

INSTRUCCIONS DE TELETREBALL DES D'EQUIPS INFORMÀTICS DOMÈSTICS

Contenido

1.- Instruccions generals	1
2.- Recomanacions de seguretat per a l'equip informàtic domèstic.	2
Annex I: Certificat digital per a l'accés a la VPN	4
Annex II: Instruccions d'Accés remot des del equip domèstic a l'ordinadors de l'oficina en l'Administració de Justícia (escriptori remot)	5
Annex III: Instal·lar Aplicacions de tercers en Mac	13
Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software.....	14
INSTAL·LACIÓ DE CERTIFICAT DIGITAL EN FITXER: Internet Explorer y Chrome	15

1.- Instruccions generals

La DGTIC, té establert, en el seu àmbit d'actuació, un conjunt d'utilitats i mesures tècniques que permeten exercir les seues tasques en la modalitat de teletreball per al personal públic de la Generalitat.

Abans de res cal recordar que solament amb tindre accés a Internet, des de qualsevol dispositiu, sense res addicional, és possible llegir i contestar correus electrònics, accedir als serveis que la Generalitat ofereix com a públics o usar serveis de videoconferència corporatius.

Per a ampliar les funcionalitats de teletreball i poder accedir a altres recursos corporatius, com les carpetes compartides o aplicacions específiques, es requereix l'ús d'una **connexió segura**. Aquestes connexions segures es basen en una plataforma de Xarxa Privada Virtual (**VPN** en les seues sigles en anglés) que proporciona un canal segur perquè els equips informàtics (ordinador personal i/portàtil) es puguin connectar a la xarxa de l'Administració de Justícia de la Comunitat Valenciana des de qualsevol lloc amb connexió a Internet.

Una vegada connectat a aqueixa xarxa privada segura, qualsevol usuari pot accedir al seu equip habitual de treball (facilitat anomenada '*escriptori remot*'), de manera que pot treballar amb l'equip informàtic utilitzat en l'oficina amb totes les aplicacions i recursos que utilitza normalment des del seu propi ordinador personal o domèstic.

Perquè siga possible aquesta connexió, **l'equip informàtic domèstic ha de disposar de:**

- **Connexió a Internet**, via cable o wifi segura xifrada
- **Sistema operatiu Windows o Mac amb suport del fabricant**
- **Hauran tindre instal·lat un antivirus, ja siga gratuït o de pagament, que garantisca les actualitzacions de seguretat** adquirit de manera legítima.
- Estar degudament **actualitzat**, almenys haver instal·lat totes les **actualitzacions de seguretat**.
- Disposar d'un **certificat digital** instal·lat en l'equip, veure [l'Annex I: Certificat digital per a l'accés a la VPN](#)

Mètode d'accés des de l'equip informàtic domèstic

Per a accedir en remot a l'escriptori del seu equip de treball:

- Obrir el navegador (Chrome, Firefox o Internet Explorer),
- Escriure l'adreça d'accés: <https://vpn.gva.es/remotojusticia> i seguir les instruccions guiades de [l'Annex II: Instruccions d'Accés remot des d'equip domèstic a l'ordinador de l'oficina en l'Administració de Justícia](#)

Davant possibles incidències telefonar a 963 985300 o 963 866011 (CAU-TIC)

2.- Recomanacions de seguretat per a l'equip informàtic domèstic.

Quan un usuari es connecte des del seu equip informàtic domèstic ha de continuar observant les mesures de seguretat definides en l'Ordre d'Ús Segur de Mitjans Tecnològics.

Almenys haurà d'observar les següents normes d'ús:

- Com a norma general, extremerà les precaucions ja que no es disposa de moltes de les mesures de seguretat que aporta treballar des del centre de treball habitual. Ha de romandre en alerta, especialment durant l'ús d'internet i en rebre correus que li semblen sospitosos.
- Durant la jornada laboral cal intentar evitar l'ús personal que se li suposa al seu equip domèstic. Durant la jornada laboral ha d'utilitzar-ho exclusivament per a tasques directament relacionades amb l'acompliment de labors professionals, ha d'evitar-se l'ús personal com poden ser les compres, la missatgeria personal, les xarxes socials o les activitats d'oci.
- Ha d'evitar la descàrrega d'informació i fitxers en el seu propi equip. I si ha de fer-ho, esborre'ls condisc haja finalitzat el seu treball amb ells.
- Intente no connectar memòries USB durant la jornada laboral, per ser un possible focus d'infeccions per *malware*.

Com s'ha comentat anteriorment, els sistemes operatius permesos per a establir la connexió amb la xarxa de la GVA són aquells que disposen de suport oficial i, per tant, disposen de totes les actualitzacions de seguretat.

En cas de detectar un comportament estrany de l'equip o sospitar d'una possible infecció, fugida d'informació o incident de seguretat, ha de comunicar-se amb els telèfons indicats en el punt anterior.

Annex I: Certificat digital per a l'accés a la VPN

És necessari disposar d'un certificat digital emés per la ACCV o el DNI electrònic per a connectar-se a través de la VPN habilitada per la GVA per al teletreball. Els casos que poden donar-se són:

- Certificat empleat públic de la ACCV en suport targeta:
 - Si té lector a la seua casa, pot accedir amb el certificat en el lector connectat a l'ordinador domèstic sense necessitat de fer cap altra acció. En el cas que necessite utilitzar el portafirmes i vulga utilitzar un certificat diferent per a signar, per exemple el certificat de pseudònim de FNMT, necessitarà descarregar i instal·lar-se el certificat software segons s'indica en [l'Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#)
 - Si no té lector a la seua casa, des del seu lloc de treball en la seu judicial haurà d'accedir a la pàgina de la ACCV (<https://www.accv.es>) i descarregar-se el certificat software segons s'indica en [l'Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#) portar-li-ho a casa en un pendrive o enviar-ho per correu electrònic i instal·lar-ho segons s'indica en l'annex V esmentat.
- DNI-e:
 - Si té lector a la seua casa pot accedir amb el DNI-e en el lector connectat a l'ordinador domèstic sense necessitat de fer cap altra acció. En aquest cas ha de tindre en compte que si necessita utilitzar el portafirmes i vol utilitzar un certificat diferent al DNI-e necessitarà descarregar i instal·lar-se el certificat software segons s'indica en [l'Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#) , i d'aqueixa forma deixar lliure el lector de targeta de l'ordinador domèstic per a poder utilitzar-lo per al certificat a l'hora de signar.
 - Si no té lector a casa, podrà fer la descàrrega del certificat software des del lloc de treball en la seu judicial segons s'indica en [l'Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#)
- No té certificat de la *ACCV ni DNI-e:

En aquest cas ha d'acudir a un Punt de Registre d'Usuari de la ACCV (punt *PRU) per a obtenir un **certificat digital de Ciutadà en suport software**. Aquest certificat és gratuït. Pot trobar més informació d'aquesta mena de certificat i com obtindre'l en <https://www.accv.es/certificados/ciudadano-software/>

Respecte als punts PRU, pot consultar les adreces i telèfons de tots els PRU de la ACCV en <https://www.accv.es/encuentra-tu-pru/> . Haurà de cridar al PRU on desitge anar per a confirmar que està donant servei i agafar cita prèvia en el cas de ser necessària.

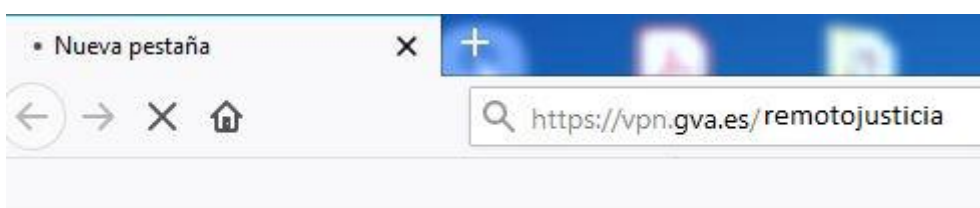
Una vegada tinga el certificat, haurà d'instal·lar-li'l en l'ordinador domèstic seguint les instruccions de [l'Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#)

Annex II: Instruccions d'Accés remot des del equip domèstic a l'ordinadors de l'oficina en l'Administració de Justícia (escriptori remot)

Les següents instruccions expliquen com accedir a l'ordinador de l'oficina des del seu ordinador domèstic.

Com a requisit previ, el certificat digital haurà d'estar instal·lat en l'equip d'acord amb el [Annex I: Certificat digital per a l'accés a la VPN](#)

En primer lloc cal obrir el navegador (Chrome, Firefox o Internet Explorer) i escriure la URL d'accés: <https://vpn.gva.es/remotojusticia>.



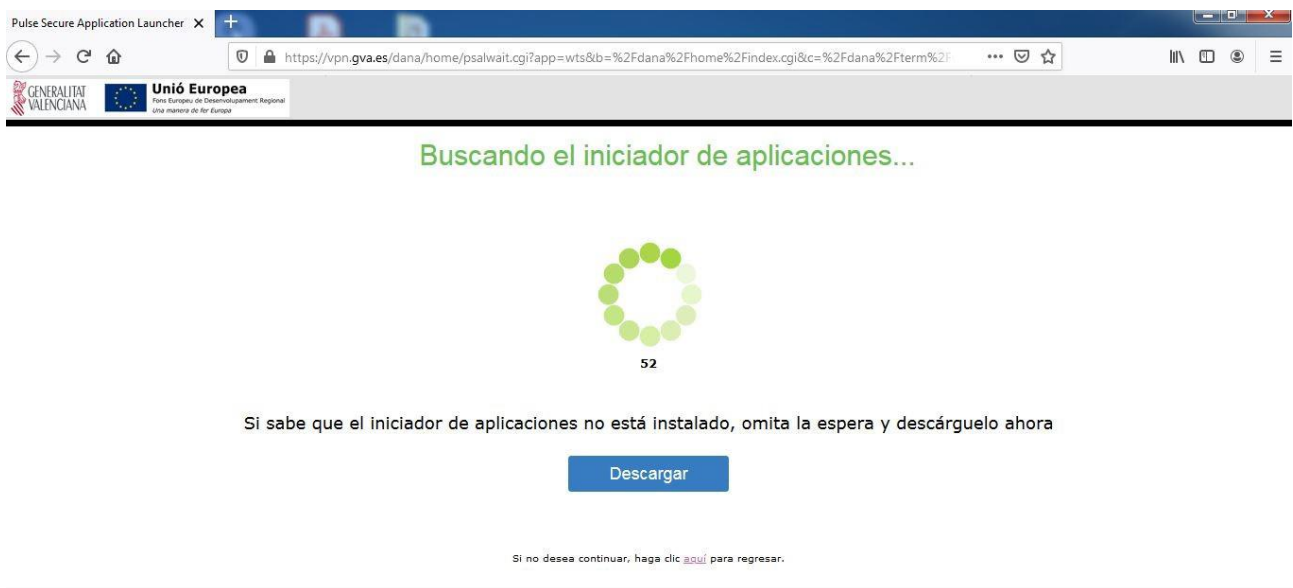
El navegador sol·licitarà l'autenticació amb el certificat digital. Triem el certificat i premem sobre "Acceptar".



A continuació apareixerà la pàgina de connexió a l'ordinador de sobretaula del seu lloc de treball



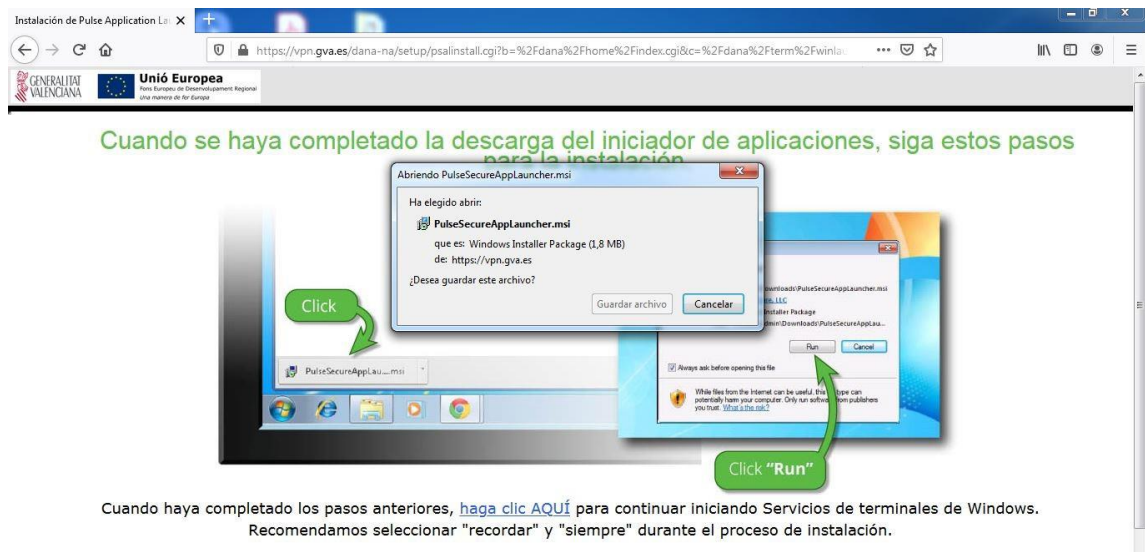
Cal prémer sobre l'enllaç “**Accés Remot *PCNNNNNNN.justicia.gva.es**”, apareixerà la següent pantalla:



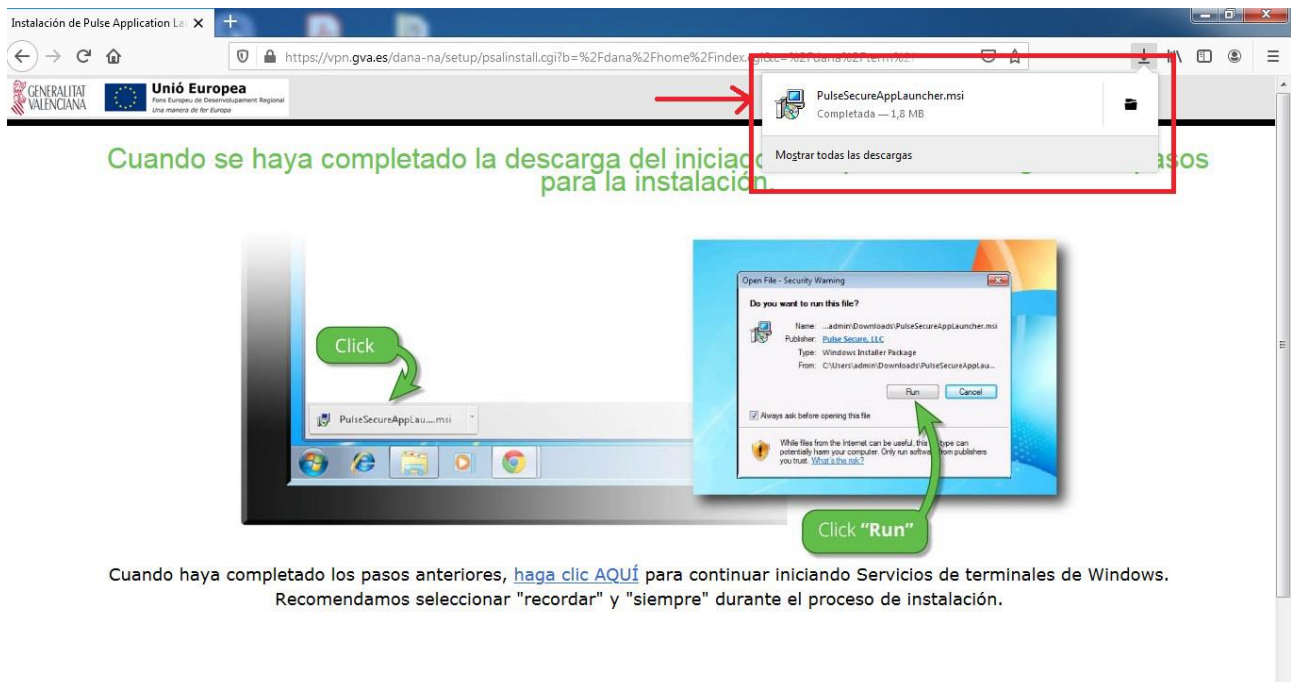
NOTA: en cas d'utilitzar un ordinador Mac per a fer la connexió remota, [en l'Annex III: INSTAL·LAR APLICACIONS DE TERCERS EN MAC](#), trobarà indicacions per a permetre la instal·lació del Plugin de Java per a Pulse en aquests ordinadors

La primera vegada que connectem, l'equip sol·licitarà la instal·lació de dos components.
El primer:

Prement sobre el botó blau que indica “**Descarregar**”, descarregarem un fitxer denominat “***PulseSecureAppLauncher.*msi**”



Després de la descàrrega hem d'executar aquest programa:



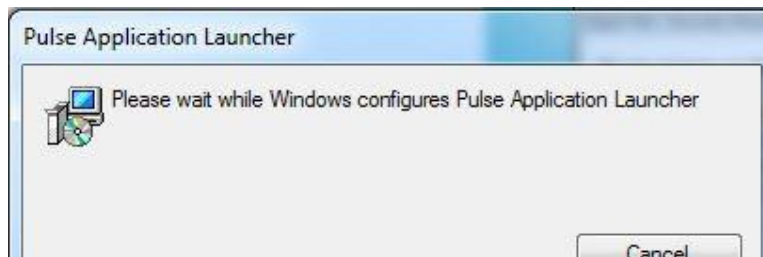
Si l'equip ens demana permís per a executar aquest component, premem sobre **"Aceptar"**:



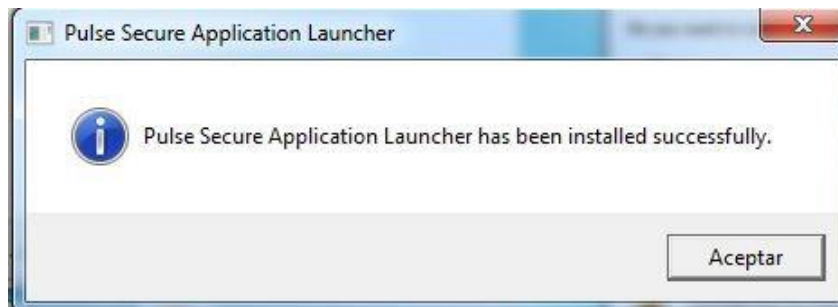
I posteriorment a **"Ejecutar"**:



Després d'això començarà la instal·lació del component **“Pulse Application Launcher”**:

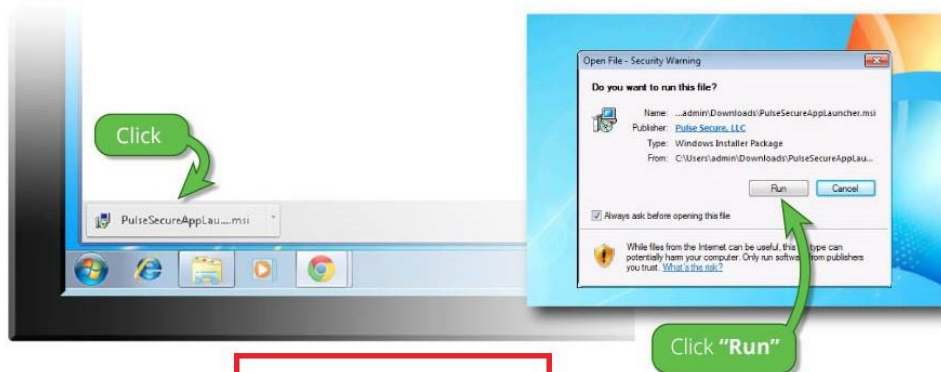


Una vegada finalitzada la instal·lació apareixerà el següent missatge. Premem **“Aceptar”**:



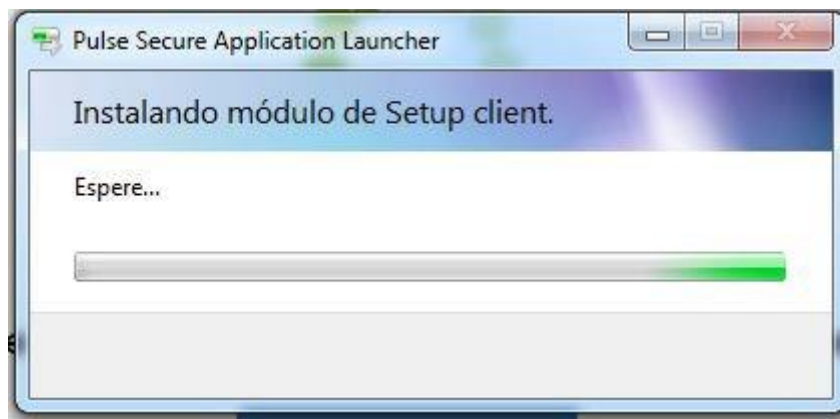
Ja està instal·lat el **primer component**.

Ara Premem sobre **“haga clic AQUI”** per a continuar amb la instal·lació del **segon component**:

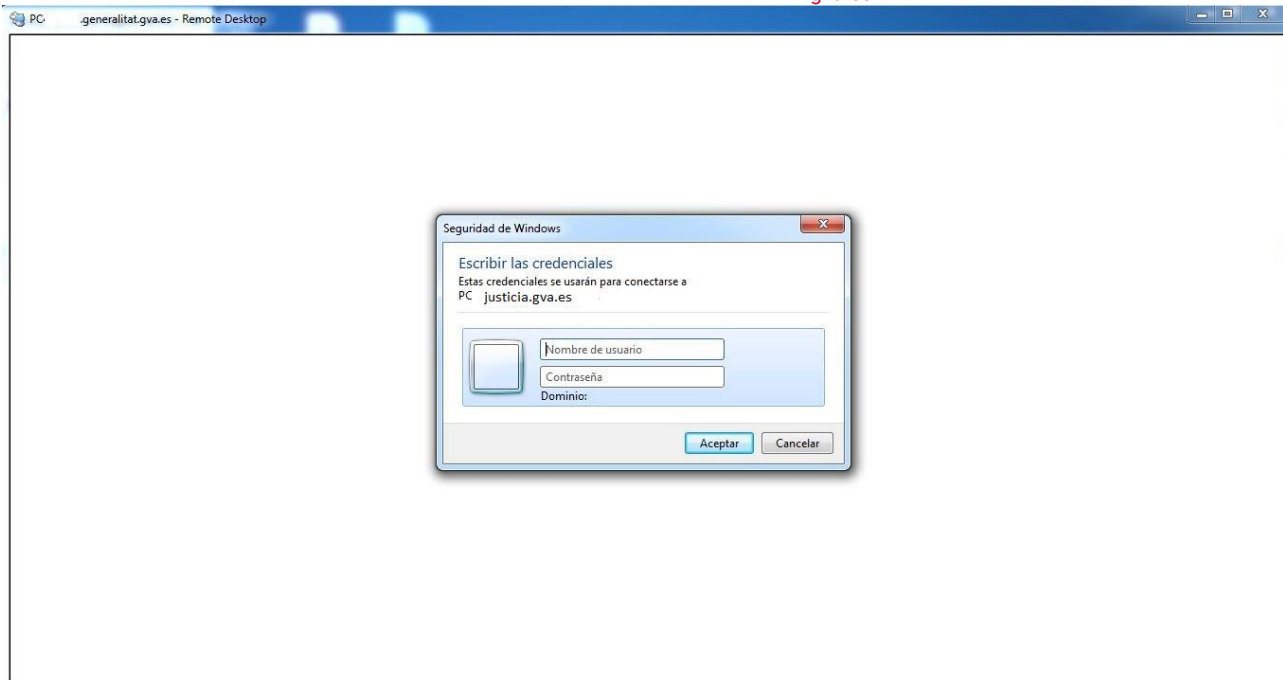


Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando Servicios de terminales de Windows. Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

Automàticament començarà la instal·lació del **segon component** necessari per a la connexió remota:



Després de finalitzar la instal·lació, l'equip d'oficina sol·licitarà les credencials d'accés, és a dir el nom d'usuari i la contrasenya del domini **JUSTICIA**:



IMPORTANT: en el camp “Nombre de usuario” , al seu usuari ha d'anteposar sense espais **JUSTICIA**

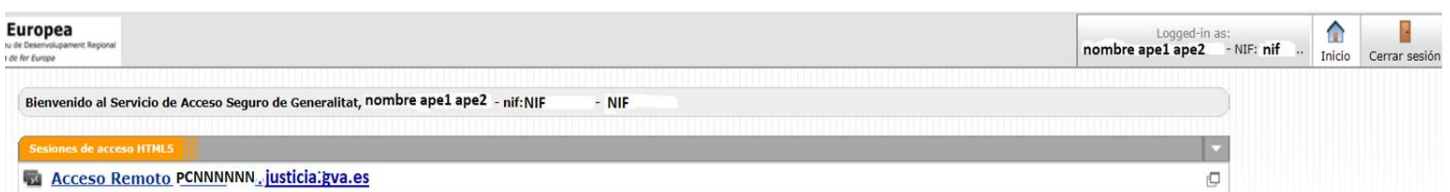
La contrasenya d'accés al seu lloc de treball **NO ÉS EL PIN de la targeta criptogràfica** amb què vosté accedeix al seu equip habitualment de manera presencial. La contrasenya que li demana ací és la que està vinculada a l'usuari. Si vosté normalment utilitzada només la targeta criptogràfica per a accedir al seu lloc de treball haurà rebut un correu amb la contrasenya que haurà d'utilitzar la primera vegada que accedisca. Quan inicié sessió la primera vegada en l'ordinador del treball li sol·licitarà que la canvie.

Després d'introduir aquestes credencials, s'obrirà l'entorn de treball de l'equip d'oficina.

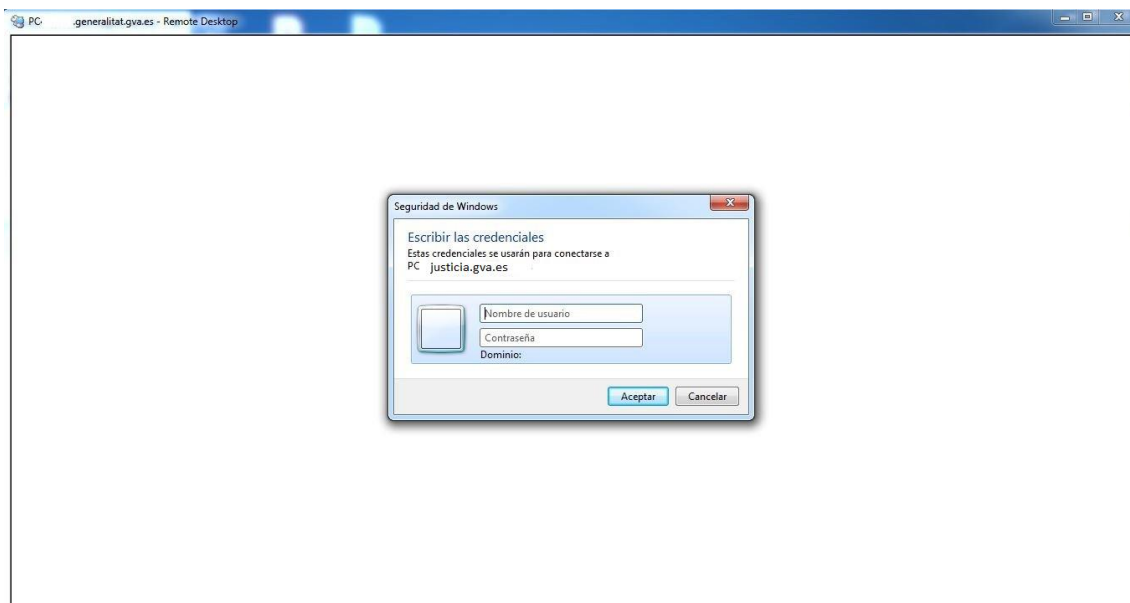
El procediment anterior caldrà realitzar-lo solament la primera vegada.

Les següents vegades que connectem, bastarà escriure en el navegador la URL d'accés:
<https://vpn.gva.es/remotojusticia>.

Apareixerà la pantalla amb l'enllaç al lloc de treball:



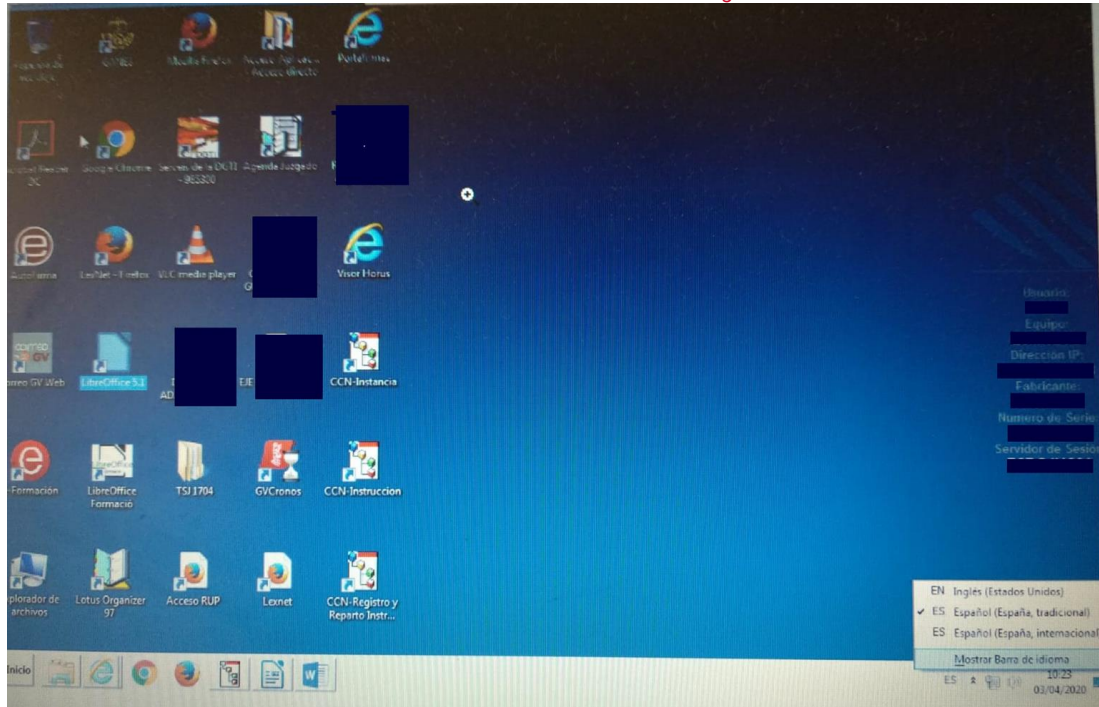
Després de prémer en l'enllaç ens sol·licitarà les credencials del domini. En introduir-les, accedirem a l'equip d'oficina:



Com s'ha indicat anteriorment en “Nombre de usuario” ha de posar el seu usuari anteposant **JUSTICIA**

Després d'això, accedirà a l'ordinador de sobretaula del seu lloc de treball de l'Administració de Justícia.

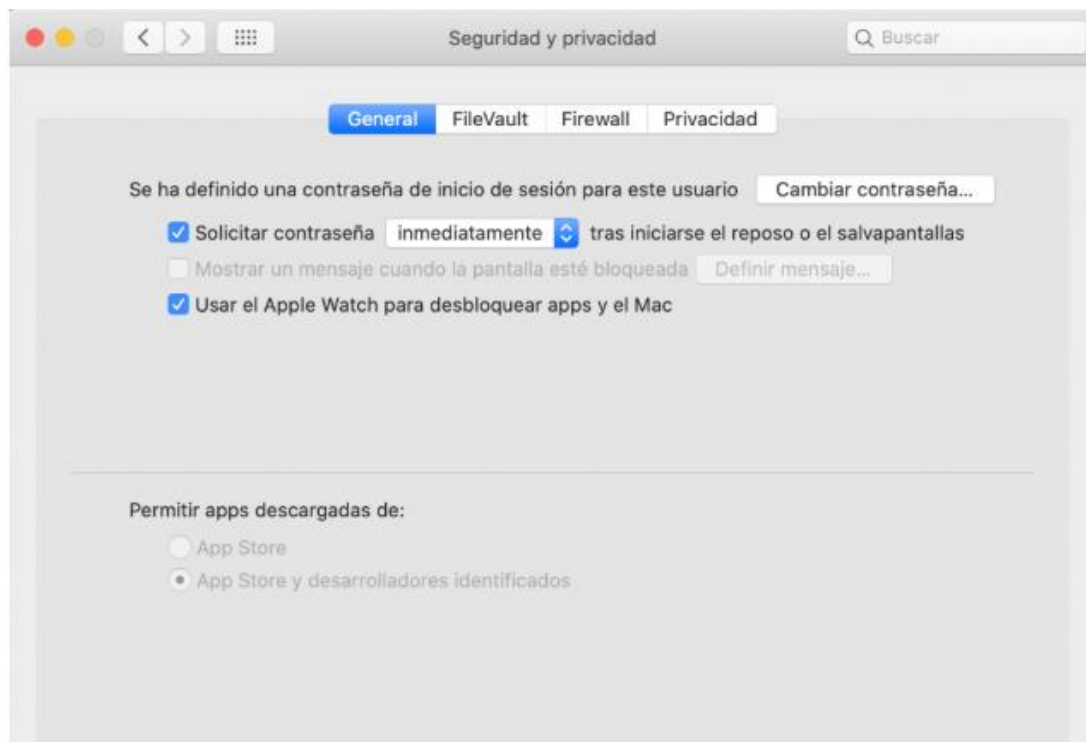
En ocasions en accedir a l'ordinador de l'oficina es canvia l'idioma del teclat. Per a posar el teclat una altra vegada en espanyol, en la barra de Windows, a la cantonada inferior dreta, estant el ratolí sobre el símbol de l'idioma, al pulsar el botó dret del ratolí es desplega un menú i cal marcar Español.



Per a acabar la sessió, prema sobre la icona de la  porta  , en la part superior dreta de la pantalla.

Annex III: Instal·lar Aplicacions de tercers en Mac

1. Anar a Preferències del Sistema>Seguritat y Privacitat
2. Prémer sobre el cadenat que apareix en la part inferior esquerra i introduir la contrasenya que utilitza per a desbloquejar el seu Mac.
3. En la part on posa «Permitir apps de tercers» s'haurà de marcar la casella de «App Store y desarrolladores identificados».



En la majoria d'ocasions eixirà una finestra emergent en la qual s'alerta que s'està instal·lant programari desconegut, cal acceptar per a continuar. També es pot donar el cas que, novament, calga acudir a l'apartat de “Seguridad y Privacidad”. En aquesta ocasió seria per a acceptar la instal·lació d'aqueixa aplicació en concret.

Annex IV: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software

Consideracions prèvies:

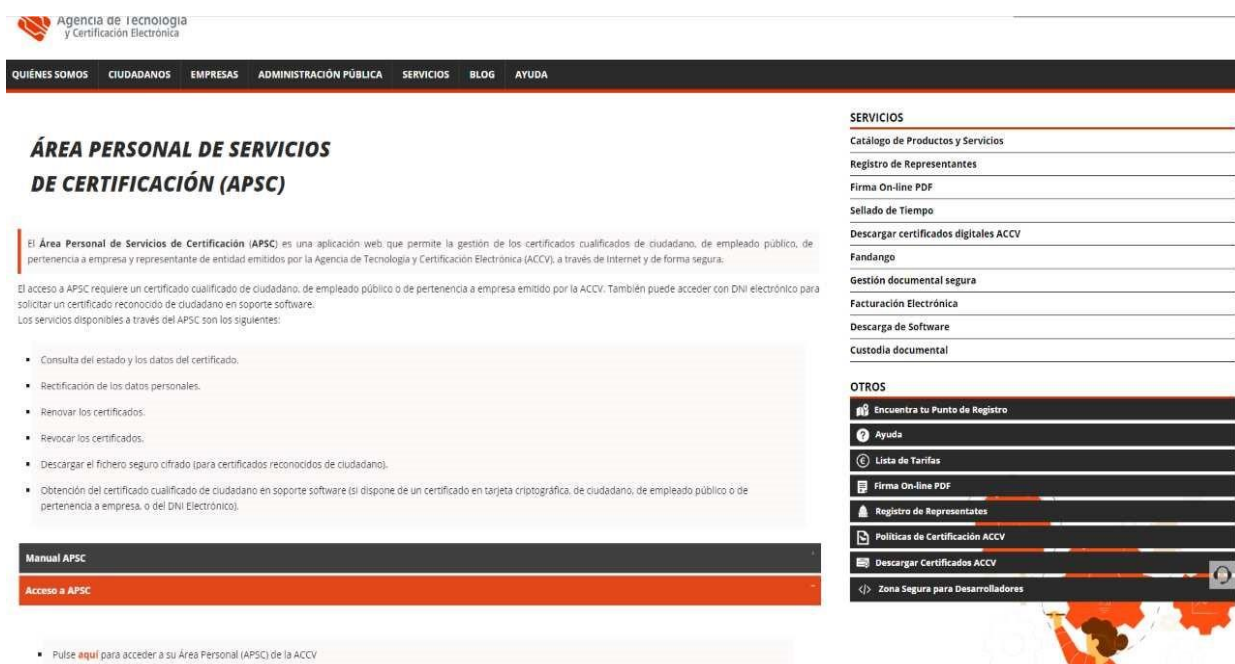
Certificats vàlids per descarregar i descarregar el certificat ACCV en software:

- Targeta criptogràfica ACCV
- DNIE

Si teniu un lector i necessiteu descarregar el certificat ACCV a SW, podeu fer-ho tal com es descriu a continuació. Si no té un lector a la seva adreça de casa, ha de descarregar des del lloc de treball a la seva seu central, i una vegada descarregat (registre a un USB, enviar-lo per correu) al PC d'ús a casa per instal·lar-lo.

Procediment a seguir:

Accedint al web <https://www.accv.es/va/servicis/apsc/> es troba l'accés a l'Àrea Personal de Serveis de Certificació (APSC) i un manual més ampliat d'Usuari.



Agencia de Tecnología y Certificación Electrónica

QUIÉNES SOMOS CIUDADANOS EMPRESAS ADMINISTRACIÓN PÚBLICA SERVICIOS BLOG AYUDA

ÁREA PERSONAL DE SERVICIOS DE CERTIFICACIÓN (APSC)

El Área Personal de Servicios de Certificación (APSC) es una aplicación web que permite la gestión de los certificados cualificados de ciudadano, de empleado público, de pertenencia a empresa y representante de entidad emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV), a través de Internet y de forma segura.

El acceso a APSC requiere un certificado cualificado de ciudadano, de empleado público o de pertenencia a empresa emitido por la ACCV. También puede acceder con DNI electrónico para solicitar un certificado reconocido de ciudadano en soporte software.

Los servicios disponibles a través del APSC son los siguientes:

- Consulta del estado y los datos del certificado.
- Rectificación de los datos personales.
- Renovar los certificados.
- Revocar los certificados.
- Descargar el fichero seguro cifrado (para certificados reconocidos de ciudadano).
- Obtención del certificado cualificado de ciudadano en soporte software (si dispone de un certificado en tarjeta criptográfica, de ciudadano, de empleado público o de pertenencia a empresa, o del DNI Electrónico).

Manual APSC

Acceso a APSC

■ Pulse [aquí](#) para acceder a su Área Personal (APSC) de la ACCV

SERVICIOS

- Catálogo de Productos y Servicios
- Registro de Representantes
- Firma On-line PDF
- Sellado de Tiempo
- Descargar certificados digitales ACCV
- Fandango
- Gestión documental segura
- Facturación Electrónica
- Descarga de Software
- Custodia documental

OTROS

- Encuentra tu Punto de Registro
- Ayuda
- Lista de Tarifas
- Firma On-line PDF
- Registro de Representantes
- Políticas de Certificación ACCV
- Descargar Certificados ACCV
- Zona Segura para Desarrolladores

En entrar al APSC amb la seua targeta criptogràfica en l'equip veurà l'opció per a obtindre el seu certificat qualificat de ciutadà en suport software.

DESCARREGAR UNA CÒPIA DEL SEU CERTIFICAT I CLAUS DE XIFRAT EN FITXER

Els passos a seguir per a descarregar una còpia d'un dels seus certificats de xifrat i claus associades són:

1. Prema en el menú **El seu CERTIFICAT DE XIFRAT** de la pàgina principal de ASPC.
2. La següent pantalla li mostrarà una llista amb els seus certificats de xifrat, amb la data de caducitat, el compte de correu-e associada i l'estat de cadascun (actiu o revocat)



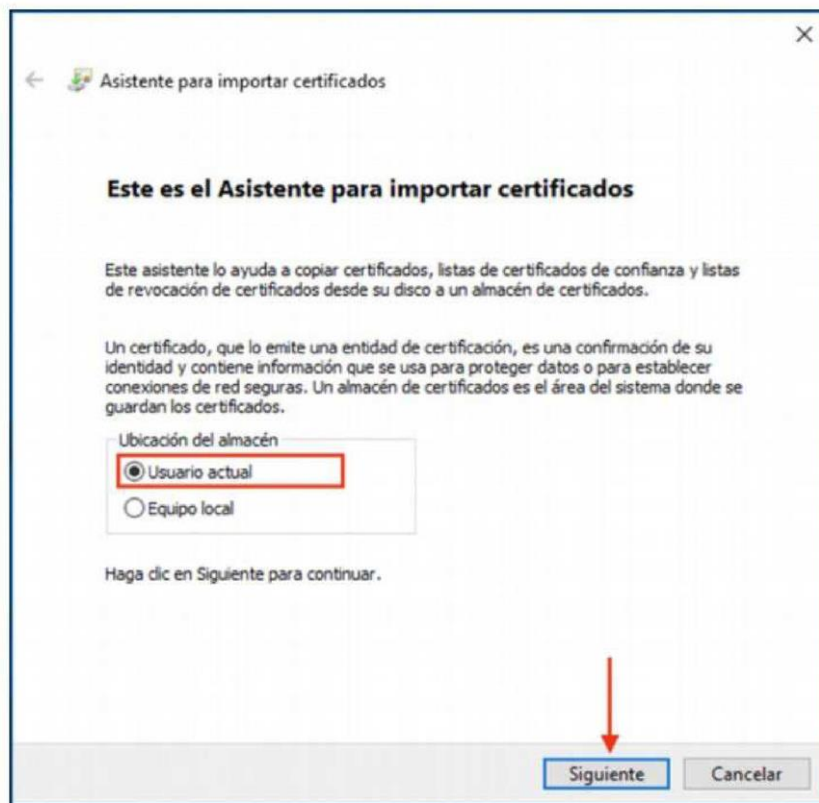
3. Seleccione el botó **Descarregar** associat a aquell dels seus certificats de xifrat a obtindre.
4. Si el seu navegador web és possible que li pregunte sobre on desitja guardar en el seu equip el fitxer amb el certificat de xifrat seleccionat i els seus claus associades. Si és així seleccione la ubicació desitjada i guarde-ho. En cas contrari, el seu navegador web guardarà el fitxer en la carpeta per defecte per a les descàrregues.

***** Si no té un lector de targetes a casa seva, serà aquest arxiu descarregat que necessitarà prendre per instal·lar-lo (Enregistri a USB, envii-li per correu) * * ***

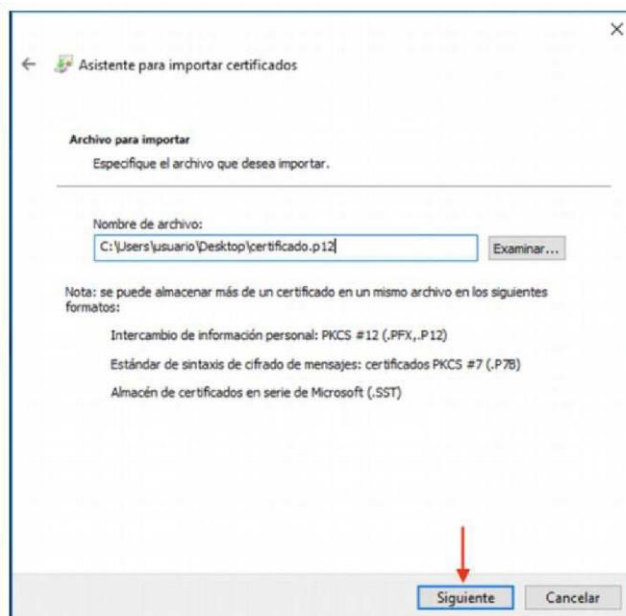
5. Finalment, faça clic en el botó **Veure** associat al certificat de xifrat que acaba de descarregar per a visualitzar la contrasenya/PIN que se li demanarà cada vegada que desitge accedir al contingut del fitxer que acaba de descarregar. Haurà d'anotar o imprimir aquesta contrasenya/PIN i guardar-la per a poder utilitzar-la amb el fitxer que acaba de descarregar

INSTAL·LACIÓ DE CERTIFICAT DIGITAL EN FITXER: Internet Explorer y Chrome

Faça **double-click** sobre el fitxer .p12 o .*pfx que conté el seu certificat digital i claus. S'obrirà l'Assistent *per a la importació de certificats*. Haurà de marcar **Usuari actual**. D'aquesta manera, el certificat s'instal·larà només per a l'usuari amb el qual ha iniciat sessió. Prema **Següent**:



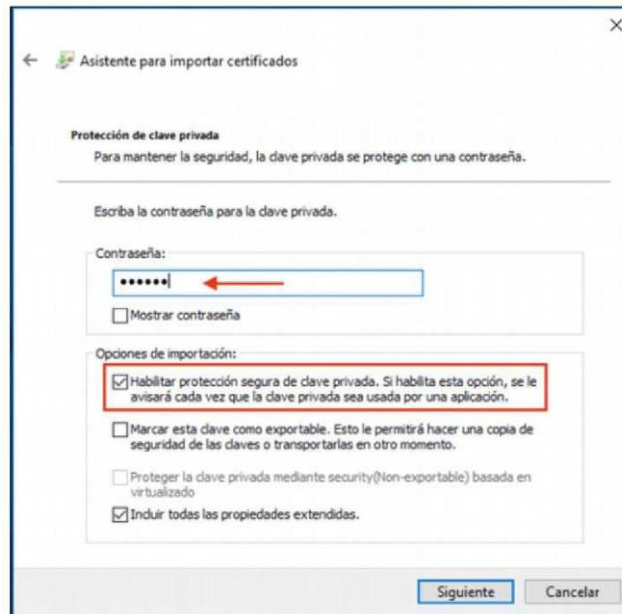
En la pantalla a continuació apareix seleccionat el seu certificat. Prema **Següent**.



En l'apartat Contrasenya ha d'introduir la seua PIN associat al certificat que està instal·lant.

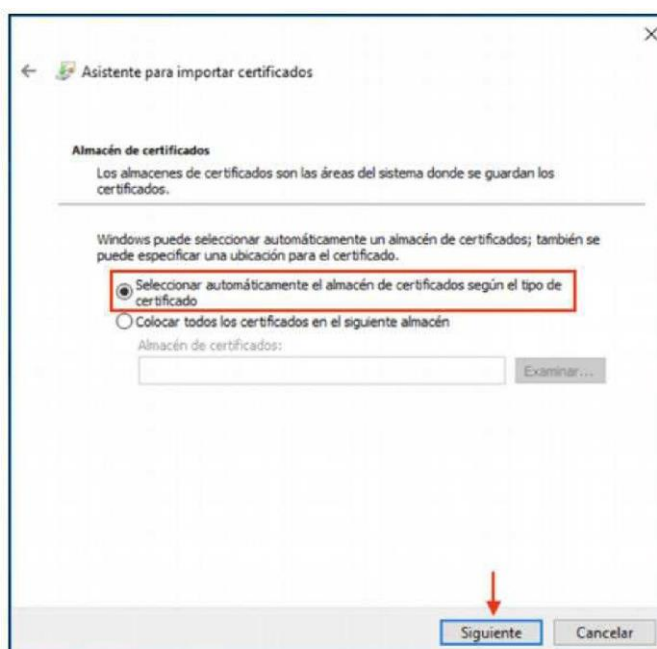
IMPORTANT: Marque l'opció Habilitar protecció segura de claus privades.

Prema **Següent**:

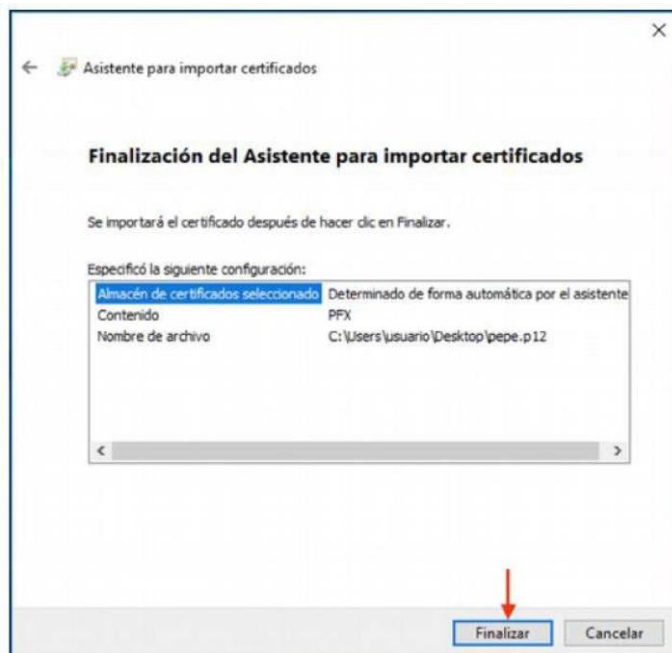


Marque l'opció Seleccionar automáticamente el magatzem de certificats segons el tipus de certificat.

Prema **Següent**.



Prema **Finalitzar**.





POSAR UNA CONTRASENYA AL CERTIFICAT (OPCIONAL)

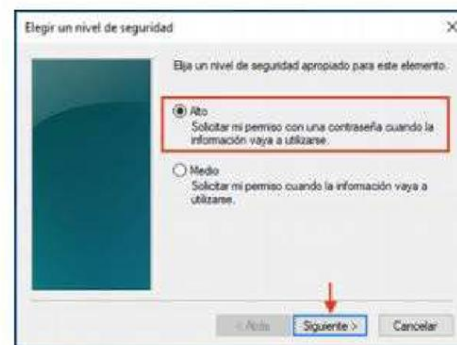
6. A continuación, tiene la opción de definir una contraseña segura que proteja el certificado que está instalando. Si la establece, ésta se le pedirá cuando vaya a emplear el certificado.

Si no quiere, pulse Aceptar para salir y finalizar la instalación sin ponerle contraseña.

Sólo si quiere establecer una contraseña segura, debe pulsar el botón **Nivel de seguridad...**

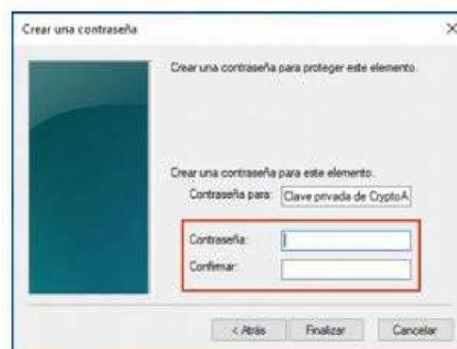


Marque la opción **Alto** y pulse el **Siguiente**.

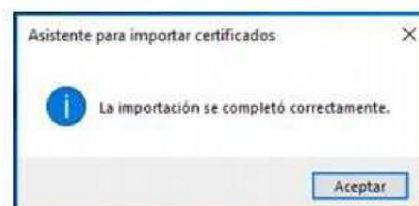


Aparecerá una ventana en la que debe introducir la nueva contraseña. Deberá elegir la **contraseña** que usted prefiera, escribirla aquí dos veces y pulsar **Finalizar**.

Por su seguridad y siempre que sea capaz de recordarla, le recomendamos que elija una contraseña de al menos 8 caracteres y que contenga letras mayúsculas, minúsculas, números y símbolos como +, -, =, *, ", !, etc.



Por último pulse **Aceptar**. El asistente le informará que la importación se completó correctamente. Entonces su certificado estará correctamente instalado y listo para ser utilizado.



INSTRUCCIONES DE TELETRABAJO DESDE EQUIPOS INFORMÁTICOS DOMÉSTICOS

Contenido

1.- Instrucciones generales	1
2.- Recomendaciones de seguridad para el equipo informático doméstico.	2
Anexo I: Certificado digital para el acceso a la VPN	4
Anexo II: Instrucciones de Acceso remoto desde el equipo doméstico al ordenador de la oficina en la Administración de Justicia (escritorio remoto)	6
Anexo III: Instalar Aplicaciones de terceros en Mac	14
Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software.....	15
Instalación del certificado en soporte software (Internet Explorer y Chrome).....	16

1.- Instrucciones generales

La DGTIC, tiene establecido, en su ámbito de actuación, un conjunto de utilidades y medidas técnicas que permiten desempeñar sus tareas en la modalidad de teletrabajo para el personal público de la Generalitat.

Antes de nada cabe recordar que solamente con tener acceso a Internet, desde cualquier dispositivo, sin nada adicional, es posible leer y contestar correos electrónicos, acceder a los servicios que la Generalitat ofrece como públicos o usar servicios de videoconferencia corporativos.

Para ampliar las funcionalidades de teletrabajo y poder acceder a otros recursos corporativos, como las carpetas compartidas o aplicaciones específicas, se requiere el uso de una **conexión segura**. Estas conexiones seguras se basan en una plataforma de Red Privada Virtual (**VPN** en sus siglas en inglés) que proporciona un canal seguro para que los equipos informáticos (ordenador personal y/portátil) se puedan conectar a la red de la Administración de Justicia de la Comunitat Valenciana desde cualquier sitio con conexión a Internet.

Una vez conectado a esa red privada segura, cualquier usuario puede acceder a su equipo habitual de trabajo (facilidad llamada '*escritorio remoto*'), de manera que puede trabajar con el equipo informático utilizado en la oficina con todas las aplicaciones y recursos que utiliza normalmente desde su propio ordenador personal o doméstico.

Para que sea posible esta conexión, **el equipo informático doméstico debe disponer de:**



- **Conexión a Internet**, vía cable o wifi segura cifrada
- **Sistema operativo Windows o Mac con soporte del fabricante**
- **Deberán tener instalado un antivirus, ya sea gratuito o de pago, que garantice las actualizaciones de seguridad** adquirido de forma legítima.
- Estar debidamente **actualizado**, al menos haber instalado todas las **actualizaciones de seguridad**.
- Disponer de un **certificado digital** instalado en el equipo, ver el [Anexo I: Certificado digital para el acceso a la VPN](#)

Método de acceso desde el equipo informático domestico

Para acceder en remoto al escritorio de su equipo de trabajo:

- Abrir el navegador (Chrome, Firefox o Internet Explorer),
- Escribir la dirección de acceso: <https://vpn.gva.es/remotojusticia> y seguir las instrucciones guiadas del [Anexo II: Instrucciones de Acceso remoto desde equipo doméstico al ordenador de la oficina en la Administración de Justicia](#)

Ante posibles incidencias llamar a 963 985300 o 963 866011 (CAU-TIC)

2.- Recomendaciones de seguridad para el equipo informático doméstico.

Cuando un usuario se conecte desde su equipo informático doméstico debe seguir observando las medidas de seguridad definidas en la Orden de Uso Seguro de Medios Tecnológicos.

Al menos deberá observar las siguientes normas de uso:

- Como norma general, extremará las precauciones ya que no se dispone de muchas de las medidas de seguridad que aporta trabajar desde el centro de trabajo habitual. Debe permanecer en alerta, especialmente durante el uso de internet y al recibir correos que le parezcan sospechosos.
- Durante la jornada laboral hay que intentar evitar el uso personal que se le supone a su equipo doméstico. Durante la jornada laboral debe utilizarlo exclusivamente para tareas directamente relacionadas con el desempeño de labores profesionales, debe evitarse el uso personal como pueden ser las compras, la mensajería personal, las redes sociales o las actividades de ocio.
- Debe evitar la descarga de información y ficheros en su propio equipo. Y si debe hacerlo, bórrelos cuando haya finalizado su trabajo con ellos.
- Intente no conectar memorias USB durante la jornada laboral, por ser un posible foco de infecciones por malware.

Como se ha comentado anteriormente, los sistemas operativos permitidos para establecer la conexión con la red de la GVA son aquellos que disponen de soporte oficial y, por lo tanto, disponen de todas las actualizaciones de seguridad.

En caso de detectar un comportamiento extraño del equipo o sospechar de una posible infección, fuga de información o incidente de seguridad, debe comunicarse con los teléfonos indicados en el punto anterior.

Anexo I: Certificado digital para el acceso a la VPN

Es necesario disponer de un certificado digital emitido por la ACCV o el DNI electrónico para conectarse a través de la VPN habilitada por la GVA para el teletrabajo. Los casos que pueden darse son:

- Certificado de empleado público de la ACCV en soporte tarjeta:
 - Si tiene lector en su casa, puede acceder con el certificado en el lector conectado al ordenador doméstico sin necesidad de hacer ninguna otra acción. En el caso de que necesite utilizar el portafirmas y quiera utilizar un certificado distinto para firmar, por ejemplo el certificado de pseudónimo de FNMT, necesitará descargar e instalarse el certificado software según se indica en el [Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software](#)
 - Si no tiene lector en su casa, desde su puesto de trabajo en la sede judicial deberá acceder a la página de la ACCV (<https://www.accv.es>) y descargarse el certificado software según se indica en el [Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software](#) llevárselo a casa en un pendrive o enviarlo por correo electrónico e instalarlo según se indica en el anexo V mencionado.
- DNI-e:
 - Si tiene lector en su casa puede acceder con el DNI-e en el lector conectado al ordenador doméstico sin necesidad de hacer ninguna otra acción. En este caso debe tener en cuenta que si necesita utilizar el portafirmas y quiere utilizar un certificado distinto al DNI-e necesitará descargar e instalarse el certificado software según se indica en el [Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software](#) , y de esa forma dejar libre el lector de tarjeta del ordenador doméstico para poder utilizarlo para el certificado a la hora de firmar.
 - Si no tiene lector en casa, podrá hacer la descarga del certificado software desde el puesto de trabajo en la sede judicial según se indica en el [Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software](#)
- No tiene certificado de la ACCV ni DNI-e:

En este caso debe acudir a un Punto de Registro de Usuario de la ACCV (punto PRU) para obtener un **certificado digital de Ciudadano en soporte software**. Este certificado es gratuito. Puede encontrar más información de este tipo de certificado y cómo obtenerlo en <https://www.accv.es/certificados/ciudadano-software/>

Con respecto a los puntos PRU, puede consultar las direcciones y teléfonos de todos los PRU de la ACCV en <https://www.accv.es/encuentra-tu-pru/>. Deberá llamar al PRU donde desee ir para confirmar que está dando servicio y coger cita previa en el caso de ser necesaria.



Una vez tenga el certificado, deberá instalárselo en el ordenador doméstico siguiendo las instrucciones del [Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software](#)

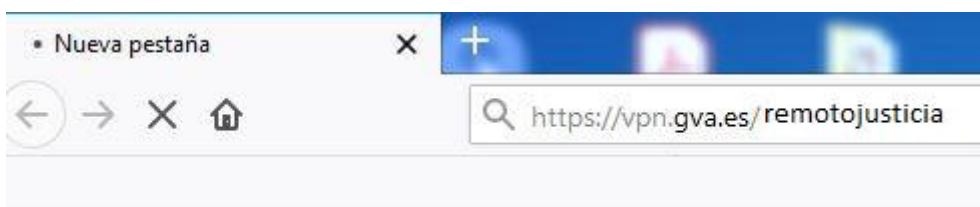
Anexo II: Instrucciones de Acceso remoto desde el equipo doméstico al ordenador de la oficina en la Administración de Justicia (escritorio remoto)

Las siguientes instrucciones explican cómo acceder al ordenador de la oficina desde su ordenador doméstico.

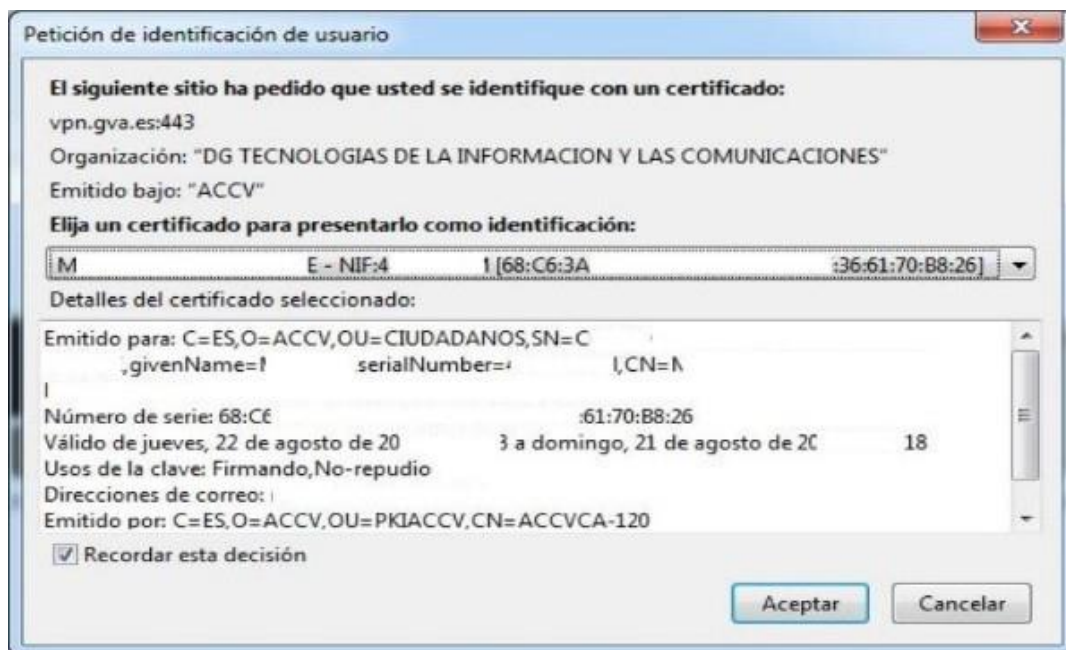
Como requisito previo, el certificado digital deberá estar instalado en el equipo de acuerdo al

[Anexo I: Certificado digital para el acceso a la VPN](#)

En primer lugar hay que abrir el navegador (Chrome, Firefox o Internet Explorer) y escribir la URL de acceso: <https://vpn.gva.es/remotojusticia>.



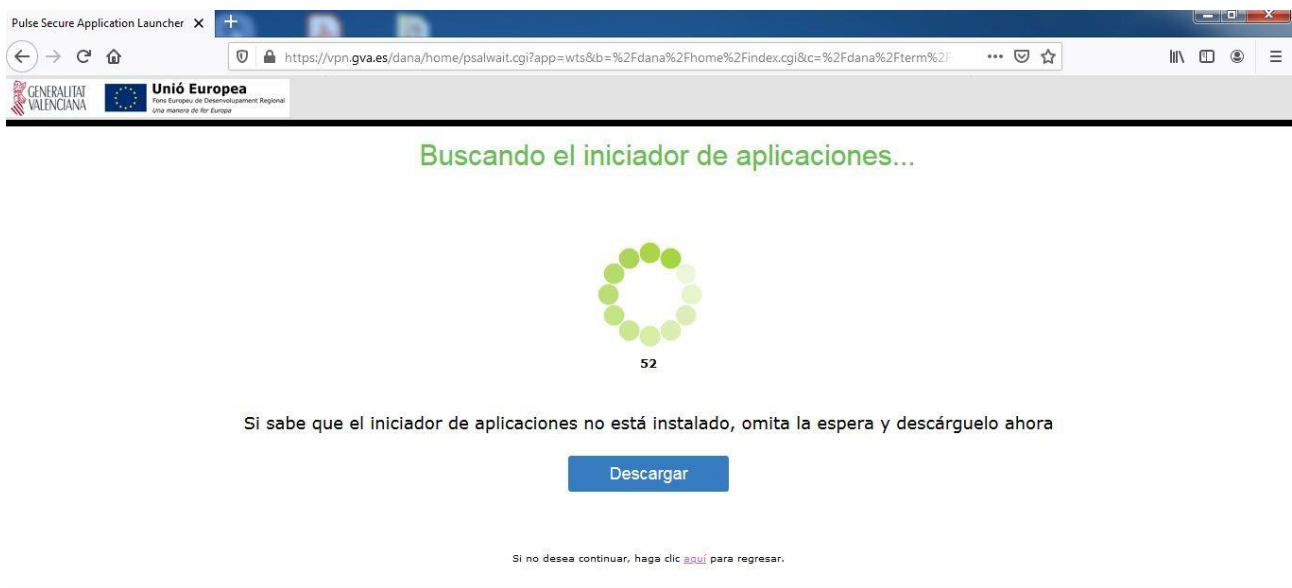
El navegador solicitará la autenticación con el certificado digital. Escogemos el certificado y pulsamos sobre **“Aceptar”**.



A continuación aparecerá la página de conexión al ordenador de sobremesa de su puesto de trabajo



Hay que pulsar sobre el enlace “**Acceso Remoto PCNNNNNN.justicia.gva.es**”, aparecerá la siguiente pantalla:

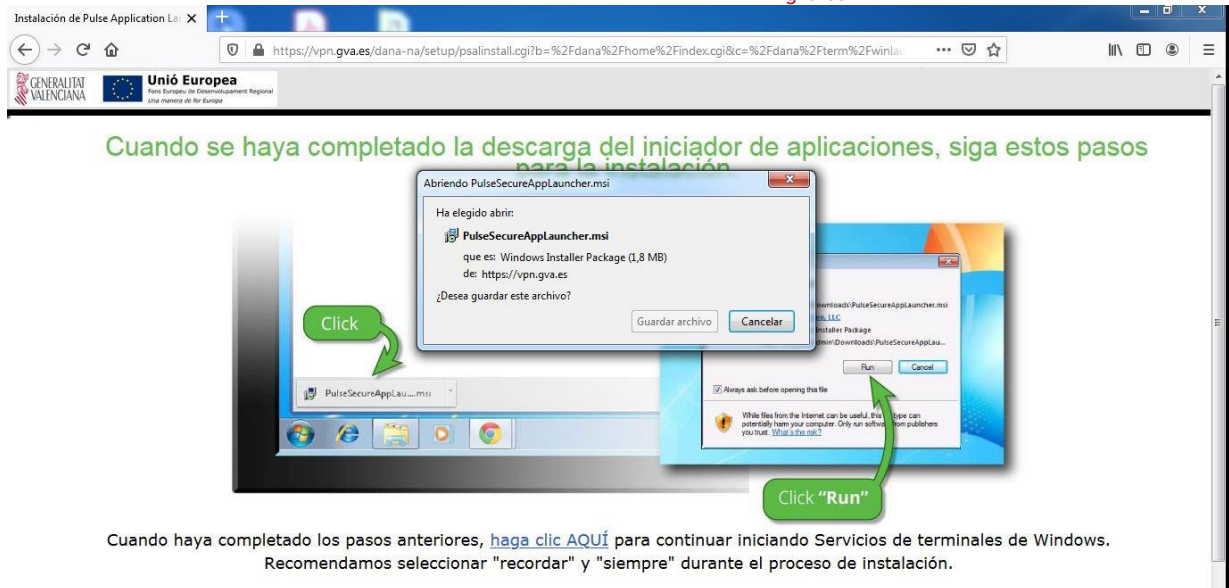


NOTA: en caso de utilizar un ordenador Mac para hacer la conexión remota, en el [Anexo III: INSTALAR APLICACIONES DE TERCEROS EN MAC](#), encontrará indicaciones para permitir la instalación del Plugin de Java para Pulse en estos ordenadores

La primera vez que conectemos, el equipo solicitará la instalación de dos componentes.

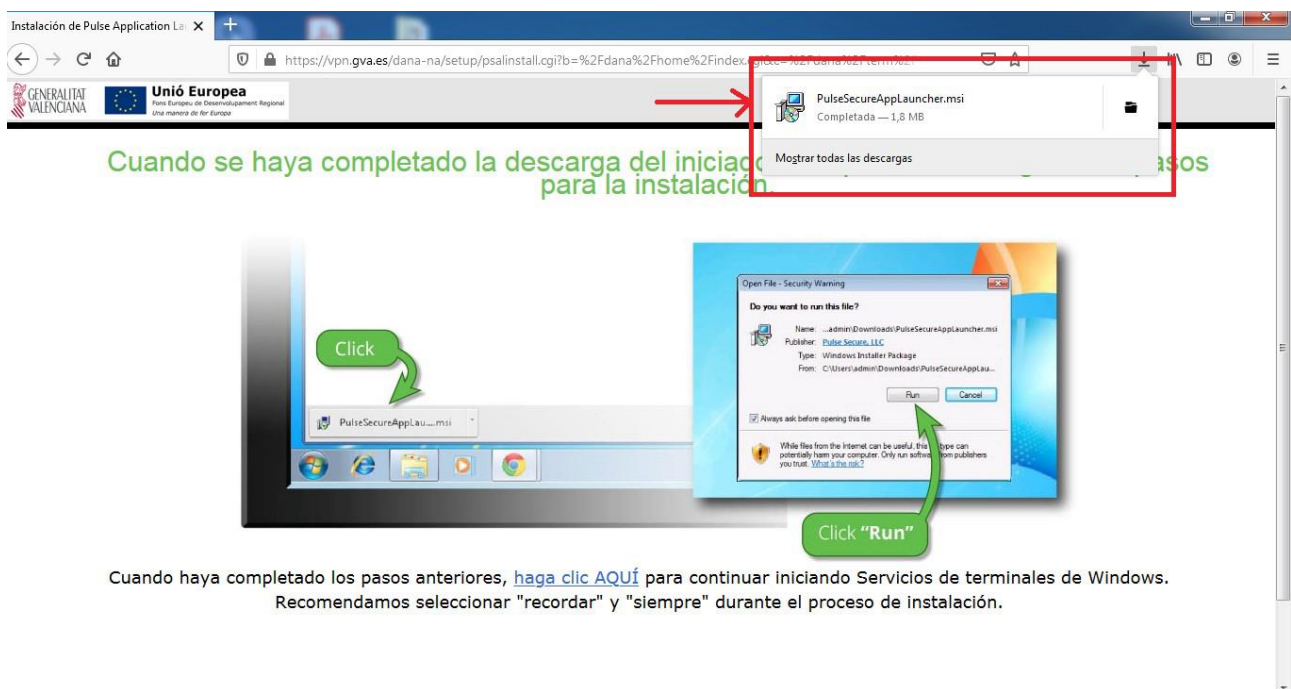
El primero:

Pulsando sobre el botón azul que indica “**Descargar**”, descargaremos un fichero denominado “**PulseSecureAppLauncher.msi**”



Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando Servicios de terminales de Windows. Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

Tras la descarga tenemos que ejecutar este programa:



Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando Servicios de terminales de Windows. Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

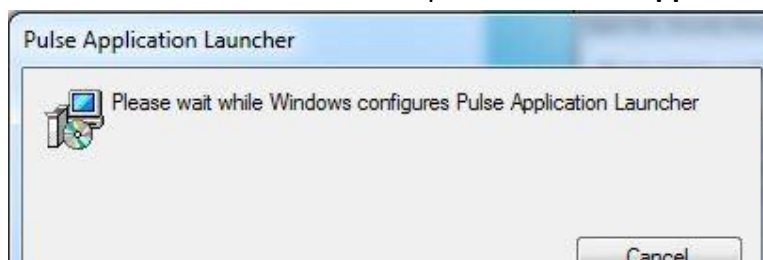
Si el equipo nos pide permiso para ejecutar este componente, pulsamos sobre "Aceptar":



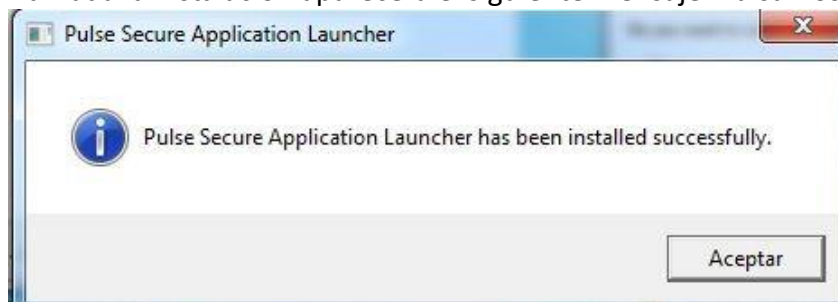
Y posteriormente en “Ejecutar”:



Tras esto comenzará la instalación del componente “**Pulse Application Launcher**”:



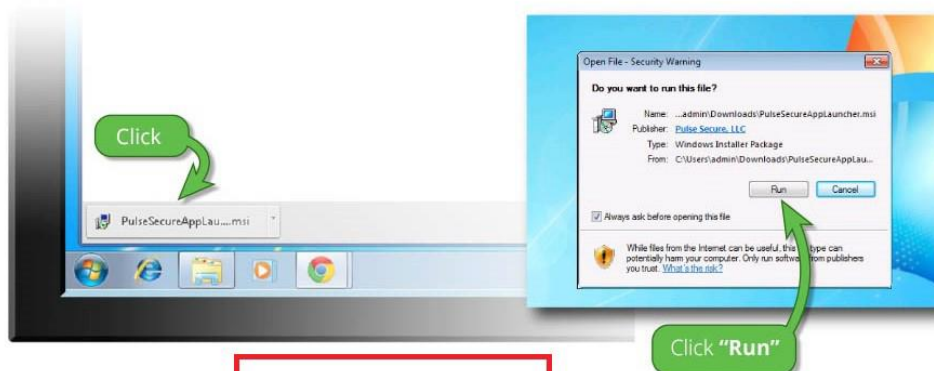
Una vez finalizada la instalación aparecerá el siguiente mensaje. Pulsamos “**Aceptar**”:



Ya está **instalado el primer componente.**

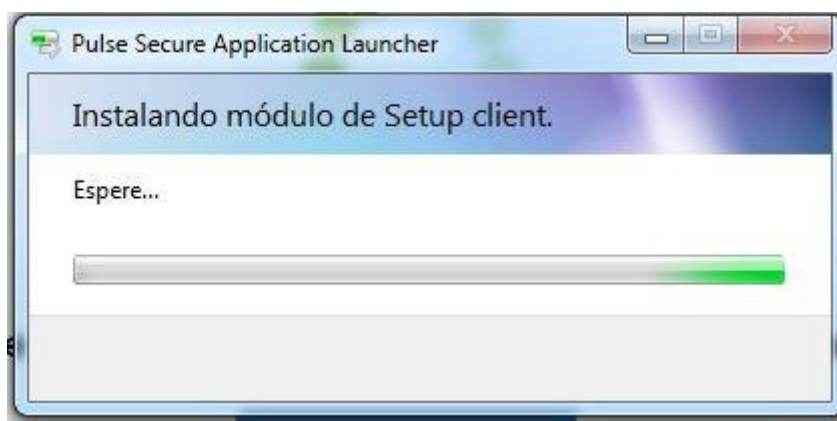
Ahora Pulsamos sobre “**haga clic AQUÍ**” para continuar con la instalación del **segundo**

componente:

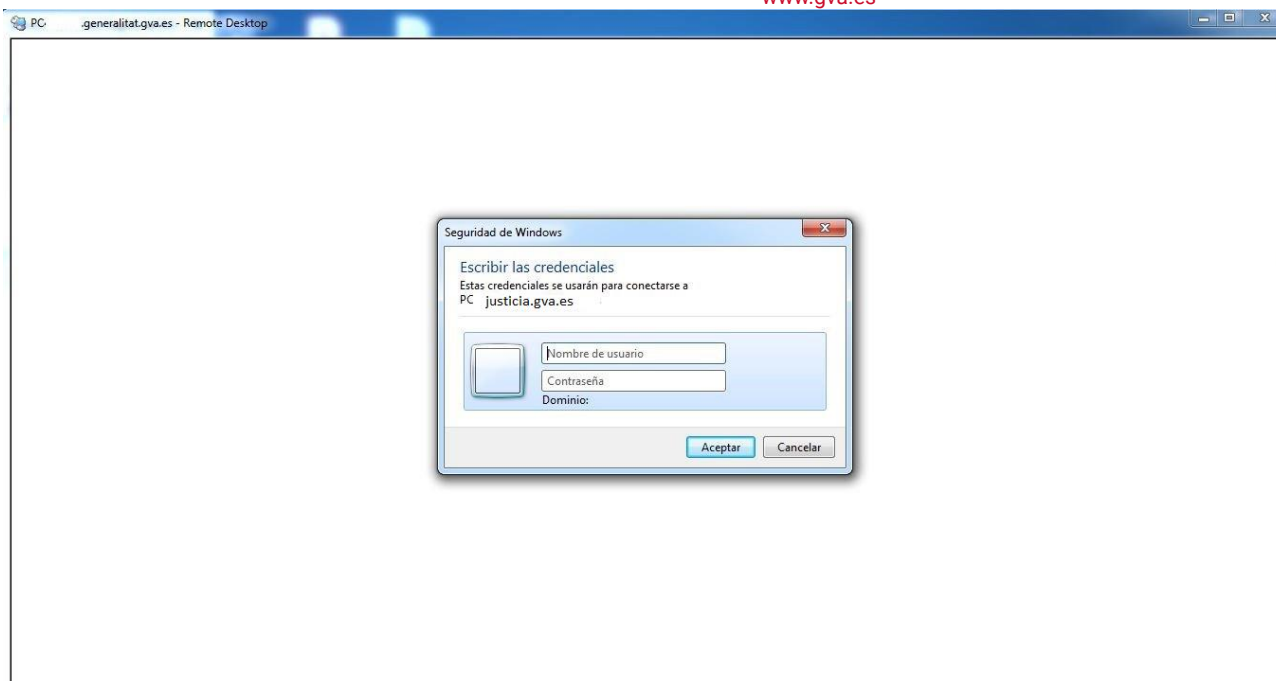


Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando Servicios de terminales de Windows. Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

Automáticamente comenzará la instalación del **segundo componente** necesario para la conexión remota:



Tras finalizar la instalación, el equipo de oficina solicitará las credenciales de acceso, es decir el nombre de usuario y la contraseña del dominio **JUSTICIA**:



IMPORTANTE: en el campo Nombre de usuario, a su usuario tiene que anteponer, sin espacios, **JUSTICIA**

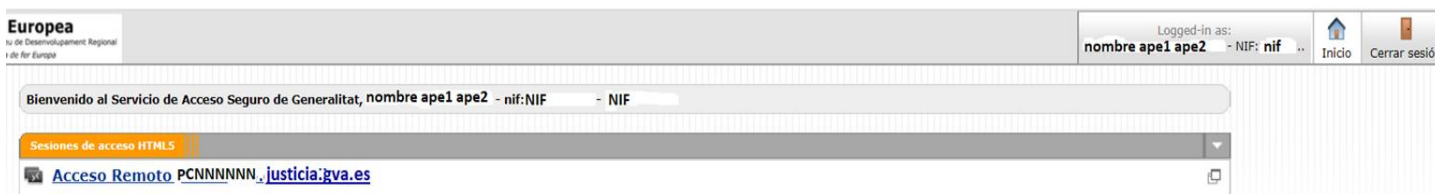
La contraseña de acceso a su puesto de trabajo **NO ES EL PIN de la tarjeta criptográfica** con que usted accede a su equipo habitualmente de forma presencial. La contraseña que le pide aquí es la que está vinculada al usuario. Si usted normalmente utilizada solo la tarjeta criptográfica para acceder a su puesto de trabajo habrá recibido un correo con la contraseña que tendrá que utilizar la primera vez que acceda. Cuando inicie sesión la primera vez en el ordenador del trabajo le solicitará que la cambie.

Tras introducir estas credenciales, se abrirá el entorno de trabajo del equipo de oficina.

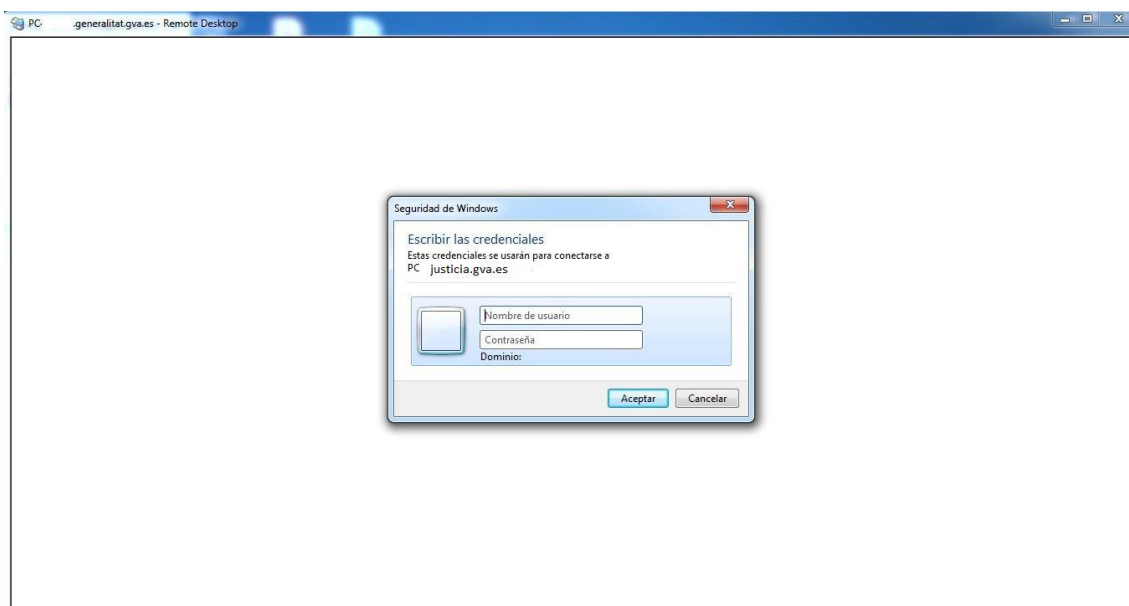
El procedimiento anterior habrá que realizarlo solamente la primera vez.

Las siguientes veces que conectemos, bastará escribir en el navegador la URL de acceso:
<https://vpn.gva.es/remotojusticia>.

Aparecerá la pantalla con el enlace al puesto de trabajo:



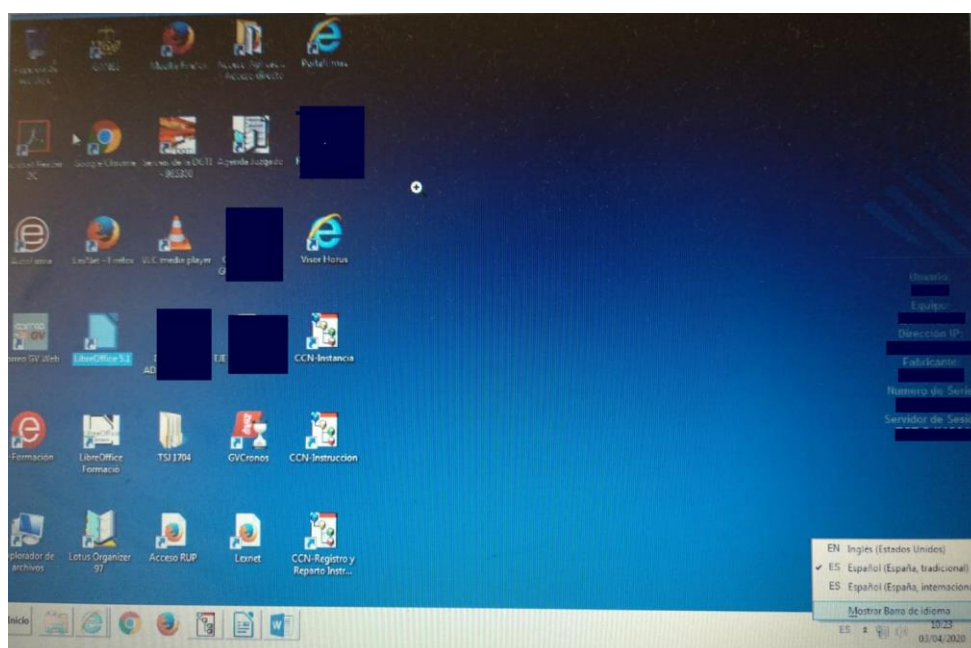
Tras pulsar en el enlace nos solicitará las credenciales del dominio. Al introducirlas, accederemos al equipo de oficina:



Como se ha indicado anteriormente en Nombre de usuarios deberá poner su usuario anteponiendo **JUSTICIA**

Tras esto, accederá al ordenador de sobremesa de su puesto de trabajo de la Administración de Justicia.

En ocasiones al acceder al ordenador de la oficina se cambia el idioma del teclado. Para poner el teclado otra vez en español, en la barra de windows, en la esquina inferior derecha, estando el ratón sobre el símbolo del idioma, al pulsar el botón derecho del ratón se despliega un menú y hay que marcar Español.

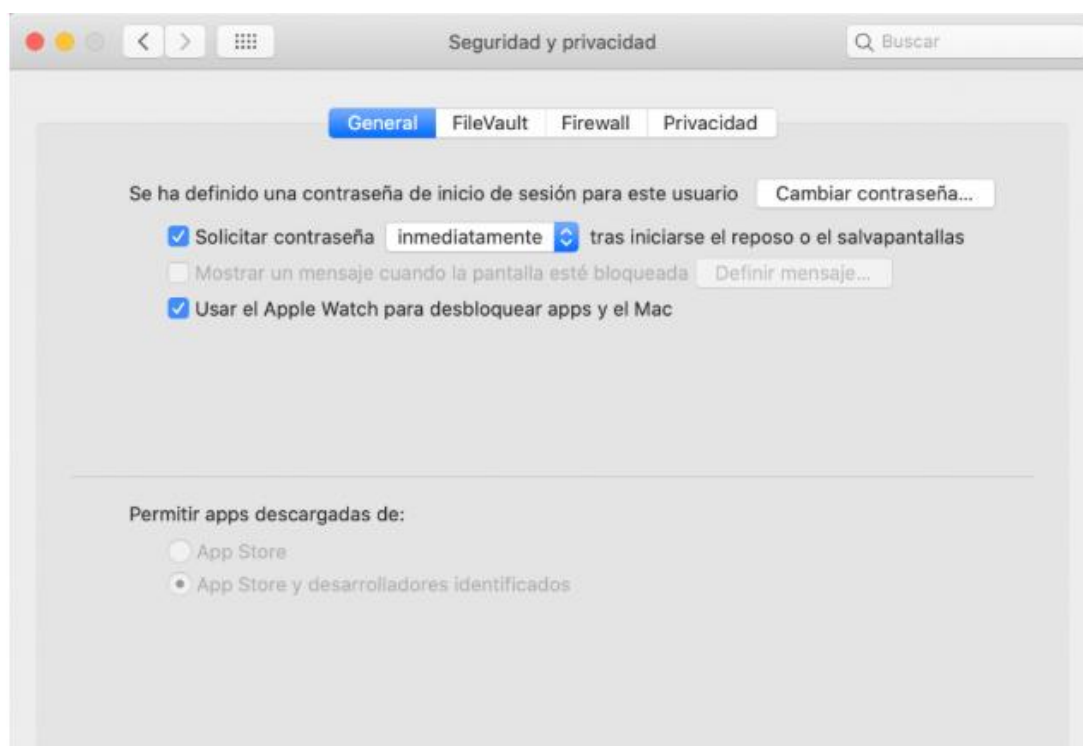


Para terminar la sesión, pulse sobre el icono de la puerta
derecha de
la pantalla.

,  en la parte superior

Anexo III: Instalar Aplicaciones de terceros en Mac

1. Ir a Preferencias del Sistema>Seguridad y Privacidad.
2. Pulsar sobre el candado que aparece en la parte inferior izquierda e introducir la contraseña que utiliza para desbloquear su Mac.
3. En la parte dónde pone «Permitir apps de terceros» se deberá marcar la casilla de «App Store y desarrolladores identificados».



En la mayoría de ocasiones saldrá una ventana emergente en la que se alerta de que se está instalando software desconocido, hay que aceptar para continuar. También se puede dar el caso de que, nuevamente, haya que acudir al apartado de Seguridad y Privacidad. En esta ocasión sería para aceptar la instalación de esa aplicación en concreto.

Anexo IV: Obtención de certificado en soporte software desde tarjeta criptográfica . Instalación del certificado software

Consideraciones previas:

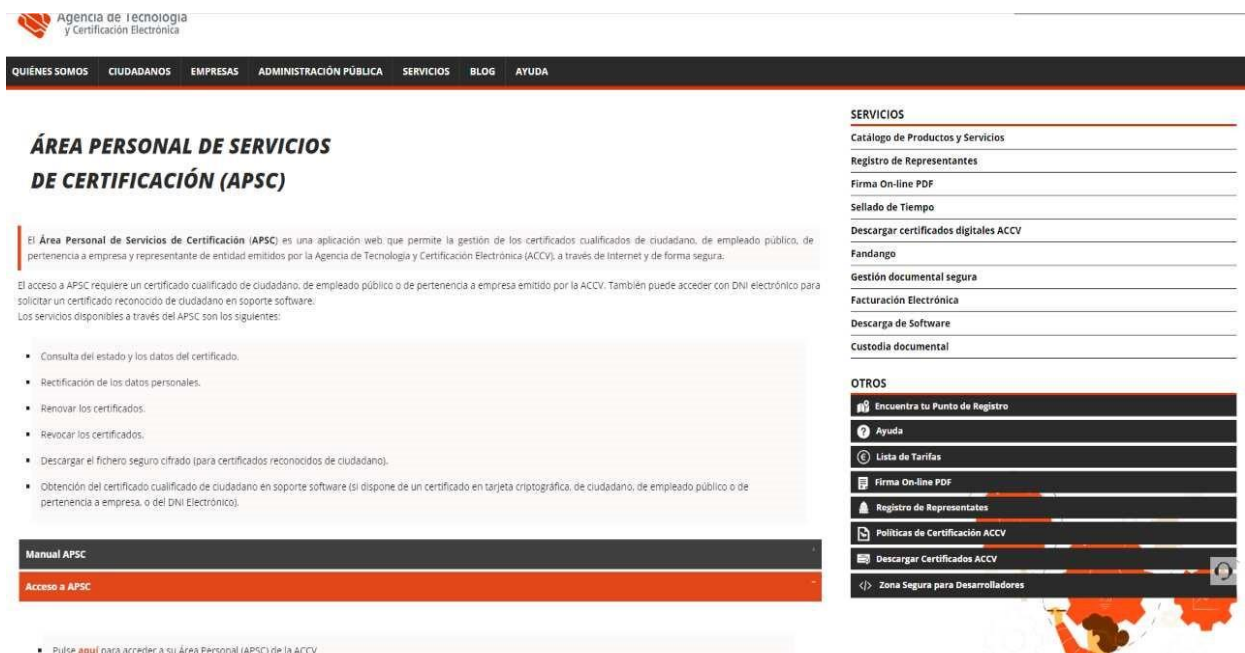
Certificados válidos para identificarse y descargar el certificado ACCV en Software:

- Tarjeta criptográfica ACCV
- DNle

Si dispone de un lector y necesita descargar el certificado ACCV en SW, puede realizarlo tal como se describe a continuación. Si no dispone de lector en su domicilio, deberá realizar la descarga desde el puesto de trabajo en su Sede de Justicia, y una vez descargado llevarlo (grabar en un USB, enviárselo por mail) al PC de uso en su domicilio para instalarlo.

Procedimiento a seguir:

Acceder a la web <https://www.accv.es/ciudadanos/area-personal-de-serviciosde-certificacion/> Allí se encuentra el acceso al **Área Personal de Servicios de Certificación (APSC)** y un manual más ampliado de Usuario.



Agencia de Tecnología y Certificación Electrónica

QUIÉNES SOMOS CIUDADANOS EMPRESAS ADMINISTRACIÓN PÚBLICA SERVICIOS BLOG AYUDA

ÁREA PERSONAL DE SERVICIOS DE CERTIFICACIÓN (APSC)

El Área Personal de Servicios de Certificación (APSC) es una aplicación web que permite la gestión de los certificados cualificados de ciudadano, de empleado público, de pertenencia a empresa y representante de entidad emitidos por la Agencia de Tecnología y Certificación Electrónica (ACCV), a través de Internet y de forma segura.

El acceso a APSC requiere un certificado cualificado de ciudadano, de empleado público o de pertenencia a empresa emitido por la ACCV. También puede acceder con DNI electrónico para solicitar un certificado reconocido de ciudadano en soporte software. Los servicios disponibles a través del APSC son los siguientes:

- Consulta del estado y los datos del certificado.
- Rectificación de los datos personales.
- Renovar los certificados.
- Revocar los certificados.
- Descargar el fichero seguro cifrado (para certificados reconocidos de ciudadano).
- Obtención del certificado cualificado de ciudadano en soporte software (si dispone de un certificado en tarjeta criptográfica, de ciudadano, de empleado público o de pertenencia a empresa, o del DNI Electrónico).

Manual APSC

Acceso a APSC

SERVICIOS

- Catálogo de Productos y Servicios
- Registro de Representantes
- Firma On-line PDF
- Sellado de Tiempo
- Descargar certificados digitales ACCV
- Fandango
- Gestión documental segura
- Facturación Electrónica
- Descarga de Software
- Custodia documental

OTROS

- Encuentra tu Punto de Registro
- Ayuda
- Lista de Tarifas
- Firma On-line PDF
- Registro de Representantes
- Políticas de Certificación ACCV
- Descargar Certificados ACCV
- Zona Segura para Desarrolladores

• Pulse [aquí](#) para acceder a su Área Personal (APSC) de la ACCV

Al entrar al APSC con su tarjeta criptográfica o DNle en el equipo, verá la opción para obtener su certificado cualificado de ciudadano en soporte software.

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

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.

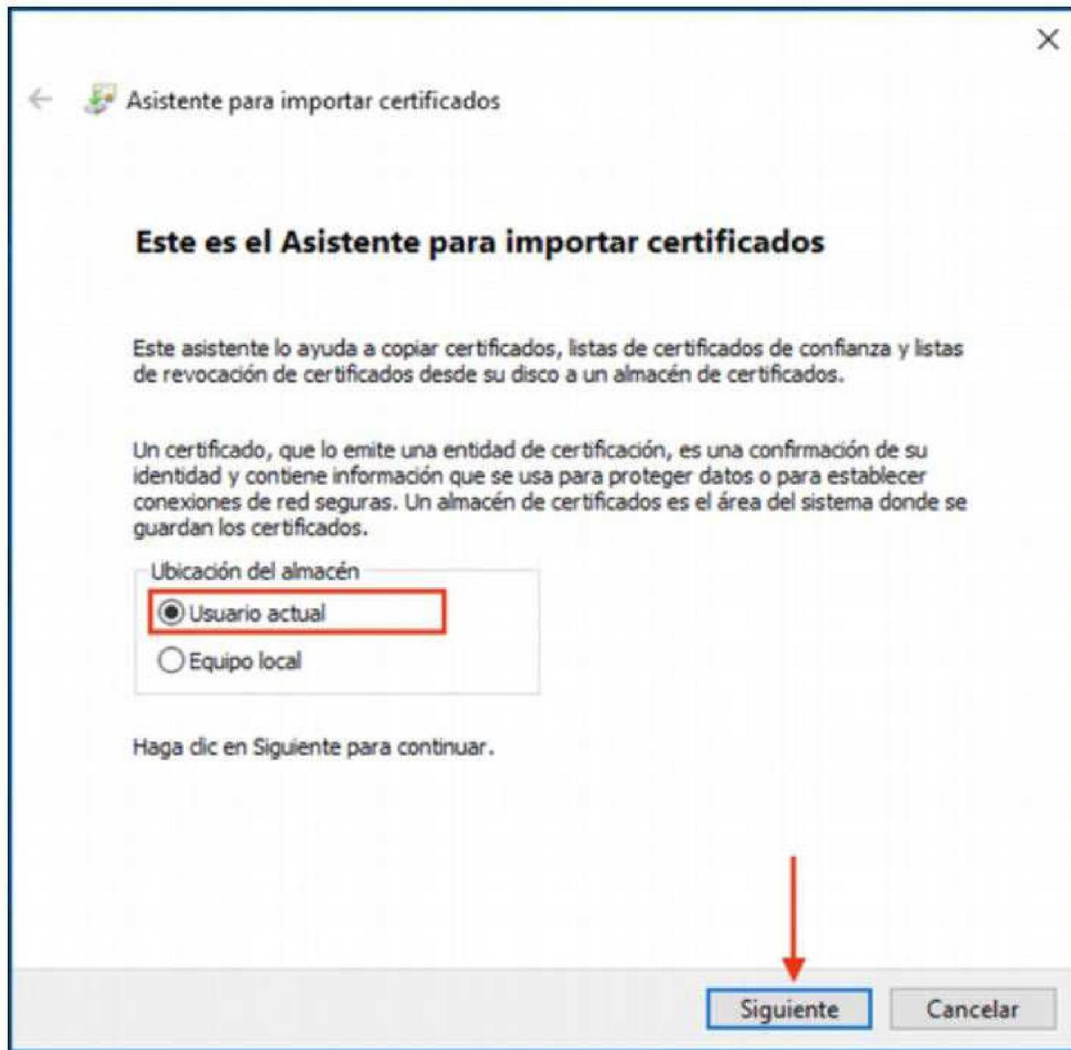
4. Su navegador web es posible que le pregunte sobre dónde desea guardar en su equipo el fichero con el certificado de cifrado seleccionado y sus claves asociadas. Si es así seleccione la ubicación deseada y guárdelo. En caso contrario, su navegador web guardará el fichero en la carpeta por defecto para las descargas.

*****Si no dispone de lector de tarjetas en su domicilio, será este archivo descargado el que tendrá que llevarse para instalarlo (grabar en USB, enviárselo por mail)*****

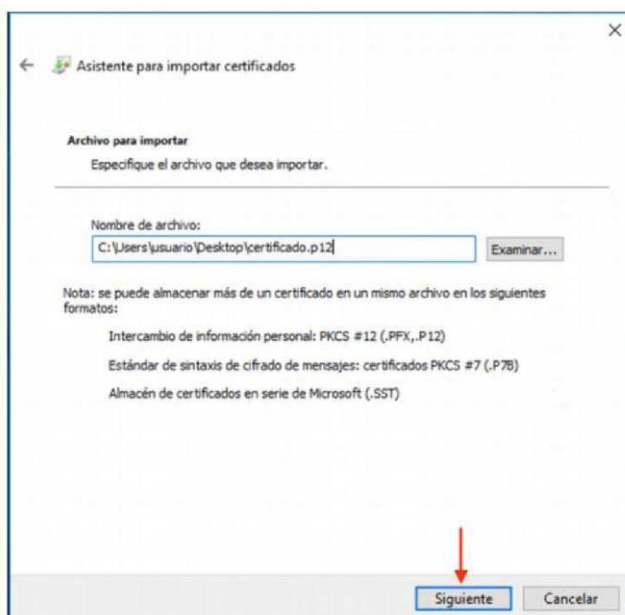
5. Finalmente, haga clic en el botón **Ver** asociado al certificado de cifrado que acaba de descargar para visualizar la contraseña/PIN que se le pedirá cada vez que desee acceder al contenido del fichero que acaba de descargar. Deberá anotar o imprimir esta contraseña/PIN y guardarla para poder utilizarla con el fichero que acaba de descargar

Instalación del certificado en soporte software (Internet Explorer y Chrome)

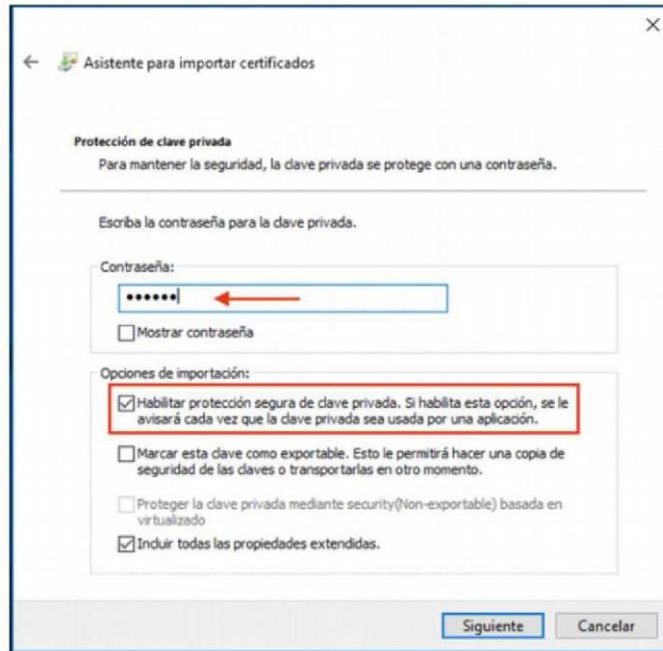
Haga **doble-clic** sobre el fichero .p12 o .pfx que contiene su certificado digital y claves. Se abrirá el *Asistente para la importación de certificados*. Deberá marcar **Usuario actual**. De este modo, el certificado se instalará solo para el usuario con el que ha iniciado sesión. Pulse **Siguiente**.



En la pantalla a continuación aparece seleccionado su certificado. Pulse **Siguiente**.

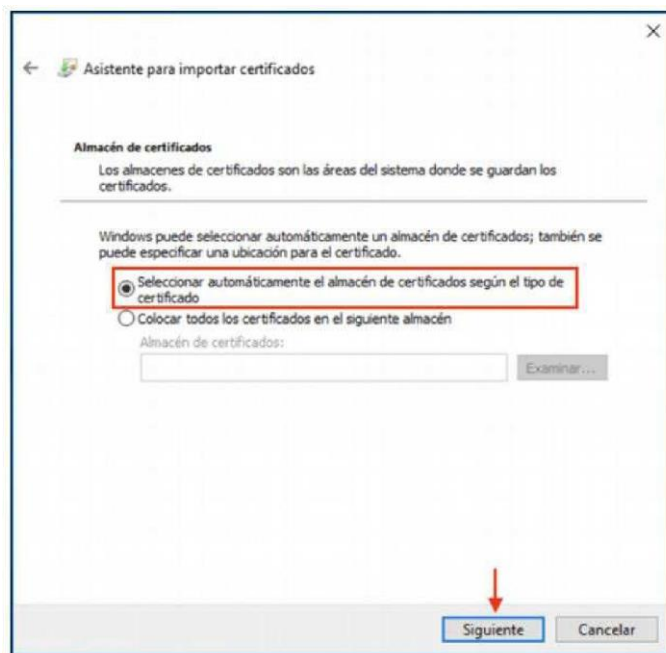


En el apartado *Contraseña* debe **introducir su PIN** asociado al certificado que está instalando.
IMPORTANTE: Marque la opción **Habilitar protección segura de claves privadas**.
Pulse **Siguiente**.



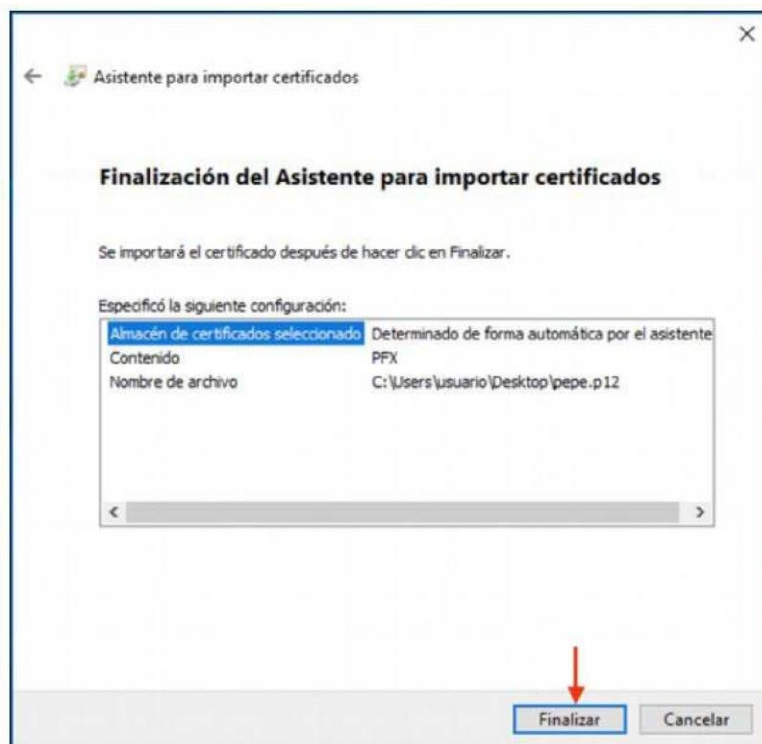
The screenshot shows the 'Asistente para importar certificados' window at the 'Protección de clave privada' step. The text indicates that the private key is protected by a password. A password field with a red arrow pointing to it is shown, along with a 'Mostrar contraseña' checkbox. Below, the 'Opciones de importación' section has four options: 'Habilitar protección segura de clave privada' (checked and highlighted with a red box), 'Marcar esta clave como exportable', 'Proteger la clave privada mediante security(Non-exportable) basada en virtualizado', and 'Incluir todas las propiedades extendidas' (checked). 'Siguiente' and 'Cancelar' buttons are at the bottom.

Marque la opción **Seleccionar automáticamente el almacén de certificados según el tipo de certificado**.
Pulse **Siguiente**.



The screenshot shows the 'Asistente para importar certificados' window at the 'Almacén de certificados' step. The text explains that certificates are stored in system areas. It offers two options: 'Seleccionar automáticamente el almacén de certificados según el tipo de certificado' (selected and highlighted with a red box) and 'Colocar todos los certificados en el siguiente almacén'. Below the second option is a text field and an 'Examinar...' button. The 'Siguiente' button at the bottom is highlighted with a red arrow.

Pulse **Finalizar**.



PONER UNA CONTRASEÑA AL CERTIFICADO (OPCIONAL)

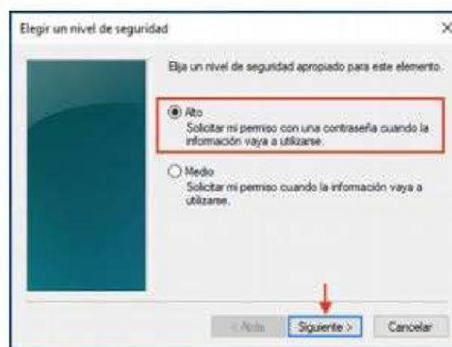
6. A continuación, tiene la opción de definir una contraseña segura que proteja el certificado que está instalando. Si la establece, ésta se le pedirá cuando vaya a emplear el certificado.

Si no quiere, pulse **Aceptar** para salir y finalizar la instalación sin ponerle contraseña.

Sólo si quiere establecer una contraseña segura, debe pulsar el botón **Nivel de seguridad...**

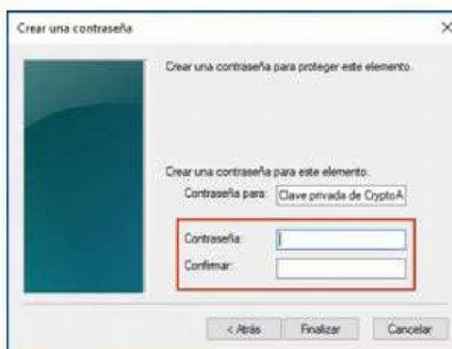


Marque la opción **Alto** y pulse el **Siguiente**.



Aparecerá una ventana en la que debe introducir la nueva contraseña. Deberá elegir la **contraseña** que usted prefiera, escribirla aquí dos veces y pulsar **Finalizar**.

Por su seguridad y siempre que sea capaz de recordarla, le recomendamos que elija una contraseña de al menos 8 caracteres y que contenga letras mayúsculas, minúsculas, números y símbolos como +, -, =, *, ", !, etc.



Por último pulse **Aceptar**. El asistente le informará que la importación se completó correctamente. Entonces su certificado estará correctamente instalado y listo para ser utilizado.

