

## Protección de certificados digitales en un PC

### Contenido

Exportar el certificado con su clave privada y protegido por contraseña .....	1
Borrar el certificado de nuestro almacén de certificados.....	5
Importar el certificado exportado, pero protegiendo su uso con contraseña .....	6

El objetivo es que al usar el certificado se solicite una contraseña. No solo lo hace más seguro, sino que nos permite controlar cuándo estamos haciendo uso de nuestro certificado, nuestra identidad.

Para poder proteger un certificado recién descargado de la FNMT, hay que seguir estos pasos:

1. Exportar el certificado con su clave privada y protegerlo por contraseña.
2. Borrar el certificado de nuestro almacén de certificados (una vez que nos aseguremos que le hemos exportado correctamente con su clave privada).
3. Importar el certificado recién exportado, pero protegiendo su uso con una contraseña.

**Si queremos es usar el certificado en varios equipos, tan solo debemos exportarlo (paso 1) e importarlo en el otro equipo (paso 3)**

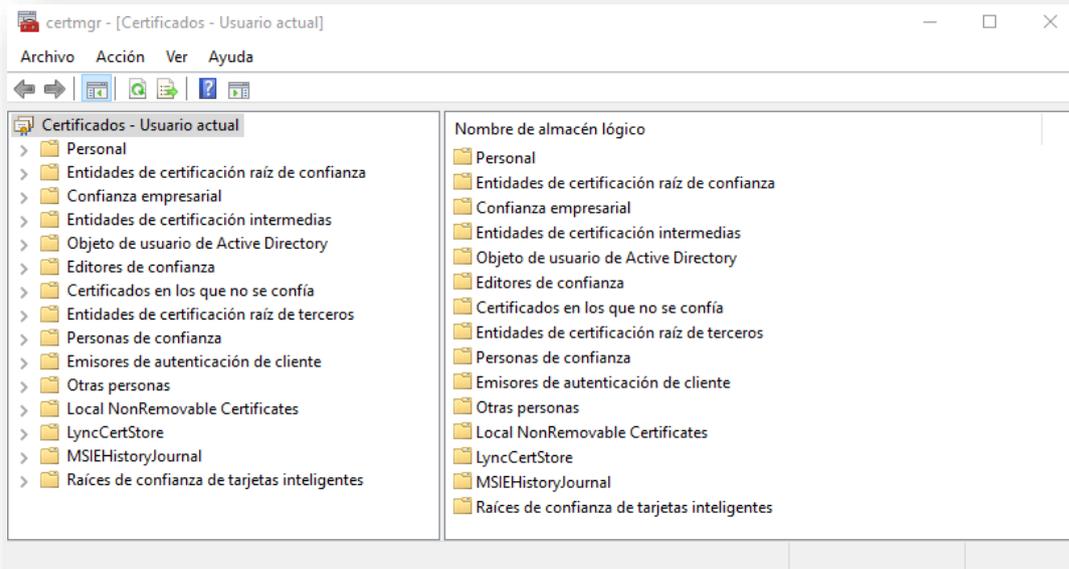
La FNMT mantiene un [listado de preguntas frecuentes relacionadas con la importación y exportación de certificados](#). Allí hay información sobre Windows, Mac y Linux.

En Windows, navegadores como Edge y Chrome usan el almacén de certificados del sistema operativo. Firefox tiene su propio almacén, pero en las últimas versiones puede usar el de Windows, lo cual es recomendable para aprovechar la protección por contraseña. Si se prefiere usar el almacén de Firefox, se recomienda activar la contraseña maestra para proteger los certificados.

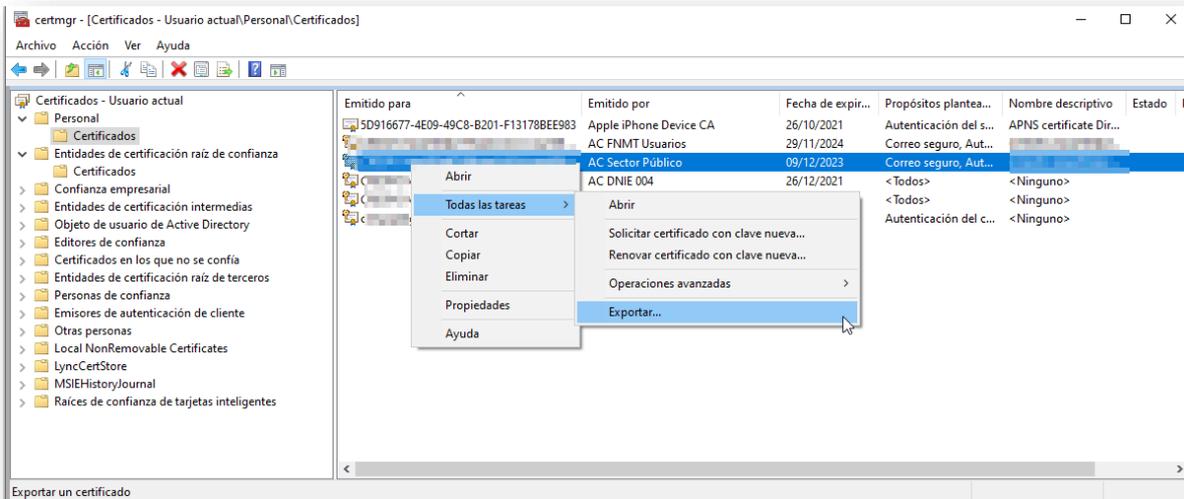
En la explicación detallada vamos a usar el almacén de certificados de Windows. [Si utiliza otro Sistema Operativo o tiene el certificado en Firefox consulte la ayuda de la FNMT](#).

### Paso 1. Exportar el certificado con su clave privada y protegido por contraseña

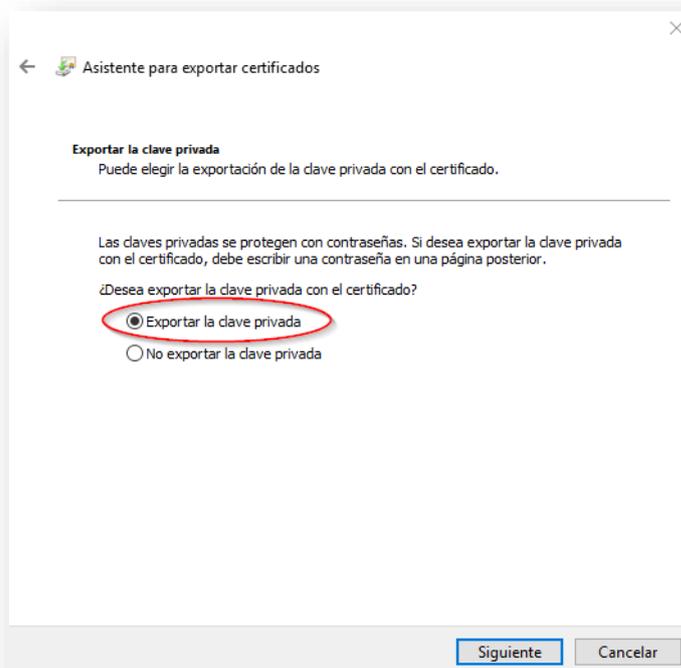
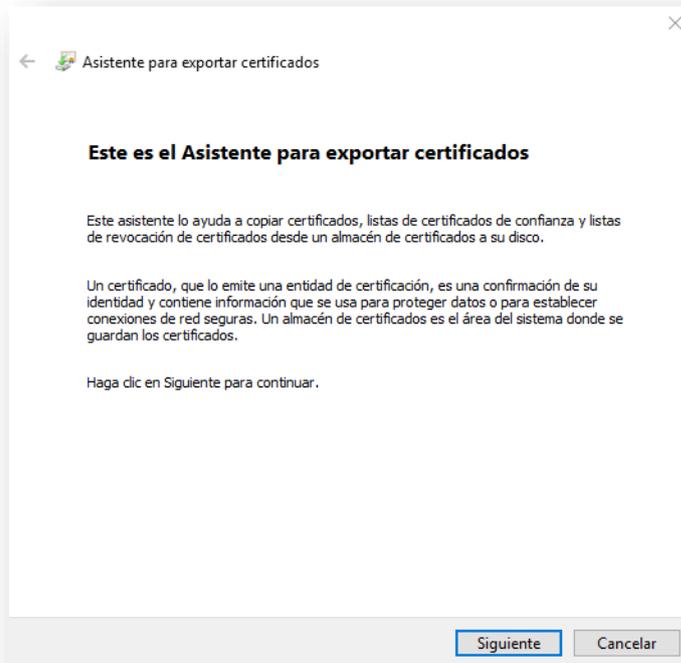
Para acceder al almacén de certificados en Windows 10/11 debemos usar la herramienta “Administrar Certificados de Usuario” (podemos buscarla en el buscador de Windows).



Seleccionamos el certificado personal (del cual tenemos clave privada) que queremos exportar y pulsamos botón derecho -> Todas las tareas -> "Exportar". **Al exportar es muy importante marcar la opción "Exportar la clave privada"**.



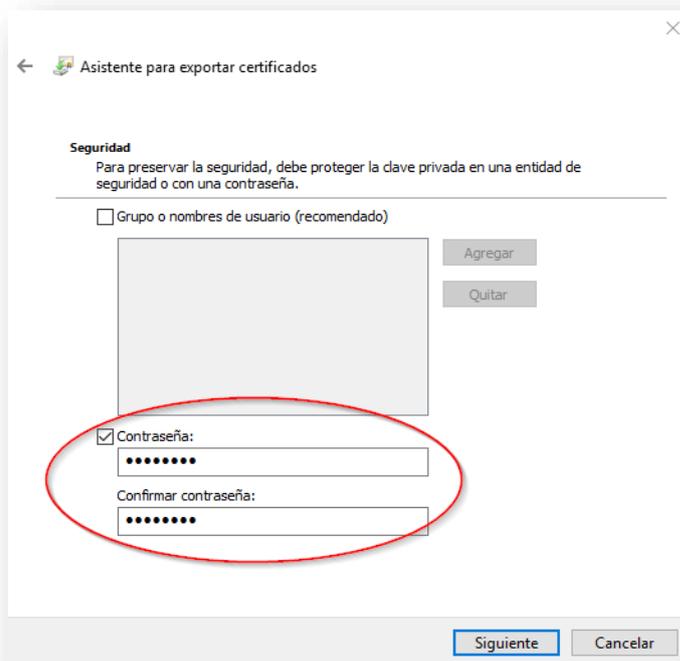
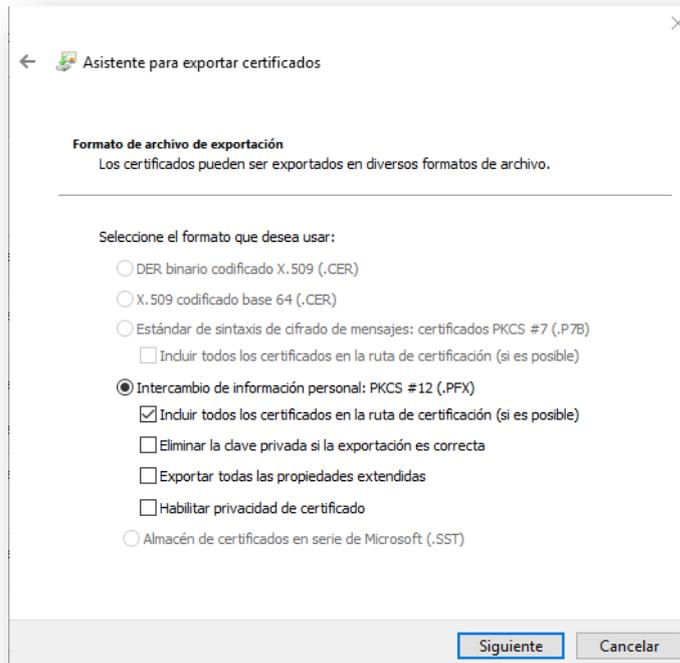
Si no exportamos la clave privada el certificado solo contendrá la parte pública por lo que no nos servirá como certificado personal para, por ejemplo, las operaciones de firma electrónica.



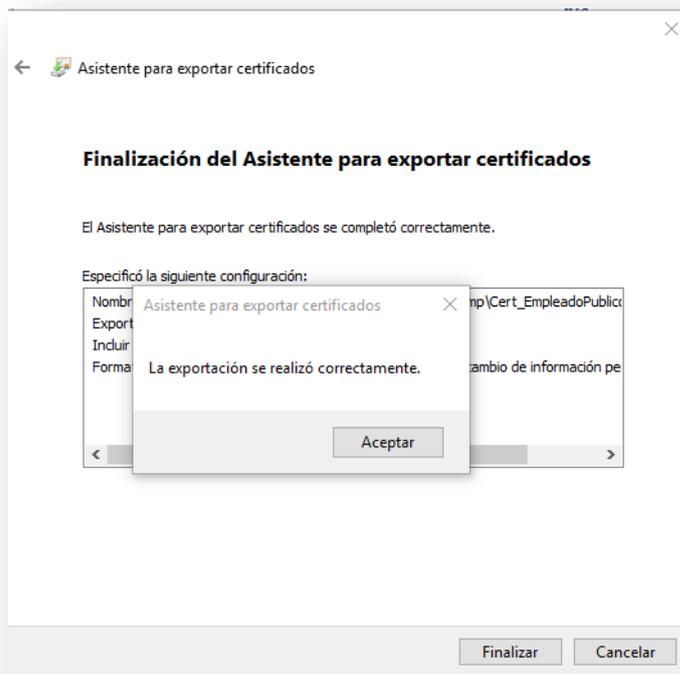
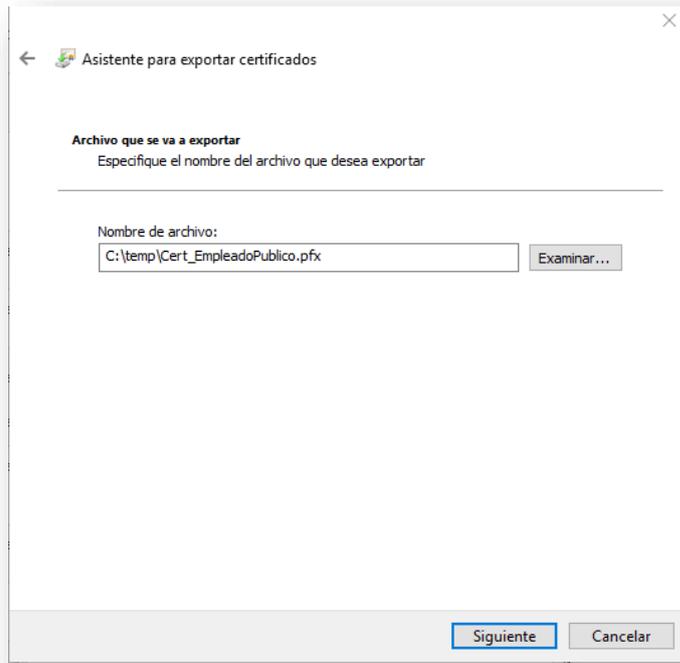
Las opciones de exportación las podemos dejar por defecto. Para proteger el fichero resultante, lo más sencillo es establecer una contraseña.



***Esta contraseña será necesaria para importar el certificado en un futuro.  
No se puede recuperar. NO LA OLVIDE.***



Debemos seleccionar una ubicación y dar un nombre al fichero que tendrá que tener la extensión .pfx. Pulsando finalizar generaremos el fichero en la ubicación que hemos indicado.



Con este proceso hemos exportado nuestro certificado con su clave privada a un fichero. Esto nos permite guardarlo en otra ubicación como copia de seguridad o llevarlo a otro ordenador, donde podremos importarlo (ver más adelante).

## Paso 2. Borrar el certificado de nuestro almacén de certificados

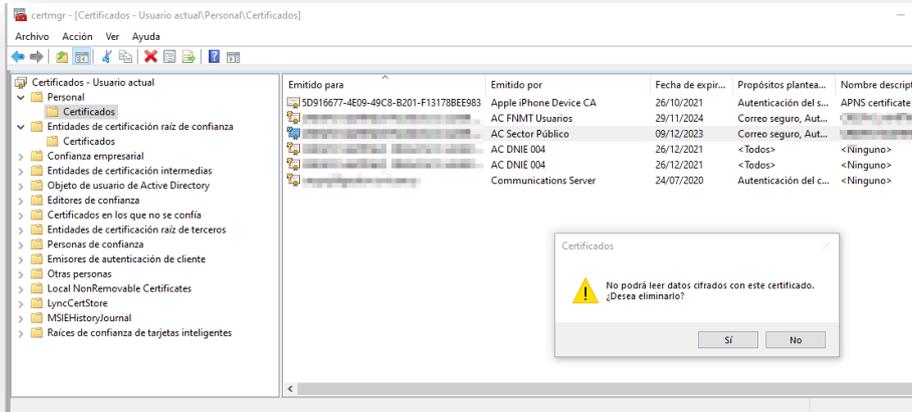
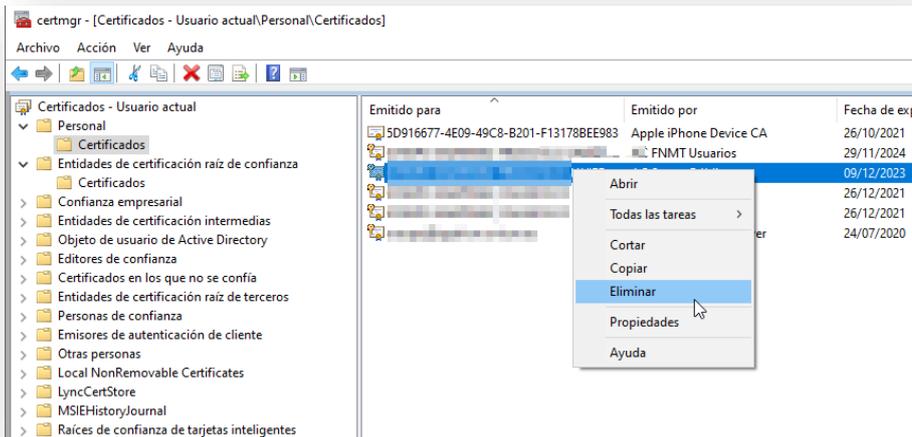
Para conseguir el objetivo de proteger el uso del certificado con una contraseña, es necesario borrar el certificado inicial (no protegido), e importarlo de nuevo, ya con protección.



**Antes de hacer este proceso, debemos tener exportado el certificado, con su clave privada, y tener certeza de la contraseña usada.**

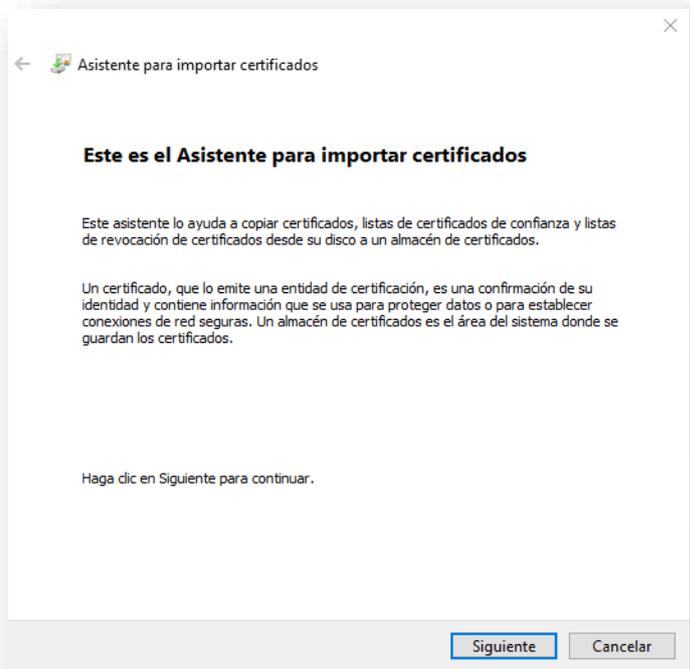
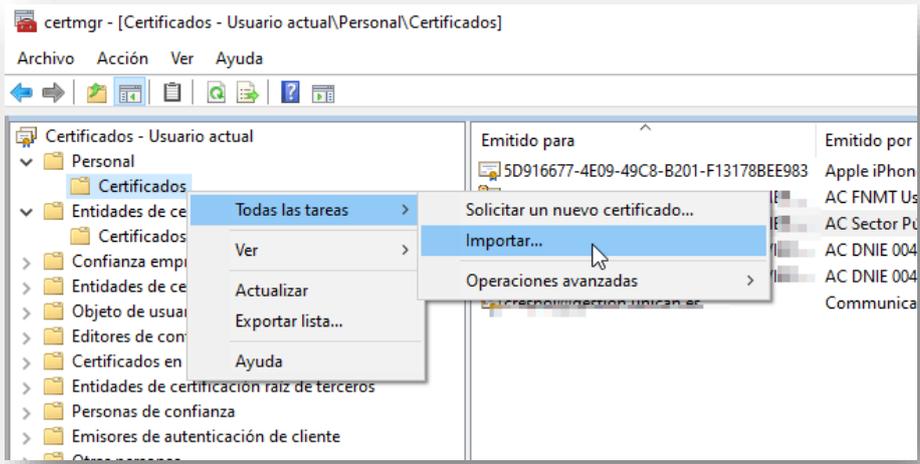
Si lo que queremos es exportar e importar el certificado a otro equipo y usarlo en ambos, este paso obviamente nos lo saltamos.

Para ello vamos al "administrador de certificados de usuario", seleccionamos el certificado que queremos borrar y usamos el botón derecho.

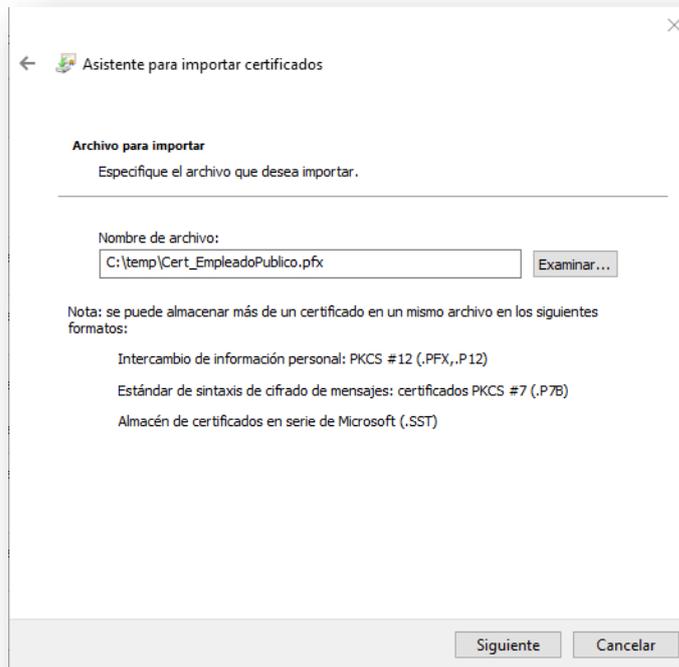
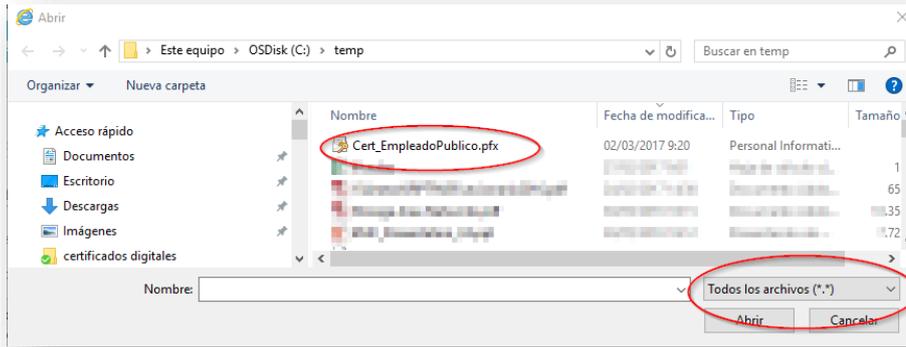


### Paso3. Importar el certificado exportado, pero protegiendo su uso con contraseña

En este paso, importaremos el certificado, con la adecuada protección de su uso. Para ello usamos la herramienta "Administrar Certificados de Usuario". Vamos a la carpeta de certificados personales y con botón derecho elegimos "Importar". También podemos importar con solo hacer doble clic sobre el fichero con certificado con clave privada (normalmente formato .pfx).



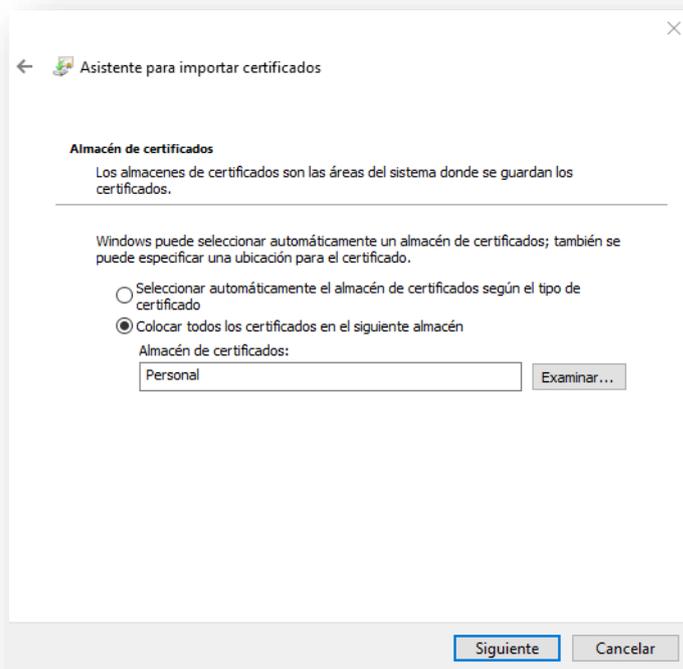
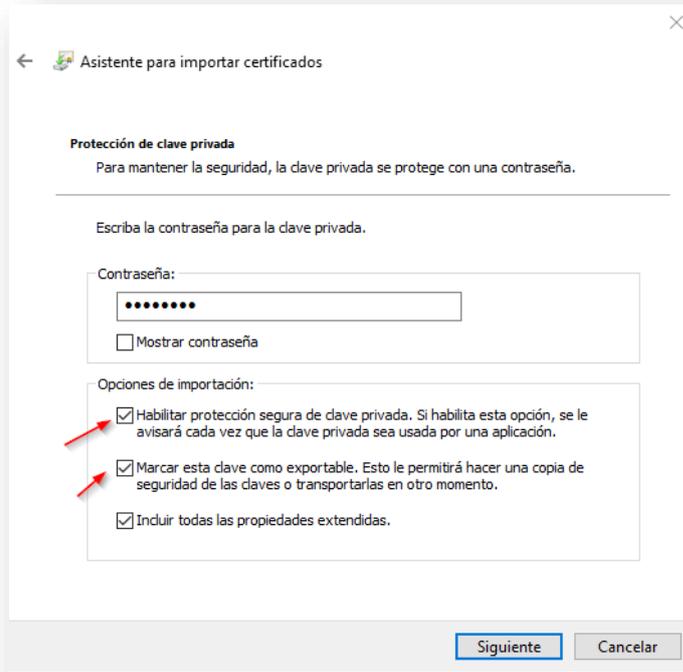
Debemos seleccionar el certificado que hemos exportado previamente con la clave privada. **Atención que se debe indicar "todas las extensiones de archivo" para poder ver los ficheros de tipo .pfx que son los que estamos buscando.**

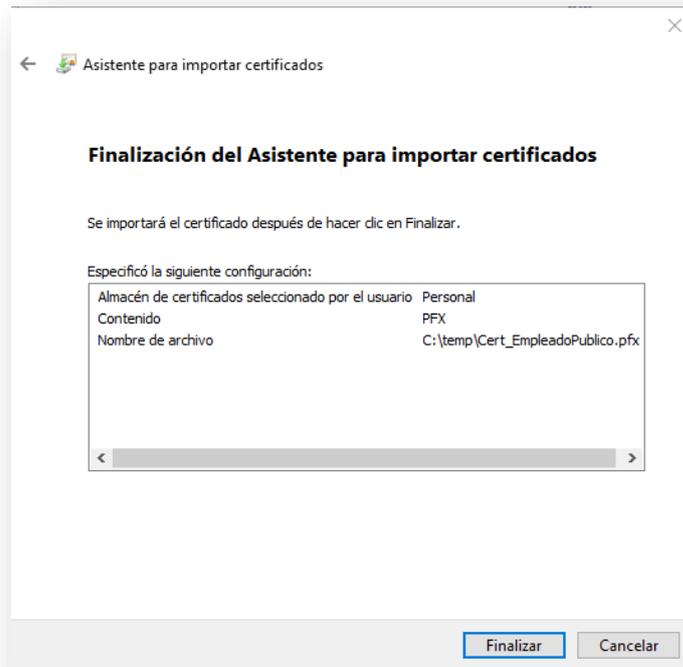


A continuación, debemos escribir la contraseña de ese fichero, con la que hemos protegido la clave privada. Además, debemos **habilitar la protección segura y debemos marcar la clave como exportable**. De esta forma podremos en el futuro exportar nuestro certificado con su clave privada.

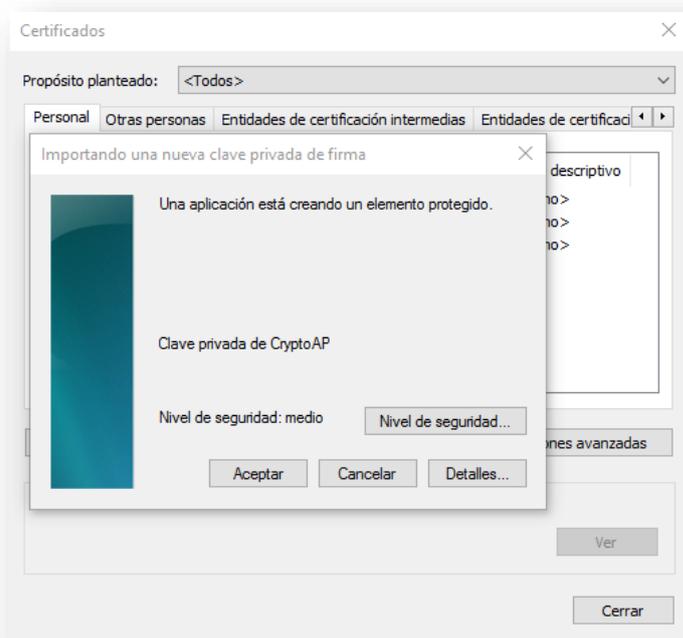


**La contraseña de uso deberá ser compleja, ya que protege tanto su uso como la posible exportación completa del certificado.**





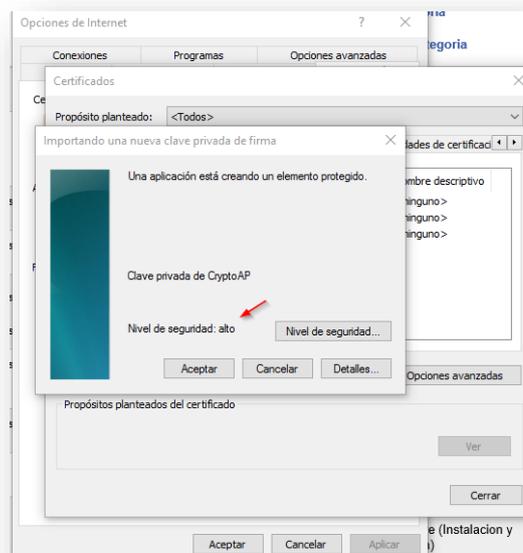
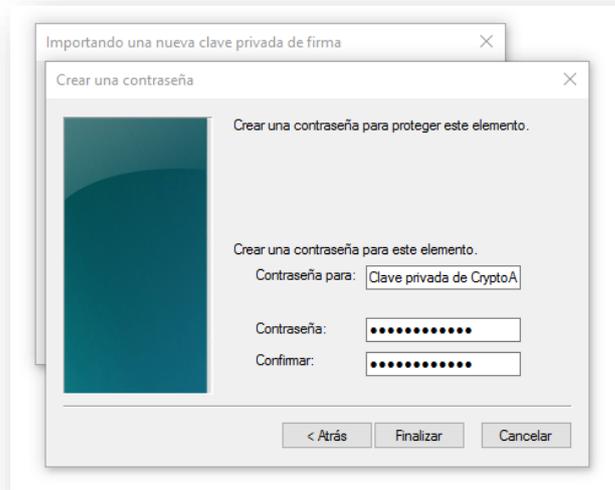
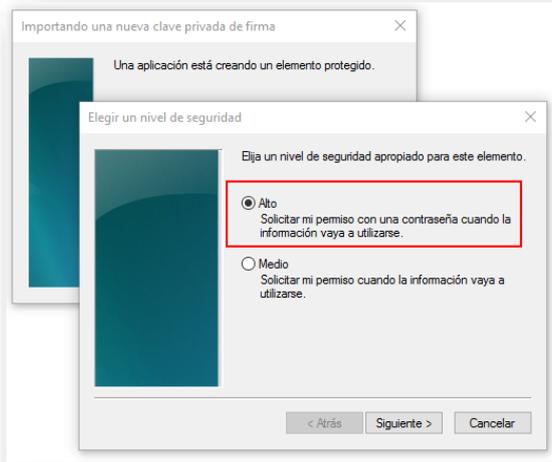
Al pulsar finalizar, nos saldrá esta otra ventana. **En ella debemos cambiar el nivel de seguridad a Alto.**

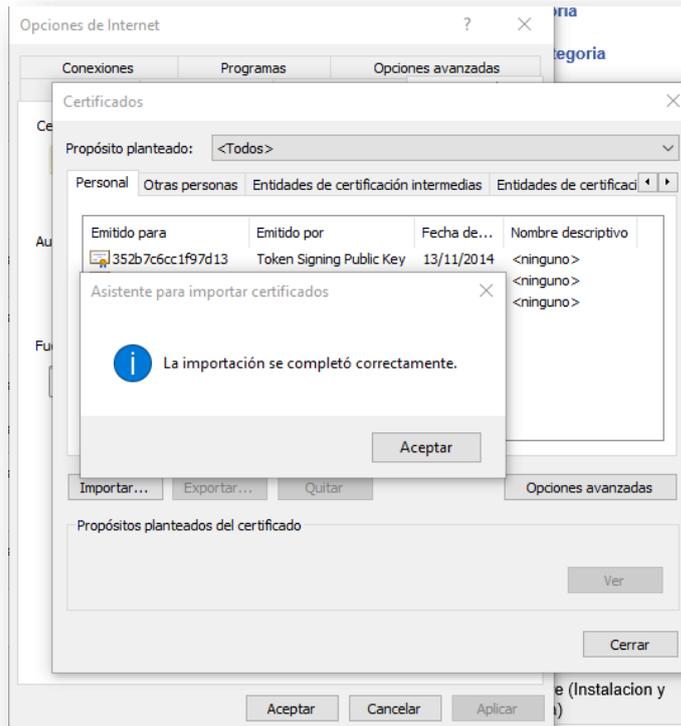


Pulsamos en el botón Nivel de Seguridad. **Elegimos nivel "Alto" y definimos una contraseña.** Esta contraseña nos sirve para proteger el uso de nuestro certificado. Nos la pedirá cada vez que usemos el certificado (por ejemplo, en un proceso de firma electrónica).



**No se debe olvidar (no se puede recuperar) ni usar la misma que protege la copia de seguridad del certificado.**





Una vez importado, si pulsamos sobre el certificado podremos comprobar que está correctamente importando con su clave privada. Si hemos seguido los pasos cada vez que vayamos a usarlo nos pedirá la contraseña antes indicada.

