

# 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: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software .....	13
INSTAL·LACIÓ DE CERTIFICAT DIGITAL EN FITXER: Edge y Chrome .....	14

## 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 puguen 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** adquirint 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 pseudònim de FNMT, necessitarà descarregar i instal·lar-se el certificat software segons s'indica en [l'Annex III: 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 III: 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 II: 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 III: 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.

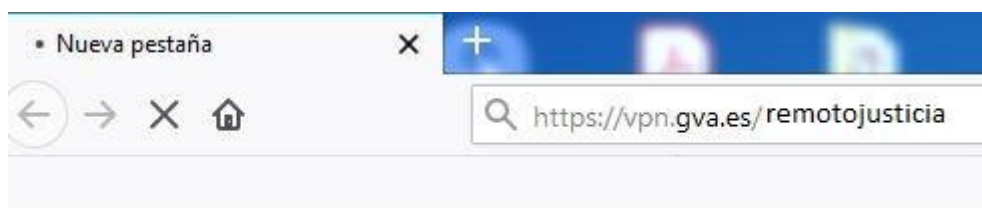
Una vegada tinga el certificat, haurà d'instal·lar-li'l en l'ordinador domèstic seguint les instruccions [de l'Annex III: Obtenció de certificat en suport software des de targeta criptogràfica . Instal·lació del certificat software](#)

## 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>.



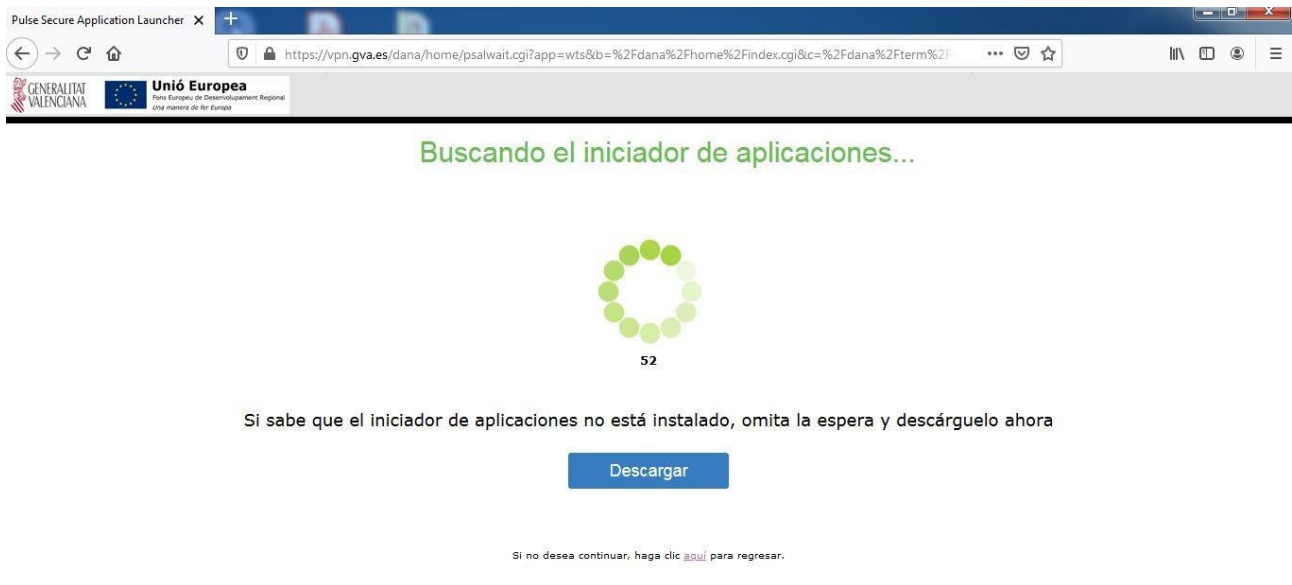
El navegador sol·licitarà l'autenticació amb el certificat digital. Triem el certificat i premem sobre "Aceptar".



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



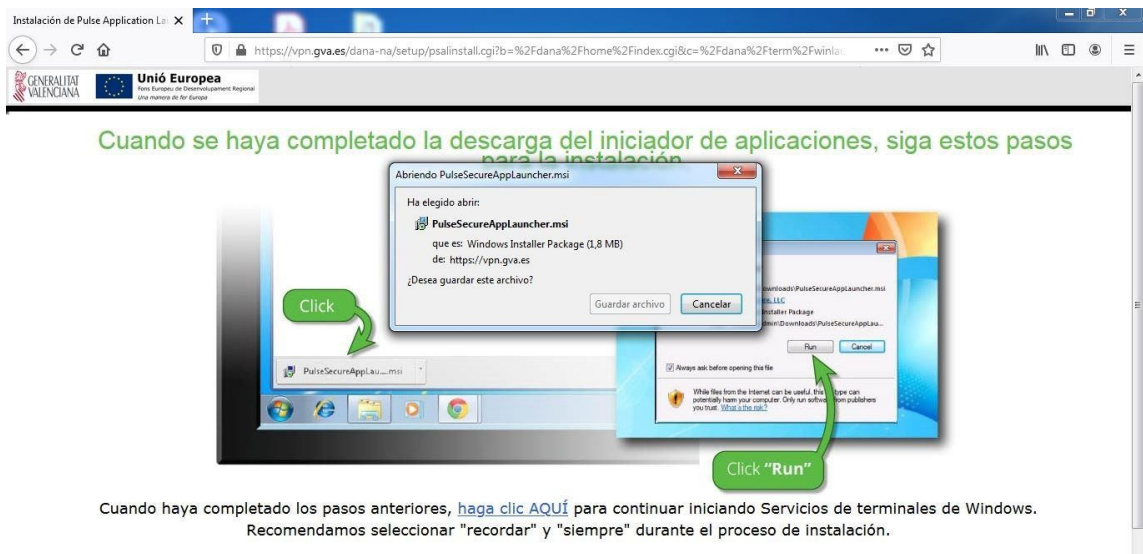
Cal prémer sobre l'enllaç “**Accés Remot \*PCNNNNNN.justícia.gva.es**”, apareixerà la següent pantalla:



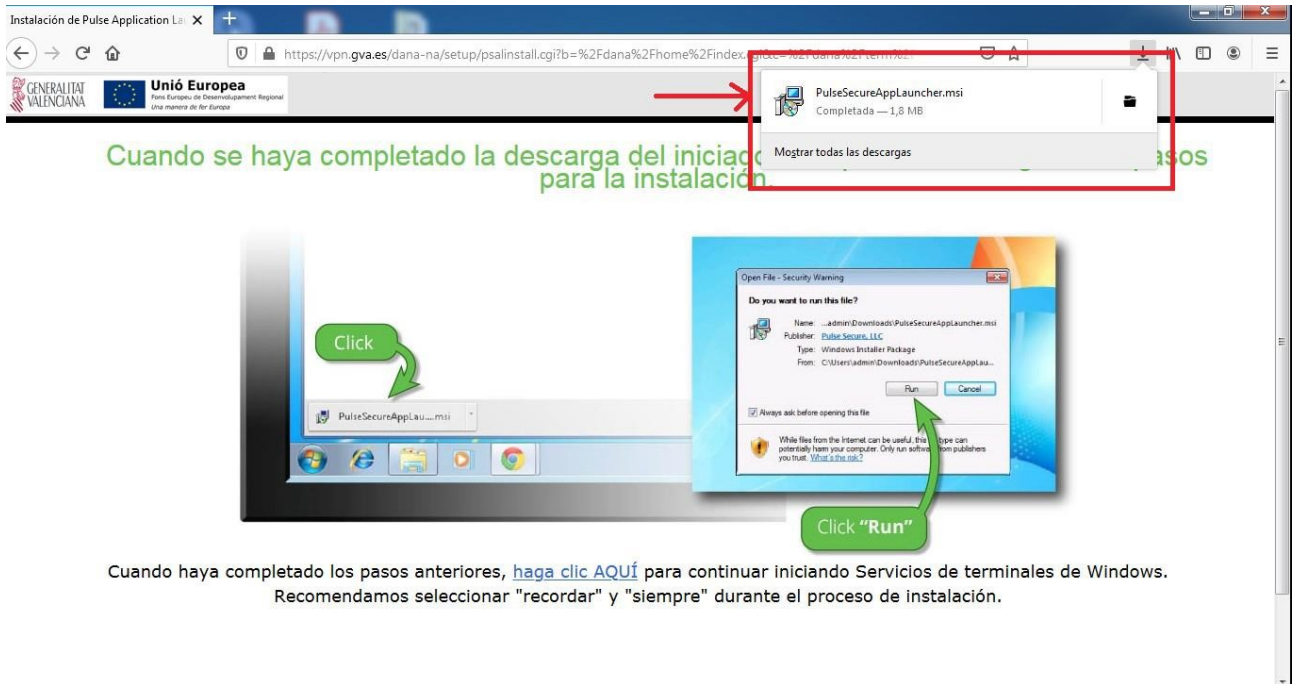
La primera vegada que connectem, l'equip sol·licitarà la instal·lació de dos components. El primer:

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





Després de la descàrrega hem d'executar aquest programa:



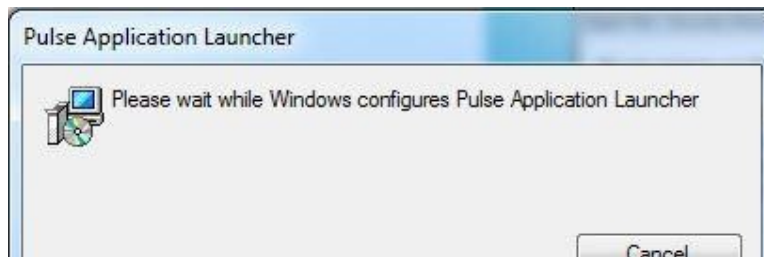
Si l'equip ens demana permís per a executar aquest component, premem sobre "Acceptar":



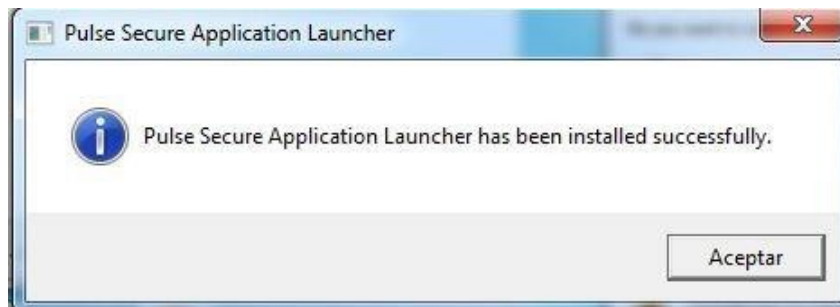
I posteriorment a "Executar":



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



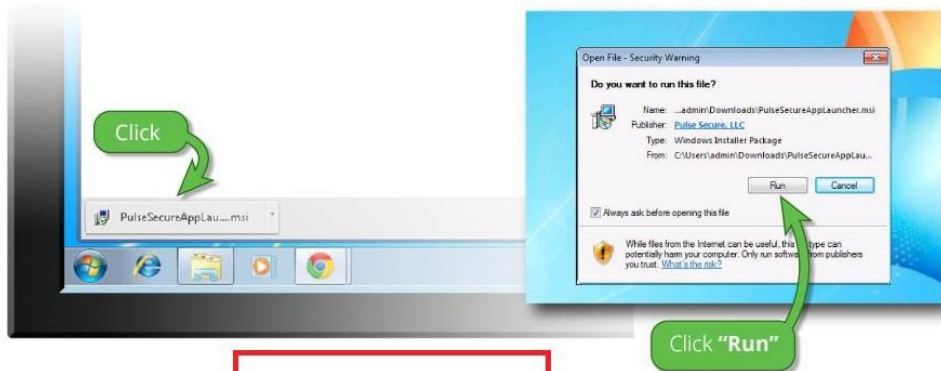
Una vegada finalitzada la instal·lació apareixerà el següent missatge. Premem **“Aceptar”**:



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

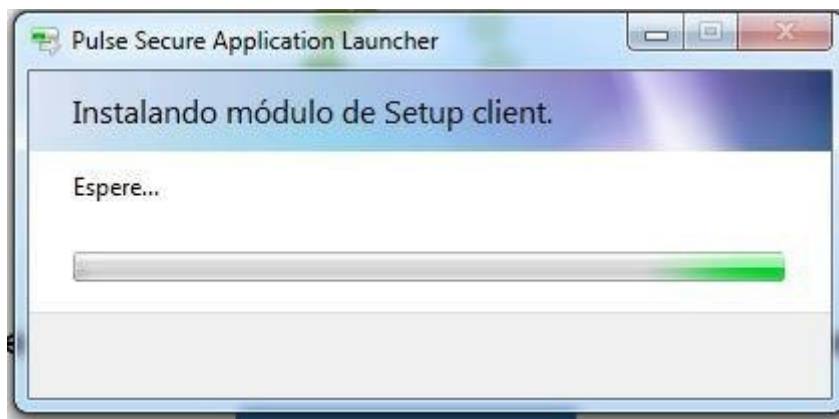
Ara Premem sobre **“haga clic AQUI”** per a continuar amb la instal·lació del **segon component**:



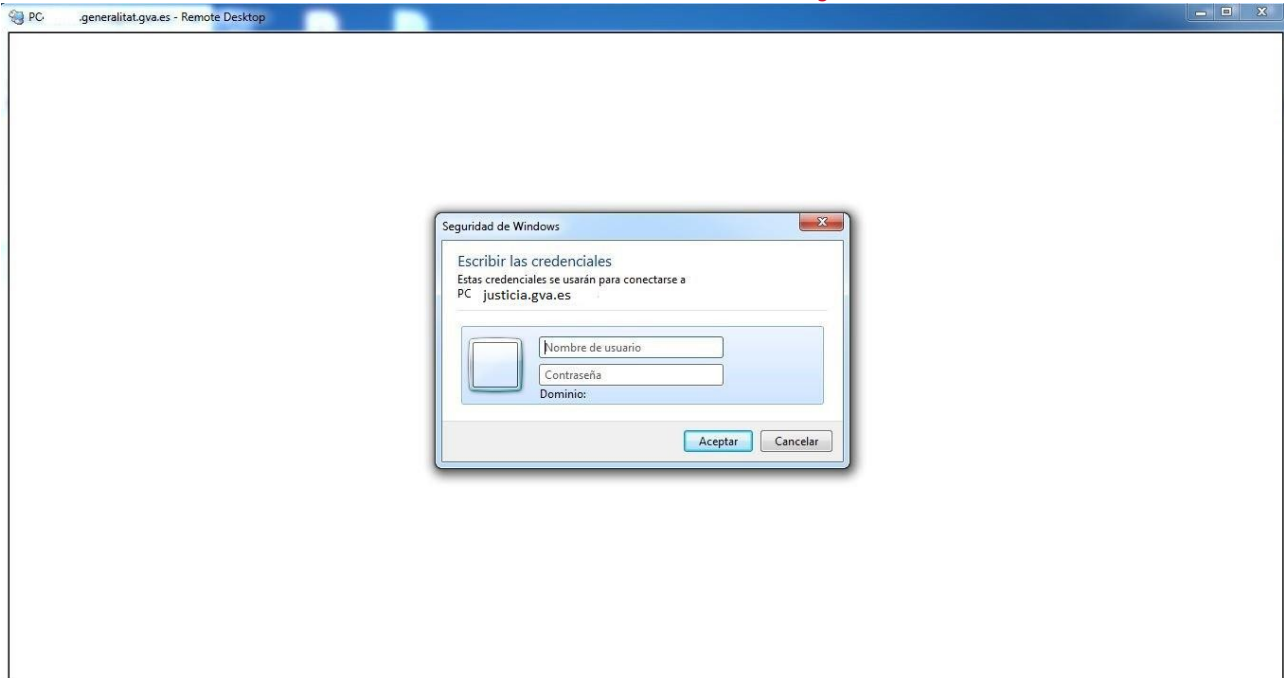


Cuando haya completado los pasos anteriores, [haga clic AQUÍ](#) para continuar iniciando Servicios de terminales de Windows. Recomendamos seleccionar "recordar" y "siempre" durante el proceso de instalación.

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\**

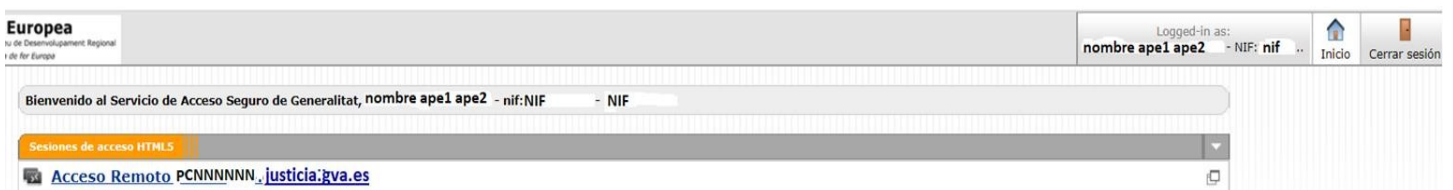
**La contrasenya** d'accés al seu lloc de treball **NO ÉS EL PIN de la targeta criptogràfica** amb què vosté accedeix al seu equip habitualment de manera presencial. La contrasenya que li demana ací és la que està vinculada a l'usuari. Si vosté normalment utilitzada només la targeta criptogràfica per 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.

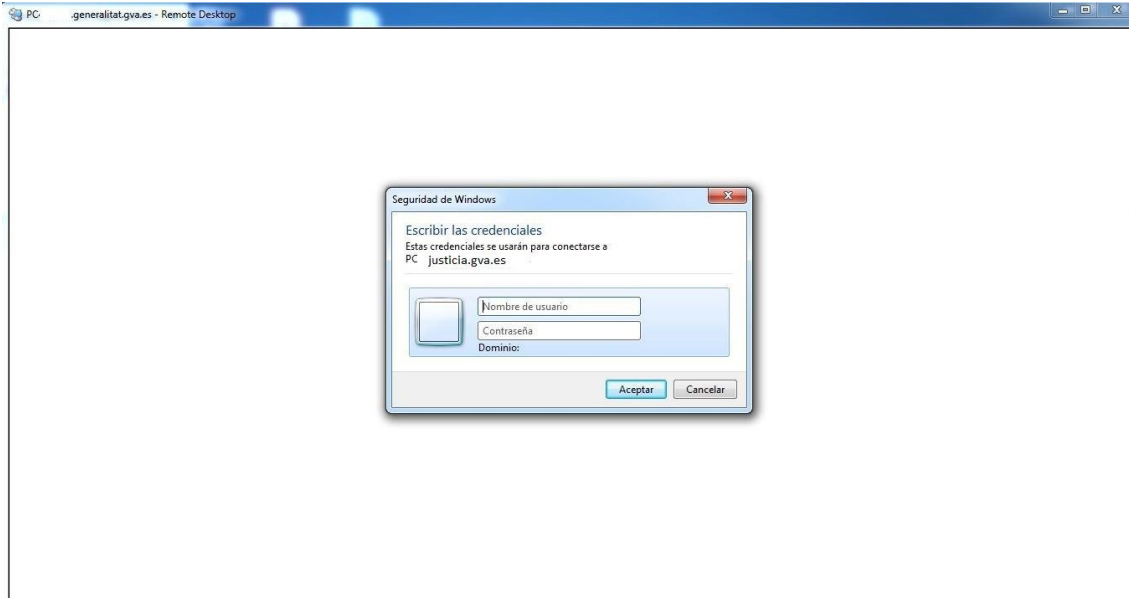
**El procediment anterior caldrà realitzar-lo solament la primera vegada.**

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:



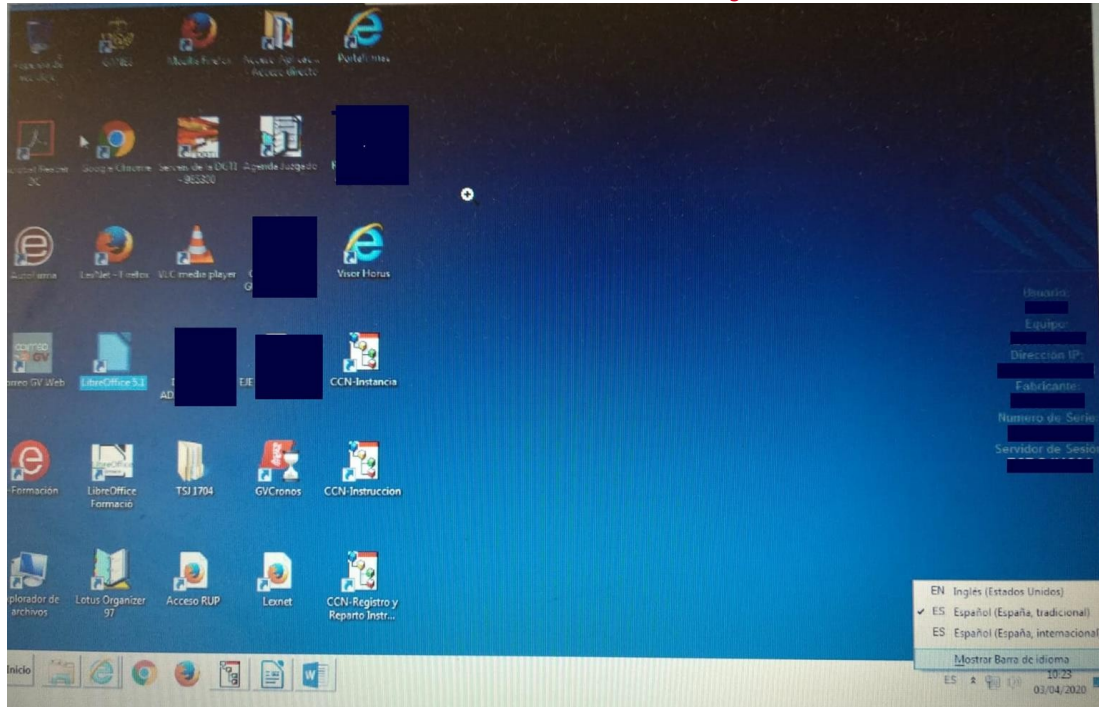
Després de prémer en l'enllaç ens sol·licitarà les credencials del domini. En introduir-les, accedirem a l'equip d'oficina:



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, a la part superior dreta de la pantalla.



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

### Consideracions prèvies:

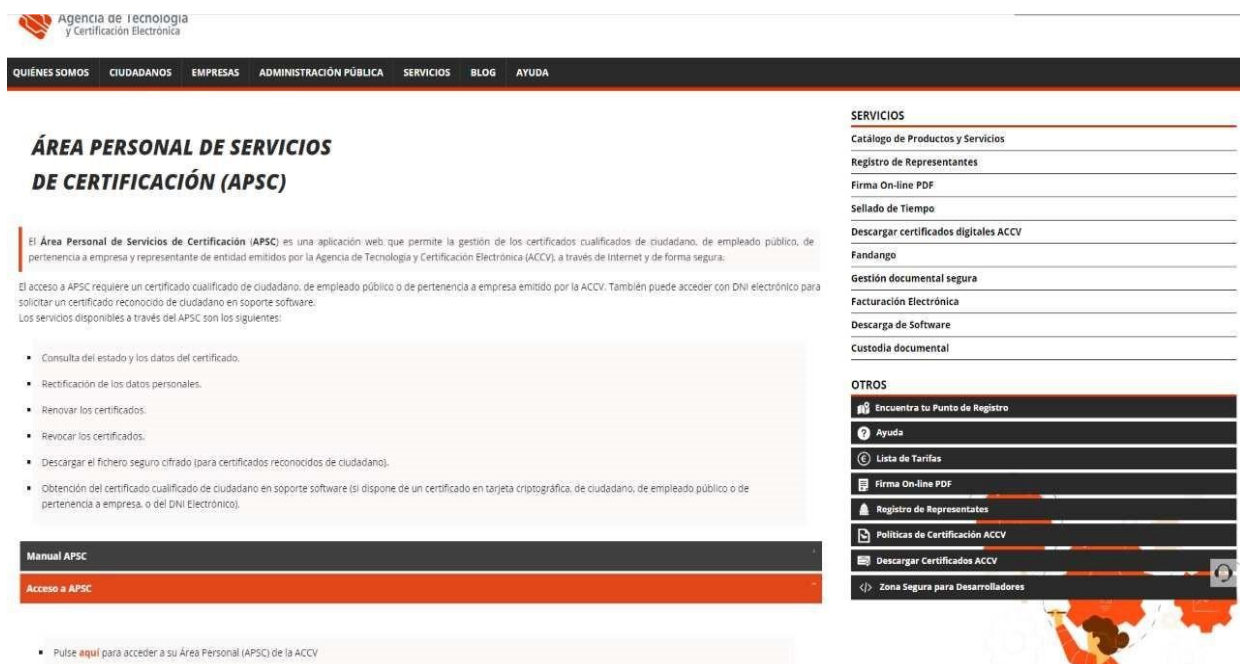
Certificats vàlids per descarregar i descarregar el certificat ACCV en software:

- 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/servicios/apsc/> es troba l'accés a l'**Àrea Personal de Serveis de Certificació (APSC)** i un manual més ampliat d'Usuari.

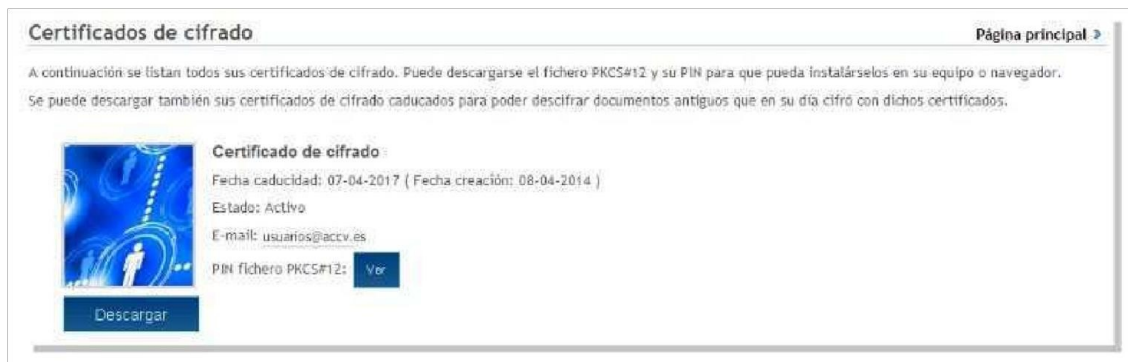


En entrar al APSC amb la seua targeta criptogràfica en l'equip veurà l'opció per a obtenir el seu certificat qualificat de ciutadà en suport software.

## 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 obtenir.

4. Su 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 guardi-ho. En cas contrari, el seu navegador web guardarà el fitxer en la carpeta per defecte per a les descàrregues.

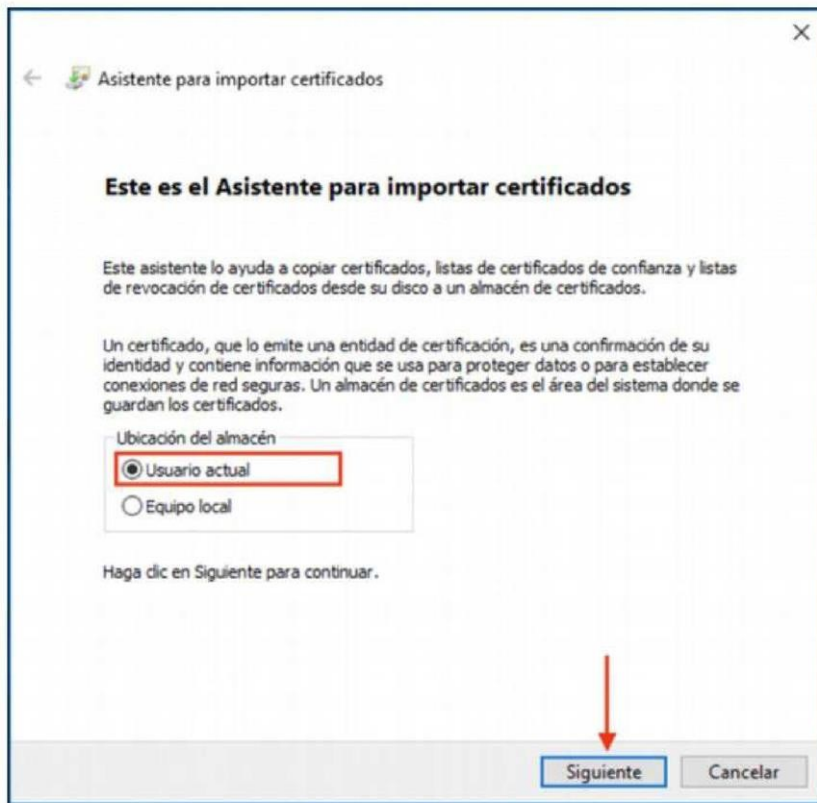
**\*\*\* Si no té un lector de targetes a casa seva, serà aquest arxiu descarregat que necessitarà prendre per instal·lar-lo (Enregistri a USB, envii-li per correu) \* \* \***

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

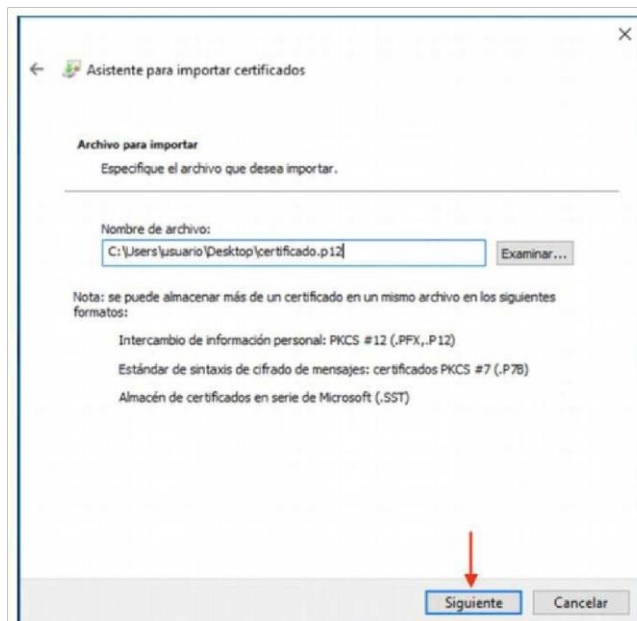
### INSTAL·LACIÓ DE CERTIFICAT DIGITAL EN FITXER: Edge y Chrome

Faça  **doble-clic** 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**:





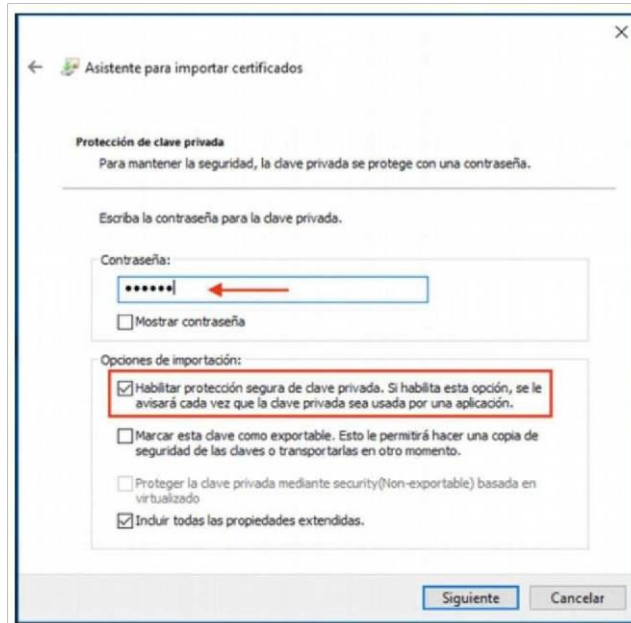
En la pantalla a continuació apareix seleccionat el seu certificat. Prema **Següent**.



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

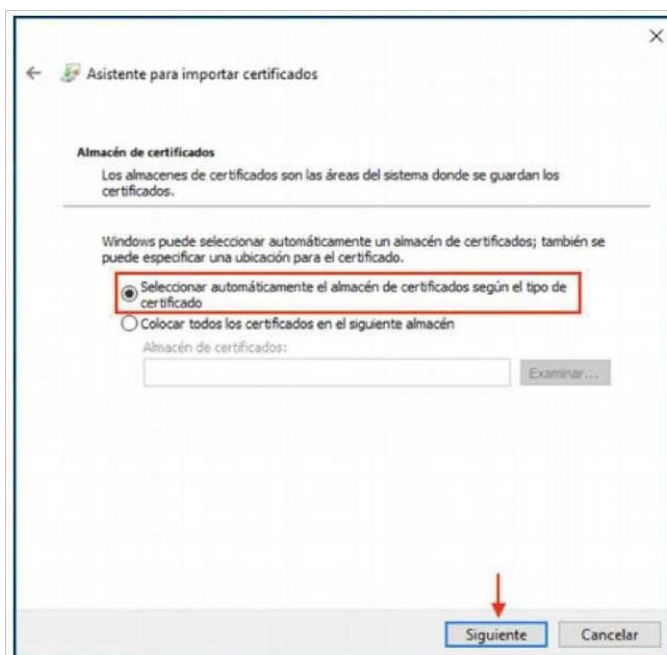
**IMPORTANT:** Marque l'opció Habilitar protecció segura de claus privades.

Prema **Següent:**



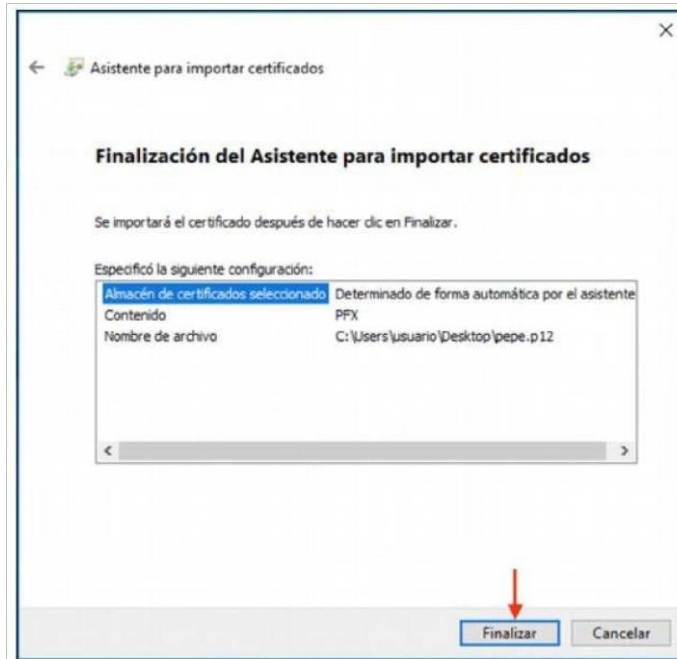
Marque l'opció **Seleccionar automàticament el magatzem de certificats segons el tipus de certificat.**

Prema **Següent.**





Prema **Finalitzar**.



## POSAR UNA CONTRASENYA AL CERTIFICAT (OPCIONAL)

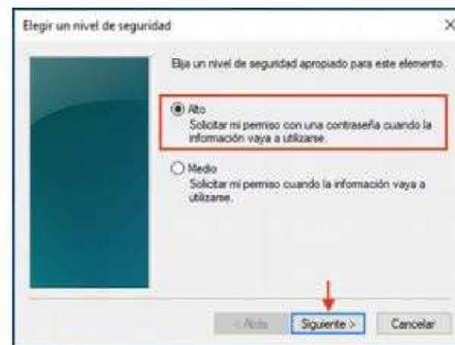
6. A continuación, tiene la opción de definir una contraseña segura que proteja el certificado que está instalando. Si la establece, ésta se le pedirá cuando vaya a emplear el certificado.

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...**

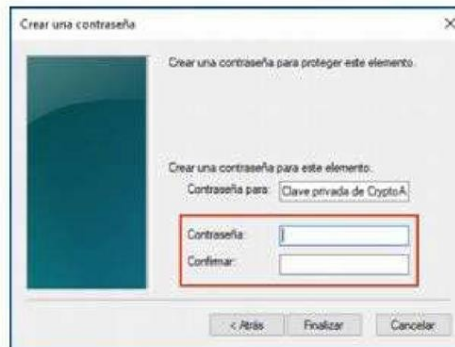


Marque la opción **Alto** y pulse el **Siguiente**.



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.

