



En este manual de usuario se detalla cómo acceder al *Área Personal de Servicios de Certificación* (APSC), qué requisitos son necesarios y qué pasos debe seguir para obtener un certificado de Representante de Entidad en soporte software emitido por la ACCV.

ÍNDICE

1. REQUISITOS PREVIOS
2. PASOS A SEGUIR

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 de DNle.

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/>
- **DNle** emitido por el Cuerpo Nacional de Policía:
https://www.dnielectronico.es/PortalDNle/PRF1_Cons02.action?pag=REF_320

Cualquier duda o consulta relativa a la instalación de su DNle debe remitirla a su Servicio de Atención al Ciudadano. Dispone de más información al respecto en el siguiente enlace:
https://www.dnielectronico.es/PortalDNle/PRF1_Cons02.action?pag=REF_2110

En caso de duda o consulta relativa a APSC o a certificados emitidos por la ACCV contacte con nosotros a través de <http://www.accv.es/contacta/> o del número **963 866 014**.

CONTRATACIÓN PREVIA

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 condiciones:

- 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. Para más información consulte www.accv.es

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

2. PASOS A SEGUIR

1. Una vez ha verificado que cumple con los requisitos previos, acceda a APSC con uno de los certificados admitidos y del que sea titular. La dirección es la siguiente:

<https://apsc.accv.es/apsc/>

En el menú de la página principal pulse sobre el botón **Obtener CERT. REPRESENTANTE**.




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.

Certificados de representante de entidad en soporte software Página principal >

A continuación se muestra la información de los certificados de representante que puede generar. Pulse en el botón de cada uno de ellos para iniciar su proceso de generación.



Certificado de representante de entidad en soporte software
CIF entidad:
Nombre entidad:
GENERAR

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

Elija uno de los siguientes soportes. Pasando el ratón sobre cada opción obtendrá ayuda de cada tipo de soporte.

Software HSM

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

Sección 2 - Fecha
Fecha: 11-02-2015

Sección 3 - Condiciones de utilización de los certificados

He leído el contrato y acepto las condiciones del mismo

Volver **Continuar**

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](#).

CÓMO SOLICITAR AYUDA

En caso de duda o consulta relativa a esta guía, puede consultar el manual completo de APSC en: <https://www.accv.es/servicios/apsc/>

También puede contactar con nosotros a través del teléfono **963 866 014** o del formulario de atención (<http://www.accv.es/contacta/>).

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"...

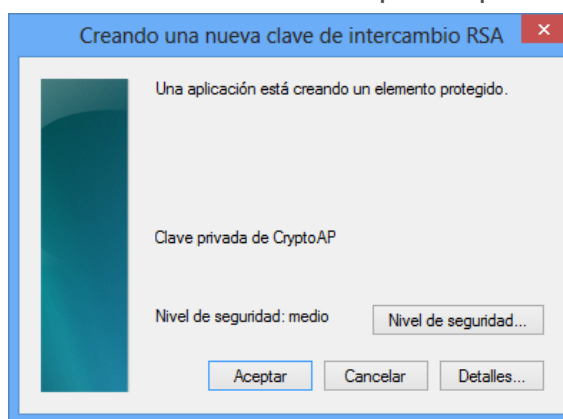
En ese caso pulse sobre la franja amarilla con el botón derecho del ratón, **Ejecutar** (debe disponer de permisos de administrador).

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...**

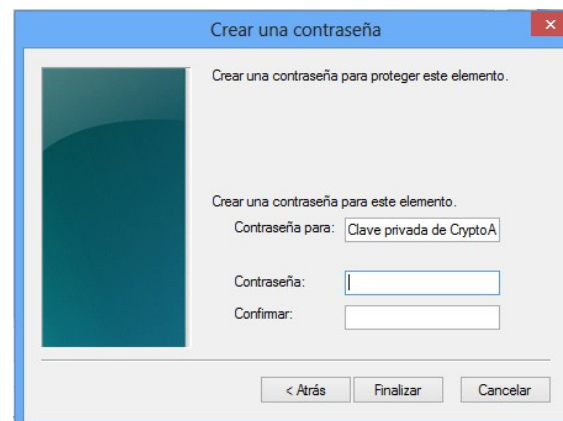
Marque la opción **Alto** y pulse el botón **Siguiente**.



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**.

Elija el PIN que le permitirá utilizar su certificado.

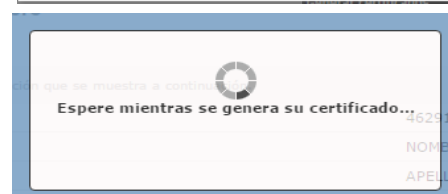
PIN(*):

Repita PIN:

(*) Por motivos de seguridad el PIN deberá contener entre 10 y 20 caracteres conteniendo obligatoriamente tanto números como letras. Se aconseja incluir mayúsculas y minúsculas así como algunos caracteres especiales.

Cerrar 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.

Generación del certificado digital en fichero

Su certificado ha sido generado. Pinche en el botón 'Descargar' para obtener el fichero. Pinche en el botón 'Ver PIN' para obtener el PIN que le permitirá abrir e instalar el certificado contenido en el fichero.

Su certificado: **Descargar** >>

PIN: **Ver PIN** >>

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, se 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 a generar y que contendrá su certificado y claves.

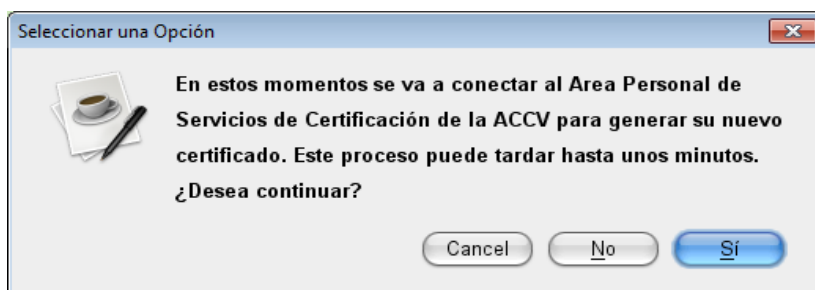
El **PIN**: no es más que una contraseña que debe definir y recordar usted. para hacer uso del certificado en fichero.



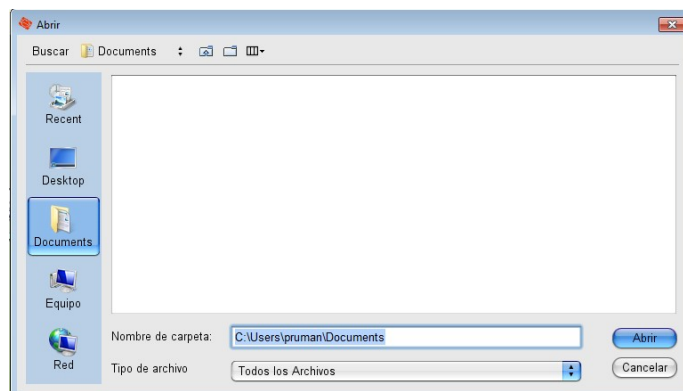
Deberá tener **6 caracteres**. Le recomendamos que elija una contraseña que contenga letras mayúsculas, minúsculas, números y símbolos como +, -, =, *, ", !, etc.

Escriba el PIN en la primera casilla, repítalo en la segunda casilla para confirmarlo y pulse el botón **Generar certificado**.

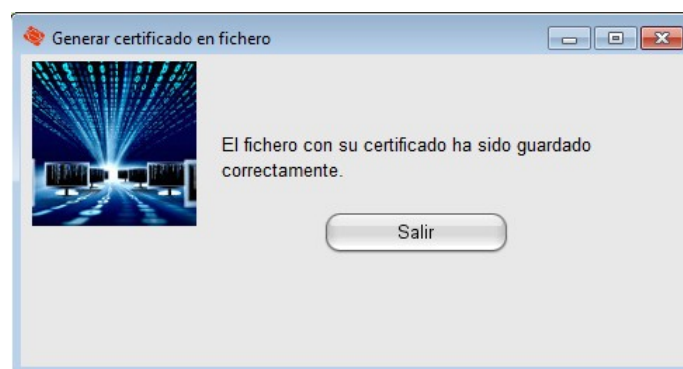
7. La aplicación le pedirá confirmación para generar su certificado. Responda **Sí**.



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/>