



# Ciudad Real Virtual

## Tus trámites a un clic\_

Cursos de formación digital  
y administración electrónica

**DNIe y Certificación Digital**



PLAN  
avanza2.0



fundación  
Insula Barataria

# **DNle y Certificados Digitales**



# ÍNDICE

<b>Introducción</b> .....	<b>5</b>
<b>Firma Digital</b> .....	<b>6</b>
¿Qué es la firma digital y para qué se utiliza?.....	6
Partes de un certificado.....	7
Obtener una firma digital a través de Internet, CERES.....	7
Comprobar la instalación del certificado.....	15
Realizar una copia de seguridad. Exportar un certificado.....	17
Importar un certificado.....	23
Período de vigencia. Revocación del certificado.....	30
¿Dónde puedo utilizar mi certificado de usuario?.....	32
Cifrar y firmar correos electrónicos.....	37
<b>DNI Electrónico</b> .....	<b>38</b>
¿Qué es el DNI Electrónico y para qué sirve?.....	38
Obtener un DNI Electrónico.....	39
Requisitos e instalación del DNI Electrónico.....	39
Verificar el funcionamiento de nuestro DNI Electrónico.....	44
¿Dónde puedo utilizar el DNI Electrónico?.....	46
<b>Medidas de Seguridad</b> .....	<b>50</b>
Las contraseñas como método de autenticación.....	50
Criterios para la creación de contraseñas seguras.....	51
Malas prácticas para la creación de contraseñas.....	<b>52</b>



## Introducción

En la vida cotidiana necesitamos una serie de datos identificativos para realizar la mayoría de los trámites burocráticos con la administración y las empresas estatales. Estos datos solemos aportarlos personándonos en las oficinas pertinentes y presentando el DNI, o cualquier otra clase de documento identificativo. Normalmente se realizan infinidad de operaciones diarias a través de los organismos públicos, lo que provoca que el proceso sea muy lento y a veces desesperante.

Para agilizar este proceso se crearon los medios de certificación digitales, como la firma digital o el DNI Electrónico, que permiten la identificación de una persona o entidad a través de Internet. Utilizando estos certificados digitales podemos realizar las mismas operaciones que realizábamos a través de los organismos públicos, sin la necesidad de presentarnos en sus oficinas y sufrir esperas interminables.

El objetivo de este módulo del manual es concienciar a la población de las ventajas que tiene el uso de este tipo de certificados en la vida cotidiana, destacando la seguridad que conlleva su utilización y la facilidad del proceso de obtención de los mismos.

En estos dos capítulos que forman dicho módulo veremos los pasos necesarios tanto para el proceso de obtención de la firma digital como para el del DNI Electrónico, su utilidad y ejemplos claros de su uso en la vida cotidiana.

## Firma Digital

### ¿Qué es la firma digital y para qué se utiliza?

La firma digital es un documento que contiene los datos identificativos de la persona. Es un tipo de certificado digital que nos permite identificarnos en Internet y de esta manera poder realizar todos los trámites necesarios con la administración pública, de una forma rápida y sencilla. Entre los trámites que podemos realizar con nuestra firma digital podemos destacar la posibilidad de realizar la Declaración de la Renta a través de Internet, modificar y actualizar nuestros datos personales o solicitar un informe de nuestra vida laboral. Éste último ejemplo lo veremos al final del capítulo.

Otra de las ventajas que tiene este tipo de certificación es que podemos realizar cualquiera de las gestiones necesarias a través de las páginas de la administración a cualquier hora del día, por lo que tampoco dependemos de los horarios de oficina ni del personal disponible.

Además de todo esto, con la firma digital podemos firmar formularios y documentos desde nuestro ordenador con la misma validez que tiene nuestra firma tradicional (manuscrita).

Todo este proceso se realiza de una manera segura y eficaz, de tal manera que la información intercambiada no es visible por terceros, lo que garantiza la integridad de la información y a su vez impide la negación de la autoría por cualquiera de las dos partes. Por tanto un certificado digital válido tiene que cumplir estos tres requisitos:

1. **Confidencialidad:** los datos enviados entre el receptor y emisor no son visibles por terceros, lo que se consigue por medio de la codificación de la información.
2. **Integridad:** al no haber posibilidad de interacción por medio de terceros se asegura que la información no ha sido modificada o alterada.

3. **No repudio:** las dos condiciones anteriores aseguran que ninguna de las dos partes pueda negar la autoría de su firma.

Todos los aspectos legales de la firma electrónica vienen recogidos en la **Ley 59/2003, de 19 de diciembre**.

### Partes de un certificado.

El certificado de firma digital consta de una criptografía de clave asimétrica, es decir, que la información se cifra utilizando dos claves:

- **Clave privada:** esta clave se guarda en el ordenador del propietario y no es conocida por nadie más.
- **Clave pública:** es la clave que podrán ver otros usuarios que dispongan de firma digital.

Estas dos claves son complementarias, ya que no se puede leer la información cifrada con la clave pública sin conocer la clave privada.

Cuando enviamos la información a otra persona, haciendo uso de nuestra firma digital, se utiliza una clave generada aleatoriamente, denominada **clave de sesión**, con la que se cifra el contenido que queremos enviar. Para enviar esa clave de sesión se cifra utilizando la clave pública del destinatario. De esta manera cuando el destinatario recibe la información utiliza sus claves pública y privada para descifrar la clave de sesión, que a su vez le permite descifrar la información recibida. Si otro usuario quisiera leer dicha información le sería imposible, ya que no dispone de la clave privada.

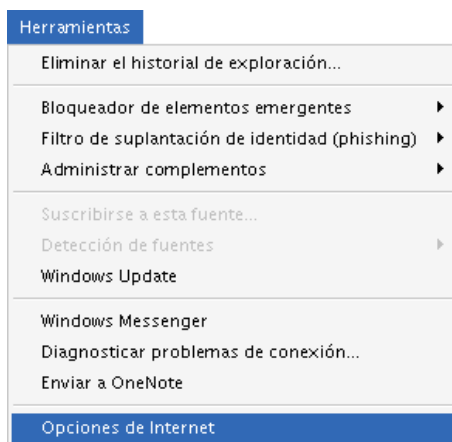
Todos estos datos son transparentes para nosotros y son proporcionados por nuestro prestador de servicios. El prestador de servicios es una autoridad certificadora con capacidad de expedir certificados electrónicos basándose en la **Ley 50/03, de 19 diciembre**. Existen múltiples empresas de certificación, aunque en este manual hemos optado por **CERES** (Certificación Española), una iniciativa de la Administración que nos permite obtener certificados válidos emitidos por la **Fábrica Nacional de Moneda y Timbre**.

### Obtener una firma digital a través de Internet, CERES.

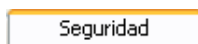
Para obtener un certificado de firma digital a través de Internet tenemos que acceder a la página web de una empresa certificadora válida. En este manual vamos a ver cuál sería el proceso de obtención completo de nuestra firma digital a través de la página de CERES (Certificación Española). A través de su página podemos obtener un certificado válido de nivel 2, emitido por la Fábrica Nacional de Moneda y Timbre (FNMT).

Antes de realizar el proceso, si vamos a utilizar Internet Explorer 7 como navegador tenemos que ajustar el nivel de seguridad para poder instalar el certificado, para ello vamos a seguir los siguientes pasos:

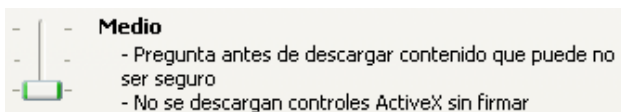
- Abrimos el navegador de Internet Explorer y hacemos clic en el menú **“Herramientas”** y en la opción **“Opciones de Internet”**.



- Hacemos clic en la ficha **“Seguridad”**.



- Aparecerá el nivel de seguridad establecido para la zona de Internet, que suele ser **“Medio-alto”**, tenemos que cambiar este valor a **“Medio”**, utilizando para ello la barra que aparece en la parte inferior de la ventana.



- Una vez que hemos establecido el nivel medio de seguridad para la zona de Internet hacemos clic en el botón “Aceptar”.

Aceptar

Si ya tenemos configurado nuestro navegador vamos a seguir estos pasos para la obtención de nuestra firma electrónica:

1. Abrimos el navegador de Internet y accedemos a la página de CERES escribiendo su dirección “[www.cert.fnmt.es](http://www.cert.fnmt.es)” en la barra de direcciones del navegador y pulsamos la tecla “Intro”.



2. En la esquina superior derecha hacemos clic sobre el enlace con el texto “Obtenga el certificado de usuario”.

Obtenga el  
CERTIFICADO DE USUARIO

- Nos aparecerá una página en la que podemos ver explicado todo el proceso de obtención del certificado paso a paso. En la página nos advierten de que no se debe formatear el ordenador durante el proceso y que debe realizarse desde el mismo equipo y con el mismo navegador. **Es muy importante que el equipo en el que realicemos el proceso sea nuestro propio ordenador y no uno público al que pueda acceder todo el mundo.**

Inicio | Contacto | Enlaces | Legislación | Noticias

Obtenga el CERTIFICADO de usuario con su DNI

Obtenga el CERTIFICADO de usuario con su usuario

<p>■ <b>Quié es CERES</b></p> <p>Certificado de usuario</p> <p>Modificar datos</p> <p>Contacto</p>	<p>■ <b>Ciudadanos</b></p> <p><b>Obtener el certificado</b></p> <p>Verificar estado</p> <p>Renovación de certificado</p>	<p>■ <b>Empresas</b></p> <p>Otros servicios</p> <p>Soporte Técnico</p>	<p>■ <b>Adm. Pública</b></p> <p>Renovación de certificado</p> <p>Preguntas Frecuentes</p>
--	--	--	---

Real Casa de la Moneda  
Fábrica Nacional de Moneda y Timbre

**CIUDADANOS**

**OBTENER EL CERTIFICADO**

**1 CERTIFICADO DE USUARIO**

Si lo desea puede consultar el siguiente documento: "Manual Firma Electrónica"

**PROCESO**

El proceso se divide en tres apartados que deben realizarse en el orden señalado.

**IMPRESIONABLE:**

No formatear el ordenador. Se debe realizar todo el proceso de obtención desde el mismo equipo, con el mismo usuario y el mismo navegador.

**IMPORTANTE:** Para usuarios de Windows Vista vía Internet Explorer 7

Antes de continuar con el proceso de Solicitud de Certificado lea atentamente la Declaración de Prácticas de Certificación.

**1 Solicitud vía internet de su Certificado.**

Al final de este proceso obtendrá un código que deberá presentar al acreditar su identidad.

**2 Acreditación de la identidad en una Oficina de Registro**

- El primer paso es solicitar el certificado a través de Internet, para lo que haremos clic en el enlace **"1 Solicitud vía internet de su certificado"**.

**1 Solicitud vía internet de su Certificado.**

- En la siguiente página introducimos nuestro DNI (o CIF en caso de ser persona Jurídica) en la caja de texto **"NIF / CIF"** que en cualquier caso tendrá una longitud de 9 caracteres, rellenando con ceros a la izquierda si es necesario.

NIF / CIF:

- Una vez introducido el DNI hacemos clic en el botón **"Enviar petición"**.

Enviar petición

7. Si todos los datos son correctos nos aparecerá una página con el **código de solicitud** asociado a nuestro DNI. Es muy importante imprimir o apuntar este código ya que lo tenemos que usar a continuación.

El código de solicitud para el NIF 01234567L es:

**917123313**

8. Una vez apuntado el código volvemos a la página anterior donde figura todo el proceso de obtención y hacemos clic sobre el enlace **“2 Acreditación de la identidad en una Oficina de Registro.”**.

**2 Acreditación de la identidad en una Oficina de Registro.**

9. El siguiente paso es personarnos en una oficina de registro con el **DNI** y el **código** que apuntamos, con el objetivo de solicitar nuestro certificado. En la oficina nos entregarán una serie de papeles con la información relativa a nuestro certificado y podremos continuar con el proceso. Como ayuda podemos buscar oficinas de registro cerca de nuestra zona haciendo clic en el enlace **“OFICINAS MÁS CERCANAS”**, que aparece en la parte inferior de la página.

El registro físico para la obtención del certificado podrá realizarlo en las Oficinas que puede encontrar a través de nuestro servicio de localización de las **OFICINAS MÁS CERCANAS**, y en las Oficinas Consulares de carrera de España en el extranjero, no siendo posible en los registros aduaneros.

10. En la siguiente página podemos realizar una búsqueda de las oficinas próximas a un lugar en concreto rellenando los datos de la búsqueda y haciendo clic en el botón **“buscar”**.

Podemos introducir la dirección de nuestro domicilio para que nos muestre las oficinas más cercanas.



11. Aparecerán las oficinas más próximas al lugar indicado ordenadas por distancia.



12. Si hacemos clic en cualquiera de los resultados podemos ver un plano de situación en el que se nos indica la situación de la oficina seleccionada.



13. Si ya nos hemos personado en la oficina de registro y todo está correcto ya sólo nos queda descargar e instalar el certificado en nuestro ordenador. Para ello, accedemos de nuevo a la página principal de CERES y volvemos a hacer clic en el enlace **“Obtenga el certificado de usuario”**. Una vez dentro vamos a realizar el tercer punto que nos faltaba, haciendo clic en el enlace **“3 Descarga de su Certificado de Usuario”**.

### **3. Descarga de su Certificado de Usuario**

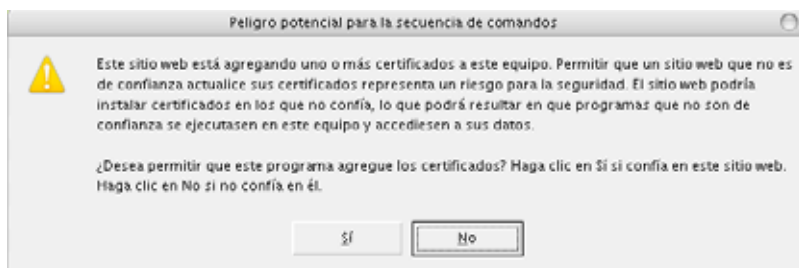
14. Una vez dentro de la página rellenamos la caja de texto **“NIF”** con nuestro DNI y la caja de texto **“Código”** con el código que obtuvimos a la hora de solicitar el certificado.

NIF	01234567L
Código	917123313

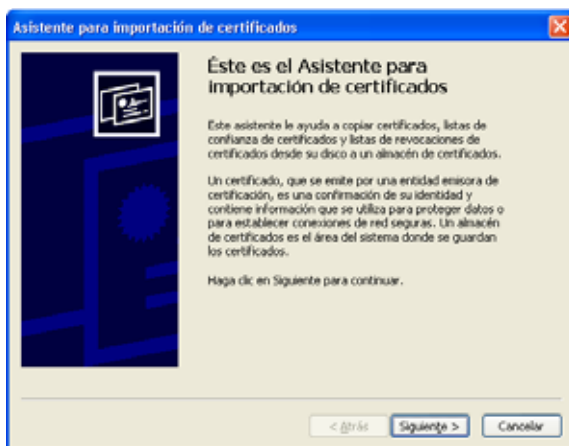
15. A continuación hacemos clic en el botón **“Enviar petición”**.

Enviar petición

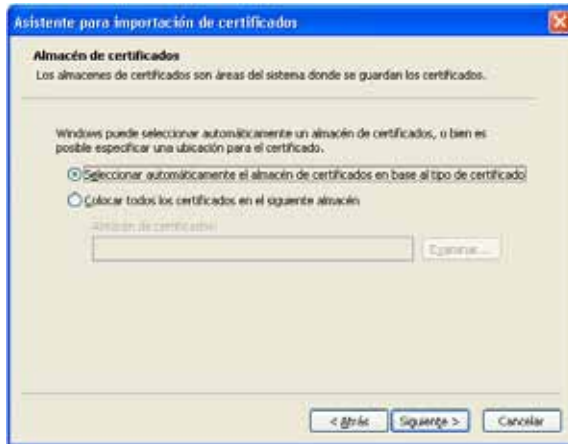
16. Tras enviar la petición aparecerá una alerta de seguridad como la que se muestra a continuación, en la que haremos clic en el botón **“Sí”** para permitir que se instale el certificado.



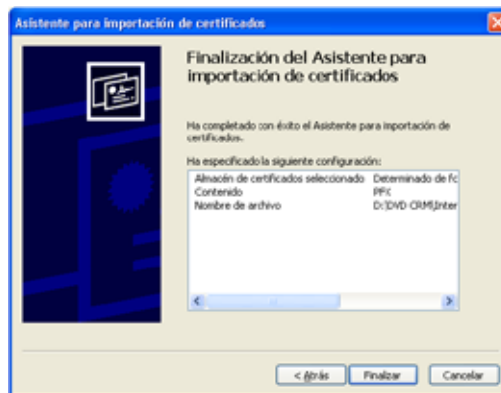
17. Después de permitir la instalación de nuestro certificado nos aparecerá la ventana del asistente de importación de certificados, en la que haremos clic en el botón “Siguiente” para continuar.



18. En la siguiente ventana podemos elegir el almacén donde se va a guardar el certificado o que el programa seleccione de manera automática el almacén más adecuado dependiendo del tipo de certificado. Dejamos marcada la opción que viene marcada por defecto y hacemos clic sobre el botón “Siguiente” para continuar.



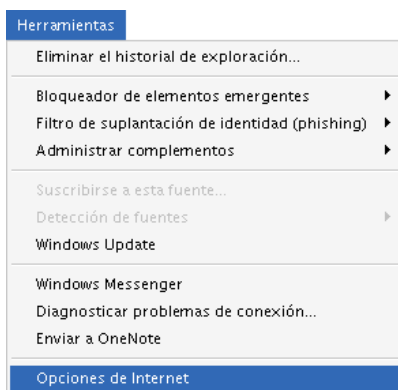
19. Una vez finalizado el proceso se mostrará una ventana con los detalles de la instalación. Para terminar hacemos clic en el botón “Finalizar”.



### Comprobar la instalación del certificado.

Para comprobar que nuestro certificado se ha instalado correctamente tenemos que acceder al **almacén de certificados**, siguiendo estos pasos:

1. Abrimos el navegador de Internet Explorer y hacemos clic en el menú “Herramientas” y en la opción “Opciones de Internet”.



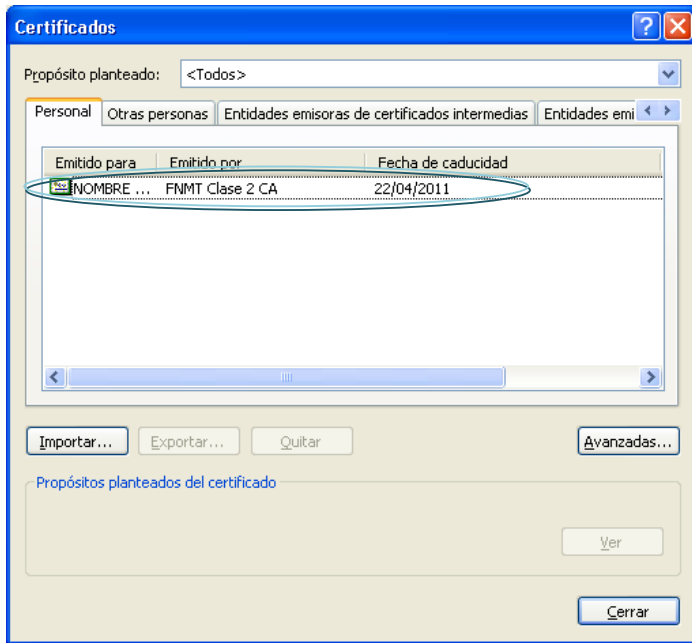
2. Hacemos clic en la pestaña **“Contenido”**.



3. Seguidamente hacemos clic en el botón **“Certificados”** situado en el apartado con el mismo nombre.



4. Al acceder a esta opción se nos mostrará una ventana con todos los certificados instalados en el navegador. Para localizar nuestro certificado tenemos que hacer clic en la pestaña **“Personal”** o en el almacén que eligiésemos a la hora de instalar el certificado. Si nuestro certificado aparece en el listado significa que la instalación se ha realizado con éxito y podemos comenzar a utilizar nuestro certificado.

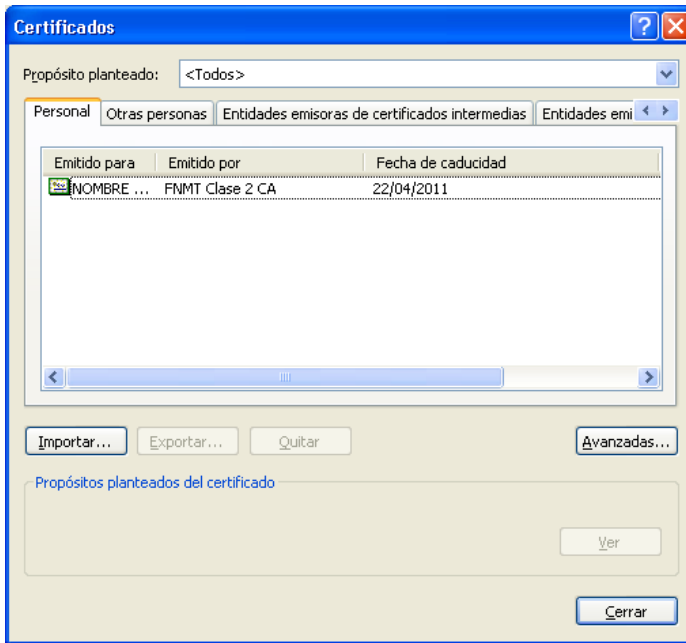


### Realizar una copia de seguridad. Exportar un certificado.

Tener una copia de seguridad de nuestro certificado de usuario es muy importante, ya que en el caso de sucederle algo a nuestro ordenador perderíamos el certificado y tendríamos que volver a reclamarlo en la Oficina de Registro.

Para realizar este proceso vamos a utilizar Internet Explorer y seguiremos estos pasos:

1. Accedemos al almacén de certificados, siguiendo los pasos que hemos visto en el apartado anterior "**Comprobar la instalación del certificado**".



2. Una vez localizado nuestro certificado, lo **seleccionamos** y hacemos clic en el botón **“Exportar”**.



3. Aparecerá el asistente para la exportación de certificados. Para continuar el proceso hacemos clic en el botón **“Siguiete”**.



4. En la siguiente ventana nos dará la opción de exportar nuestra clave privada. Si optamos por no exportar la clave privada nos creará un archivo que nos permitirá importar e instalar nuestro certificado en cualquier equipo, sin ninguna restricción. Por el contrario, si elegimos la opción de exportar la clave privada podremos introducir una contraseña para proteger la instalación de nuestro certificado. En nuestro caso hemos seleccionado la opción **“Exportar la clave privada”** para mostrar cómo sería todo el proceso. Para continuar hacemos clic en el botón **“Siguiente”**.



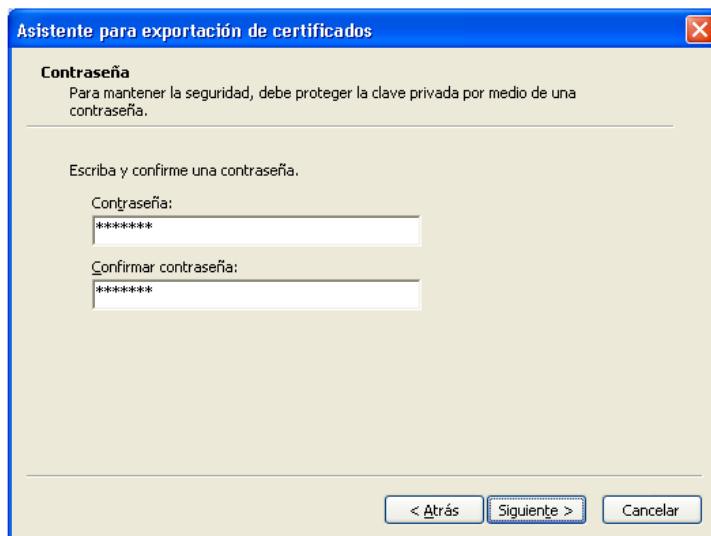
- En este punto se nos muestran los formatos disponibles para la exportación de nuestro certificado. Los formatos disponibles dependerán de la opción que elegimos en la pantalla anterior. En cualquiera de los dos casos dejaremos marcado el formato que viene seleccionado por defecto y hacemos clic en el botón “**Siguiente**”.



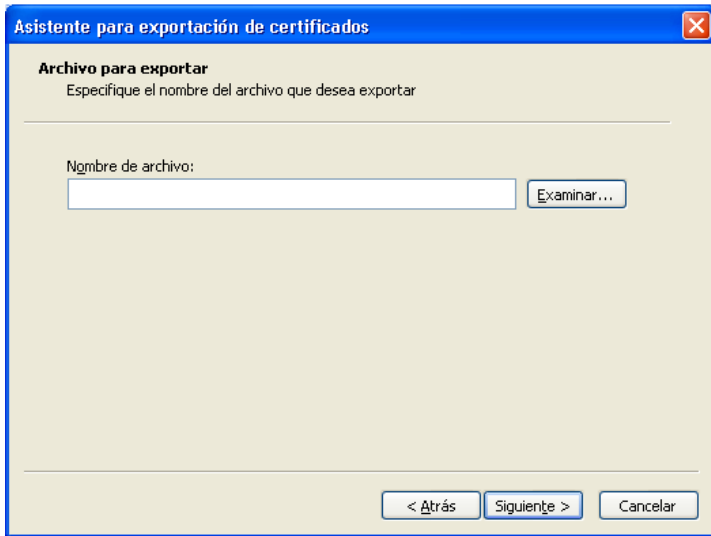
Opción “**No exportar la clave privada**”

Opción “**Exportar la clave privada**”

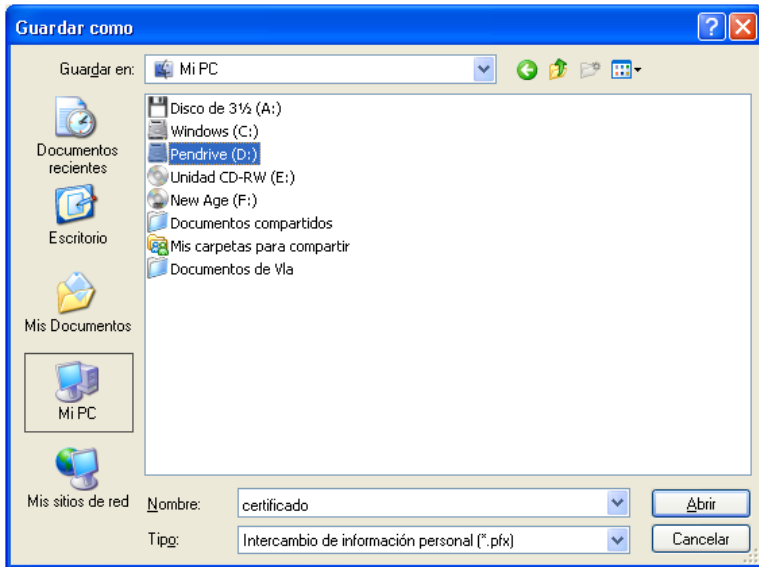
- Si optamos por exportar la clave privada, en la siguiente ventana podremos escribir la contraseña con la que protegeremos nuestro certificado. Introducimos la contraseña en las cajas “**Contraseña**” y “**Confirmar Contraseña**” y hacemos clic en el botón “**Siguiente**” para continuar.



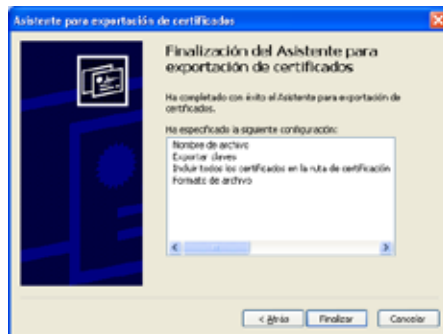
7. Ahora tenemos que especificar el nombre y la ruta en la que se guardará la copia de seguridad de nuestro certificado. Para ello, hacemos clic en el botón **“Examinar”** y utilizamos el explorador de Windows que aparecerá para localizar la ruta donde queramos guardar el archivo.

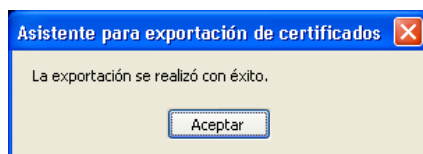


8. En nuestro caso vamos a exportar el certificado a un pendrive para poder llevárnoslo a otro ordenador. Para hacer esto, conectamos el pendrive al ordenador y lo seleccionamos, haciendo clic en el acceso directo **“Mi PC”** y doble clic en la unidad de disco que corresponda. Una vez que estemos en la ruta deseada de nuestro pendrive escribimos un nombre para el certificado, en la caja de texto **“Nombre”** y hacemos clic en el botón **“Guardar”**. Para continuar hacemos clic en el botón **“Siguiente”**.



9. En la siguiente ventana podemos visualizar la configuración que hemos utilizado para exportar nuestro certificado, si todo es correcto hacemos clic en el botón “**Finalizar**” y si no ha habido ningún problema nos aparecerá una ventana con el mensaje “**La exportación se realizó con éxito**”.

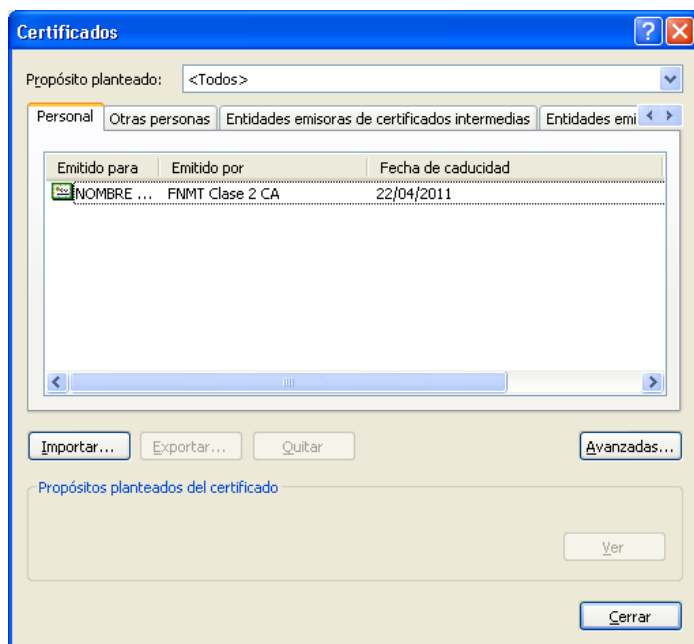




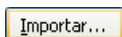
### Importar un certificado.

En el apartado anterior hemos visto cómo realizar una copia de seguridad de nuestro certificado, exportando los datos a un archivo. En este caso vamos a ver los pasos que tenemos que seguir para realizar el proceso contrario e instalar nuestro certificado utilizando el archivo que habíamos exportado:

1. Accedemos al almacén de certificados, siguiendo los pasos del apartado “**Comprobar la instalación del certificado**”, que hemos visto anteriormente.



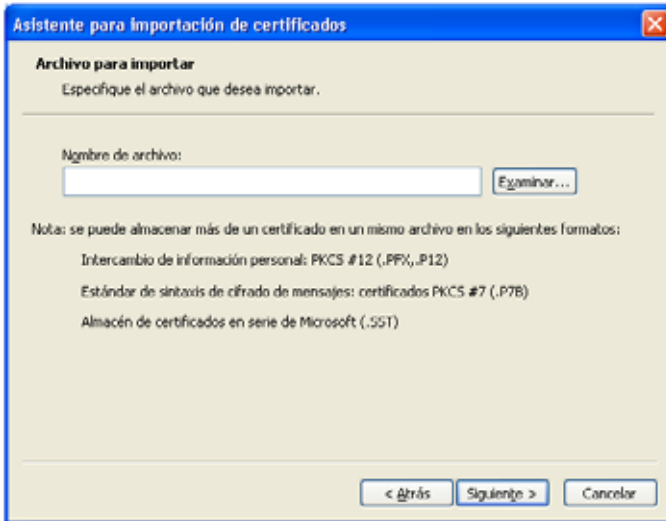
- Una vez localizado nuestro certificado, lo **seleccionamos** y hacemos clic en el botón **“Importar”**.



- Aparecerá el asistente para la importación de certificados. Para continuar el proceso hacemos clic en el botón **“Siguiente”**.



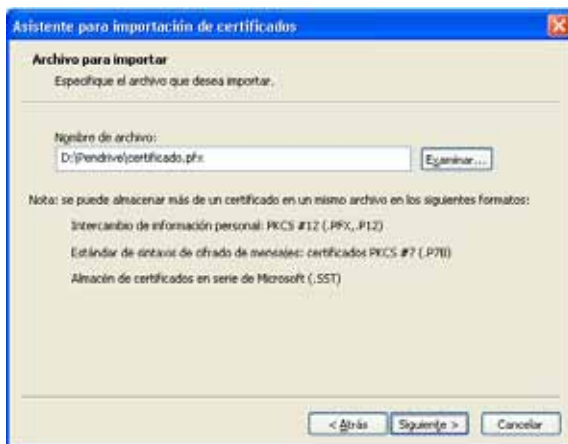
- En la siguiente ventana tenemos que introducir la ruta del archivo que exportamos y que contiene la información para instalar nuestro certificado. Para buscarlo manualmente hacemos clic en el botón **“Examinar”**.



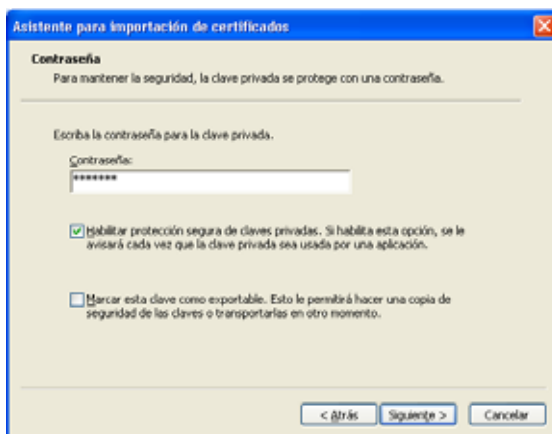
5. En nuestro caso cuando exportamos el archivo lo guardamos en un pendrive, por lo que para poder encontrar dicho archivo tendremos que conectar el pendrive al ordenador y utilizar el acceso directo "Mi PC" para acceder a la unidad deseada. Una vez dentro del pendrive seleccionamos el archivo correspondiente y hacemos clic en el botón "Abrir".



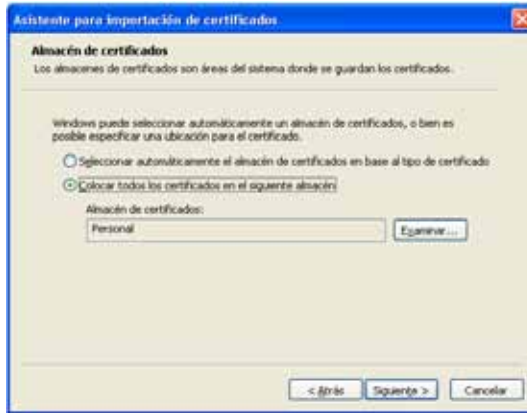
6. Volveremos a ver la ventana anterior con la ruta y el nombre del archivo escritos en la caja de texto “Nombre de archivo”. Para continuar hacemos clic en el botón “Siguiente”.



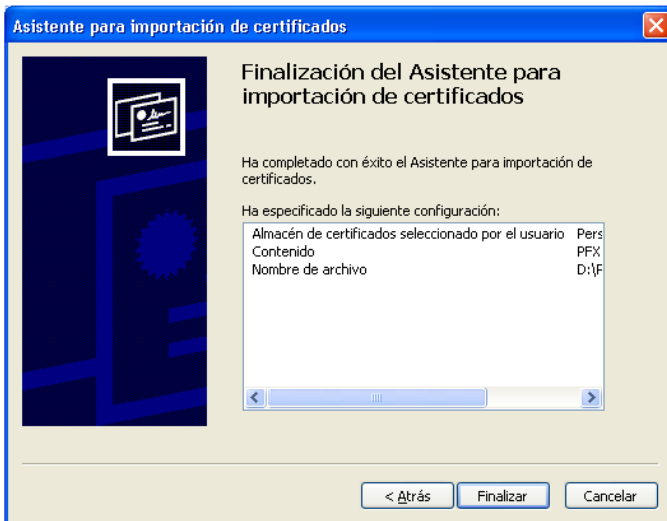
7. En caso de que seleccionásemos la opción de exportar la clave privada, a la hora de exportar el certificado, se mostrará una ventana donde tendremos que escribir la contraseña que elegimos. Una vez escrita la contraseña vamos a marcar la casilla “Habilitar protección segura de claves”, que nos permitirá configurar el nivel de seguridad del certificado una vez instalado.

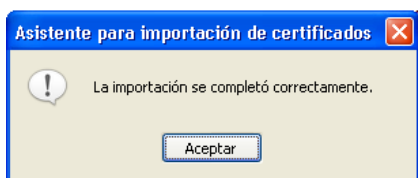


8. En la siguiente ventana podemos elegir el almacén en el que se instalará el certificado una vez finalizado el proceso. Dejamos marcada la opción que viene seleccionada por defecto y hacemos clic en el botón **“Siguiente”**.

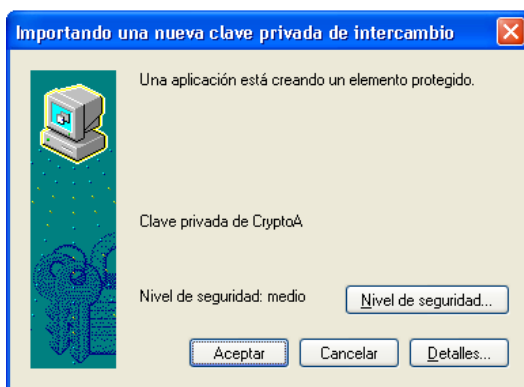


9. Una vez finalizado el proceso se nos muestra un resumen de la configuración establecida. Hacemos clic sobre el botón **“Finalizar”** y sobre **“Aceptar”** en la siguiente ventana, en la que nos avisará de que la instalación se realizó correctamente.

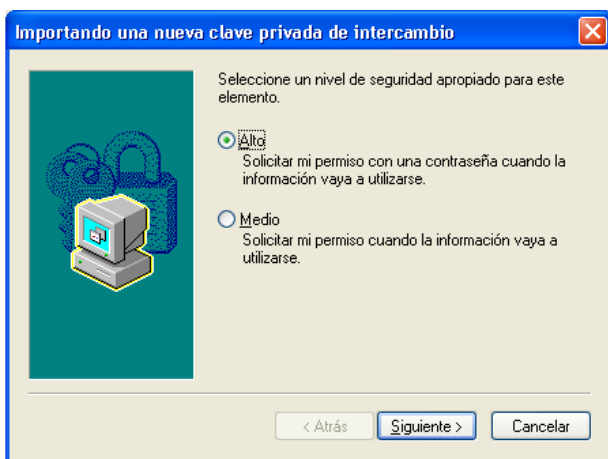




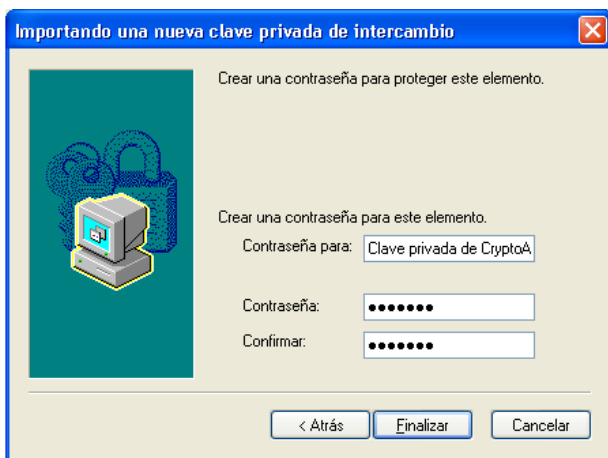
10. En la siguiente ventana podremos configurar el nivel de seguridad haciendo clic en el botón **"Nivel de seguridad..."**. Esta ventana sólo aparecerá en caso de que habilitemos la protección segura de claves en el paso número 7.



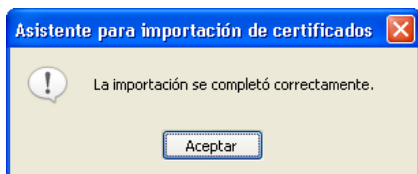
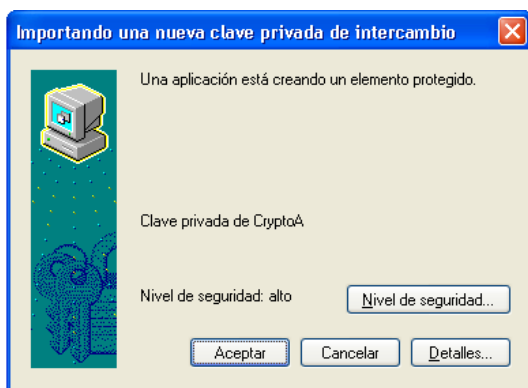
11. Si establecemos el nivel de seguridad como medio, el navegador nos solicitará permiso cuando se vaya a utilizar nuestro certificado. En nuestro caso vamos a seleccionar el valor **"Alto"**, para que además de avisarnos al usar nuestro certificado, también tengamos que introducir una contraseña. Para continuar hacemos clic en el botón **"Siguiente"**.



12. Ahora introducimos la contraseña deseada en las cajas de texto "Contraseña" y "Confirmar" y hacemos clic en el botón "Finalizar".

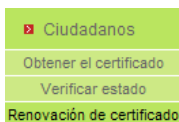


13. Volveremos a la ventana en la que nos muestra el nivel de seguridad seleccionado. Si todo es correcto hacemos clic sobre el botón "Aceptar" y aceptaremos de nuevo la ventana en la que nos avisa de que el proceso de importación se realizó con éxito.

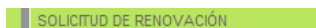


### Periodo de vigencia. Revocación del certificado.

El certificado de usuario tiene un periodo de vigencia de tres años. Para poder seguir utilizándolo transcurrido dicho periodo tendremos que renovarlo antes de la fecha de caducidad. Para ello accedemos a la página de CERES (“[www.cert.fnmt.es](http://www.cert.fnmt.es)”) y dentro del apartado “Ciudadanos” hacemos clic en enlace “Renovación de certificado”.



Seleccionamos la opción “Solicitud de renovación” del menú lateral izquierdo.



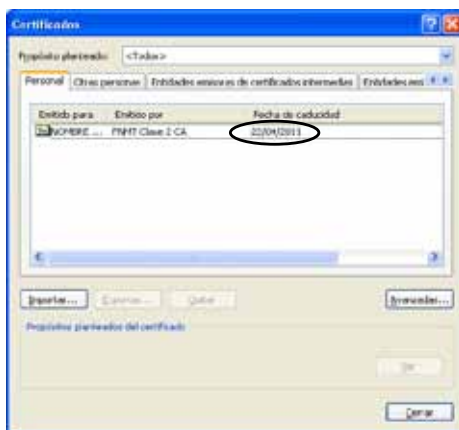
Leemos la declaración de privacidad y condiciones de uso y los aceptamos, haciendo clic en el botón “Aceptar” que encontraremos al final de la página.

**ACEPTAR**

Ahora se mostrarán los datos relativos a nuestro certificado. Si algo no es correcto podremos modificarlo haciendo clic en el botón **“Modificar”**, en caso contrario hacemos clic en el botón **“Renovar Certificado”**. Si todo es correcto nos mostrará un código que tendremos que introducir para descargar nuestro certificado renovado.

**RENOVAR CERTIFICADO**

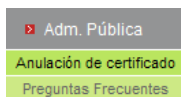
Podemos comprobar en cualquier momento la fecha de caducidad de nuestro certificado, accediendo al almacén de certificados de nuestro navegador. En caso de utilizar Internet Explorer tendremos que hacer clic en el menú **Herramientas** → **Opciones de Internet** → Pestaña **Contenido** → Botón **Certificados** y ahí podremos comprobar la fecha de caducidad de todos los certificados de los que dispongamos.



También podemos anular en cualquier momento nuestro certificado de usuario, si creemos que la seguridad de nuestra clave ha podido verse comprometida. Para ello, accedemos a la página de CERES (**“www.cert.fnmt.es”**) y hacemos clic en el enlace **“Obtenga el certificado de usuario”**.



Ahora hacemos clic en el enlace **“Anulación de certificado”**.



Seleccionamos de nuevo la opción **“Anulación de certificado”** del menú lateral izquierdo.



Una vez hecho esto, firmamos la anulación y la enviamos para que se haga efectiva, haciendo clic en los botones **“Firmar”** y **“Enviar”**, respectivamente.



### ¿Dónde puedo utilizar mi certificado de usuario?

En la página de CERES disponemos de un amplio listado de direcciones de páginas web en las que podemos hacer uso de nuestro certificado de usuario.

Para ver este listado basta con acceder a la página de CERES, escribiendo su dirección en la barra de direcciones **“www.cert.fnmt.es”** y pulsando la tecla **“Intro”**.

Una vez dentro de la página veremos un enlace en el lateral izquierdo de la página con el texto **“DONDE USAR EL CERTIFICADO”**.

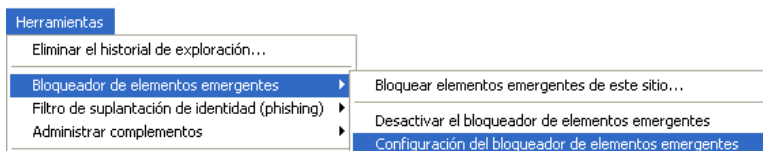


Al hacer clic en el enlace se cargará la página con todas las direcciones de Internet que permiten el uso de nuestro certificado de usuario. Para acceder a una página concreta del listado basta con hacer clic sobre su enlace y este nos llevará directamente a la dirección que hay escrita.

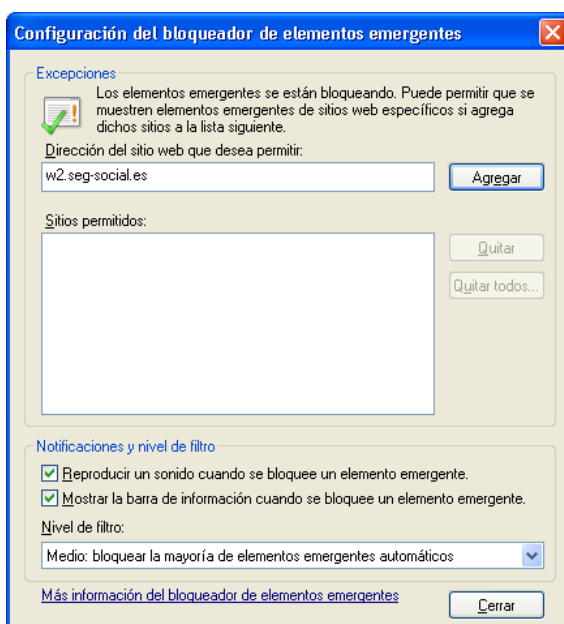
Vamos a ver un ejemplo de uso de nuestro certificado de usuario, solicitando un informe de vida laboral en la página de la Seguridad Social. Antes de nada, si utilizamos Internet Explorer como navegador, tenemos que indicarle que la página de la Seguridad Social

es totalmente fiable y que no debe bloquear ningún elemento de la misma. El proceso es muy sencillo:

- Una vez abierto el navegador hacemos clic en el menú “**Herramientas**”, seleccionamos la opción “**Bloqueador de elementos emergentes**” y dentro de esta la opción “**Configuración del bloqueador de elementos emergentes**”.



- En esta ventana, en la caja que aparece debajo del texto “**Dirección del sitio web que desea permitir**”, introducimos la dirección “**w2.seg-social.es**”. Una vez nos hemos asegurado de que la dirección está correctamente escrita hacemos clic en el botón “**Agregar**” que aparece a la derecha y veremos como la dirección se desplaza al listado de “**Sitios permitidos**”. Ya podemos cerrar la ventana haciendo clic en el botón “**Cerrar**” que aparece en la esquina inferior derecha de la ventana.



Una vez que hemos añadido la página de la Seguridad Social al listado de sitios fiables del navegador vamos a seguir los pasos que aparecen a continuación para solicitar un informe de vida laboral:

1. Accedemos a la página web de la Seguridad Social, bien desde el enlace que aparece en la página de CERES o escribiendo su dirección en la barra de direcciones “[www.seg-social.es](http://www.seg-social.es)” y pulsando la tecla “Intro”.



2. Para ver los servicios disponibles hacemos clic sobre el enlace “Sede electrónica”. En la pantalla que nos aparece accederemos a “Ciudadanos”.



3. Se abrirá una página con el listado de servicios que ofrece la Seguridad Social, dividido por servicios a los que podemos acceder sin certificado digital y a los que podemos acceder con certificado digital. Para ver los servicios disponibles con certificado digital hacemos clic en la pestaña “Servicios con Certificado Digital”.

### Servicios con Certificado Digital

4. Ahora nos aparecerá un listado de todos los trámites que podemos realizar con nuestro certificado digital o DNIe. Seleccionamos la opción **“Informe de vida laboral”**.

Servicios sin Certificado Digital	Servicios con Certificado Digital	Servicios con Certificado SII/CDN
	<ul style="list-style-type: none"><li><b>Informe de vida laboral:</b> Los informes de vida laboral contienen información respecto de las situaciones de alta o baja de una persona en el conjunto de los distintos regímenes del sistema de la Seguridad Social.</li><li><b>Informe de vida laboral actualizado:</b> A través de este servicio se programará al ciudadano un informe de vida laboral actualizado basándose en un rango de fechas, o bien a un régimen de encuadramiento o bien por código de cuenta de cotización.</li><li><b>Solicitud cambio de domicilio:</b> Con este servicio el usuario podrá realizar el cambio de domicilio que consta en la base de datos de la Seguridad Social.</li><li><b>Solicitud de rectificación de Informe de Vida Laboral:</b> Con este servicio se podrá solicitar la rectificación de datos de los diferentes situaciones que constan en los informes de vida laboral, así como la incorporación de situaciones inexistentes en todos ellos.</li><li><b>Solicitud de número de la Seguridad Social:</b> A través de este servicio se puede solicitar la asignación del número de Seguridad Social, siempre y cuando nunca haya tenido atribuido uno con anterioridad.</li><li><b>Solicitud de inscripción y asignación de CEE para empresas individuales:</b> A través de este servicio el empresario individual puede solicitar la asignación de código de cuenta principal y código de cuenta secundario.</li><li><b>Informe de Situación de Empresa Individual:</b> A través de este servicio el empresario individual podrá obtener un informe de cada uno de sus Códigos de Cuenta de Cotización.</li><li><b>Consultación de historial móvil y correo electrónico:</b> A través de este servicio se podrá realizar la consulta y/o modificación del historial móvil, teléfono fijo y correo electrónico.</li><li><b>Informe de vida laboral a fecha concreta:</b> A través de este servicio se podrá consultar u obtener un informe en el que</li></ul>	

5. En la siguiente página veremos una breve explicación de la forma de obtener el informe de vida laboral. Si lo hacemos con certificado digital lo obtendremos de forma inmediata mientras que si no lo hacemos sin certificado lo recibiremos en nuestro domicilio por correo ordinario. Para comenzar el proceso hacemos clic en el enlace **“Acceso al servicio”**.

#### SERVICIO A CIUDADANOS

### Informe de Vida Laboral.

[Acceso al servicio](#)

**Ampliación:**  
Personas con número de la Seguridad Social.

**Descripción:**  
El informe de vida laboral se puede obtener a través de dos vías distintas: los servicios con **certificado digital** y sin certificado digital.  
Con el servicio de obtención de informes de vida laboral **con certificado digital**, la impresión y/o consulta del informe se realiza en el mismo momento de su petición, a través de su propio ordenador.  
Con el servicio de obtención de informes de vida laboral **sin certificado digital**, el informe se obtiene a través del correo ordinario sin necesidad de presentarse en ninguna Administración de la Seguridad Social.  
El informe de vida laboral consta de una primera página en la que figuran los datos identificativos del solicitante, el número de días en situación de alta o la fecha de expiración del informe, notas informativas y otros posibles hechos en función de las circunstancias concretas de cada persona en su relación con la Seguridad Social.  
La segunda y, en su caso, posteriores páginas incluyen los diferentes periodos que tenga acreditados la persona titular del informe en el sistema de la Seguridad Social.  
Las **notas aclaratorias** del contenido del informe de vida laboral figuran en esta web.

6. En este paso tendremos que seleccionar el certificado con el que queremos autenticarnos:



7. Si todo es correcto se visualizará nuestro informe directamente en formato PDF y además tendremos la posibilidad de guardarlo o imprimirlo.

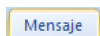
También podemos realizar la declaración de la Renta directamente en la web de la Agencia Tributaria o solicitar un borrador, todo sin movernos de nuestro ordenador y de una forma muy sencilla. Además de todo lo anterior se pueden realizar una infinidad de gestiones

más, tanto en estas dos páginas como en todas las que aparecen en el listado de la página de CERES. Estos trámites telemáticos con las distintas administraciones serán objeto de estudio en temas posteriores.

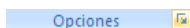
### Cifrar y firmar correos electrónicos.

Haciendo uso de un gestor de correo electrónico podemos enviar mensajes cifrados a otras personas y firmar correos recibidos utilizando nuestro certificado de usuario. En nuestro caso vamos a utilizar **Microsoft Office Outlook 2007** como gestor de correo.

Para realizar ambos procesos tenemos que seguir los mismos pasos. En caso de querer firmar un mensaje tendremos que abrirlo primero, si por el contrario lo que queremos es cifrarlo, tendremos que crear uno nuevo y rellenar todos los datos necesarios antes de su envío. Tras estos pasos hacemos clic en la pestaña **“Mensaje”**.



Accedemos a las opciones avanzadas, haciendo clic en el icono con la flecha inclinada que aparece a la derecha del marco **“Opciones”**.



En la siguiente ventana hacemos clic en el botón **“Configuración de seguridad”**.

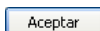


En esta ventana disponemos de dos casillas de verificación que podemos activar tanto para cifrar el mensaje como para firmarlo.

Cifrar el contenido del mensaje y los datos adjuntos

Agregar firma digital a este mensaje

Una vez activada la casilla correspondiente basta con pinchar en el botón **“Aceptar”**, para guardar los cambios y enviar el mensaje como hacemos normalmente. Siguiendo este proceso, el mensaje quedará firmado o cifrado con los datos de nuestro certificado de usuario.



## DNI Electrónico

### ¿Qué es el DNI Electrónico y para qué sirve?

El DNI Electrónico o DNIE es la evolución del DNI corriente para adaptar su uso a las necesidades de una sociedad sumergida en las Nuevas Tecnologías.

El DNIE tiene la misma funcionalidad que el DNI tradicional, es decir, sirve para conocer los datos identificativos de una persona con nacionalidad española, con la única diferencia de que el DNIE también hace posible la identificación por medios telemáticos, lo que a su vez nos permite firmar formularios y solicitudes a través de Internet o acceder a servicios de la administración y el gobierno sin movernos de casa.



Físicamente el DNIE sigue teniendo las mismas medidas, pero se ha confeccionado con un material plástico más resistente que permite una duración de unos 10 años aproximadamente. También se ha cambiado la disposición de los datos identificativos y se han incrementado los mecanismos de seguridad que impiden su falsificación.

Pero el gran cambio del DNIE es que incorpora un chip incrustado que permite leer los datos identificativos de la persona por medio de lectores apropiados.



Este chip contiene todos nuestros datos identificativos, así como una fotografía digital de nuestra firma manuscrita, una plantilla con nuestra huella dactilar y una serie de certificados electrónicos para podernos identificar y firmar electrónicamente.

### **Obtener un DNI Electrónico.**

Para poder obtener nuestro DNIE debemos personarnos en una oficina de expedición válida. Si no conocemos su situación podemos buscar una oficina en la siguiente página:

**[http://www.policia.es/documentacion/docu\\_esp/oficinas.html](http://www.policia.es/documentacion/docu_esp/oficinas.html)**

Los documentos que necesitamos presentar son los siguientes:

- Certificado de nacimiento, expedido por el Registro Civil correspondiente, con una antelación máxima de tres meses a la fecha de la solicitud del DNIE.
- Dos fotografías recientes y en color, tamaño carnet (32 x 26 mm), con fondo claro y liso.
- Certificado de empadronamiento del ayuntamiento donde tengamos el domicilio, expedido con una antelación máxima de tres meses a la fecha de la solicitud del DNIE.

Además de estos documentos, deberemos abonar la tasa legalmente establecida en el momento de la expedición.

Tanto el proceso de entrega de los documentos necesarios como el abono de las tasas y la expedición del DNIE se realizarán en la misma visita. Una vez finalizado el proceso de expedición nos harán entrega de un sobre que contiene un PIN generado de forma aleatoria y que necesitaremos para poder utilizar nuestro DNI Electrónico.

Podemos encontrar toda la información necesaria sobre el DNIE en su página oficial "[www.dnielectronico.es](http://www.dnielectronico.es)".

### **Requisitos e instalación del DNI Electrónico.**

Para poder utilizar nuestro DNIE necesitamos una serie de elementos, tanto hardware (equipo físico) como software (programas y controladores).

- **Hardware:**
  - o Ordenador personal Intel Pentium III o superior.
  - o Lector de tarjetas inteligentes compatible PC/SC (Personal Computer/Smart Card), que cumpla la normativa "ISO-7816".
  
- **Software:**
  - o Sistema Operativo Compatible: Windows 2000, XP o Vista, Linux, Unix y Mac OS.
  - o Controladores para el funcionamiento del lector de tarjetas inteligentes.
  - o Navegador web actualizado: Internet Explorer 6.0 ó superior, Mozilla Firefox 1.5 ó superior y Netscape 4.78 ó superior.
  - o Si somos usuarios de Windows necesitamos instalar el servicio CSP (Cryptographic Service Provider), cuya. En este apartado veremos cómo descargarlo e instalarlo. En caso de ser usuarios de Unix/Linux o Mac OS se requiere tener instalado el módulo PKCS#11.

En cuanto a los requisitos hardware, si no contamos con ellos, deberemos adquirirlos en un centro de venta apropiado, recordando las especificaciones técnicas necesarias para cada componente. Los lectores de tarjetas podemos encontrarlos en varios formatos:

- **Lectores en teclado:** el lector de tarjetas viene incorporado en el teclado del ordenador.
- **Lectores con conexión USB:** el lector se conecta al ordenador por medio de una clavija USB.
- **Lectores con conexión PCMCIA:** el lector se conecta al ordenador por medio de una tarjeta PCMCIA, especialmente diseñada para su conexión a equipos portátiles a través del puerto correspondiente.

Para la instalación de los controladores necesarios para el correcto funcionamiento de nuestro lector de tarjetas inteligentes debemos seguir las instrucciones de instalación del fabricante, que acompañan al lector de tarjetas. Estos controladores normalmente vendrán incorporados en un soporte de almacenamiento tipo CD.

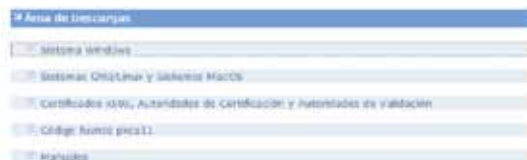
En el caso del navegador no suele ser necesaria la actualización, ya que normalmente se suele realizar de forma automática, pero en el caso de necesitarlo podemos hacerlo manualmente desde el propio navegador o desde su página oficial.

El servicio CSP deberemos instalarlo manualmente, así que vamos a ver los pasos necesarios para su descarga e instalación, que nos permitirá utilizar nuestro DNIE a través de Internet:

1. Accedemos a la página de descargas de la web oficial del DNIE: **“[www.dnielectronico.es/descargas/index.html](http://www.dnielectronico.es/descargas/index.html)”**.



2. Dentro de la página visualizaremos un área de descargas, con distintos apartados para cada uno de los sistemas operativos existentes y otras opciones. Si nuestro sistema operativo pertenece a la familia Windows haremos clic en el enlace **“Sistema Windows”**.



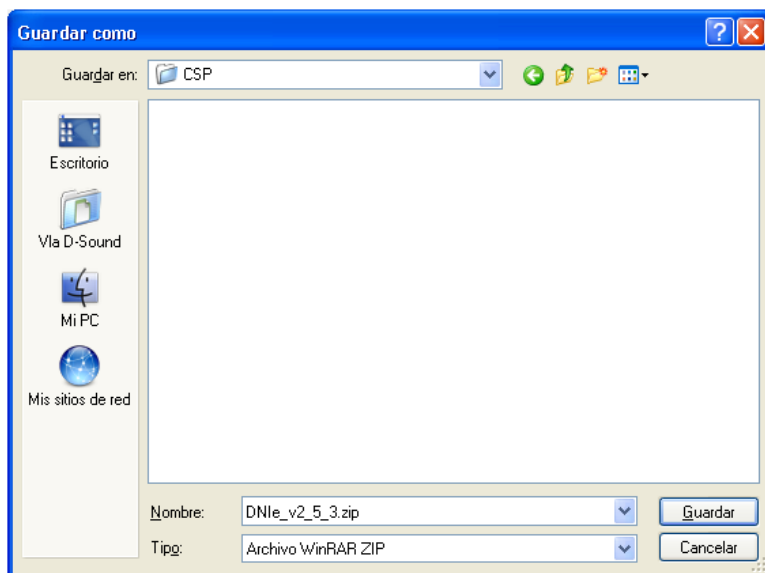
3. En la siguiente página nos aparecerán las acciones disponibles para sistemas Windows. Para descargar el CSP hacemos clic en el enlace **“Sistemas Windows. Compatible con Vista”**.



4. Aparecerá la ventana de descargas para elegir qué hacer con el archivo. Hacemos clic en el botón **“Guardar”**.



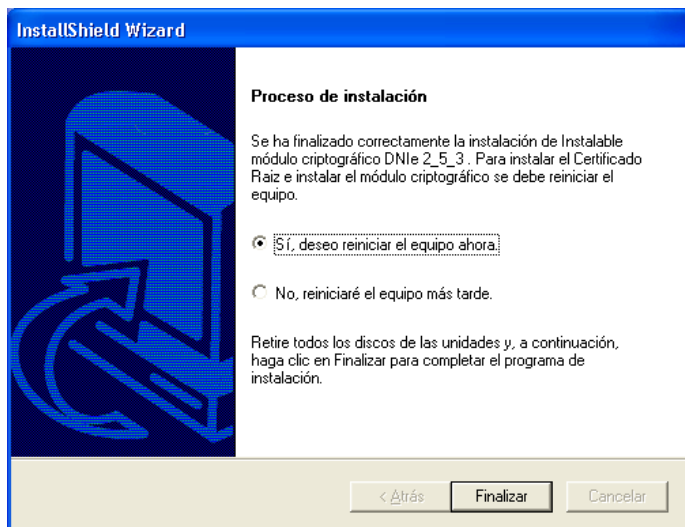
5. Nos aparecerá el explorador de Windows para elegir la carpeta donde queremos guardar el archivo. Una vez elegida la carpeta hacemos clic en el botón **“Guardar”** y aparecerá la ventana con el progreso de la descarga del archivo.



6. Una vez descargado el archivo nos situaremos en la ruta donde lo hayamos guardado, utilizando para ello el Explorador de Windows, y extraeremos su contenido con un compresor como WinZip, Winrar o FilZip. Una vez extraído veremos un icono como el que aparece a continuación.



7. Para terminar con el proceso hacemos doble clic sobre el icono del archivo que hemos descomprimido y la instalación se realizará automáticamente. Una vez finalizado el proceso de instalación nos aparecerá una ventana en la que podemos elegir entre reiniciar el equipo en ese momento o no reiniciarlo si tenemos pensado hacerlo más tarde. Para terminar hacemos clic en el botón **“Finalizar”** y una vez reiniciado el equipo ya dispondremos del servicio CSP para poder hacer uso de nuestro DNI Electrónico.




### Verificar el funcionamiento de nuestro DNI Electrónico.

Si ya hemos realizado la instalación del software necesario y contamos con los requisitos hardware indicados, ahora ya sólo nos queda comprobar que nuestro DNle funciona correctamente. Para ello vamos a seguir los pasos que aparecen a continuación:

1. Introducimos nuestro DNle en el lector de tarjetas y accedemos a la página oficial del DNI Electrónico escribiendo su dirección en la barra de direcciones.

**[www.dnielectronico.es](http://www.dnielectronico.es)**

2. En la página principal, hacemos clic en el enlace **“Compruebe su DNI”**.

 **Compruebe su DNI**

Verifique el estado de los certificados digitales y compruebe el funcionamiento de su DNI electrónico

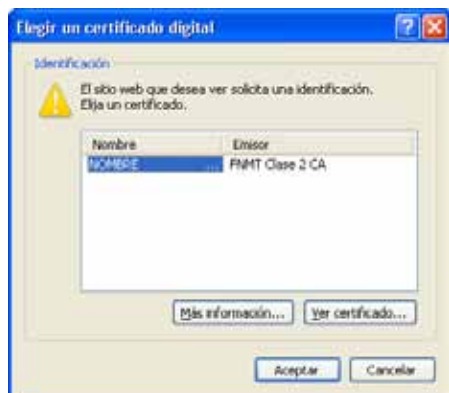
3. Utilizando las barras de desplazamiento o la rueda del ratón nos desplazamos hacia la parte inferior de la página y hacemos clic en el enlace “**Comprobación de certificados**”.

[Comprobación de certificados](#)

Al hacer clic nos pedirá introducir el PIN que nos entregaron. Si una vez introducido nos aparece una pantalla como la siguiente, sabremos que nuestro DNIE funciona correctamente y ya estamos listos para empezar a utilizarlo.



Si por el contrario nos aparece una ventana como la siguiente significará que algo no funciona correctamente.



En este caso comprobaremos que el DNIE se ha insertado correctamente en el lector de tarjetas, nos aseguraremos de que el PIN introducido sea correcto y revisaremos que hemos seguido todos los pasos necesarios. Si el fallo persiste al volver a realizar todos los pasos deberemos acudir a la oficina de expedición para revisar el estado del chip y las posibles causas que pueden impedir su funcionamiento.

### ¿Dónde puedo utilizar el DNI Electrónico?

Una vez que hemos verificado que nuestro DNIE funciona correctamente podemos acceder a la página oficial del DNI Electrónico para comprobar las direcciones donde es posible realizar trámites utilizando nuestro DNIE.

Podemos navegar por su web “[www.dnielectronico.es](http://www.dnielectronico.es)” para buscar dicha información o acceder directamente a la página de servicios disponibles, introduciendo la siguiente dirección en la barra de direcciones de nuestro navegador:

[www.dnielectronico.es/servicios\\_disponibles/index.html](http://www.dnielectronico.es/servicios_disponibles/index.html)

En esta página encontraremos una serie de servicios divididos por categorías, según el organismo que ofrezca dicho servicio.

### Inicio / Servicios Disponibles / **Servicios Disponibles**

#### Servicios Disponibles

Ofrecer servicios a los ciudadanos y a las empresas por medios telemáticos es un objetivo prioritario tanto para la Administración General del Estado, como para las Administraciones de las Comunidades Autónomas

- 📁 **Servicios DNI-e de la Administración General del Estado**
- 📁 Servicios DNI-e de las Comunidades Autónomas
- 📁 Servicios DNI-e de la Administración Local
- 📁 Otros Organismos Públicos
- 📁 Sector Privado

Al hacer clic en una categoría se mostrará una página con una serie de enlaces, en los que al hacer clic nos llevarán a la página oficial del organismo seleccionado.

### Inicio / SERVICIOS DISPONIBLES/ **Administración General del Estado**

#### Administración General del Estado

- 📁 Agencia Española de Protección de Datos
- 📁 **Gerencia de Informática de la Seguridad Social**
- 📁 INEM - Servicio Público de Empleo Estatal
- 📁 Ministerio de Administraciones Públicas
- 📁 Ministerio de Administraciones Públicas - MUFACE
- 📁 Ministerio de Administraciones Públicas - DIAP
- 📁 Ministerio de Cultura
- 📁 Ministerio de Economía y Hacienda - Dirección General del Catastro
- 📁 Ministerio de Economía y Hacienda - Dirección General de Costes de Personal y Pensiones Públicas
- 📁 Ministerio de Economía y Hacienda - Dirección General de Defensa de la Competencia
- 📁 Ministerio de Economía y Hacienda - Dirección General de Seguros y Fondos de Pensiones
- 📁 Ministerio de Economía y Hacienda - Dirección General del Tesoro y Política Financiera
- 📁 Ministerio de Economía y Hacienda - Instituto de Contabilidad y Auditoría de Cuentas
- 📁 Ministerio de Economía y Hacienda - Junta de Contratación
- 📁 Ministerio de Economía y Hacienda - Inspección General
- 📁 Ministerio de Economía y Hacienda - Dirección General de Patrimonio
- 📁 Ministerio del Interior
- 📁 Ministerio del Interior - Dirección General de Tráfico
- 📁 Ministerio de Fomento
- 📁 Ministerio de Industria, Turismo y Comercio
- 📁 Instituto Nacional de Estadística
- 📁 Ministerio de Medio Ambiente y Medio Rural y Marino
- 📁 Ministerio de Medio Ambiente y Medio Rural y Marino - FEGA
- 📁 Ministerio de Sanidad y Consumo - Instituto de Salud Carlos III
- 📁 Ministerio de Trabajo e Inmigración

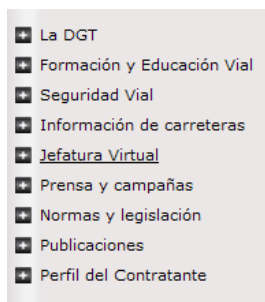
Para poder realizar los trámites necesarios sólo tenemos que seguir las indicaciones que encontraremos en cada página, que nos irá guiando en todo momento, recordando no extraer el DNIe del lector de tarjetas para que los datos se puedan leer correctamente.

Como ejemplo vamos a ver los pasos necesarios para consultar el saldo de puntos de nuestro carnet de conducir:

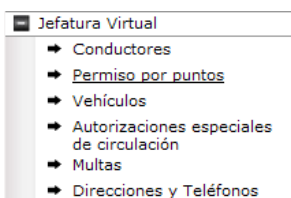
- Primero tenemos que insertar nuestro DNI Electrónico en el lector de tarjetas y acceder a la página de la DGT, introduciendo su dirección “[www.dgt.es](http://www.dgt.es)” en la barra de direcciones y pulsando la tecla “Intro”.



- Seguidamente hacemos clic en el enlace “**Jefatura Virtual**”, que aparece en el menú lateral izquierdo de la página, para ver los servicios disponibles.



- Se desplegarán todas las opciones que pertenecen a la Jefatura Virtual. Nosotros hacemos clic en el enlace “**Permiso por puntos**”.



- En el centro de la página veremos un listado con las acciones que podemos realizar. En nuestro caso vamos a hacer clic en el enlace **“Saldo de puntos y antecedentes (Con certificado)”**.



- En la siguiente ventana nos aparecerá un listado con los certificados que tengamos instalados, seleccionamos el que corresponda, que en nuestro caso será el correspondiente al DNI Electrónico y hacemos clic en el botón **“Aceptar”**.



- A continuación se mostrarán nuestros datos personales junto con el saldo actual de los puntos de nuestro carnet de conducir.



Vemos como también nos muestra el “Historial de antecedentes” en el que podemos ver en detalle los movimientos realizados sobre nuestros puntos.

## Medidas de seguridad

Durante los apartados anteriores hemos visto la obtención y posterior utilización del certificado digital y DNI electrónico. Como hemos podido comprobar el uso de los mismos está directamente relacionado con la autenticación o identificación de una persona o entidad, es decir, usamos los certificados digitales para decir ante un tercero (normalmente la Administración) que somos nosotros y no otra persona, por eso sustituye a la firma manuscrita (que también nos identifica inequívocamente).

Cuando hablamos de autenticarnos ante otra persona o entidad cobra especial importancia la seguridad, es decir, si no tomamos las medidas de seguridad oportunas otra persona se podrá apropiarse fácilmente de nuestra identidad y así poder realizar cualquier trámite, compra o transacción en nuestro nombre. En el caso que nos ocupa las medidas de seguridad estarán muy relacionadas con el uso de contraseñas seguras, ya que es la forma que tenemos de usar nuestro certificado digital solo nosotros, ya que nuestra contraseña no es conocida por nadie más (o al menos eso sería lo ideal).

### Las contraseñas cómo método de autenticación

Las contraseñas son las claves que se utilizan para obtener acceso a información personal o autenticarnos con nuestro certificado digital o DNLe.

Si algún delincuente o un usuario malintencionado consigue apoderarse de esa información, puede utilizar el nombre para abrir nuevas cuentas de tarjetas de crédito, solicitar una hipoteca o suplantarle en transacciones en línea. En muchos casos, no llegaríamos a darnos cuenta de un ataque de ese tipo hasta que fuera demasiado tarde.

A priori podíamos pensar que se trata de una forma de identificación del usuario débil, a lo que podíamos aducir los siguientes motivos:

- Dado que las contraseñas deben recordarse, normalmente se eligen de forma que sean fáciles de recordar. La consecuencia es que serán igualmente fáciles de adivinar.

- Se presentan variadas ocasiones para robarlas: alguien puede mirar por encima del hombro de la persona que está escribiendo su contraseña; existen distintos tipos de software que permiten obtener contraseñas ajenas.
- Se pueden compartir por varios usuarios.
- Uso de contraseñas cortas.
- Pueden ser anotadas en otros dispositivos o medios menos seguros (cuadernos, hojas,...) dejándose al alcance, incluso a la vista, de otras personas.

En los siguientes apartados veremos diferentes formas de que nuestras contraseñas sean seguras y las podemos usar como un método de autenticación fuerte.

### Crterios para la creaci3n de contraseñas seguras

Para un atacante, una contraseña segura debe parecerse a una cadena aleatoria de caracteres. Se puede conseguir que la contraseña sea así siguiendo los siguientes criterios:

- **Que no sea corta:** Cada carácter que agrega aumenta el grado de protección que ofrece ésta. Las contraseñas deben tener 8 caracteres como mínimo; 14 caracteres o más sería lo ideal.
- **Combine letras, números y símbolos:** Cuantos menos tipos de caracteres haya en la contraseña, más larga deberá ser ésta. No se limite a los caracteres más comunes, su contraseña será mucho más segura si elige entre todos los símbolos del teclado.
- **Utilice palabras y frases que le resulte fácil recordar, pero que a otras personas les sea difícil adivinar:** El medio más sencillo de recordar sus contraseñas y frases codificadas consiste en anotarlas. Al contrario que lo que se cree habitualmente, no hay nada malo en anotar las contraseñas, si bien estas anotaciones deben estar debidamente protegidas para que resulten seguras y eficaces.

## Malas prácticas para la creación de contraseñas

Algunos métodos que suelen emplearse para crear contraseñas resultan fáciles de adivinar para un delincuente. A fin de evitar contraseñas poco seguras, se debe eludir:

- **Contraseñas fáciles de adivinar:** Como contraseña se utiliza nuestro propio nombre, el de nuestra pareja o el de alguien conocido. También se suele utilizar una dirección, fecha de nacimiento, etc. Resultaría fácil de averiguar por alguien que nos conozca.
- **Usar contraseñas predecibles o palabras del diccionario:** Existen programas capaces de identificar contraseñas a partir de diccionarios, por lo que no es aconsejable hacer uso de palabras del vocabulario.
- **Recordatorio de contraseñas:** Internet Explorer incorpora la posibilidad de recordar el campo de contraseña cuando se accede a un formulario de identificación de usuario, ya sea un correo electrónico, una página web con registro de usuario,... Si se decide hacer uso de dicha función, se debe ser consciente que cualquier individuo que tenga acceso al equipo con nuestro usuario, también tendrá acceso a los lugares donde se tenga la clave guardada por defecto.
- **Uso de la misma contraseña:** No es recomendable utilizar la misma contraseña para todo. Contar con distintas contraseñas para cada una de las cuentas es la mejor manera de mantener la integridad de los datos.
- **No proteger el lugar de almacenamiento de las contraseñas:** de nada sirve tener una contraseña segura si posteriormente esta se almacena en un sitio inseguro. Por ejemplo, podemos tener una puerta acorazada de máxima seguridad para evitar robos en nuestro domicilio, pero si dejamos la llave debajo del felpudo de la puerta lo más seguro es que alguien la encuentre y pueda acceder sin problemas al domicilio.