# Manual de Usuario del Certificado Digital

Cabildo de Gran Canaria

Septiembre de 2012

# Contenidos

# 1. Firma Electrónica

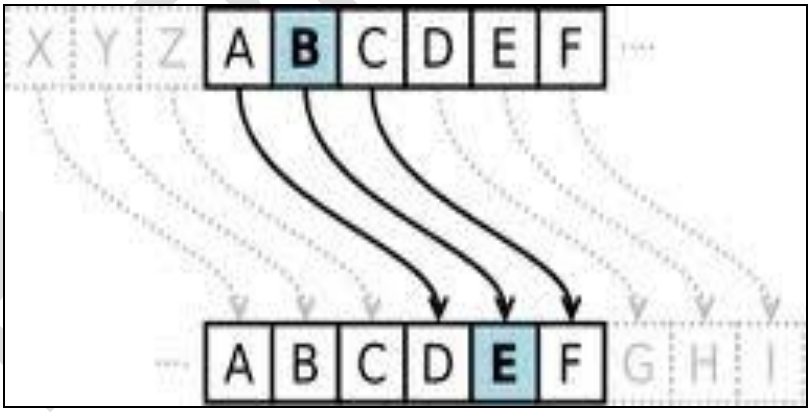
## 1.1. Criptografía

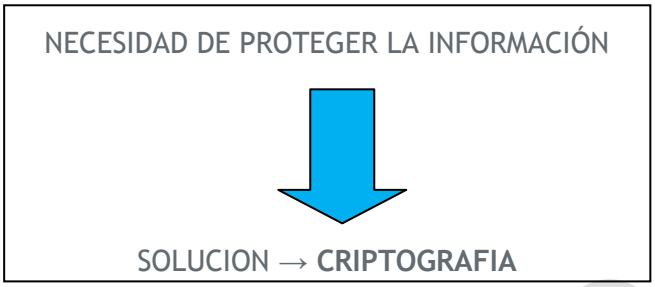
**CRIPTOGRAFÍA**: La principal aplicación de la criptografía es la de proteger información para evitar que sea accesible por observadores NO autorizados.

A lo largo de la historia siempre ha habido necesidad de proteger la información:

- para comprobar la identidad del interlocutor
- únicamente el destinatario seleccionado debe recibir la información y ésta no puede haber sido modificada.

En el Imperio Romano, Julio César utilizó una forma simple para comunicarse con sus generales: desplazar cada letra del alfabeto un número determinado de posiciones.






En el "mundo electrónico" actual, la **seguridad** toma gran importancia ya que se requiere de algún sistema que solvente el principal problema que surge al no existir contacto directo entre las partes implicadas y los riesgos que esto conlleva.

CRIPTOGRAFIA
- FIRMA ELECTRONICA
- CERTIFICADO DIGITAL

## 1.2. Proteger la información

Los **certificados digitales** y la **firma electrónica** son instrumentos capaces de garantizar la seguridad en las comunicaciones y la identidad de los usuarios, permitiendo la comprobación de la procedencia y asegurando la integridad de los mensajes intercambiados a través de la red.

Ambos se basan en tres fundamentos:

- **Confidencialidad:** sólo se muestran los datos o páginas al usuario autorizado a ello.
- **Integridad**: nos aseguramos de que los mensajes intercambiados llegan a su destinatario sin modificaciones.
- **No repudio**: que el emisor o el receptor no se puede desdecir del propio mensaje.

## 1.3. Que es la Firma Electrónica

> *La firma electrónica es el conjunto de datos electrónicos que sirve para demostrar la autenticidad de un mensaje*

Permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.

## 1.4. Aclaraciones

- Una **Firma Digital** es aquella firma electrónica que está basada en los sistemas de criptografía de clave pública ***(PKI - Public Key Infrastructure)***.


*Ilustración 1: Ejemplo de Firma Digital*

- Una **Firma Digitalizada**, no tiene nada que ver con las anteriores. Se trata de una simple representación gráfica de la firma manuscrita obtenida a través de un escáner, que puede ser "pegada" en cualquier documento.

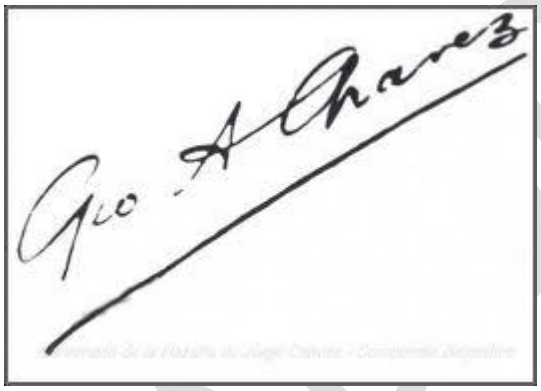


*Ilustración 2: Ejemplo de Firma Digitalizada*

# 2. Certificado Digital

## 2.1. Que es

*Instrumento en soporte digital para acreditar la identidad y firmar documentos de manera electrónica.*

El Certificado Digital es un documento digital que contiene sus datos identificativos y le permite identificarse en Internet e intercambiar información con otras personas con la garantía de que sólo Ud. y su interlocutor pueden acceder a ella.

Pueden ser emitidos por diversas entidades: **Prestador de Servicios de Certificación.**



## 2.2. Para que sirve

*Permite realizar trámites de forma segura con la Administración Pública a través de Internet*

El Certificado de Usuario es la herramienta básica para la realización de gestiones las 24 horas del día, desde su propio ordenador sin necesidad de desplazarse.


## 2.3. Tipos de Certificados Digital

Según el ámbito de utilización, podrían clasificarse en tres grandes bloques:

**CIUDADANOS**

*http://www.cert.fnmt.es/index.php?cha=cit&lang=es*

**EMPRESAS**

*http://www.cert.fnmt.es/index.php?cha=com&lang=es*

**ADMINISTRACIÓN PUBLICA**

*http://www.cert.fnmt.es/index.php?cha=adm&lang=es*

Algunos de los certificado digitales más representativos son:

- **Personal o de Usuario:** acredita la identidad del titular
- **De persona jurídica:** identifica una empresa o sociedad como tal a la hora de realizar trámites ante las administraciones o instituciones

- **De representante:** el titular del certificado se identifica no únicamente como persona física perteneciente a una empresa sino que añade su cualificación como representante legal ó apoderado general de la misma

- **De empleado Público:** permiten identificar telemáticamente a los suscriptores como Administraciones Públicas, y a los firmantes como personas al servicio de las mismas. (*requiere tarjeta criptográfica*)

# 3. Obtención Certificado Digital

La FNMT a través de su departamento **CERES** (CERtificación ESpañola) facilita el certificado digital a través de la página *www.cert.fnmt.es*:

El proceso de solicitud s compone de tres pasos:

1) Solicitar el certificado a través de la web.

2) Acreditar tu identidad en una oficina de registro o utilizar tu DNIe y lector de tarjetas para realizar una acreditación virtual.

3) Descargar el certificado desde el equipo solicitante.

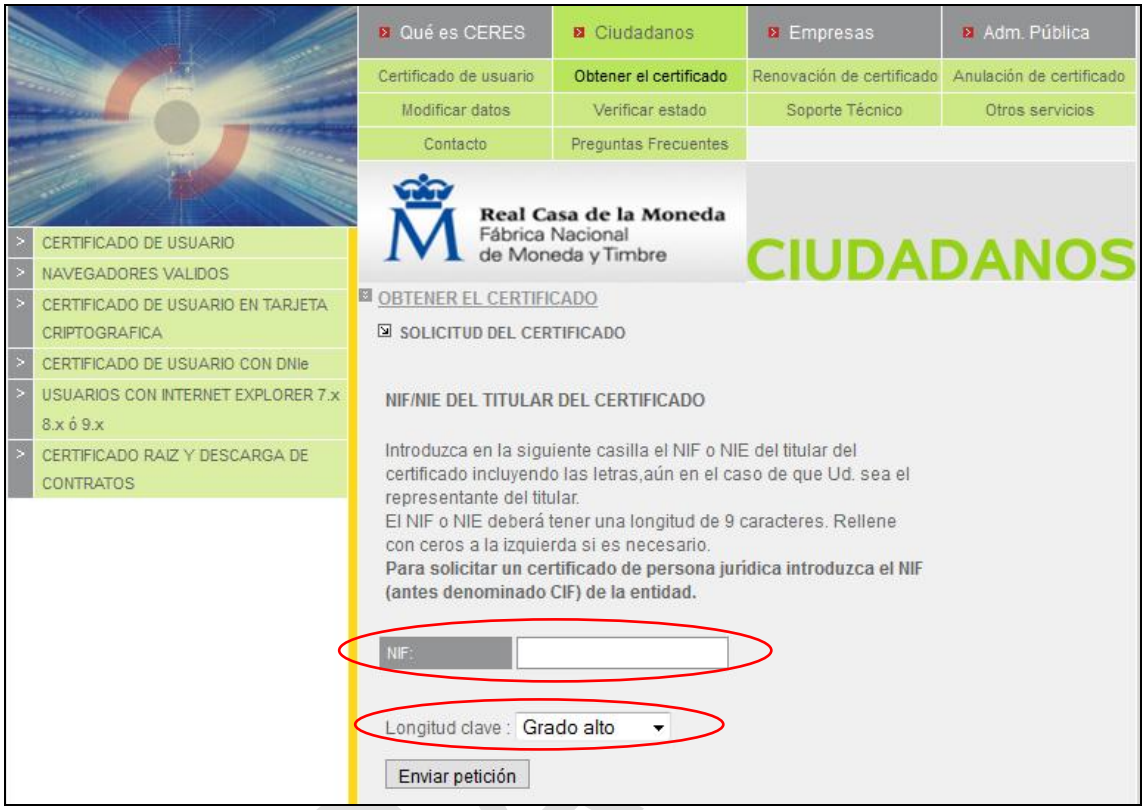
## 3.1. Solicitar Certificado

Para realizar el primer punto, se debe acceder a la página *www.cert.fnmt.es* y seleccionar la opción "*Obtenga el CERTIFICADO de Usuario*" (parte superior derecha de la pantalla).


Cuando se accede a la nueva página, se debe pulsar sobre el enlace "*Solicitud del certificado*" situado en el menú del margen izquierdo de la pantalla.


En la pantalla a la que se accede se muestran dos campos:

- **NIF:** se debe introducir el NIF del solicitante
- **Nivel de Seguridad:** Si su ordenador pueda ser utilizado por varias personas y quiere que el uso de su certificado esté protegido con una contraseña, deberá seleccionar la opción "Alto". Si no es así, seleccione la opción "Medio". para continuar el proceso.

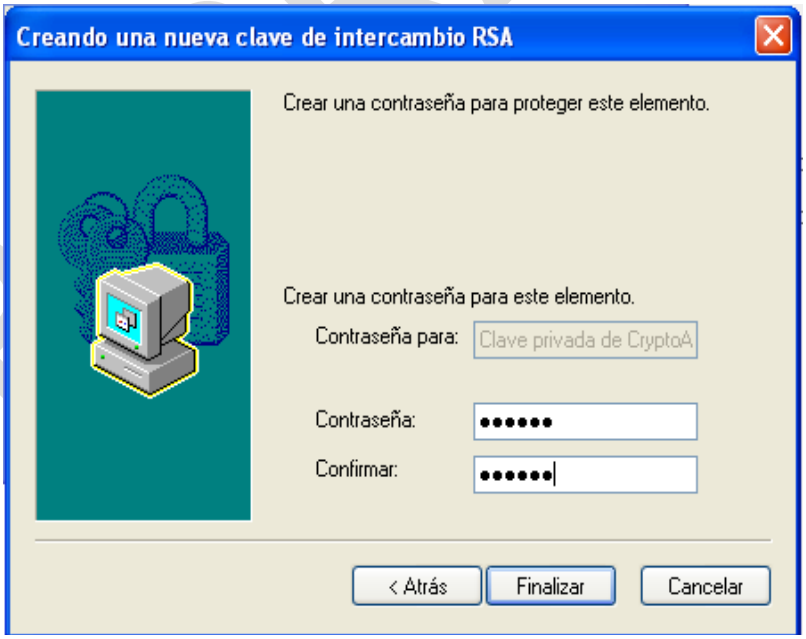



### 3.1.1. Configurar Nivel de Seguridad

Se recomienda que cuando varias personas puedan tener acceso al mismo ordenador, se seleccione la opción “Alto” para el nivel de seguridad.

- Nivel Medio: **NO SE SOLICITA NINGUNA CONTRASEÑA PARA USAR EL CERTIFICADO**
- Nivel Alto: **SE SOLICITA CONTRASEÑA PARA USAR EL CERTIFICADO**


El sistema le va a solicitar que establezca una contraseña para el acceso a su certificado y que confirme la misma. Esa contraseña le será solicitada cada vez que pretenda hacer uso del certificado y podría denominarse **contraseña de uso**.

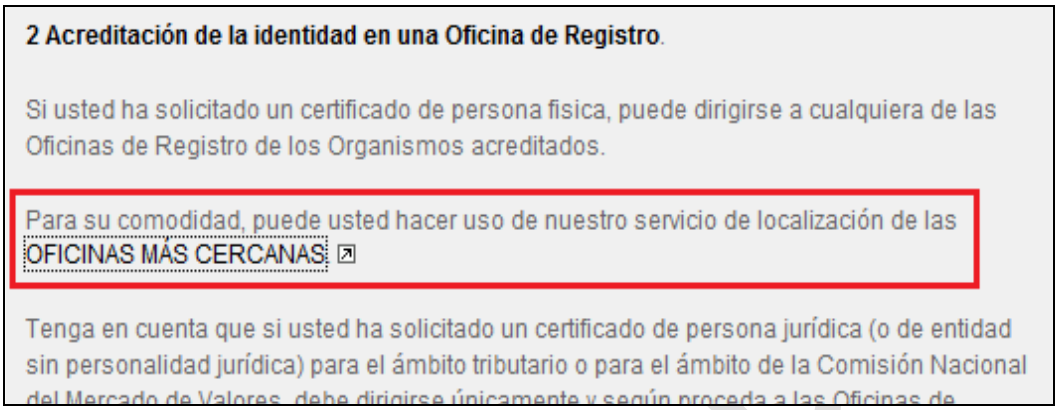


Una vez seleccionado el nivel de seguridad y aceptado el mismo, aparece en la pantalla el código de solicitud asociado al certificado, que se debe imprimir o apuntar para dirigirse a cualquiera de las Oficinas de Registro de los Organismos acreditados.


## 3.2. Acreditar identidad

Este punto es muy importante y su finalidad es la de identificarse como la persona que realmente ha solicitado el certificado. Con el código obtenido en el punto anterior y el documento identificativo (DNI, NIE. pasaporte) se deberá presentar en una oficina de acreditación. En dicha oficina se consignarán una serie de datos personales (apellidos, nombre, e-mail,…) y se emitirá un contrato de uso del certificado que deberemos firmar por triplicado.

Se puede hacer uso del servicio de localización de las OFICINAS MAS CERCANAS que le aparece en la pantalla de obtención del certificado:

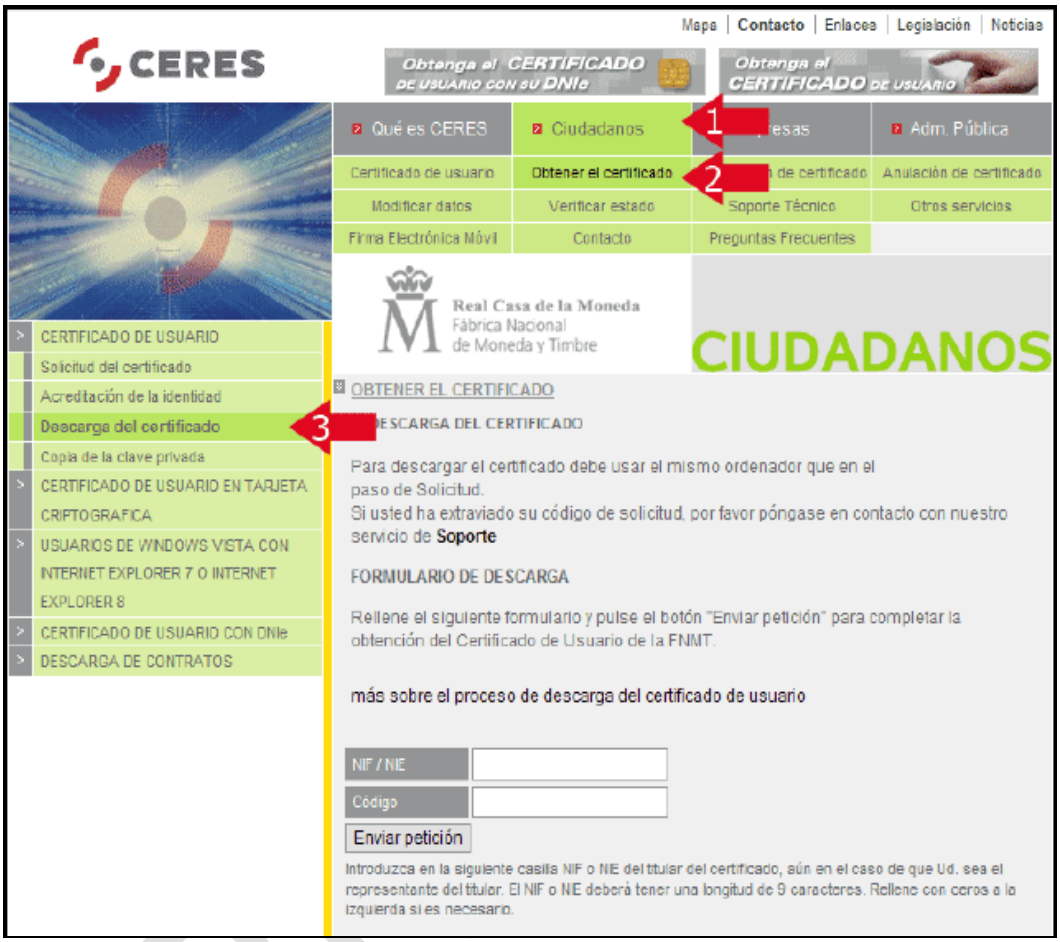



## 3.3. Descargar Certificado

Una vez que acreditada la identidad en una Oficina de Registro, se podrá realizar la descarga del certificado desde la página web, y sin que medie ningún aviso o notificación.

***La FNMT indica que es necesario esperar alrededor de 24 horas entre la visita a la oficina de acreditación y la descarga***

Se puede descargar el certificado desde la pantalla que se muestra al pulsar la opción “Descarga del certificado”.




### 3.3.1. Como verificar si el Certificado Digital está instalado

- **Internet Explorer** → Accediendo al menú Herramientas -> Opciones de Internet -> pestaña Contenido, pulsar el botón Certificados, y consultar en la pestaña Personal los certificados de usuario instalados para ese navegador.

- **Mozilla Firefox** → Accediendo al menú Herramientas -> Opciones -> Avanzado -> pestaña Cifrado y pulsar en Ver Certificados, que mostrará la lista de certificados de usuario disponibles para ese navegador en la pestaña Sus certificados.

# 4. Copia de Seguridad del Certificado Digital

Una vez instalado el certificado digital de usuario en el ordenador, es conveniente realizar una copia de seguridad para:

- poder utilizarlo en otros ordenadores.
- no perderlo como consecuencia de un borrado de datos en el ordenador o una avería.

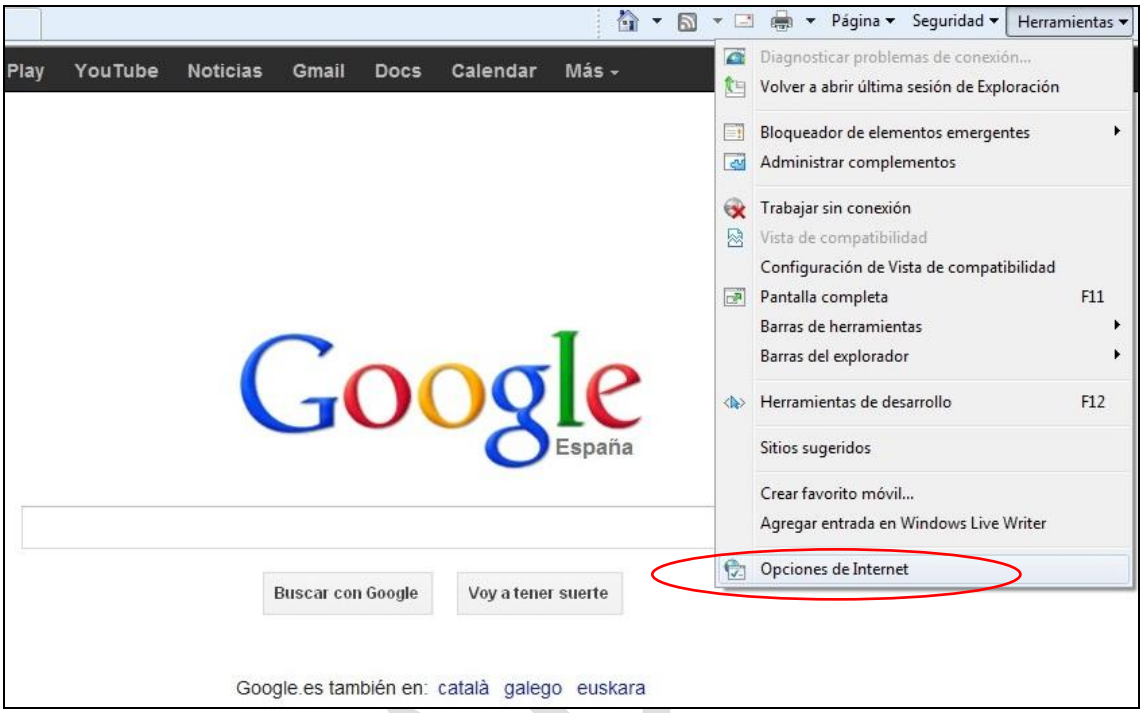
***Para hacer una copia de seguridad del certificado es necesario exportarlo del navegador en el que se ha instalado.***

## 4.1. Exportar el Certificado Digital

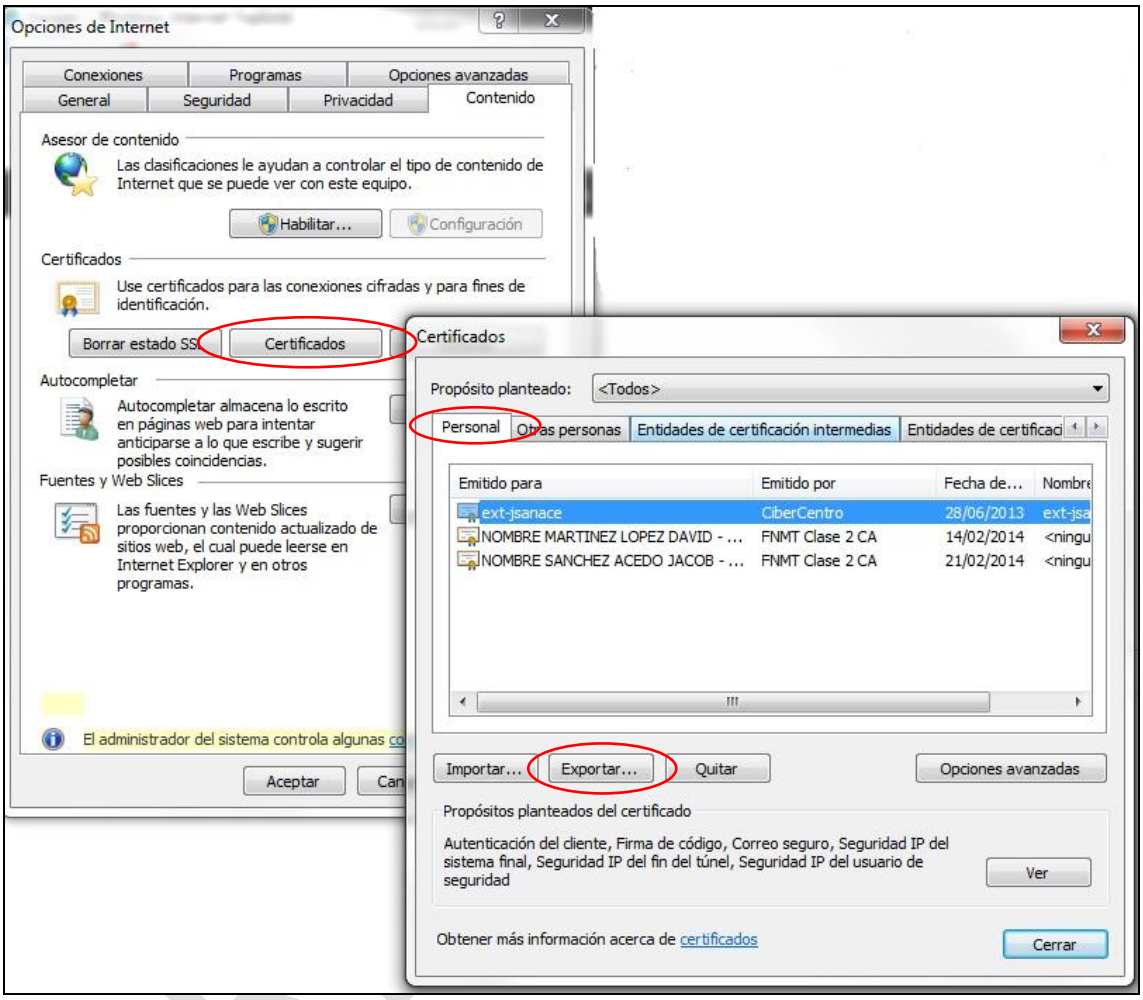
A continuación se detalla el proceso de **exportación** de un Certificado Digital en Internet Explorer, aunque el proceso es similar para otros navegadores y versiones.

**Exportación en Internet Explorer**

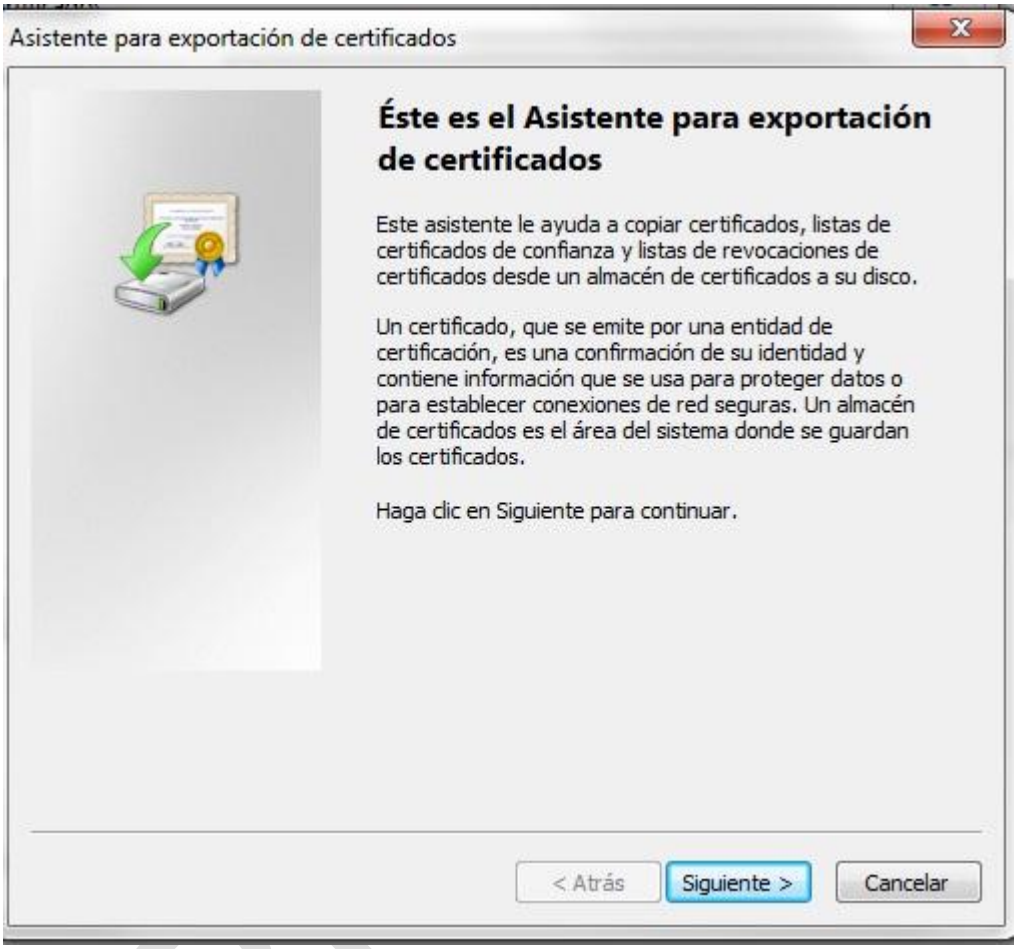
Accediendo al menú Herramientas → Opciones de Internet → pestaña Contenido, se muestra el botón Certificados.




Al pulsarlo nos aparecerán varias pestañas. Elegimos la de *"Personal"* y allí aparecerán los certificados que estarán instalados para ese navegador.

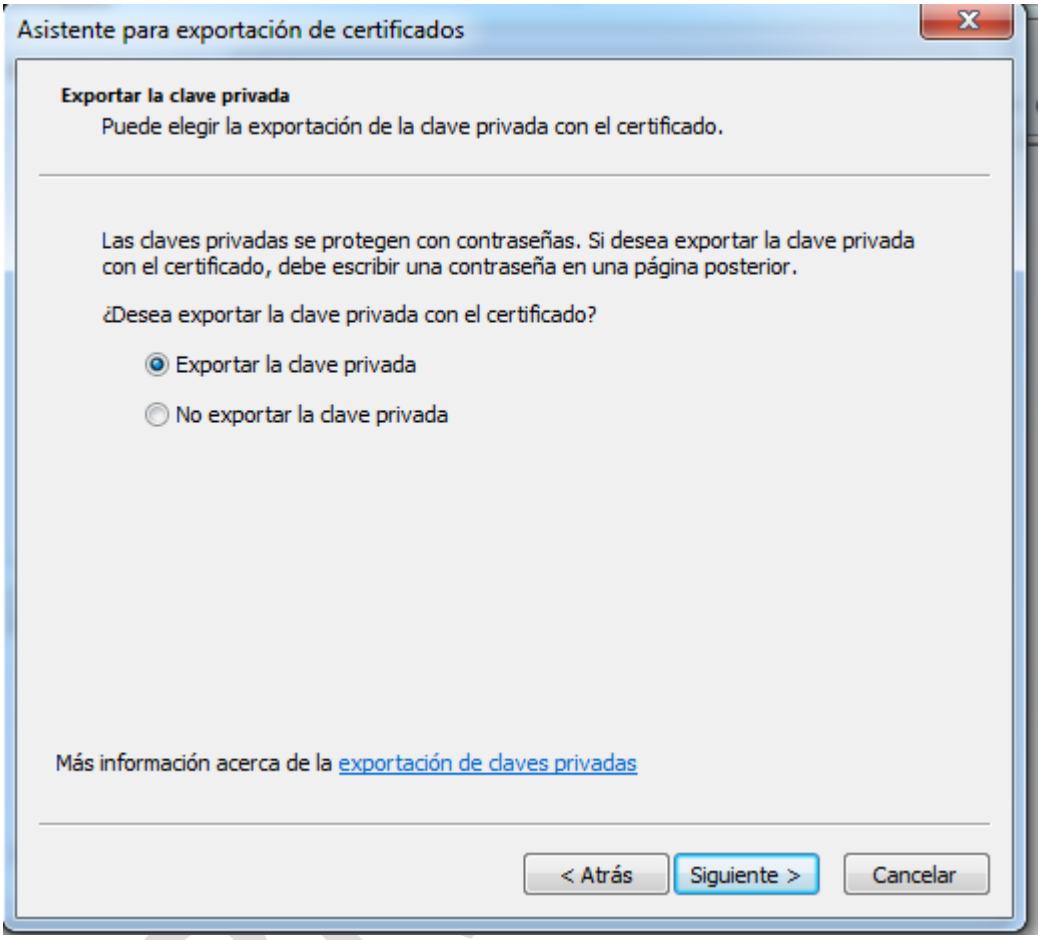



Seleccionamos el que queremos exportar y a continuación pulsamos el botón de "*Exportar…*" para iniciar el asistente.



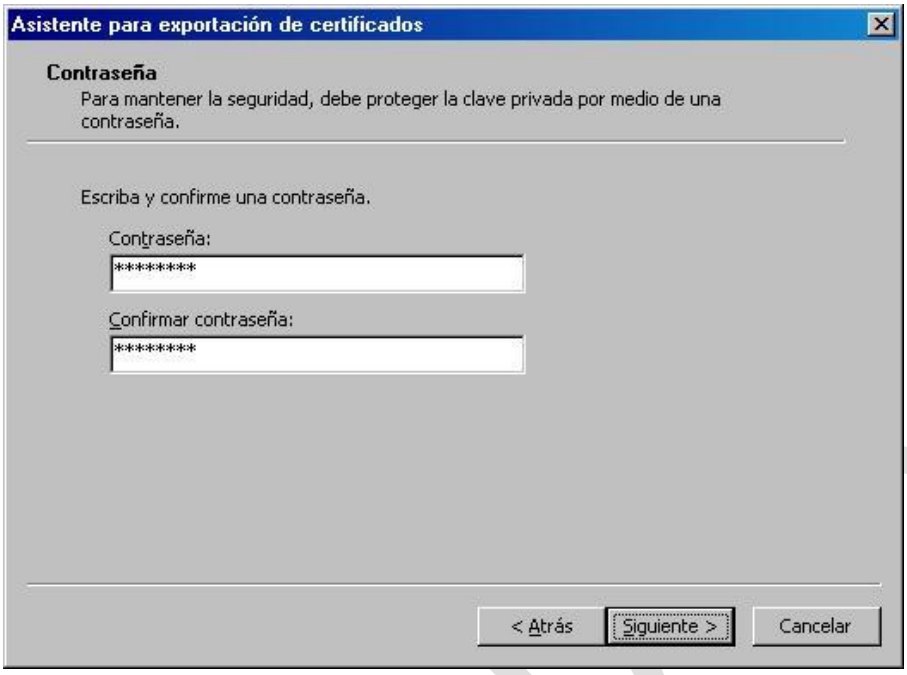

Al pulsar el botón "*Siguiente*" se solicita el modo en que se quiere hacer la exportación. Los certificados siempre se pueden exportar de dos maneras, con clave privada o sin ella:

- el certificado se exporta con clave privada cuando se quiere realizar copias de seguridad o se va a realizar una posterior importación en otro ordenador o navegador.
- el certificado se exporta sin clave privada cuando se va a ceder a terceros para que nos envíen información cifrada, información que está destinada para nosotros.




Al seleccionar la opción de exportarlo con clave privada, se accede a una pantalla donde se pide una contraseña y su validación para proteger el archivo que contiene el certificado exportado y poder instalarlo en otros equipos. Esta contraseña podría denominarse **contraseña de exportación** y es diferente y la contraseña de uso que se introdujo en el proceso de solicitud.

Se debe introducir esta contraseña y pulsar el botón "*Siguiente*".




***Hay que guardar y custodiar esta contraseña ya que usted es el único que la posee y si la pierde nadie le puede ayudar a recuperarla.***

En el siguiente cuadro de diálogo indicaremos la ruta (*disco duro, carpeta, disquete, pendrive, etc…*) y el nombre del archivo que queremos que contenga el certificado exportado, pulsamos el botón "Siguiente".


Se habrá completado correctamente la exportación, y se pulsa "*Finalizar*".

***Nunca debe entregar esta copia con la clave privada a nadie bajo ningún concepto. Su certificado digital es como "su DNI en el mundo Internet".***

El fichero resultante de la exportación varía en función del navegador y de si lleva clave privada o no:

| Extensión del fichero | Navegador utilizado | Incluye Clave privada |
|---|---|---|
| **.pfx** | Internet Explorer | SI |
| **.p12** | Mozilla Firefox | SI |

| | | |
|---|---|---|
| **.cer** | Internet Explorer | NO |
| **.crt** | Mozilla Firefox | NO |

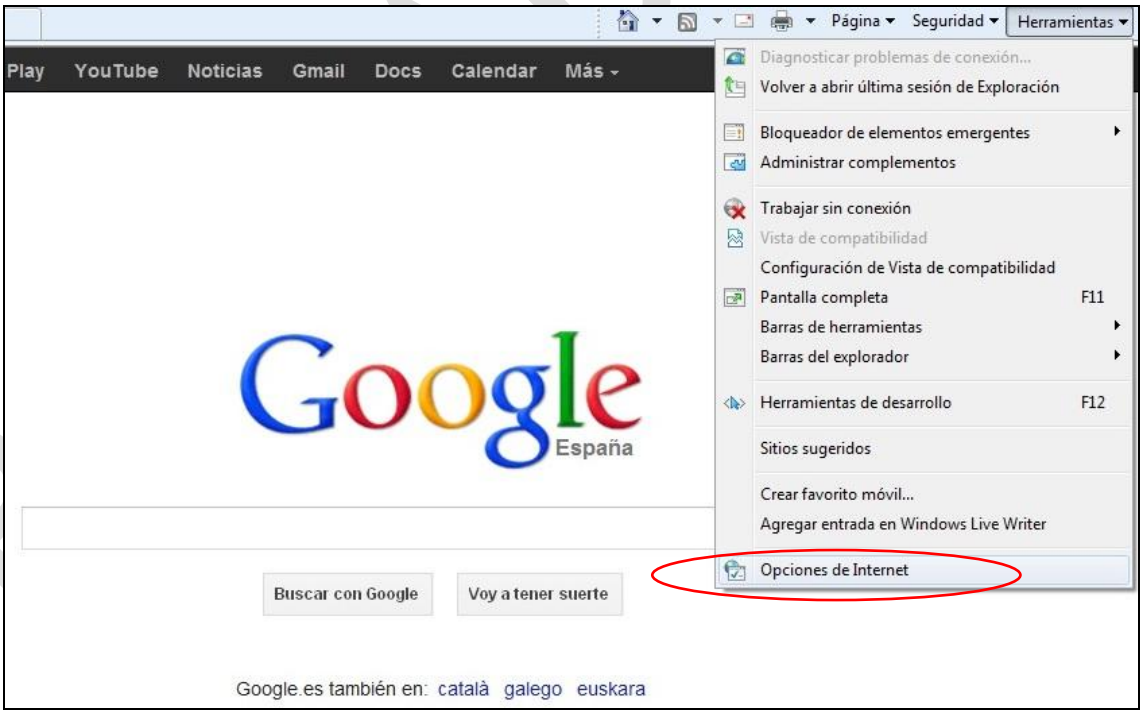
# 5. Importar Certificado Digital

Si se quiere instalar un certificado en otro ordenador o bien se ha tenido que formatear el disco duro donde se encontraba originalmente el certificado, etc., se podrá realizar la importación gracias a la copia de seguridad que se ha generado en el proceso anterior.

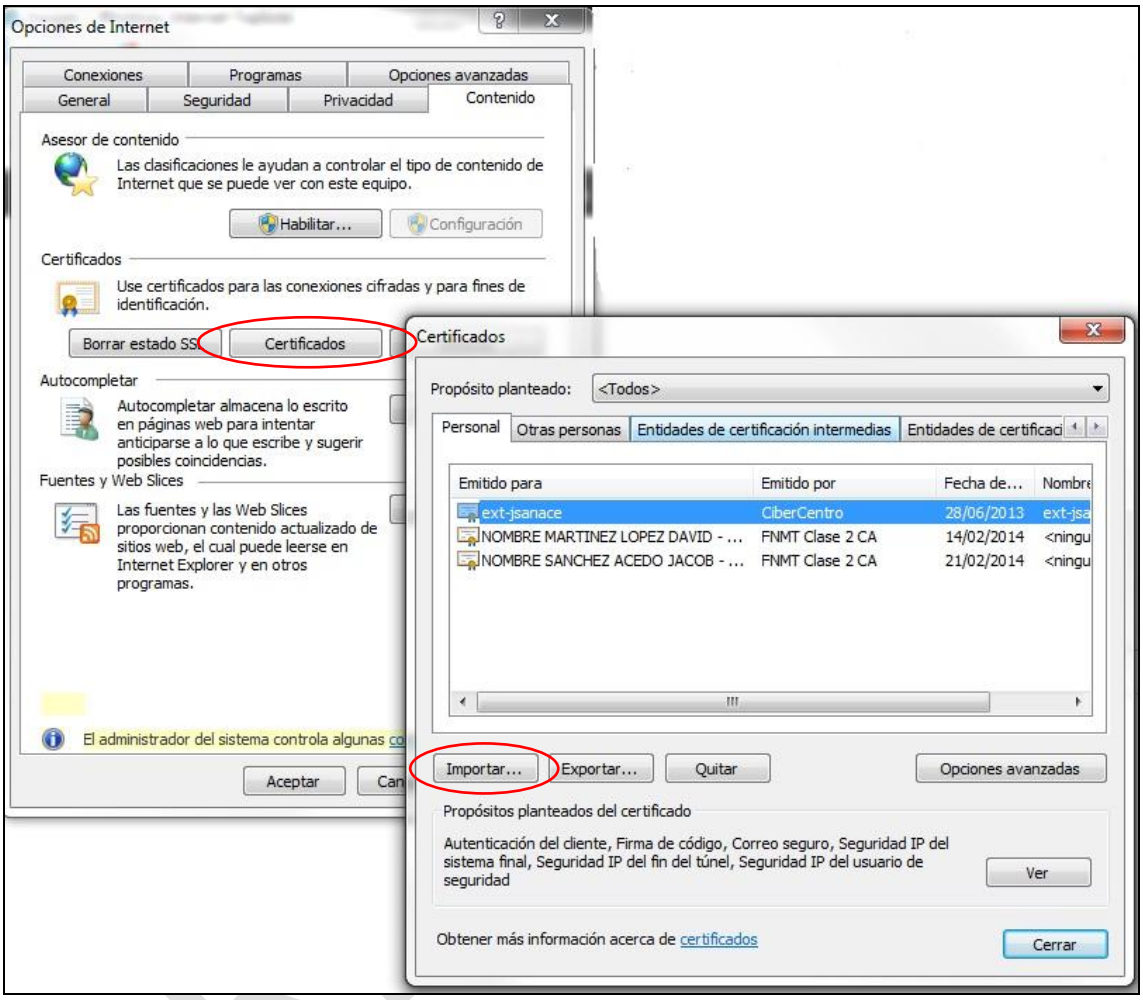
A continuación se detalla el proceso de **importación** de un Certificado Digital en Internet Explorer, aunque el proceso es similar para otros navegadores y versiones.

## Importación en Internet Explorer

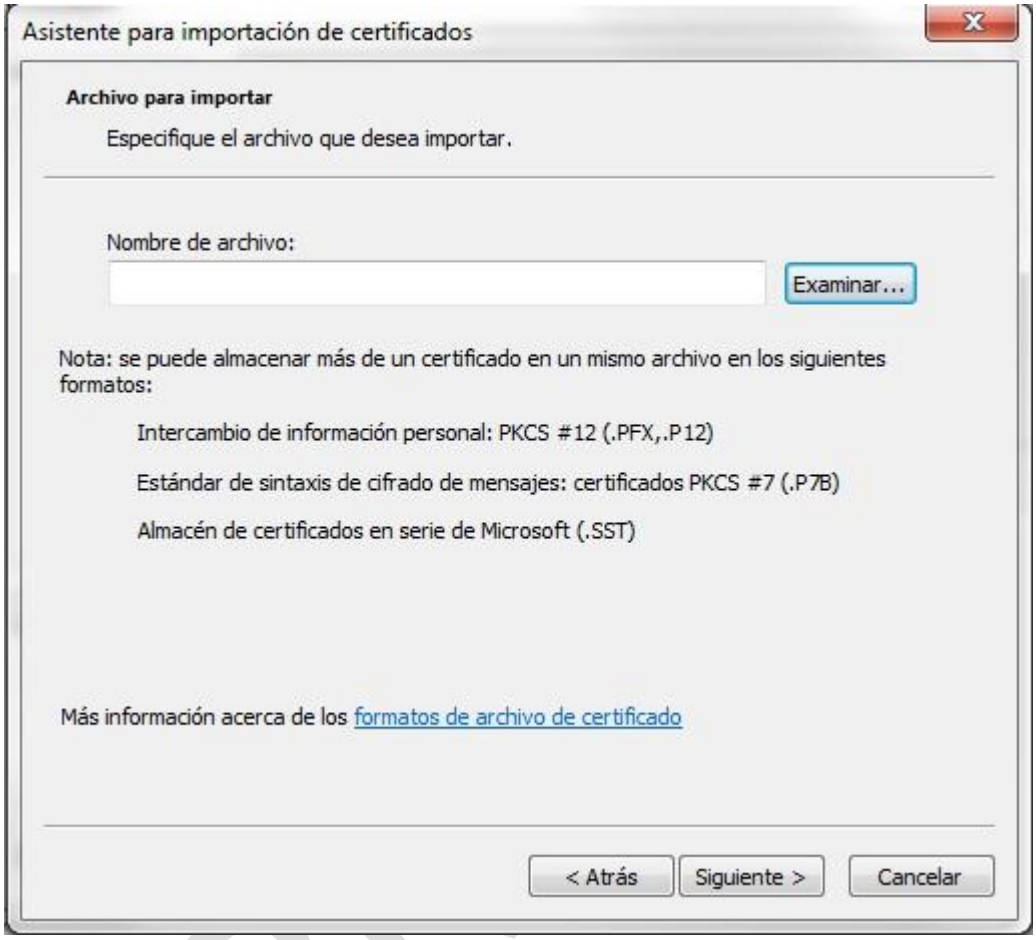
Accediendo al menú Herramientas → Opciones de Internet → pestaña Contenido, se muestra el botón Certificados.



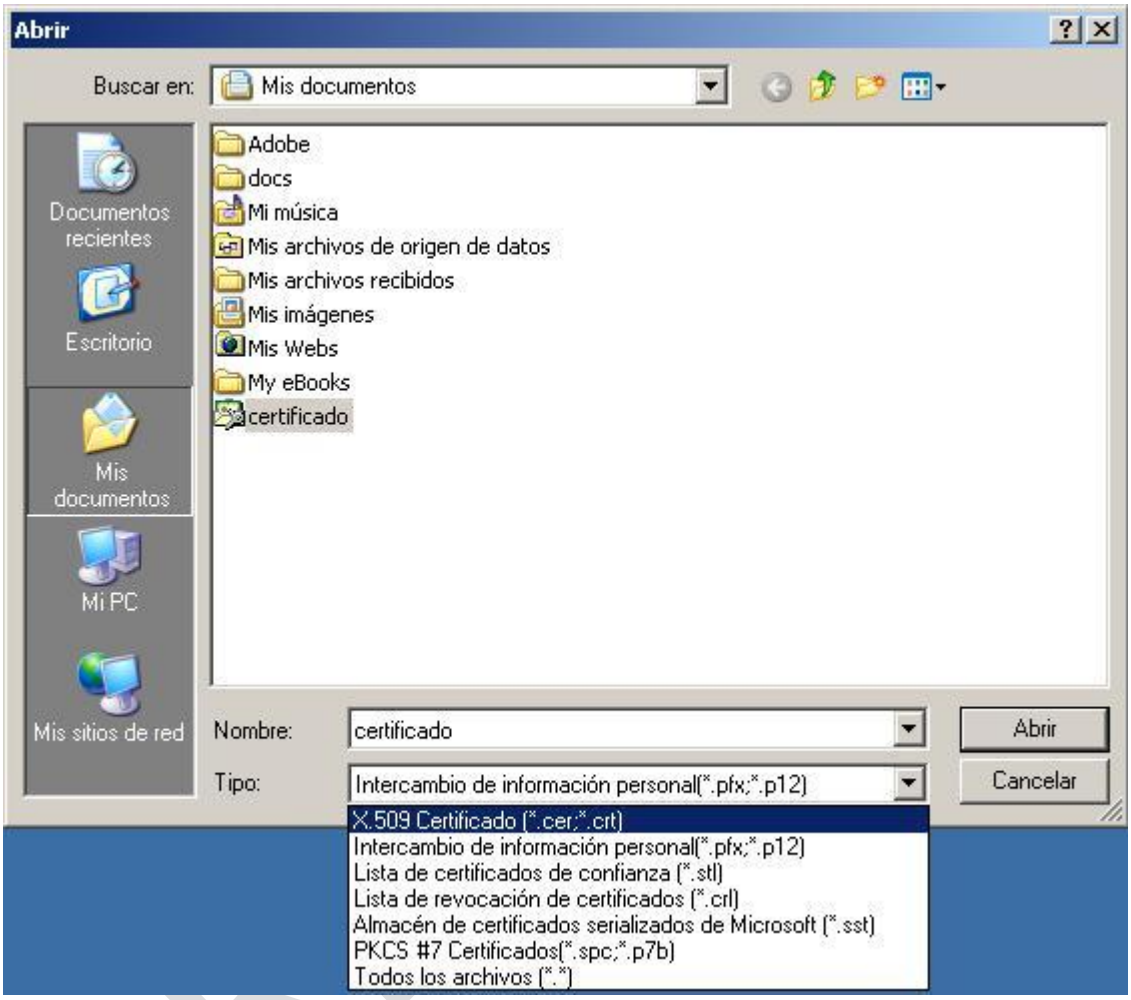

Al pulsarlo se accede a la pantalla de Certificados, en donde se seleccionará la opción *"Importar…"* para iniciar el asistente.




Seleccionamos el que queremos exportar y a continuación pulsamos el botón de "*Exportar…*" para iniciar el proceso. Se le indica al asistente en qué lugar o soporte se encuentra el certificado que se quiere importar, pulsando sobre "*Examinar…*".




Para poder visualizar el fichero hay que indicar que el **tipo** es "*Intercambio de información personal (*.pfx,*p12)*" o "*Todos los archivos*" en su defecto.




A continuación, el asistente abre una ventana denominada Contraseña, donde se solicita la clave que se utilizó al hacer la copia de seguridad del certificado en el proceso de Exportación (*contraseña de exportación*) y otros dos campos más:

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

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


La siguiente ventana es la de Almacén de Certificados, que es el área del sistema donde se guardan los certificados. Se deja la opción que el asistente marque por defecto y se pulsa el botón "*Siguiente*", mostrándose de esta forma la pantalla para finalizar el procedimiento de importación


Asistente para importación de certificados
Finalización del Asistente para importación de certificados
Ha completado con éxito el Asistente para importación de certificados.
Ha especificado la siguiente configuración:
Almacén de certificados seleccionado por el usuario
Pers
Contenido
PFX
Nombre de archivo
C:\D
< Atrás
Finalizar
Cancelar

# 6. Revocación, Renovación y Eliminación

Los certificados tienen un periodo de vigencia y además se pueden cancelar o revocar, siempre que el titular lo desee.

## 6.1. Revocar Certificado digital

La revocación de un certificado digital es la anulación de su vigencia antes de la fecha de caducidad especificada en él.

La revocación puede solicitarse en cualquier momento, siempre que la vigencia del certificado no haya finalizado, especialmente cuando el titular crea que el certificado puede haber sido copiado o robado.

*REVOCAR = ANULAR VALIDEZ*

**PROCEDIMIENTO REVOCACIÓN**

1) Si el titular del certificado o su representante, están en posesión del mismo, la revocación se efectuará a través de Internet.

2) Si el titular del certificado o su representante no disponen del mismo por extravío, pérdida o robo, deberá personarse en una Oficina de Acreditación, para, una vez identificado, firmar el modelo de solicitud de revocación del certificado.

3) Servicio de revocación telefónica:
La FNMT-RCM pone a su disposición un servicio de revocación telefónica para certificados de persona física exclusivamente. Este servicio es 24x7. 902200616

## 6.2. Renovar Certificado Digital

Cuando el certificado está próximo a su fecha de caducidad (*desde 60 días antes hasta el mismo día*), se puede renovar sin tener que desplazarse a la oficina de registro desde la propia página de la FNMT.

Para renovar el certificado es necesario realizar una serie de configuraciones en su navegador y enviar una solicitud firmada tal y como se explica de forma detalla en la página:

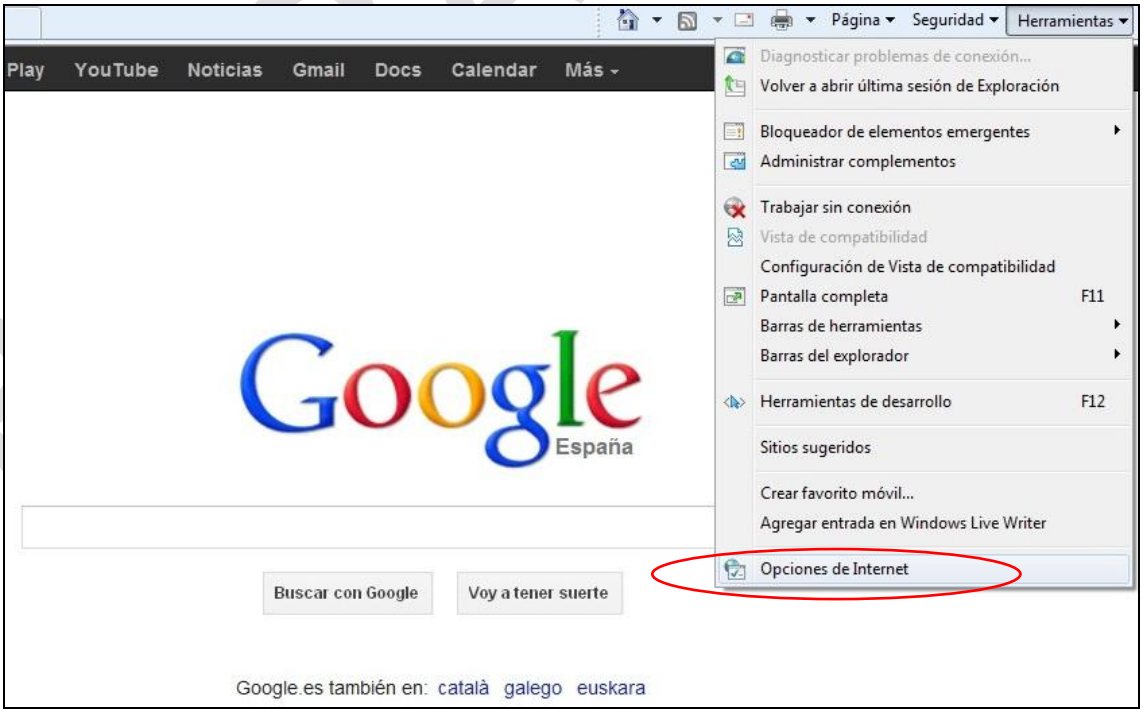
*http://www.cert.fnmt.es/index.php?cha=cit&sec=5&page=70&lang=es*

## 6.3. Eliminar Certificado digital

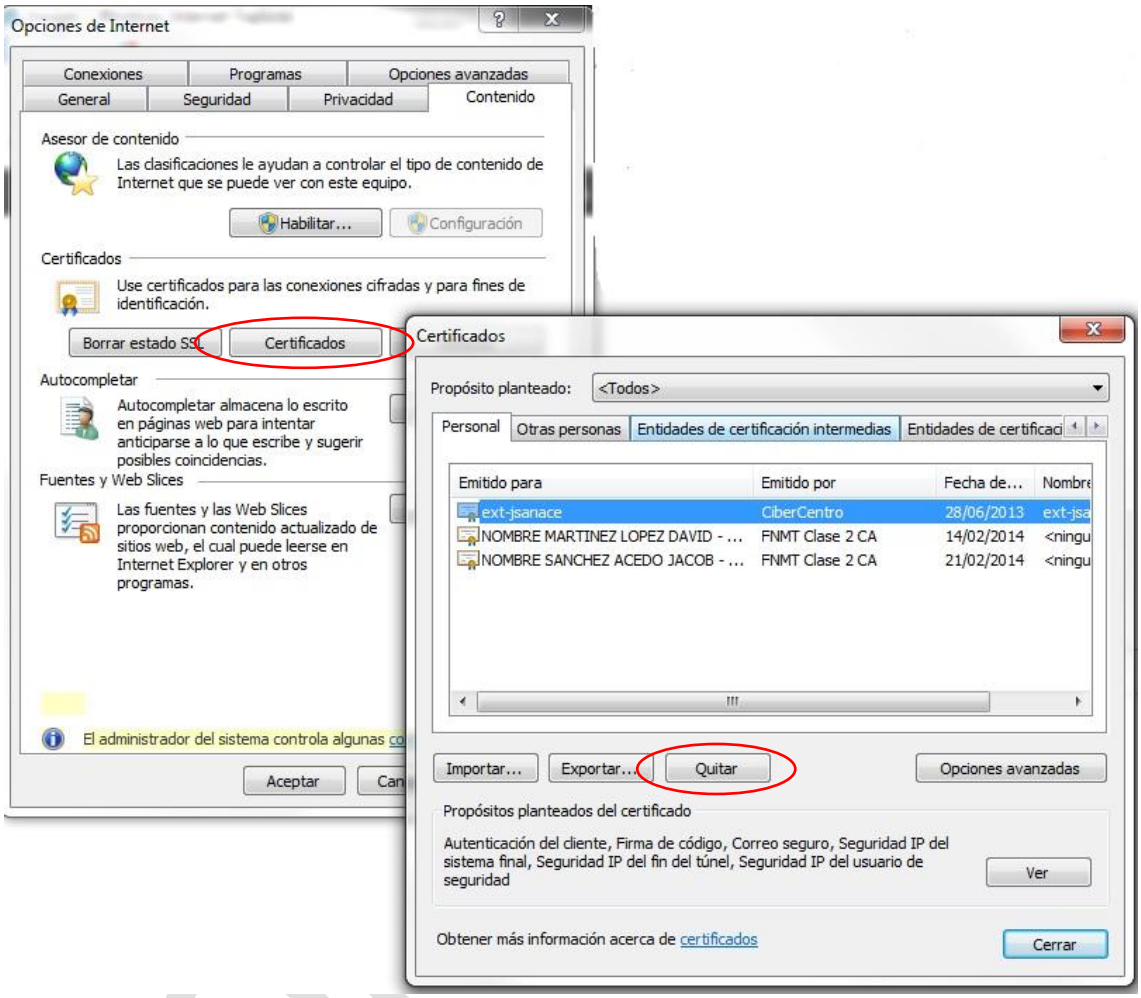
A continuación se detalla el proceso de **eliminación** de un Certificado Digital en Internet Explorer, aunque el proceso es similar para otros navegadores y versiones.

**Importación en Internet Explorer**

Accediendo al menú Herramientas → Opciones de Internet → pestaña Contenido, se muestra el botón Certificados.



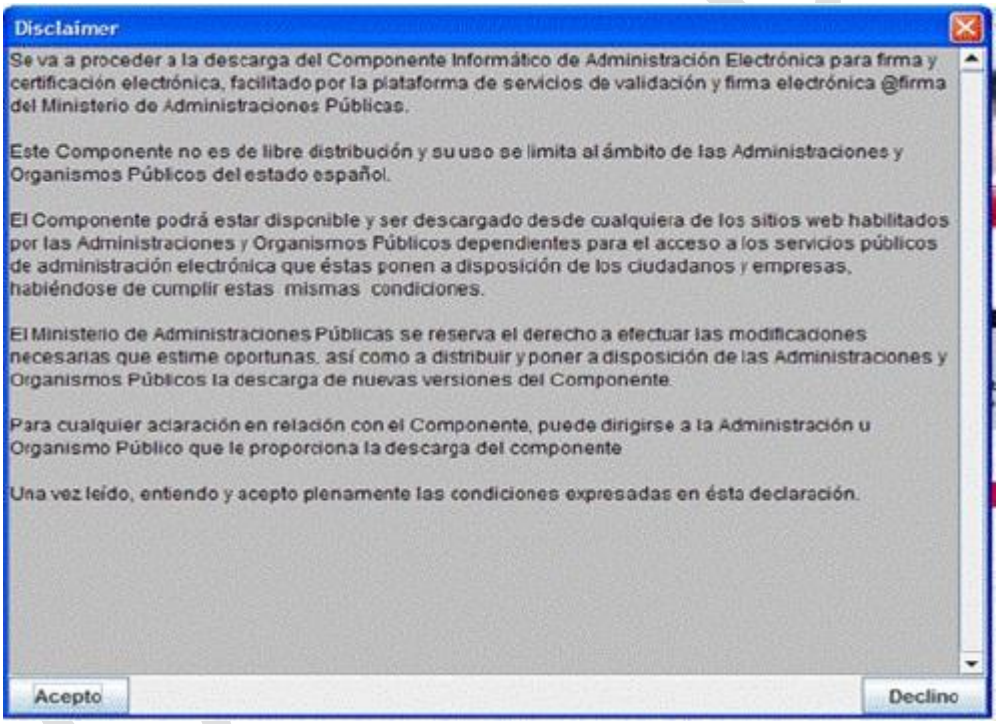

Al pulsarlo se accede a la pantalla de Certificados, en donde se seleccionará la opción *"Quitar…"* para eliminarlo del navegador.


Opciones de Internet
Conexiones
Programas
Opciones avanzadas
General
Seguridad
Privacidad
Contenido
Asesor de contenido
Las clasificaciones le ayudan a controlar el tipo de contenido de Internet que se puede ver con este equipo.
Habilitar...
Configuración
Certificados
Use certificados para las conexiones cifradas y para fines de identificación.
Borrar estado SSL
Certificados
Autocompletar
Autocompletar almacena lo escrito en páginas web para intentar anticiparse a lo que escribe y sugerir posibles coincidencias.
Fuentes y Web Slices
Las fuentes y las Web Slices proporcionan contenido actualizado de sitios web, el cual puede leerse en Internet Explorer y en otros programas.
El administrador del sistema controla algunas co
Aceptar
Certificados
Propósito planteado:
<Todos>
Personal
Otras personas
Entidades de certificación intermedias
Entidades de certificaci
Emitido para
Emitido por
Fecha de...
Nombre
ext-jsanace
CiberCentro
28/06/2013
ext-jsa
NOMBRE MARTINEZ LOPEZ DAVID - ...
FNMT Clase 2 CA
14/02/2014
<ningu
NOMBRE SANCHEZ ACEDO JACOB - ...
FNMT Clase 2 CA
21/02/2014
<ningu
Importar...
Exportar...
Quitar
Opciones avanzadas
Propósitos planteados del certificado
Autenticación del cliente, Firma de código, Correo seguro, Seguridad IP del sistema final, Seguridad IP del fin del túnel, Seguridad IP del usuario de seguridad
Ver
Obtener más información acerca de certificados
Cerrar

# 7. Uso del Componente de Firma (@FIRMA)

En algunas aplicaciones para poder firmar electrónicamente es necesario tener instalado el cliente **@firma5**. La instalación de este componente se hará únicamente la primera vez que se cargue el formulario asociado a un procedimiento que requiera firma electrónica.

Al cargar dicho formulario se mostrará la siguiente ventana de aceptación:




Pide confirmación antes de proceder a la instalación del cliente de @Firma.

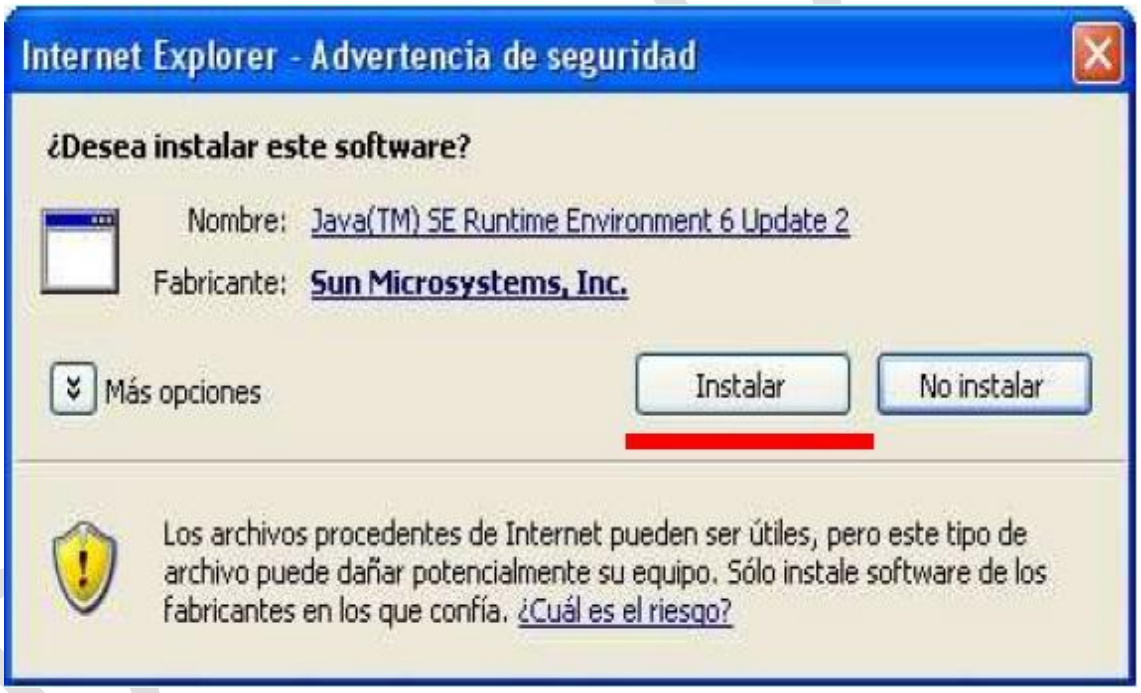

Informa que el cliente de Firma Electrónica se ha cargado correctamente.


Mensaje
El 'Cliente de Firma Electrónica de @Firma 5' ha sido instalado correctamente.
Aceptar

# 8. Uso de Java y Firma Electrónica

Para poder utilizar la firma electrónica también es necesario tener instalado el Runtime de Java (JRE), en el caso de que no lo tenga instalado. Cuando se accede por primera vez a la pantalla de aceptación del correspondiente formulario, el sistema le pedirá permiso para instalarlo. Si usted tiene habilitado el bloqueo de elementos emergentes a su navegador, verá la siguiente pantalla


Se acepta la instalación y aparecerá la siguiente pantalla:




A continuación se procederá a la instalación de la máquina virtual de Java™. Hay que seguir las instrucciones del proceso de instalación. Para poder ejecutar aplicaciones Java, hace falta tener configurado el navegador correctamente.

La primera vez que se accede a la ejecución de la aplicación de Firma Digital, se pedirá permiso para ejecutarla.


Si selecciona la casilla "Confiar siempre en este editor", las siguientes veces que acceda la web, no se le pedirá permiso para ejecutar la aplicación. En este momento ya estará el sistema preparado para poder firmar.

# 9. Certificado Digital en Tarjeta Criptográfica

También existe la posibilidad de almacenar el certificado digital en un soporte físico denominado tarjeta criptográfica. Bien solicitando un nuevo certificado y descargándolo en este soporte o bien, importando un certificado ya existente en el citado soporte.

En este caso el solicitante deberá proveerse de la misma, así como de un lector de tarjetas en el caso de que su equipo no venga provisto del mismo.

- Las claves se generan en la tarjeta criptográfica
- Nadie podrá copiarlas ya que nunca salen de la tarjeta

El proceso de solicitud del certificado en tarjeta, requiere igualmente la realización de los tres pasos señalados anteriormente, con la diferencia de que la solicitud y la descarga han de hacerse con la tarjeta en el lector:

1) Solicitud del certificado a través de la web, seleccionado la opción "CERTIFICADO DE USUARIO EN TARJETA CRIPTOGRÁFICA" con la tarjeta dentro del lector, para que las claves se generen en la tarjeta en vez de en el navegador.

2) Acreditar tu identidad en una oficina de registro o utilizar tu DNIe y lector de tarjetas para realizar una acreditación virtual.

3) Descargar el certificado desde el equipo solicitante con la tarjeta dentro del lector para que se guarde en la misma.

# 10. Certificado de Empleado Público

Los certificados de Empleado Público o también llamados de Personal Adscrito a la Administración, son certificados de persona física, emitidos a los trabajadores de la Administración Pública.

De acuerdo con el Art. 22 del RD 1671/2009, los certificados de empleado sólo podrán ser utilizados en el desempeño de las funciones propias del puesto que ocupen y serán revocados al cesar en sus funciones dentro de ese mismo ámbito.

Este certificado emitido por la FNMT, confirma de forma conjunta la siguiente información:

- la identidad de su titular, número de identificación personal, cargo, puesto de trabajo y/o condición de autorizado.
- al órgano, organismo o entidad de la Administración Pública, bien sea ésta General, autonómica, Local o institucional, donde ejerce sus competencias, presta sus servicios, o desarrolla su actividad.

***Los certificados de empleado público sirven para identificar a los empleados de los organismos en el ejercicio de sus competencias.***

A diferencia de los certificados digitales de usuario convencionales, estos certificados llevan unos costes asociados porque requieren de un soporte físico denominado tarjeta criptográfica.

**Dentro del Cabildo de Gran Canaria existe la posibilidad de solicitar este tipo de Certificado. Para más información, ponerse en contacto con el Servicio de Gestión de Recursos Humanos.**