseña Nueva”**.

  IMPORTANTE: si la contraseña es de menos de 16 caracteres debe cumplir al menos estas condiciones (mínimo 3): una letra mayúscula, una letra minúscula, un número o un carácter especial.

  - **"Repite la contraseña"**: repetimos la contraseña anterior de forma idéntica.
- Al terminar hacemos clic en **"Modificar Contraseña"**.

- 3. Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve un código OTP de verificación para continuar.
  - Introducimos el código OTP que enviaron y hacemos clic en **"Modificar contraseña"**.
- Una última pantalla **"Resultado cambio de contraseña"** confirmará el cambio de contraseña para Cl@ve Permanente.

CL@VE PERMANENTE: CÓMO RECUPERAR LA CONTRASEÑA

Para cambiar la recuperar la contraseña de Cl@ve Permanente si se ha perdido, olvidado o bloqueado hay que seguir los siguientes pasos:

- Accedemos a la página **"Procedimientos"** del portal de Cl@ve desde este enlace: http://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html
- Bajo el título **"Gestión de la contraseña"** y en el apartado **"Olvido de Contraseña"** hacemos clic en **"Accede al servicio"**.
- En la pantalla **"Servicios de gestión de contraseña - Cl@ve permanente"** rellenamos el formulario con los datos solicitados:
  - **"Tipo de Documento"**: si es un DNI o un NIE.
  - **"Número de Documento"**.
  - **"Código de Activación"**: que es el número que viene en el documento PDF **"Justificante de alta en el sistema de identificación y firma Cl@ve"** que está en el apartado **"Código para activar su contraseña de acceso a servicios electrónicos de la administración general del estado en el sistema de Cl@ve permanente"**.
  - El último campo es una verificación de seguridad. Responde la pregunta que formulan utilizando alguna de las palabras que te dan para seleccionar.
- Al terminar hacemos clic en **"Siguiente"**.
- Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve un código OTP de verificación para continuar.
- Introducimos el código OTP que enviaron y hacemos clic en **"Siguiente"**.
- Una vez identificados en el servicio rellenamos el formulario con los datos de la contraseña nueva que deseas:
  - **"Contraseña Nueva"**.

IMPORTANTE: si la contraseña es de menos de 16 caracteres debe cumplir al menos estas condiciones (mínimo 3): una letra mayúscula, una letra minúscula, un número o un carácter especial.

  - **"Repite la contraseña"**: repetimos la contraseña anterior de forma idéntica.

- Al terminar hacemos clic en **"Emitir"**.
- Una última pantalla **"Resultado cambio de contraseña"** confirmará el cambio a tu nueva contraseña para Cl@ve Permanente.

CL@VE PERMANENTE: CÓMO DARSE DE BAJA

Se puede acceder al servicio de darse de baja de Cl@ve Permanente con el usuario y la contraseña de Cl@ve Permanente o con nuestro certificado digital.

Para darse de baja de Cl@ve Permanente hay que seguir los siguientes pasos:

- Accedemos a la página **"Procedimientos"** del portal de Cl@ve desde este enlace: http://clave.gob.es/clave_Home/Clave-Permanente/Procedimientos.html
- Para identificarnos en el servicio seguimos estos pasos iniciales según sea nuestro caso:
  - **A) Con usuario y contraseña:**
    - Debajo del título **"Gestión de la contraseña"** hacemos clic en **"Accede al servicio con usuario y contraseña"**.
    - Se abrirá la ventana **"Plataforma de Autenticación - Sede Electrónica de la Seguridad Social"**. Rellenamos el formulario con los datos del **"DNI/NIE"** y la **"Contraseña"** de Cl@ve Permanente.
    - Una vez rellenados hacemos clic en **"Autenticar"**.
  - **B) Con certificado digital:**
    - Debajo del título **"Gestión de la contraseña"** hacemos clic en **"Accede al servicio con certificado digital"**.
    - Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
    - Hacemos clic en **"Aceptar"**.
- Una confirmación advierte de si estamos seguros de querer darnos de baja como usuarios. Hacemos clic en **"Sí, estoy de acuerdo"**.
- Según la forma como nos hemos identificado en el servicio el paso final varía:
  - **A) Con usuario y contraseña:**
    - Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve un código OTP de verificación para confirmar nuestra baja.
    - Introducimos el código OTP que enviaron y hacemos clic en **"Siguiente"**.
  - **B) Con certificado digital:** la baja es inmediata, sin confirmación.
- Una última pantalla confirmará nuestra baja en Cl@ve Permanente.

Nota: una vez hecha la baja en Cl@ve Permanente el usuario es desactivado, así como todos sus servicios. Si se desea usar de nuevo el servicio hay que hacer de nuevo todo el proceso de alta descrito en "Cl@ve Permanente: cómo dar de alta el usuario y crear la contraseña"

CL@VE FIRMA: CÓMO USARLA

Cl@ve Firma permite firmar documentos electrónicos a través de certificados en la nube. Estos certificados centralizados se emiten o activan al utilizar el servicio por primera vez.

Cuando se utiliza un trámite telemático servicio electrónico que requiere usar Cl@ve Firma hay que seguir los siguientes pasos iniciales:

- El uso de Cl@ve Firma está tipificado como un trámite de Seguridad Alta, por lo tanto, cuando ingresemos al servicio tendremos que identificarnos con nuestro usuario y contraseña de Cl@ve Permanente y además recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve con un código OTP de verificación para continuar.
- Una vez terminado el trámite y aceptadas las condiciones de uso se procede a la firma digital.
- Se mostrará la pantalla para utilizar Cl@ve Firma.

> **IMPORTANTE**: Si es la primera vez que utilizas Cl@ve Firma se generarán los certificados centralizados necesarios antes de poder firmar.

Cl@ve Firma: primer uso, emisión de los certificados para firmar

Al utilizar Cl@ve Firma por primera vez hay que seguir los siguientes pasos:

- Se mostrará la pantalla **"Solicitud del certificado centralizado"** para proceder el certificado de firma correspondiente. Para emitir el certificado centralizado hay que seguir los siguientes pasos:
  - Hacemos clic en **"Solicitar Certificado"**.
- En la pantalla **"Emisión de tu certificado de firma centralizado"** introduciremos en el formulario la contraseña de Cl@ve Permanente.
  - Hacemos clic en **"Emitir"**.
- Sucederán dos cosas:
  - Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve con un código OTP de verificación.
  - En la pantalla **"Emisión de tu certificado de firma centralizado"** haremos clic en la **casilla de verificación "Acepto"** y en el formulario introduciremos el código OTP que recibimos.
    - Hacemos clic en **"Emitir"**.

- Si el proceso de generación de los certificados resulta exitoso volveremos al servicio o trámite que estamos haciendo y el mensaje **"Solicitud del certificado centralizado"** nos confirmará que el certificado de firma centralizado ha sido generado, hacemos clic en **"Continuar"**.
- Ya estamos listos para firmar electrónicamente con Cl@ve Firma…

Cl@ve Firma: cómo firmar

Una vez que los certificados de Cl@ve Firma son emitidos hay que seguir los siguientes pasos para firmar:

- Al momento de firmar electrónicamente con Cl@ve Firma sucederán dos cosas:
  - Recibiremos un SMS al teléfono móvil que indicamos al registrarnos en el sistema Cl@ve con un código OTP de verificación para continuar.
  - En la pantalla **"Firma"** rellenaremos el formulario con los datos que nos solicitan:
    Usuario (DNI/NIE) y contraseña de Cl@ve Permanente.
    El código OTP recibido.
    - Hacemos clic en **"Continuar"**.
- Si el proceso se realizó con éxito terminaremos el trámite que estamos realizando con, por ejemplo, la generación de un documento PDF con nuestra firma electrónica.

SISTEMA CL@VE: CÓMO MODIFICAR LOS DATOS DE REGISTRO

Para modificar tus datos en el sistema Cl@ve con el DNIe/3.0 o el Certificado Digital hay que seguir los siguientes pasos:

- Accedemos a la página **"Registro y obtención de Cl@ve PIN"** desde este enlace: https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/GC27.shtml
- Debajo del título "Si quiere registrarse con certificado o DNI electrónico (también podrá renunciar al sistema o modificar los datos del registro)" hacemos clic en "Registro, renuncia y modificación de datos en Cl@ve con certificado o DNI electrónico".
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En **"Identificación"** hacemos clic en **"Enviar"** para continuar.
- En la pantalla **"Modificación de fecha de validez del DNI-TIE"** estarán disponible las opciones de:
  - **"Renunciar al servicio"**.
  - **"Modificación de datos"**.

- Hacemos clic en la **casilla de selección simple** de **"Modificación de datos"**. Ahora podemos modificar los datos:
  - **"Teléfono móvil"**.
  - **"Correo electrónico"**.
  - **"Fecha de validez del DNI-NIE"**.
- Para modificarlos reemplazamos los datos existentes. En el caso del correo electrónico lo repetimos para confirmar.
- Hacemos clic en la **casilla de selección** de **"Se han leído y aceptado las condiciones"**.
- Hacemos clic en **"Enviar"**.
- Se generará el documento PDF **"Justificante de modificación de datos en el sistema de identificación y firma Cl@ve"** que abrirá una nueva pestaña. Con nuestros datos, número de expediente y fecha de modificación de tus datos. Este justificante no tiene el apartado con el código de activación que vimos en "Sistema Cl@ve: registro online con DNIe o Certificado Electrónico".

SISTEMA CL@VE: CÓMO GENERAR UN CÓDIGO DE ACTIVACIÓN

En el caso de perder el código de activación necesario para el proceso de alta o las gestiones en Cl@ve Permanente se puede generar un código nuevo.

Para generar un nuevo código de activación con el DNIe/3.0 o el Certificado Digital hay que seguir los siguientes pasos:

- Accedemos a la página **"Registro y obtención de Cl@ve PIN"** desde este enlace: https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/GC27.shtml
- Debajo del título **"Si quiere registrarse con certificado o DNI electrónico (también podrá renunciar al sistema o modificar los datos del registro)"** hacemos clic en **"Registro, renuncia y modificación de datos en Cl@ve con certificado o DNI electrónico"**.
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En **"Identificación"** hacemos clic en **"Enviar"** para continuar.
- En la pantalla **"Modificación de fecha de validez del DNI-TIE"** estarán disponible las opciones de:
  - **"Renunciar al servicio"**.
  - **"Modificación de datos"**.

- Hacemos clic en la **casilla de selección** simple de **"Modificación de datos"**.
- Hacemos clic en la **casilla de selección** de **"Regenerar Código de Activación (solo marcar en caso de necesidad de renovación del código de activación)"**.
- Hacemos clic en la **casilla de selección** de **"Se han leído y aceptado las condiciones"**.
- Hacemos clic en **"Enviar"**.
- Se generará el documento PDF **"Justificante de modificación de datos en el sistema de identificación y firma Cl@ve"** que abrirá una nueva pestaña. Con nuestros datos, número de expediente, fecha de modificación de tus datos y en el apartado **"Código para activar su contraseña de acceso a servicios electrónicos de la administración general del estado en el sistema de Cl@ve permanente"** un nuevo **"Código de Activación"**.

SISTEMA CL@VE: CÓMO RENUNCIAR AL SISTEMA

Para anular el registro hecho en el sistema Cl@ve con el DNIe/3.0 o el Certificado Digital hay que seguir los siguientes pasos:

- Accedemos a la página **"Registro y obtención de Cl@ve PIN"** desde este enlace: https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/GC27.shtml
- Debajo del título **"Si quiere registrarse con certificado o DNI electrónico (también podrá renunciar al sistema o modificar los datos del registro)"** hacemos clic en **"Registro, renuncia y modificación de datos en Cl@ve con certificado o DNI electrónico"**.
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En **"Identificación"** hacemos clic en **"Enviar"** para continuar.
- En la pantalla **"Modificación de fecha de validez del DNI-TIE"** estarán disponible las opciones de:
  - **"Renunciar al servicio"**.
  - **"Modificación de datos"**.
- Hacemos clic en la **casilla de selección simple** de **"Renunciar al servicio"**.
- Hacemos clic en la **casilla de selección** de **"Se han leído y aceptado las condiciones"**.
- Hacemos clic en **"Enviar"**.

- Se generará el documento PDF **"Justificante de renuncia en el sistema de identificación y firma Cl@ve"** que abrirá una nueva pestaña con los datos de tu renuncia al sistema Cl@ve.

  Nota: una vez hecha la baja en el sistema Cl@ve son desactivados todos sus servicios. Si se desea usar de nuevo el servicio hay que hacer otra vez todo el proceso de alta descrito en "Sistema Cl@ve: registro online con DNIe o Certificado Electrónico" y "Sistema Cl@ve: registro con carta de invitación".

  IMPORTANTE: también se puede renunciar a Cl@ve personándose en una Oficina de Registro. Más información sobre este procedimiento presencial en el enlace: http://clave.gob.es/clave_Home/registro/Renuncia.html.

SISTEMA CL@VE: CÓMO GESTIONAR LOS DATOS DE REGISTRO CON CL@VE PIN

Para modificar tus datos básicos con Cl@ve PIN sigue los siguientes pasos:

- Accedemos a la página **"Registro y obtención de Cl@ve PIN"** desde este enlace: https://www.agenciatributaria.gob.es/AEAT.sede/procedimientoini/GC27.shtml
- Debajo del título **"Si quiere utilizar Cl@ve PIN para modificar los datos de registro, excepto el número de teléfono"** hacemos clic en **"Modificación de los datos de registro, excepto el número de teléfono, con Cl@ve PIN"**.
- Se abrirá la ventana emergente **"Petición de identificación de usuario"** para identificarnos digitalmente con el sistema que tengamos disponible, si tenemos ambos seleccionamos el que queremos usar en el menú desplegable **"Elija un certificado para presentarlo como identificación"**.
- Hacemos clic en **"Aceptar"**.
- En la pantalla **"Modificación de fecha de validez del DNI-TIE"** estará seleccionada y disponible la opción **"Modificación de datos"**.
- Se podrán modificar los datos:
  - **"Correo electrónico"**.
  - **"Fecha de validez del DNI-NIE"**.
- Para modificarlos reemplazamos los datos existentes. En el caso del correo electrónico lo repetimos para confirmar.
- Hacemos clic en la **casilla de selección** de **"Se han leído y aceptado las condiciones"**.
- Hacemos clic en **"Enviar"**.
- Se generará el documento PDF **"Justificante de modificación de datos en el sistema de identificación y firma Cl@ve"** que abrirá una nueva pestaña. Con nuestros datos, número de expediente y fecha de modificación de tus datos. Este justificante no tiene el apartado con el código de activación que vimos en "Sistema Cl@ve: registro online con DNIe o Certificado Electrónico".


Promoción de la autonomía personal para la inserción laboral.
Me
2.0
@dministro

ANEXO

CONSEJOS PARA CREAR UNA CONTRASEÑA

Es necesario preservar la seguridad y privacidad de nuestros sistemas de identidad o en multitud de trámites y servicios telemáticos o incluso los dispositivos electrónicos, y para ello es fundamental como medida básica crearles contraseñas (o passwords) de acceso que sean fuertes y robustas. Para crear contraseñas de calidad hay que seguir los siguientes consejos:

- Que contenga letras en minúsculas y mayúsculas.
    - No utilices palabras que estén en el diccionario.
    - Ni palabras o nombres que estén relacionadas con tu identidad personal, como puede ser tu nombre, motes, ciudad natal o de residencia, el nombre de tu mascota, etc.
- Que contenga números:
    - No utilices números que estén relacionados contigo, como tu fecha de nacimiento, teléfono, DNI, etc.
- Que contenga signos ortográficos o caracteres especiales: como pueden ser: @:#,$.%-!_/;€.
- Que contenga un mínimo de 8 caracteres.
- Mezcla los consejos anteriores en algo que te pueda resultar fácil recordar.
    - Si vas a utilizar una palabra que sea conocida para ayudarte a recordarla prueba escribiendo y cambiando letras números, en lo que se denomina escritura “L33t sp3ak”, caracteres especiales. Luego puedes escribirla del revés. Por ejemplo: mUrC13L4g@ (¿A qué se lee murciélago?) o 5eV3RL€d (¿Puedes leer “del revés”?).
- No tengas una misma contraseña para todo, por muy compleja que sea.
- No las compartas con nadie. Y si tienes que hacerlo por alguna circunstancia cámbiala luego.
- Apúntalas en un lugar seguro y protegido, apartado del dispositivo donde uses la contraseña.
- Haz cambios regulares de tus contraseñas.
- Activas las opciones de autentificación extra que ofrezcan los servicios electrónicos, como usar el móvil para verificar un cambio.
- Recuerda desconectar todas tus claves que uses en ordenadores o dispositivos públicos.
- Protege tus dispositivos móviles y las aplicaciones más sensibles a la privacidad.

BIBLIOGRAFÍA Y REFERENCIAS

La e-Administración y Servicios Telemáticos

- PAe Portal de la Administración Electrónica, Administración General del Estado http://administracionelectronica.gob.es/
- Punto de acceso general http://administracion.gob.es/ antes Red 060 http://www.060.es/
- Manual Práctico de Supervivencia en la Administración Electrónic@ - Manual de ayuda integral para usuarios de Administración electrónica http://www.microlopez.org/manual-practico-de-supervivencia-en-la-administracion-electronica/
- Agenda Digital para España http://www.agendadigital.gob.es/Paginas/Index.aspx
- Administración pública electrónica https://es.wikipedia.org/wiki/Administración_pública_electrónica

Identidad digital

- PAe Firma Electrónica: Identidad Digital en las Administraciones Públicas http://firmaelectronica.gob.es/Home/Empresas/Identidad-Digital.html
- PAe Firma electrónica, Aprende a usar tu firma electrónica paso a paso http://firmaelectronica.gob.es/
- Certificados electrónicos y digitales. Firma electrónica (VÍDEO) https://youtu.be/EU6vgU077xU
- Firma Digital (VÍDEO) https://youtu.be/0gch2r2l3JE
- ¿Qué es la firma digital? (VÍDEO) https://youtu.be/LakHFzApC5Q

Criptografía

- Criptografía https://es.wikipedia.org/wiki/Criptograf%C3%ADa
- ¿Qué es y cómo surge la criptografía?: un repaso por su historia http://www.genbetadev.com/seguridad-informatica/que-es-y-como-surge-la-criptografia-un-repaso-por-su-historia
- Breve historia de la criptografía http://www.eldiario.es/turing/criptografia/Breve-historia-criptografia_0_261773822.html
- Cómo funciona la criptografía (VÍDEO) https://youtu.be/Q8K311s7EiM
- Introducción a la criptografía. Tipos de sistemas criptográficos y algoritmos más utilizados. MOOC Ciberseguridad: Ataques y contramedidas (Universidad Rey Juan Carlos) https://youtu.be/AKFEWeKynd0
- Tutorial básico de Criptografía – FNMT-RCM CERES http://www.cert.fnmt.es/curso-de-criptografia
- Cifrado César (cifrado por desplazamiento, código de César o desplazamiento de César) https://es.wikipedia.org/wiki/Cifrado_C%C3%A9sar

- Cifrado por sustitución https://es.wikipedia.org/wiki/Cifrado_por_sustituci%C3%B3n
- Escítala https://es.wikipedia.org/wiki/Esc%C3%ADtala
- Cifrado por transposición https://es.wikipedia.org/wiki/Cifrado_por_transposici%C3%B3n

DNI Electrónico / 3.0

- Portal Oficial sobre el DNI electrónico http://www.dnielectronico.es/PortalDNIe/
- DNI Electrónico "Guía de referencia básica" (PDF) http://www.dnielectronico.es/PDFs/Guia_de_referencia_basica_v1_5.pdf
- PAe Firma Electrónica: DNI Electrónico http://firmaelectronica.gob.es/Home/Ciudadanos/DNI-Electronico.html
- Portal DNIe: comprobar bloqueo de DNI y utilizar VALIDe http://www.dnielectronico.es/PDFs/ComprobacionBloqueoPIN.pdf
- El DNI electrónico ha muerto: ¡larga vida al DNI 3.0! http://www.elconfidencial.com/tecnologia/2013-10-02/el-dni-electronico-ha-muerto-larga-vida-al-dni-3-0_35442/

Certificado electrónico

- El blog oficial de CERES http://tucertificadodigital.es/
- Certificado digital FNMT "Manual de buenas prácticas" (PDF) https://www.sede.fnmt.gob.es/documents/11614/75209/Manual_buenas_practicas.pdf
- Certificado digital: cómo solicitar tu certificado digital, Certificados CERES Fnmt (VÍDEO) https://youtu.be/p19J0TOpIks
- .pfx = .p12 https://www.chilkatsoft.com/p/p_439.asp
- Stack overflow: convert pfx format to p12 http://stackoverflow.com/questions/6819079/convert-pfx-format-to-p12
- Microsoft support: Certificados digitales de la fnmt en windows 7 (Última revisión: 09/26/2013) https://support.microsoft.com/es-es/kb/978599

Sistema Cl@ve

- Cl@ve Firma, definiciones http://clave.gob.es/clave_Home/dnin/definiciones.html
- Cl@ve PIN preguntas frecuentes http://www.agenciatributaria.es/AEAT.internet/Inicio/La_Agencia_Tributaria/Campanas/Cl_ve_PIN/_INFORMACION/Preguntas_frecuentes/Preguntas_frecuentes.shtml

- Tutorial Instalación y uso de clave (cl@ve Pin y cl@ve Permanente): Administración Electrónica (VÍDEO)
  https://youtu.be/rg0RC-G4YS4
- Agencia Tributaria Cl@ve PIN - Nuevo sistema de autenticación e identificación (VIDEO)
  https://youtu.be/c5yUuGA2Hfk
- Agencia Tributaria, Cl@ve PIN: Vídeos explicativos (VIDEO)
  http://www.agenciatributaria.es/AEAT.internet/PIN_24H/videos.shtml

Apps

- 10 apps para impulsar el gobierno abierto.
  http://www.compromisoempresarial.com/carrusel/2015/01/10-apps-para-impulsar-el-gobierno-abierto/

Varios

- VALIDe verificar, probar y visualizar certificados y firmas https://valide.redsara.es/valide/
- El Gobierno Vasco publica un glosario de términos sobre Administración electrónica (PDF)
  http://web.archive.org/web/20120630132809/https://www.cenatic.es/hemeroteca-de-cenatic/3-sobre-el-sector-del-sfa/39707-el-gobierno-vasco-publica-un-glosario-de-terminos-sobre-administracion-electronica

CRÉDITOS Y LICENCIA

Título: “Guía: Los servicios electrónicos para la autonomía personal: identidad digital”

Coordinación de contenidos: Marta Tante García, Coordinadora de proyectos y responsable de comunicación de la Federación Nacional ASPAYM y Gustavo A. Díaz González, Coordinador de Me@dministro.

Elaboración de contenidos: Marta Tante García, Coordinadora de proyectos y responsable de comunicación de la Federación Nacional ASPAYM, Gustavo A. Díaz González, Coordinador de Me@dministro y Federico Vallmitjana Baixeras, delegado experto Me@dministro 2.0.

Con la colaboración de: Fundación Vodafone España, Ilunion Consultoría y Accesibilidad.

Responsable edición digital: Federación Nacional ASPAYM.

Disponible esta publicación en: www.aspaym.org

2ª edición electrónica: diciembre de 2018.