

1. OBJETIVO.

Guiar al lector en el proceso de Instalación del certificado digital para luego realizar el cambio de contraseña.

2. ALCANCE

Aplica desde la importación del certificado hasta la finalización del proceso de instalación del certificado PKCS# 12 (firma electrónica para Persona Jurídica).

3. DESARROLLO

3.1 PROCEDIMIENTO DE INSTALACIÓN DEL CERTIFICADO DIGITAL.

- a) Ubicar el certificado digital en formato P12 (icono de un sobre con una llave)

- b) Dar doble clic al certificado para seguir los pasos del “Asistente para importación de certificados”. Ver Figura 1 Asistente Importación Certificados



Figura 1 Asistente Importación Certificados

c) En el campo de nombre de archivo dejar la ruta por defecto y dar clic en siguiente: Ver Figura 2 Archivo a Importar

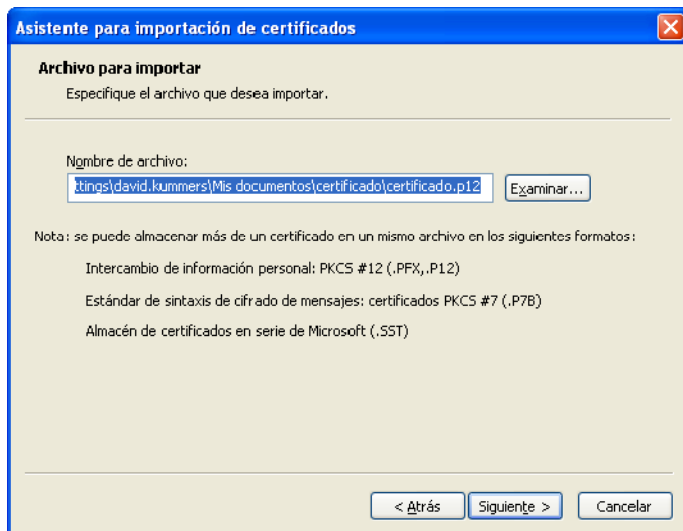


Figura 2 Archivo a Importar

d) En siguiente paso se solicitará la contraseña asignada inicialmente al certificado digital, es necesario que la ingrese y marque las dos casillas "Habilitar protección segura de claves privadas" y "Marcar esta clave como exportable", luego haga clic en siguiente. Ver Figura 3 Contraseña

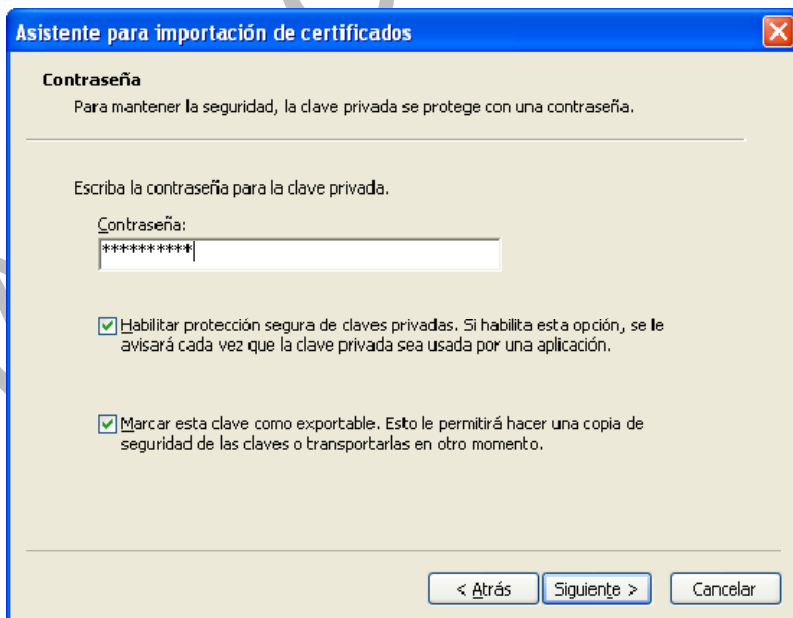


Figura 3 Contraseña

e) Aparecerá seleccionada la primera opción “Seleccionar automáticamente el almacén de certificados en base al tipo de certificado”, debe quedar marcada esa opción, haga clic en siguiente. Ver Figura 4 Almacén Certificado

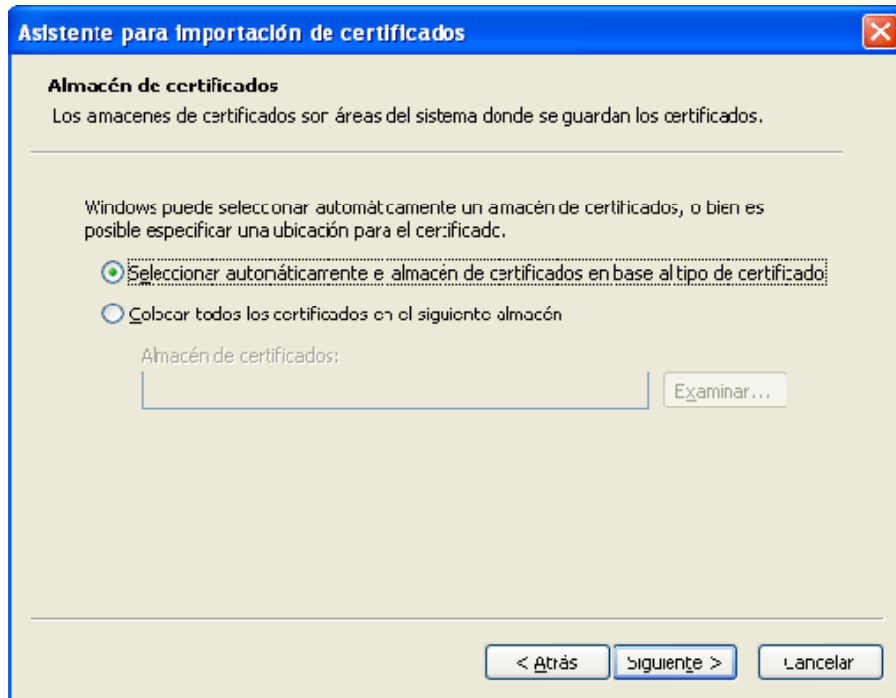


Figura 4 Almacén Certificado

f) Haga clic en finalizar.

g) En la ventana que aparece “Importando una nueva clave privada de intercambio haga clic sobre el botón de “Nivel de seguridad” Ver Figura 5 Nueva Clave

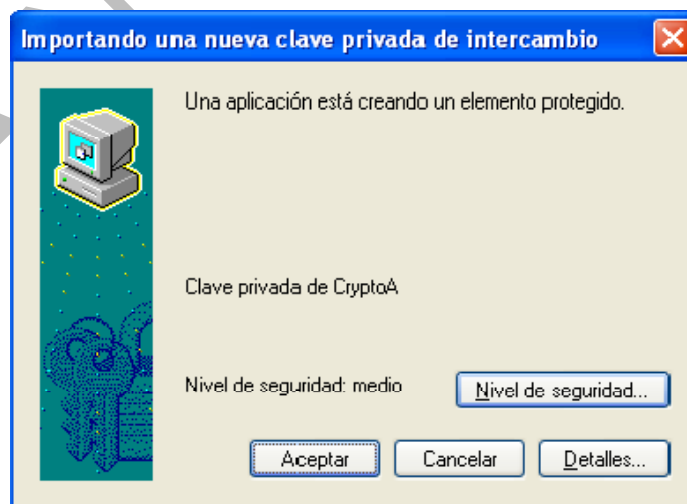


Figura 5 Nueva Clave

h) Seleccione nivel de seguridad alto, haga clic en siguiente, luego ingrese de nuevo la misma contraseña en el primer y segundo campo, luego haga clic en finalizar. Ver Figura 6 Cambio Clave}

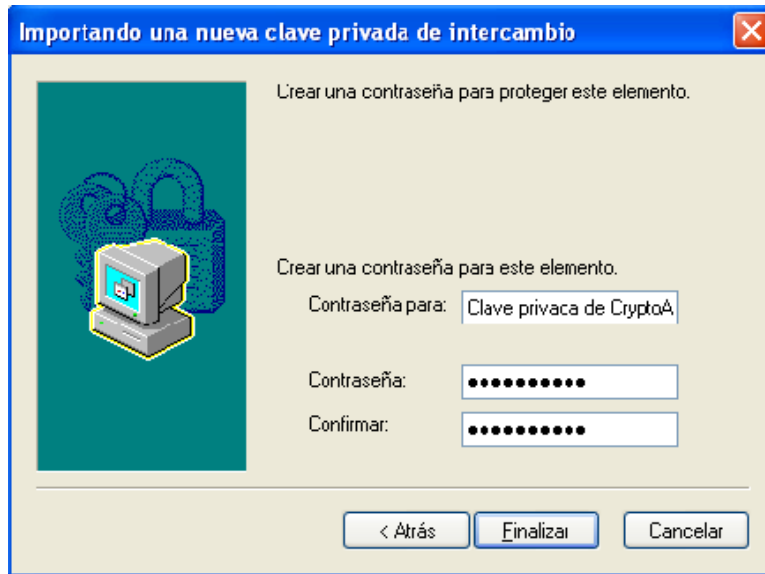


Figura 6 Cambio Clave

i) Haga clic en aceptar para finalizar la instalación del certificado digital.

3.2 CAMBIO DE CONTRASEÑA DEL CERTIFICADO DIGITAL.

a) Vaya a Inicio – Panel de Control. Ver Figura 7 Ubicación Panel de Control.

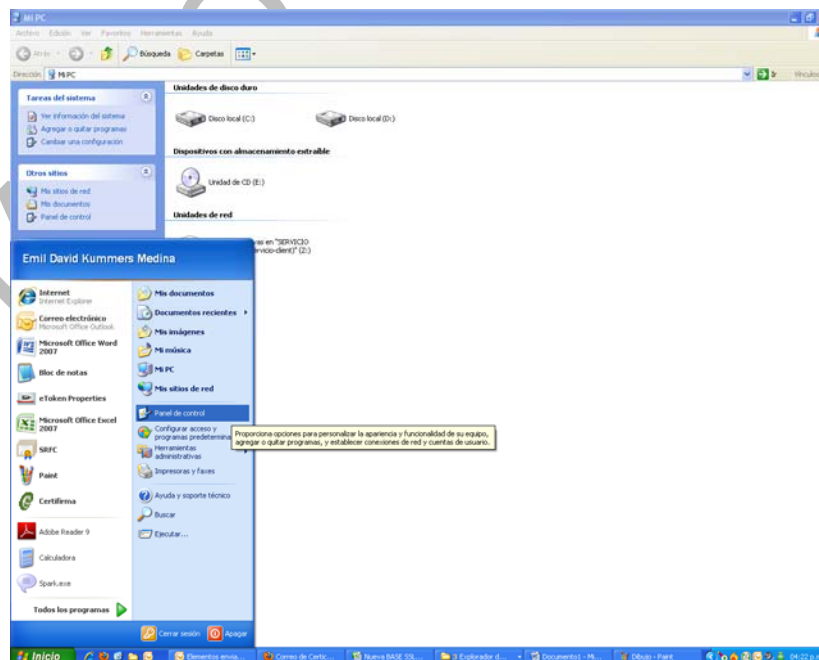


Figura 7 Ubicación Panel de Control

b) Haga doble clic en "Opciones de internet" Ver Figura 8 Panel de control

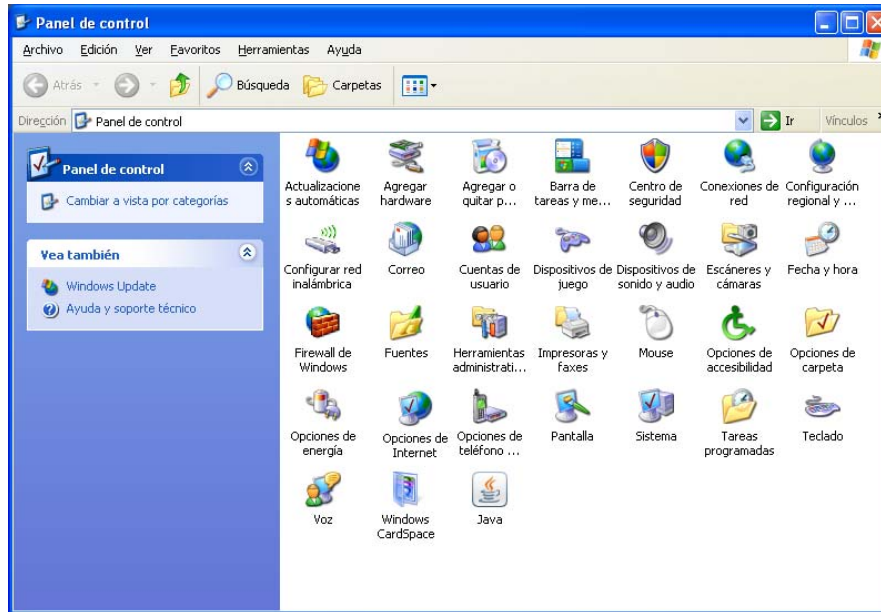


Figura 8 Panel de control

c) En el cuadro de opciones de internet haga clic en la pestaña de contenido y luego en el botón de Certificados. Ver Figura 9 Opciones de Internet

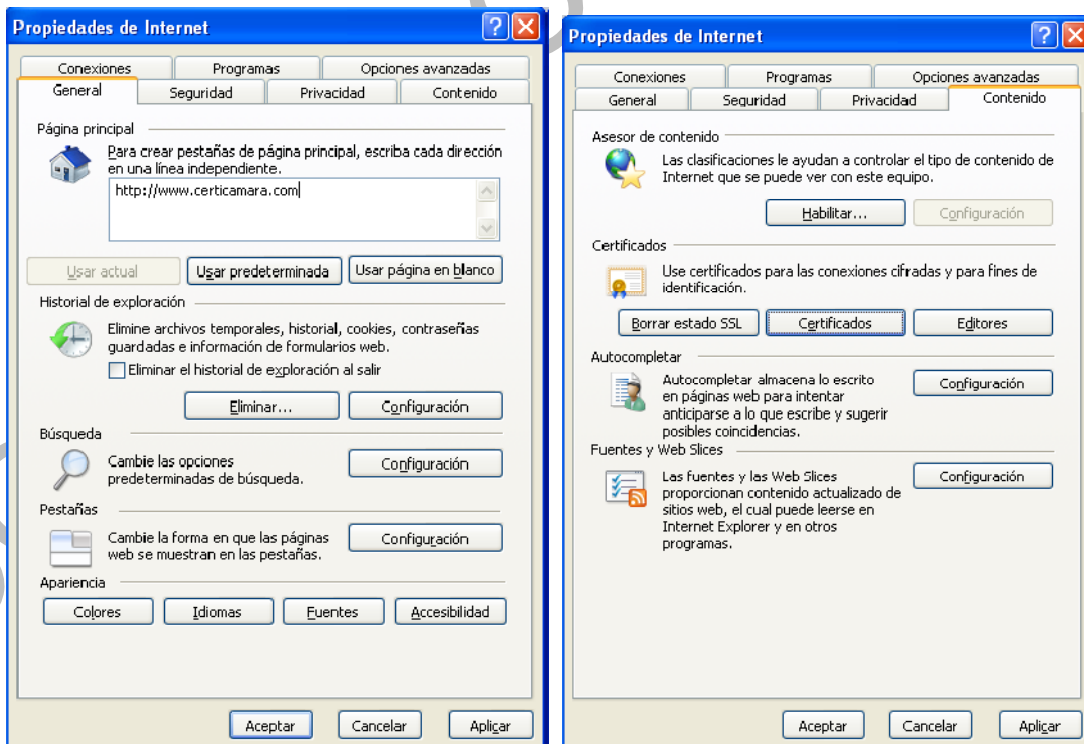


Figura 9 Opciones de Internet

d) Seleccione el certificado digital y haga clic en el botón de ver. Figura 10 Certificado

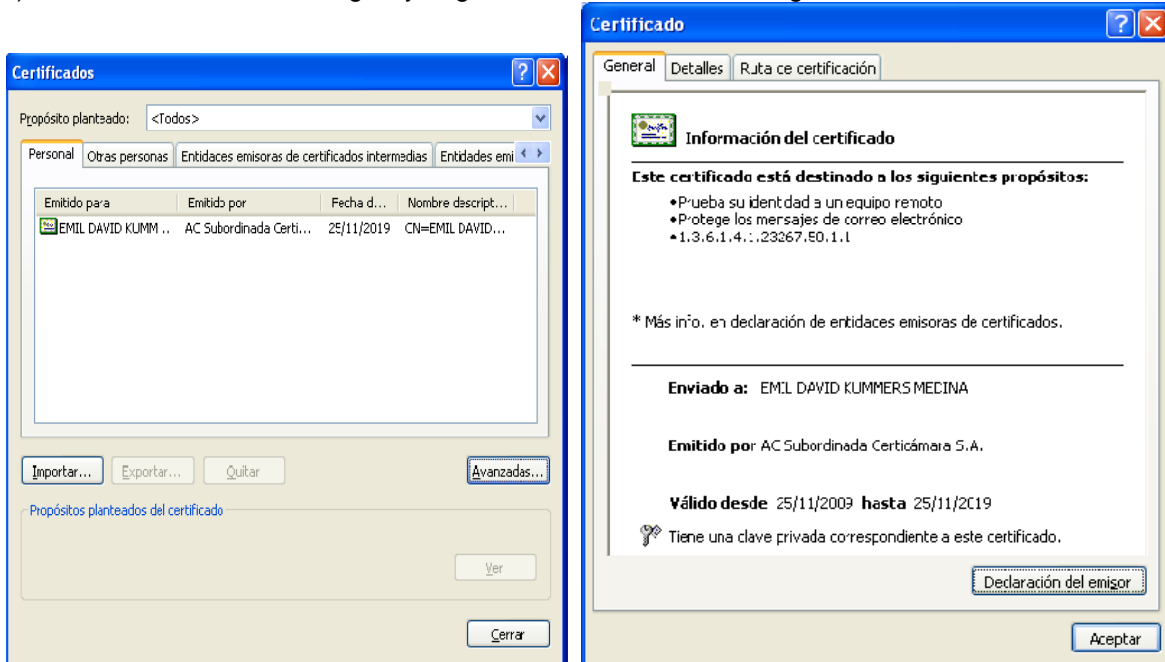


Figura 10 Certificado

e) Haga clic en la pestaña de "Detalles" y luego en el botón de "Copiar en archivo". Ver Figura 11 Detalles

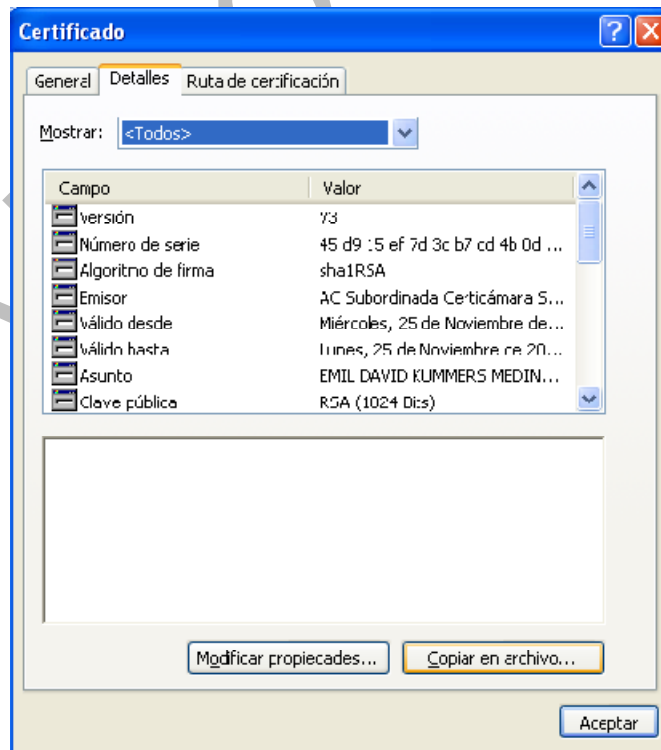


Figura 11 Detalles

f) Haga clic en siguiente y seleccione la opción de “Exportar la clave privada”. Ver Figura 12 Clave Privada

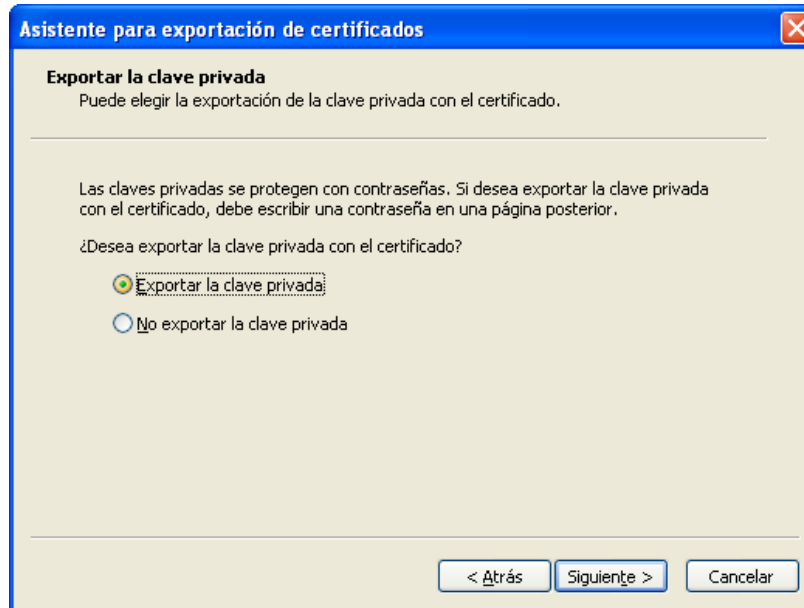


Figura 12 Clave Privada

g) Haga clic en el botón de “Exportar la clave privada” y luego clic en siguiente.

h) En el siguiente cuadro por favor no modifique ninguna opción de las que vienen por defecto, haga clic en siguiente, Ver Figura 13 Explorar Certificado

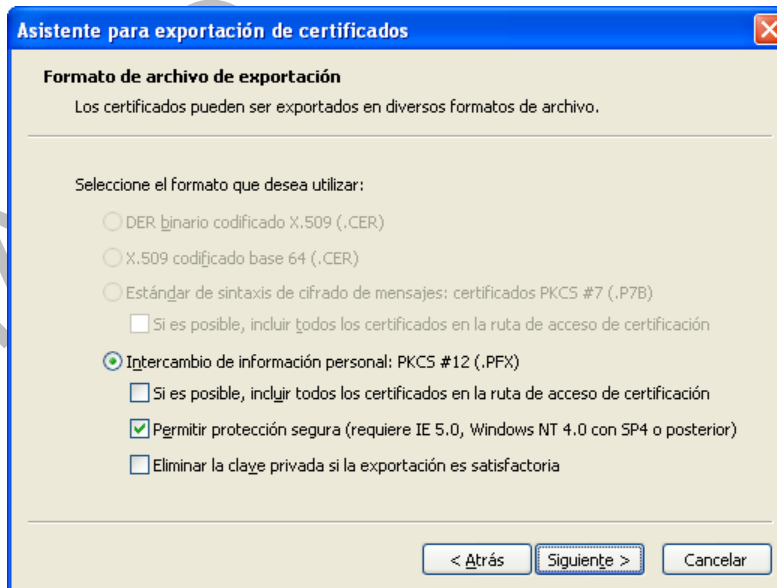
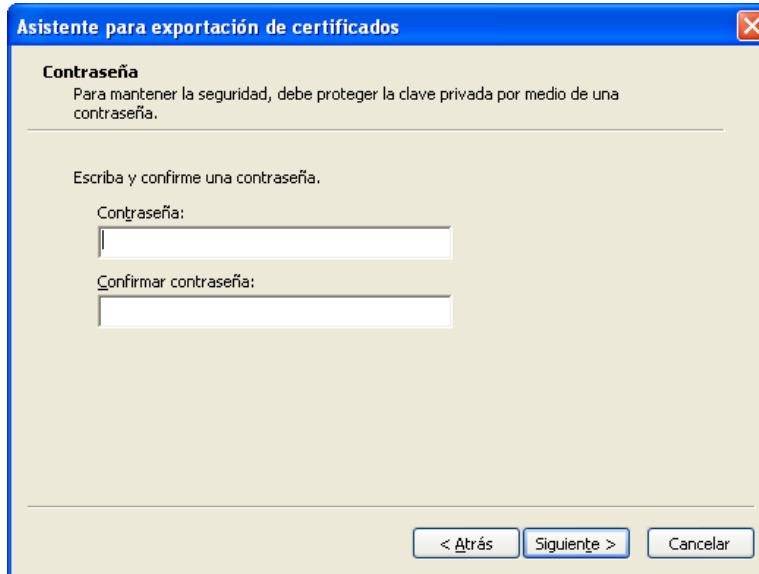


Figura 13 Explorar Certificado

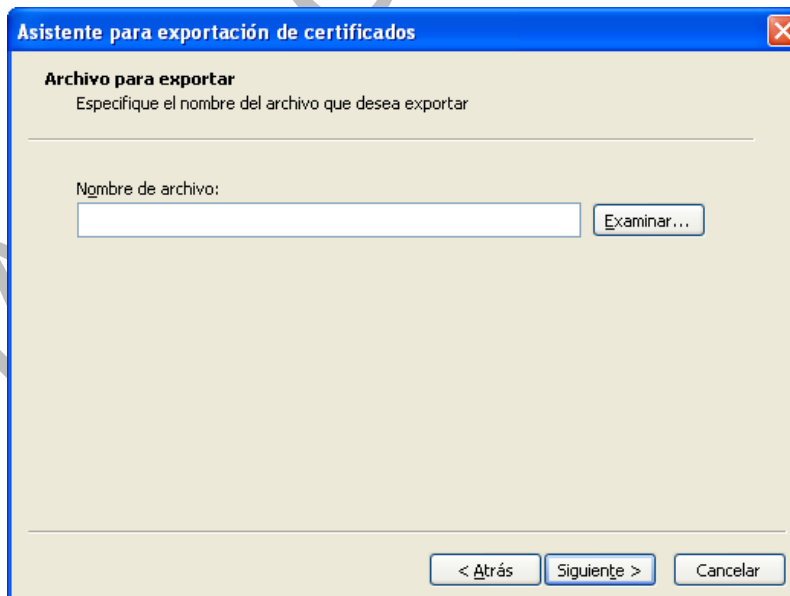
i) En el siguiente cuadro debe introducir la nueva contraseña que va a asignar al certificado digital. Preferiblemente la contraseña que se asigne debe ser como mínimo de 6 caracteres ya sea sólo números y/o sólo letras”. Ver Figura 14 Cambio contraseña



The screenshot shows a dialog box titled "Asistente para exportación de certificados" with a close button (X) in the top right corner. The main heading is "Contraseña". Below it, a text label reads: "Para mantener la seguridad, debe proteger la clave privada por medio de una contraseña." There is a horizontal line separator. Below the separator, the text says "Escriba y confirme una contraseña." There are two input fields: "Contraseña:" and "Confirmar contraseña:". At the bottom right, there are three buttons: "< Atrás", "Siguiente >", and "Cancelar".

Figura 14 Cambio contraseña

j) En el siguiente cuadro haga clic en examinar y seleccione la ubicación donde desea guardar su certificado digital, luego de seleccionar la ruta de almacenamiento haga clic en guardar y luego en siguiente. Ver Figura 15 Ruta Archivo



The screenshot shows a dialog box titled "Asistente para exportación de certificados" with a close button (X) in the top right corner. The main heading is "Archivo para exportar". Below it, a text label reads: "Especifique el nombre del archivo que desea exportar". There is a horizontal line separator. Below the separator, the text says "Nombre de archivo:". There is an input field and a button labeled "Examinar...". At the bottom right, there are three buttons: "< Atrás", "Siguiente >", and "Cancelar".

Figura 15 Ruta Archivo

k) Haga clic en finalizar.

l) En el cuadro de “Exportando su clave de intercambio privada” introduzca la contraseña que le asigne INICIALMENTE a su certificado digital. Ver Figura 16 Intercambio Privada

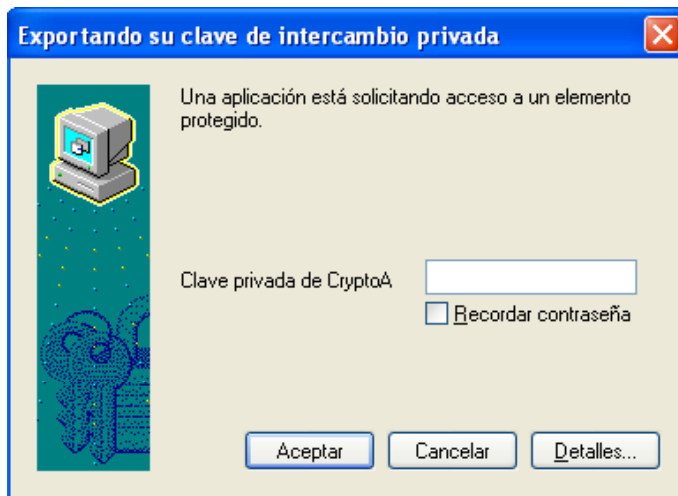


Figura 16 Intercambio Privada

m) Ubique la carpeta donde almacenó su certificado digital para luego instalarlo donde se requiera.

4. DEFINICIONES

- **PKCS#12:** (Public-Key Cryptography Standards) se refiere a un grupo de estándares de criptografía de clave pública concebidos y publicados por los laboratorios de RSA en California. ARSA Security se le asignaron los derechos de licenciamiento para la patente de algoritmo de clave asimétrica RSA y adquirió los derechos de licenciamiento para muchas otras patentes de claves.
- **Certificado digital o Firma Electrónica** (también conocido como certificado de clave pública o certificado de identidad) es un documento digital mediante el cual un tercero confiable (una autoridad de certificación) garantiza la vinculación entre la identidad de un sujeto o entidad (por ejemplo: nombre, dirección y otros aspectos de identificación) y una clave pública.

Sistemas de cifrado de clave pública o sistemas de cifrado asimétricos se inventaron con el fin de evitar por completo el problema del intercambio de claves de los sistemas de cifrado simétricos. Con las claves públicas no es necesario que el remitente y el destinatario se pongan de acuerdo en la clave a emplear.

COPIA NO CONTROLADA