Universitat d'Alacant
Universidad de Alicante

SEGURIDAD EN LAS REDES

BUA

CID
COMPETENCIAS EN INFORMACIÓN DIGITAL

ÍNDICE

OBJETIVOS

- Comprender los conceptos básicos de la autenticación digital
- Conocer qué es un Certificado Digital y qué podemos hacer con él
- Saber cómo solicitar e instalar el Certificado Digital de la FNMT
- Gestionar el ciclo de vida de los Certificados Digitales
- Aprender como firmar digitalmente un documento
- Conocer las distintas formas de firmar digitalmente un documento
- Aprender qué es la autenticación multifactor, y por qué es necesario usarla
- Conocer el método de 2FA para entrar en UAClod

CERTIFICADOS DIGITALES

El proceso imparable de digitalización de cada vez más facetas de nuestra actividad profesional, educativa, personal o de ocio se ha visto incrementado exponencialmente a raíz de la pandemia y la expansión del teletrabajo. La influencia disruptiva de internet ha revolucionado los modelos de negocio y las formas de interactuar de las personas tanto a nivel personal como en sus relaciones con las administraciones públicas, las entidades financieras, las plataformas de comercio electrónico o la miríada de servicios que han florecido con la revolución digital y de las redes sociales.

La Universidad de Alicante no es ajena a este proceso, habrás podido comprobar que, curso a curso, las funcionalidades del Campus Virtual van aumentando tanto a nivel docente como administrativo.

En muchos de estos escenarios es fundamental **la identificación unívoca** y sin ningún género de dudas de la persona implicada: certificar que tú eres realmente tú, que la persona interesada es realmente quien dice ser es un requisito indispensable en la implementación de estos procesos de transformación digital. Esta necesidad de validación es especialmente crítica cuando hablamos de relaciones contractuales, en las cuales la autenticidad y la veracidad de la identidad es fundamental. También la Universidad de Alicante introduce **nuevas medidas de protección**, como el establecimiento del **doble factor de autenticación (2FA)** para reforzar la seguridad en la identificación de las personas usuarias.

Es en este entorno donde los **certificados digitales** constituyen la piedra angular que otorga **credibilidad, veracidad y autenticación** a todas las necesidades planteadas.

CONCEPTOS PREVIOS

CERTIFICADO DIGITAL

Un **certificado digital** es un fichero o archivo digital emitido por una tercera parte de confianza (una Autoridad de Certificación) que garantiza la vinculación entre la identidad de una persona o entidad y su clave pública.
El certificado digital, por tanto, **permite identificar a su titular de forma inequívoca.**

La identificación mediante un certificado digital tiene la misma validez que la presentación del DNI en la atención presencial, por lo que los trámites que realice mediante certificado digital tienen la misma eficacia jurídica que los que realice de forma presencial.

Los certificados digitales sólo tienen utilidad si los respalda una Autoridad Certificadora (Certification Authority o CA) que los valide.

TIPOS DE CERTIFICADOS DIGITALES

- **Certificados de firma electrónica (identifican persona física):** permite firmar identificándonos como persona física para, por ejemplo, manifestar consentimiento o no repudio o se identifique en el entorno digital. Recordemos que **sólo las personas físicas tienen la capacidad de firmar documentos.**
- **Certificados de sello electrónico (identifica persona jurídica)**: permite sellar documentos autenticándose como entidad jurídica, pero sin estar respaldado por su representante legal. Por lo tanto, **con este certificado sellamos documentos que no requieran de una representación legal**. Ejemplo de uso típico: la factura electrónica, que no requiere para su sellado de la firma de un representante legal o apoderado.
  Una persona jurídica no firma, puede sellar, y sin su representante legal no puede firmar
- **Certificados de autenticación web:** son de uso casi universal en la navegación web, vienen representados por el icono del candado cerrado en la barra de navegación.

TIPOS DE CERTIFICADOS DIGITALES EN FUNCIÓN DEL SOPORTE

En función del soporte, podemos hablar de dos tipos de certificados digitales:

- **Certificado de tarjeta** o chip, en el cual el certificado electrónico se halla contenido en una tarjeta criptográfica, como es el caso del DNI electrónico o **DNIe**
- **Certificado software**, que es un fichero digital que emite una autoridad de certificación (como el certificado emitido por la Fábrica Nacional de Moneda y Timbre o FNMT), y cuyo soporte físico se halla en el propio ordenador de la persona usuaria o en el dispositivo en que se encuentre respaldado como copia de seguridad.

En realidad, más que dos tipos son dos formas de trabajar con los certificados: el certificado software (por ejemplo, el de la FNMT) nos ofrece una mayor versatilidad puesto que es un archivo que nos descargamos, del cual podemos tener una copia de seguridad y que podemos importar y exportar en cualquier ordenador que utilicemos.
El DNIe no deja de ser una tarjeta que llevamos con nosotros y que porta un chip en cuyo interior están los certificados digitales protegidos por un PIN de seguridad

La mayoría de las páginas web en las que tenemos que hacer trámites funcionan tanto con el certificado de la FNMT como con el DNIe.
Entonces, ¿cuál utilizaremos en cada ocasión? Pues muy sencillo: el que nos resulte más cómodo.

CERTIFICADOS ADMITIDOS POR LAS ADMINISTRACIONES

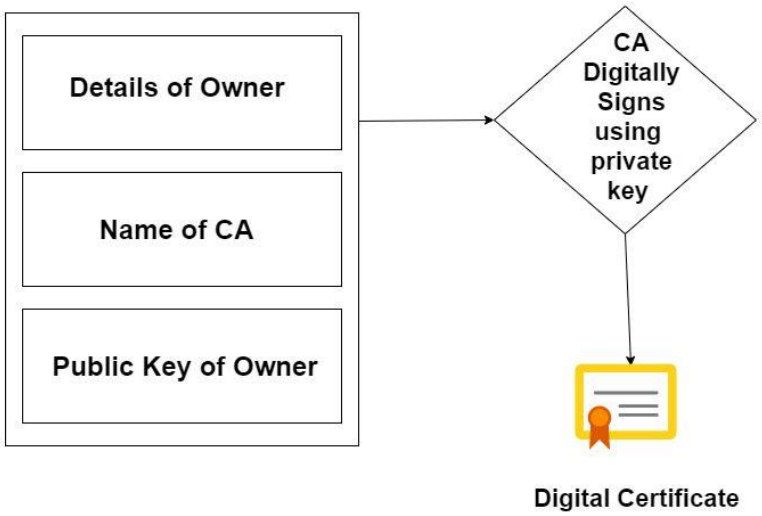
De acuerdo con la Ley 11/2007, de Acceso Electrónico de los Ciudadanos a los Servicios Públicos (LAECSP) y la Ley 59/2003, de Firma Electrónica, los tipos de certificados admitidos son:

- certificado de persona física
- certificado de persona jurídica
- certificado de sello electrónico para la actuación automatizada
- certificado de sede electrónica administrativa
- certificado de empleado público.

¿QUÉ INFORMACIÓN CONTIENE UN CERTIFICADO DIGITAL?

Técnicamente hablando, un certificado digital es una clave pública con cierta información adjunta que, en el caso del estándar X509v3, utilizado por los navegadores, contiene la siguiente información:

- Identificación del titular del certificado: Nombre, dirección, etc.
- Clave pública del titular del certificado.
- Fecha de validez.
- Número de serie.
- Identificación del emisor del certificado.



¿QUÉ ME PERMITE HACER EL CERTIFICADO DIGITAL?

- Autenticar a la persona usuaria
- Permitir la confidencialidad del mensaje
- Salvaguardar la integridad del documento
- El no repudio

DNI ELECTRÓNICO (DNIE)

¿Qué es el DNI Electrónico?
Es un documento emitido por la Dirección General de la Policía que acredita físicamente la identidad de su titular y que, además, permite

- **Acreditar electrónicamente y de forma inequívoca la identidad del titular**
- **Firmar digitalmente documentos electrónicos**, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita

El chip del DNIe contiene los mismos datos de filiación que aparecen impresos en la tarjeta (datos personales, fotografía, firma digitalizada y huella dactilar digitalizada), más los certificados de Autenticación y de Firma Electrónica.

CERTIFICADOS ELECTRÓNICOS EN EL DNIE

Con el DNI electrónico se obtienen dos certificados:

- **Certificado de Autenticación (Digital Signature)**: Garantiza electrónicamente la identidad de la persona física al realizar una transacción telemática.
  Este Certificado asegura que la comunicación electrónica se realiza con la persona que dice ser, con el certificado de identidad y la clave privada asociada al mismo.
- **Certificado de Firma**: Permite la firma de trámites o documentos, sustituyendo a la firma manuscrita. Garantiza pues, la identidad de la persona que suscribe y es poseedora de la clave privada de identificación y firma.

PLAZO DE VALIDEZ DE LOS CERTIFICADOS ELECTRÓNICOS CONTENIDOS EN EL DNIE

Teniendo en cuenta la legislación vigente (que marca el máximo de validez en 60 meses) y con el fin de asumir los objetivos del Esquema Nacional de Seguridad para el aseguramiento e interoperabilidad de las gestiones electrónicas, el plazo de validez de los certificados electrónicos contenidos en el DNI será de 24 meses.

RENOVACIÓN DE LOS CERTIFICADOS DEL DNIE

La renovación es **voluntaria, gratuita y por iniciativa del ciudadano**, y requiere la presencia física de la persona titular del DNI en la oficina de expedición, donde haciendo uso de uno de los puntos de actualización del DNIe habilitados al efecto, y previa comprobación de la identidad mediante el propio DNIe y las plantillas biométricas (huellas dactilares) escaneadas durante el proceso de expedición de la tarjeta del DNIe, se podrán generar, de forma desatendida, los nuevos certificados.

CLAVE DIGITAL

En un Certificado, las claves digitales son los elementos esenciales para la firma e identificación de la persona firmante, y están basadas en la **criptografía de clave pública o asimétrica**, lo que implica que lo que cifra o codifica una clave sólo lo puede descifrar o decodificar exclusivamente la otra

Existen dos claves, **la clave privada** y **la clave pública**, que trabajan de forma complementaria.

La diferencia entre ellas es que la clave privada está pensada para que nunca salga del certificado y esté siempre bajo el control de la persona firmante, que ha de protegerla mediante PIN y no comunicarla nunca a otras personas.
La clave pública, en cambio, ha de ser publicada o comunicada a todas aquellas personas usuarias que quieran comunicarse de modo seguro con la persona propietaria mencionada.

La clave pública se guarda en el certificado electrónico.

AUTORIDAD DE CERTIFICACIÓN

Una **Autoridad de certificación** es una entidad de confianza, responsable de emitir y revocar los certificados digitales utilizados en la firma electrónica, previa comprobación de la identidad de la persona física.
Jurídicamente es un caso particular de Prestador de Servicios de Certificación.
En España existen varias autoridades de certificación o Prestadores de servicios electrónicos de confianza que emiten certificados cualificados.

CERES (CERTIFICACIÓN ESPAÑOLA)

El proyecto CERES es una iniciativa de la Administración liderada por la Fábrica Nacional de Moneda y Timbre (la FNMT). Es una Entidad Pública de Certificación que, utilizando técnicas y sistemas criptográficos de clave pública garantiza:

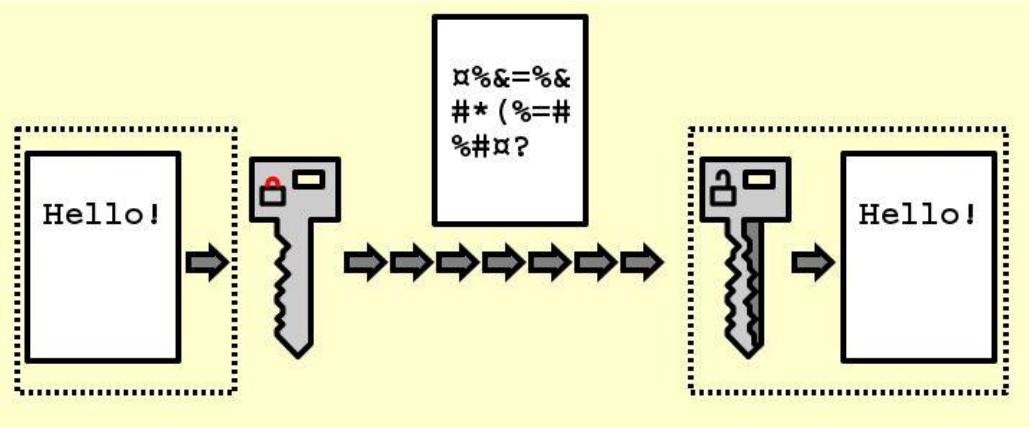
- La **identidad de los usuarios**, tanto ciudadanos como Administraciones Públicas
- La **confidencialidad de las comunicaciones**
- La **integridad de la información digital** intercambiada.

Los certificados electrónicos emitidos por CERES permiten la realización de trámites telemáticos a través de internet con plenas garantías de seguridad, evitando desplazamientos, esperas y errores de cumplimentación de formularios.

Si quieres conocer el Catálogo de servicios de CERES pincha en este **enlace**

CIFRADO O ENCRIPTADO

La encriptación o cifrado es un proceso técnico de seguridad por el cual la información contenida en un mensaje, documento o archivo es transformada de tal manera que su contenido se codifica o enmascara quedando ilegible y permitiendo ocultar los datos que se envían, reciben o almacenan.
A la inversa, la desencriptación o descifrado permite hacer legible una información que estaba cifrada u oculta.



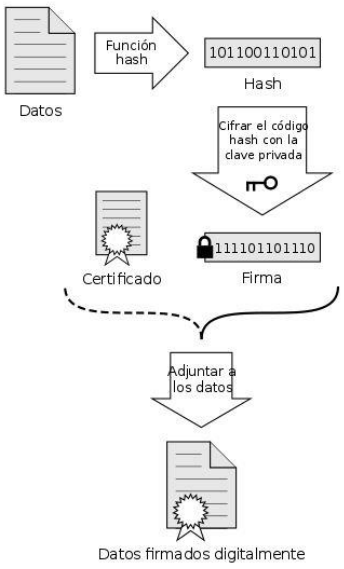
Usando **criptografía de clave pública** el emisor del mensaje cifrará el mensaje aplicando la clave pública del destinatario. Será por tanto el destinatario el único que podrá descifrar el mensaje aplicando su clave privada

FIRMA DIGITAL

Una firma digital es un **conjunto de datos asociados a un contenido o documento** y que **permite asegurar**:

- **la identidad** de la persona firmante
- **la integridad** del fichero o documento

La persona firmante generará un resumen o huella digital del contenido mediante un algoritmo o función hash.
Este resumen o huella digital lo cifrará con su clave privada y como resultado obtenemos lo que denominamos firma digital, que se envía adjunta al mensaje original

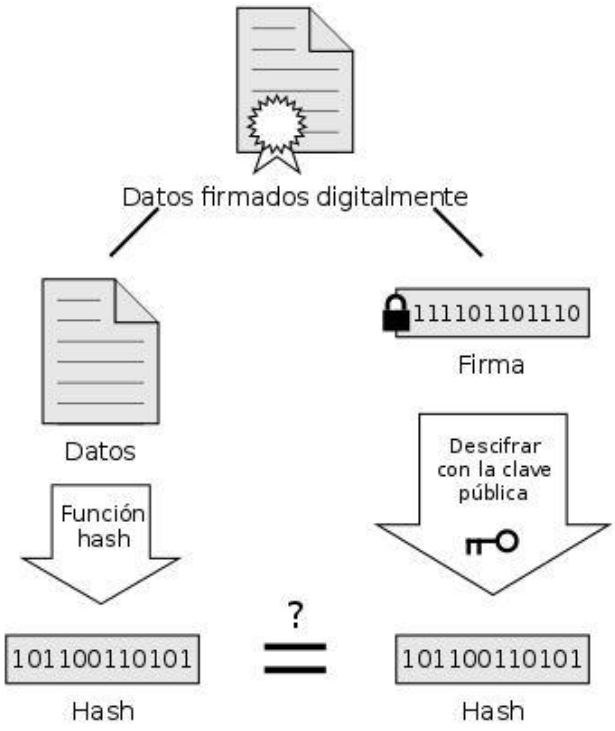


La persona o personas destinatarias del mensaje podrán comprobar que el mensaje no se ha modificado desde su creación porque podrán generar la misma huella digital y, además, podrá comprobar la autoría descifrando la firma digital con la clave pública de la persona firmante, obteniendo como resultado de nuevo la huella digital del mensaje.
La firma digital no implica que el mensaje se haya cifrado

HUELLA DIGITAL

Una huella digital es un **conjunto de datos asociados a un mensaje que permiten asegurar que el mensaje no fue modificado**.

La huella digital o resumen de un mensaje se obtiene aplicando una función -denominada **hash**- a ese mensaje, lo que da como resultado un conjunto de datos singular de longitud fija.



Si los códigos hash coinciden, la firma es válida.

Una *función hash* tiene entre otras las siguientes propiedades:

- Dos mensajes iguales producen huellas digitales iguales.
- Dos mensajes parecidos producen huellas digitales completamente diferentes.

- Dos huellas digitales idénticas pueden ser el resultado de dos mensajes iguales o de dos mensajes completamente diferentes.
- Una función hash es irreversible, no se puede deshacer, por tanto su comprobación se realizará aplicando de nuevo la misma función hash al mensaje.

OBTENCIÓN DEL CERTIFICADO DIGITAL DE PERSONA FÍSICA DE LA FMNT

DESCARGA DEL CERTIFICADO DIGITAL

El certificado digital se descarga de internet y lo instalas en tu ordenador.

Durante el proceso, es muy importante que uses:

- el mismo ordenador
- el mismo navegador
- el mismo usuario.

En lo que respecta al navegador, en la página de la FNMT se indica que puede usarse la última versión de los navegadores más populares:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Opera
- Safari

Sin embargo, nuestra experiencia indica que Safari suele dar algunos problemas, mientras que Firefox presenta la particularidad de que guarda los certificados digitales en su propio almacén de certificados, lo que dificulta su uso por parte de otras aplicaciones.

Por todo esto, te recomendamos **usar preferentemente Chrome o Edge** para trabajar con tus certificados digitales.

OBTENER EL CERTIFICADO DIGITAL DE LA FNMT

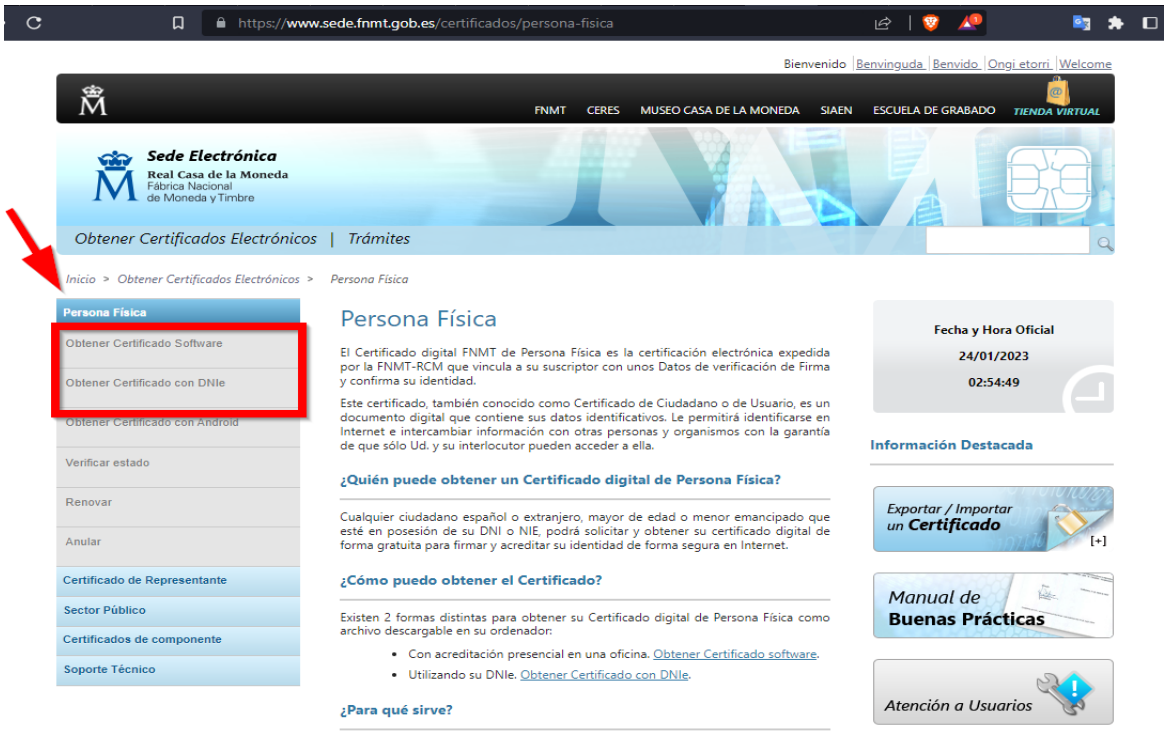
PROCESO DE OBTENCIÓN DEL CERTIFICADO DIGITAL DE LA FNMT

Para iniciar el proceso de obtención de tu certificado digital personal de la FNMT, en primer lugar, entra en la página de la sede electrónica de la FNMT, el proyecto CERES (CERtificación ESpañola):

Y pincha en el apartado 'Obtenga/Renueve su certificado Ciudadano'

La siguiente pantalla es la de obtención del certificado para persona física.

Aquí te informa de algunos aspectos interesantes del certificado electrónico de persona física: como quién lo puede obtener, los dos posibles métodos de obtención del certificado y un listado de sus usos.



De todo el contenido de la página, destacaríamos dos apartados:

¿QUIÉN PUEDE OBTENER UN CERTIFICADO DIGITAL DE PERSONA FÍSICA?

Cualquier ciudadano español o extranjero, mayor de edad o menor emancipado que esté en posesión de su DNI o NIE (Número de Identidad de Extranjero).

¿CÓMO PUEDO OBTENER EL CERTIFICADO?

Hay dos formas distintas de obtener el Certificado Digital de Persona Física descargable en tu ordenador:

1. Personándote presencialmente en una oficina (principalmente de la Agencia Tributaria o de la Seguridad Social) para identificarte
2. Utilizando el DNIe

Ambos procesos son, en líneas generales, muy similares. La principal diferencia entre ambas opciones es que en el primer caso debes acudir presencialmente a una oficina (de la Agencia Tributaria o de la Seguridad Social) para acreditar tu identidad, cosa que no es necesaria si dispones de

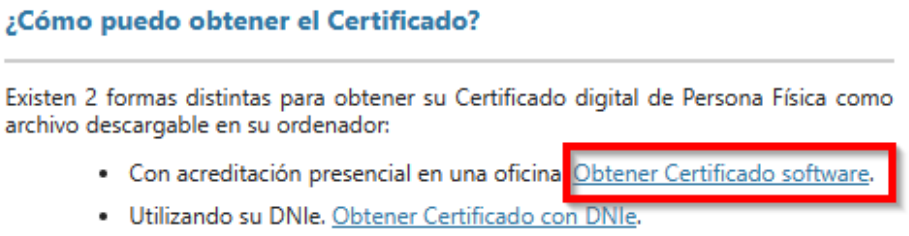
DNIe con sus certificados válidos, puesto que el proceso será enteramente telemático y sin necesidad de acudir a ninguna oficina

.

OBTENCIÓN DEL CERTIFICADO SOFTWARE PASO A PASO

Te vamos a documentar la opción de 'Obtener Certificado Software' porque su obtención es algo más farragosa que la opción de 'Obtener certificado con DNIe'.

Pulsa en la opción de '***Obtener Certificado software***'



En la siguiente pantalla, tienes detallados los 4 pasos necesarios para obtener tu certificado digital:

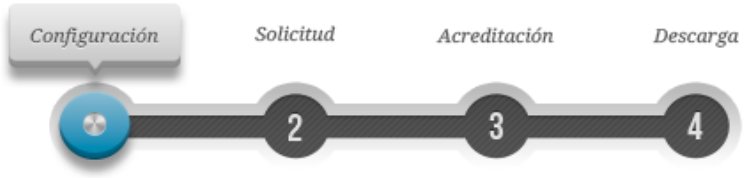
Obtener Certificado software

El proceso de obtención del Certificado software (como archivo descargable) de usuario, se divide en cuatro pasos que deben realizarse en el orden señalado:

1. **Configuración previa.** Para solicitar el certificado es necesario instalar el software que se indica en este apartado.
2. **Solicitud vía internet de su Certificado.** Al finalizar el proceso de solicitud, usted recibirá en su cuenta de correo electrónico un Código de Solicitud que le será requerido en el momento de acreditar su identidad y posteriormente a la hora de descargar su certificado.
3. **Acreditación de la identidad en una Oficina de Acreditación de Identidad.** Una vez completada la fase anterior y esté en posesión de su Código de Solicitud, para continuar con el proceso deberá Acreditar su Identidad en una de nuestras Oficinas de Acreditación de Identidad.
   Para su comodidad, puede usted hacer uso de nuestro servicio LOCALIZADOR DE OFICINAS.

   NOTA: En las oficinas de la AEAT, Seguridad Social y en otras oficinas se requiere de cita previa, consulte con la propia oficina.
4. **Descarga de su Certificado de Usuario.** Aproximadamente 1 hora después de que haya acreditado su identidad en una Oficina de Acreditación de Identidad y haciendo uso de su Código de Solicitud, desde aquí podrá descargar e instalar su certificado y realizar una copia de seguridad (**RECOMENDADO**).

Comienza por el primer punto:



1. Configuración previa

Antes de comenzar con el proceso de solicitud del certificado, has de instalar la aplicación CONFIGURADOR FNMT-RCM; para usuarios o usuarias de Windows. La versión a descargar es la de 64bits en la inmensa mayoría de ocasiones.

IMPORTANTE: introducir una dirección de correo electrónico a la que puedas acceder ya que allí se te enviará el Código de Solicitud necesario para acreditar tu identidad presencialmente.

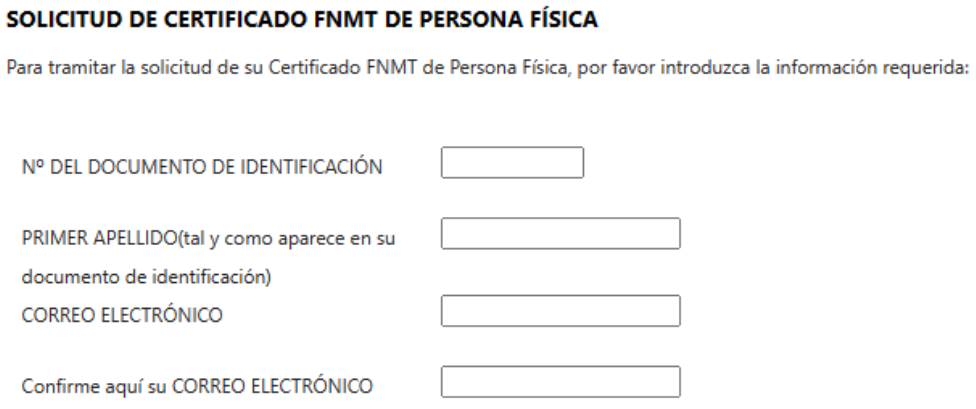
Hay que realizar todo el proceso de petición desde el mismo equipo y el mismo usuario.

No hay que formatear el ordenador entre el proceso de solicitud y el de descarga del certificado.

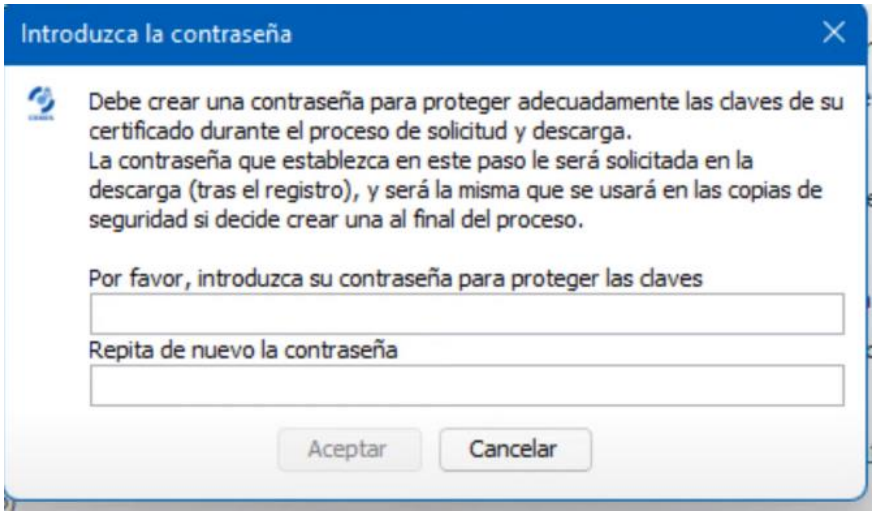
Instalar la aplicación es trivial, no presenta dificultad reseñable.

Una vez instalada la aplicación, pasa a realizar la solicitud del certificado.

Importante escribir correctamente tu dirección de correo electrónico, ya que es allí donde más tarde recibirás el código



Al pinchar en ‘Enviar Petición’, el programa instalado al principio (el configurador FNMT-RCM) te abrirá una ventana pidiendo que introduzcas una contraseña para proteger tu certificado.



Esta contraseña es importante porque, sin ella, no podrás recuperar tu certificado. A continuación, la aplicación pasa a gestionar tu cita presencial en una oficina de la AEAT o de la SS.

3. Acreditar Identidad

Ya puedes acudir a una oficina de acreditación de la identidad, previa petición de cita.

Si eres ciudadano o ciudadana española, debes llevar:

- Código de Solicitud: el que enviaron a tu correo
- DNI, pasaporte o carnet de conducir (válidos, vigentes y en formato original o en fotocopia compulsada).

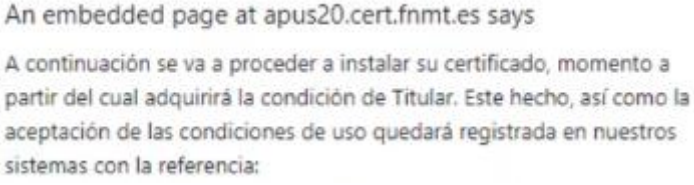
4. Descargar Certificado

Una vez hayas acudido a identificarte a una oficina, en el plazo aproximado de una hora, ya podrás proceder a descargar en tu ordenador el certificado digital.

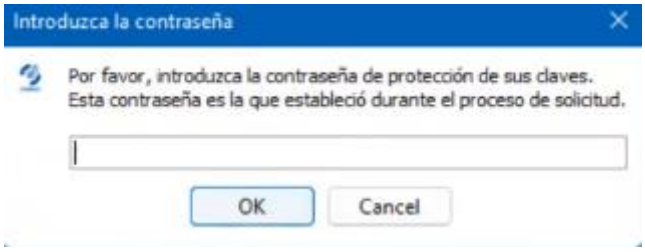
Desde la página de obtención del certificado, rellena el formulario con tu DNI: primer apellido y el código de solicitud que te enviaron al correo. No olvides aceptar las condiciones.

Una vez esté todo correcto, pincha en el botón de 'Descargar Certificado'.

El navegador te da un aviso de que se va a instalar el certificado, momento a partir del cual obtendrás la condición de Titular y podrás utilizarlo.

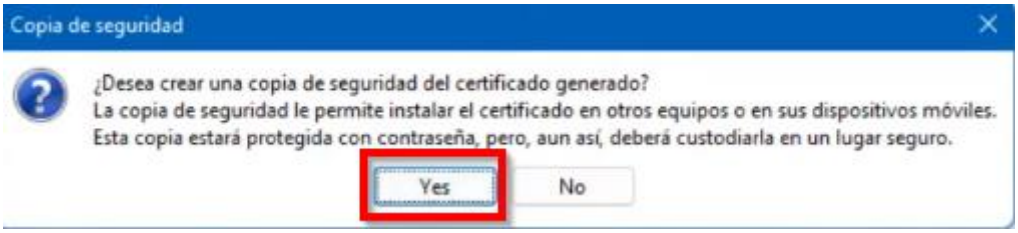


Después, tendrás que introducir exactamente la misma clave que introdujiste al solicitar el certificado. Si no la introduces correctamente, no podrás bajarte el certificado.



Una vez introducido el código, se inicia el proceso de generar el certificado.

Te saldrá otro aviso preguntándote si quieres realizar una copia de seguridad del certificado generado:



La copia de seguridad es muy importante para poder conservar tu certificado digital, instalarlo en otros ordenadores que uses o simplemente asegúrate poder usarlo en tu equipo principal si fuera necesario formatearlo o perdieras los datos.

Al dar tu conformidad, te saldrá un cuadro de diálogo para guardar el archivo con extensión .p12 donde desees.

ALGUNOS VIDEOTUTORIALES

A continuación, te sugerimos algunos vídeos que podrán ilustrarte en todo lo visto anteriormente

-Tutorial: obtener certificado digital FNMT 2022 (España)

-Tutorial: Cómo instalar BIEN tu certificado digital personal de la FNMT (en Windows)

-Tutorial: Obtención del Certificado Digital con DNIe sin cita previa

GESTIÓN DE LOS CERTIFICADOS DIGITALES

Los certificados digitales, una vez obtenidos, precisan ser **gestionados con diligencia** para que cumplan con eficiencia su principal función: **identificarnos en el mundo digital de forma inequívoca**.

Para ello, debes conocer qué pasos dar en cada momento del ciclo de vida del certificado.

Los certificados pueden **renovarse** antes de su fecha de expiración para así poder seguir usándolos sin tener que repetir todo el proceso de petición, pero también pueden ser **revocados** si sospechas que está en riesgo la seguridad del certificado, o por toda una serie de circunstancias que comentaremos cumplidamente.
Por último pero no por ello menos importante: debes **guardar** siempre a buen recaudo una copia de tu certificado para poder reinstalarlo por problemas técnicos o por si necesitaras instalarlo en más ordenadores.

VALIDACIÓN

¿QUÉ ES LA VALIDACIÓN DE UNA FIRMA ELECTRÓNICA?

Es el proceso por el cual se comprueba:

- La **identidad** de la persona firmante
- La **integridad** del documento firmado
- La **validez temporal** del certificado utilizado

Puesto que en el proceso de la firma electrónica la persona firmante utiliza la clave privada de su certificado electrónico, puedes verificar los dos primeros puntos desde una aplicación sin conexión a internet utilizando el certificado incluido en la misma firma.

Sin embargo, el proceso de validación de la firma no puede separarse del proceso de validación del certificado usado para la firma. Y por eso, la validación de la firma implica también la validación del certificado.

¿QUÉ NECESITAMOS SABER DE UN CERTIFICADO DIGITAL?

- Que es **válido**
- Que **no está revocado** en el momento de la firma
- Que la **autoridad certificadora** que lo emitió **es de confianza**

El certificado electrónico solamente se puede validar mientras esté **activo**, ya que una vez caducado desaparece de las listas de revocación de la Autoridad de Certificación y ya no se puede comprobar cuál era el estado en el momento de la firma.

Si el certificado no es válido, o está caducado o revocado, la firma no puede ser validada correctamente puesto que no podemos saber cuál era el **estado del certificado** en el momento de la firma.

Por tanto, las tres validaciones dependen de la capacidad de validar el certificado, para lo cual es necesaria una conexión a internet que permita acceder a una plataforma de validación de certificados.

PLATAFORMAS DE VALIDACIÓN

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

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

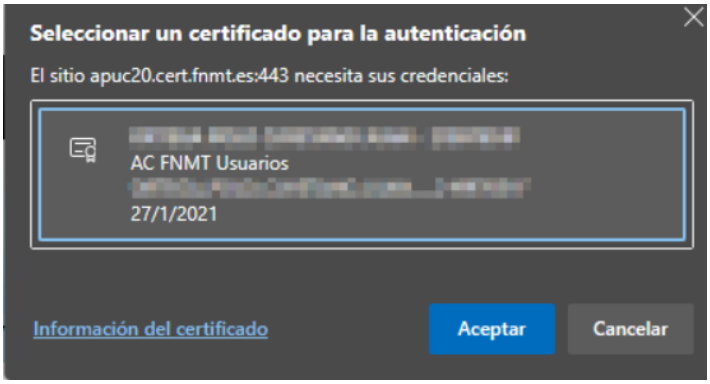
La información sobre los Certificados electrónicos revocados (no vigentes) se almacena en las denominadas listas de revocación de certificados (CRL) mantenidos por las Autoridades de Validación.

La validación o verificación del estado de un certificado se puede realizar a través de internet accediendo al servicio que proporciona las Autoridad de Validación o de Certificación que ha emitido el certificado.

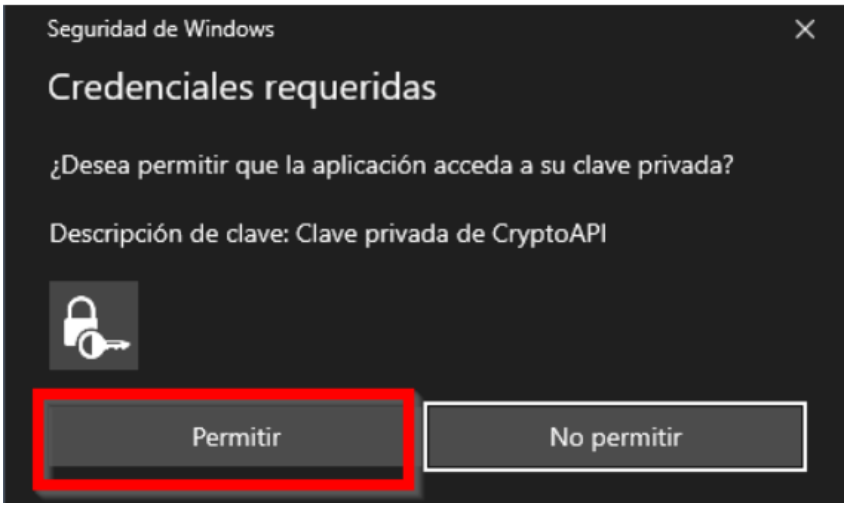
VALIDACIÓN A TRAVÉS DE LA PÁGINA DE LA FNMT

Por ejemplo, para el caso de los certificados emitidos por la FNMT, puedes verificar si el certificado digital personal de la FNMT es válido o ha sido revocado accediendo a la página https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado

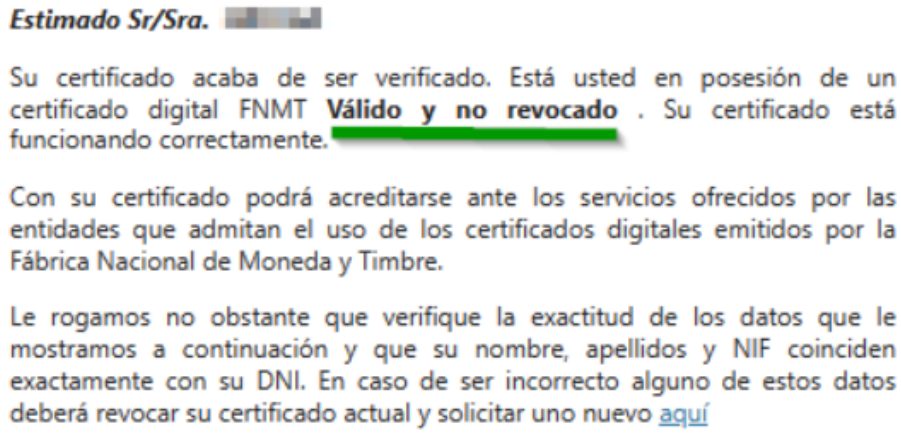
Pincha en 'Solicitar verificación', en un navegador en el que tengas instalado el certificado de la FNMT. Se te abrirá una ventana en la que podrás seleccionar el certificado de la FNMT que desees para su autenticación; como sólo tienes el de persona física, no aparecerá ninguno más:



Una vez aceptes, te sale la información de que vamos a utilizar tu certificado. Como siempre, lo permites



Esperas unos momentos hasta que la página te ofrece el resultado:



Estimado Sr/Sra. [redacted]

Su certificado acaba de ser verificado. Está usted en posesión de un certificado digital FNMT **Válido y no revocado** . Su certificado está funcionando correctamente.

Con su certificado podrá acreditarse ante los servicios ofrecidos por las entidades que admitan el uso de los certificados digitales emitidos por la Fábrica Nacional de Moneda y Timbre.

Le rogamos no obstante que verifique la exactitud de los datos que le mostramos a continuación y que su nombre, apellidos y NIF coinciden exactamente con su DNI. En caso de ser incorrecto alguno de estos datos deberá revocar su certificado actual y solicitar uno nuevo aquí

Te informa de que tu certificado es válido y no ha sido revocado, y te ofrece además información adicional personal y técnica:

Información sobre la identidad (valores personales)

Identificador	Valor
Nombre	[redacted]
Primer apellido	[redacted]
Segundo apellido	[redacted]
NIF	[redacted]
Dirección de correo electrónico	

Información sobre las claves (valores técnicos)

Identificador	Valor
Número de serie del certificado	[redacted]
Autoridad emisora	CN=AC FNMT Usuarios, OU=Ceres, O=FNMT-RCM, C=ES
Propietario	[redacted]
Comienzo de la validez del certificado	27 enero 2021 06:07:40
Fin de validez del certificado	27 enero 2025 06:07:40

Como has visto, los certificados emitidos por la FNMT pueden verificarse muy fácilmente a través de la propia FNMT, que ejerce tanto de Autoridad de Certificación como de Autoridad de Validación. Si dispones de un certificado emitido por otra entidad pública, puedes validarlo a través de la plataforma VALIDe.

VALIDACIÓN A TRAVÉS DE LA PLATAFORMA VALIDE

Accede al servicio de VALIDe a través de la siguiente URL:

https://valide.redsara.es/valide/inicio.html

*<<**VALIDe** es una aplicación de **VALI**dación de firma y certificados online y **De**mostrador de servicios de @firma.*

VALIDe permite:

- determinar la validez de firmas y certificados digitales
- generación y validación de firmas electrónicas
- demostración de servicios web de @firma

¿QUÉ CERTIFICADOS SON RECONOCIDOS POR LA PLATAFORMA?

La plataforma @firma admite certificados digitales reconocidos conforme el estándar ITU-T X.509 v3, emitidos por múltiples prestadores de servicios de certificación.

Para validar tu certificado, pincha en la sección ‘Validar Certificado’, desde donde pasas a la siguiente página:

RENOVACIÓN

RENOVACIÓN DE LOS CERTIFICADOS DIGITALES

Los certificados electrónicos tienen un periodo de validez, pasado el cual no pueden usarse ni para firmar ni para identificarse. El certificado queda invalidado el mismo día que indica la fecha de expiración.

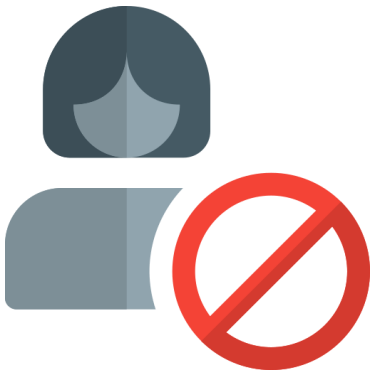
Cada Autoridad de Certificación establece unos plazos determinados antes de que el certificado caduque para poder renovarlos sin necesidad de otra identificación. Es importante saber que todo el proceso de renovación de un certificado, desde la solicitud de renovación hasta la descarga final, ha de realizarse desde el mismo navegador en el que se encuentra instalado.

Por otra parte, dependiendo de la autoridad certificadora y del tipo de certificado, éste podrá o no ser renovado de forma telemática.
Hay que tener en cuenta que, si el certificado caduca, hay que volver a realizar íntegramente todo el proceso de solicitud del certificado.
En el caso de la FMNT, únicamente se permite la renovación de los certificados de persona física y de representante para administradores únicos y solidarios.

REVOCACIÓN

REVOCACIÓN DE LOS CERTIFICADOS DIGITALES

La anulación o revocación de los certificados digitales **permite anular la validez de los mismos antes de su fecha límite** de caducidad.
La revocación puede ser solicitada en cualquier momento, y en especial, cuando la persona titular sospeche que sus claves privadas sean conocidas por otros, cuando sospeche que su certificado puede haber sido copiado, que su PIN sea conocido, en caso de extravío o, en general, cuando se planteen dudas acerca de su seguridad.



PRINCIPALES CAUSAS DE REVOCACIÓN DE UN CERTIFICADO DIGITAL

- Solicitud voluntaria de la persona suscriptora.
- Pérdida o daños en el soporte del Certificado.
- Fallecimiento de la persona suscriptora o de su representado, incapacidad sobrevenida, total o parcial, de cualquiera de ellos.
- Finalización de la representación o extinción de la entidad representada.
- Inexactitudes en los datos aportados por la persona suscriptora para la obtención del certificado.
- Que se detecte que las claves de la persona suscriptora o de la Autoridad de Certificación han sido comprometidas.

Una vez revocado, el certificado ya no puede ser reactivado y es necesario volver a iniciar todo el proceso de solicitud.
Por otra parte, cualquier firma digital realizada con la clave privada asociada a ese certificado con posterioridad a la fecha efectiva de revocación no tendrá validez.

El procedimiento para la revocación de los certificados deberá ser documentado por cada Autoridad Certificadora, usualmente a través de su página web.

REVOCACIÓN CERTIFICADO FNMT

A modo ilustrativo, en el Portal Administración Electrónica se citan las tres formas de revocación de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT):

- A través de **Internet**: si el titular del certificado o su representante, en caso de entidades, están en posesión del mismo.
- En la **Oficina de Acreditación**: si el titular del certificado o representante no disponen del mismo por extravío, pérdida o robo, deberá personarse en una de estas Oficinas de Acreditación para, una vez identificado, firmar el modelo de solicitud de revocación del certificado. Las Oficinas de Acreditación transmiten diariamente los registros tramitados a la FNMT para que ésta proceda a la revocación del certificado.

- **Por teléfono**: 902 200 616. Esta opción únicamente deberá utilizarse en aquellos casos en que no pudieras desplazarte a una Oficina de Acreditación o no fuera posible revocar el certificado de manera online.

REVOCACIÓN CERTIFICADO DNIE

En el caso del DNIe, la persona interesada debe **personarse en cualquier Oficina de Expedición del DNIe** para revocar el Certificado.

La revocación del mismo es inmediata a la tramitación de cada solicitud verificada como válida.

ALMACENAMIENTO

ALMACENAMIENTO DE LOS CERTIFICADOS DIGITALES

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

Los certificados digitales se guardan en determinadas ubicaciones predeterminadas, conocidas genéricamente como ***"Almacén de certificados"***, que varían en función del sistema operativo de tu ordenador.

- En **Windows,** la ubicación predeterminada es precisamente el ***Almacén de Certificados***
- En **macOS**, los certificados se guardan en el **llavero**, en su correspondiente categoría *'Mis certificados'.*

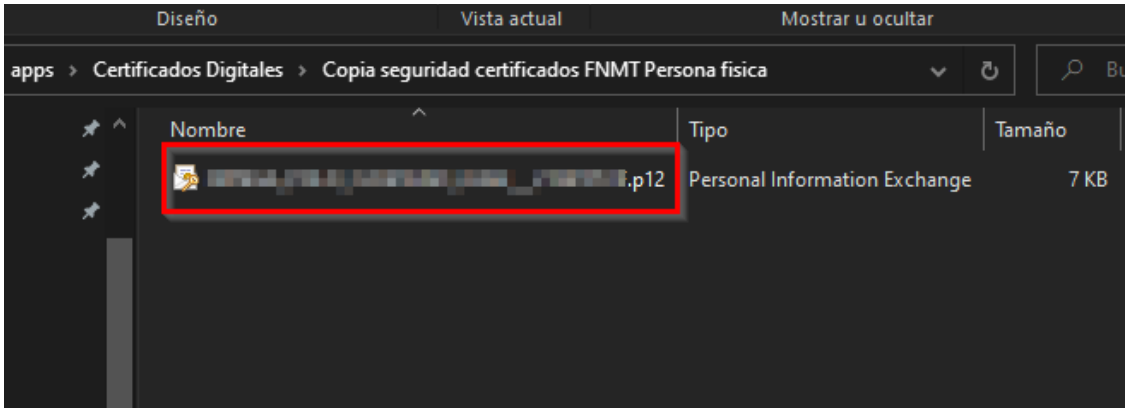
- En **Linux**, la ubicación predeterminada para instalar certificados es / etc / ssl / certs, lo que permite que los diversos servicios puedan utilizar el mismo certificado sin demasiadas complicaciones de permisos de archivo.

En el caso de los **certificados contenidos en una tarjeta digital,** como es el caso del DNIe, **la propia tarjeta** es el almacén de los mismos.

IMPORTACIÓN E INSTALACIÓN DE CERTIFICADOS

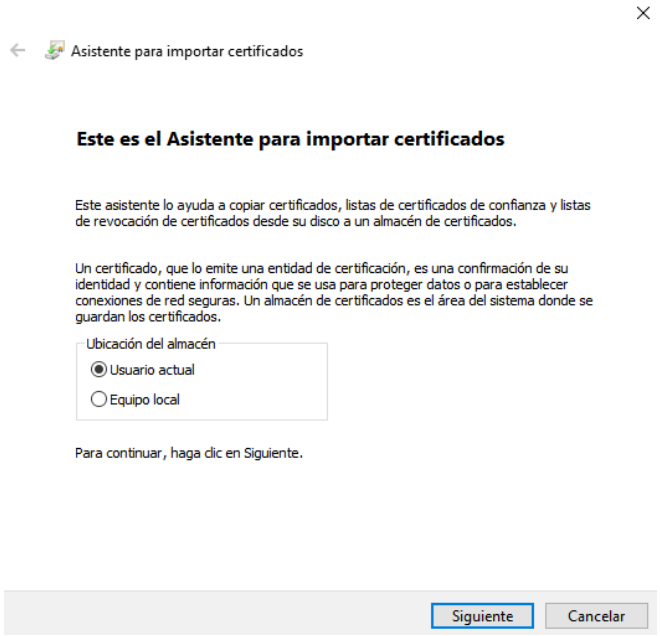
INSTALACIÓN DE TU CERTIFICADO DIGITAL PERSONAL

Los archivos que contienen tu certificado digital personal suelen tener las extensiones .p12 o .pfx, así que, para instalar tu certificado digital personal en nuestro ordenador, primero has de localizar con el explorador de archivos de windows la copia de seguridad del certificado

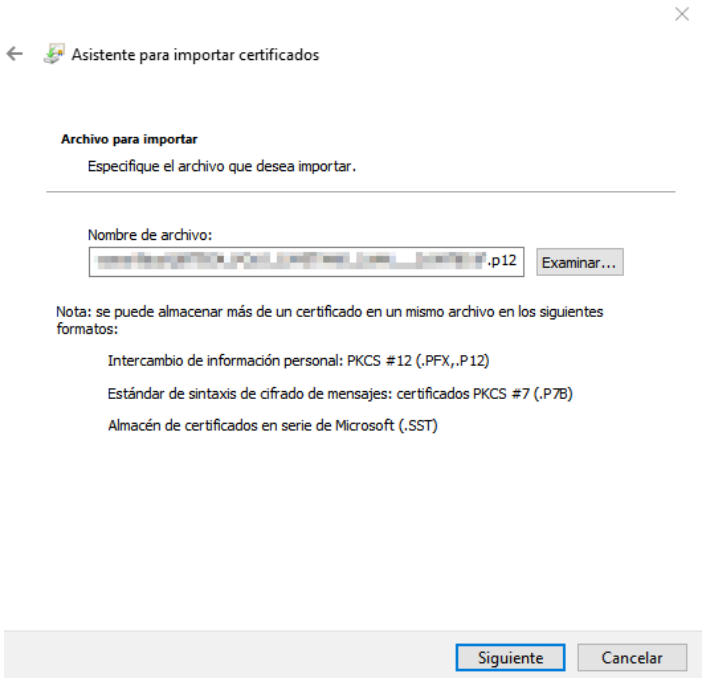


Para instalarlo en el equipo, simplemente haz doble click sobre él, con lo cual se lanzará el asistente para importar certificados que te guiará en los diversos pasos necesarios para instalar el certificado.

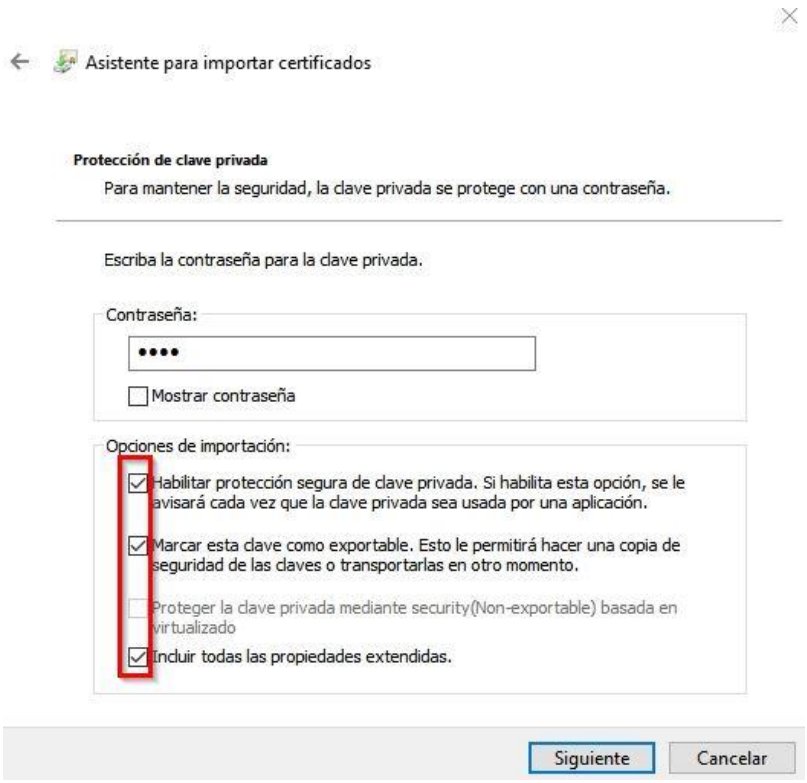
El primer paso es elegir la ubicación del almacén en que se instalará el certificado; puesto que se trata de un certificado personal, siempre elige el almacén del usuario actual.



A continuación te informa de la ruta donde está el archivo y de unos aspectos técnicos (que son meramente informativos)



Avanza al siguiente paso, donde tienes que elegir las opciones de la importación, algunas de ellas son importantes



En primer lugar, debes de introducir la contraseña que utilizas para generar el certificado. Si no la tienes, el certificado no te sirve de nada puesto que no podrás usarlo.

En cuanto a las opciones de importación del certificado, tienes:

HABILITAR PROTECCIÓN SEGURA DE CLAVE PRIVADA.

Si lo marcas, cada vez que se vaya a usar el certificado digital en este ordenador, te va a informar y te va a pedir permiso (incluso con clave). Esto es importante porque si cualquier programa malicioso pretende hacer uso del certificado, vas a verlo y se lo puedes impedir.

MARCAR ESTA CLAVE COMO EXPORTABLE

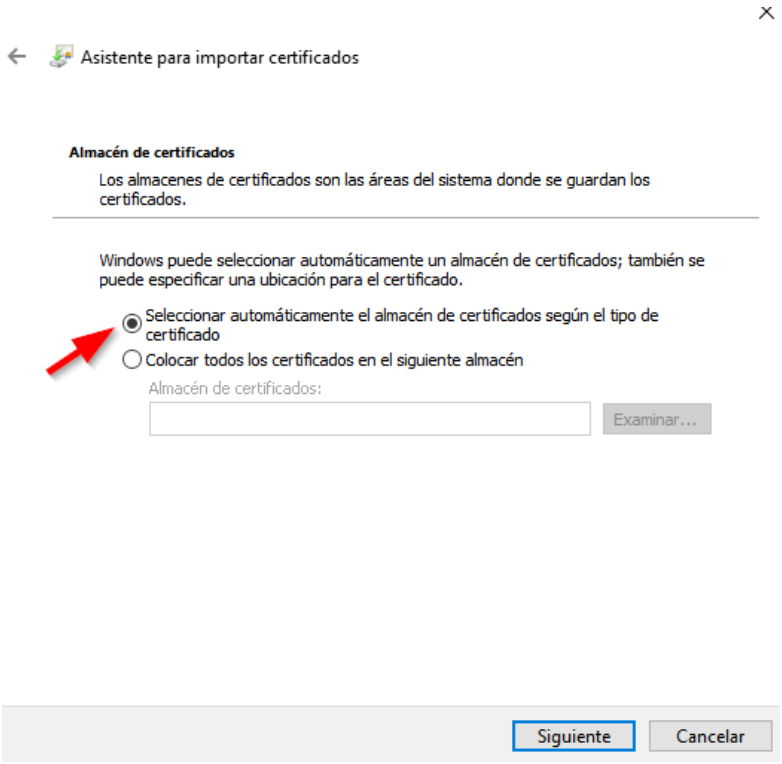
Permite hacer una copia de seguridad de la clave privada o exportarla para que, en el caso de que perdieras el archivo .p12 original, puedas generar otro para usar tu certificado en otros equipos, si así fuera necesario.

INCLUIR TODAS LAS PROPIEDADES EXTENDIDAS

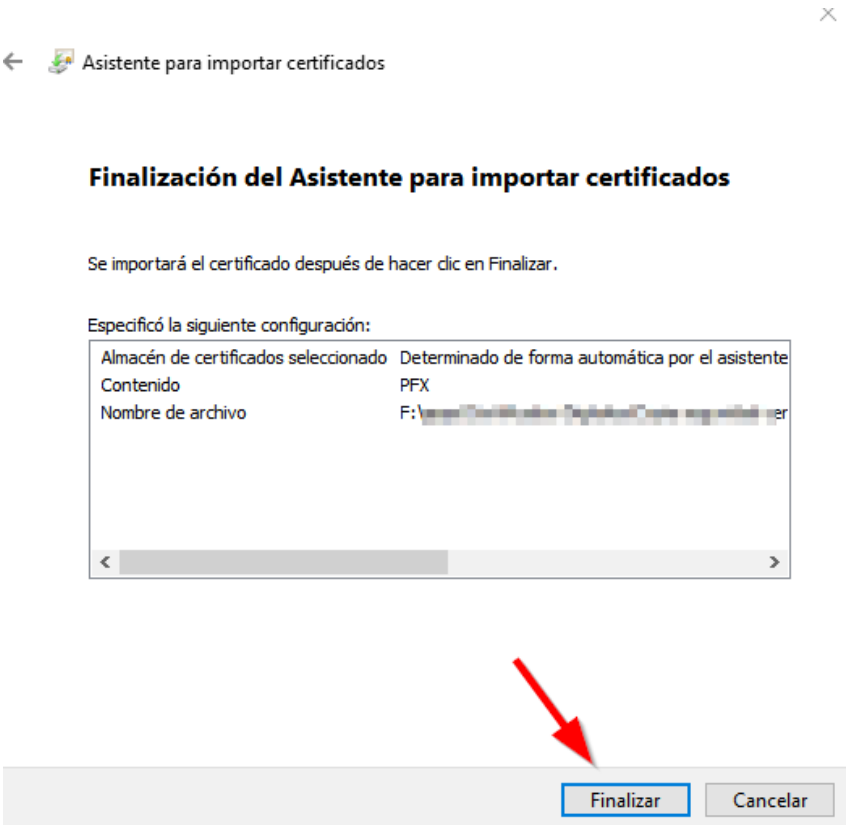
Lo marcarás también porque además del certificado te va a instalar también el certificado raíz de la FNMT en el caso de que no lo tuvieras.

El certificado raíz lo que va a permitirte es que windows reconozca estos certificados y los gestione sin problemas.

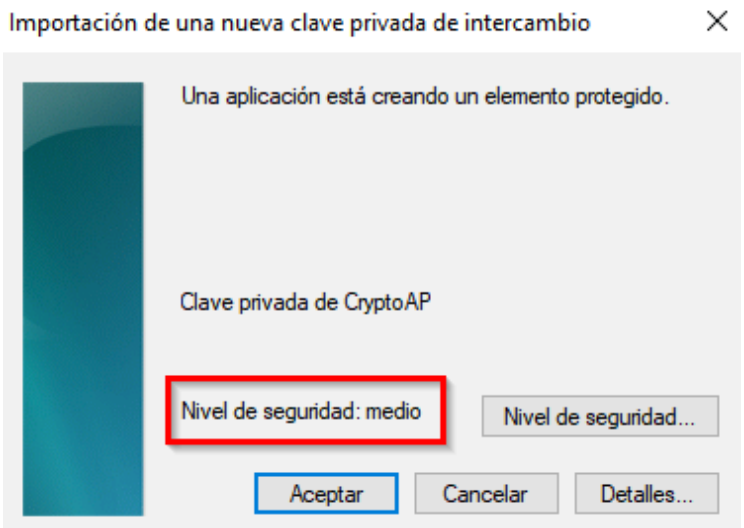
El siguiente paso permite que los certificados se guarden en la ubicación por defecto que te ofrece el sistema o en una nueva que elijas. Deja la opción de selección automática.

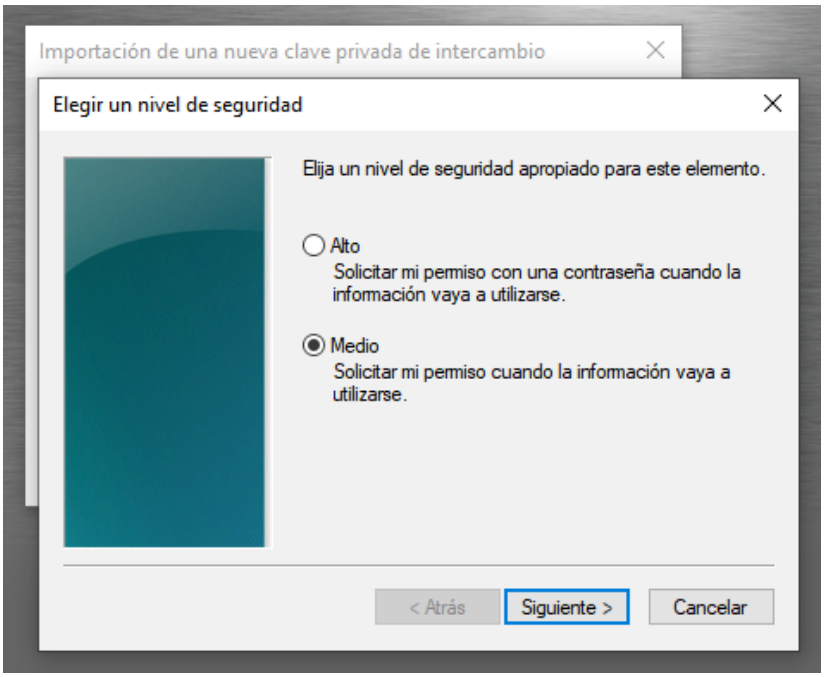


Por último, tienes la finalización del Asistente para importar certificados

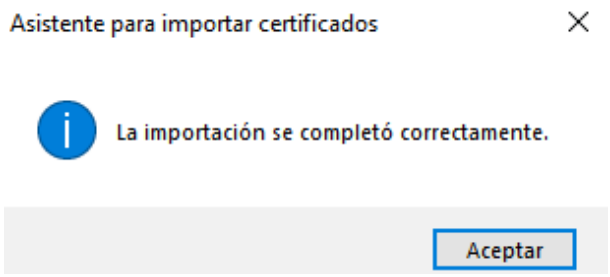


Lo siguiente que te aparece es la opción de importación de una nueva clave privada de intercambio; esto obedece a que has marcado la opción de proteger el acceso al certificado. Elige el nivel de seguridad medio, en el cual cada vez que el certificado vaya a usarse, el sistema te pedirá nuestra conformidad.





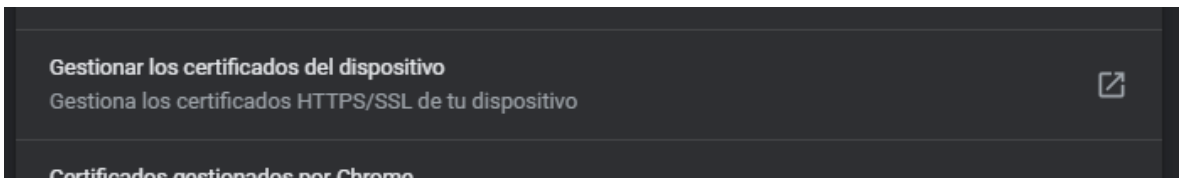
Para finalizar, te da una advertencia de seguridad de que va a instalar un certificado de una entidad de certificación (CA) que afirma representar a AC RAIZ FNMT-RCM



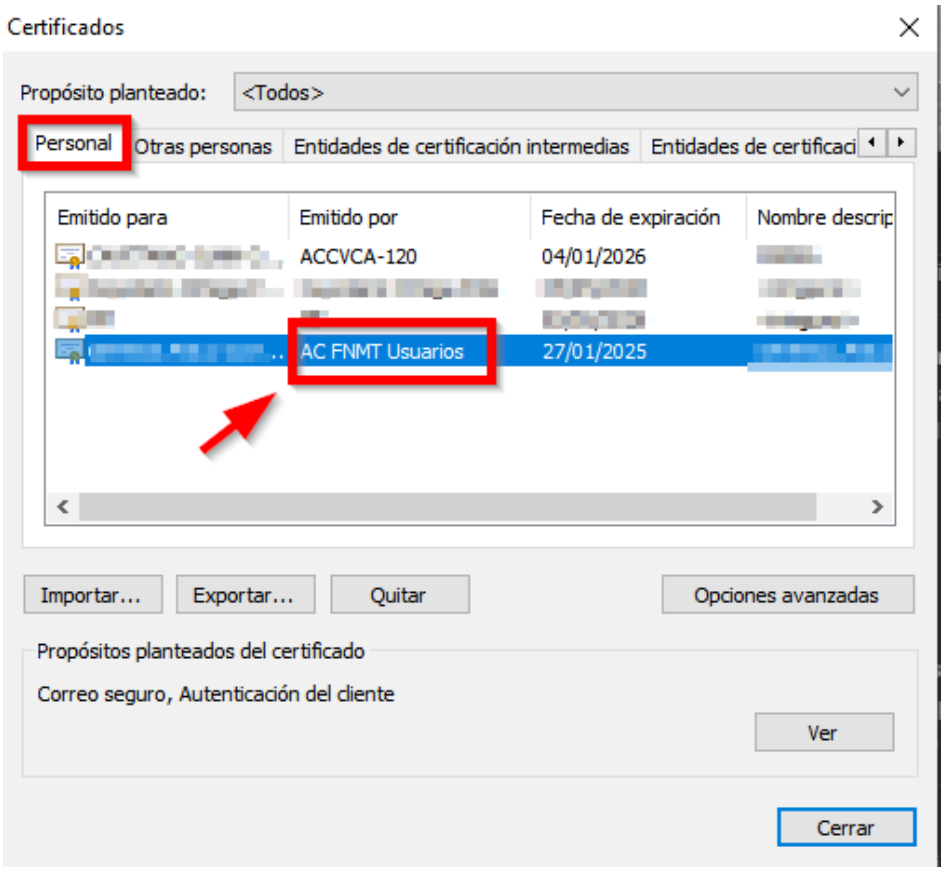
Por último, comprueba que el certificado esté correctamente instalado.

Desde Chrome, accede a

Configuración > Privacidad y Seguridad > Gestionar los certificados del dispositivo



Se te abrirá una ventana donde puedes ver qué certificados tienes instalados:



Entre otros, tienes instalado el certificado digital personal de la FNMT, y su fecha de expiración.

VIDEOTUTORIALES

-Tutorial: Certificado Digital, importación y exportación

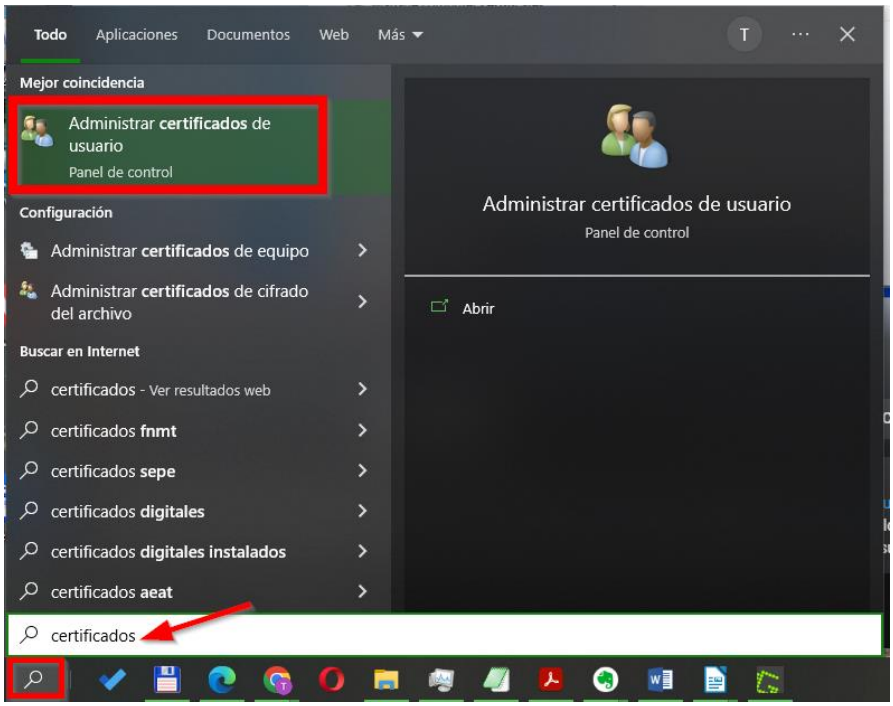
-Tutorial: Certificado Digital: solicitud, revocación y uso

EXPORTACIÓN Y BACKUP DE CERTIFICADOS

CÓMO HACER UN BACKUP DE TU CERTIFICADO DIGITAL PERSONAL (FNMT)

Con este procedimiento, puedes exportar tu certificado digital de la FNMT por si quieres instalarlo en otro ordenador, o guardarlo como copia de seguridad.

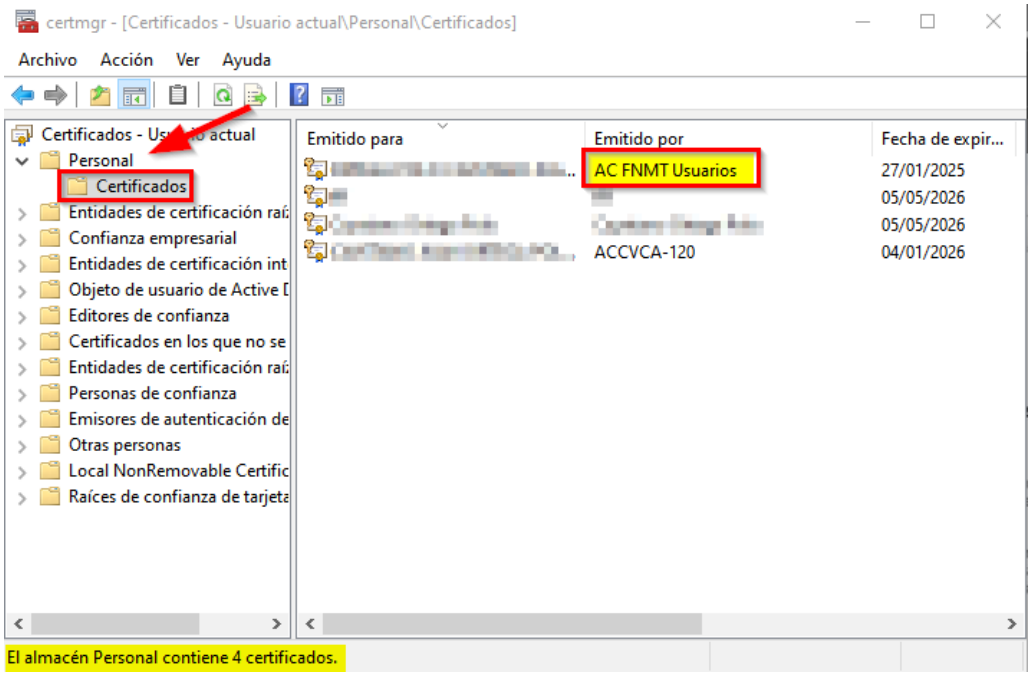
Partimos de la base de que tienes el certificado digital correctamente instalado. Si es así, ve a la búsqueda del sistema y escribe 'certificados'



Elige la opción de ‘Administrar certificados de usuario’

Al clicar sobre la opción, se te abre una ventana con los certificados del usuario actual. En la parte inferior izquierda te indica que el almacén personal contiene 4 certificados; si no tuvieras ningún certificado instalado, también te lo indicaría.

Elige la carpeta ‘Personal’ y, al desplegarla, verás los certificados que tienes instalados en el ordenador.

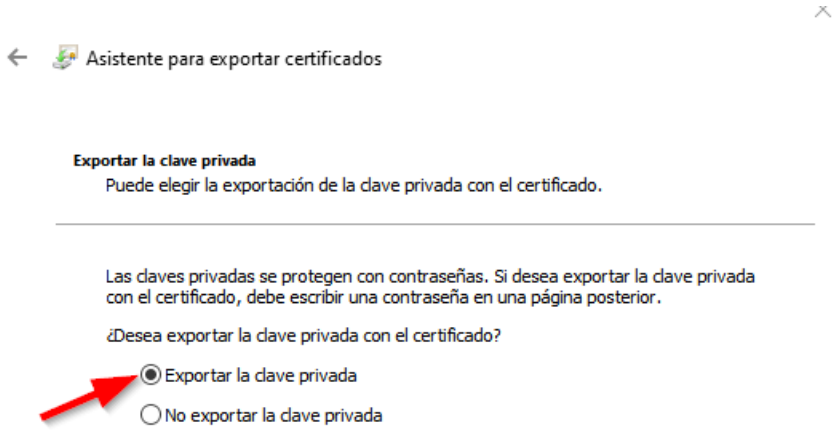


Elige aquél que quieras exportar o hacer una copia de seguridad (en tu caso, el de la FNMT), y, con el botón derecho del ratón, selecciona:

Todas las tareas > Exportar

Se te abre el asistente para exportar certificados

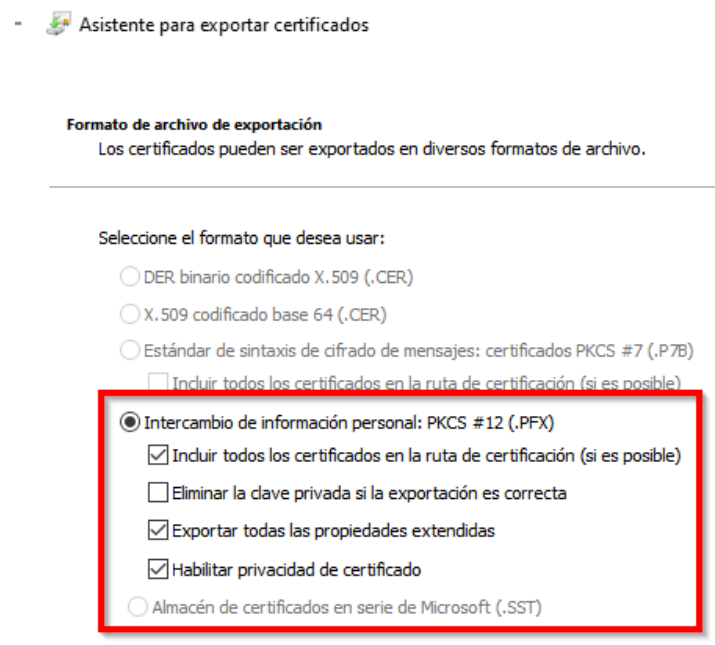
En la siguiente pantalla, marca 'Exportar la clave privada'



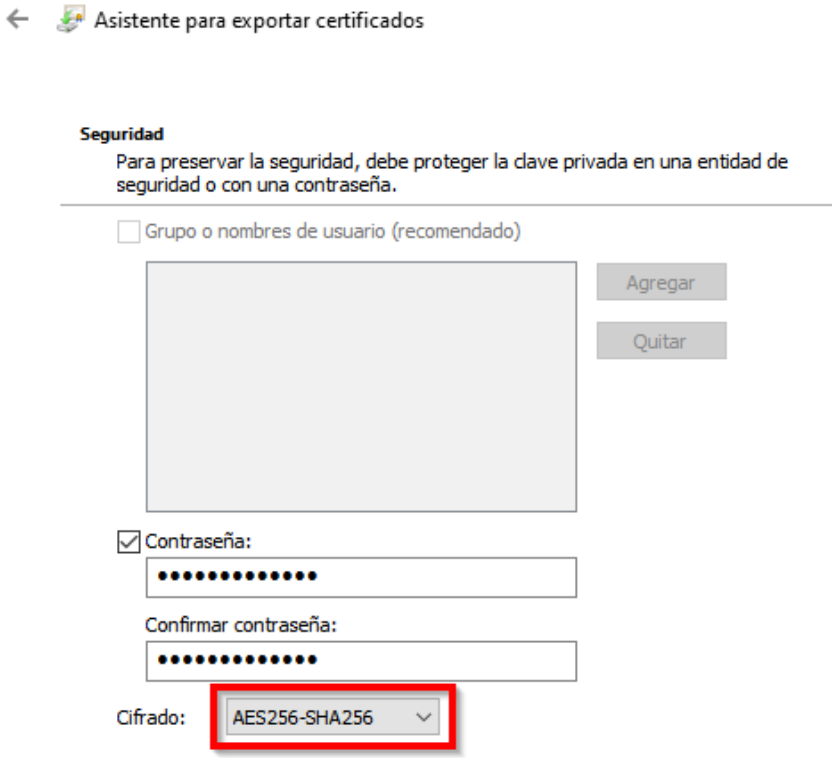
Las siguientes opciones hacen referencia al formato en que quieres exportar el certificado: es el formato p12, con extensión de archivo .PFX

Marca las opciones:

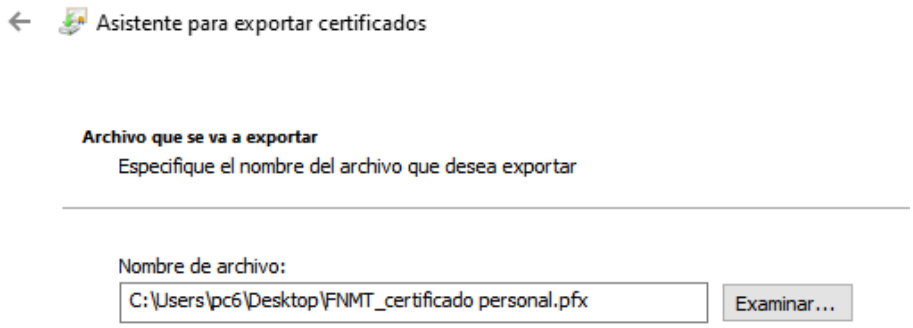
- *'Incluir todos los certificados en la ruta de certificación (si es posible)'*: así te saca tanto tu certificado como la ruta de certificación, es decir, también los certificados raíz de la FNMT, muy interesante si quieres instalarlo en otro equipo y que el sistema lo reconozca correctamente.
- *'Exportar todas las propiedades extendidas'*
- *'Habilitar privacidad del certificado'*: para que te pida una clave cuando vaya a recuperarse o importarse y, en caso de extravío del archivo, que nadie pueda usarlo.



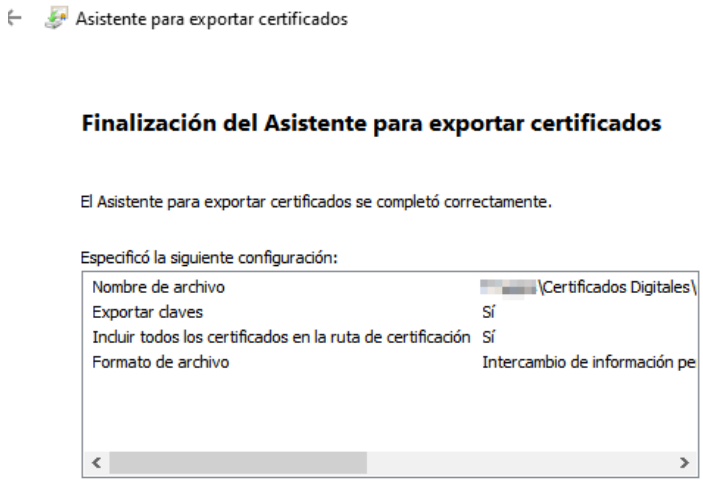
En la siguiente pantalla, introduce la contraseña que quieras poner para su uso y elige el método de cifrado, en este caso el robusto AES256



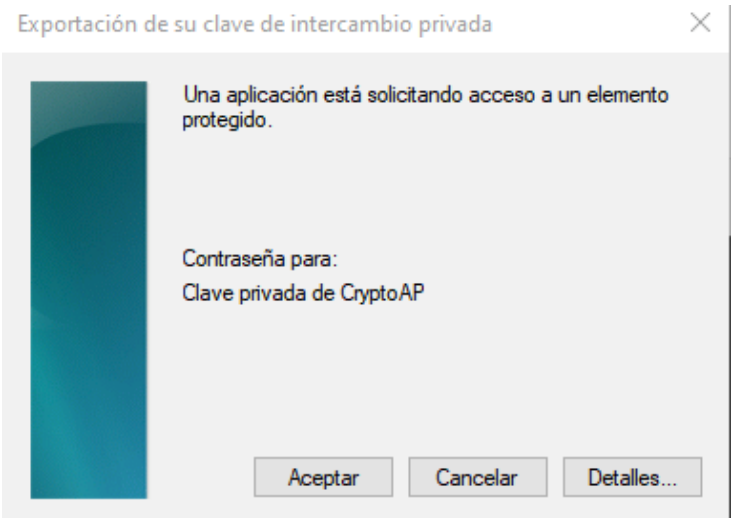
Por último, pulsa *'Examinar'* para elegir una ubicación para el archivo y escribe también el nombre de nuestro certificado. Ha de ser un nombre lo suficientemente descriptivo como para que luego lo halles con facilidad, por ejemplo, ***FNMT_certificado personal.pfx***



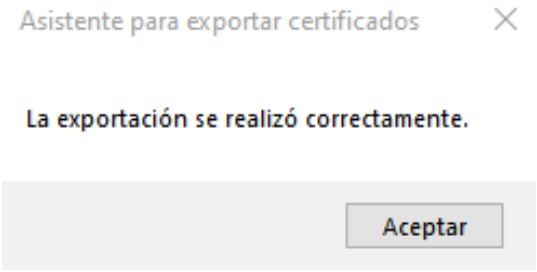
A continuación, el asistente te ofrece un resumen de las opciones elegidas:



Pincha en Finalizar, te saltará el aviso de que estás usando la clave privada para hacer la exportación



Y listo, certificado exportado con éxito



Ya puedes guardarlo en una ubicación segura para su uso en el futuro.

VIDEOTUTORIAL

Hacer backup de tu certificado digital (FNMT) en Windows

FIRMA DE DOCUMENTOS CON CERTIFICADOS

Tras haber visto los conceptos básicos necesarios para comprender qué es un certificado digital, tras haber conocido cómo obtenerlo y gestionarlo (renovarlo, revocarlo, almacenarlo), y tras haber repasado cómo exportarlo, hacer una copia de seguridad y cómo importarlo a otra máquina, llega el momento de conocer el **uso más común de los certificados digitales**: **firmar un documento digital** con idéntica validez legal que si lo hicieras presencialmente con tu firma manuscrita y tu documentación en regla.

Para ello, y estando en posesión de un certificado digital personal de la FNMT válido, firmaremos un documento PDF (el formato que más suele usarse para estos fines) de dos formas distintas:

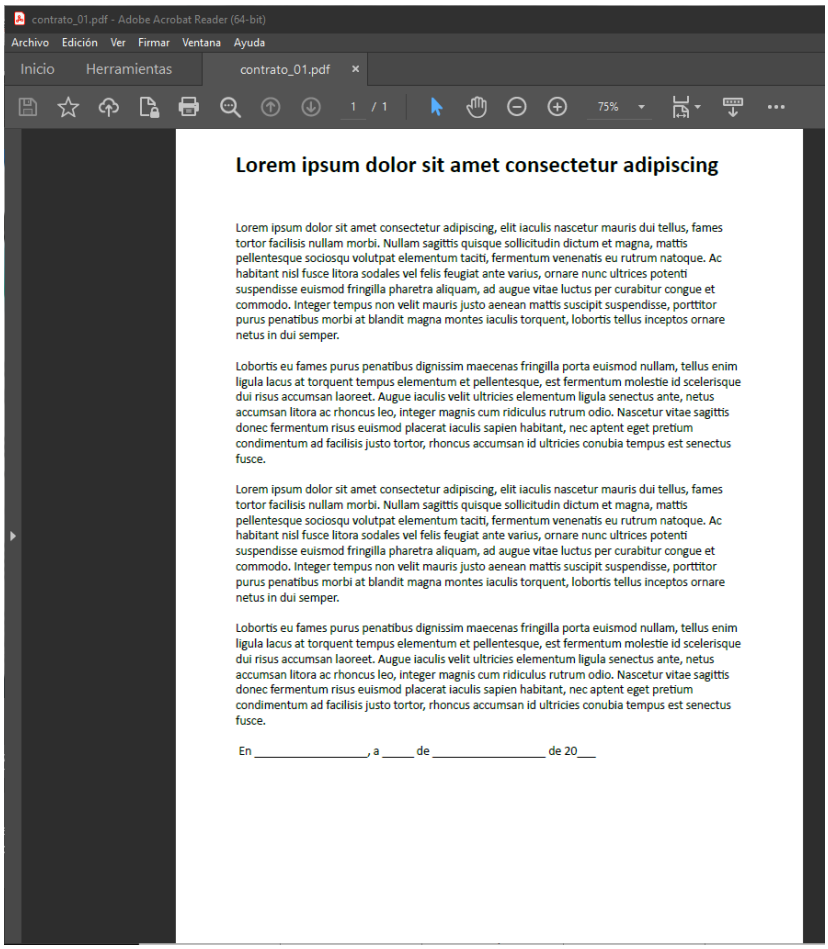
- Directamente **desde el Adobe Acrobat Reader**, el visor PDF gratuito más usado que, además, tiene un menú que te permitirá firmar con nuestro certificado con gran facilidad
- Con la aplicación **Autofirma**

FIRMA EN ACROBAT READER

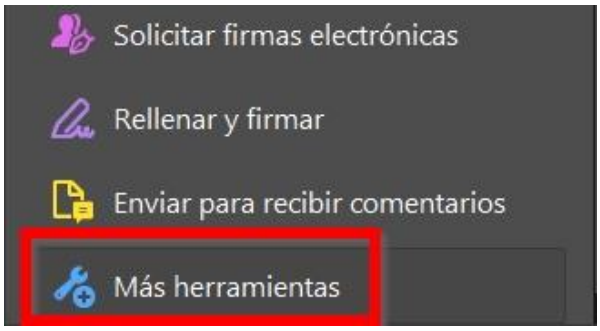
FIRMAR CON ACROBAT READER

FIRMAR DIGITALMENTE UN PDF CON ADOBE ACROBAT READER

Abre con el Acrobat Reader el documento que quieras firmar:

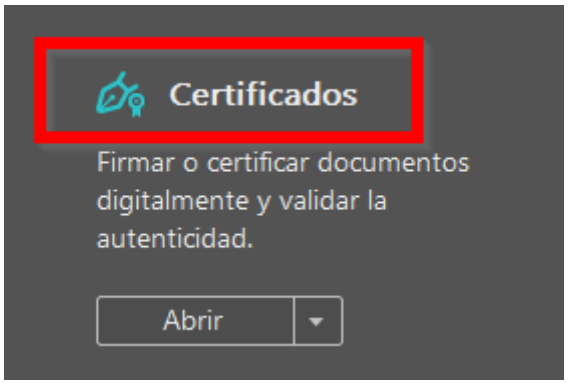


En el menú lateral *'Herramientas'*, busca dentro de la opción *'Más herramientas'*



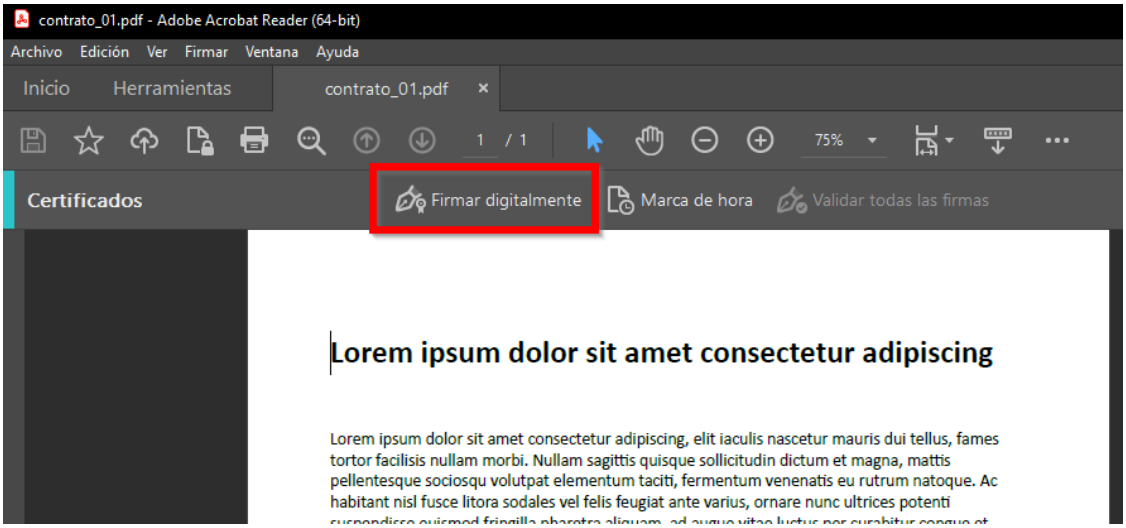
Elige la opción ***'Certificados' > Abrir***

⚠ No seleccionar nunca la opción 'Rellenar y firmar', pues ésta es para añadir firmas manuscritas que no tienen plena validez legal en España.

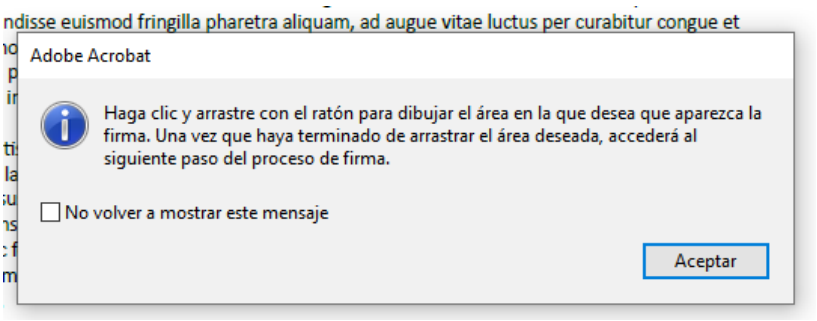


⚠ La disposición puede variar según la versión del Acrobat Reader de que dispongas. Te recomendamos que te descargues siempre la última versión disponible desde https://get.adobe.com/es/reader/

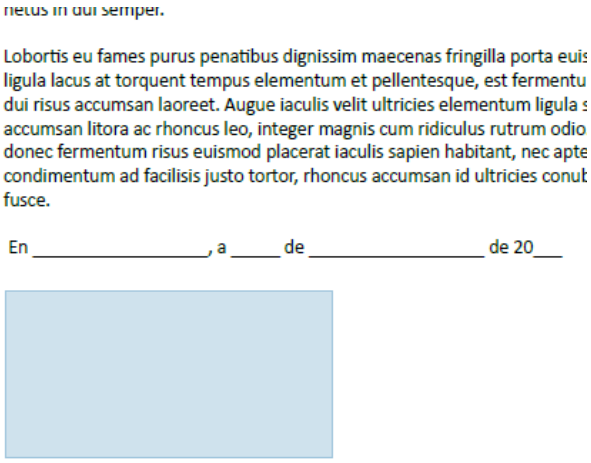
Una vez hayas abierto la opción 'Certificados', te aparecerá un menú en la parte superior del documento. Elige 'Firmar Digitalmente'



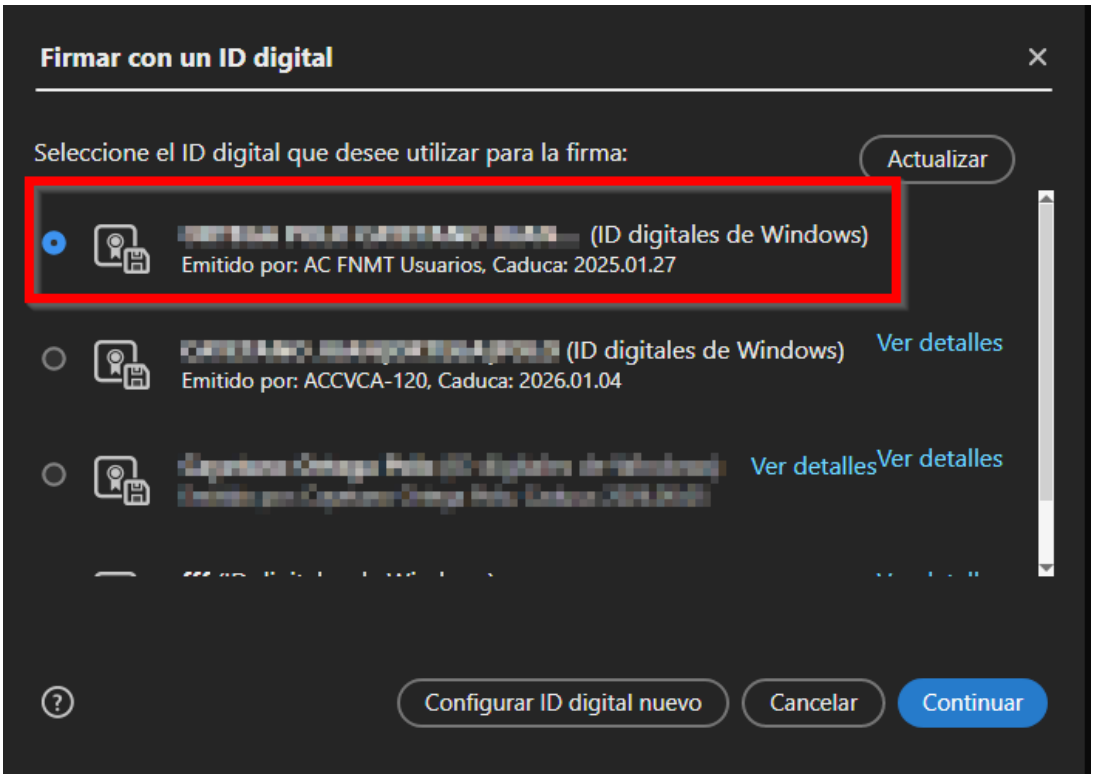
Te aparecerá una indicación de que dibujes el área donde quieres que aparezca la firma; usualmente, al final del documento



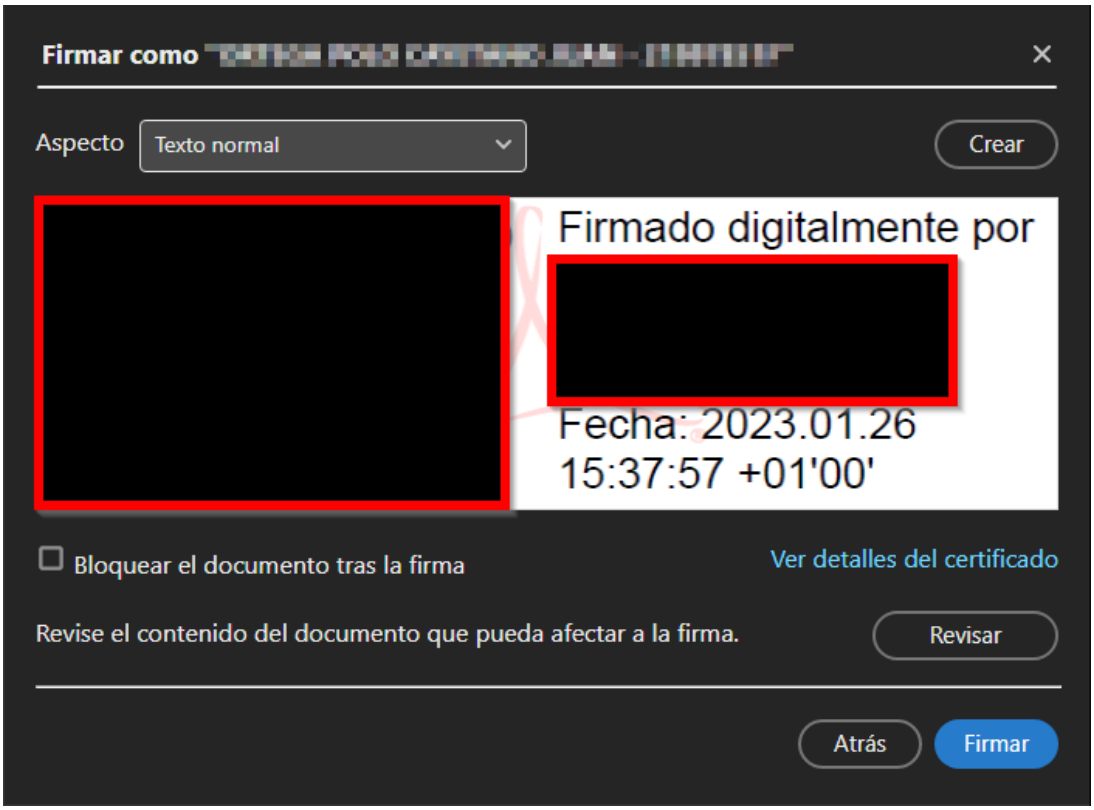
Dibuja el área para la firma:



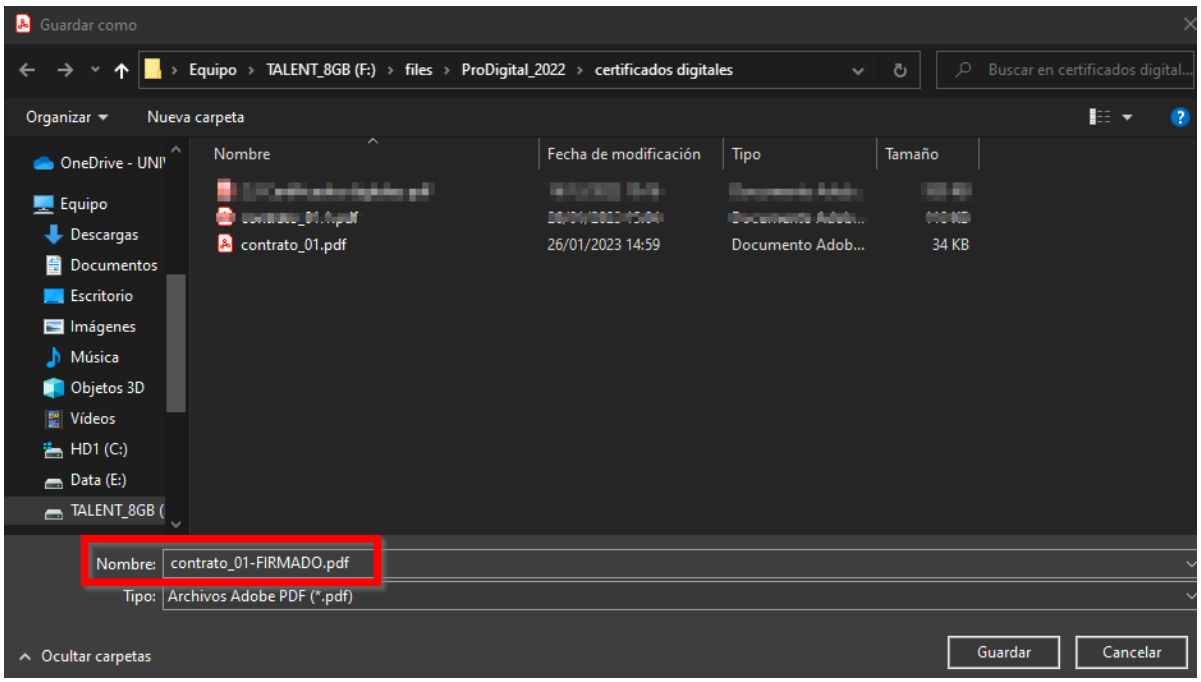
Y, tras soltar el ratón, aparecerá una ventana con todos los certificados digitales que tienes instalados. Elige el de la FNMT y pulsa en 'Continuar'



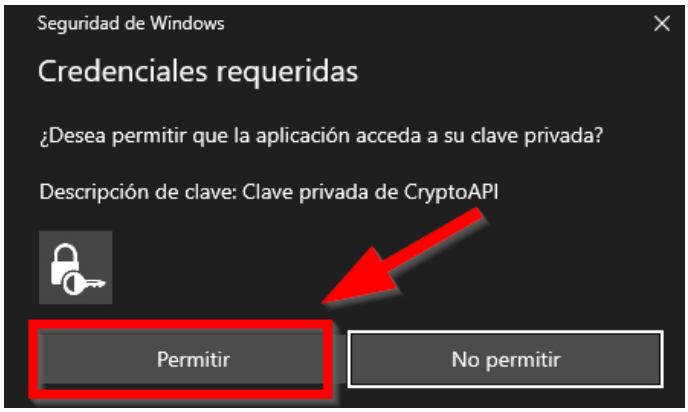
Te aparecerá otra imagen de cómo quedaría tu firma, con indicación de la fecha y hora de la misma



Si estás conforme, pulsa en 'Firmar' y te aparecerá un cuadro de diálogo en el que puedes poner el nombre con que se guardará el documento. Suele resultar útil conservar el documento original y añadir a éste alguna indicación de que está firmado.



El sistema te pide permiso para usar tu certificado digital (evidentemente, elige 'Permitir')



Y ya tienes tu documento firmado con plena validez legal en España

Comprobar siempre que, en el PANEL DE FIRMAS (barra en azul de la parte superior del documento) te indique

Firmado y todas las firmas son válidas

FIRMA CON ACROBAT READER / VIDEOTUTORIALES

VIDEOTUTORIAL

-Cómo firmar digitalmente archivos PDF (España, FNTM) con Acrobat Reader

FIRMA CON AUTOFIRMA

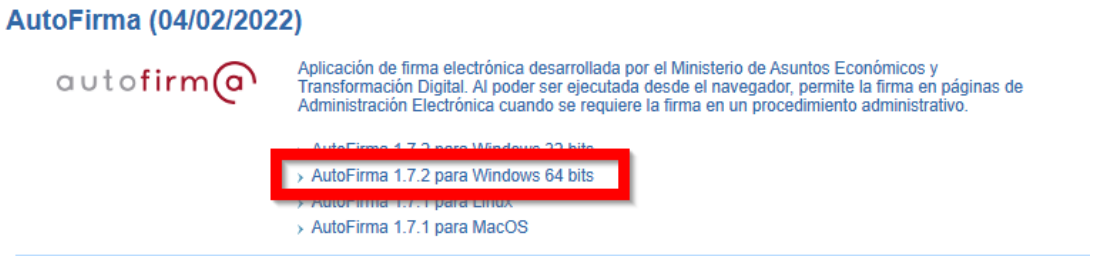
FIRMAR CON AUTOFIRMA

FIRMAR DIGITALMENTE UN DOCUMENTO CON AUTOFIRMA

Vamos a ver a continuación el proceso para firmar un documento (cualquier documento) con la aplicación Autofirma.

En primer lugar, descarga la aplicación desde su página.

Tienes versiones para windows (32 y 64 bits), Mac y Linux. Haremos nuestra exposición basándonos en la app para el sistema operativo windows, mayoritario entre las personas usuarias. El procedimiento para Mac y Linux, sin embargo, es muy similar.

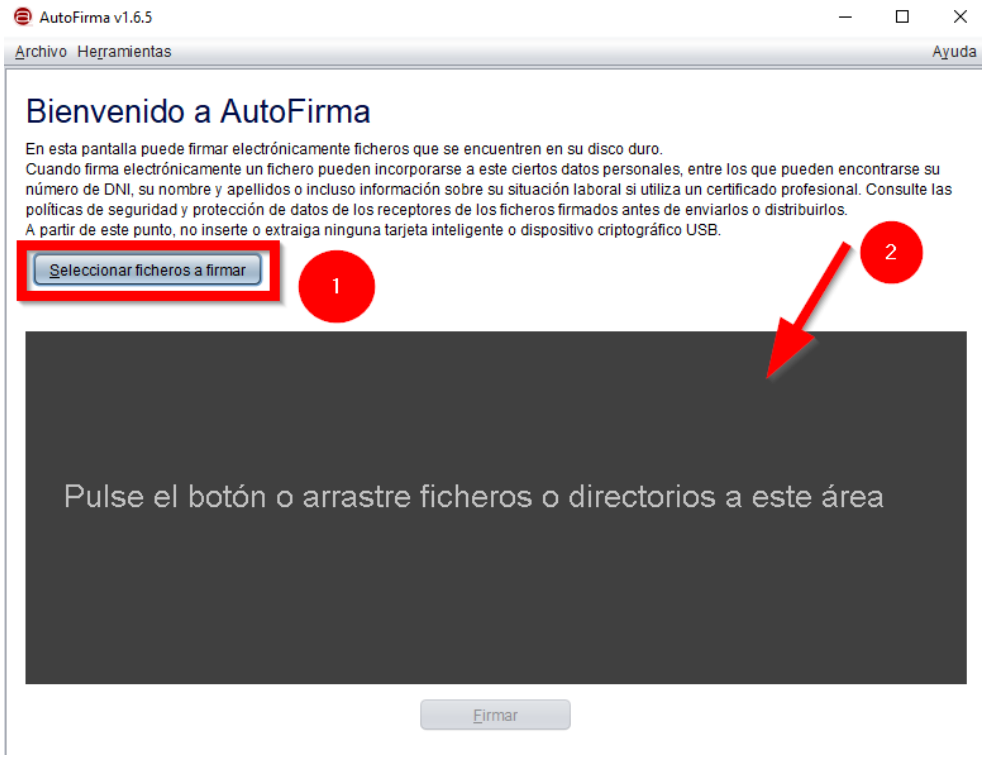


La inmensa mayoría de sistemas Windows 10 modernos son de **64 bits**, así que esa es la versión que bajarás a tu ordenador.

El procedimiento de instalación es común a cualquier otra aplicación de Windows que hayas realizado, por lo cual continuaremos la exposición suponiendo que ya tienes Autofirma correctamente instalado en tu ordenador. Si tienes dudas al respecto, en uno de los vídeos ilustrativos del final de este punto tienes el proceso detallado. Además, en el propio paquete de la aplicación dispones de un detallado manual de instalación.

Bien, una vez arranques Autofirma, la aplicación te muestra su pantalla principal, que es muy sencilla y te permite elegir cómo abrir tu fichero a firmar:

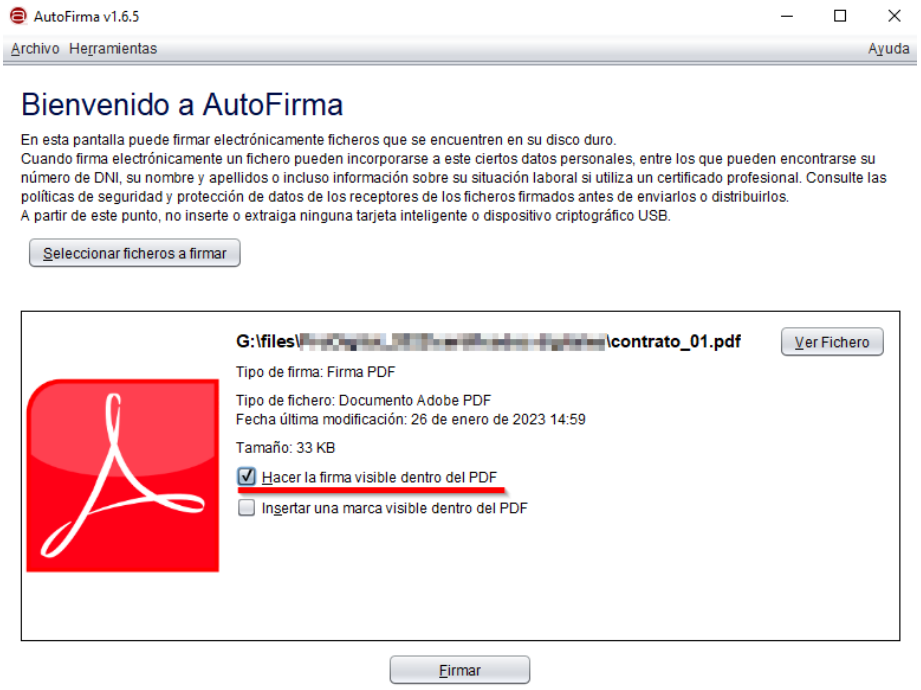
1. Seleccionando ficheros a firmar con el botón
2. Arrastrando los ficheros al recuadro indicado



Por cualquiera de los dos métodos, abre el documento a firmar, y se te abrirá otro cuadro de diálogo en el que elegirás la opción

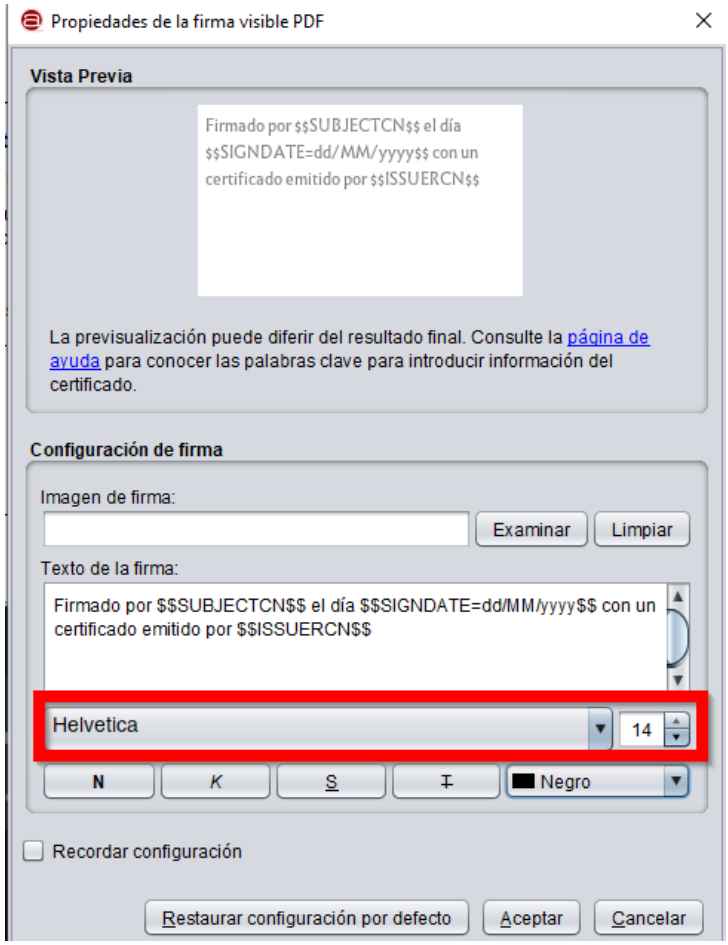
'Hacer la firma visible dentro del PDF'

La otra opción es para insertar una imagen con nuestra firma manuscrita

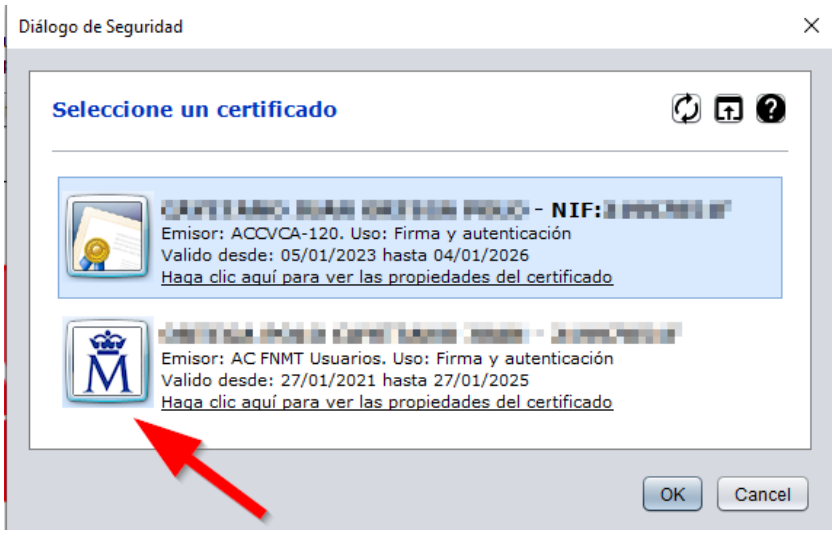


Pincha el botón de ***'Firmar'*** y, en la siguiente pantalla, elige la zona del documento donde quieras que se inserte la firma. En tu caso, al final del mismo.

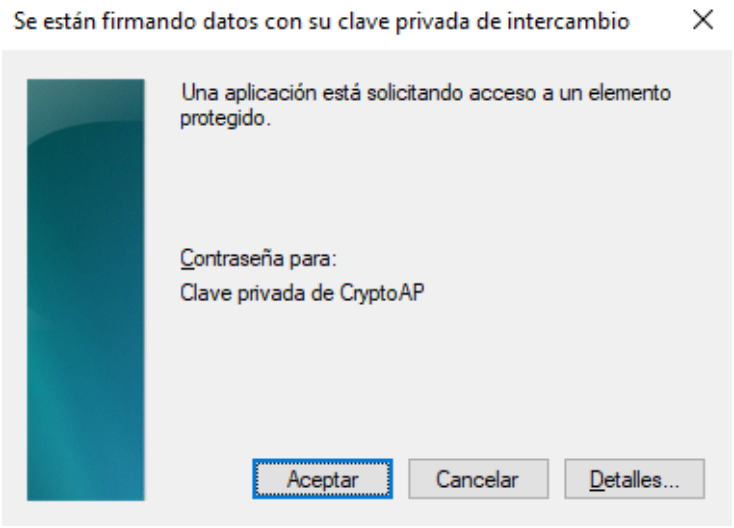
La siguiente pantalla te permite elegir qué quieres que aparezca en tu firma electrónica, y también puedes elegir algunas otras opciones de estilo, como la tipografía o el color de la misma. Por estética, cambia el tipo de letra a Helvética 14 y deja el resto de valores por defecto



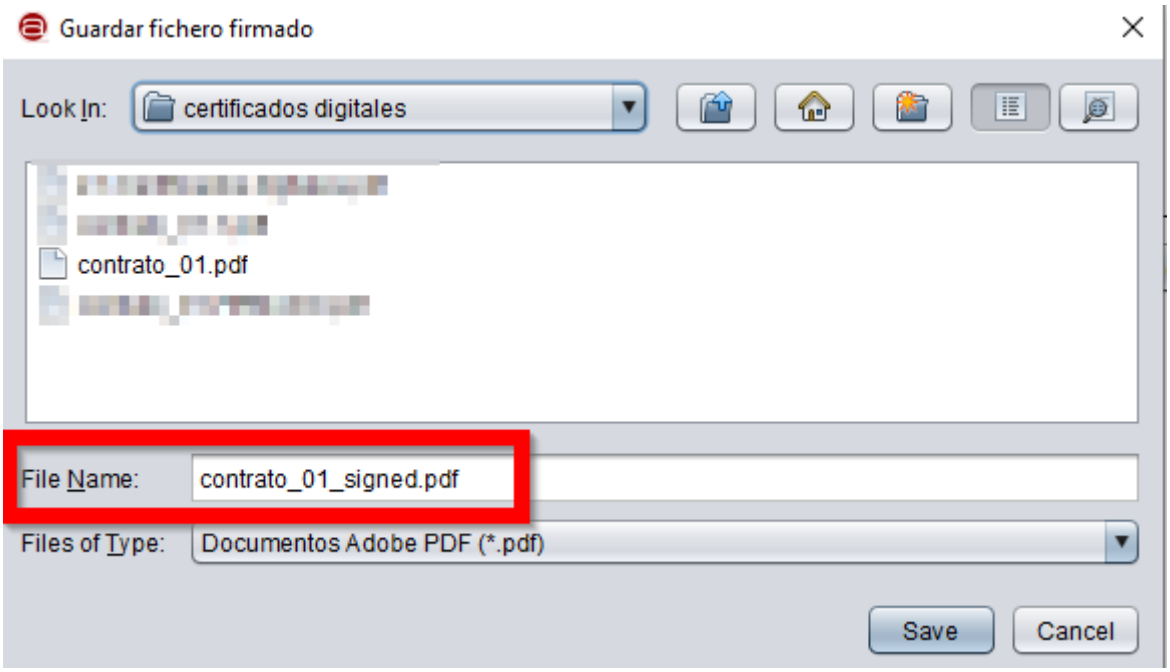
A continuación, pincha en ***'Aceptar'*** y el sistema te permite elegir qué certificado de los que tienes instalados quieres usar, en tu caso, elige el de la FNMT



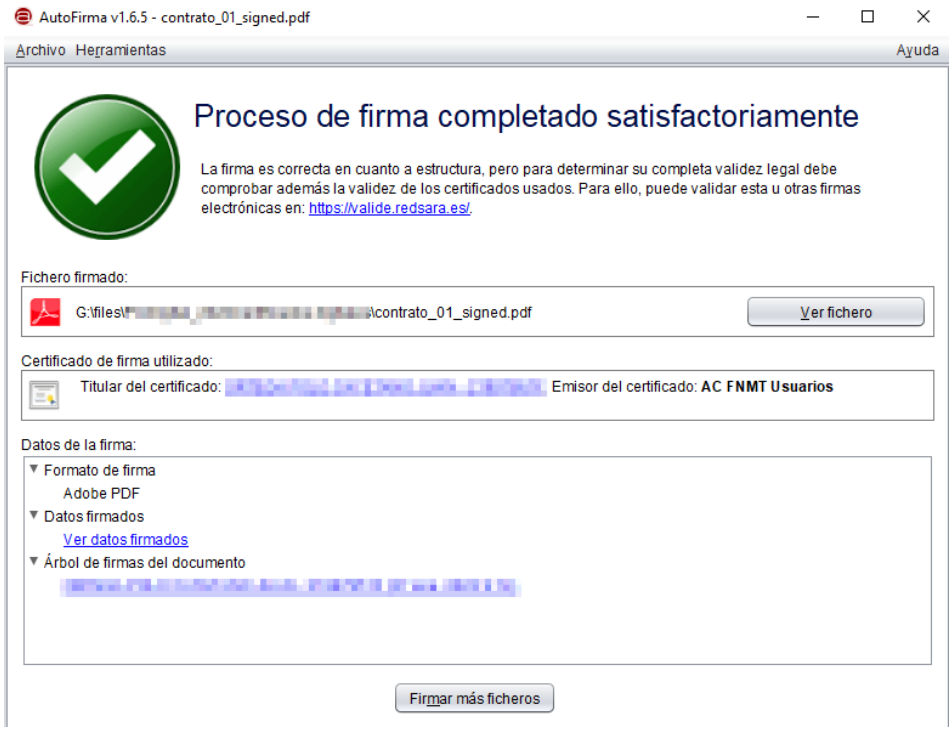
Tras pulsar 'OK', salta el ya familiar aviso de que se va a usar tu certificado digital:



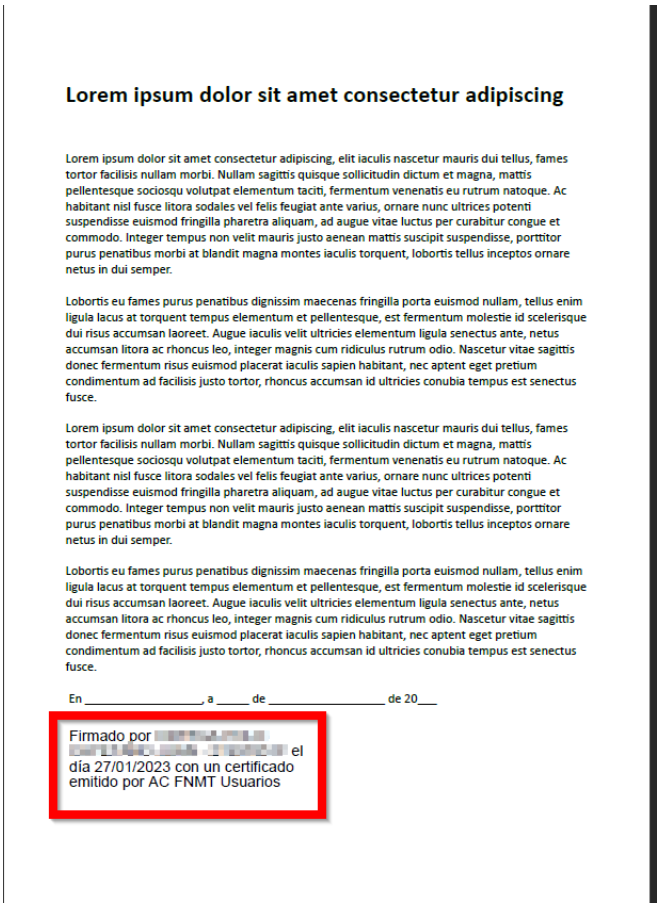
Por último, la aplicación te pide que guardes el documento firmado con el nombre que elijas (por defecto, añade ***_signed*** -firmado- al nombre original de tu archivo, para que distingas la versión que tiene la firma digital)



Tras guardar el archivo, Autofirma te indica que el proceso de firma se ha completado satisfactoriamente:



Si ahora eliges 'Ver fichero', puedes ver qué aspecto tiene tu documento firmado:



Lorem ipsum dolor sit amet consectetur adipiscing

Lorem ipsum dolor sit amet consectetur adipiscing, elit iaculis nascetur mauris dui tellus, fames tortor facilisis nullam morbi. Nullam sagittis quisque sollicitudin dictum et magna, mattis pellentesque sociosqu volutpat elementum taciti, fermentum venenatis eu rutrum natoque. Ac habitant nisl fusce litora sodales vel felis feugiat ante varius, ornare nunc ultrices potenti suspendisse euismod fringilla pharetra aliquam, ad augue vitae luctus per curabitur congue et commodo. Integer tempus non velit mauris justo aenean mattis suscipit suspendisse, porttitor purus penatibus morbi at blandit magna montes iaculis torquent, lobortis tellus inceptos ornare netus in dui semper.

Lobortis eu fames purus penatibus dignissim maecenas fringilla porta euismod nullam, tellus enim ligula lacus at torquent tempus elementum et pellentesque, est fermentum molestie id scelerisque dui risus accumsan laoreet. Augue iaculis velit ultricies elementum ligula senectus ante, netus accumsan litora ac rhoncus leo, integer magnis cum ridiculus rutrum odio. Nascetur vitae sagittis donec fermentum risus euismod placerat iaculis sapien habitant, nec aptent eget pretium condimentum ad facilisis justo tortor, rhoncus accumsan id ultricies conubia tempus est senectus fusce.

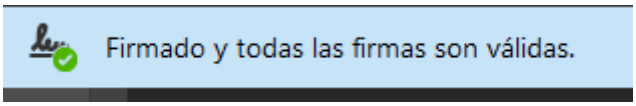
Lorem ipsum dolor sit amet consectetur adipiscing, elit iaculis nascetur mauris dui tellus, fames tortor facilisis nullam morbi. Nullam sagittis quisque sollicitudin dictum et magna, mattis pellentesque sociosqu volutpat elementum taciti, fermentum venenatis eu rutrum natoque. Ac habitant nisl fusce litora sodales vel felis feugiat ante varius, ornare nunc ultrices potenti suspendisse euismod fringilla pharetra aliquam, ad augue vitae luctus per curabitur congue et commodo. Integer tempus non velit mauris justo aenean mattis suscipit suspendisse, porttitor purus penatibus morbi at blandit magna montes iaculis torquent, lobortis tellus inceptos ornare netus in dui semper.

Lobortis eu fames purus penatibus dignissim maecenas fringilla porta euismod nullam, tellus enim ligula lacus at torquent tempus elementum et pellentesque, est fermentum molestie id scelerisque dui risus accumsan laoreet. Augue iaculis velit ultricies elementum ligula senectus ante, netus accumsan litora ac rhoncus leo, integer magnis cum ridiculus rutrum odio. Nascetur vitae sagittis donec fermentum risus euismod placerat iaculis sapien habitant, nec aptent eget pretium condimentum ad facilisis justo tortor, rhoncus accumsan id ultricies conubia tempus est senectus fusce.

En _____, a ____ de _____ de 20___

Firmado por [redacted] el día 27/01/2023 con un certificado emitido por AC FNMT Usuarios

Y, en la cabecera del Adobe Acrobat, en la barra de firmas, comprueba que todas las firmas son válidas:



Pues listo, ya tienes tu documento firmado.

TUTORIALES DEL USO DE AUTOFIRMA

VIDEOTUTORIALES

-Tutorial: Cómo instalar Autofirma

-Tutorial:Firma digital con Autofirma: PDF, Word y cualquier otro archivo

AUTENTICACIÓN MULTIFACTOR

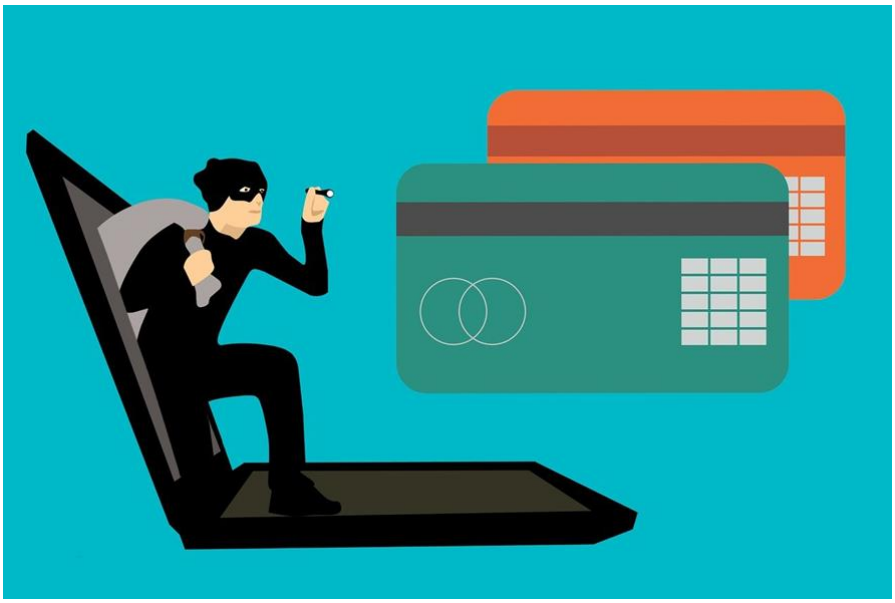
Gran parte de las funcionalidades de las aplicaciones que tienes instaladas en tu ordenador y otros dispositivos electrónicos son posible gracias a la conexión a los servidores remotos, desde los cuales se reciben los datos necesarios para su correcto desempeño.

> **Ejemplo**
>
> Piensa, por ejemplo, en el funcionamiento de Instagram: si bien la aplicación está instalada en el móvil, necesita una conexión continua con los servidores de META para asegurar el flujo constante de información: subir tus fotos, stories y estados y recibir todos los datos necesarios para alimentar tu feed.

Esta conexión a los servidores remotos se realiza de tres vías principales (o una combinación de ellas):

1. Mediante una red cableada clásica (Ethernet)
2. Mediante una red inalámbrica (WiFi), bien sea en tu casa, a través de tu router inalámbrico, en la universidad a través de eduroam o en cualquier otro lugar a través del acceso a redes públicas o privadas
3. Mediante la conexión celular inalámbrica de tu móvil (3G, 4G o 5G)

La conexión a estas redes se realiza usualmente mediante autenticación con un nombre de usuario y una contraseña. Esta forma de autenticarte, **con un solo factor o paso,** se conoce como **1FA** y presenta el problema de que es muy débil: si tu usuario y contraseña cae en manos ajenas, bien porque te lo roban o bien porque se produce una brecha de seguridad en la empresa depositaria de las mismas, los ladrones pueden hacerse pasar por ti y, por ejemplo, obtener tus datos personales que luego pueden revender en la dark web.



Ejemplo

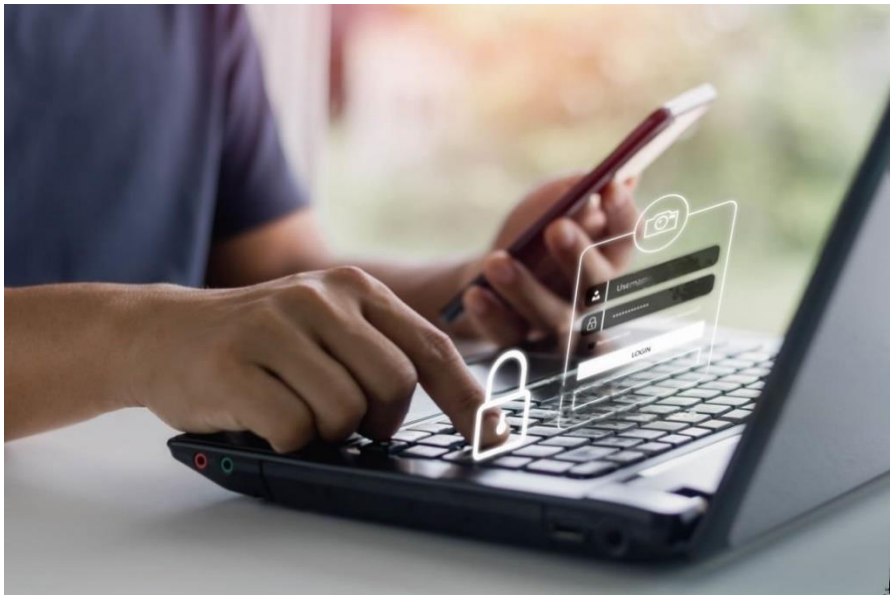
En 2021, la información privada de 533 millones de usuarios de Facebook se hizo pública y se expuso online de manera gratuita y al alcance de cualquiera.
El origen de la brecha fue la explotación de una vulnerabilidad en sus sistemas, que llevo a la exposición de nombres, direcciones de mail, números telefónicos, fechas de nacimiento y ubicaciones, aparte por supuesto de los datos de acceso de las personas afectadas.

Es para reforzar la débil seguridad de los sistemas de autenticación usuario+contraseña que nacen los **sistemas de autenticación multi-factor** (es decir, que requieren más de dos elementos para verificar la identidad de un usuario o usuaria).

2FA (TWO FACTOR AUTHENTICATION, O DOBLE FACTOR DE AUTENTICACIÓN

> << *El doble factor de autenticación, verificación en dos pasos o 2FA es un* ***método de doble identificación****, que persigue incrementar la seguridad y privacidad de tus cuentas y perfiles usando dos elementos o pasos para verificar tu identidad.*

Esto significa añadir un paso más al proceso de introducir usuario + contraseña para acceder a tus cuentas.



De esta manera, aumentarás la seguridad del acceso, pues aunque tu usuario y contraseña caiga en malas manos o los pierdas (éste sería el primer factor), el sistema te requerirá el segundo paso, la autenticación en el segundo factor de autenticación para demostrar que realmente tú eres tú.
El 2FA es un método que seguro que ya conocías porque algunas empresas, sobre todo entidades financieras, lo usaban cuando detectaban un intento de ingreso en tu cuenta desde un dispositivo no habitual. En estos casos, la aplicación o la web te daban la opción de remitirte un código de verificación bien a tu móvil, bien a tu mail (previamente registrados en tu perfil) que demostrase que tú eres quien decía ser.

¿CÚANTOS MÉTODOS DE VERIFICACIÓN EN DOS PASOS HAY?

Vamos a listar a continuación los métodos de verificación en dos pasos (2FA) más populares y utilizados. Es muy probable que algunos de ellos ya los conozcas (por ejemplo, la verificación mediante el envío de un SMS o de un email), otros tienen inconvenientes que los hacen poco aconsejables (llevar un USB físico o un largo código anotado siempre encima).

VERIFICACIÓN VÍA EMAIL

Tras escribir usuario + contraseña, te envían una clave temporal por email.

VERIFICACIÓN VÍA SMS

Un clásico: tras escribir usuario + contraseña, te envían una clave temporal vía SMS. Es un método rápido y sencillo; el único requisito es tener que dar tu número de móvil a la aplicación con la que quieras autenticarte.

PREGUNTA DE SEGURIDAD

En este caso, la capa de seguridad adicional consiste en responder a una pregunta de seguridad cuya respuesta ya hayas dado antes. Es tan insegura como parece, porque las respuestas las puede conocer mucha gente de tu entorno. Además, has de añadirla con anterioridad y no es cambiante.

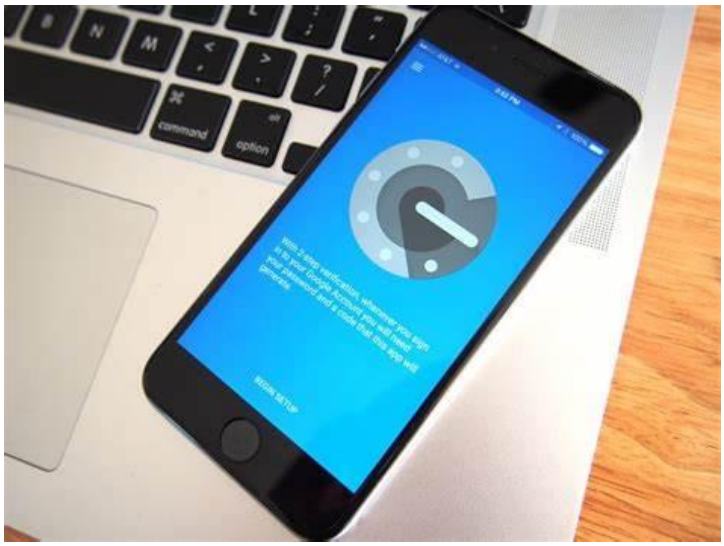
LLAVE DE SEGURIDAD

La validación se produce mediante un dispositivo que has de llevar encima y permite validar que, en efecto, eres quien dices ser. Puede tratarse de una llave de seguridad USB o también de dispositivos NFC o Bluetooth.

Este método es muy seguro, pero presenta el inconveniente de la pérdida, robo o extravío del dispositivo que uses como llave

APLICACIONES DE AUTENTICACIÓN

En este caso, tras introducir nombre + contraseña, tendrás que verificar tu identidad con la contraseña temporal OTP (*One-Time Password*, o contraseña de un solo uso) que generará la aplicación que tengas configurada (Microsoft Authenticator o Google Authenticator se encuentran entre las más populares). Es probablemente el método más seguro, y el elegido también por la UA como método 2FA



BIOMETRÍA

Algunos ordenadores portátiles permiten ya la identificación facial de la persona, aunque es más común que puedas identificarte con la huella dactilar. En ordenadores portátiles y teléfonos móviles es mucho más común usar tus datos biométricos como identificadores. Es también un método muy seguro.

CÓDIGOS DE RECUPERACIÓN

Algunos servicios, cuando te identificas, generan un código de recuperación que te piden que guardes. Método útil, aunque con el inconveniente de tener a mano los códigos generados.

CÓDIGOS EN LA MISMA APP O SERVICIO

Hay aplicaciones móviles que también tienen la función de generar códigos necesarios para iniciar sesión en nuevos dispositivos.

EL 2FA EN LA UNIVERSIDAD DE ALICANTE

Desde el curso académico 2023-2024, y previo periodo de prueba entre el profesorado y personal técnico, de gestión y de administración y servicios, la Universidad de Alicante apuesta por generalizar el uso del 2FA para acceder a todos los servicios accesibles desde UACloud / Campus Virtual.

El método elegido por la UA es el de la verificación mediante una aplicación de autenticación TOTP, que genera un código temporal que será el que tengas que introducir en UACloud.

¿QUÉ SIGNIGICA TOTP?

> << *Time-based One-time Password, o contraseña de un solo uso basada en la hora es un algoritmo que permite generar una contraseña de un solo uso (OTP, o One-Time Password) que hace uso de la hora actual como fuente de singularidad.*

Las contraseñas de un solo uso son códigos de seguridad que se pueden utilizar una sola vez para autenticarte antes de que se restablezcan. Son pues contraseñas dinámicas.

Esta capa de protección adicional, consistente en cambiar continuamente las contraseñas de un solo uso ha demostrado ser muy eficaz contra el robo de nuestros datos.

La configuración del 2FA es sumamente sencilla:

1. Instala una aplicación TOTP en el móvil o en el ordenador, que será la que uses siempre para generar el doble factor.
2. Vincula la aplicación con UACloud
3. Introduce el código TOTP
4. Accede a UAClood

El Servicio de Informática de la UA ha habilitado un portal para responder a todas las dudas del colectivo universitario y explicar paso a paso la configuración inicial del servicio.

> << *Ten en cuenta que, tras tu primera identificación, el sistema te permite identificar el navegador con el que accedas como un acceso de confianza, con lo cual sólo te pedirá el uso del 2FA cada 30 días.*