Manual de usuario de APSC
Gestión de certificados personales emitidos por la ACCV

v 2.5.2009

En este manual de usuario se detalla cómo acceder al *Área Personal de Servicios de Certificación* (APSC), qué requisitos son necesarios y cómo utilizar las diferentes funcionalidades que ofrece la aplicación para la gestión de los certificados personales emitidos por la ACCV.

ÍNDICE

1. REQUISITOS PREVIOS

CERTIFICADO DIGITAL

Para acceder a APSC debe disponer al menos de un certificado digital de persona física o jurídica emitido por la ACCV o DNIe.

Dicho certificado digital y sus claves asociadas deben haber sido configurados previamente en su navegador web para poder identificarse de forma segura a través de Internet. Puede confirmar si su certificado digital y sus claves están correctamente configurados en:

- Certificados emitidos por la **ACCV**: https://www.accv.es/ayuda/comprobacion-firma-electronica/comprobacion-firma-electronica/
- **DNIe** emitido por el Cuerpo Nacional de Policía: https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_320

VERIFICACIÓN DE CORREO-E

Durante los procesos de emisión y renovación de su certificado digital, la cuenta de correo-e que tenga asociada a dicho certificado deberá verificarse mediante un enlace de comprobación que será enviado en una notificación a dicha cuenta.

Por su sencillez, y para facilitar la lectura y comprensión de los procesos, a lo largo del manual este requisito no se especificará de forma descriptiva en cada supuesto. Sin embargo el lector

debe conocer su existencia y entender la necesidad de verificar la cuenta de correo-e asociada a su certificado a la hora de seguir de los pasos descritos a continuación.

Cualquier duda o consulta relativa a la instalación de su DNIe debe remitirla a su Servicio de Atención al Ciudadano. Dispone de más información al respecto en el siguiente enlace: **https://www.dnielectronico.es/PortalDNIe/PRF1_Cons02.action?pag=REF_**2110

En caso de duda o consulta relativa a este manual puede contactar con nosotros a través del **963 866 014** o del formulario de atención (http://www.accv.es/contacta/).

2. CÓMO PUEDE ACCEDER A APSC

Una vez ha verificado que cumple con los requisitos previos, usted podrá acceder a APSC identificándose con su certificado a través de la siguiente dirección: https://apsc.accv.es/apsc/

3. QUÉ PUEDE HACER A TRAVÉS DE APSC

A continuación se describen las gestiones que APSC le permite realizar. Rogamos lea detenidamente una sección antes de realizar las acciones que describe.

3.1. MODIFICAR SUS DATOS DE CONTACTO

A través de esta opción usted puede ejercer el DERECHO DE RECTIFICACIÓN tal y como establece el artículo 16 de la Ley Orgánica 15/1999, de Protección de Datos de Carácter Personal.

La opción permite al usuario modificar sus **datos de contacto**. El resto de datos forman parte de su certificado digital y sólo se podrán cambiar:

- Si su certificado es de Ciudadano,
  - Acudiendo a un Punto de Registro de Usuario (PRU) para solicitar la revocación de su certificado actual y el alta de uno nuevo con los datos que usted aporte.
  - Si está en periodo de renovación (el cual se inicia 70 días antes de que su certificado caduque), podrá modificar su cuenta de correo electrónico al generarse un nuevo certificado.

- Si su certificado es de Empleado Público o de Pertenencia a Empresa,
  - Contactando con el responsable de su certificado digital en su organismo/entidad para solicitar a esta persona la revocación de su certificado actual y el alta de uno nuevo con los datos correctos.
  - Si está en periodo de renovación (el cual se inicia 70 días antes de que su certificado caduque), podrá modificar su cuenta de correo electrónico al generarse un nuevo certificado.

Para acceder pulse el botón **Datos personales** del menú de la página principal de APSC y siga las instrucciones facilitadas por la aplicación.

Recuerde que no podrá modificar los datos que se le mostrarán en las casillas sombreadas sin revocar su certificado.

A través de esta funcionalidad Usted puede ver y modificar sus datos tal y como establece el artículo 16 de la Ley de Protección de Datos de Carácter Personal.

DATOS PERSONALES

3.2. OBTENER UN CERT. CUALIFICADO DE CIUDADANO EN SOPORTE SOFTWARE

Si usted aún no dispone de un certificado cualificado de Ciudadano en soporte software, puede obtener uno a través de APSC identificándose con su DNIe, con su certificado cualificado de

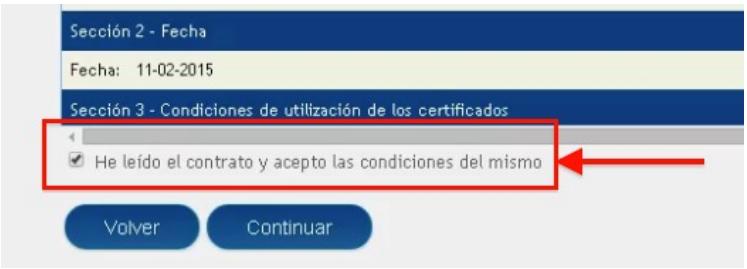
Empleado Público o de Pertenencia a Empresa. Los pasos a seguir son:

1. Acceda a APSC y pulse sobre el botón **Obtener CERTIFICADO CIUDADANO** del menú de la página principal.

2. En la pantalla que se le mostrará, selecciones la opción de generación en **Software**.

3. A continuación, revise sus datos de contacto y asegúrese que todos los campos obligatorios han sido introducidos. Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados. Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.



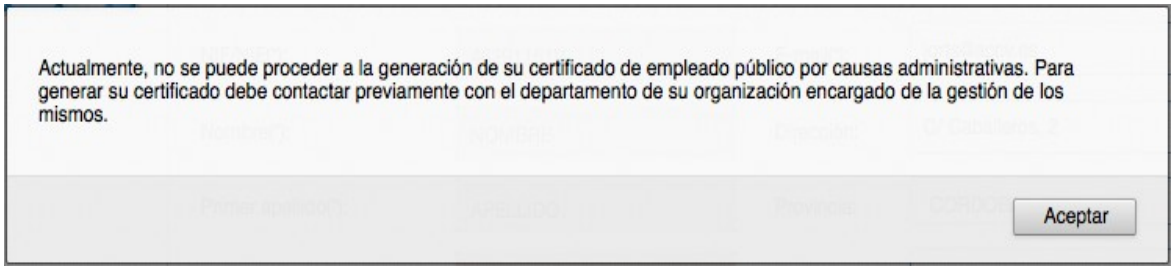
A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

3.3. OBTENER UN CERT. CUALIFICADO DE EMPLEADO PÚBLICO EN SOFTWARE

Si usted trabaja para la Administración Pública y dispone de certificado cualificado de Empleado Público en tarjeta criptográfica emitido por la ACCV y **en vigor**, puede obtener un certificado equivalente de Empleado Público en soporte software a través de APSC.

⚠ Para poder obtener un certificado cualificado de Empleado Público en soporte software a través de APSC es necesario que su organismo/entidad haya contratado previamente el servicio con la ACCV. Si trata de realizar esta acción y obtiene un mensaje similar al que puede observarse a continuación, contacte con el responsable de los certificados de Empleado Público en su organismo/entidad para que contrate el servicio con la ACCV y pueda usted realizar la generación.



Los pasos a llevar a cabo son:

Si lo desea puede generar un certificado de empleado público en soporte software con sus datos.

1. Acceda a APSC con su certificado cualificado de Empleado Público en tarjeta criptográfica y pulse sobre el botón **Obtener CERTIFICADO E. PÚBLICO** del menú de la página principal.

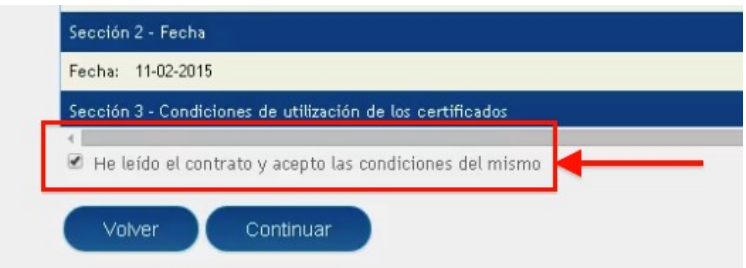
2. En la pantalla que se le mostrará, seleccione la opción de generación en **Software**.

3. A continuación,revise sus datos de contacto y asegúrese que todos los campos obligatorios han sido introducidos.

   Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

   Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus



condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.

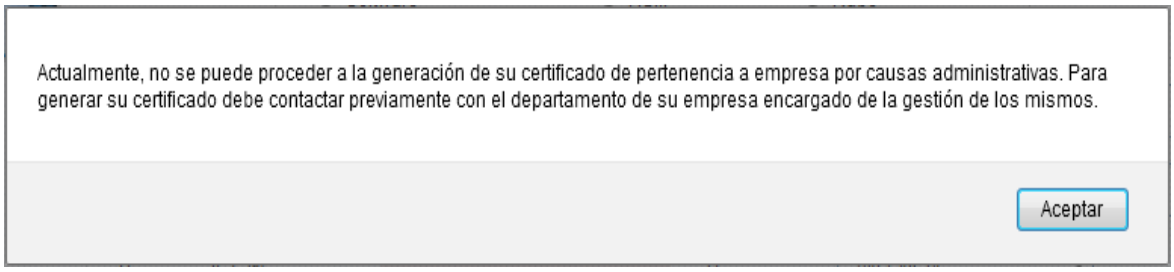
A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

3.4. OBTENER UN CERT. CUALIFICADO DE PERTENENCIA A EMPRESA EN SOFTWARE

Si usted dispone de certificado cualificado de Pertenencia a Empresa en tarjeta criptográfica emitido por la ACCV y **en vigor**, puede obtener un certificado equivalente de Pertenencia a Empresa en soporte software a través de APSC.

⚠ Para poder obtener un certificado cualificado de Pertenencia a Empresa en soporte software a través de APSC es necesario que su organismo/entidad haya contratado previamente el servicio con la ACCV. Si trata de realizar esta acción y obtiene un mensaje similar al que puede observarse a continuación, contacte con el responsable de los certificados de Pertenencia a Empresa en en su organismo/entidad para que contrate el servicio con la ACCV y pueda usted realizar la generación.



Los pasos a llevar a cabo son:

1. Acceda a APSC con su certificado cualificado de Pertenencia a Empresa en tarjeta criptográfica y pulse sobre el botón **Obtener CERTIFICADO P.EMPRESA** del menú de la página principal.

2. En la pantalla que se le mostrará, seleccione la opción de generación en **Software**.

3. A continuación,revise sus datos de contacto y asegúrese que todos los campos obligatorios han sido introducidos.

   Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

   Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus

condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.

A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

3.5. OBTENER UN CERT. DE SELLO-e DE ENTIDAD EN SOPORTE SOFTWARE

Si usted es el representante de una entidad, pública o privada, y dispone de un certificado de persona física (de Ciudadano, de Empleado Público, de Pertenencia a Empresa o de Representante de Entidad) emitido por la ACCV o DNIe **en vigor**, puede obtener un certificado de Sello Electrónico de Entidad en soporte software a través de APSC.

⚠ Para poder obtener un certificado de Sello Electrónico de Entidad en soporte software a través de APSC es necesario que cumpla con **una** de estas dos opciones:

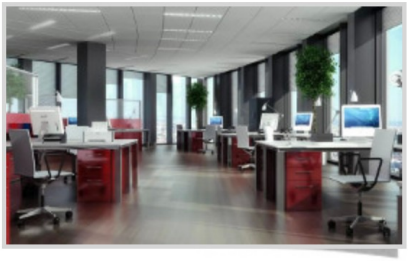
- O bien, dispone de un certificado de Representante de Entidad en vigor a su nombre, en soporte software o tarjeta criptográfica. En este caso deberá identificarse frente a APSC con ese certificado y no otro.
- O bien, ha contratado previamente con la ACCV la adquisición de un certificado de Sello Electrónico de Entidad. Dipone de más información en **www.accv.es**

En caso contrario no dispondrá de la opción al acceder a APSC.

Los pasos a llevar a cabo son:

1. Acceda a APSC con uno de los certificados admitidos y del que sea titular.

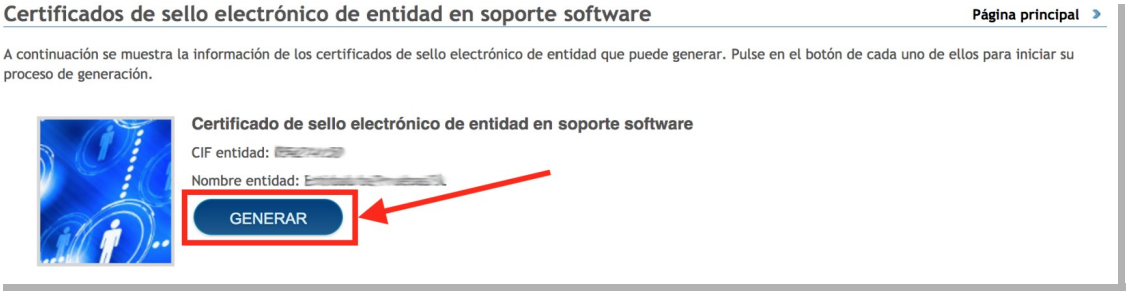
   Pulse sobre el botón **Obtener CERT. S.E. ENTIDAD** del menú de la página principal.



Dispone de autorización para generar un certificado de sello electrónico de entidad en soporte software. Pulse sobre el botón para ir a la página de generación del certificado.

Obtener CERT. S. E. ENTIDAD

2. En la pantalla siguiente observará un listado con los datos de las entidades para las cuales usted puede generar un certificado de Sello Electrónico de Entidad en soporte software. Pulse sobre el botón **Generar** de aquella para la cual desee obtener el certificado.



3. A continuación se le mostrará una nueva pantalla donde deberá seleccionar la opción de generación en **Software**.

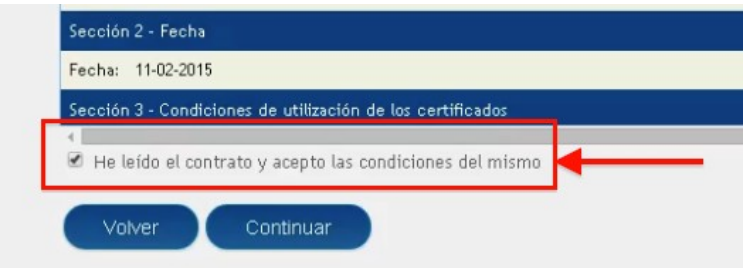
Hecho esto, deberá revisar sus datos de contacto y asegurarse que todos los campos obligatorios han sido introducidos y son correctos.

Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*.

   Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.



A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

3.6. OBTENER UN CERT. DE REPRESENTANTE DE ENTIDAD EN SOPORTE SOFTWARE

Si usted es el representante de una entidad, pública o privada, y dispone de un certificado de personal (de Ciudadano, de Empleado Público, de Pertenencia a Empresa o de Sello Electrónico de Entidad) emitido por la ACCV o DNIe **en vigor**, puede obtener un certificado de Representante de Entidad en soporte software a través de APSC.

⚠ Para poder obtener un certificado de Representante de Entidad en soporte software a través de APSC es necesario que cumpla con **una** de estas dos opciones:

- O bien, dispone de un certificado de Sello Electrónico de Entidad en vigor a su nombre, en soporte software o tarjeta criptográfica. En este caso deberá identificarse frente a APSC con ese certificado y no otro.
- O bien, ha contratado previamente con la ACCV la adquisición de un certificado de Representante de Entidad. Dipone de más información en **www.accv.es**

En caso contrario no dispondrá de la opción al acceder a APSC.

Los pasos a llevar a cabo son:

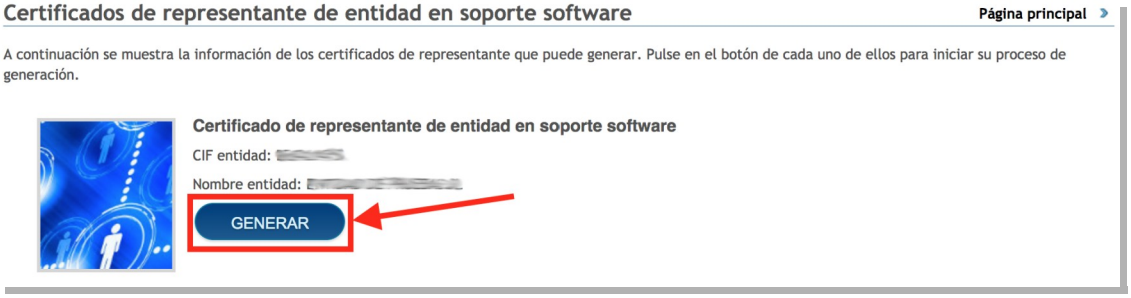
1. Acceda a APSC con uno de los certificados admitidos y del que sea titular.

   Pulse sobre el botón **Obtener CERT. REPRESENTANTE** del menú de la página principal.

Dispone de autorización para generar un certificado de representante de entidad en soporte software. Pulse sobre el botón para ir a la página de generación del certificado.

Obtener CERT. REPRESENTANTE

2. En la pantalla siguiente observará un listado con los datos de las entidades para las cuales usted puede generar un certificado de Representante de Entidad en soporte software. Pulse sobre el botón **Generar** de aquella para la cual desee obtener el certificado.



3. A continuación se le mostrará una nueva pantalla donde deberá seleccionar la opción de generación en **Software**.

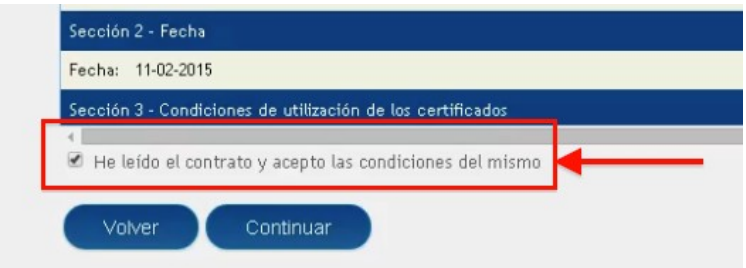
Hecho esto, deberá revisar sus datos de contacto y asegurarse que todos los campos obligatorios han sido introducidos y son correctos.

Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*.

   Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.



A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

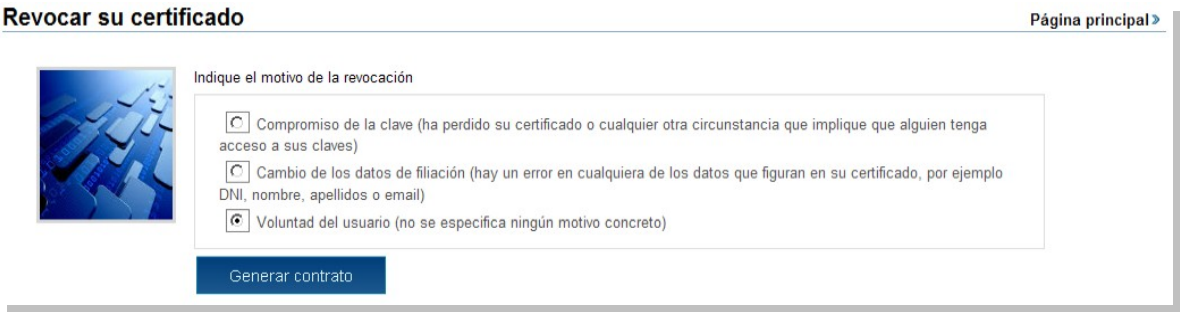
3.7. REVOCAR SU CERTIFICADO DIGITAL

Revocar un certificado es un proceso **irreversible** que anula su validez antes de la fecha de caducidad que consta en el mismo. La revocación suele realizarse cuando el usuario detecta que alguno de los datos de su certificado es incorrecto o que la seguridad de su certificado se puede haber visto comprometida.

Los pasos que debe seguir para la revocación a través de APSC de uno de sus certificados personales emitidos por la ACCV son:

1. Pulse en el menú **REVOCAR** de la página principal de APSC.
   Se le mostrará un listado con los certificados personales activos de los que dispone.

2. Presione sobre el botón **Revocar** asociado al certificado del listado que desea anular.
3. Se le mostrará un mensaje indicando que este proceso es irreversible. Pulse **Aceptar**.
4. Lea los motivos de revocación, seleccione el que más se ajuste a su situación y pulse en **Generar contrato**.



5. Lea el texto de la solicitud de revocación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.

6. Espere mientras se revoca su certificado digital. La pantalla a continuación le indicará el fin del proceso de revocación. Vuelva a la página principal de APSC.

3.8. DESCARGAR UNA COPIA DE SU CERT. Y CLAVES DE CIFRADO EN FICHERO

El cifrado de datos es un proceso que nos permite ocultar el contenido de un mensaje o de un documento para que sólo el destinatario final pueda leerlo.

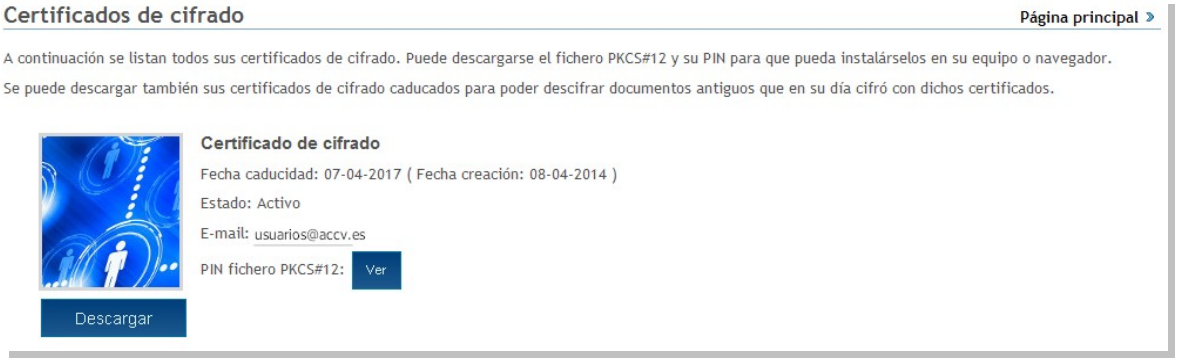
Desde APSC usted puede descargar una copia en fichero (en formato .p12) de los certificados digitales de cifrado (junto con sus claves asociadas) que la ACCV le haya emitido.

⚠ Esta opción sólo estará accesible si usted es o ha sido titular de un certificado cualificado de Ciudadano emitido por la ACCV.

⚠ Se trata de una opción para usuarios con conocimientos avanzados, por lo que sólo se recomienda su uso por personas que conozcan o se hayan informado sobre las bases del cifrado asimétrico.

Los pasos a seguir para descargar una copia de uno de sus certificados de cifrado y claves asociadas son:

1. Pulse en el menú **Su CERTIFICADO DE CIFRADO** de la página principal de APSC..
2. La siguiente pantalla le mostrará una lista con sus certificados de cifrado, con la fecha de caducidad, la cuenta de correo-e asociada y el estado de cada uno (activo o revocado).



3. Seleccione el botón **Descargar** asociado a aquel de sus certificados de cifrado a obtener.
4. Su navegador web es posible que le pregunte sobre dónde desea guardar en su equipo el fichero con el certificado de cifrado seleccionado y sus claves asociadas. Si es así **seleccione la ubicación deseada y guárdelo**.

   En caso contrario, su navegador web guardará el fichero en la carpeta que usted haya configurado por defecto para las descargas.
5. Finalmente, haga clic en el botón **Ver**. asociado al certificado de cifrado que acaba de descargar para visualizar la contraseña/PIN que se le pedirá cada vez que desee acceder al contenido del fichero que acaba de descargar con su el certificado de cifrado seleccionado y sus claves asociadas.

   Deberá anotar o imprimir esta contraseña/PIN y guardarla para poder utilizarla con el fichero que acaba de descargar.

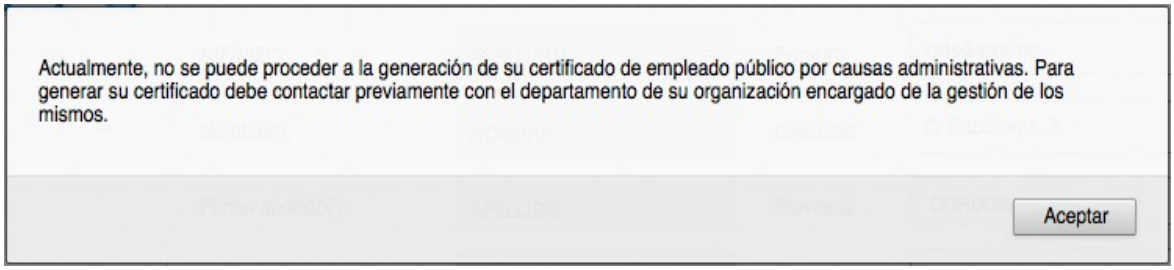
3.9. RENOVAR SU CERTIFICADO DIGITAL EN SOPORTE SOFTWARE

Para poder disponer de esta opción usted debe poseer un certificado personal en soporte software emitido por la ACCV que se encuentre en periodo de renovación, es decir, deben de quedar **menos de 70 días** para que dicho certificado expire.

⚠ NO será posible realizar la renovación a través de APSC si la última vez que renovó dicho certificado ya lo hizo a través de APSC.

Si usted se encuentra en esta situación, APSC le mostrará un mensaje informándole durante el proceso de renovación.

⚠ Si el certificado que usted desea renovar es de Empleado Público o Pertenencia a Empresa, es necesario que su organismo/entidad haya contratado previamente el servicio con la ACCV. Si trata de realizar esta acción y obtiene un mensaje similar al que puede observarse a continuación, contacte con el responsable de los certificados de Empleado Público o Pertenencia a empresa – según proceda - en su organismo/entidad para que contrate el servicio con la ACCV y pueda usted realizar la renovación.



Los pasos para la renovación son los siguientes:

1. Pulse sobre el botón **RENOVAR** del menú de la página principal de APSC.

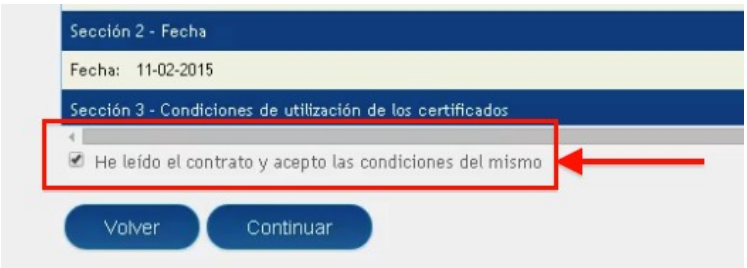
   Se mostrará un listado con la información de renovación de todos sus certificados activos.

2. Presione sobre el botón **RENOVAR** asociado al certificado de la lista que desea renovar.

3. En la siguiente pantalla que se le mostrará, revise sus datos de contacto y, si fuera el caso, rectifique aquellos que hayan cambiado. Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

   Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.



A partir de este punto, los pasos a seguir dependen del navegador web que esté utilizando. Escoja a continuación su navegador web para conocer el resto de pasos:

- Para Internet Explorer (versiones anteriores a la 11) pinche **aquí**.
- Para Internet Explorer 11 y Edge pinche **aquí**.
- Para Firefox y Google Chrome pinche **aquí**.
- Para Safari pinche aquí.

3.10. RENOVAR SU CERTIFICADO DIGITAL EN TARJETA CRIPTOGRÁFICA

Para poder disponer de esta opción usted debe poseer un certificado personal en soporte tarjeta criptográfica emitido por la ACCV y que se encuentre en periodo de renovación, es decir, deben de quedar **menos de 70 días** para que dicho certificado expire.

Puede comprobar la fecha de caducidad de sus certificados a través del menú **RENOVAR** de APSC.

⚠ La renovación de un certificado digital en tarjeta criptográfica a través de APSC sólo está soportada en sistemas **MS Windows**.

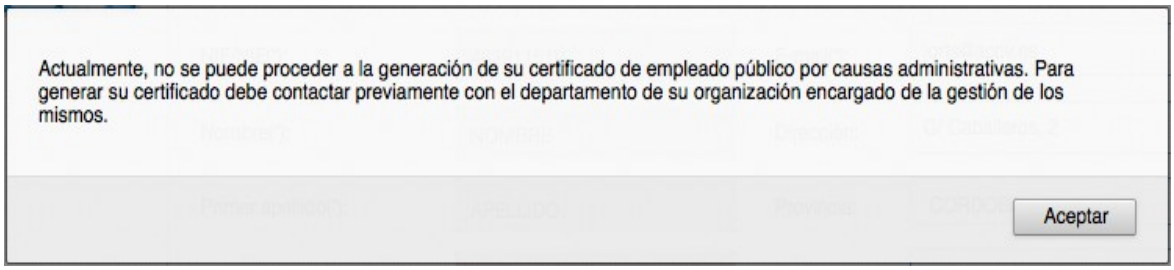
⚠ NO será posible llevar a cabo su renovación a través de APSC si su tarjeta es de fabricante **SIEMENS o es el modelo Starcos SPK 2.4** de Giesecke & Devrient (G&D). Será necesario obtener una nueva tarjeta criptográfica.

Puede determinar el fabricante y modelo de su tarjeta mediante la siguiente aplicación para MS Windows: http://www.accv.es/fileadmin/Archivos/software/ACCV_detectar_tarjeta.exe

⚠ NO será posible realizar la renovación a través de APSC si la última vez que renovó dicho certificado ya lo hizo a través de APSC.

Si usted se encuentra en esta situación, APSC le mostrará un mensaje informándole durante el proceso de renovación.

⚠ Si el certificado que usted desea renovar es de Empleado Público o Pertenencia a Empresa, es necesario que su organismo/entidad haya contratado previamente el servicio con la ACCV. Si trata de realizar esta acción y obtiene un mensaje similar al que puede observarse a continuación, contacte con el responsable de los certificados de Empleado Público o Pertenencia a empresa – según proceda - en su organismo/entidad para que contrate el servicio con la ACCV y pueda usted realizar la renovación.



⚠ En este caso, **usted debe disponer de una versión de Java** instalada en su equipo y accesible desde su navegador web. Puede verificar esta circunstancia en el siguiente enlace: http://java.com/es/download/installed.jsp

Los pasos para la renovación son los siguientes:

1. Pulse sobre el botón **RENOVAR** del menú de la página principal de APSC.

   Se mostrará un listado con la información de renovación de todos sus certificados activos.

2. Presione sobre el botón **RENOVAR** asociado al certificado en tarjeta de la lista que desea renovar.

3. En la siguiente pantalla que se le mostrará, revise sus datos de contacto y, si fuera el caso, rectifique aquellos que hayan cambiado. Los datos que se le mostrarán en las casillas sombreadas no pueden ser modificados.

   Pulse **Generar contrato.**

4. Lea el texto del Contrato de Certificación y acepte sus condiciones marcando la casilla *He leído el contrato y acepto las condiciones del mismo*. Se activará entonces el botón **Continuar.** Presiónelo para formalizar la solicitud.

5. En la siguiente pantalla pulse sobre el botón **Launch** para abrir la aplicación Java que le permitirá renovar su certificado en tarjeta criptográfica.

⚠ Es posible que en este punto su navegador web le pregunte qué programa desea utilizar para ejecutar la aplicación Java que está descargando. Deberá escoger la opción relativa a **Java Web Start**.

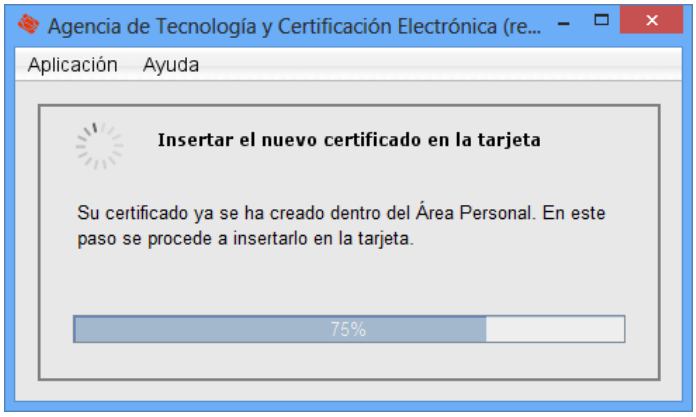
⚠ Al mismo tiempo, algunos navegadores web no están configurados para ejecutar directamente aplicaciones Java como la que se descarga en este punto. Deberá en ese caso descargarla primero a su equipo, para luego ejecutarla haciendo doble clic sobre ella. La aplicación se denomina *renovacion.jnlp*

⚠ Es posible que al pulsar sobre **Launch** obtenga diferentes mensajes de seguridad originados por su navegador web y/o por Java en los que se pedirá su confirmación para continuar. Deberá presionar **Aceptar/Ejecutar/Instalar** según corresponda.

6. Se abrirá la aplicación Java que le permitirá realizar la renovación del certificado y las claves de su tarjeta criptográfica. **Introduzca el PIN** de su tarjeta (no el del DNIe) en la casilla correspondiente y pulse sobre **Comprobar PIN**.

7. La aplicación confirmará que el PIN es correcto y pedirá su confirmación para continuar. Haga clic en el botón **Sí**.

8. La aplicación revocará su antiguo certificado, obtendrá uno nuevo (junto a las correspondientes claves) y sustituirá uno por otro en su tarjeta.



9. Finalmente, la aplicación le indicará que la renovación se ha realizado satisfactoriamente.

   Presione sobre el botón **Salir** para cerrar la aplicación.

   Al mismo tiempo, cierre **todas** las ventanas de su navegador web y extraiga su tarjeta criptográfica del lector.

Mediante esta funcionalidad usted ha revocado su antiguo certificado personal en tarjeta y ha obtenido uno nuevo que lo sustituye.

4. CÓMO LOCALIZAR UN PUNTO DE REGISTRO DE USUARIO (PRU)

Los Puntos de Registro de Usuario (PRU) son ubicaciones donde los ciudadanos, los empleados públicos y las empresas pueden comunicarse con la ACCV. En ellos se pueden solicitar y obtener nuevos certificados digitales personales, revocar y renovar existentes, modificar los datos de contacto, etc

Si usted tiene dificultades para realizar alguna de las acciones que APSC permite hacer de forma telemática, puede acudir a uno de nuestros PRU y realizarla de forma presencial.

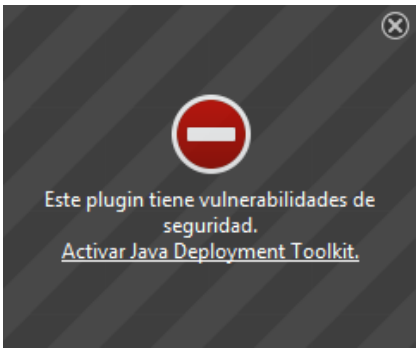
En caso necesario puede localizar su Punto de Registro de Usuario (PRU) más cercano en https://www.accv.es/encuentra-tu-pru/

Para realizar cualquier gestión deberá identificarse con su DNI, NIE o pasaporte español en vigor.

5. MENSAJES Y ERRORES COMUNES

ALERTA DE SEGURIDAD SOBRE EL PLUGIN DE JAVA DEPLOYMENT TOOLKIT EN FIREFOX

Descripción: Al tratar de realizar algunas de las operaciones que permite APSC mediante Mozilla Firefox se obtiene un mensaje similar al de la imagen de la derecha.

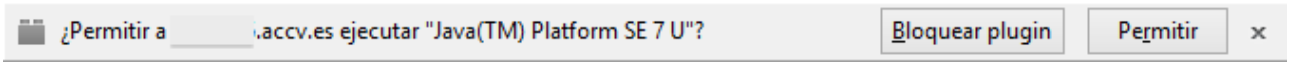


Causa: No se ha deshabilitado el plugin *Java Deployment Toolkit* en Mozilla Firefox.

Solución: Acceder al menú **Opciones** (o Herramientas – según versión) > **Complementos** de Mozilla Firefox. En la sección **Plugins** buscar *Java Deployment Toolkit* y seleccionar la opción **No activar nunca**. Finalmente, **reiniciar** Mozilla Firefox.

MENSAJE DE SOLICITUD DE PERMISO PARA EJECUTAR JAVA EN FIREFOX

Descripción: Al tratar de realizar algunas de las operaciones que permite APSC mediante Mozilla Firefox se obtiene un mensaje similar al siguiente.



Causa: No se le ha indicado a Mozilla Firefox que debe permitir siempre la ejecución de Java.

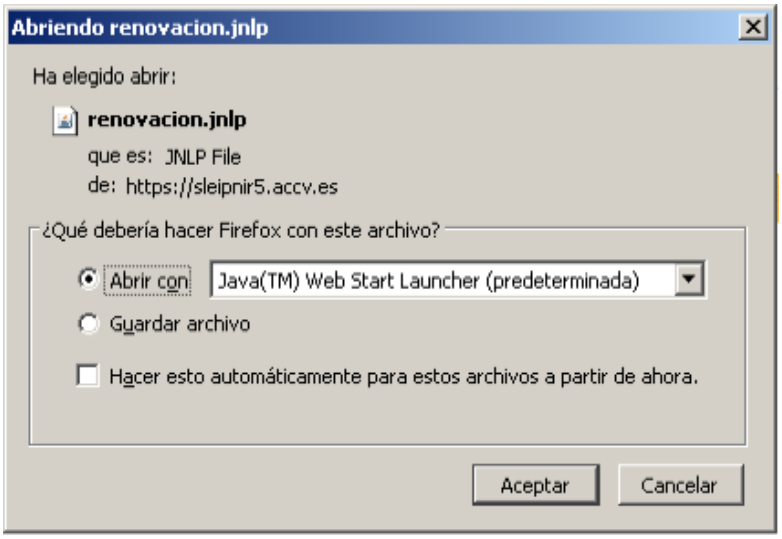
Solución: Acceder al menú **Opciones** (o Herramientas – según versión) > **Complementos** de Mozilla Firefox. En la sección **Plugins** buscar *Java(TM) Platform y seleccionar la opción* ***Activar siempre***.. Finalmente, **reiniciar** Mozilla Firefox.

CONSULTA SOBRE QUÉ PROGRAMA UTILIZAR PARA ABRIR LA APLICACIÓN DE RENOVACIÓN DE LA ACCV

Descripción: Durante el proceso de renovación de un certificado digital en tarjeta criptográfica aparece un mensaje similar al siguiente.

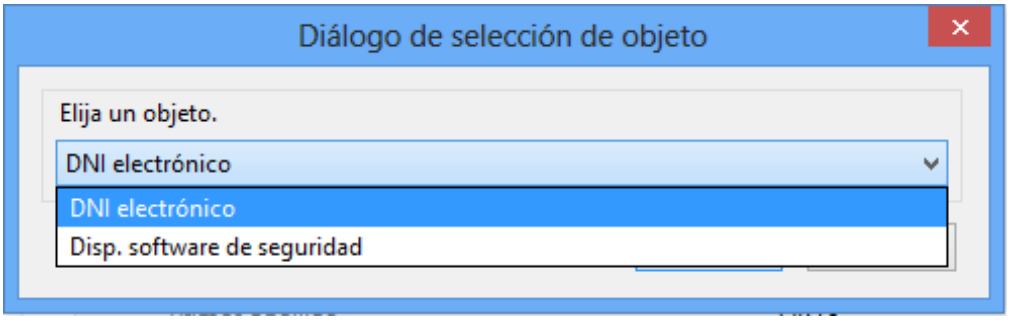
Causa: El navegador web no tiene configurada por defecto ningún programa para abrir aplicaciones JNLP (*Java Network Launching Protocol*).j

Solución: Seleccionar **Abrir con**, escoger la opción relativa a **Java Web Start** y presionar **Aceptar**. De este modo abrirá correctamente la aplicación Java desarrollada por la ACCV para la renovación de certificados digitales en tarjeta criptográfica. Podrá entonces continuar con el proceso normalmente.



CONSULTA SOBRE EL ALMACÉN QUE ALBERGARÁ UN CERTIFICADO EN SOPORTE SOFTWARE GENERADO DESDE APSC CON OTRO EN TARJETA CRIPTOGRÁFICA

Descripción: Utilizando Mozilla **Firefox** durante el proceso de **obtención de un certificado** digital en soporte software mediante un certificado en tarjeta criptográfica de fabricante **G&D**, se muestra una ventana similar a la siguiente.



Causa: No se ha extraído la tarjeta criptográfica del lector cuando se indica durante el proceso de obtención de un certificado digital en soporte software a través de APSC.

Solución: Seleccionar **Disp. software de seguridad** y presionar **Aceptar**.

MENSAJE DE SOLICITUD DE PERMISO PARA EJECUTAR JAVA EN GOOGLE CHROME

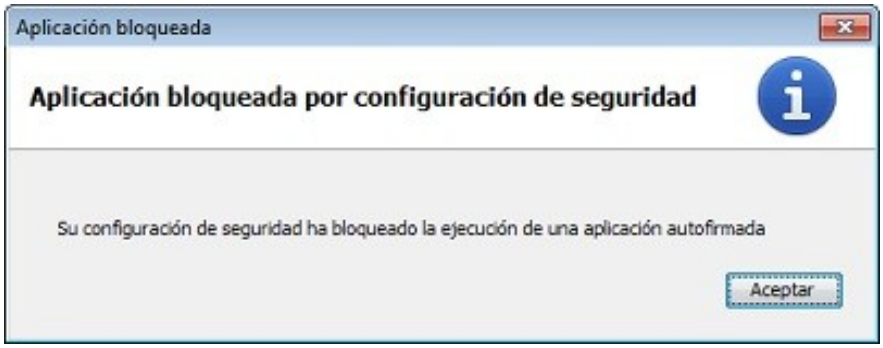
Descripción: Al tratar de realizar algunas de las operaciones que permite APSC mediante Google Chrome se obtiene un mensaje similar al siguiente.

Causa: Google Chrome restringe la ejecución de Java por motivos de seguridad.

Solución: Hacer clic sobre el botón **Ejecutar siempre en este sitio**. Si al seleccionar esta opción Google Chrome no continuara con la ejecución normal de APSC, trate de iniciar de nuevo la gestión que desea.

ALERTA SOBRE EL BLOQUEO DE JAVA EN ALGUNAS DE LAS GESTIONES DE APSC

Descripción: Al tratar de realizar algunas de las operaciones que permite APSC se obtiene un mensaje de Java que indica que "*su configuración de seguridad ha bloqueado la ejecución de una aplicación autofirmada*".



Causa: No se ha bajado previamente el Nivel de se Seguridad a Media.

Solución: Acudir al **Panel de Configuración de Java** siguiendo las indicaciones correspondientes a su versión de Sistema Operativo:

MS Windows - **http://www.java.com/es/download/help/win_controlpanel.xml**

Mac OS X - **https://www.java.com/es/download/help/mac_controlpanel.xml**

Linux - Abra el archivo ControlPanel.html que se encuentra normalmente en el directorio $JAVA_HOME/jre/

Una vez en el Panel de Configuración de Java, seleccionar la pestaña **Seguridad** y bajar el nivel de seguridad a **Alta**. A continuación, edite la **Lista de excepciones de sitios** para agregar https://genera.accv.es y https://apsc.accv.es. Pulse **Aceptar**, **Aplicar** y **Aceptar**.

Finalmente, trate de iniciar de nuevo la gestión que desea hacer mediante APSC desde el principio.

Le recomendamos que una vez haya realizado las gestiones pertinentes con APSC, restituya el nivel de seguridad de Java al que tenía previamente.

ANEXO A. PASOS COMUNES PARA LA OBTENCIÓN DE CERTIFICADOS EN SOPORTE SOFTWARE

Se detallan en función del navegador los pasos comunes entre la generación y la renovación de certificados en soporte software.

▸ INTERNET EXPLORER (versiones anteriores a la 11)

5. En la siguiente pantalla pulse **Generar certificado** para obtener su nuevo certificado en soporte software.

6. Puede aparecer en la parte superior de la página la advertencia: Este sitio web necesita ejecutar el siguiente complemento "*Microsoft Certificate Enrollment Control*"...

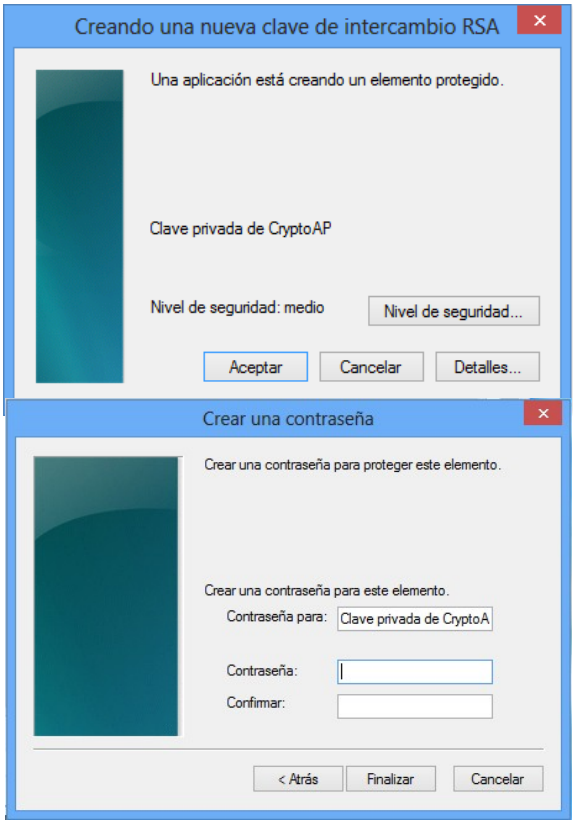
   En ese caso pulse sobre la franja amarilla con el botón derecho del ratón, **Ejecutar** (debe disponer de permisos de administrador).

7. Se le mostrará un mensaje preguntando si desea solicitar un certificado. Responda que **Sí**.

8. A continuación defina una contraseña segura para proteger el acceso a su nuevo certificado digital y claves asociadas. El navegador se la solicitará cada vez que se vaya a hacer uso del mismo.

   Pulse sobre el botón **Nivel de Seguridad**...

   Marque la opción **Alto** y pulse el botón **Siguiente**.



9. **Especifique la contraseña** que desea para su nuevo certificado digital y claves.

   Escríbala de nuevo en el campo *Confirmar*.

   Pulse **Finalizar**.

10. Tras unos segundos Internet Explorer le preguntará si permite que se agregue un nuevo certificado. Responda que **Sí**.

11. Finalmente, APSC le confirmará que su certificado ha sido generado correctamente. Cierre **todas** las ventanas de su navegador web para reiniciarlo.

Le recordamos que si desea disponer de una copia en fichero (extensión .pfx o .p12) de su nuevo certificado personal, puede obtenerla siguiendo las instrucciones de: http://www.accv.es/fileadmin/Archivos/manuales_sw/exportar_ie_c.pdf

▸ FIREFOX Y GOOGLE CHROME

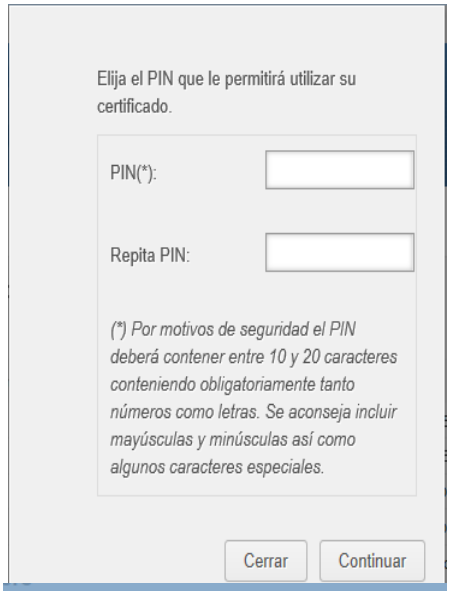
5. En la siguiente pantalla pulse **Generar certificado** para obtener su nuevo certificado en soporte software.

6. En este momento se le pedirá que defina usted un PIN que protegerá el fichero que se dispone a generar y que albergará su certificado personal y claves criptográficas.

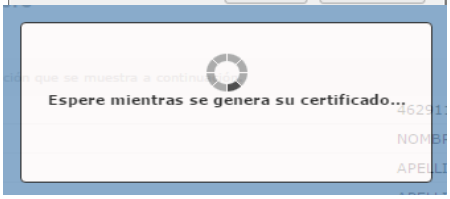
   Por motivos de seguridad dicho PIN deberá tener **10 caracteres** como mínimo y como máximo 20.

   Entre los caracteres deberán haber obligatoriamente **números y letras.** Y se aconseja incluir mayúsculas, minúsculas y símbolos como +, -, =, *, ", !, etc.

   Una vez introducido dos veces el PIN, pulse **Continuar**.

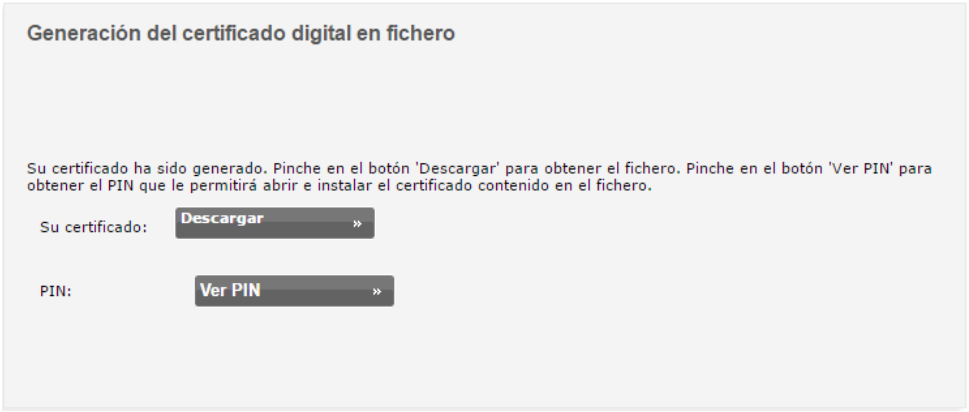


7. Deberá esperar unos segundos mientras se genera su certificado personal.



8. Finalmente, mediante el botón **Descargar** podrá guardar en su ordenador el fichero .p12 que contiene su nuevo certificado personal y claves. El nombre del fichero seguirá la siguiente sintaxis: *<NIF/NIE del titular>_<nombre del titular>_<1er apellido del titular>.p12*

   Presionando sobre **Ver PIN** puede verificar el PIN que usted ha asignado a dicho fichero .p12 en el paso 3 de esta guía y que se le requerirá cuando vaya a instalarlo.



9. Una vez descargado el fichero .p12, **cierre todas las ventanas** de su navegador web.

10. Para finalizar, **debe instalar su certificado** en su navegador web a través del fichero .p12 que acaba de generar. Siga los pasos de la guía correspondiente al navegador web que vaya a utilizar y que puede descargar desde www.accv.es, menú *Ayuda*, sección *Certificado digital en soporte software*, enlace *Instalar el certificado digital en fichero*.

Le recomendamos que guarde una copia de respaldo del fichero .p12 que ha generado en un dispositivo externo como una memoria USB o un CD-ROM. Dispositivo que deberá conservar en un lugar seguro. De ese modo, mientras su certificado permanezca en vigor, podrá

recuperarlo cuando lo necesite.

▸ SAFARI

5. En la siguiente pantalla pulse **Generar certificado** para obtener su nuevo certificado en soporte software.

6. Tras unos segundos, e abrirá **Acceso a Llaveros** mostrando su nuevo certificado personal en la categoría *Certificados* del llavero *inicio de sesión*.

7. Cierre Acceso a Llaveros y vuelva a su navegador Safari. APSC le confirmará que su certificado ha sido generado correctamente. Cierre **todas** las ventanas de su navegador web para reiniciarlo.

Finalmente, le recordamos que si desea disponer de una copia en fichero (extensión .pfx o .p12) de su nuevo certificado personal, puede obtenerla siguiendo las instrucciones de: http://www.accv.es/fileadmin/Archivos/manuales_sw/mac_exporta_sf_c.pdf

▸ INTERNET EXPLORER 11 Y EDGE

⚠ En este caso, **usted debe disponer de una versión de Java** instalada en su equipo y accesible desde su navegador web. Puede verificar esta circunstancia en el siguiente enlace: http://java.com/es/download/installed.jsp

5. En la siguiente pantalla pulse sobre el botón **Launch** para descargar y ejecutar la aplicación Java que le permitirá generar su nuevo certificado.

⚠ Es posible que en este punto su navegador web le pregunte qué programa desea utilizar para ejecutar la aplicación Java que está descargando. Deberá escoger la opción relativa a **Java Web Start**.

⚠ Al mismo tiempo, algunos navegadores web no están configurados para ejecutar directamente aplicaciones Java como la que se descarga en este punto. Deberá en ese caso descargarla primero a su equipo, para luego ejecutarla haciendo doble clic sobre ella. La aplicación se denomina *generacionRenovacion.jnlp*

⚠ Es posible que al pulsar sobre **Launch** obtenga diferentes mensajes de seguridad originados por su navegador web y/o por Java en los que se pedirá su confirmación para continuar. Deberá presionar en **Aceptar**, **Continuar, Instalar** y/o **Ejecutar** según corresponda.

6. Se abrirá la aplicación *Generar certificado en fichero* pidiéndole el PIN que protegerá el fichero que va ha generar y que contendrá su certificado y claves.

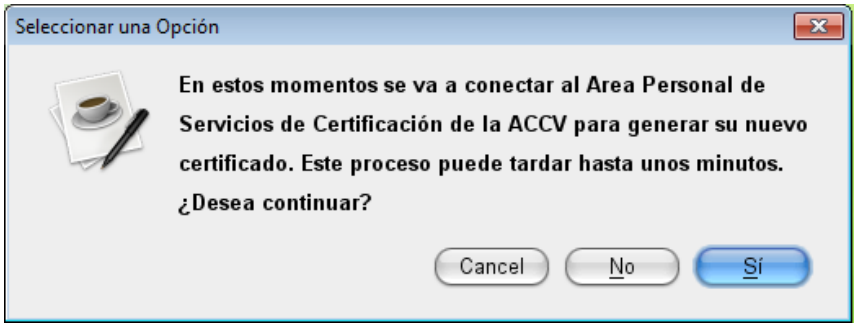
El **PIN**: no es más que una contraseña que debe definir y recordar usted. para hacer uso del certificado en fichero.

Deberá tener **6 caracteres.** Le recomendamos que elija una contraseña que contenga letras mayúsculas, minúsculas, números y símbolos como +, -, =, *, ", !, etc.

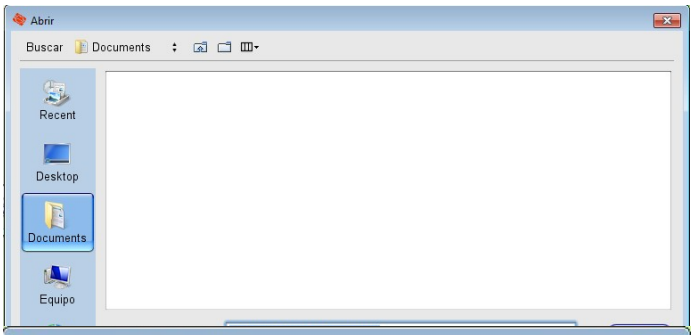
Escriba el PIN en la primera casilla, repítalo en la segunda casilla para

confirmarlo y pulse el botón **Generar certificado**.

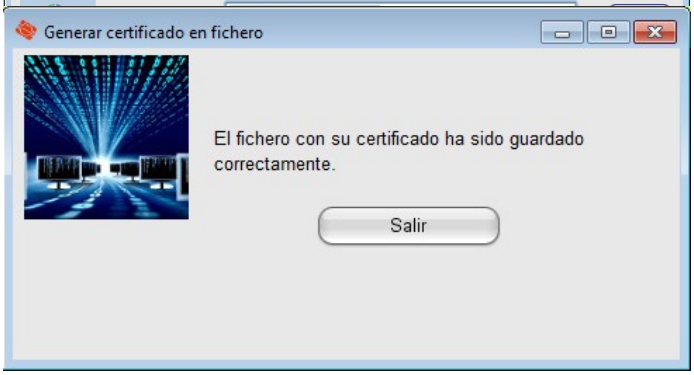
7. La aplicación le pedirá confirmación para generar su certificado. Responda **Sí**.



8. Tras unos minutos de espera, se le mostrará una ventana del sistema donde deberá **escoger la ubicación** en su equipo donde desea guardar el fichero que albergarán su nuevo certificado y claves asociadas. Por ejemplo, el *Escritorio*.



9. Finalizada la operación, observará el siguiente mensaje confirmándole que se ha generado correctamente en la ubicación que ha indicado el fichero acabado en **_firma.p12**.



Pulse **Salir**.

El fichero acabado en **_firma.p12** contiene su certificado y claves para su identificación a través de Internet y la firma electrónica de documentos.

SÓLO en el caso de que el certificado que esté usted obteniendo siguiendo estas instrucciones sea de Ciudadano, dispondrá de un segundo fichero en la ubicación seleccionada. Se trata de un fichero de nombre acabado en **_cifrado.p12** que contiene su certificado y claves para el cifrado de información. Es un fichero para usuarios con conocimientos avanzados, por lo que sólo se recomienda su uso por personas que conozcan o se hayan informado sobre las bases del cifrado asimétrico.

Le recomendamos que guarde una copia de respaldo del fichero o ficheros generados en un dispositivo externo como una memoria USB ó CD-ROM.

10. Completado el proceso de generación, cierre **todas** las ventanas de su navegador web para reiniciarlo.

Finalmente, cierre todas la para poder emplear su certificado y claves con su navegador web, deberá tomar el fichero acabado en **_firma.p12** y registrarlo previamente siguiendo las indicaciones de la guía correspondiente del siguiente enlace: https://www.accv.es/ayuda/cert-sw/instalar-fichero/