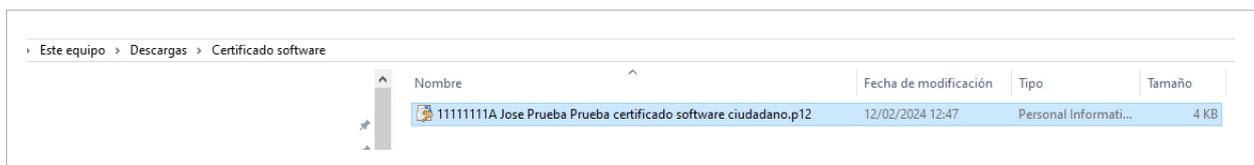


# MANUAL PARA INSTALAR EL CERTIFICADO SOFTWARE DE CIUDADANO

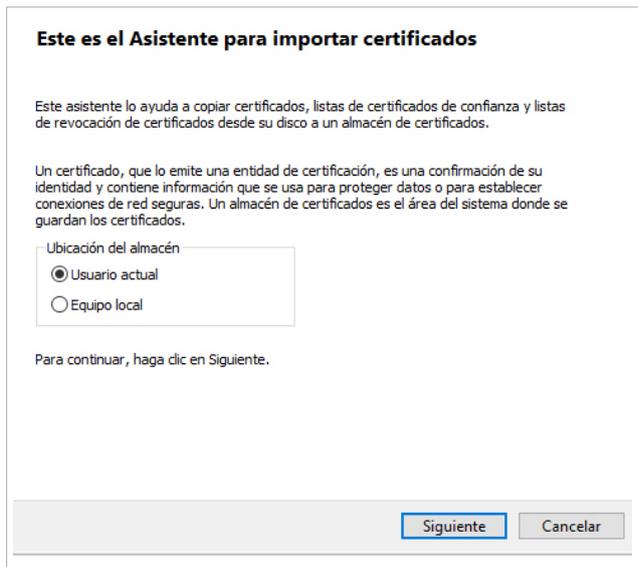
# MANUAL PARA INSTALAR EL CERTIFICADO SOFTWARE DE CIUDADANO EN UN ORDENADOR DE MANERA SEGURA PARA QUE LE PIDA AL USUARIO LA CONTRASEÑA DE USO Y EVITAR QUE TERCEROS PUEDAN UTILIZARLO

Aquellas personas que deseen instalar su certificado software de ciudadano en un ordenador en el que lo vaya a utilizar, de manera segura para que pida contraseña de uso, deben seguir los siguientes pasos:

1. Realizar doble clic sobre nuestro certificado software de ciudadano.



2. Se abrirá una ventana en la que se nos informa que el certificado se instalará como usuario local y pulsamos "Siguiente".



3. En la siguiente pantalla pulsaremos "Siguiente".



**Archivo para importar**  
Especifique el archivo que desea importar.

---

Nombre de archivo:

Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:

- Intercambio de información personal: PKCS #12 (.PFX,-P12)
- Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
- Almacén de certificados en serie de Microsoft (.SST)

4. En la siguiente ventana introduciremos la contraseña de instalación del certificado y es muy importante que marquemos la primera opción “Habilitar protección segura de clave privada”, eso permitirá que el uso de nuestro certificado no quede expuesto y sólo pueda hacerse uso de él mediante la introducción de la contraseña de uso que nos pedirá cuando finalice la instalación.

**Protección de clave privada**  
Para mantener la seguridad, la clave privada se protege con una contraseña.

---

Escriba la contraseña para la clave privada.

Contraseña:

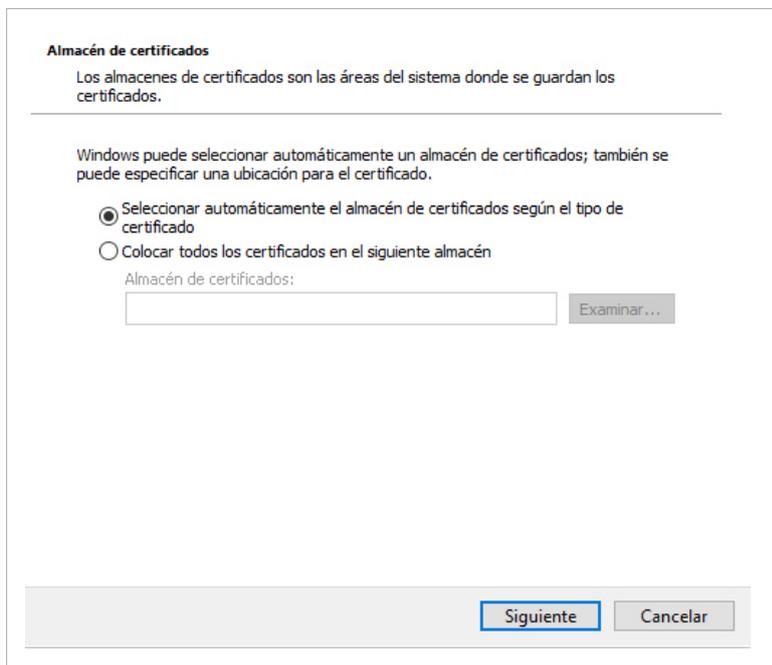
Mostrar contraseña

Opciones de importación:

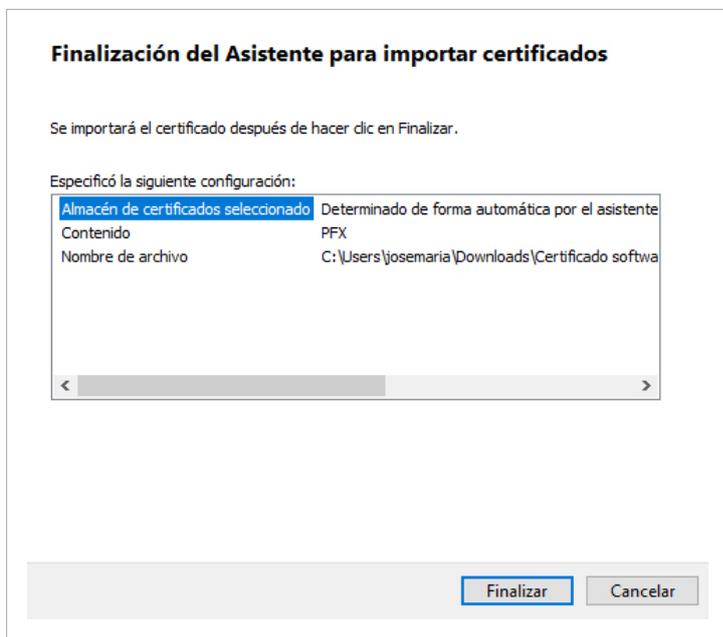
- Habilitar protección segura de clave privada. Si habilita esta opción, se le avisará cada vez que la clave privada sea usada por una aplicación.
- Marcar esta clave como exportable. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento.
- Proteger la clave privada mediante security(Non-exportable) basada en virtualizado
- Incluir todas las propiedades extendidas.

5. En la siguiente pantalla pulsamos “Siguiente”.



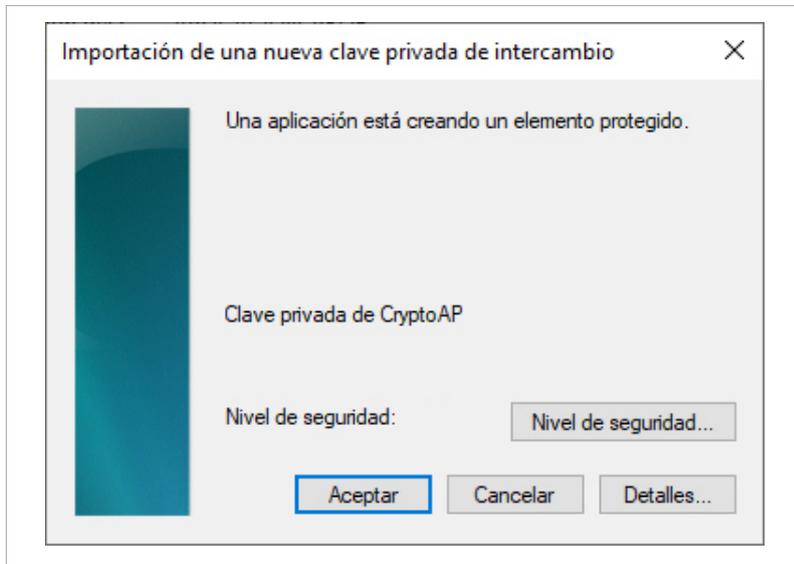


6. En la siguiente pantalla pulsamos “Finalizar”.

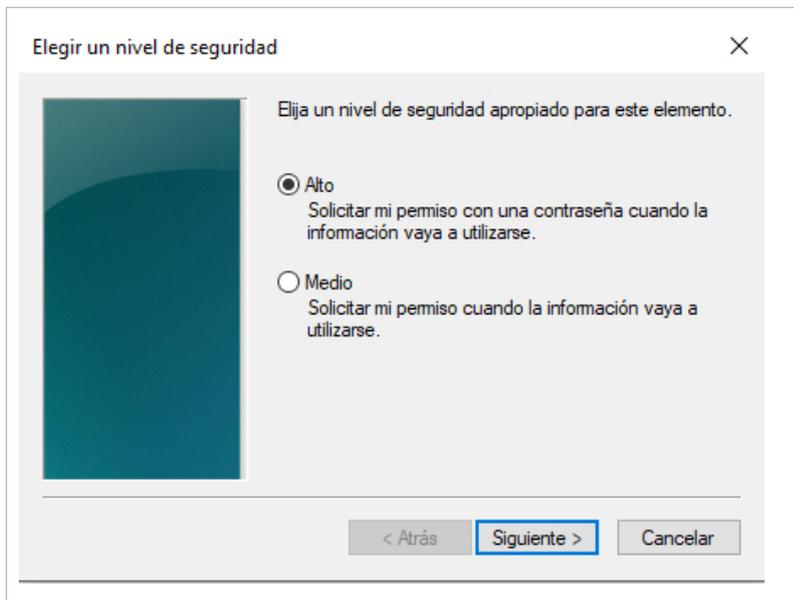


7. Al finalizar se nos abrirá la siguiente ventana donde debemos pulsar en el botón “Nivel de seguridad” para cambiar el nivel de seguridad a ALTO, con el fin de evitar que cualquier otro usuario pueda utilizar nuestro certificado, dado que nos pedirá la contraseña cada vez que queramos utilizarlo en ese equipo.



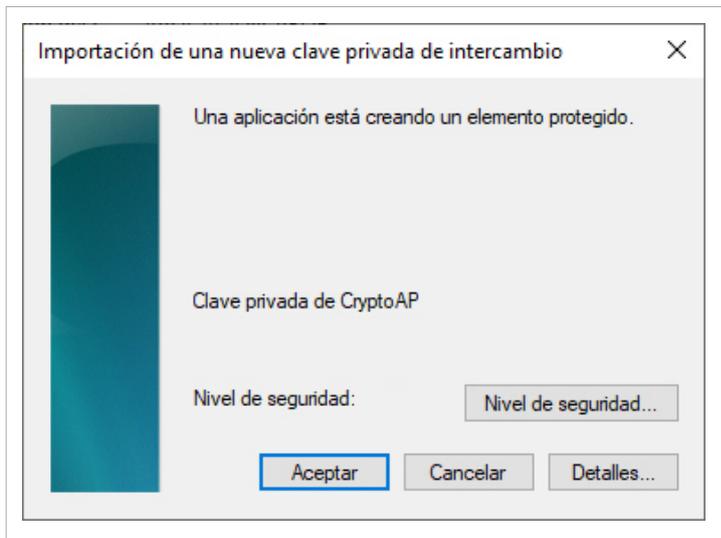


Elegimos la opción ALTO y pulsamos siguiente:

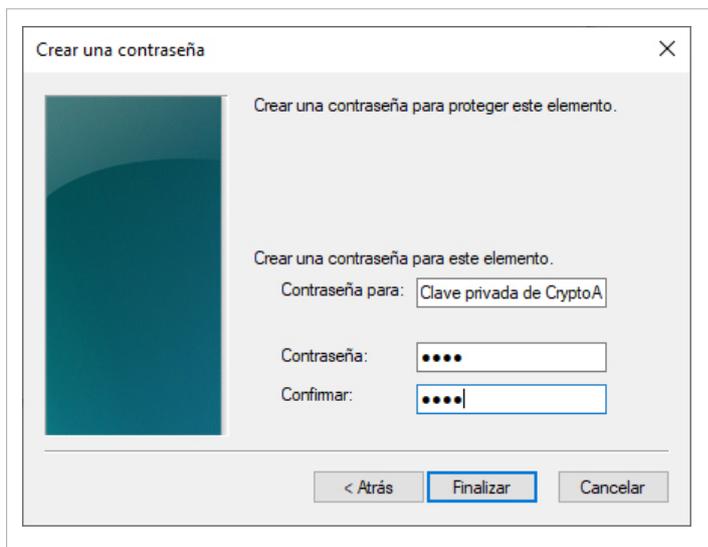


8. Una vez elegido nivel alto de seguridad pulsamos "Aceptar".

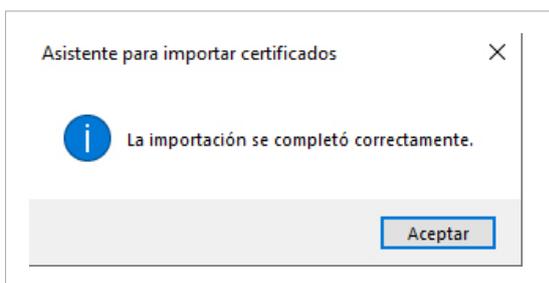




9. Introducimos la contraseña que queremos usar cada vez que utilicemos el certificado, no hay limitaciones en cuanto a tamaño o contenido, puede ser corta y contener sólo números. Una vez introducida la contraseña de uso pulsamos “Finalizar”

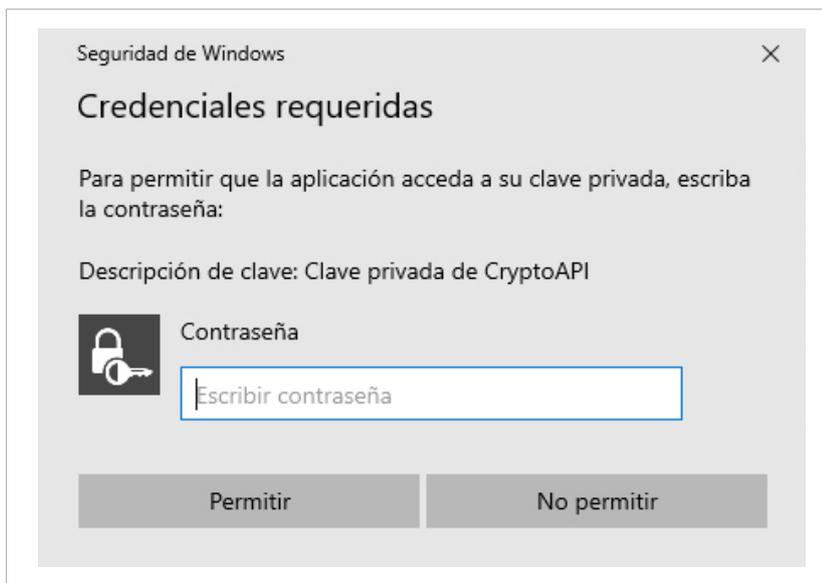


10. Se nos mostrará un mensaje de que el certificado se ha importado correctamente.



- Desde ese momento el equipo tendrá nuestro certificado instalado, podremos hacer uso de él para realizar cualquier acción que lo precise, siempre y cuando introduzcamos la contraseña de uso que le hemos asociado al instalarlo.

Ejemplo de solicitud de contraseña al utilizar el certificado software:





T 963 922 000 · Conde de Montornés 7. 46003 Valencia

[www.micof.es](http://www.micof.es)