

# Cómo importar, exportar, desinstalar el certificado digital del PKCs12 en los navegadores



Chrome

/



Edge

## Contenido

1 Descripción .....	2
2 Requisitos Previos .....	2
3 Firma Electrónica Avanzada (FEA) .....	3
4 Cómo importar el certificado digital del p12 o pfx .....	4
5 Cómo exportar (generar una copia) del certificado digital .....	9
6 Cómo desinstalar (quitar) el certificado digital.....	15
7 Datos de Contacto .....	16

## PKCs12

### 1 Descripción

Este manual describe los pasos a realizar para la **importación (instalación)**, **exportación (copia de seguridad)** o **desinstalar (quitar)** el certificado digital del archivo **PKCs12 (p12 o pfx)** en un entorno **Windows** para poder hacer uso de la **Firma Electrónica Avanzada (FEA)**.

### 2 Requisitos Previos

Para poder realizar el **envío telemático** correspondiente, es necesario cumplir con los siguientes requisitos:

- Contar con el siguiente **Sistema Operativo (S.O.)** de **Windows**
- Contar con alguno de los siguientes navegadores instalados **Chrome** o **Edge**.
- Contar con el archivo **PKCs12** con extensión **p12** o **pfx**
- En caso de requerir una **copia de seguridad**, disponer de un medio electrónico (**USB**) para realizar la **exportación**.
- Realizar las **actualizaciones** correspondientes de su equipo.

Recordar que los certificados digitales compatibles con el gestor de **certificados** de **Windows** son los correspondientes a los **archivos p12** o **pfx**.

**Google Chrome** puede leer los **certificados digitales** directamente del **sistema operativo**, al igual que **Edge**.

De esta manera, para poder usar nuestro **certificado digital** en **Google Chrome** o **Edge** **no debemos** realizar ninguna configuración especial en los navegadores. Simplemente basta con tener el archivo **PKCs12** e instalarlo en **Windows** para poder usarlo en los navegadores antes mencionados.

### 3 Firma Electrónica Avanzada (FEA)

La FEA a utilizar se obtiene a través de la **Autoridad Certificadora de Firma Electrónica Avanzada del Estado de Hidalgo (ACFEAEH)** y para poder hacer uso de ella:

- Es necesario contar con los archivos con extensión **p12 o pfx** el cual contiene el certificado digital (**\*.cer**) de la **Autoridad Certificadora (AC\_\*.cer)**, así como el par de **llaves pública (\*.cer)** y **privada (\*.key)**, requeridas para hacer uso de la FEA por parte de su propietario.
- Si **no cuenta** con los archivos, le recomendamos **“Contactar al Agente Certificador de la ACFEA o al Enlace de Certificación Digital de su Dependencia o Entidad u Organismo”**.

Para saber cuál es el procedimiento para la obtención del **Certificado Digital de FEA**, visite nuestro sitio web <http://firmaelectronica.hidalgo.gob.mx>, en él se detalla de manera sencilla los pasos a seguir; Para acceder de manera directa de clic en [Procedimiento de Certificación Digital](#) (se debe tener en cuenta que todos los pasos que se indican se deberán seguir en el mismo orden).



Procedimiento de la instalación del archivo **AC\_\*.cer**; Acceder de manera directa de clic en [Manuales de Procedimientos](#) (Instalación del certificado).

## PKCs12

### 4 Cómo importar el certificado digital del p12 o pfx

Para su instalación se deberán seguir los pasos que a continuación se describen:

Paso 1. Iniciar el **“Asistente para importar certificados”**, este asistente te guiará paso a paso en el proceso donde tienes que **seleccionar** la ubicación del **certificado digital** que quieres **instalar** en tu equipo, podrá realizarlo de dos formas:

- a) Seleccionar el archivo **p12 o pfx**, dar **clic derecho** y mostrará las siguientes opciones (**Imagen 1**) dar clic en **“Instalar PFX”** e iniciará el **“Asistente”** (**Ventana 1**) o

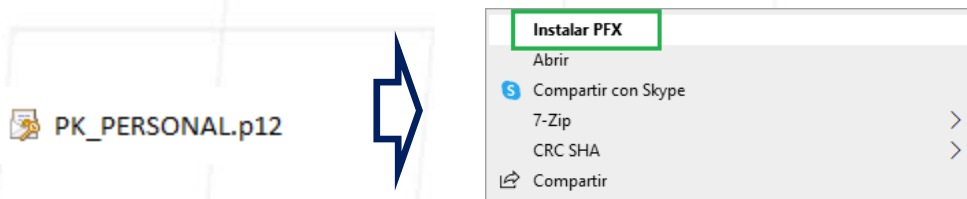
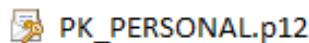
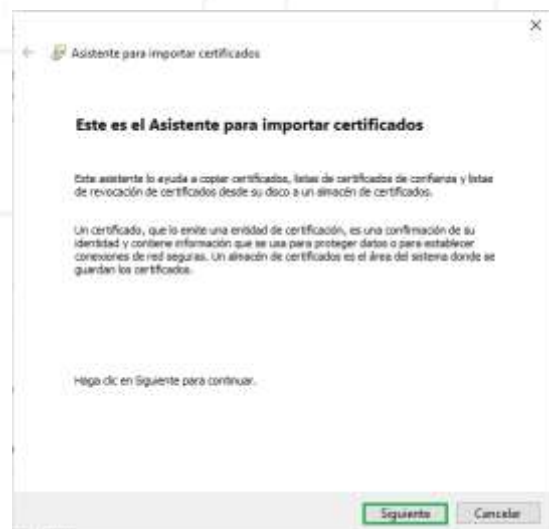


Imagen 1. Instalar PFX

- b) Seleccionar el archivo **p12 o pfx**, dar **doble clic** en el archivo e iniciará el **“Asistente”** (**Ventana 1**).



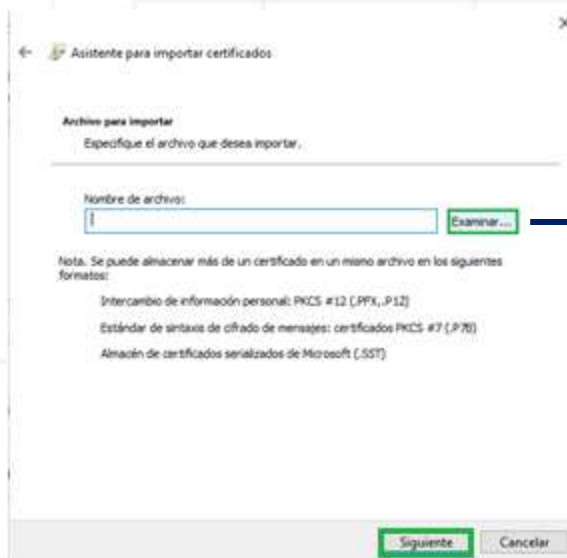
Paso 2. **Asistente para importar certificados**, para **ambos** casos procederá a la instalación (**Ventana 1**), y a continuación damos clic en el botón **“Siguiente”**.



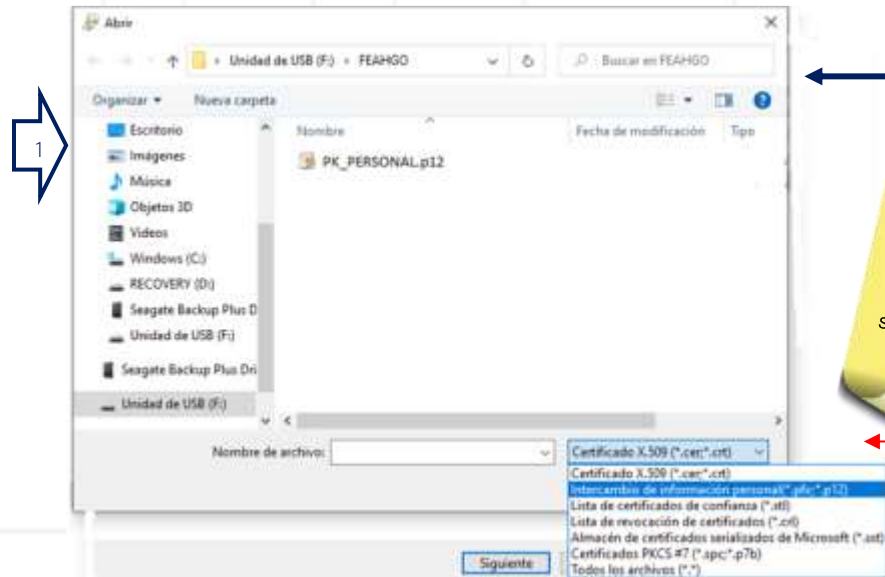
Ventana 1. Asistente para importar certificados

## PKCs12

Paso 3. Damos clic en el botón “Examinar” (Ventana 2) e indicará dónde se encuentra ubicado el archivo p12 o pfx (1), seleccionamos el archivo y a continuación damos clic en el botón “Siguiente”.



Ventana 2. Asistente para importar certificados



Al buscar el archivo, hay que verificar que la extensión del "Tipo de archivo" sea "Intercambio de información personal (\*.pfx; \*.p12)", como se muestra en la ventana.

## PKCs12

Paso 4. En la “Protección de la clave privada”, teclear la contraseña que ingresamos cuando en su momento se generó la clave de la llave privada, y posteriormente seleccionamos las 2 casillas indicadas en la ventana, y a continuación damos clic en el botón “Siguiente” (Ventana 3).



**IMPORTANTE**

Si desea que el certificado digital al finalizar el proceso de importación (“el certificado ya instalado”) pueda ser exportado de nuevo, marque también la casilla: “Marcar esta clave como exportable”. Esto le permitirá hacer una copia de seguridad de las claves o transportarlas en otro momento”. Si no marca esta casilla, el certificado que se está instalando en el equipo que está realizando la importación, ya no podrá ser de nuevo “exportado”.

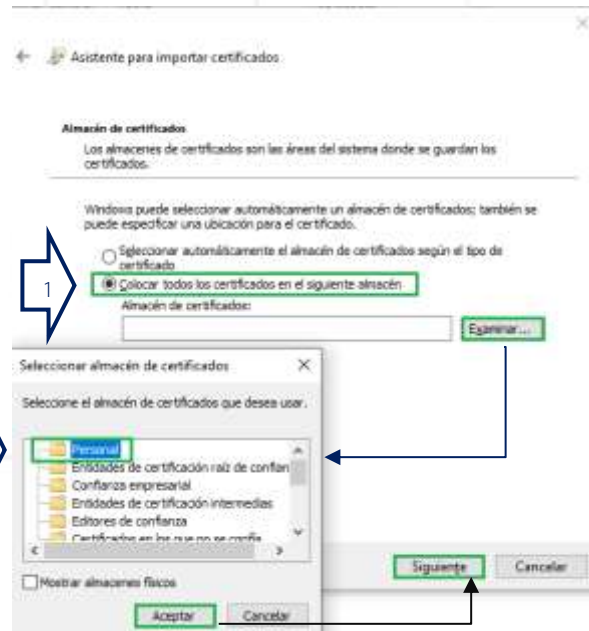
Ventana 3. Protección de clave privada

\*Si en este paso, no le solicita la contraseña, significa que el certificado digital que está intentando instalar **no contiene** una llave privada.

Paso 5. En la ventana de “Almacén de Certificados” especificar la ubicación del certificado digital activando la opción de “Colocar todos los certificados en el siguiente almacén” (1), a continuación, damos clic en el botón “Examinar”, seleccionamos el almacén que se desea usar en este caso en “Personal” (2), damos clic en el botón “Aceptar”, y a continuación damos clic en el botón “Siguiente” (Ventana 4).



## PKCs12



Ventana 4. Ubicación del almacén

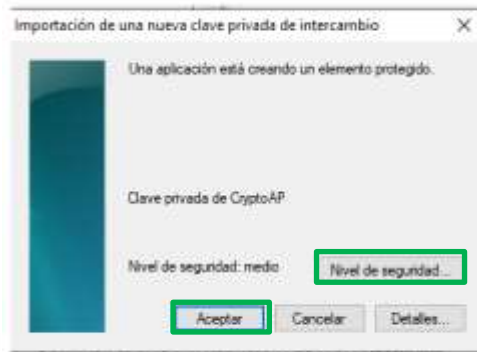
Paso 6. Para la “Finalización del Asistente” damos clic en el botón “Finalizar”, para concluir la importación del certificado digital (Ventana 5).



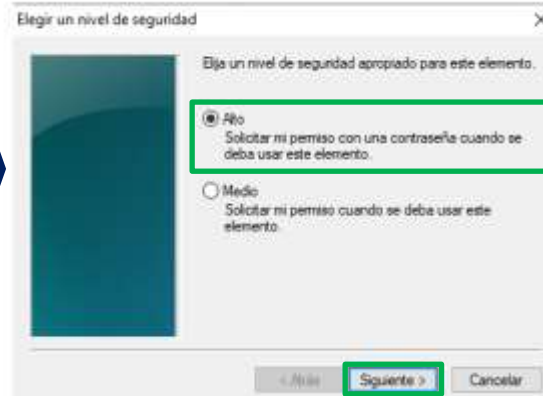
Ventana 5. Finalización del Asistente

## PKCs12

Paso 7. Crear el nivel de seguridad de la llave privada. Para ello damos clic en el botón “Nivel de Seguridad” (Ventana 6), se recomienda seleccionar nivel “Alto”, posteriormente dar clic en el botón de “Siguiente” (Ventana 7).

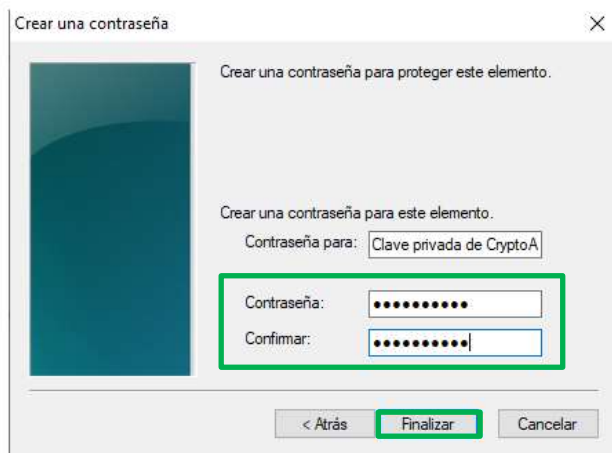


Ventana 6. Importación



Ventana 7. Nivel de Seguridad

Paso 8. Teclear la contraseña asignada por usted y confirmarla, por último, damos clic en el botón “Finalizar” (Ventana 8) y “Aceptar” (Ventana 9).

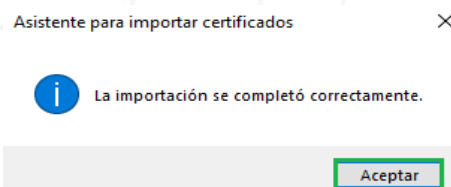


Ventana 8. Contraseña



Ventana 9. Creación

Una vez completado la importación damos clic en el botón “Aceptar” (Ventana 10).





## PKCs12

### Ventana 10. Importación completa

## 5 Cómo exportar (generar una copia) del certificado digital

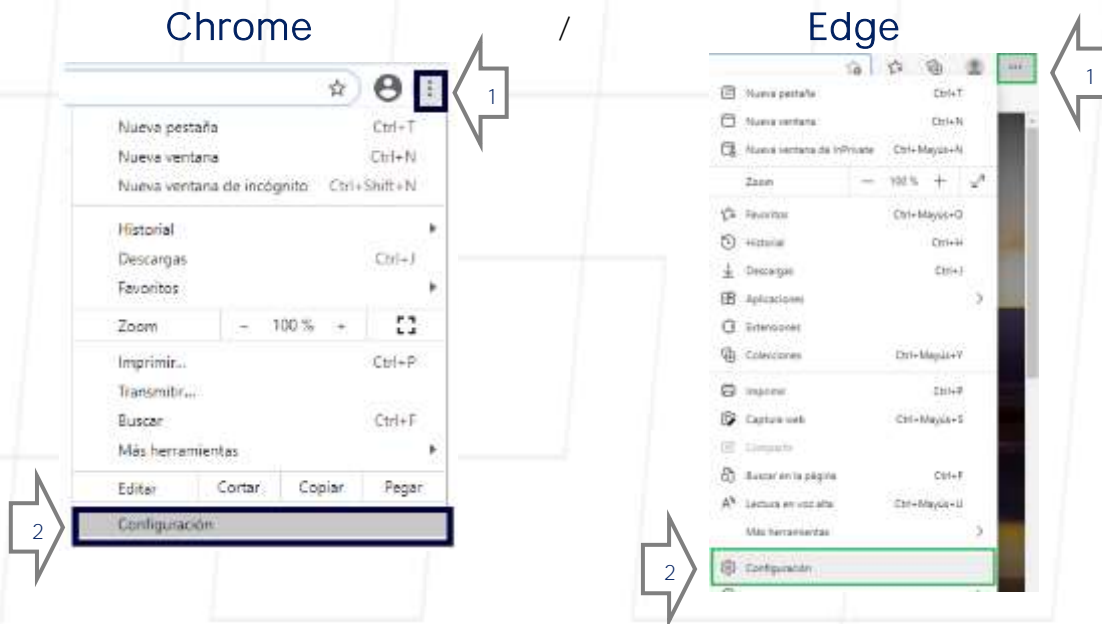
Una vez instalado el archivo **PKCs12** en su computadora, si por algún motivo en otro momento se requiere una **copia del certificado digital** a un dispositivo **USB**, deberá realizar los siguientes pasos:



Se recomienda comprobar que la **llave pública (\*.cer)** haya quedado instalada correctamente.

Para su **copia de seguridad** se deberán seguir los pasos que a continuación se describen:

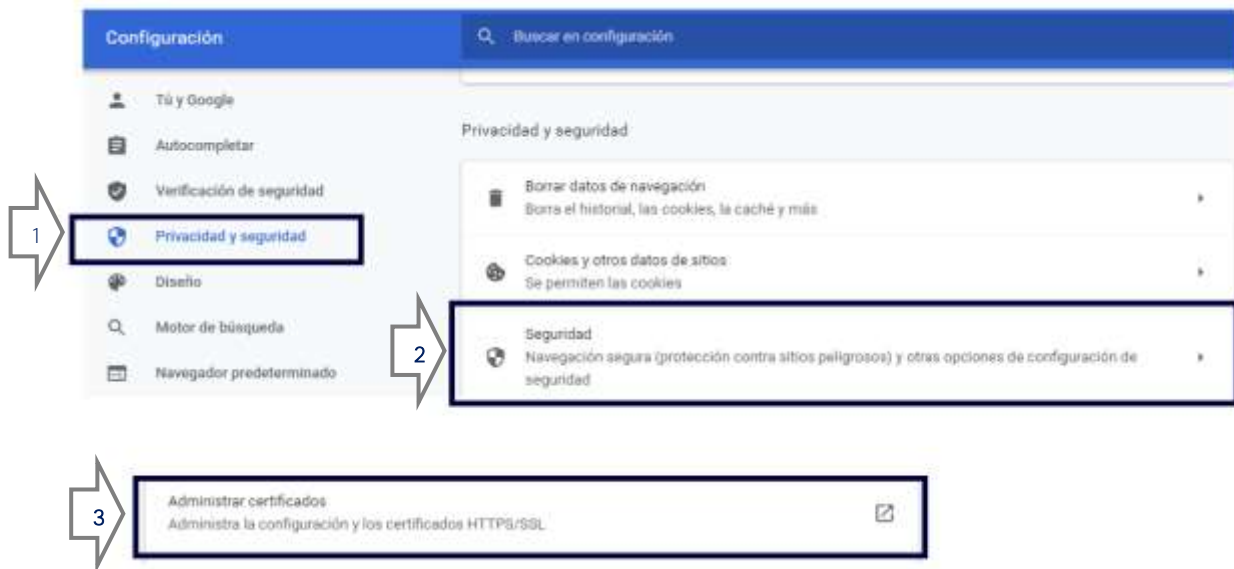
**Paso 1.** En el navegador **Chrome** o **Edge**, deberás ubicar en la parte superior derecha el botón del menú de **tres puntos (1)**, dar un clic para desplegarlo y pulsar la opción **“Configuración” (2)**.



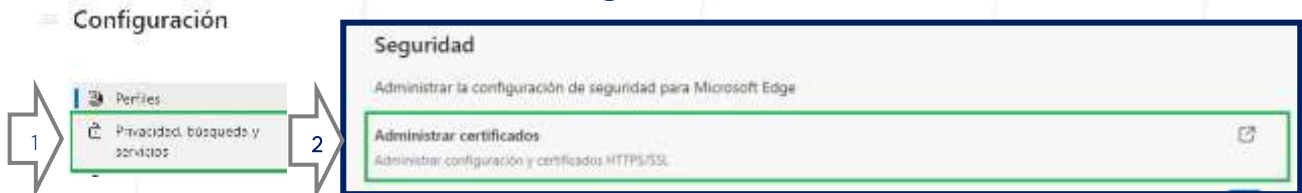
## PKCs12

Paso 2. En la columna izquierda entra en la categoría de “Privacidad” (1) y dentro de las opciones de “Seguridad” (2), daremos un clic en “Administrar Certificados” (3), para visualizar los certificados digitales que tienes instalados en el navegador.

### Chrome

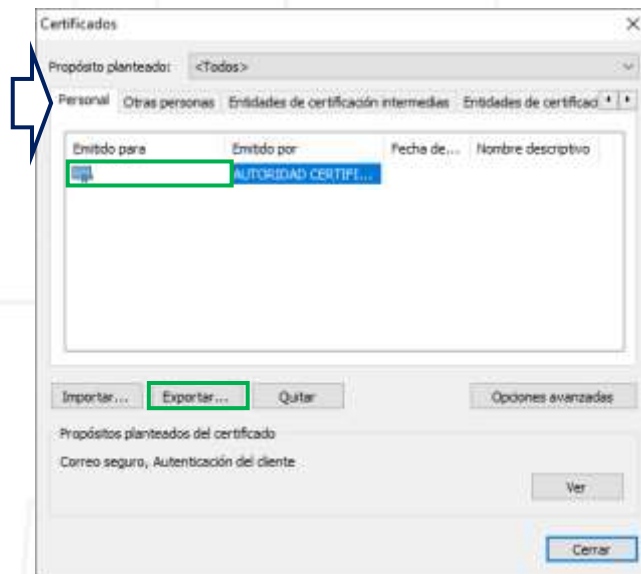


### Edge



## PKCs12

Paso 3. Se abrirá una ventana llamada “Certificados” en la pestaña “Personal” selecciona el **certificado digital** correspondiente, para generar el archivo p12 o pfx por medio del botón “Exportar” (Ventana 1).



Ventana 1. Certificados

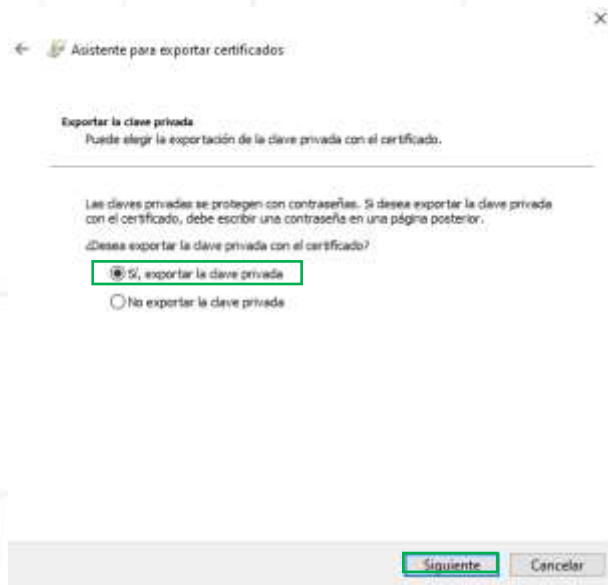
Paso 4. Inicialá el “Asistente para exportar certificados” que lo guiará a través del proceso, damos clic en el botón “Siguiente” (Ventana 2).



Ventana 2. Asistente para exportar certificados

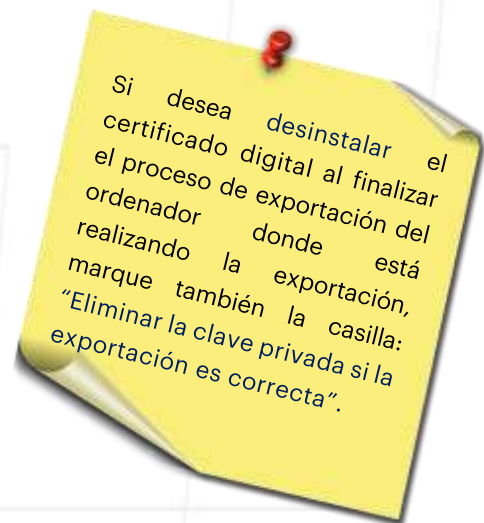
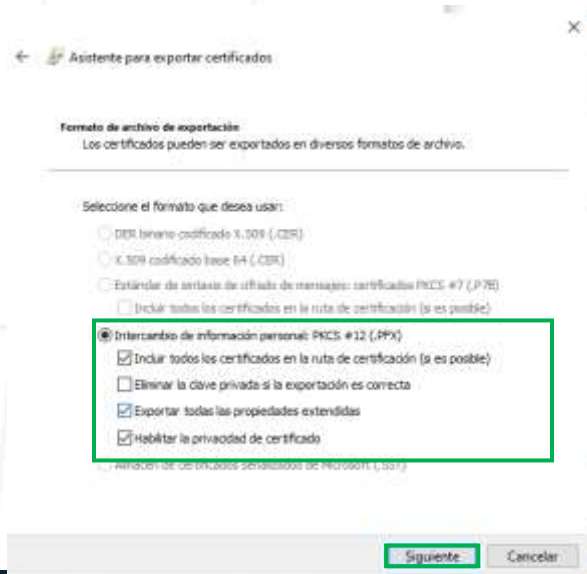
## PKCs12

Paso 5. En este punto es muy importante observar que por default está seleccionada la opción “No exportar la clave privada”, por lo que debemos seleccionar la opción “Si, exportar la clave privada”, sino solo estaremos exportando el certificado digital, damos clic en el botón “Siguiente” (Ventana 3).



Ventana 3. Exportar la clave privada

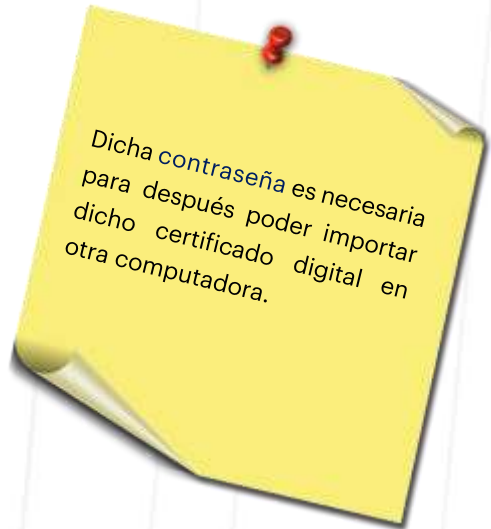
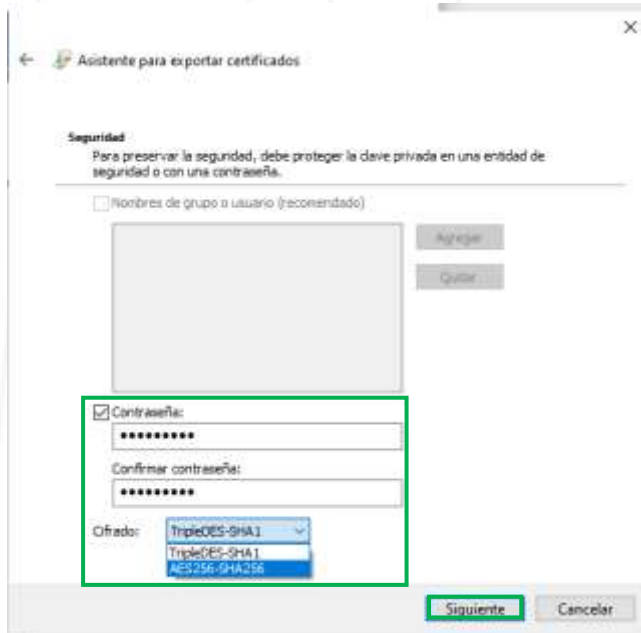
Paso 6. Formato de archivo de exportación, por default seleccionada la opción Intercambio de información personal marque las casillas que aparecen en la ventana (1ra, 3ra y 4ta casilla), posteriormente damos clic en el botón “Siguiente” (Ventana 4).



## PKCs12

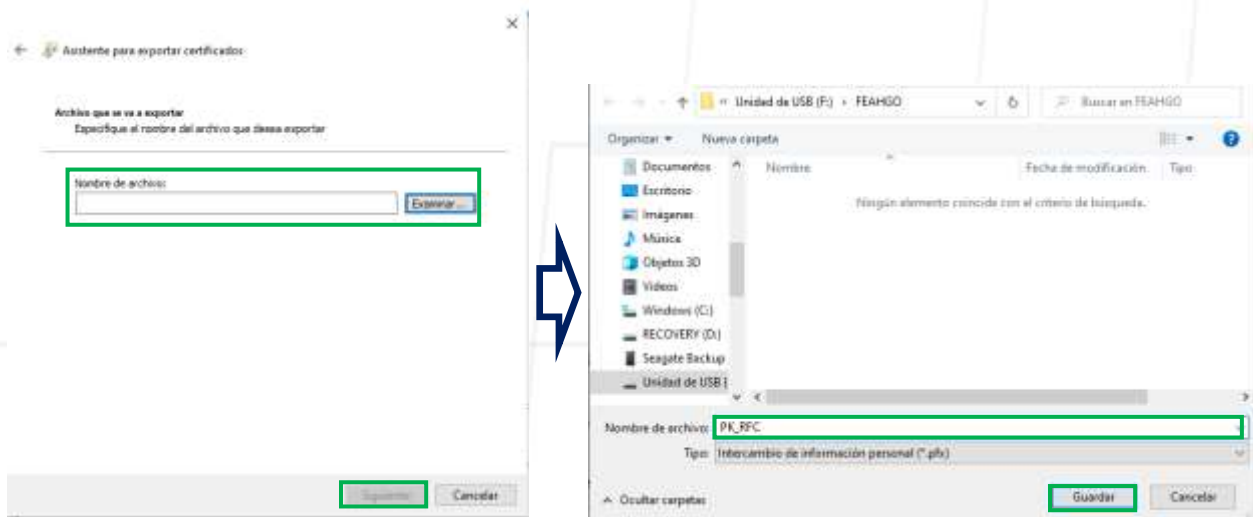
### Ventana 4. Formato de archivo de exportación

Paso 7. **Seguridad**, ingrese la **contraseña** asignada a la **llave privada**, que utiliza a la hora de firmar electrónicamente y **confirmarla**, seleccionar el **cifrado SHA-256**. En seguida damos clic en el botón **“Siguiente”** (Ventana 5).



### Ventana 5. Ingrese contraseña y cifrado SHA256

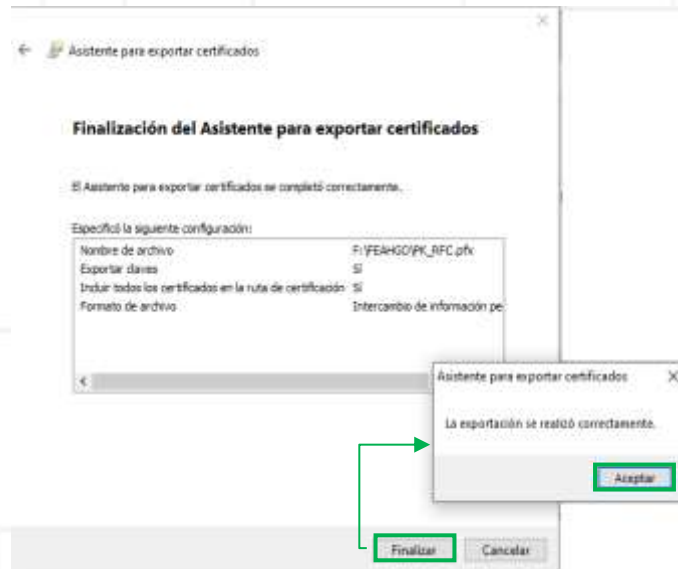
Paso 8. En la siguiente ventana damos clic en el botón de **“Examinar”** para especificar el **nombre del archivo**, así como la ruta donde se desea guardar el archivo PKCs12, y posteriormente en el botón **“Guardar”** y el botón **“Siguiente”** (Ventana 6).



## PKCs12

Ventana 6. Archivo que se va exportar

Paso 9. **Finalización del Asistente**, si todo se realizó correctamente, nos mostrará un **resumen de la configuración** con la que realizamos nuestro archivo, damos clic en el botón de **“Finalizar”** (Ventana 7).



Ventana 7. Finalización del asistente

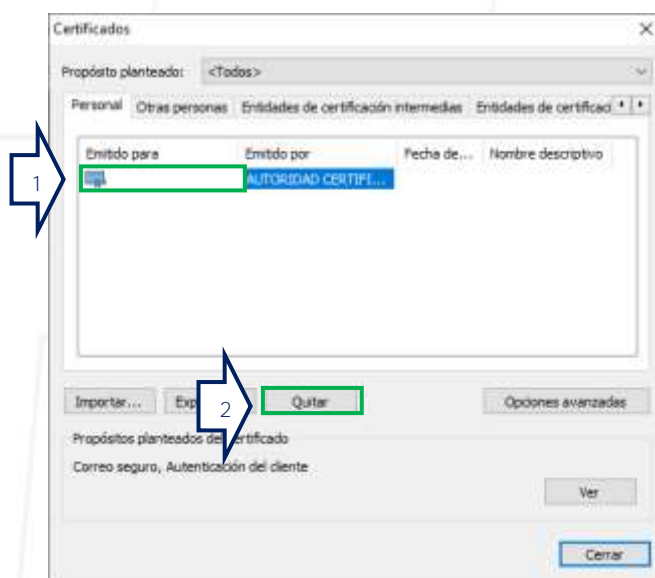


## PKCs12

### 6 Cómo desinstalar (quitar) el certificado digital

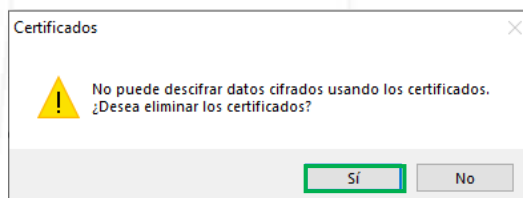
Sigue los pasos anteriores 1 y 2 de la referencia **Como exportar (generar una copia) del certificado digital** y posteriormente realiza lo siguiente:

**Paso 1.** En la ventana de **certificados**, nos muestra por default la pestaña de **“Personal”** donde deberemos seleccionar el **certificado digital** (1) deseado y dar clic en el botón **“Quitar”** (2) cuando desea **desinstalar el certificado digital** del navegador (**Ventana 1**).



Ventana 1. Certificados

Confirmando la eliminación dando clic en el botón **“Sí”**.



## PKCs12

### 7 Datos de Contacto

Si desea obtener información sobre esta guía, así como obtener asesoría y soporte del uso de la **Firma Electrónica Avanzada** contáctenos a:

Dirección General de Innovación Gubernamental y Mejora Regulatoria  
Autoridad Certificadora de Firma Electrónica Avanzada

Teléfono: 800. 623. 4762

Correo electrónico: [autoridad.certificadora@hidalgo.gob.mx](mailto:autoridad.certificadora@hidalgo.gob.mx)

[www.firmaelectronica.hidalgo.gob.mx](http://www.firmaelectronica.hidalgo.gob.mx)