CONFIGURACIÓN PARA ACCESO CON CERTIFICADOS ACA PARA SISTEMAS MICROSOFT WINDOWS 10 / WINDOWS 11

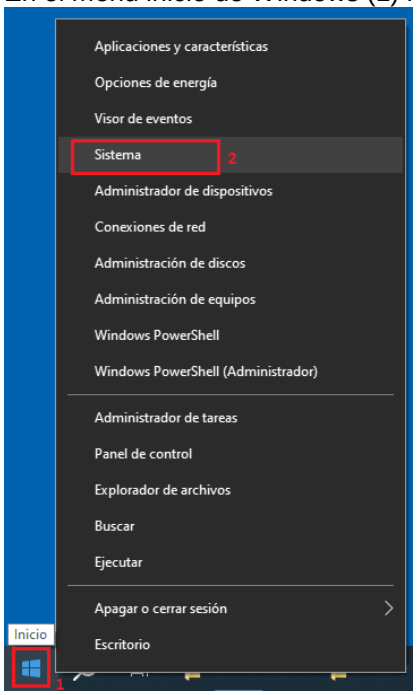
(No hay soporte para versiones anteriores de Microsoft Windows: 7 / 8 / 8.1)

REQUISITOS PREVIOS:

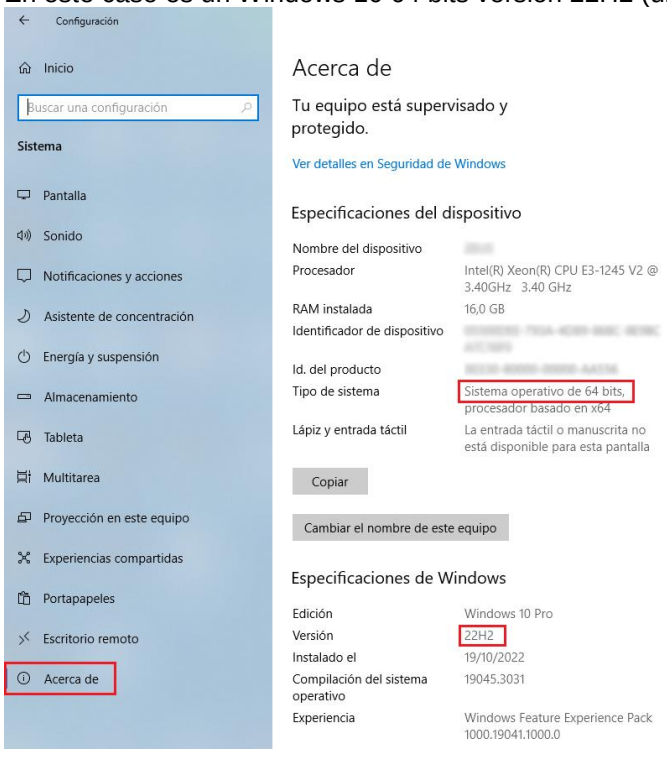
A) CONOCER EL TIPO Y LA VERSIÓN DEL SISTEMA OPERATIVO:

EJEMPLO EN WINDOWS 10:

En el menú inicio de Windows (1) hacemos click con el botón derecho del ratón y pinchamos en Sistema (2):

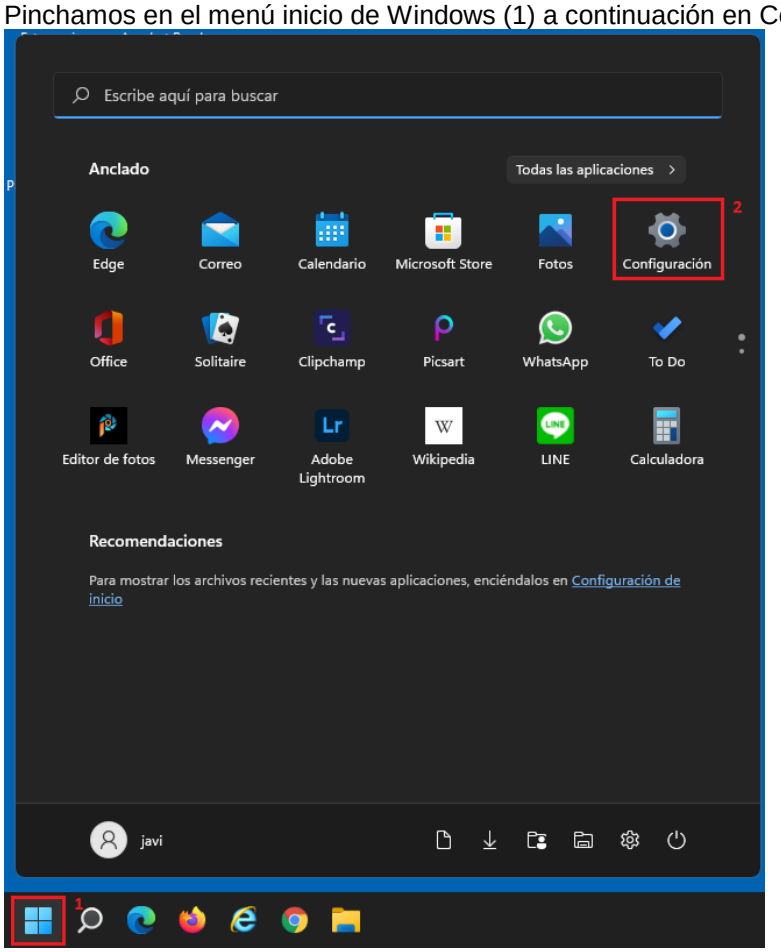


Nos interesa saber si se trata de un sistema operativo de 32 o de 64 bits:
En este caso es un Windows 10 64 bits versión 22H2 (última versión a la fecha)

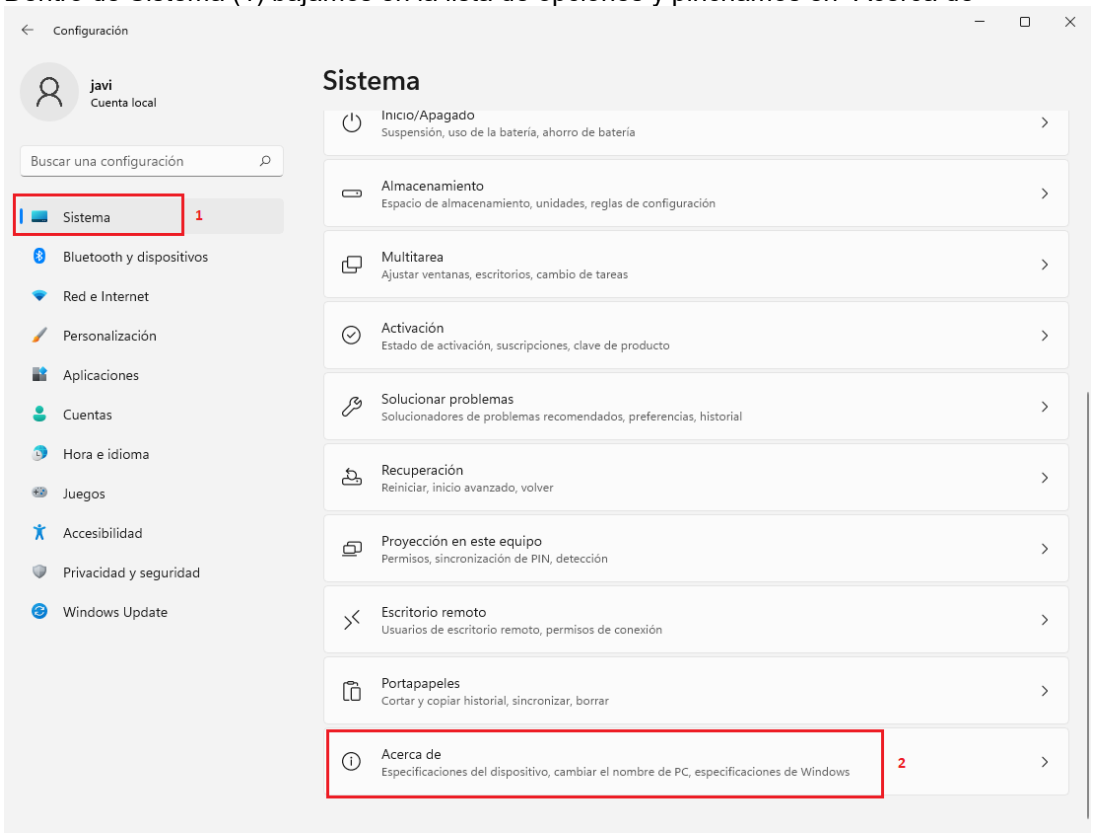


EJEMPLO EN WINDOWS 11:

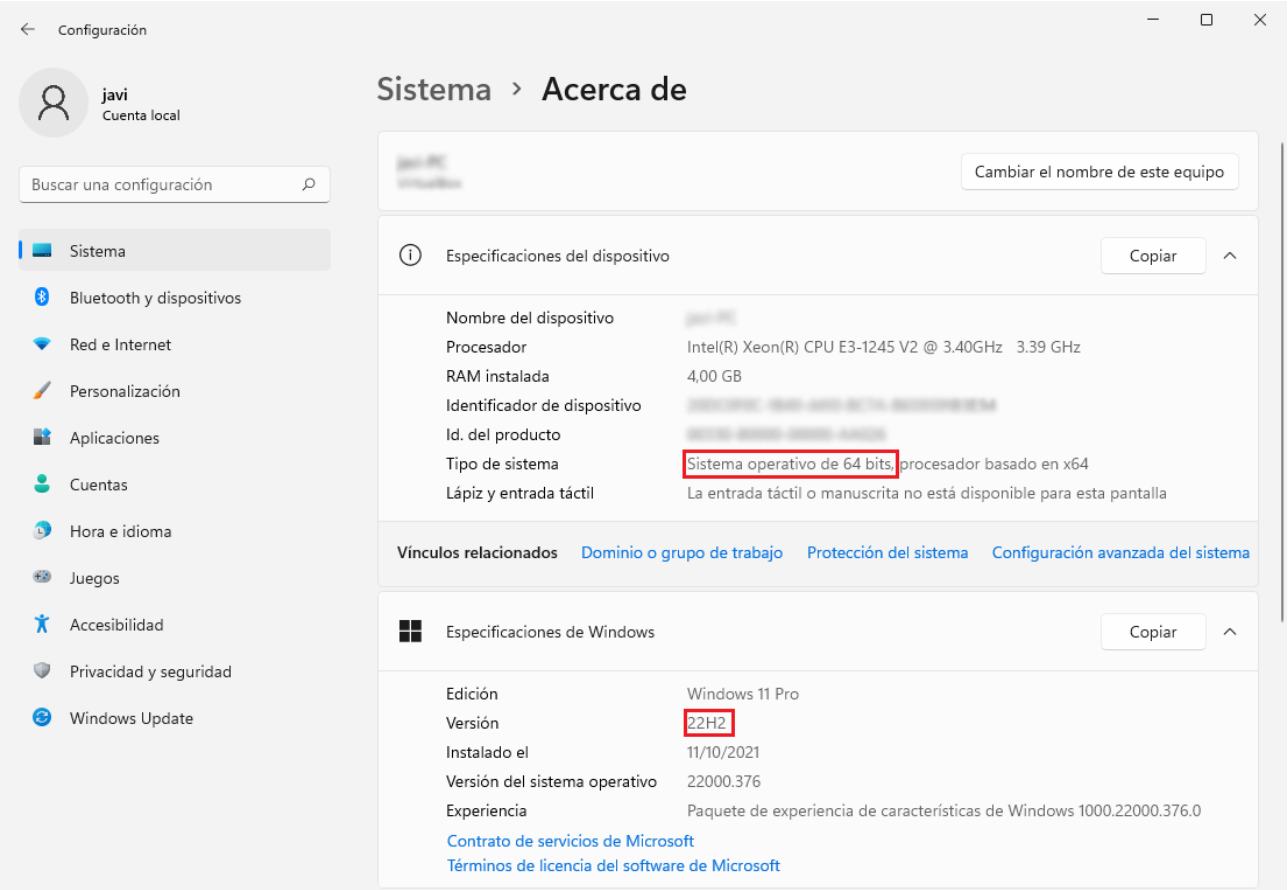
Pinchamos en el menú inicio de Windows (1) a continuación en Configuración (2):



Dentro de Sistema (1) bajamos en la lista de opciones y pinchamos en “Acerca de”



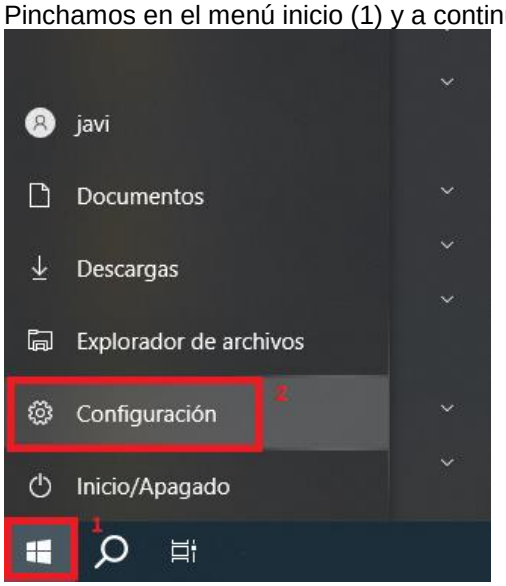
Nos interesa saber si se trata de un sistema operativo de 32 o de 64 bits:
En este caso es un Windows 11 de 64 bits versión 22H2 (última versión a la fecha)



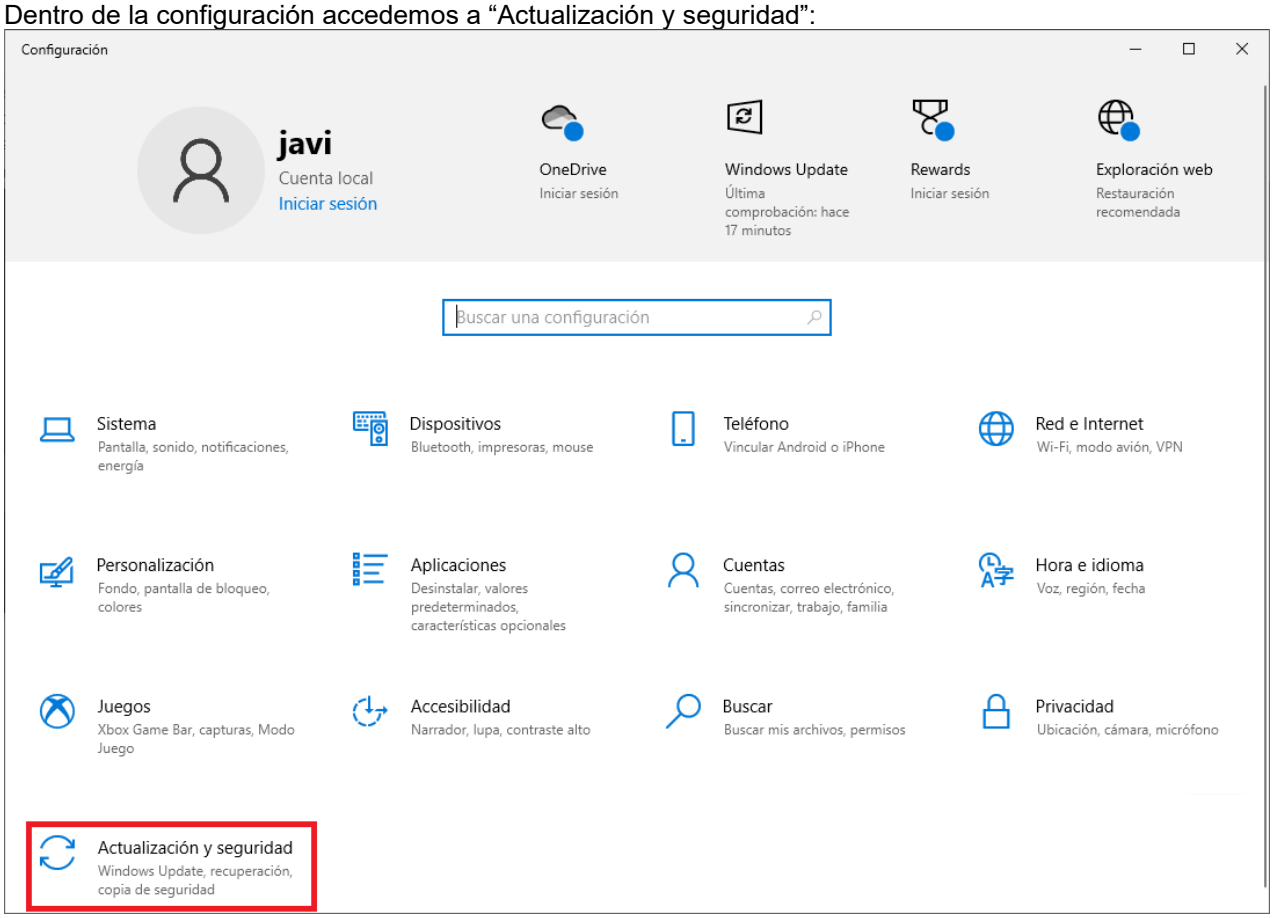
B) ACTUALIZAR EL SISTEMA OPERATIVO A LA ÚLTIMA VERSIÓN DISPONIBLE:

EJEMPLO EN WINDOWS 10:

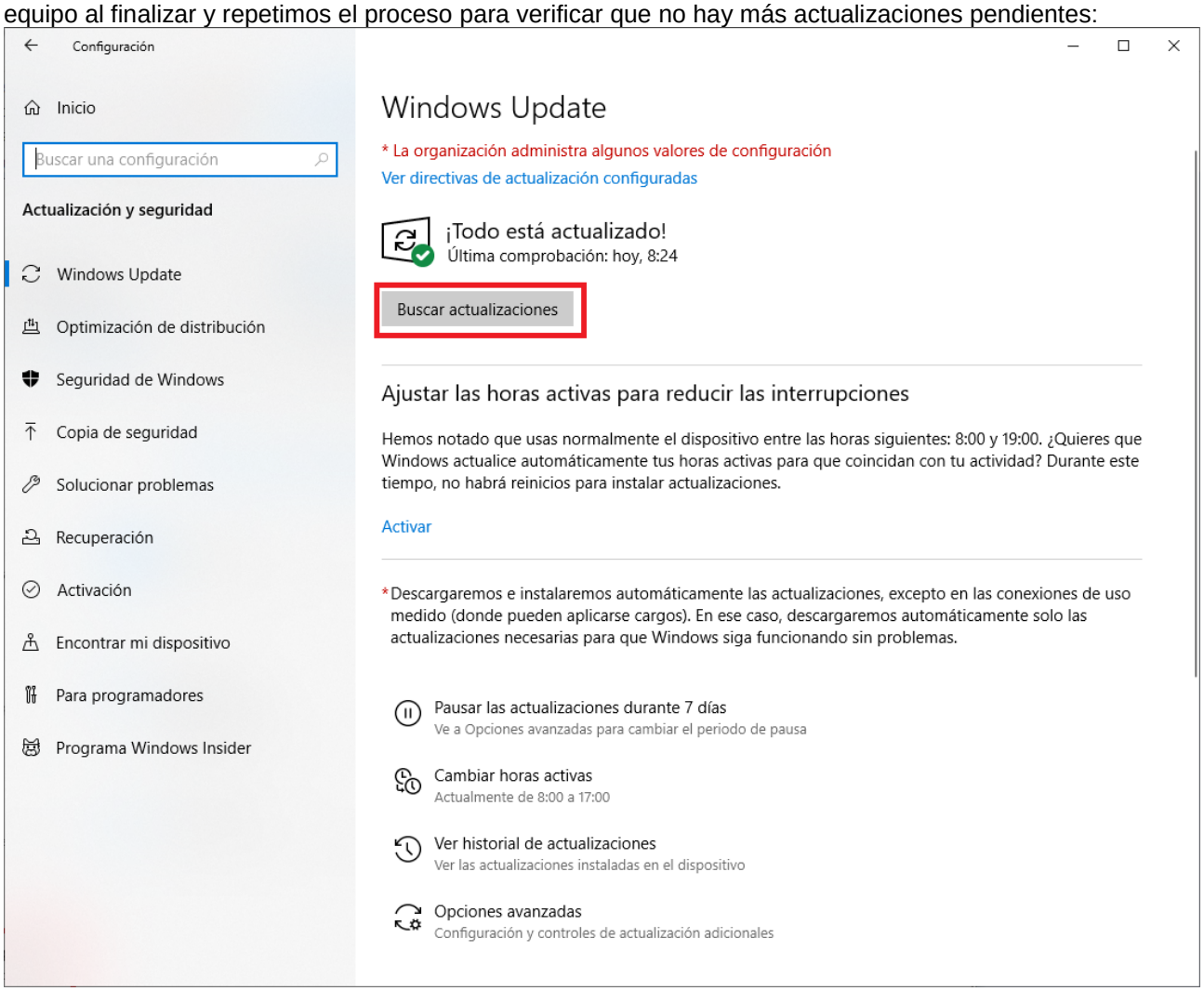
Pinchamos en el menú inicio (1) y a continuación en Configuración (2):



Dentro de la configuración accedemos a “Actualización y seguridad”:

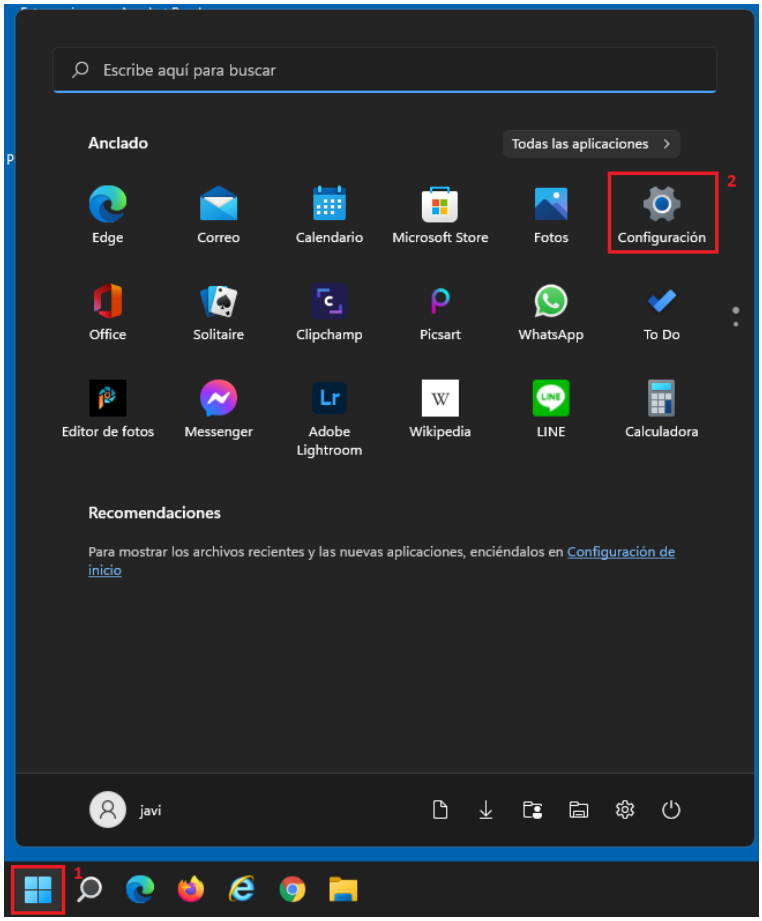


Buscamos todas las actualizaciones disponibles para el S.O. y las instalamos. Si es preciso reiniciamos el equipo al finalizar y repetimos el proceso para verificar que no hay más actualizaciones pendientes:

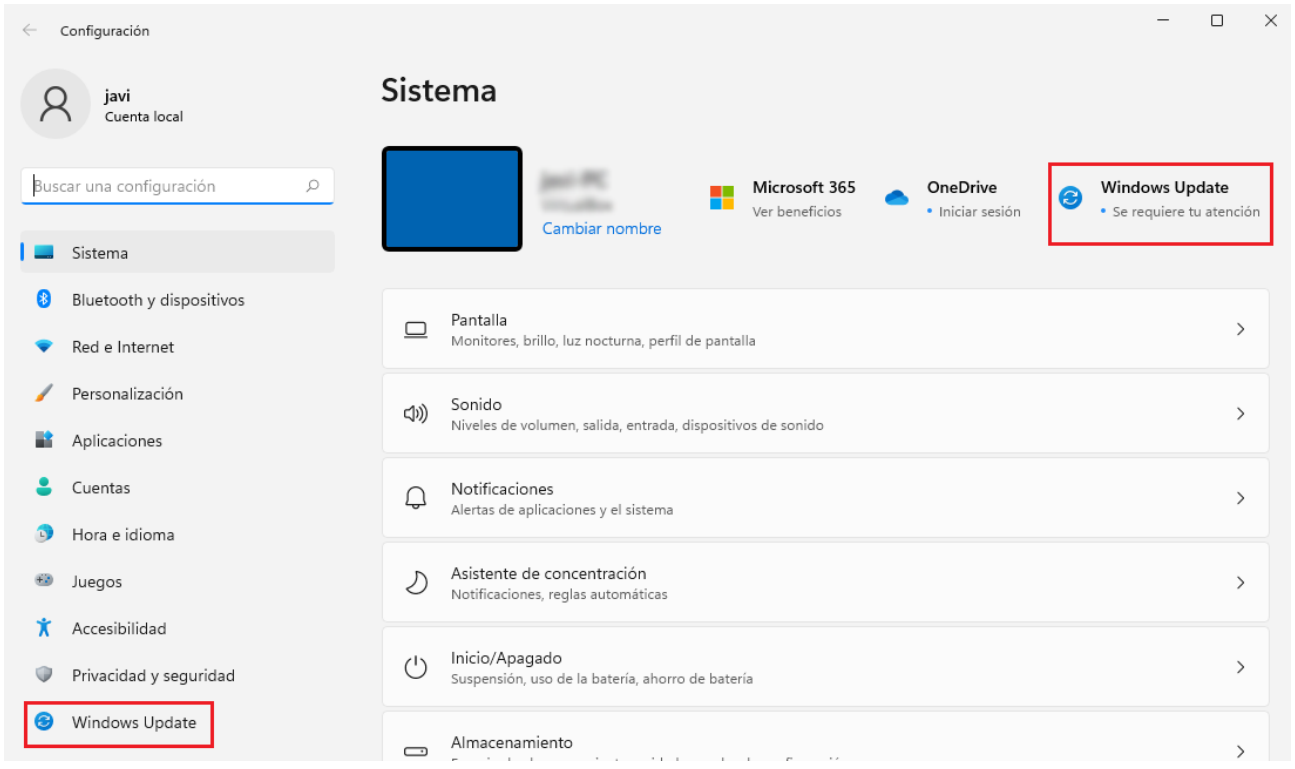


EJEMPLO EN WINDOWS 11:

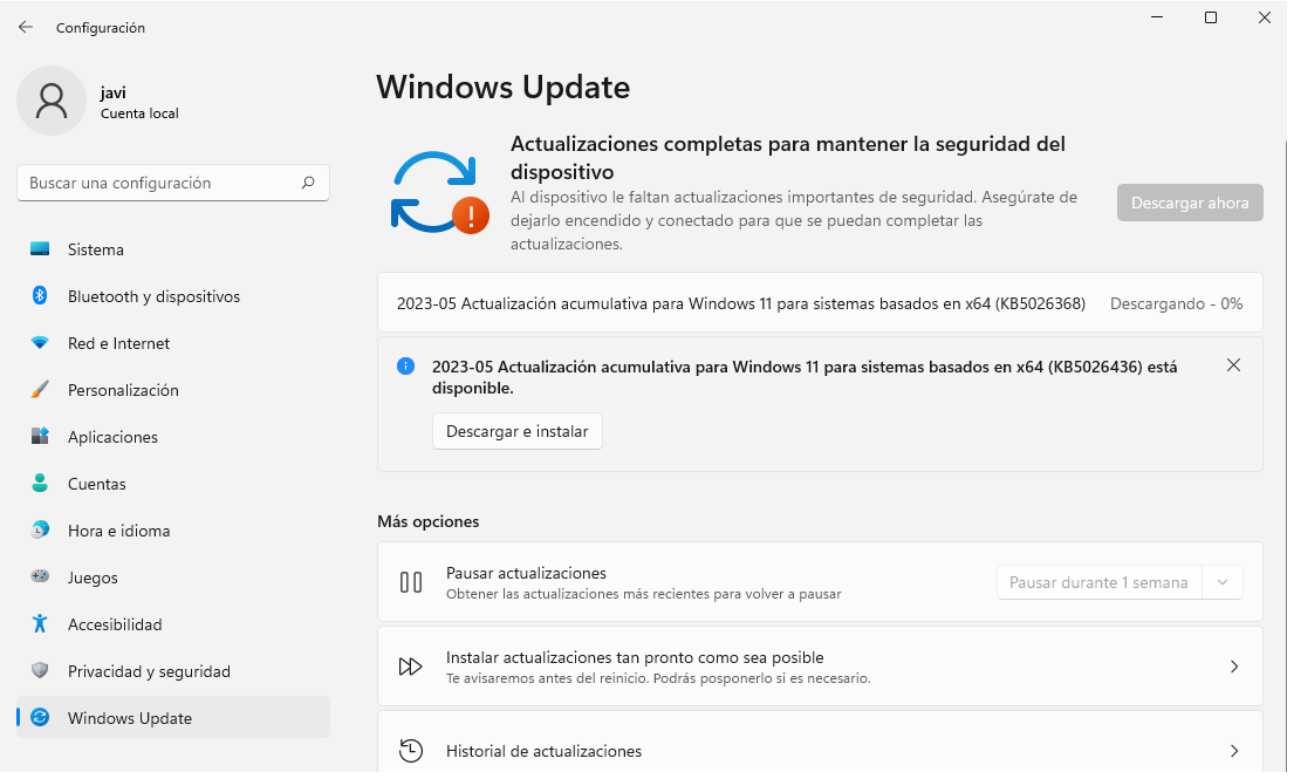
Pinchamos en el menú inicio (1) y a continuación en Configuración (2):



Pinchamos en Windows Update:



Buscamos todas las actualizaciones disponibles para el S.O. y las instalamos. Si es preciso reiniciamos el equipo al finalizar y repetimos el proceso para verificar que no hay más actualizaciones pendientes:



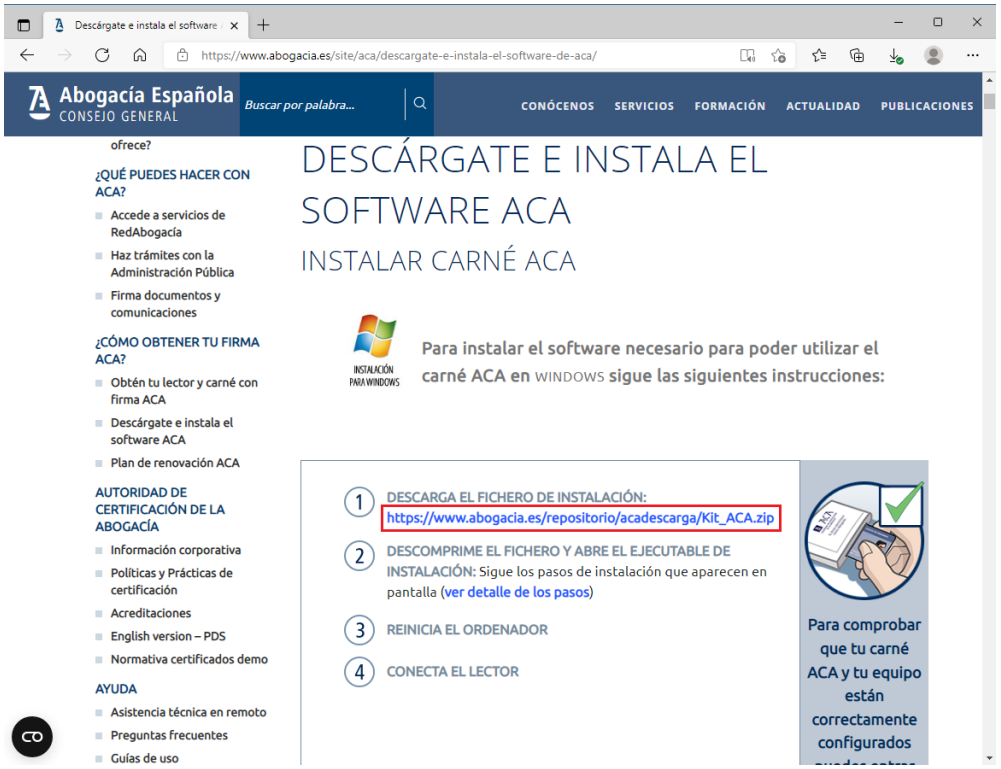
SOFTWARE ACA:

1.- INSTALACIÓN DEL SOFTWARE BIT4ID-PKI MANAGER QUE GESTIONA LA TARJETA ACA:

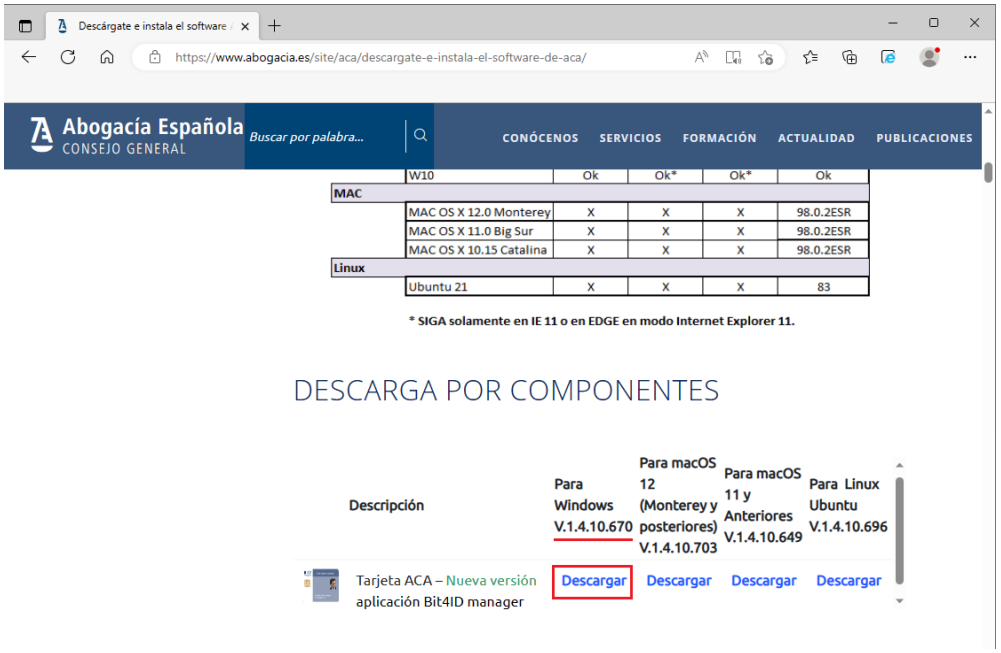
¿Dónde descargar la última versión del software para la tarjeta ACA?

https://www.abogacia.es/site/aca/descargate-e-instala-el-software-de-aca/

Si no tenemos ninguna versión previa de Bit4id instalada, descargamos e instalamos el Kit ACA:



A continuación, descargamos e instalamos la última actualización disponible:



LECTORES DE TARJETAS:

No todos los lectores funcionan, motivo por el que ACA recomienda el uso de lectores Bit4id. Tanto desde RedAbogacía como desde el Colegio no se proporciona soporte para lectores de otros fabricantes.

¿Dónde adquirir un lector Bit4id?

On-line:

- **PC-Componentes**
  https://www.pccomponentes.com/buscar/?query=bit4id&or-relevance
- **Compra en la Web del fabricante Bit4id:**
  https://shop.bit4id.com/es/producto/minilector-evo/
- **Amazon**
  https://www.amazon.es/s?k=bit4id+mini+lector+evo

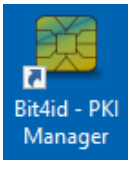
Tienda física en A Coruña:

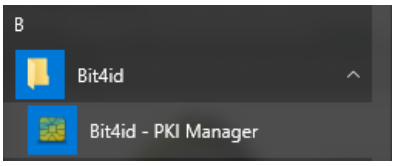
- **CAYLIS** Avda. de Arteixo, 12 - 15004, A Coruña
  Teléfono: 881 990 441 Email: info@caylis.es

También existen teclados del fabricante Bit4id y del fabricante Cherry que incorporan lectores de tarjeta compatibles con ACA:

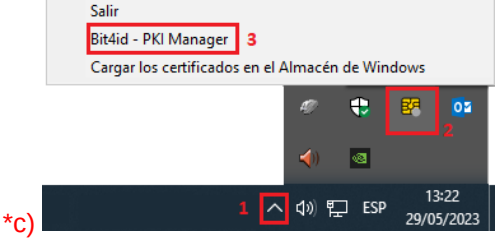
Acceso al Programa de Gestión de la Tarjeta (Bit4id - PKI Manager):

a) Puede acceder desde el Acceso directo creado en el escritorio de Windows por el programa de instalación, **b)** Desde el Menú Inicio de Windows: Aplicaciones -> Bit4id - PKI Manager

*a) 

*b) 

c) Desde la barra de herramientas de Windows click en (1), click botón derecho en (2) y click en (3)

*c) 

2.- CAMBIO Y DESBLOQUEO DEL PIN, INFORMACIÓN DEL CERTIFICADO Y DE LA TARJETA:

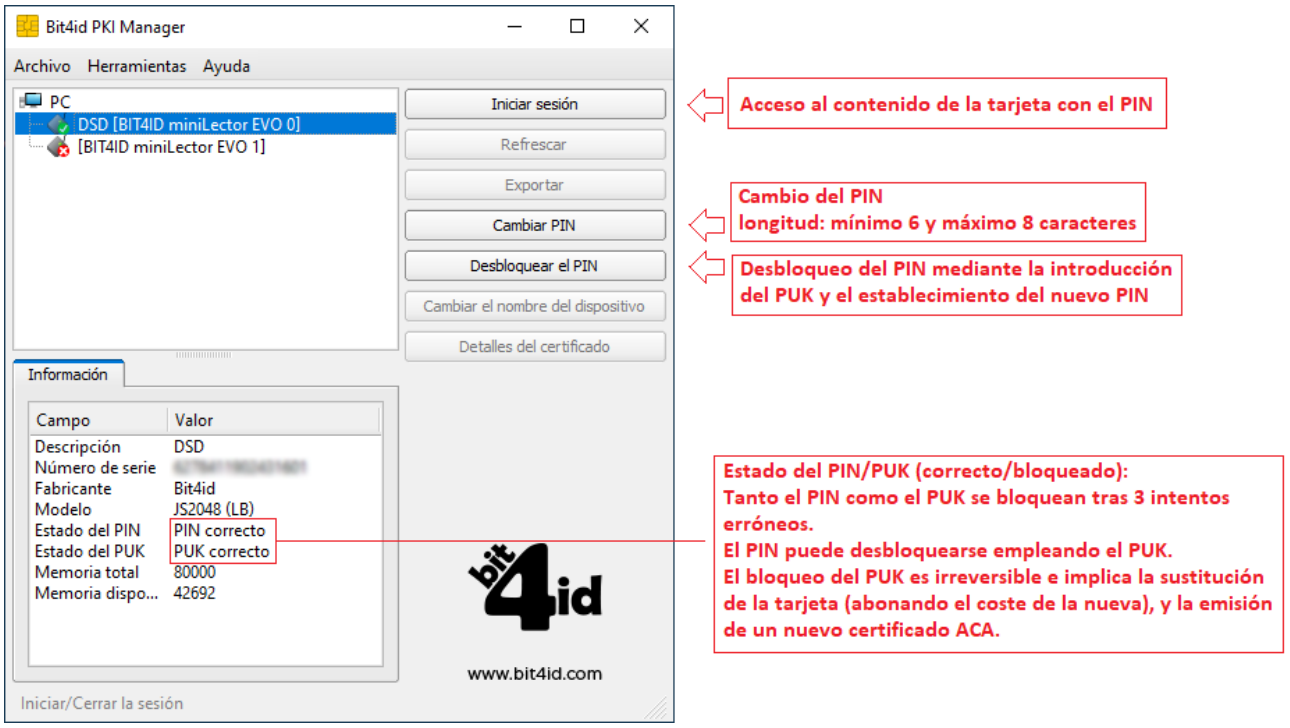
Para cualquier operación de firma o autenticación mediante el certificado ACA se le pedirá que introduzca el PIN de la tarjeta. Recuerde que la clave privada del certificado NO es exportable, por ese motivo no se puede instalar en los equipos. Siempre es necesario el uso del carné físico para cualquier operación con el certificado ACA. Su funcionamiento es como el DNI electrónico, no como los certificados instalables de la FNMT.

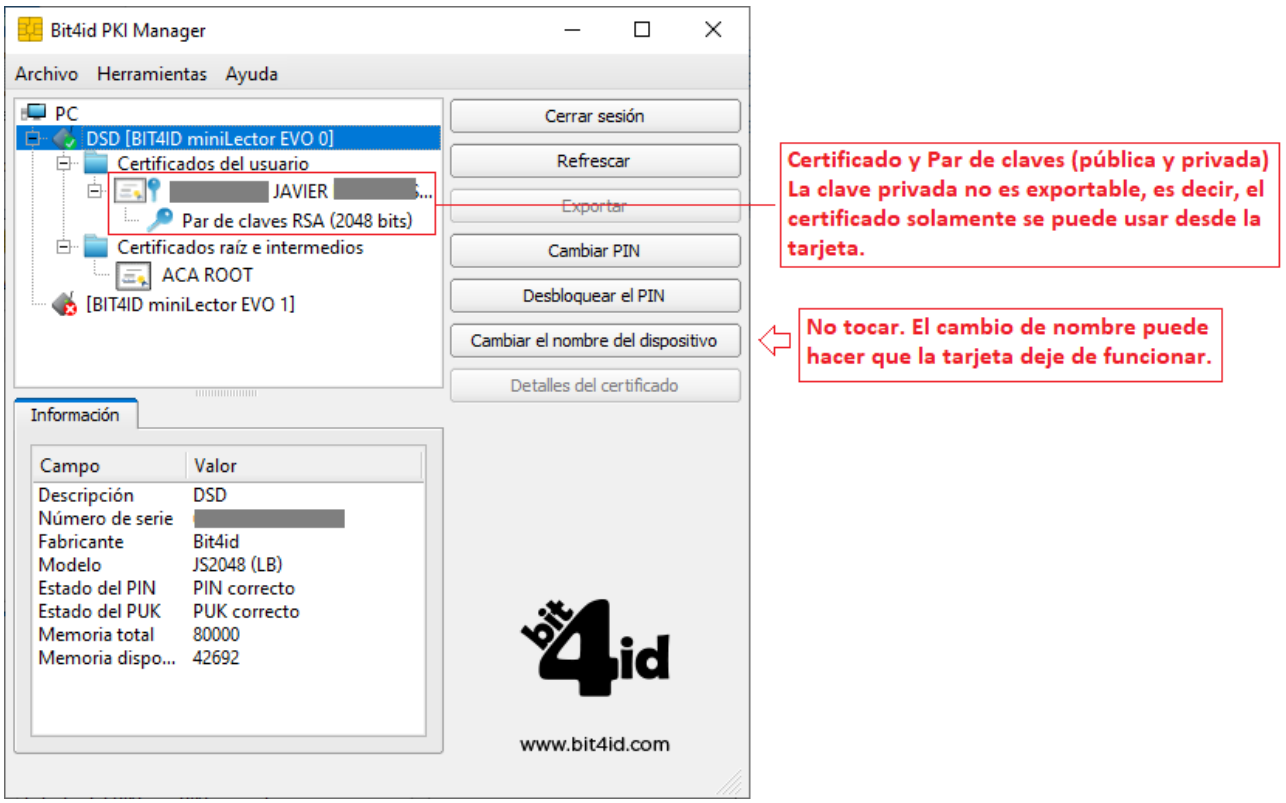
- Longitud del PIN: **entre 6 y 8 caracteres** (números, letras -distingue mayúsculas- o símbolos)
- Longitud del PUK: **8 caracteres** (números, letras o símbolos)

EN NINGÚN CASO PONGA UN PIN O UN PUK DE MÁS O MENOS CARACTERES DE LOS INDICADOS, YA QUE LUEGO NO FUNCIONARÁ LA TARJETA.

Si se equivoca tres veces al introducir el PIN la tarjeta se bloqueará. Para desbloquearla deberá usar el Programa de Gestión de la Tarjeta. Se le pedirá el PUK de la tarjeta para su desbloqueo.

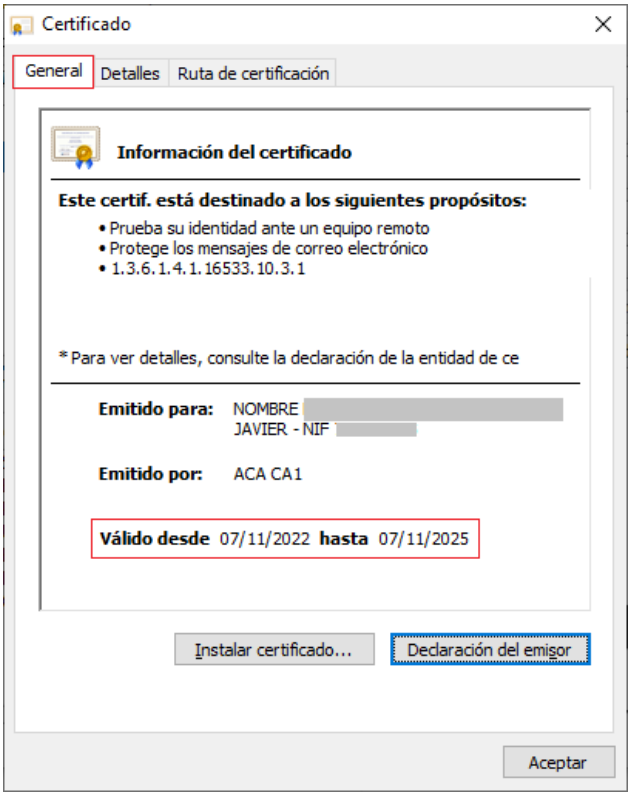
Aviso: **Si se introduce un PUK erróneo tres veces la tarjeta se bloqueará irreversiblemente**. En tal caso, deberá solicitar un nuevo certificado ACA en el Colegio y abonar el importe de la nueva tarjeta.





Al hacer doble click sobre el certificado podemos verificar, entre otros, las fechas de emisión y caducidad del certificado.

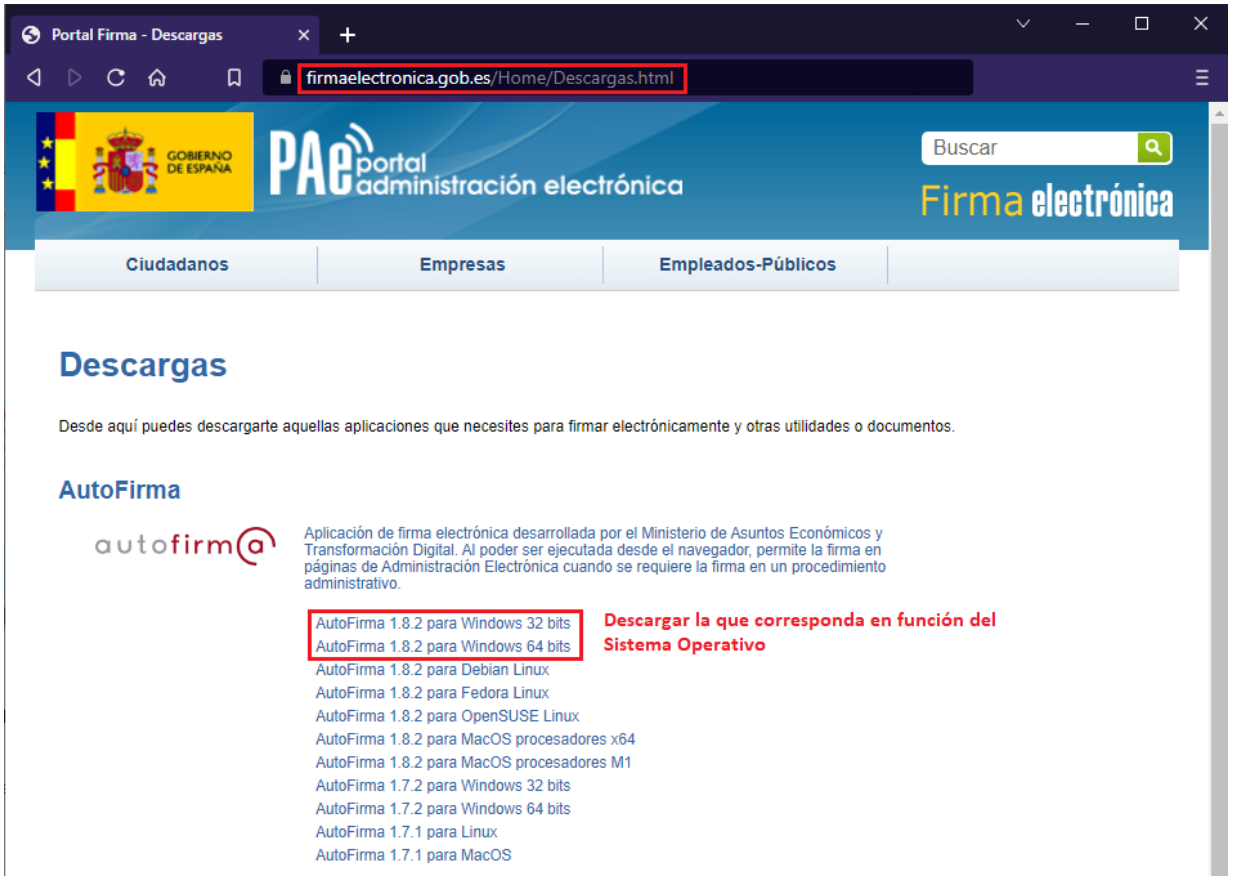
Insistimos en que la opción “Instalar certificado” NO instalará el certificado y no permitirá su posterior uso sin la tarjeta ya que la clave privada no es exportable. NO funciona como los certificados software de la FNMT (.pfx)



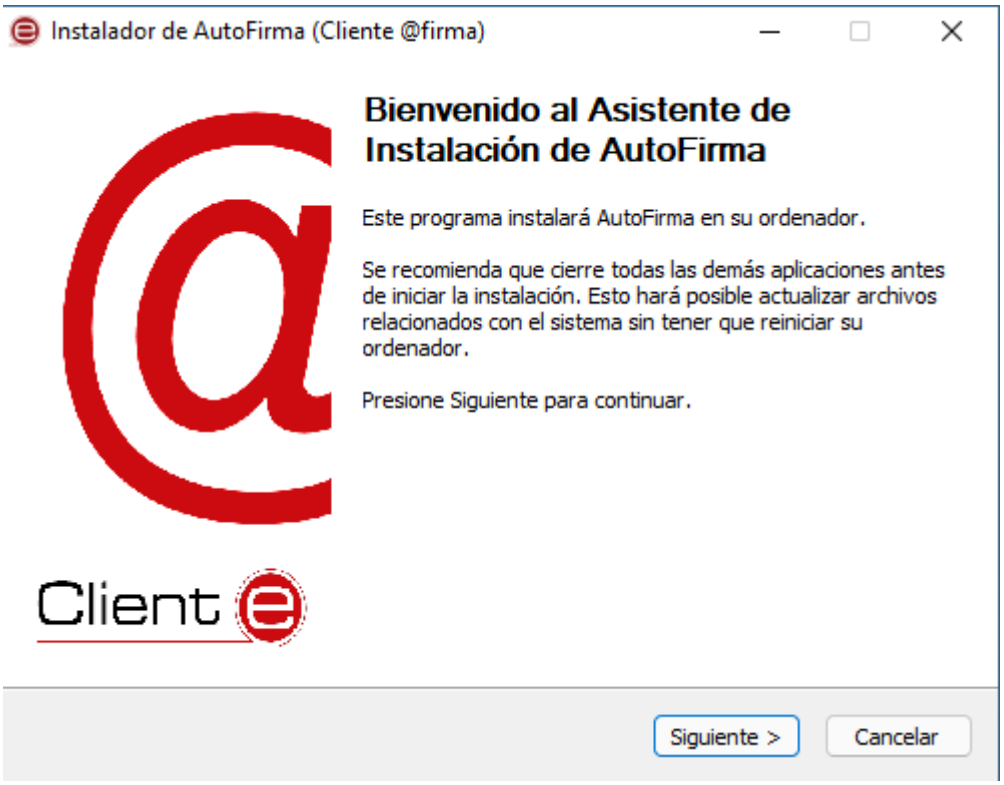
AUTOFIRMA:

Descargamos la versión que se corresponda con nuestro sistema operativo (32 bits o 64 bits) desde la página oficial:

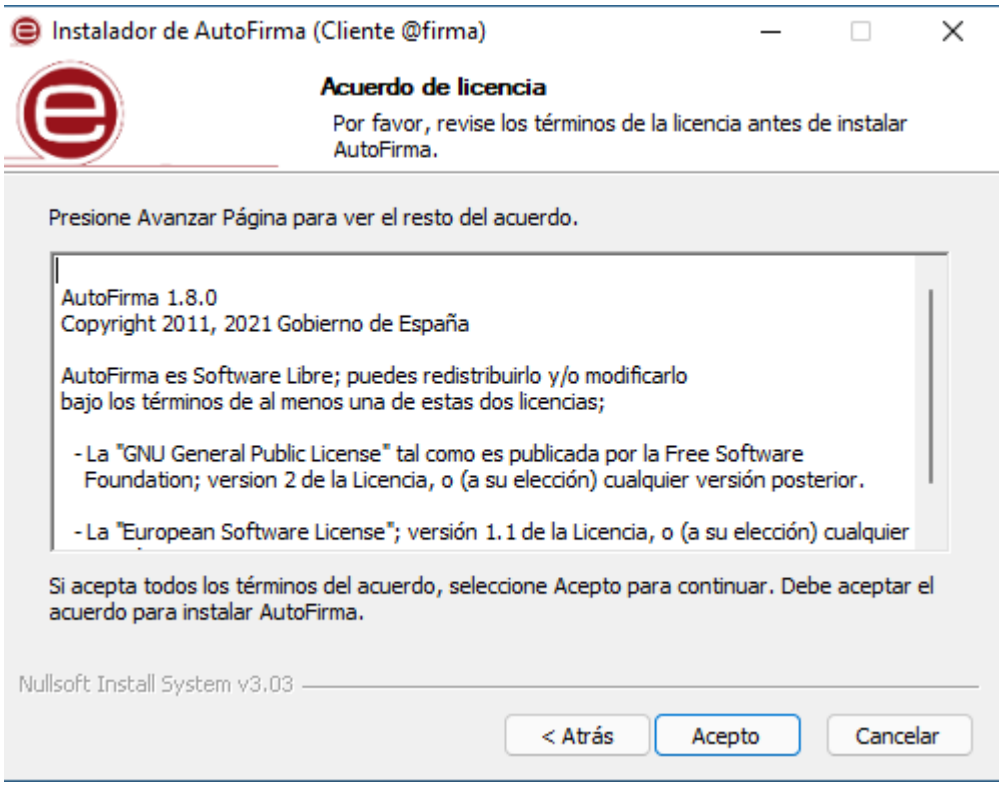
https://firmaelectronica.gob.es/Home/Descargas.html



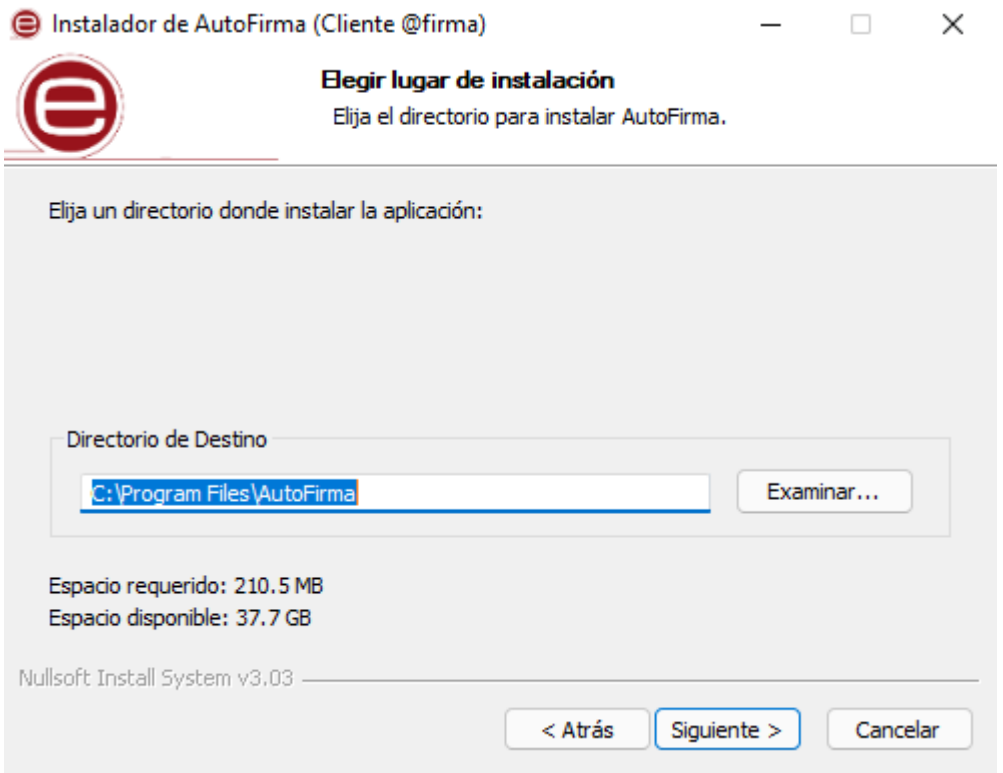
Una vez descargado **CERRAMOS TODOS LOS NAVEGADORES** y ejecutamos el instalador. Comenzamos la instalación haciendo click en “Siguiente”:



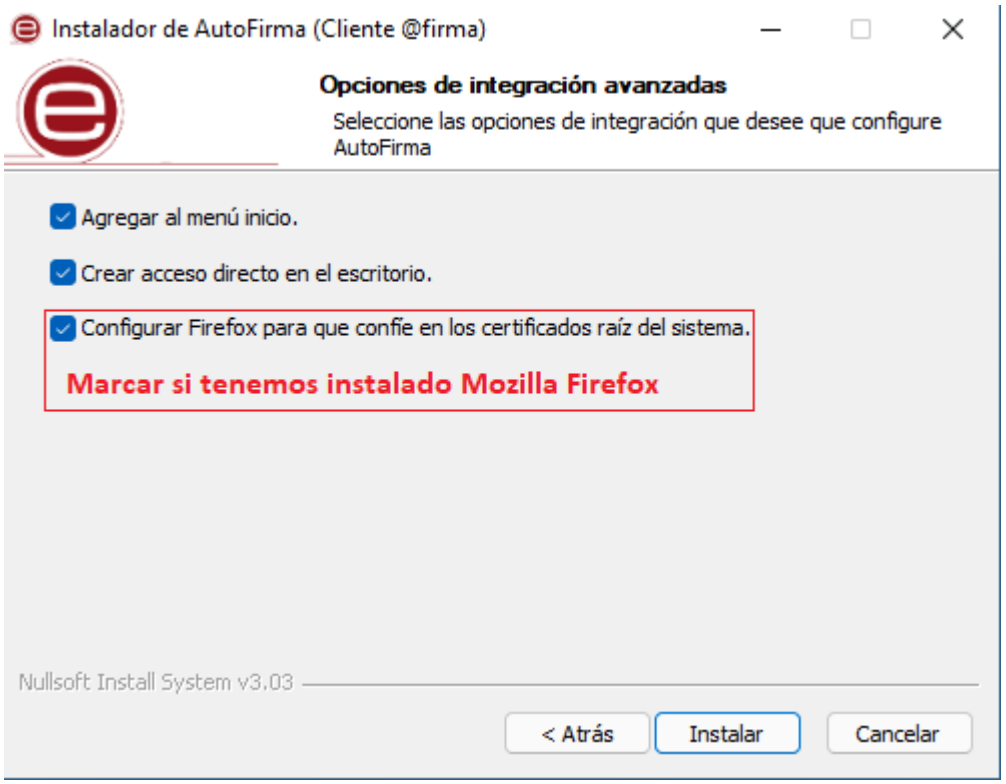
Aceptamos los términos de la licencia:



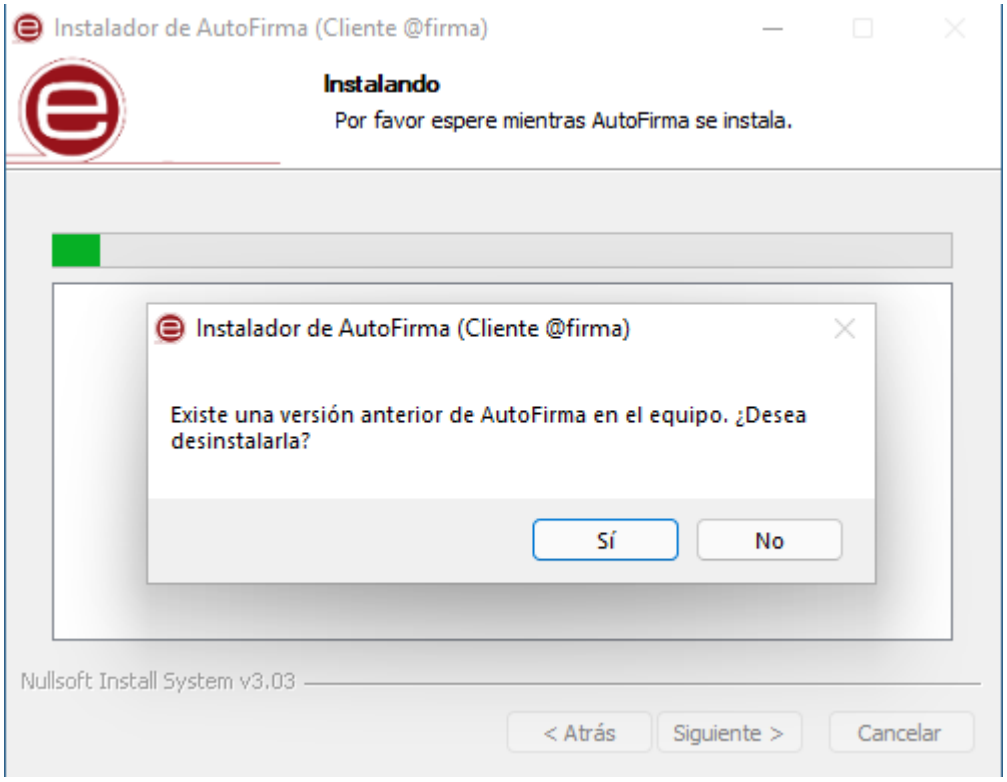
Dejamos como carpeta de instalación la que viene por defecto y continuamos:



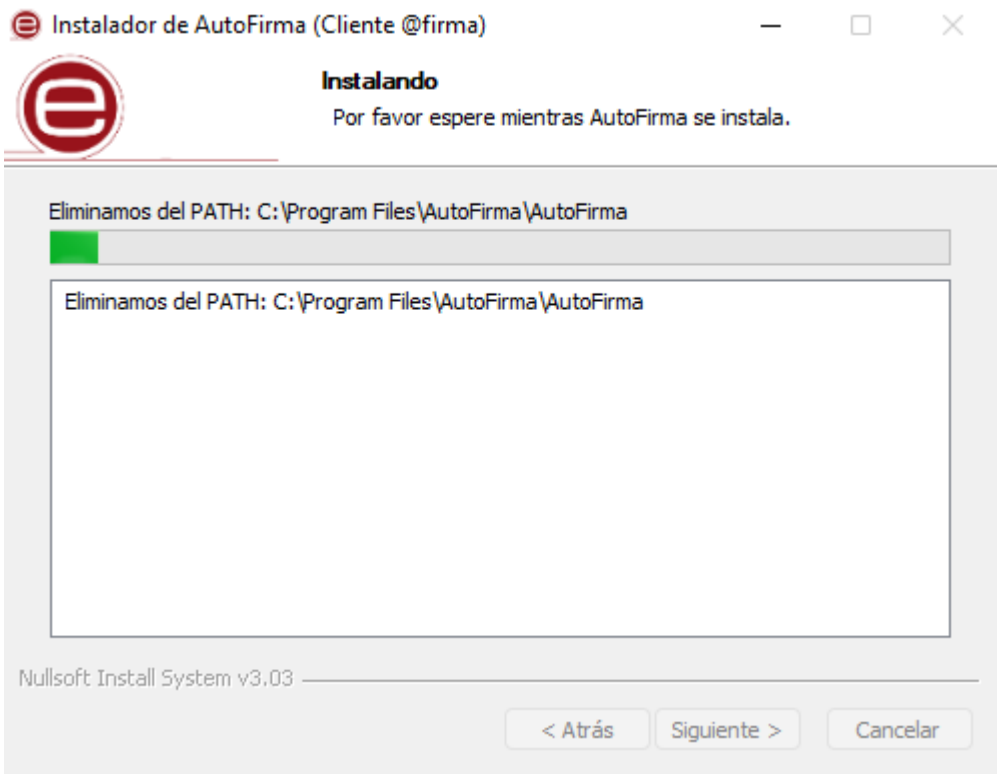
Si tenemos instalado el navegador **Mozilla Firefox** debemos marcar la casilla correspondiente:



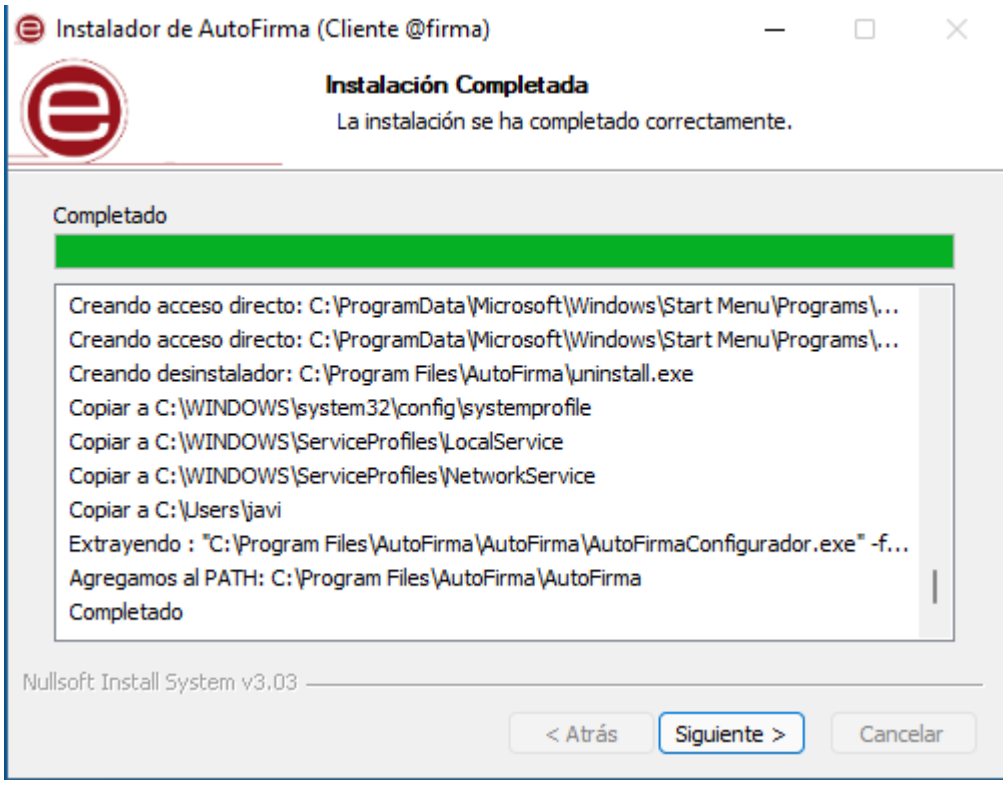
Si ya teníamos una versión antigua de Autofirma instalada se detectará y debemos desinstalarla:



Esperamos a que Autofirma se instale:



Finalizada la instalación hacemos click en “Siguiente”:

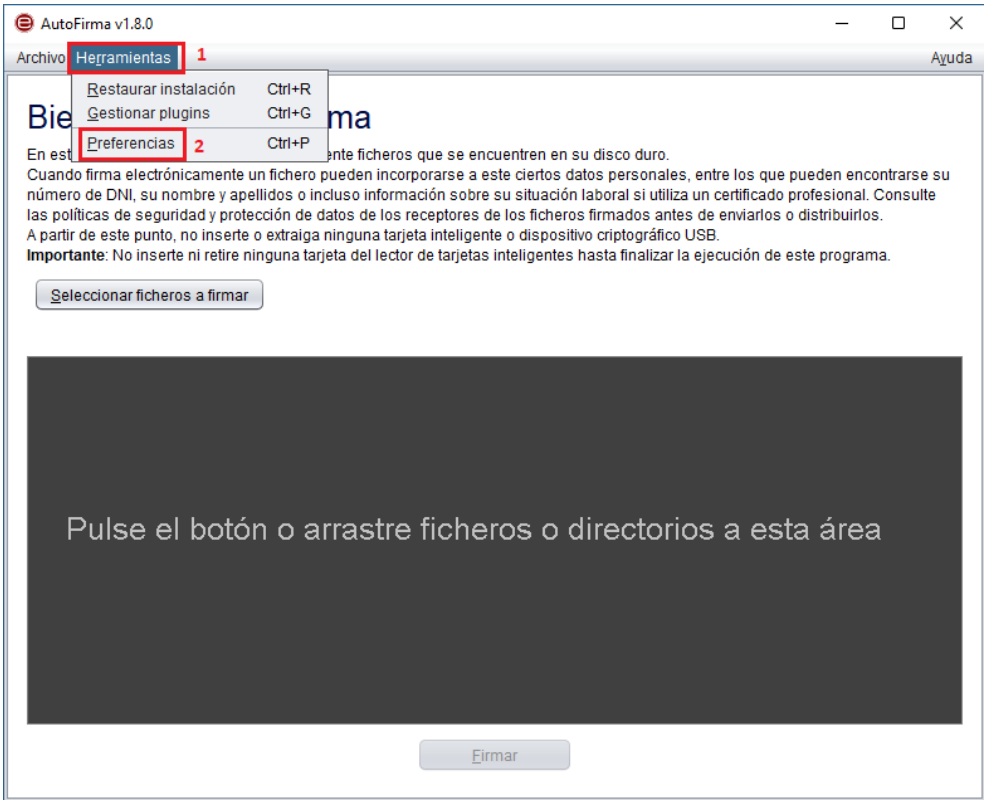


Para finalizar hacemos click en “Terminar”:

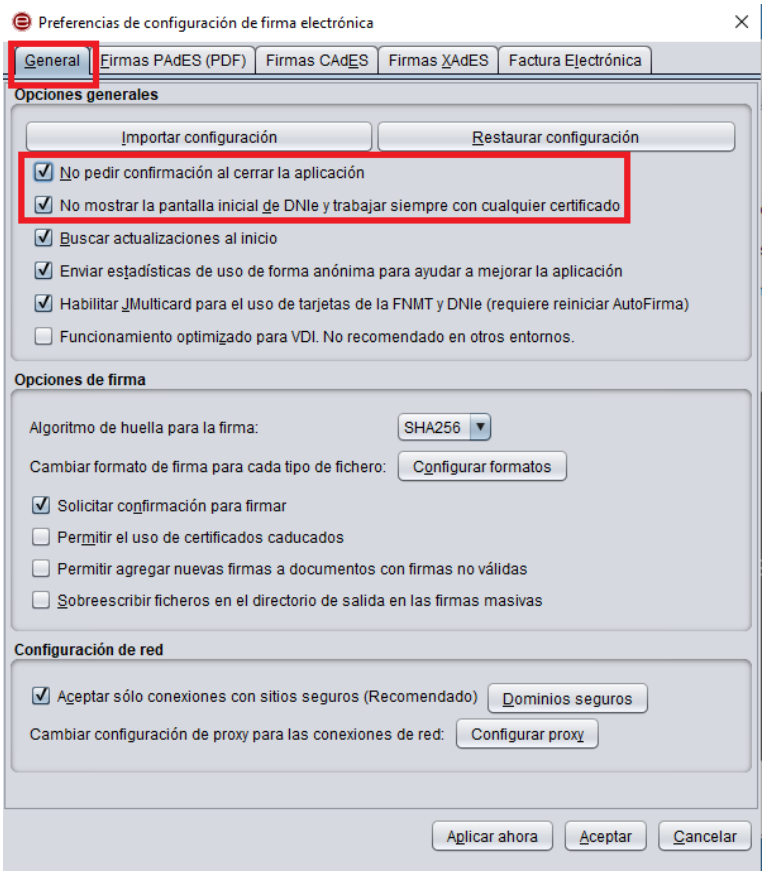
Abrimos Autofirma por primera vez tras la instalación:

Si la tarjeta ACA está conectada y/o disponemos de algún otro certificado instalado nos mostrará la siguiente ventana. Marcamos la opción “No volver a mostrar esta pantalla…” y pinchamos en “Usar cualquier certificado”

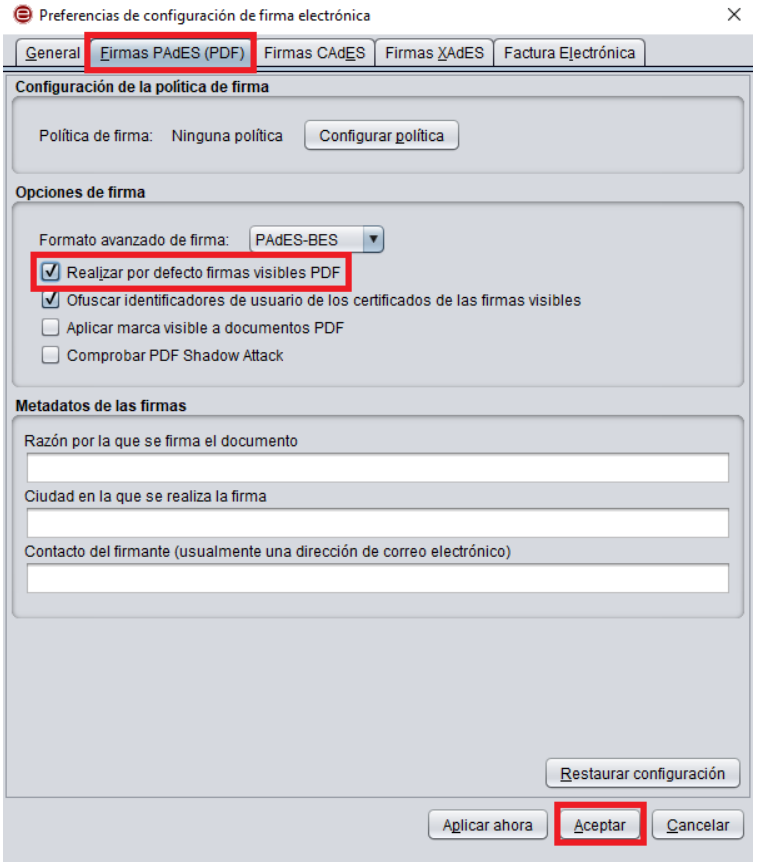
En el menú superior pinchamos en Herramientas (1) y a continuación en Preferencias (2):



En la primera pestaña verificamos que las 2 primeras casillas están seleccionadas, si no lo están las marcamos. No tocamos nada más en esta ventana:



En la segunda pestaña verificamos que está marcada la casilla “Realizar por defecto firmas visibles PDF” y aceptamos los cambios:



LexNET WEB:

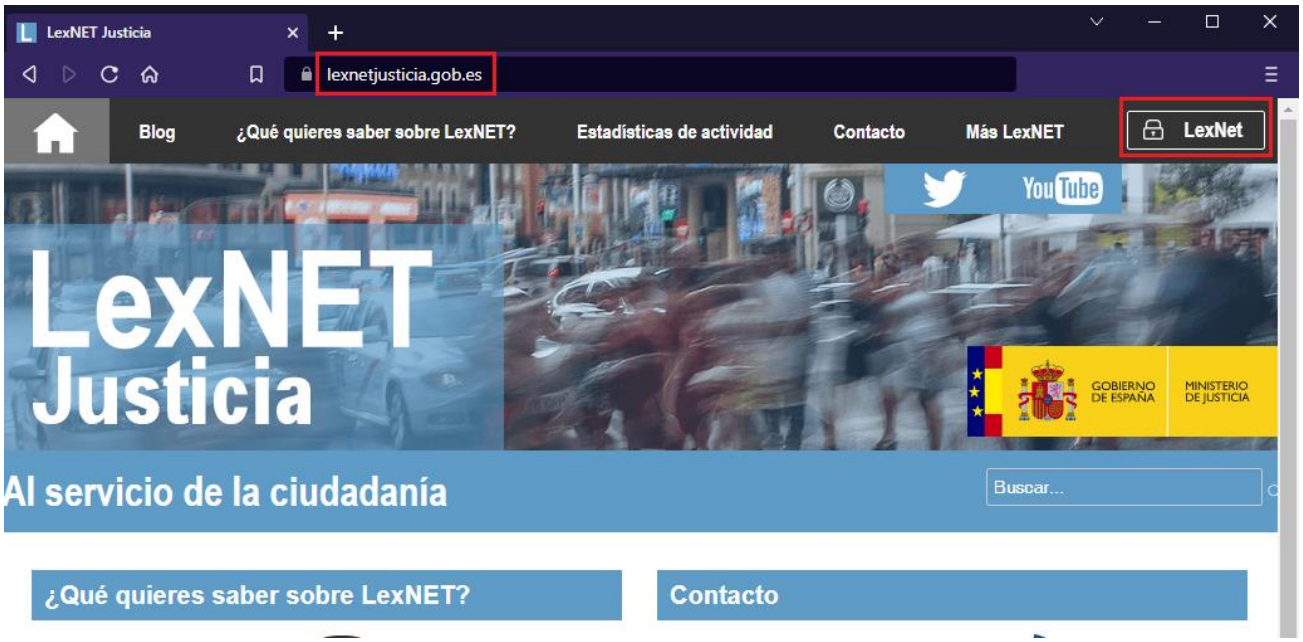
El acceso a LexNET, desde que el 08/05/2023 que dejase de funcionar la versión de escritorio, solamente es posible a mediante el uso de un navegador: Microsoft Edge, Google Chrome, Mozilla Firefox, …

Salvo Google Chrome que no lo permite y hay que eliminar el historial de manera manual con cierta frecuencia, en el resto de navegadores se recomienda configurar la eliminación automática del historial de navegación cada vez que se cierren, para evitar problemas con el acceso a las páginas seguras con certificado.

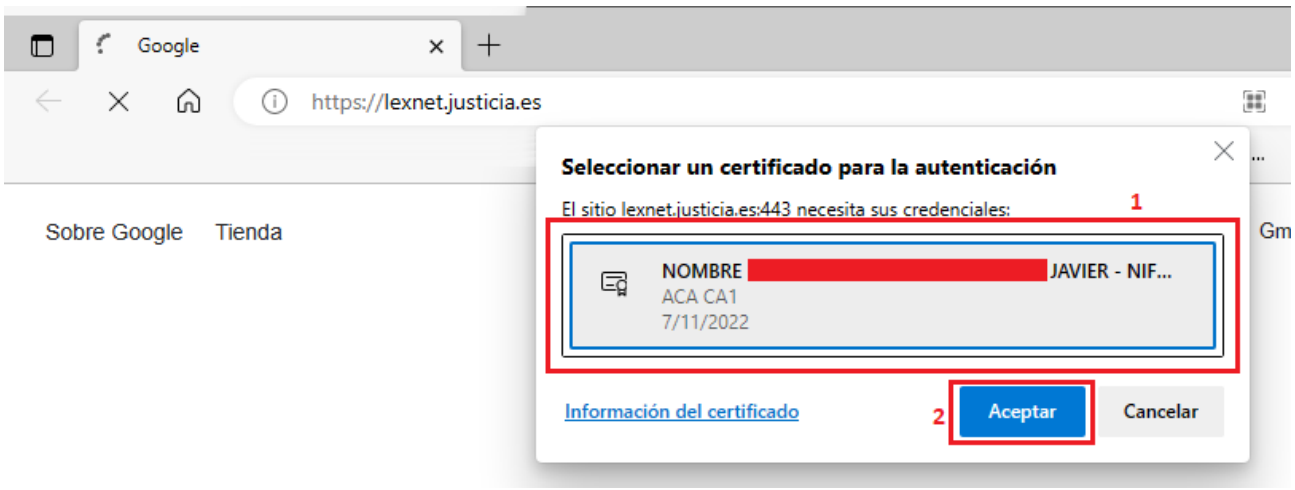
Acceso a LexNET:

La dirección web de acceso a LexNET es: https://lexnet.justicia.es/

Este acceso está disponible también en el menú superior de la página informativa sobre LexNET del ministerio de justicia: https://lexnetjusticia.gob.es/



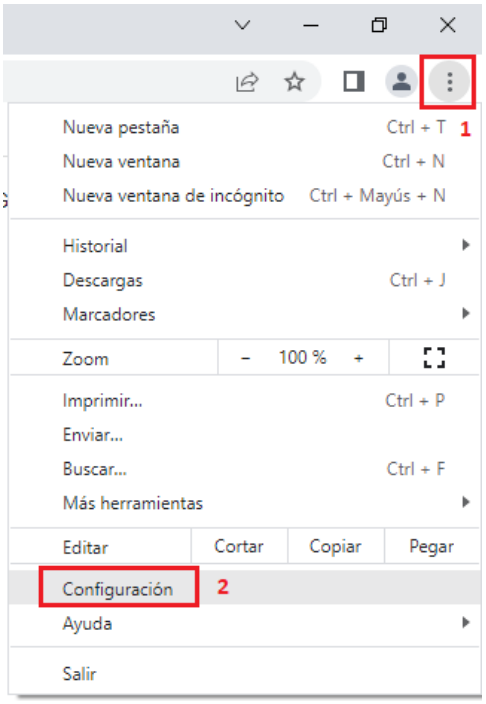
¡AVISO!: En el navegador Microsoft EDGE es siempre necesario seleccionar el certificado (1) antes de hacer click en el botón aceptar (2):



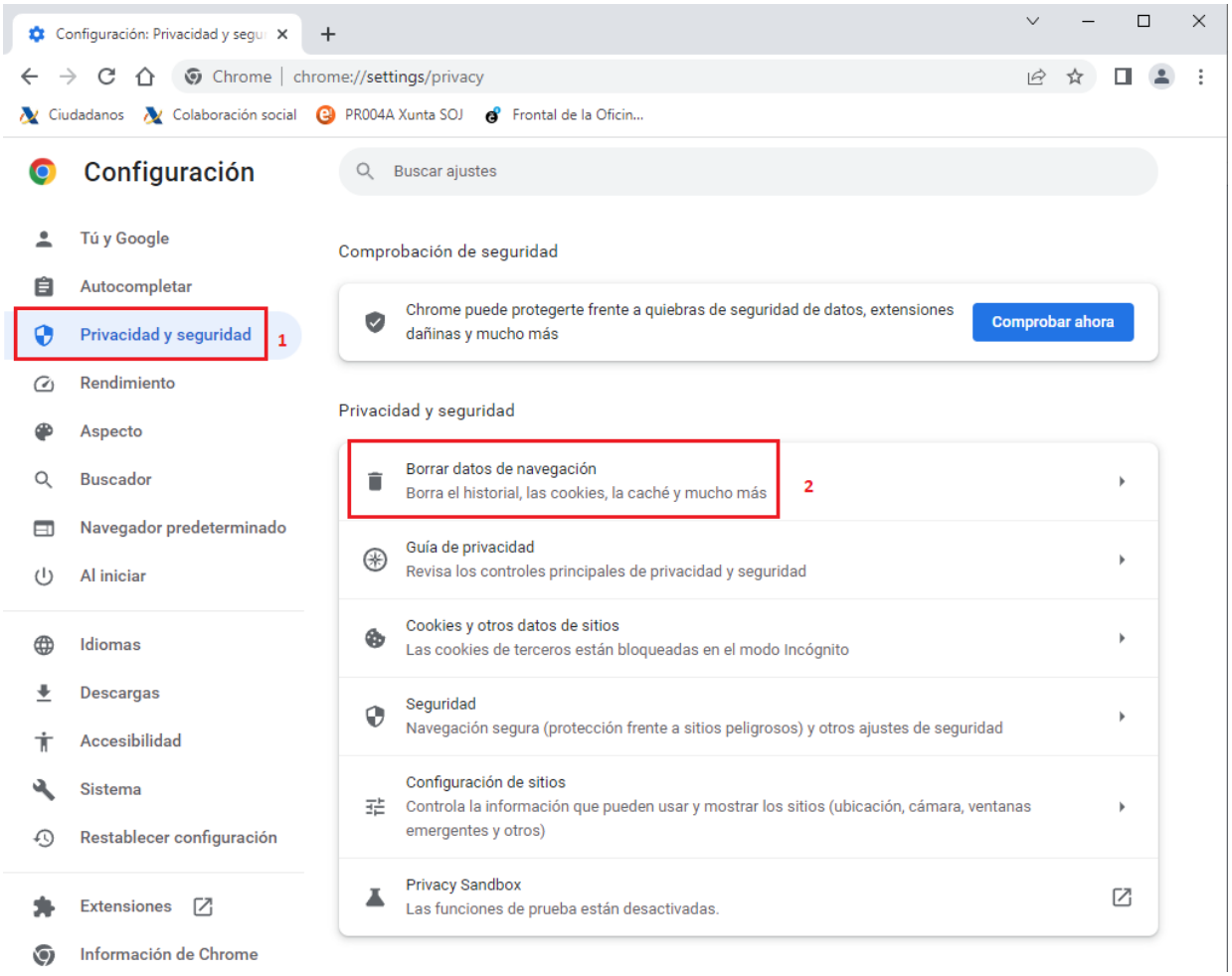
Borrado del historial en Google Chrome y configuración de Microsoft Edge y Mozilla Firefox para que lo borren al cerrarse:

<u>Google Chrome</u>:

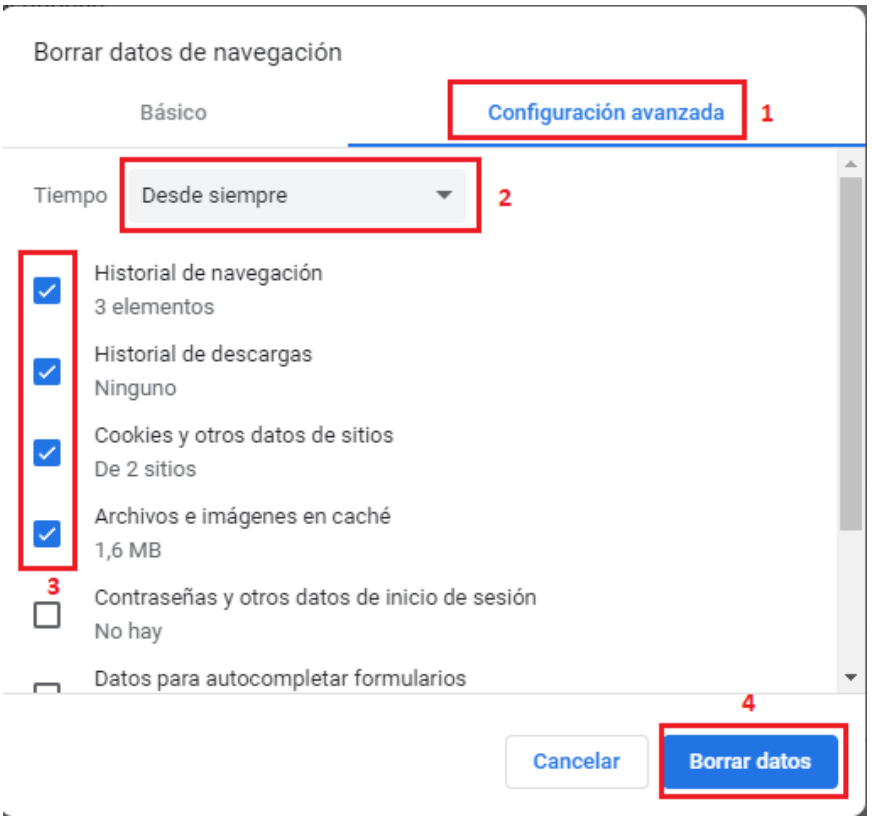
Pinchamos en el menú superior (1) y a continuación en Configuración (2):



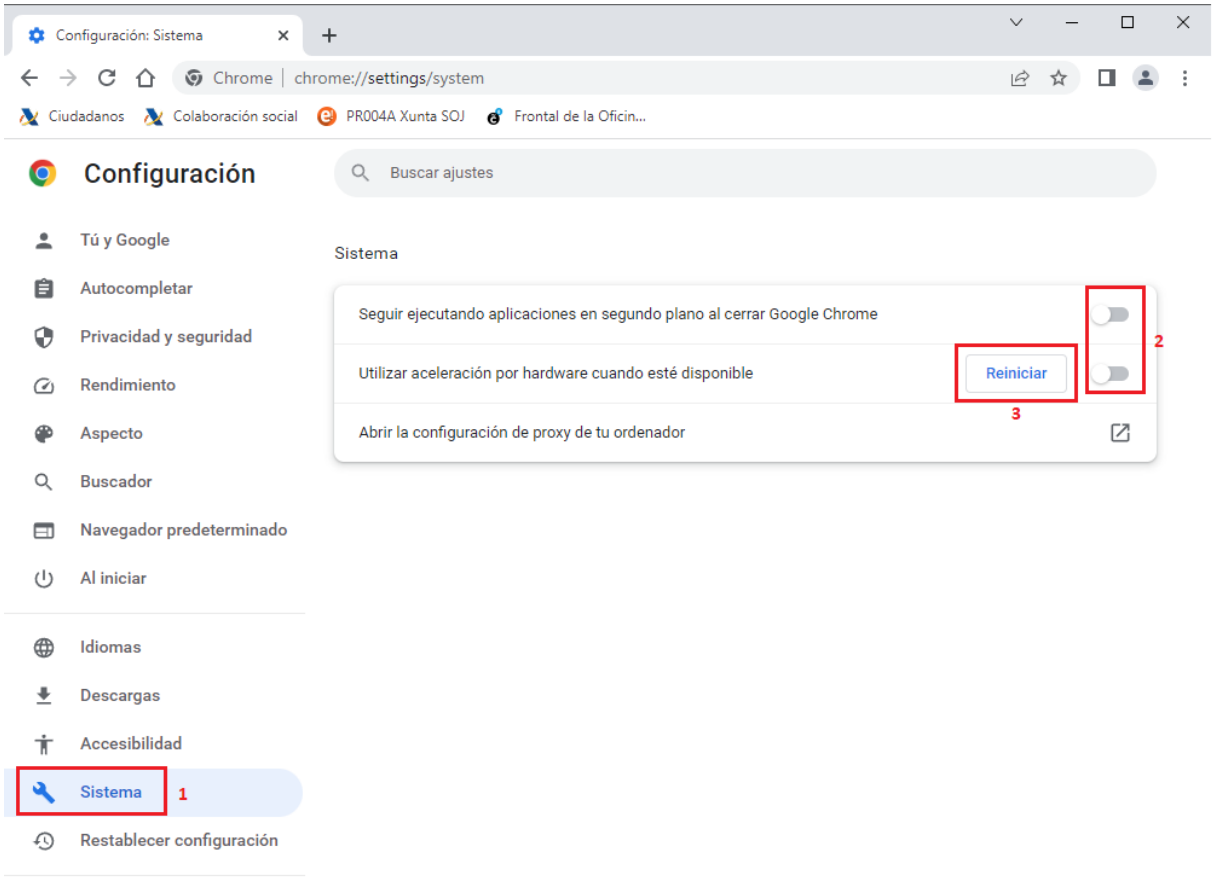
Pinchamos en el menú Privacidad y seguridad (1) y a continuación en Borrar datos de navegación (2):



Seleccionamos la Configuración avanzada (1), en Tiempo seleccionamos Desde siempre (2), marcamos las primeras cuatro casillas (3) y por último en Borrar datos (4)

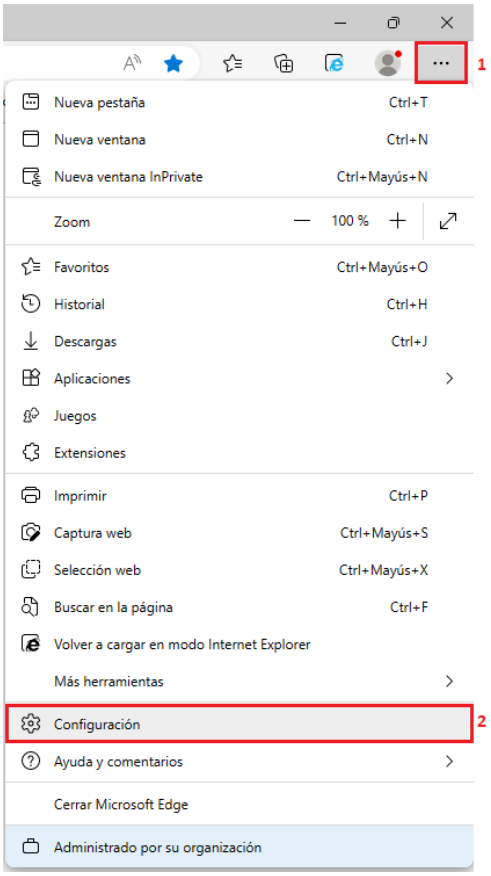


Asimismo, y no sólo para LexNET, es recomendable desactivar dentro de Sistema (1) las Opciones (2) y a continuación reiniciar el navegador (3):

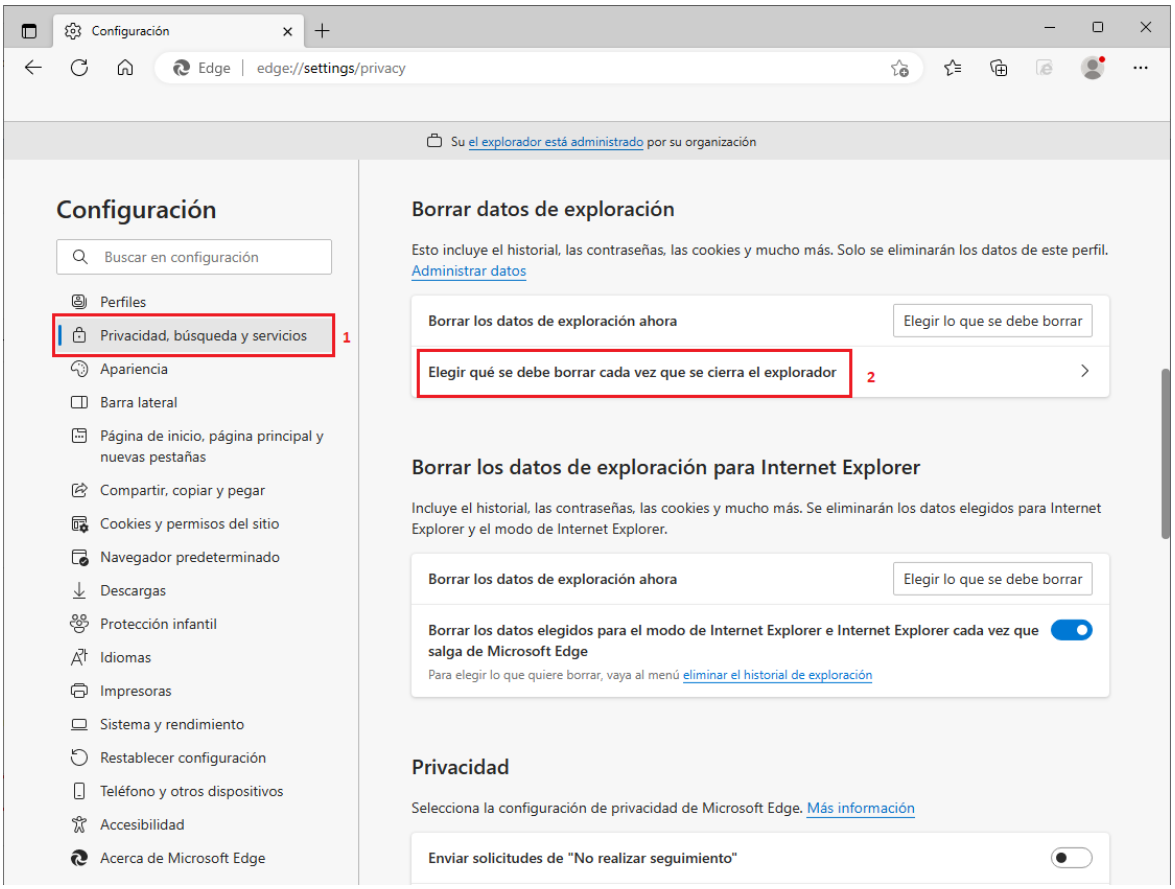


Microsoft Edge:

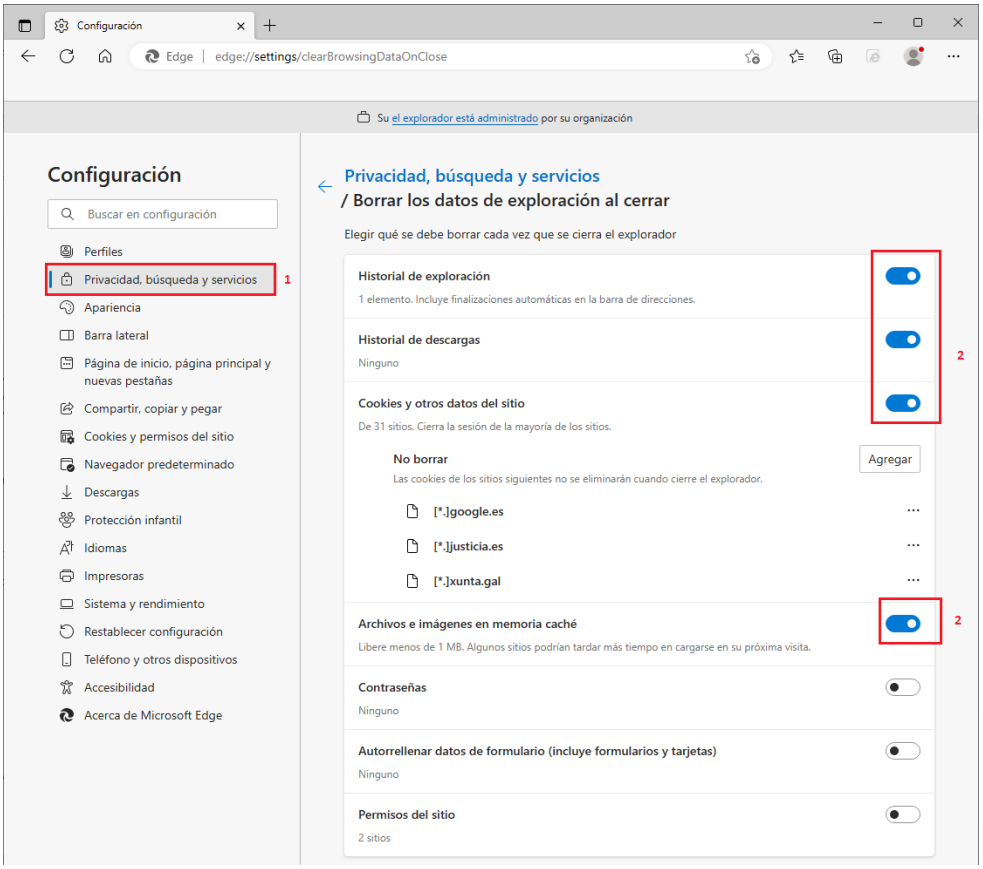
Pinchamos en el menú superior (1) y a continuación en Configuración (2):



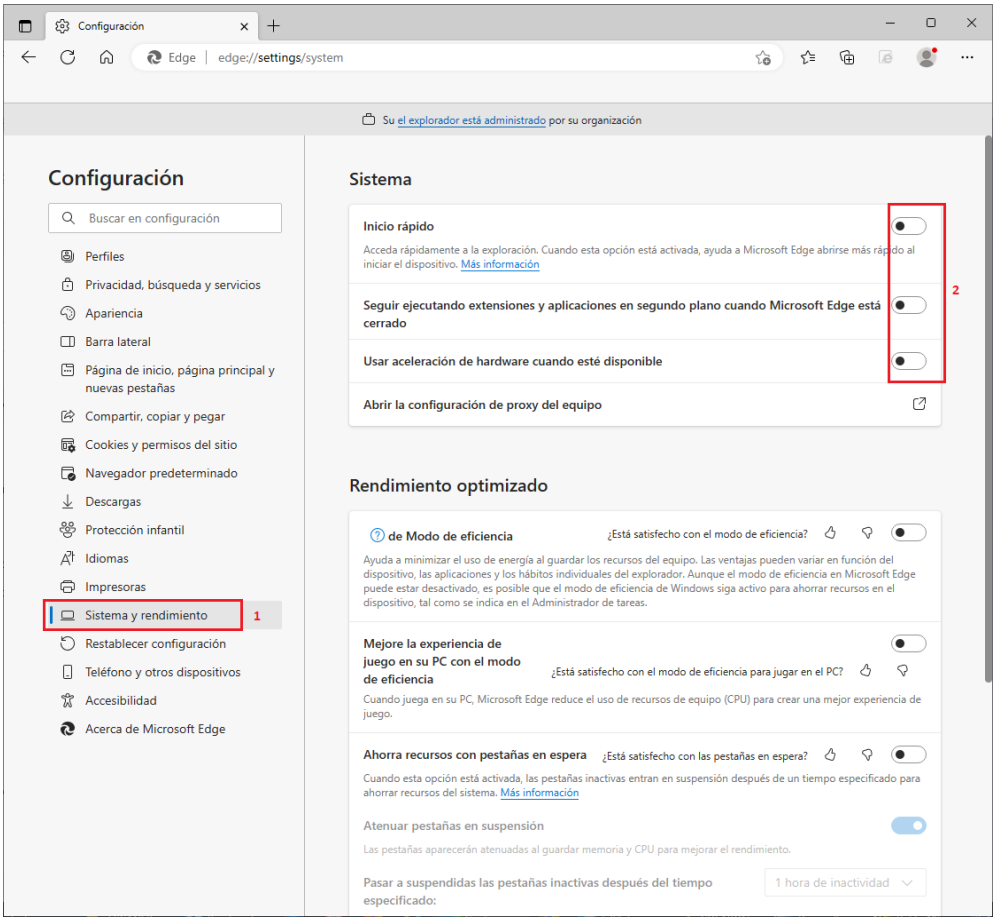
Pinchamos en privacidad, búsqueda y servicios (1). Buscamos la opción Borrar datos de exploración y pinchamos en Elegir qué se debe borrar cada vez que se cierre el explorador (2):



Activamos las primeras cuatro primeras opciones como en la imagen:

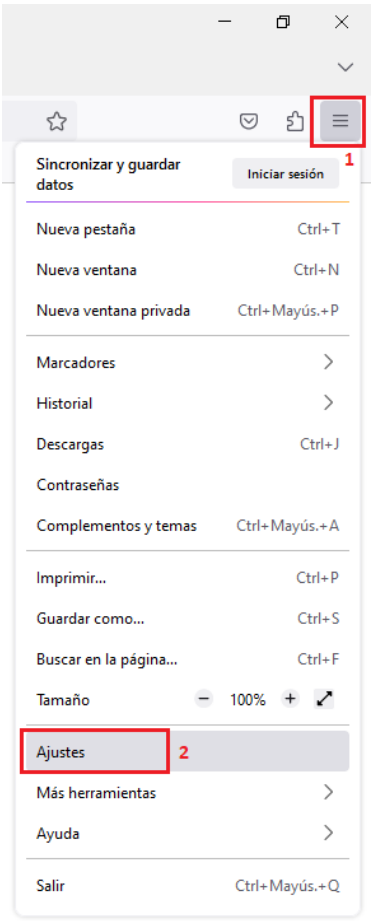


Asimismo, y no sólo para LexNET, es recomendable desactivar dentro de Sistema y rendimiento (1) las Opciones (2) y a continuación reiniciar el navegador (3):

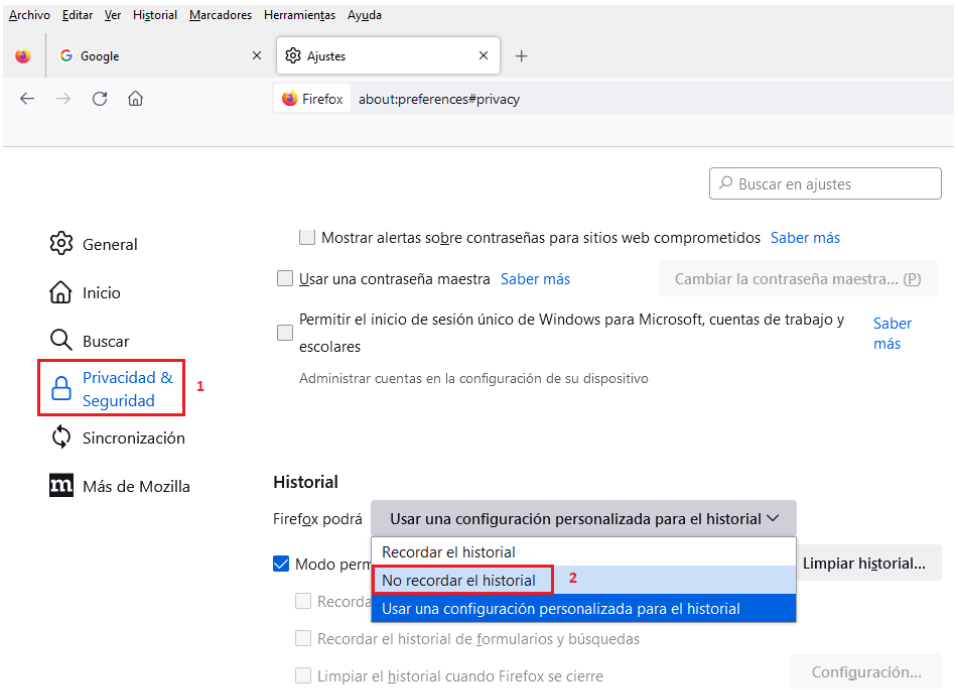


Mozilla Firefox:

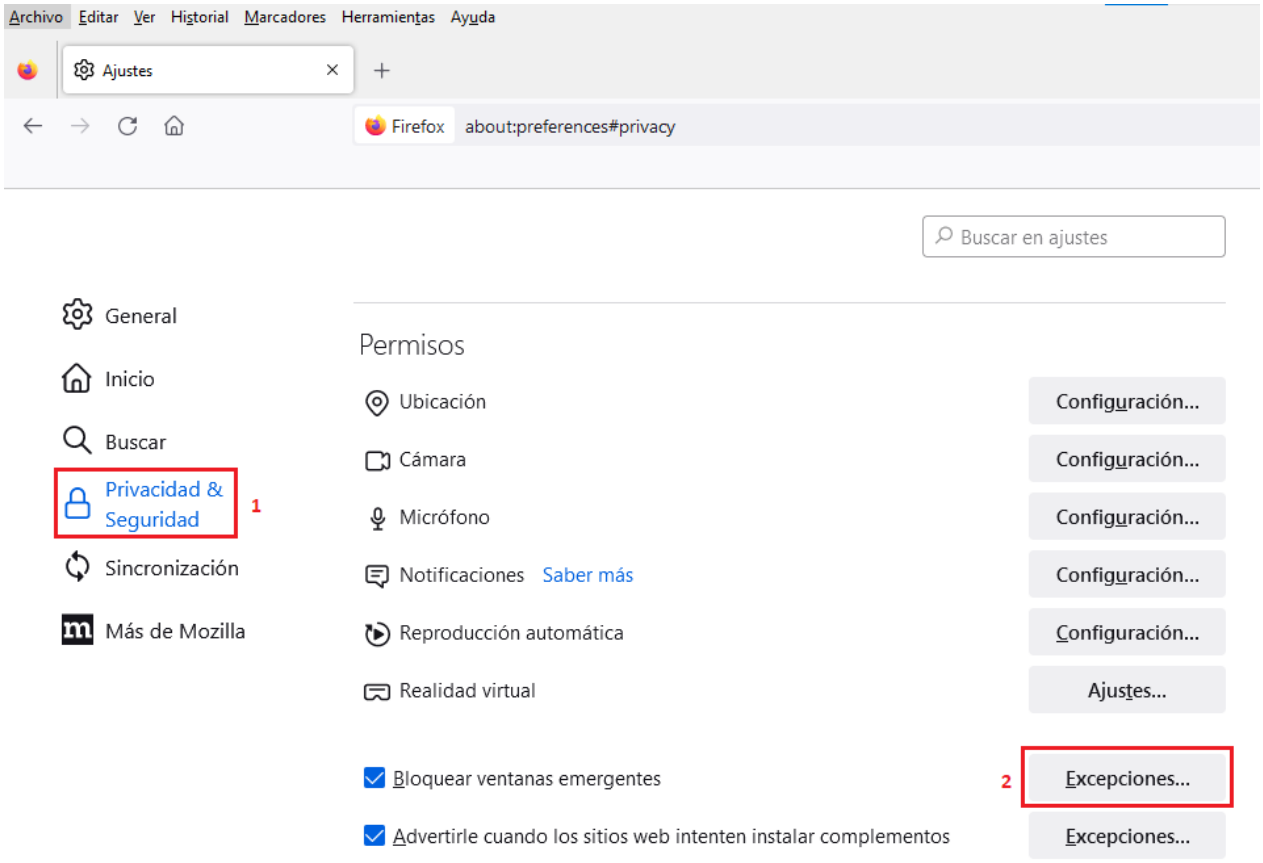
Pinchamos en el menú superior (1) y a continuación en Ajustes (2)



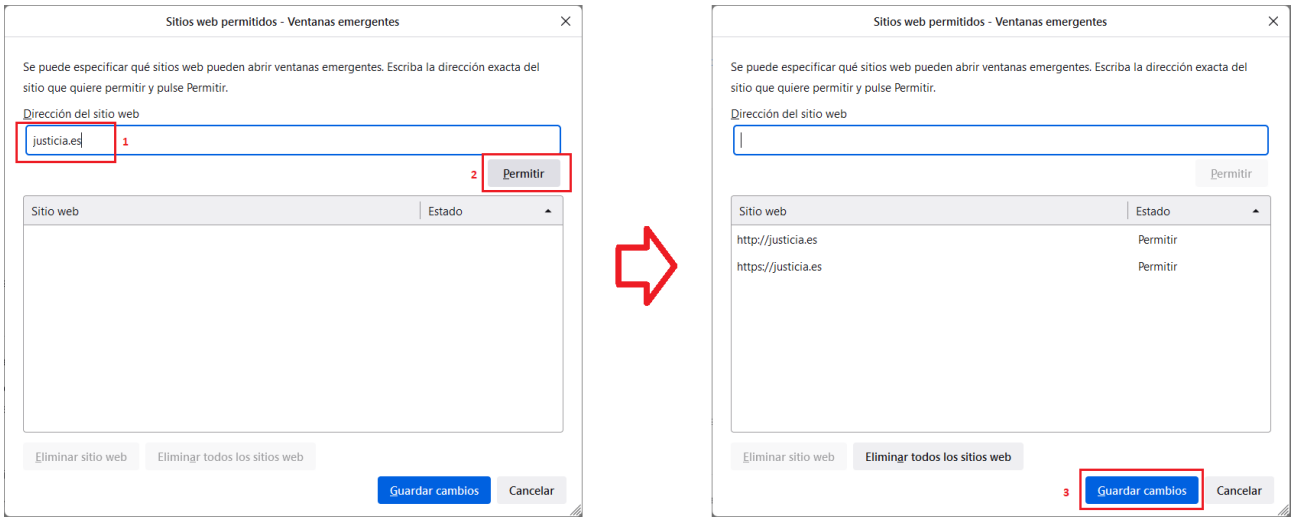
Pinchamos en el menú Privacidad & Seguridad (1) y buscamos Historial. En el desplegable “Firefox podrá” seleccionamos No recordar el historial (2) y reiniciamos el navegador:



Por último, para evitar problemas con LexNET, también dentro del menú Privacidad & Seguridad (1), buscamos el apartado de Permisos y en la opción Bloquear ventanas emergentes pinchamos en Excepciones (2):

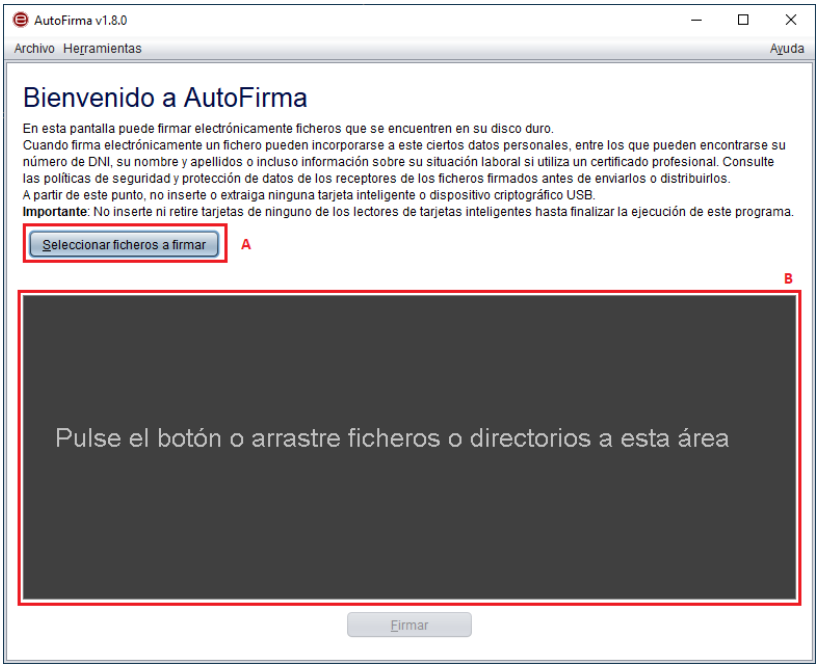


Agregamos el dominio justicia.es (1) y pinchamos en Permitir (2). Se agregarán los dominios, a continuación en Guardar cambios (3)

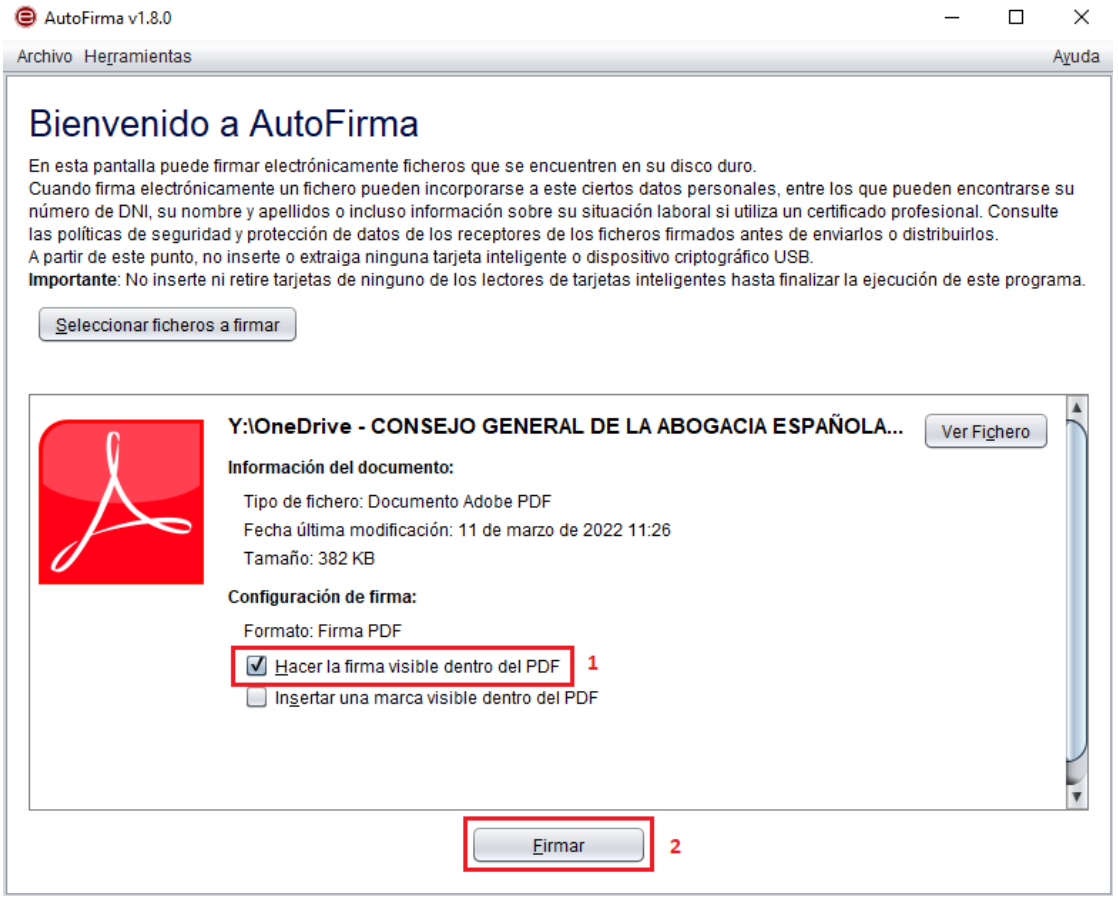


FIRMA DE DOCUMENTOS PDF CON AUTOFIRMA:

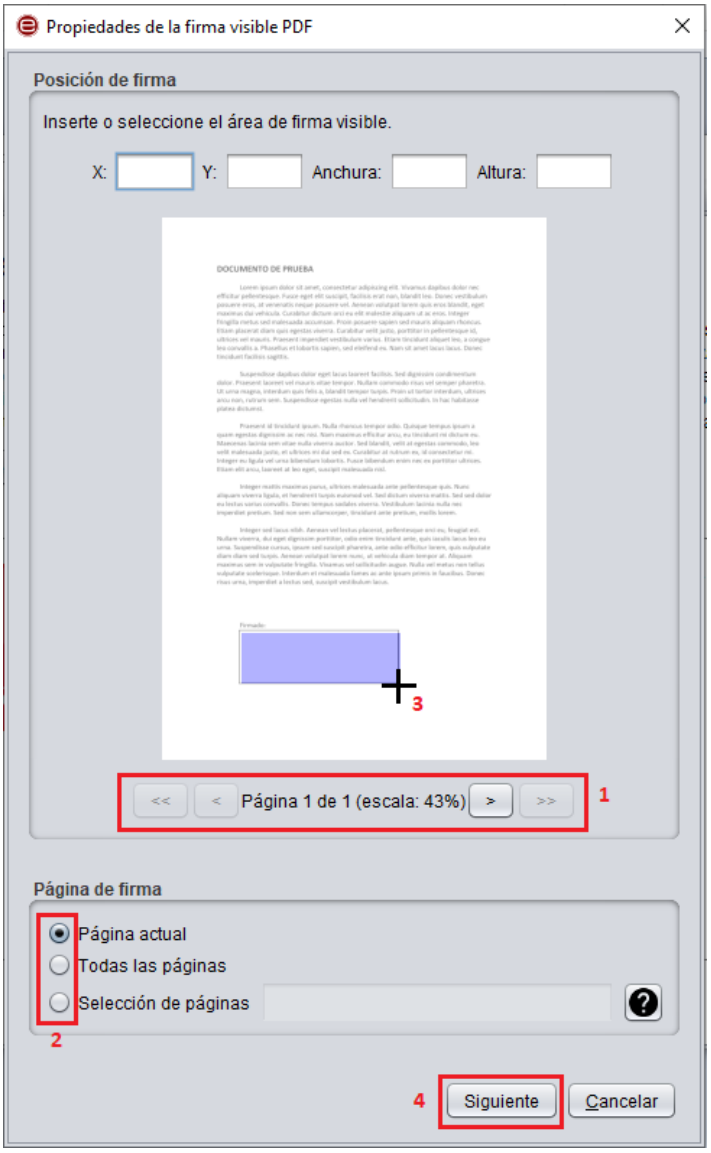
Abrimos AutoFirma y seleccionamos el fichero/s (A) a firmar o lo arrastramos y soltamos en la zona (B)



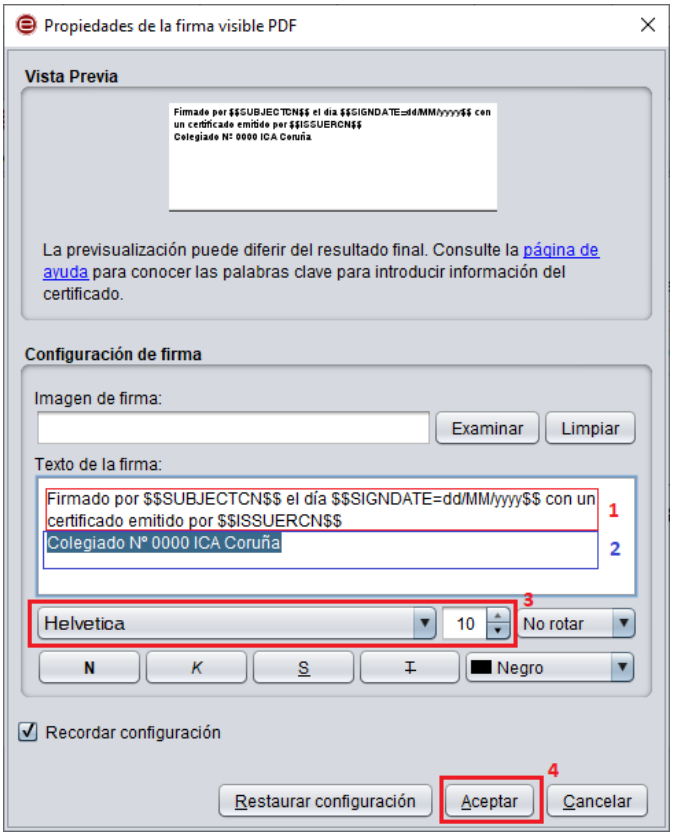
Si AutoFirma está configurado como se indica en el apartado previo de instalación y configuración, ya nos aparecerá marcada la opción Hacer firma visible dentro del PDF (1), si no fuese así la marcamos. A continuación pinchamos en Firmar (2):



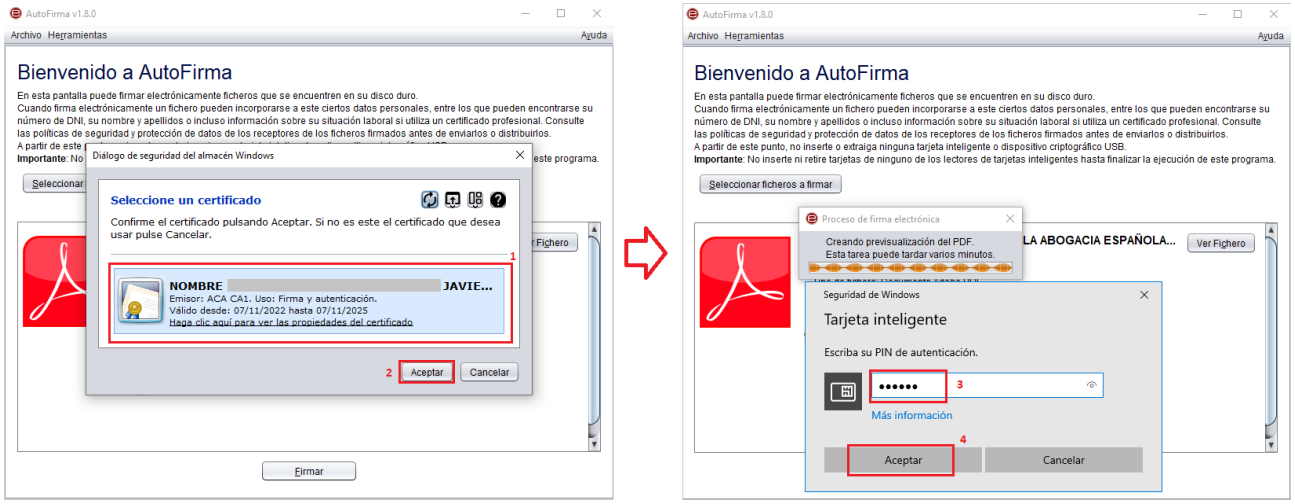
Podemos desplazarnos por las páginas del PDF y previsualizar dónde queremos insertar la marca visible de la firma (1). También podemos especificar la página/s específicas en las que queremos que se muestre la firma (2). Una vez previsualizada la página en la que queremos insertar la marca visible, dibujamos con el ratón el área que ocupará (3). Por último, pinchamos en el botón Siguiente (4):



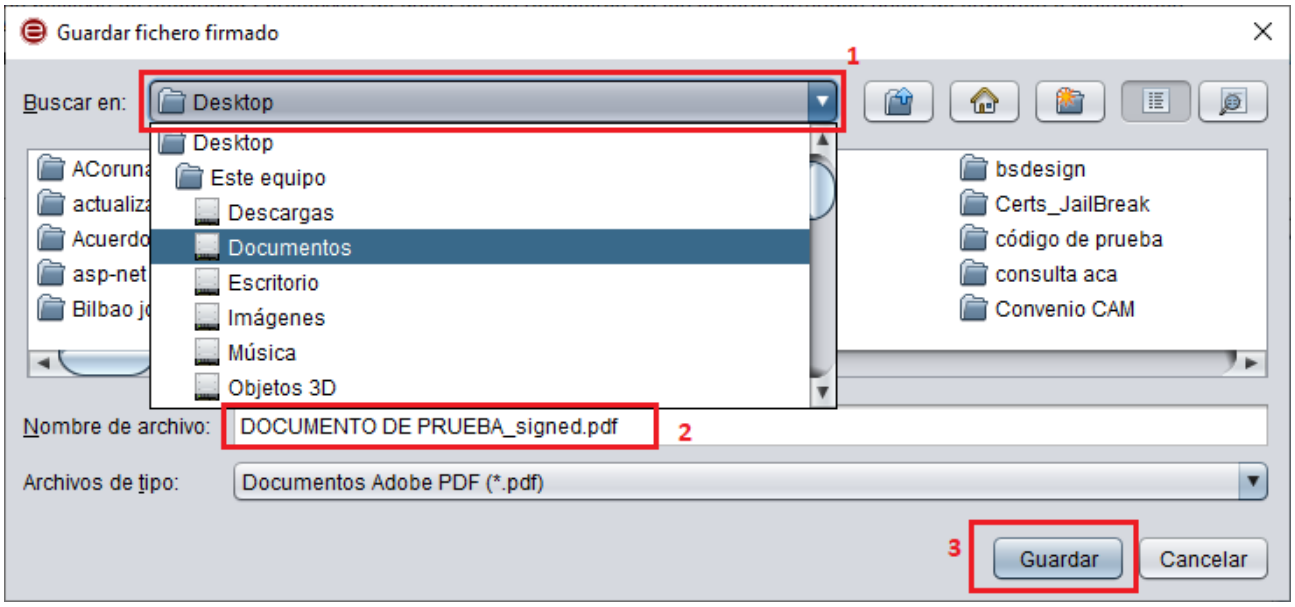
El texto de la Firma (1) no se debe modificar, sí se puede agregar un texto adicional como en el ejemplo (2). Recomendamos también cambiar el tipo de fuente y el tamaño de la misma para que no se corte el texto en áreas reducidas, como en el ejemplo (3). A continuación hacemos click en Aceptar (4):



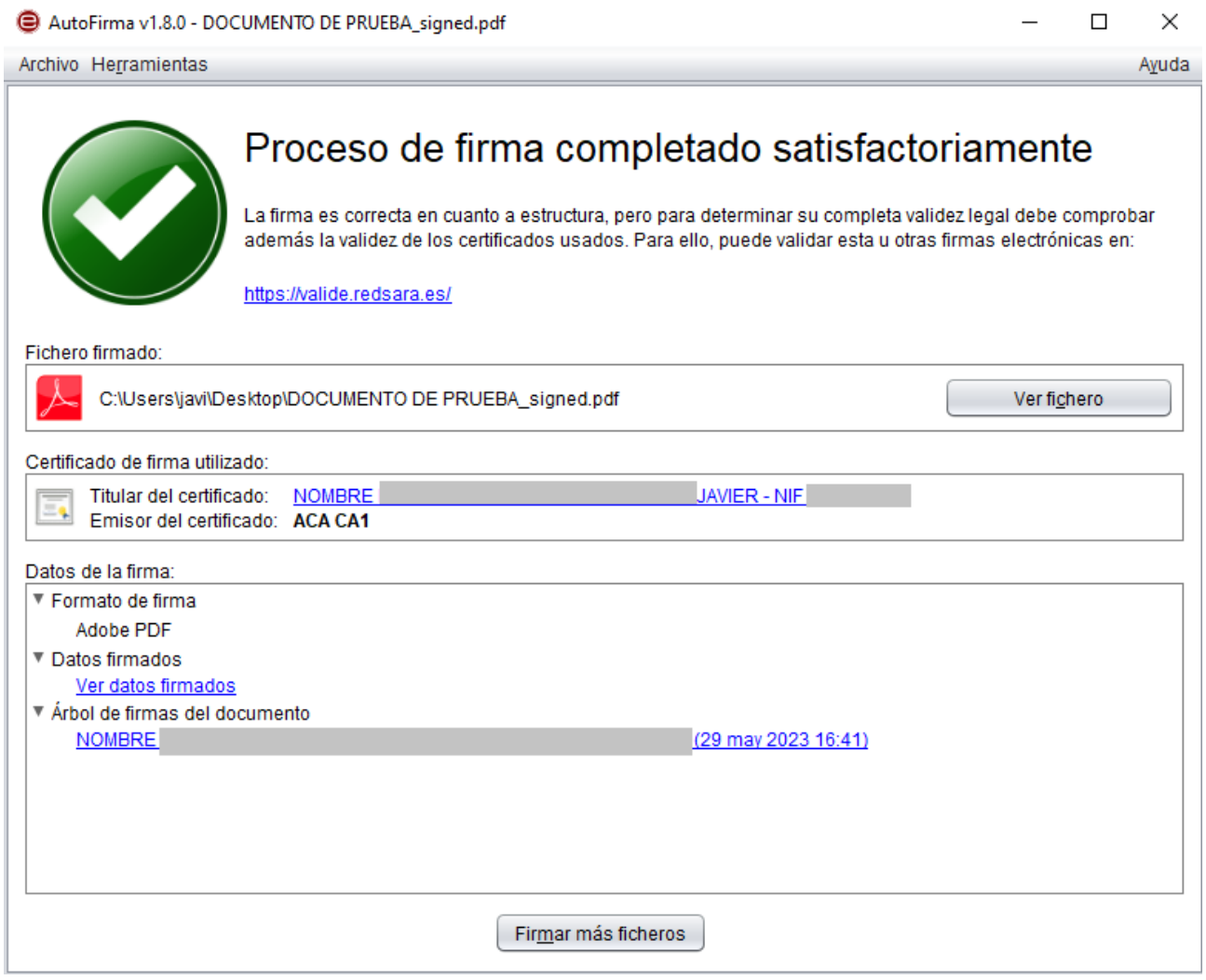
A continuación seleccionaremos el certificado para la firma (1) y pinchamos en Aceptar (2). Nos pedirá el PIN de la tarjeta ACA (3), una vez introducido pinchamos en Aceptar (4):



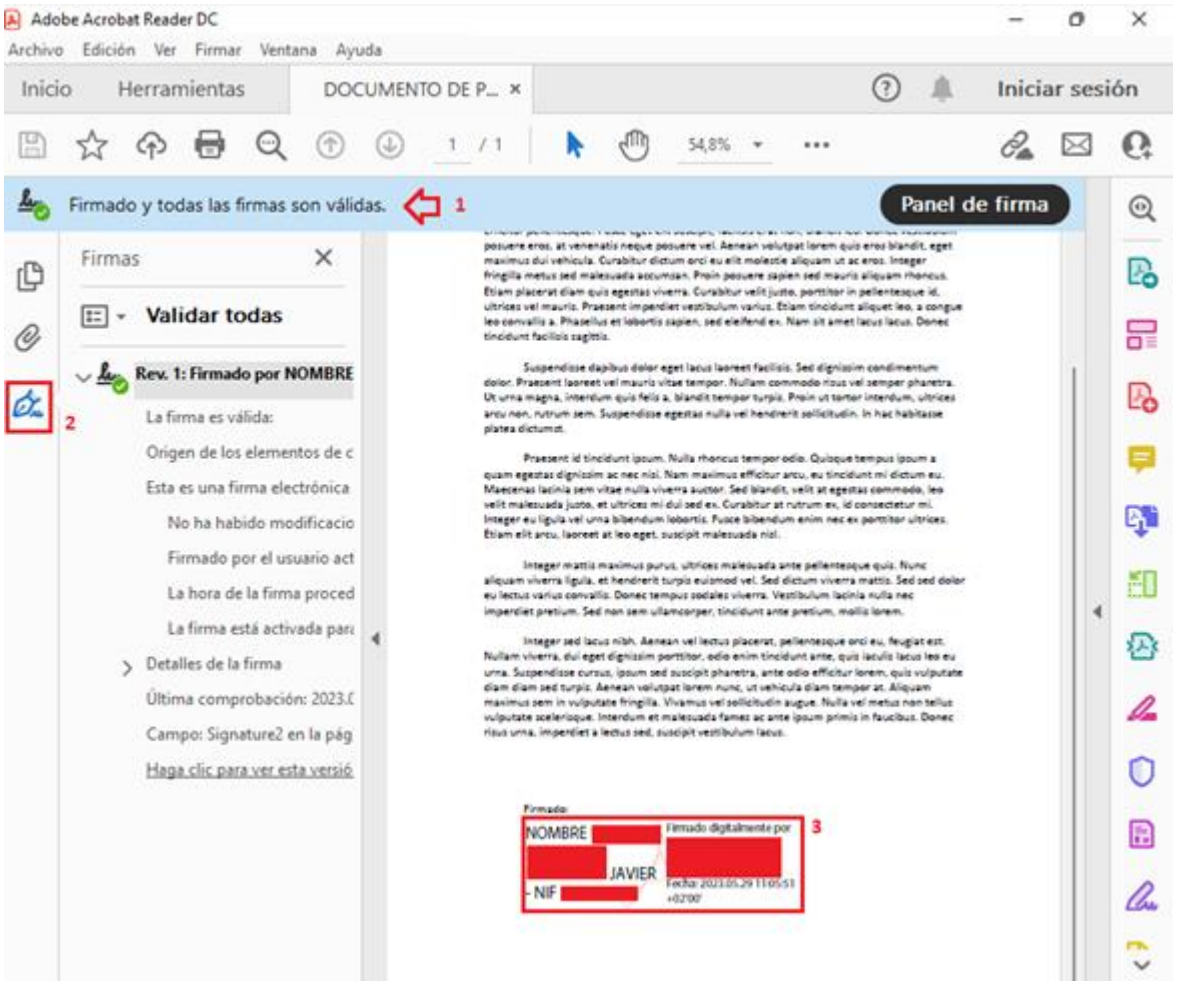
Seleccionamos dónde queremos guardar el documento PDF firmado (1). Por defecto lo guardará en la misma carpeta que el documento PDF original, añadiendo al nombre del fichero "_signed". A continuación hacemos click en el botón Guardar (3).
Si hemos seleccionado el PDF original en el paso (1) o si hemos borrado el texto "_signed" del nombre (2) nos preguntará si deseamos sobrescribir el PDF original:



El proceso de firma ha concluido:



Verificación de la firma (1) y (2):



Configuración de Adobe Reader DC para la validación y firma de documentos PDF con certificados ACA en sistemas Microsoft Windows:

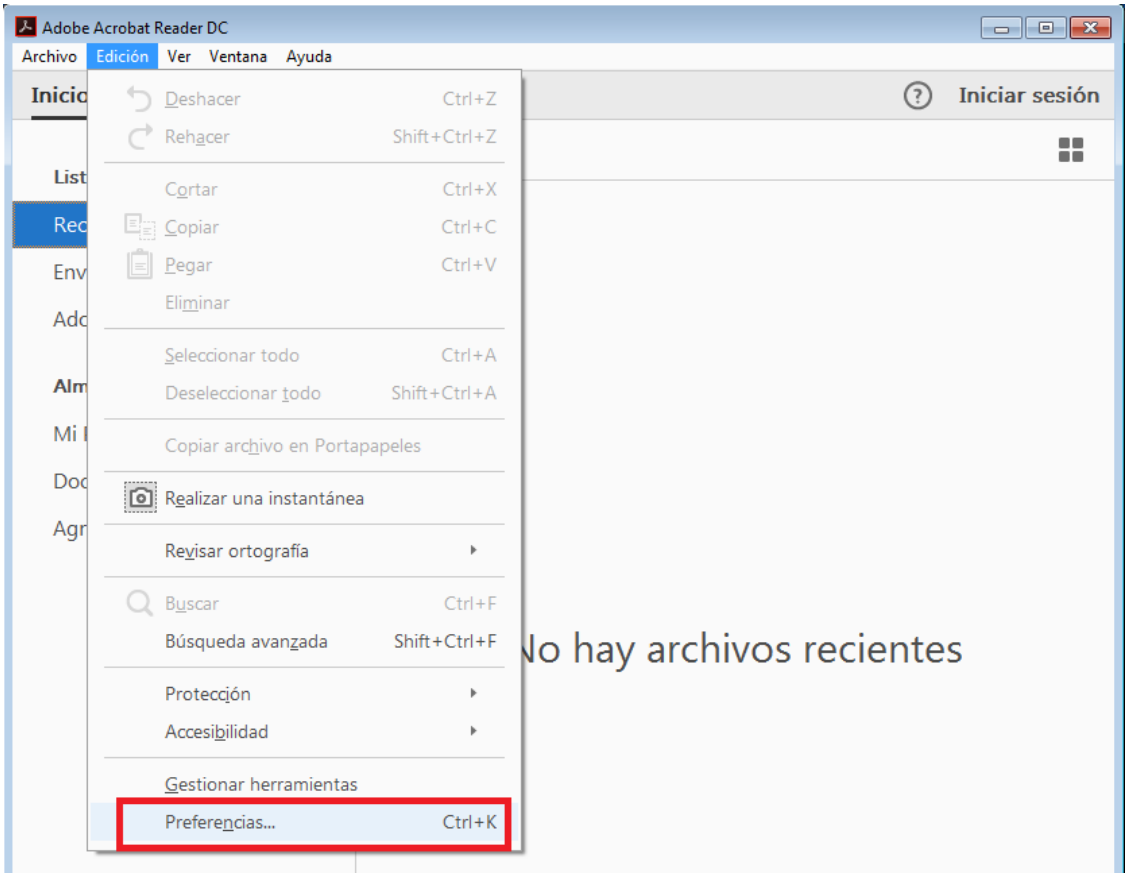
(Desde el Colegio recomendamos el uso de AutoFirma en lugar de Adobe Reader para firmar PDFs)

Requisitos previos:

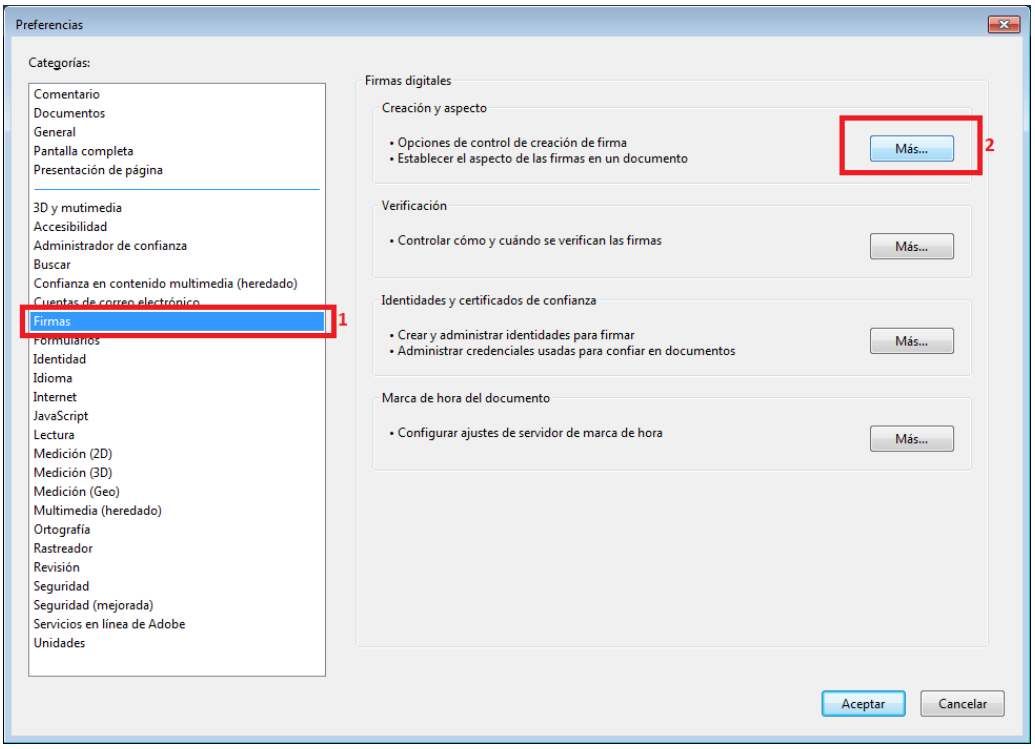
- Tener instalado el software de ACA que gestiona la tarjeta/certificado: Bit4id – PKI Manager
- Tener instalado el software Adobe Reader DC: https://get.adobe.com/es/reader/

1.- Estableciendo el formato de Firma en Adobe Reader:

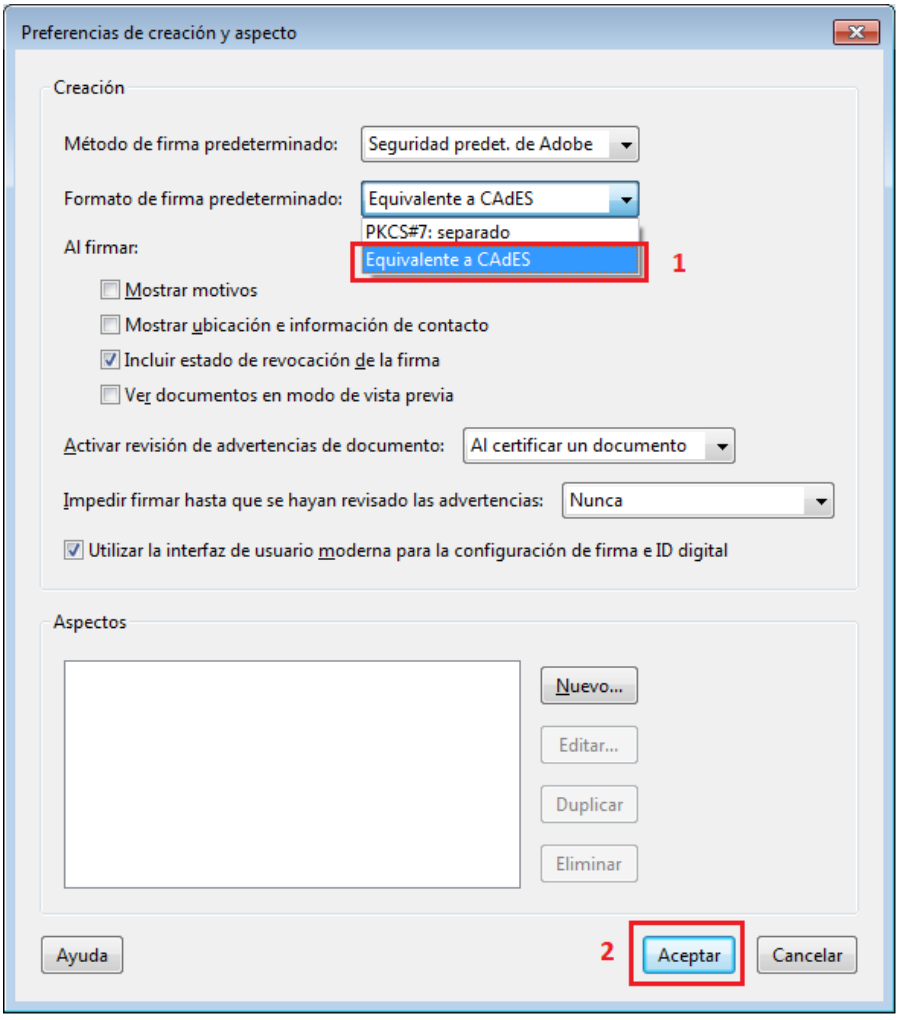
Abrimos las preferencias de Adobe Reader: Edición -> Preferencias:



Seleccionamos, dentro del catálogo de Categorías de la izquierda "Firmas" (1), y en el apartado Firmas digitales: Creación y aspecto pinchamos en el botón "Más..." (2):



En la pantalla de Preferencias de creación y aspecto, comprobamos que esté seleccionada la opción "Equivalente a CadES" (1) en el desplegable y a continuación pinchamos en "Aceptar" (2):

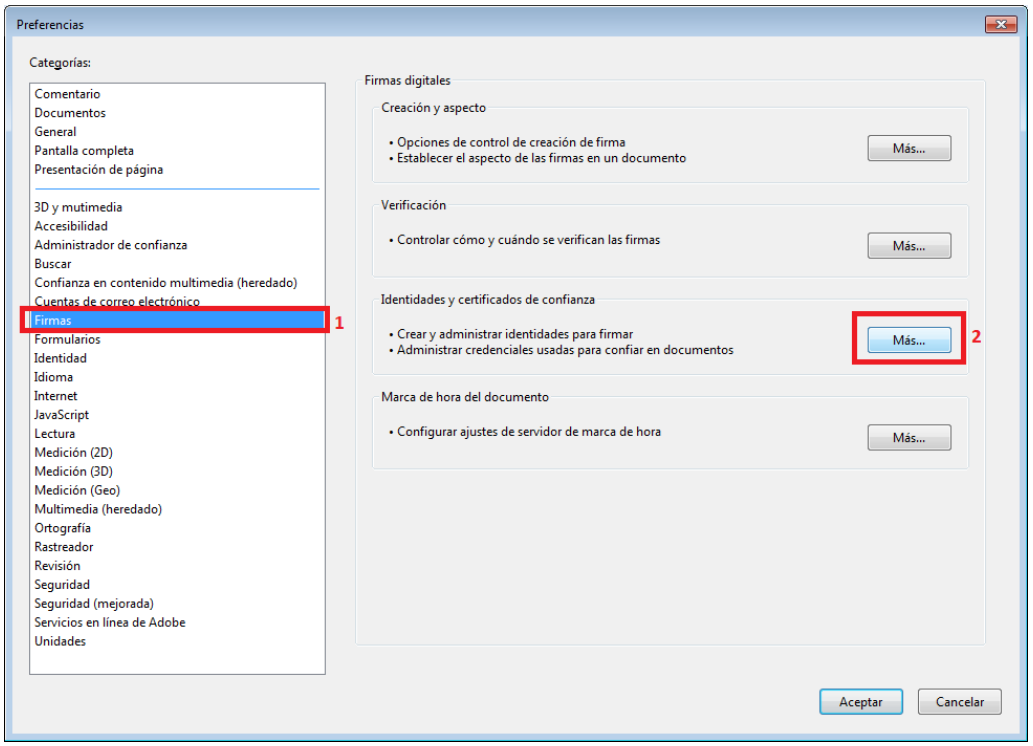


2.- Configuración para la Firma de PDFs con certificados ACA:

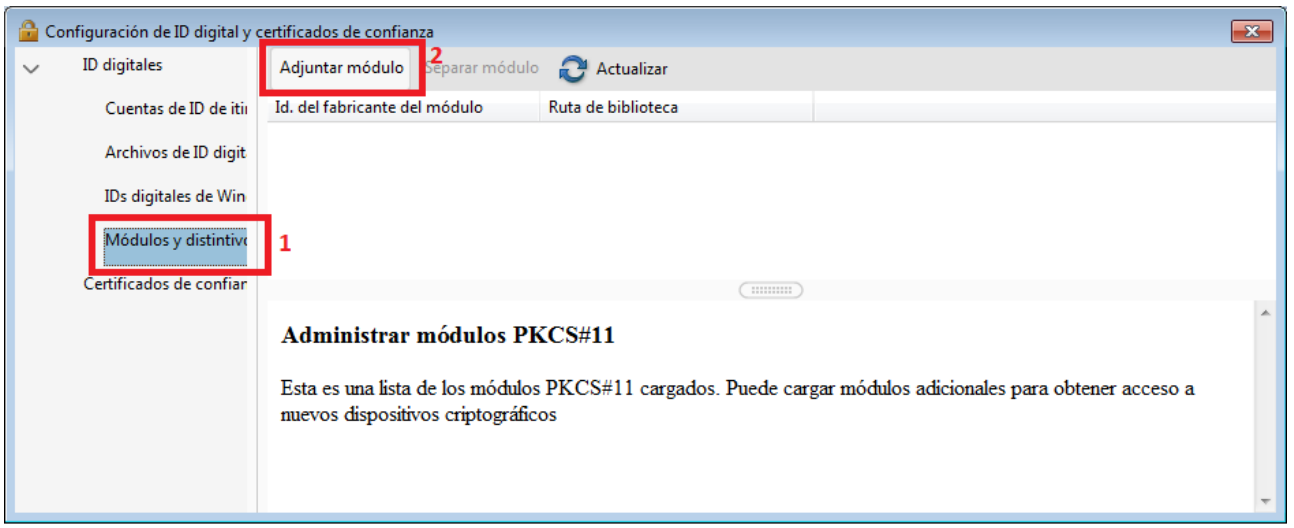
El primer paso será adjuntar el Módulo criptográfico que nos permitirá acceder a la tarjeta ACA y usar el certificado:

Para ello, como en los pasos anteriores, abrimos las preferencias de Adobe Reader: Edición -> Preferencias

En Preferencias, seleccionamos la Categoría "Firmas" (1) y en el apartado "Identidades y certificados de confianza" y pinchamos en el botón "Más..." (2):

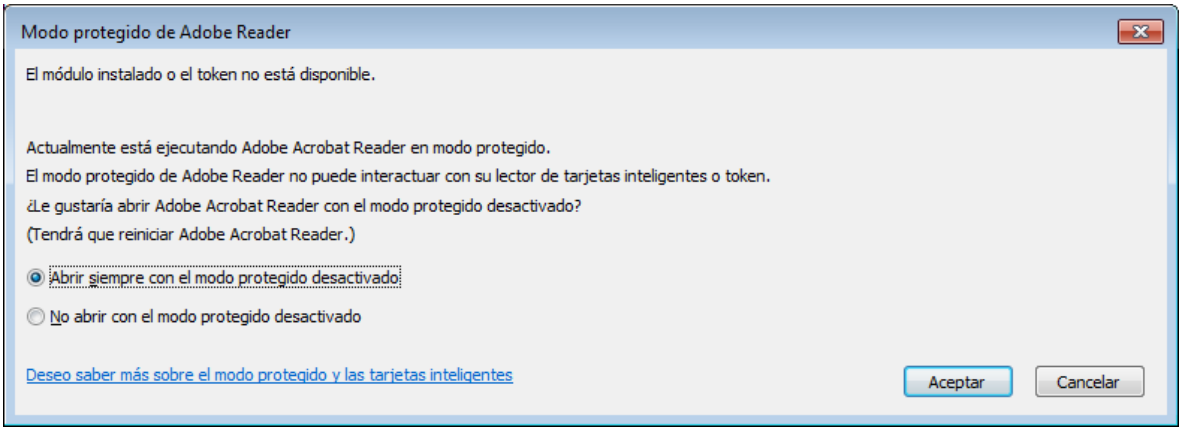


En el menú de la izquierda seleccionamos "Módulos y distintivos" (1) y a continuación en "Adjuntar módulo" (2) **(*) Ver aviso en página siguiente**:



(*) Aviso:

Es posible que aparezca deshabilitada la opción de "Adjuntar módulo" en el paso anterior y en su lugar se nos muestre el siguiente mensaje:



En este caso habrá que seleccionar la opción "Abrir siempre con el modo protegido desactivado" y a continuación pinchar en el botón "Aceptar".

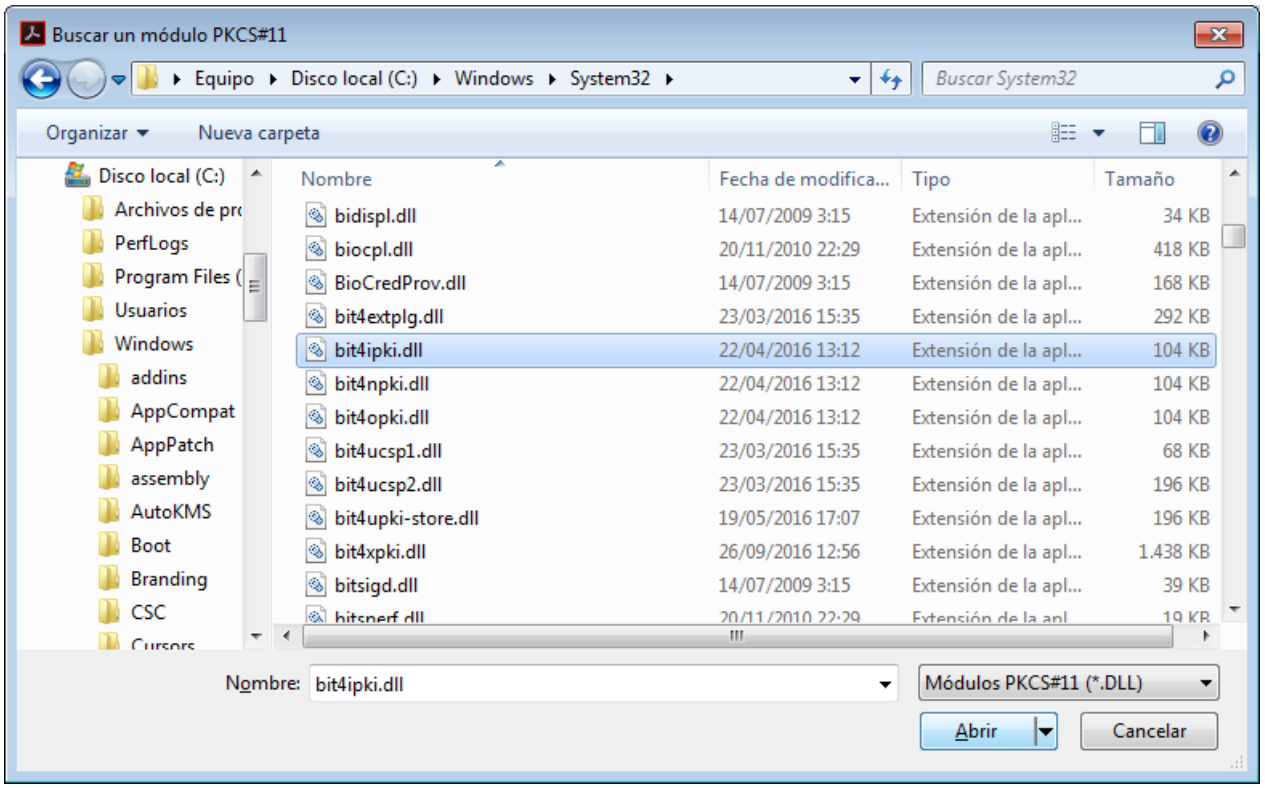
Hecho esto tendremos que cerrar todas las ventanas de opciones de Adobe y posteriormente cerrar completamente Adobe Reader para que los cambios surtan efecto. Volvemos a abrir Adobe Reader e iniciamos nuevamente el proceso descrito en este Apartado 3.

En el caso de que sí aparezca la opción "Adjuntar módulo" continuaremos el proceso de configuración.

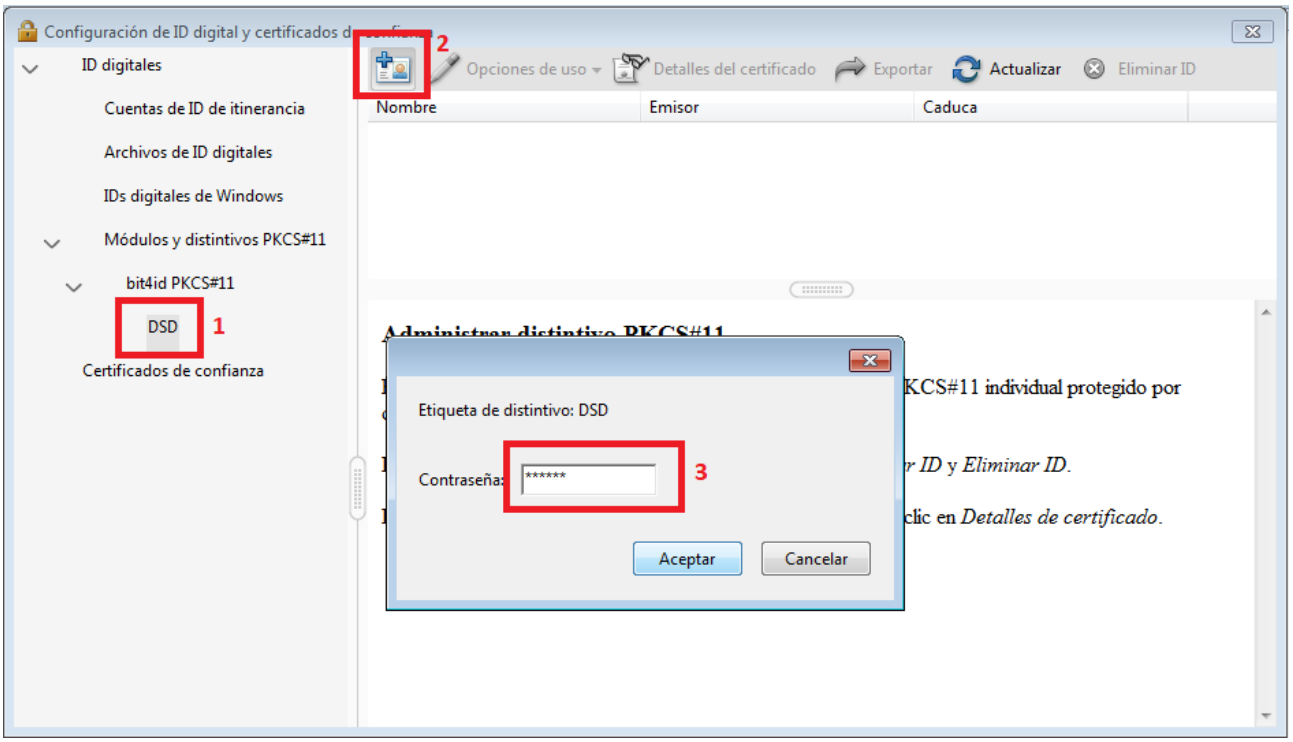
Después de pinchar en "Adjuntar Modulo" buscamos y seleccionamos el modulo y pinchamos en "Abrir":

C:\Windows\System32\bit4pki.dll

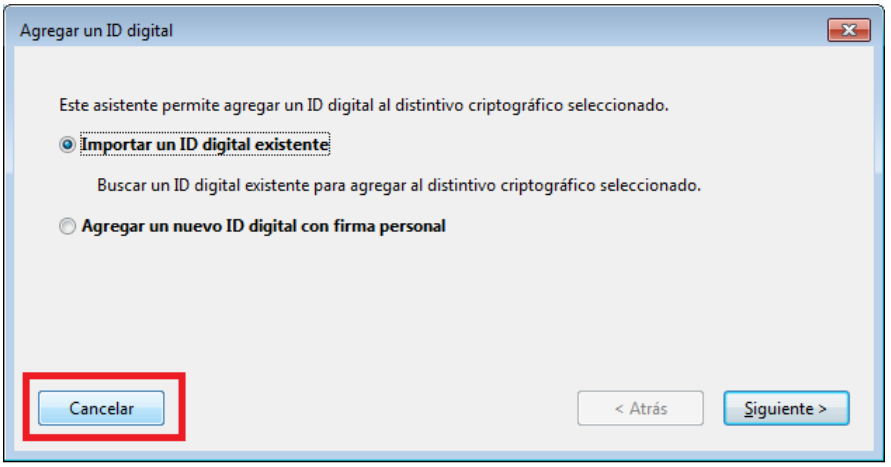
La librería indicada se corresponde con la última versión del Software de ACA (Bit4id), que se presupone instalado ya que es un requisito previo indispensable.



Al expandir la opción "Módulos y distintivos" observamos que se ha cargado correctamente el módulo criptográfico "bit4id PKCS#11" y se muestra el acceso a la tarjeta ACA denominada "DSD" (1). Lo marcamos, a continuación pinchamos en el icono "Añadir certificado" (2) y nos pedirá el PIN de nuestra tarjeta ACA. Introducimos el PIN y pinchamos el botón "Aceptar":

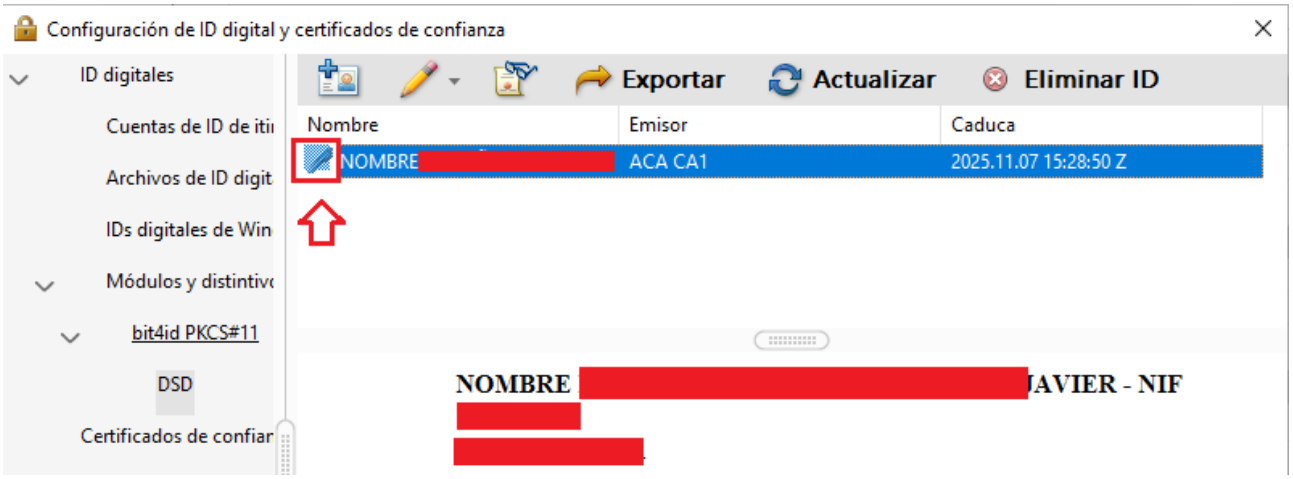


Se mostrará la siguiente ventana, donde pincharemos el botón "Cancelar":



Ahora seleccionamos la tarjeta (DSD 1) y nuestro certificado (2), una vez seleccionado debe verse marcado en azul como en la imagen. A continuación, en el menú superior, pinchamos "Opciones de uso" y seleccionamos la opción "Usar para firmar" (3):

Tras el paso anterior, nuestro certificado debe aparecer con la imagen de una estilográfica delante , como se muestra en la siguiente imagen:

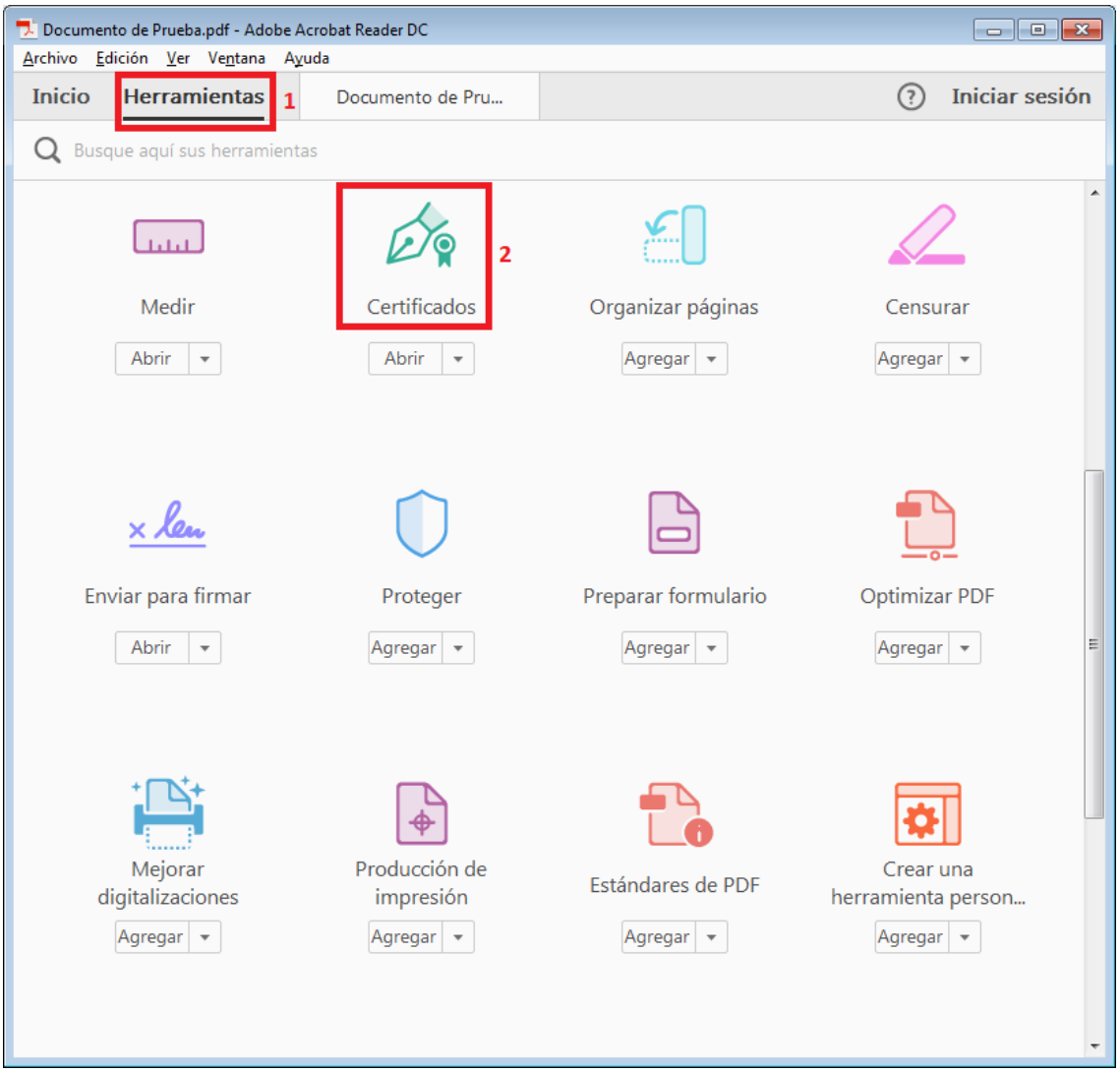


Cerramos todas las ventanas de Opciones y cerramos Adobe Reader para aplicar todos los cambios.

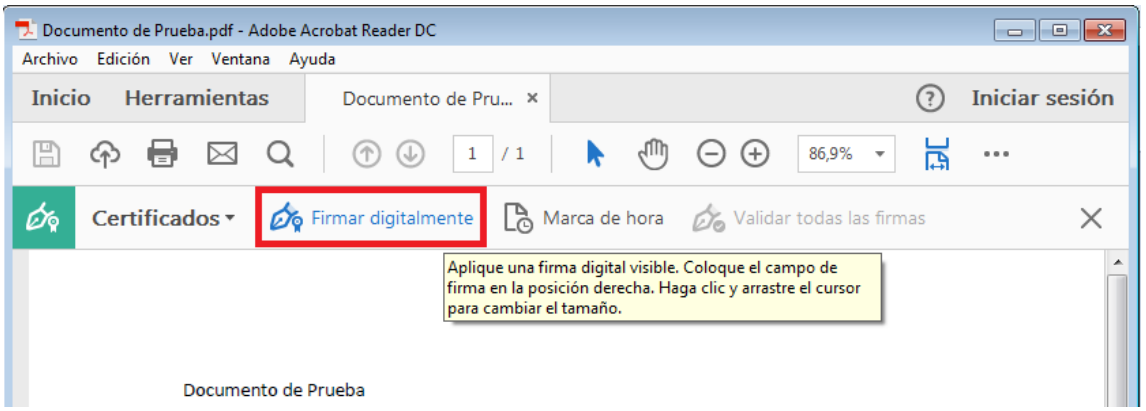
Ya tenemos la aplicación lista para firmar archivos PDF con nuestro certificado ACA.

3.- Firmando PDFs en Adobe Reader con certificados ACA:

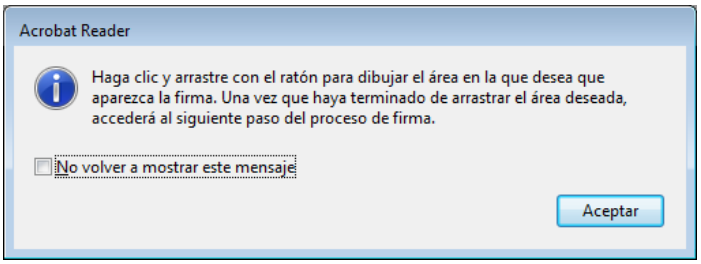
Abrimos el PDF que deseamos firmar, a continuación pinchamos en el menú "Herramientas" (1) y seguidamente en la imagen "Certificados" (2)



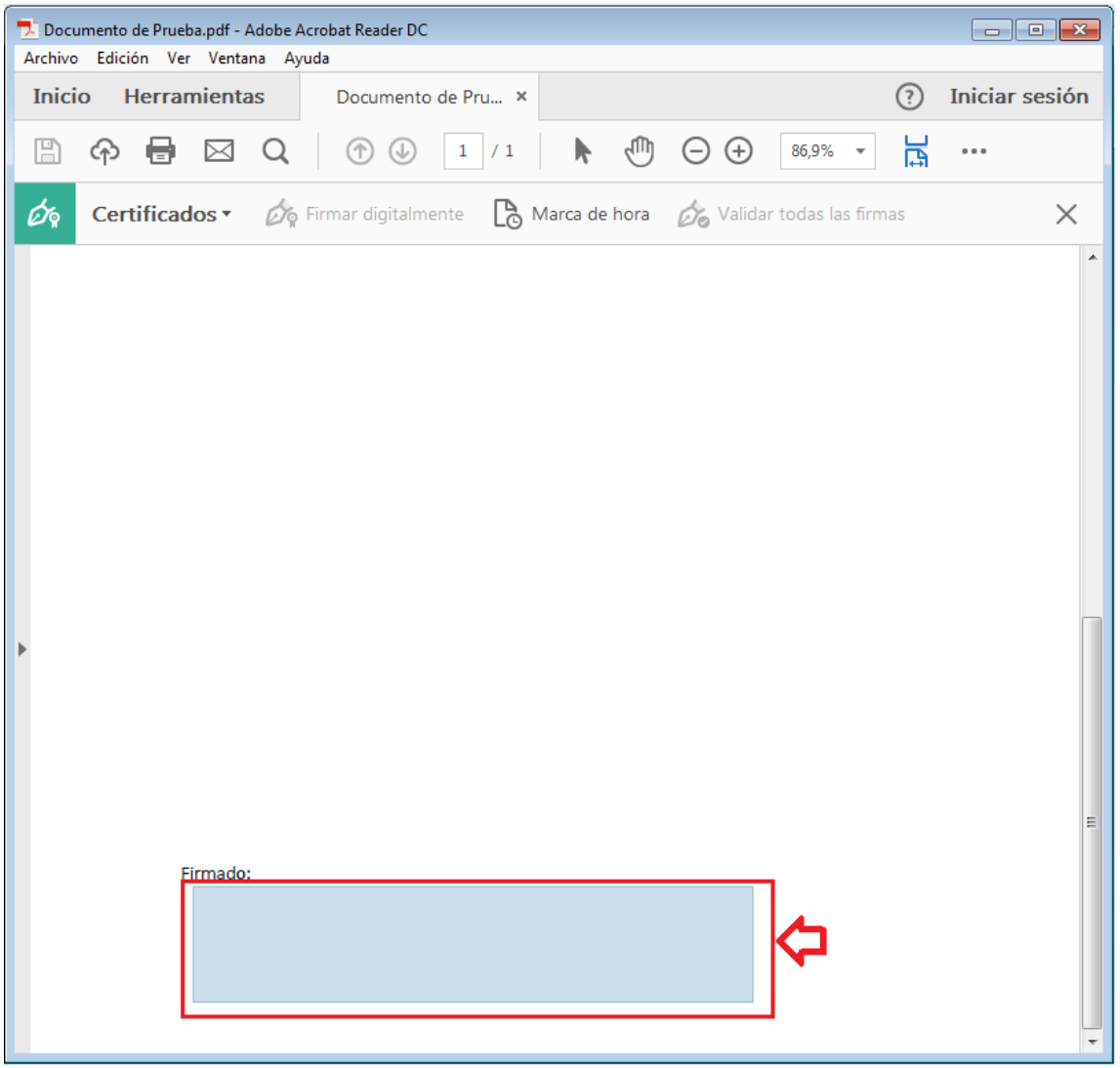
Se visualizará el PDF que hemos abierto previamente con una nueva barra de herramientas, donde pincharemos en la opción "Firmar digitalmente



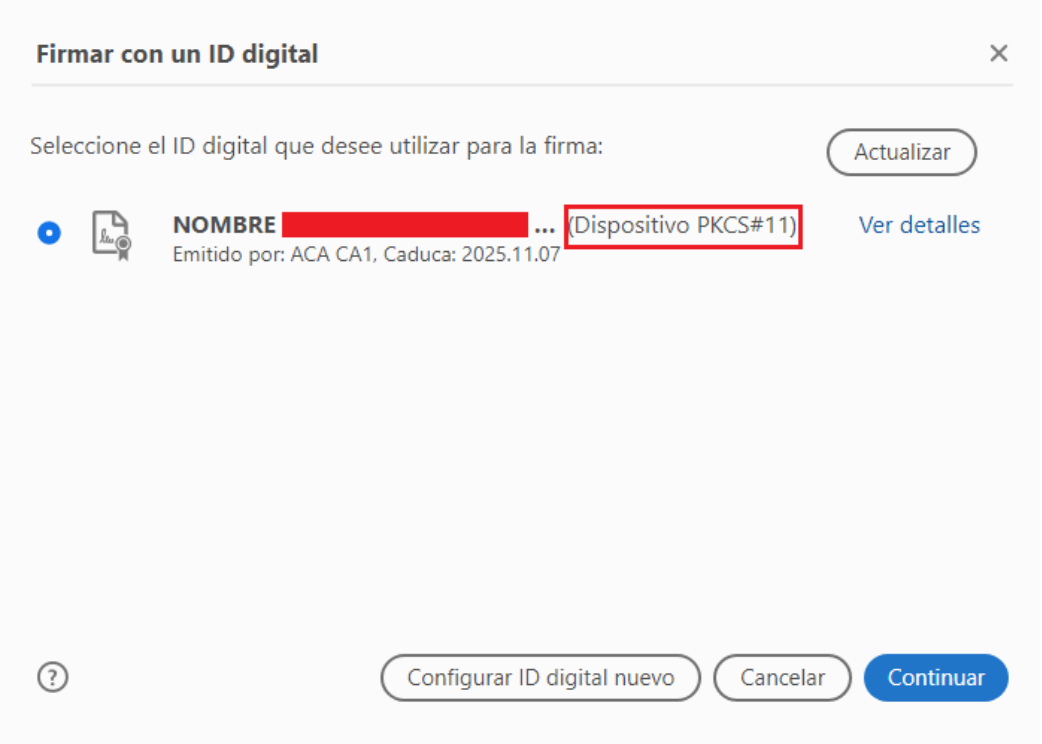
Se mostrará el siguiente mensaje de aviso, indicando que dibujemos con el ratón el área donde queremos visualizar la firma visible en el documento.



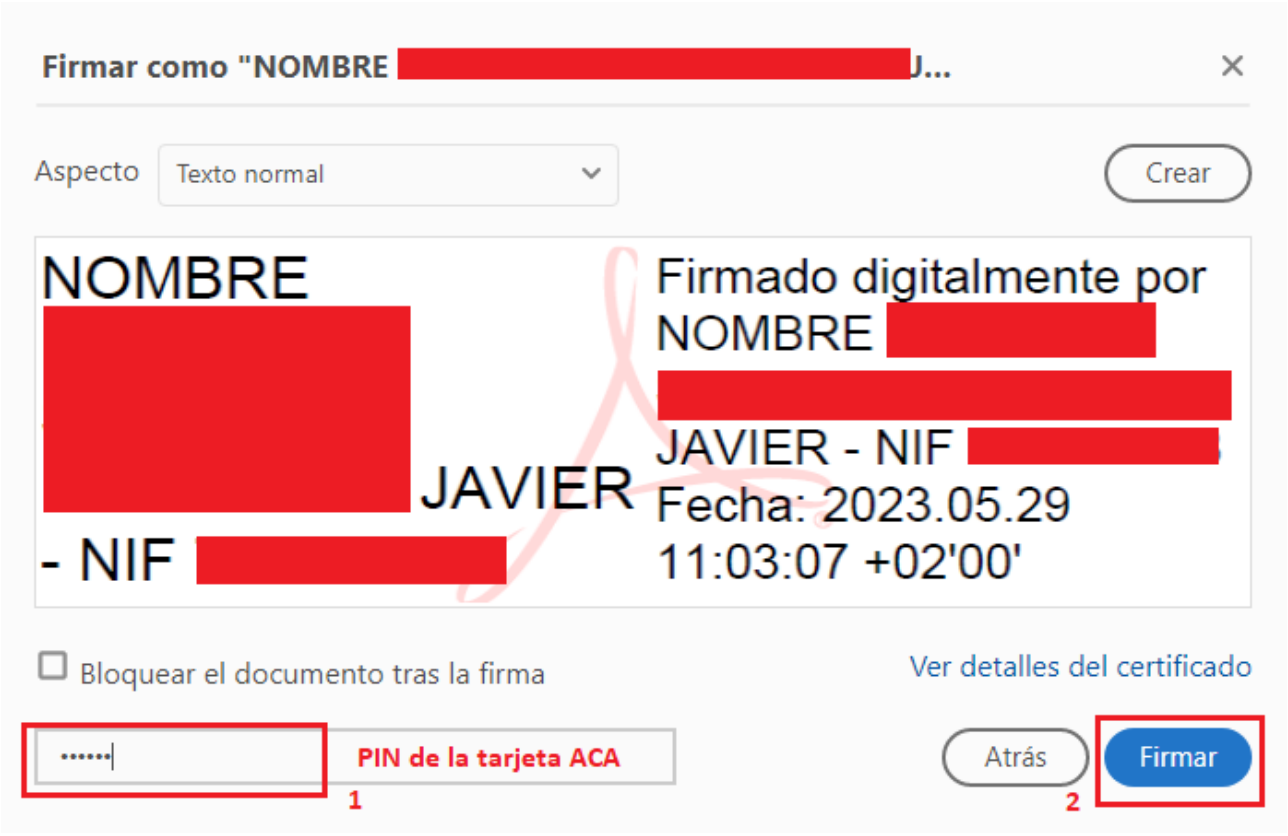
A continuación dibujamos con el ratón, manteniendo pulsado el botón izquierdo, el área donde se insertará la firma visible. (Normalmente lo haremos al final de la última página del documento PDF)
Una vez dibujada el área soltamos el botón izquierdo del ratón para finalizar.
El área en azul de la imagen muestra dónde se visualizará la firma del ejemplo.



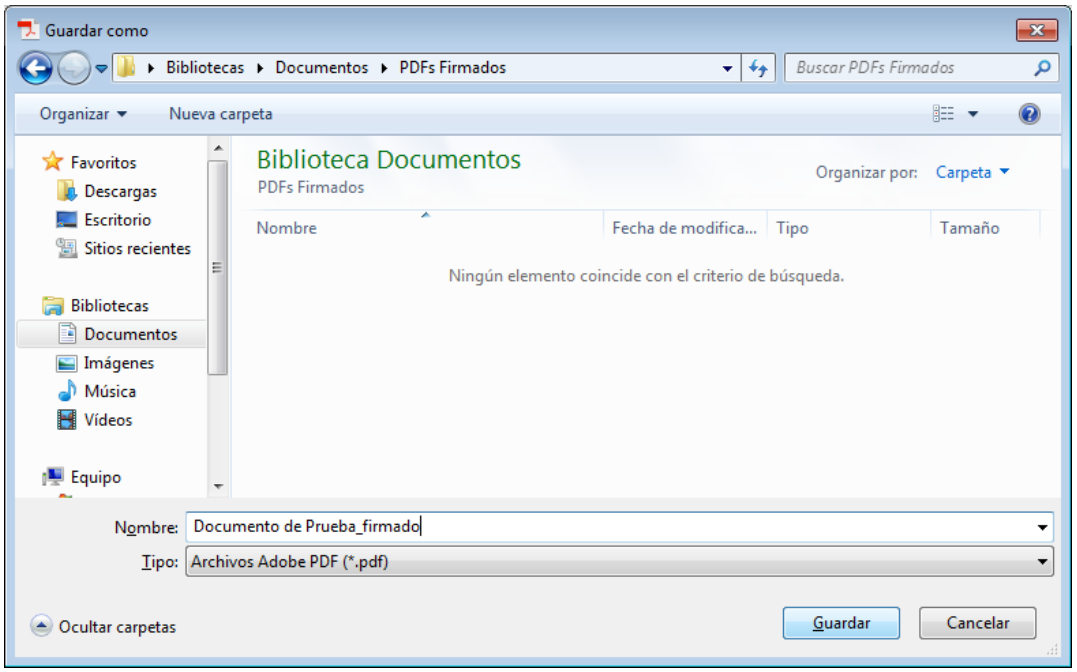
Automáticamente se nos pedirá que seleccionemos el certificado para la firma. Comprobamos que realmente está leyendo el certificado almacenado en la tarjeta si visualizamos (Dispositivo PKCS#11), como en la siguiente imagen. Pinchamos en el botón "Continuar":



Ahora se nos pedirá el PIN de la tarjeta para proceder a la firma. Introducimos el Pin (1) y pinchamos en "Firmar" (2)



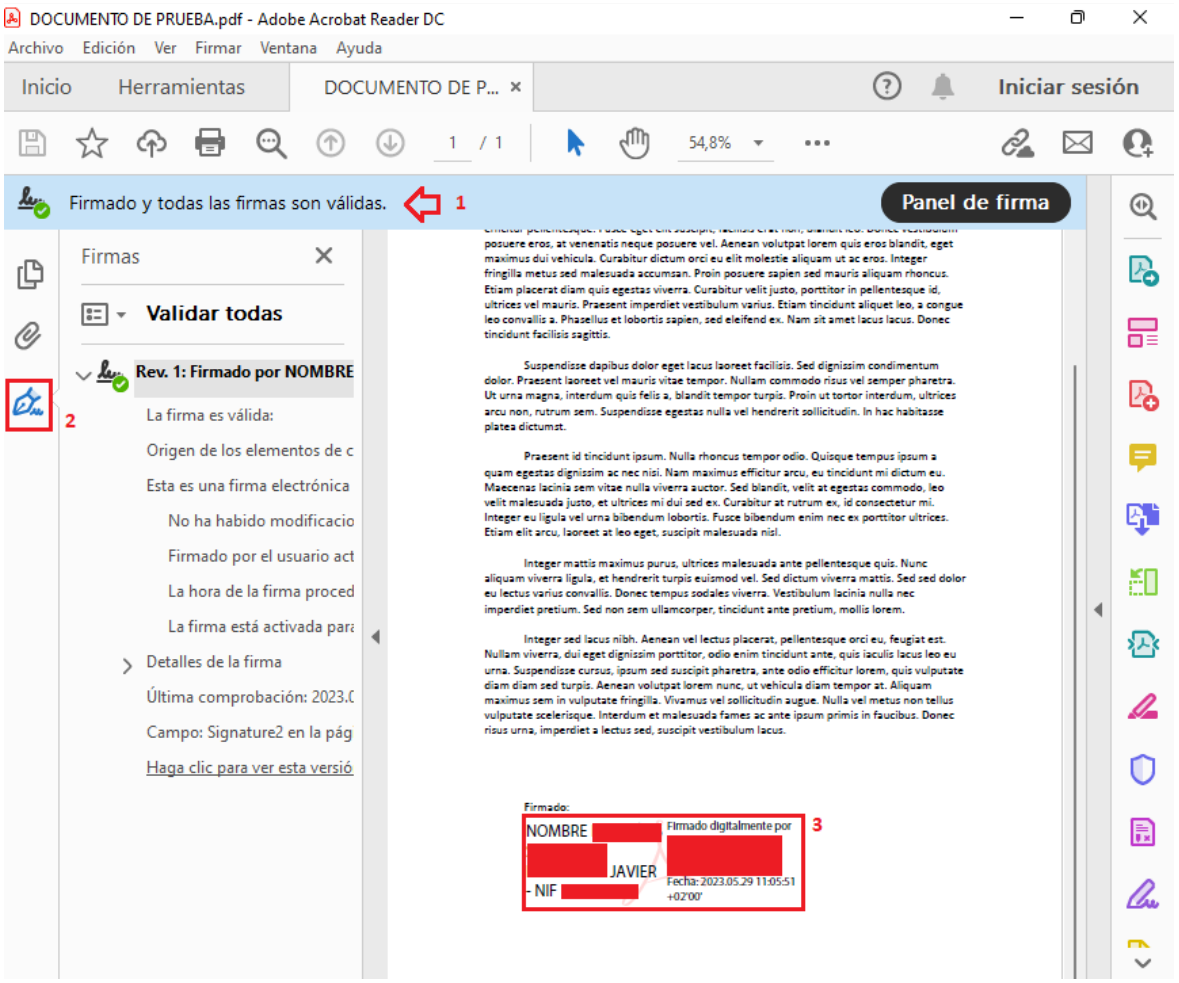
Adobe Reader nos preguntará dónde queremos guardar el PDF firmado. Seleccionamos la ubicación y el nombre de archivo deseado y guardamos el PDF. (También podemos sobreescribir el fichero si lo deseeamos)



4.- Verificación de las Firmas en Adobe Reader:

* La primera vez que abrimos un documento PDF puede tardar en realizar la validación porque Adobe tiene que descargar los certificados Raíz de ACA. A veces, la primera vez, será necesario cerrar y volver a abrir Adobe Reader o el documento para que se complete la validación.

Al abrir el documento que acabos de firmar, veremos que la firma se valida correctamente, marca verde (1). Si pinchamos en el panel de firmas (2) veremos los detalles de la firma y del certificado. Asimismo, comprobaremos que la firma visible también se visualiza documento (3)



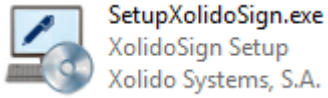
Xolido Sign - Aplicación gratuita para la firma de documentos PDF en sistemas Microsoft Windows

Instrucciones básicas para la descarga, instalación, configuración y uso de XolidoSign:

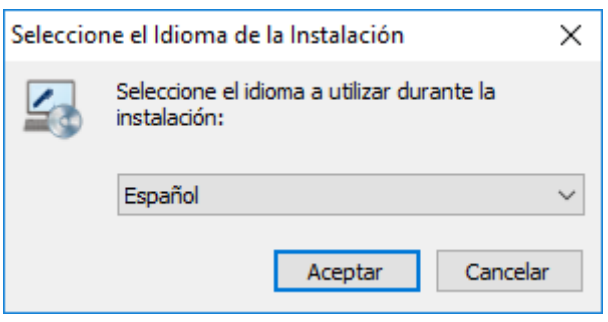
1.- Descarga: Descargue XolidoSign Desktop sólo desde la página web oficial:
https://www.xolido.com/lang/xolidosign/xolidosigndesktop/

2.- Instalación: Dependiendo del navegador que haya usado para la descarga, es posible que se le pregunte automáticamente si desea ejecutar el programa de instalación o no:

- Si su navegador le pregunta si desea ejecutar "SetupXolidoSign.exe", responda que sí.
- Si por el contrario no le pregunta, vaya a la carpeta de descargas y haga doble click en el programa de instalación "SetupXolidoSign.exe":

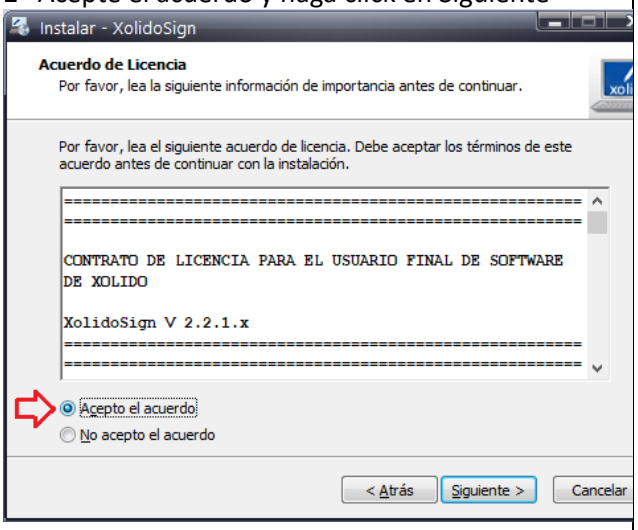


Una vez iniciado el proceso de instalación, siga los pasos como se muestra en las imágenes:

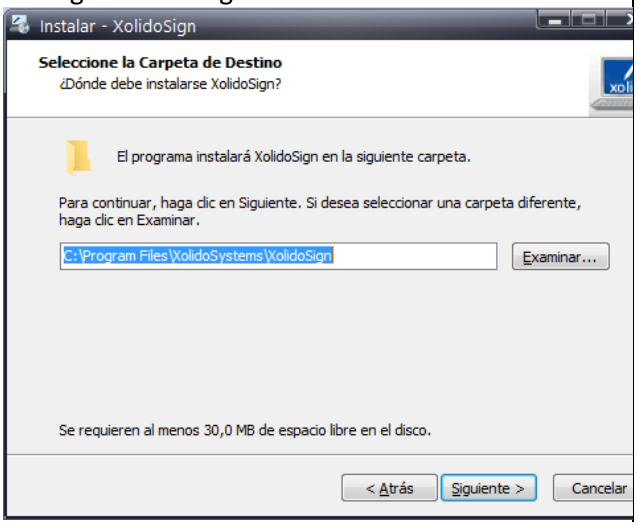


1º Haga click en Siguiente

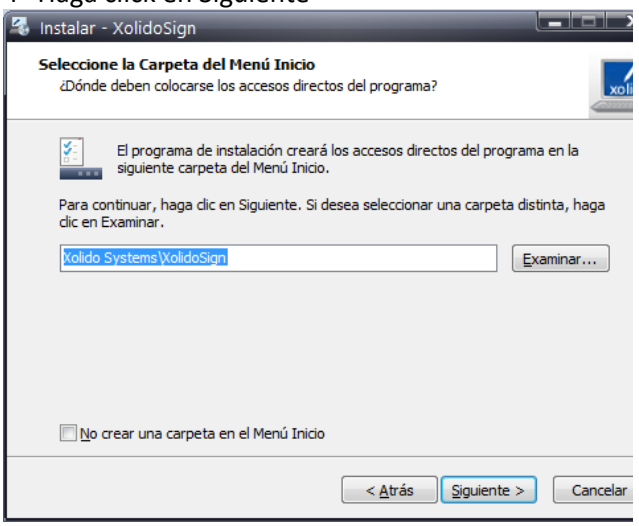
2º Acepte el acuerdo y haga click en Siguiente



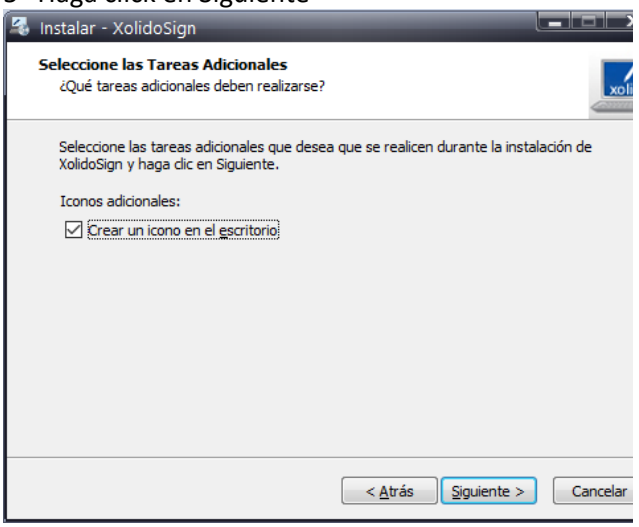
3º Haga click en Siguiente



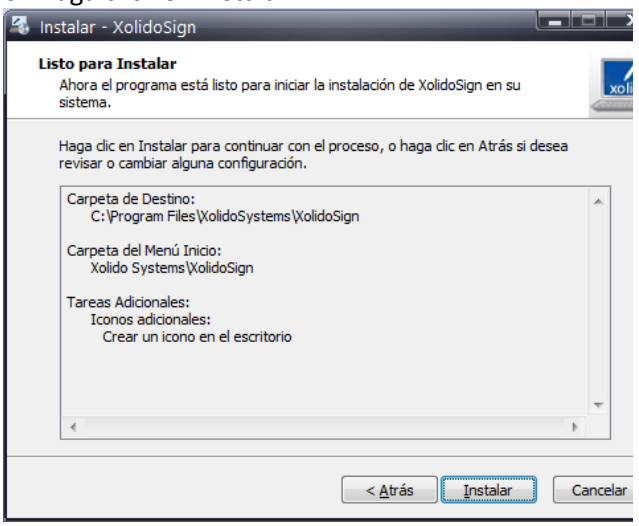
4º Haga click en Siguiente



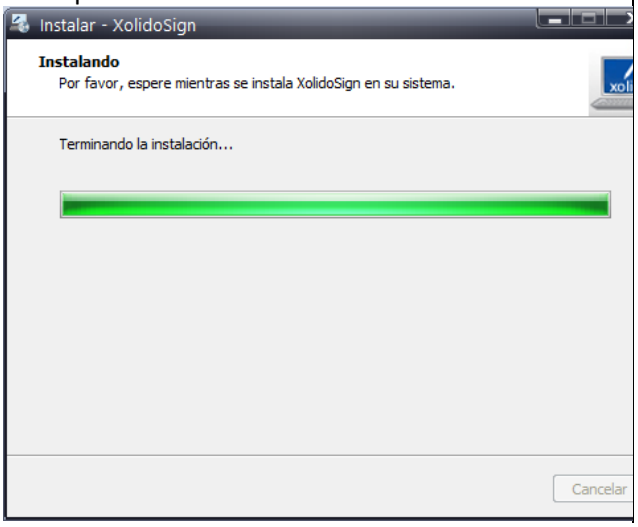
5º Haga click en Siguiente



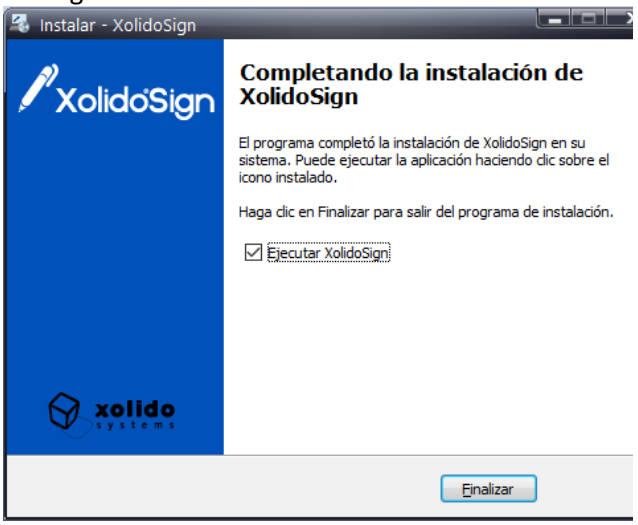
6º Haga click en Instalar



7º En proceso de instalación…



8º Haga click en Finalizar

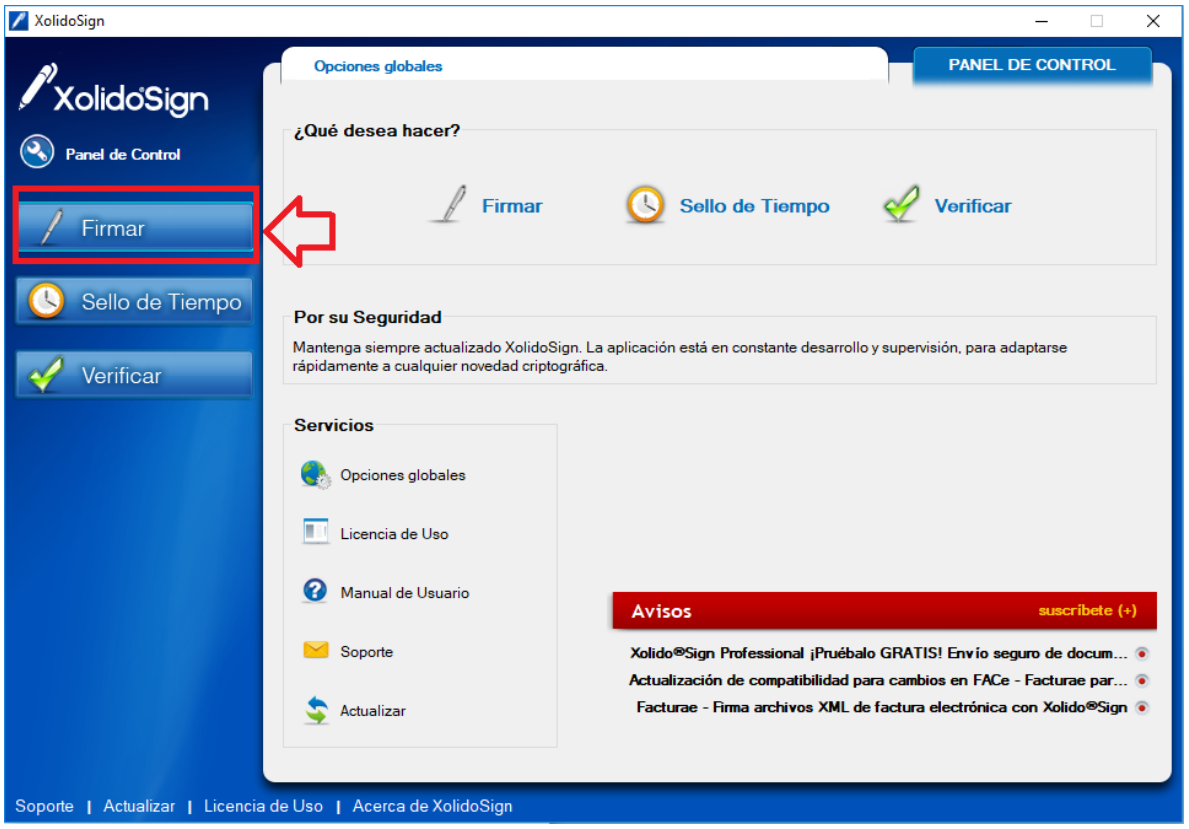


En este punto la instalación se habrá completado.
Se abrirá automáticamente XolidoSign.

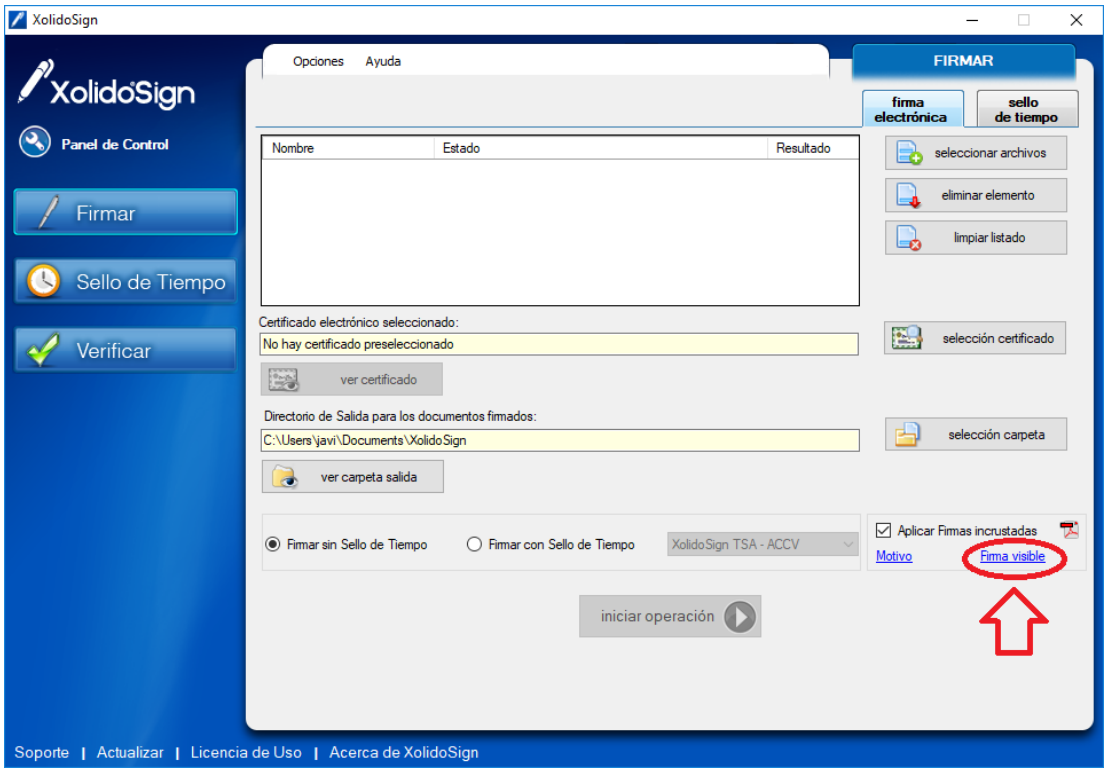
3.- Configuración inicial: Abra el programa (XolidoSign) que acaba de instalar, si no lo tiene ya abierto:

(Icono del programa)

En la pantalla de inicio de la aplicación pinchamos en el botón “Firmar”

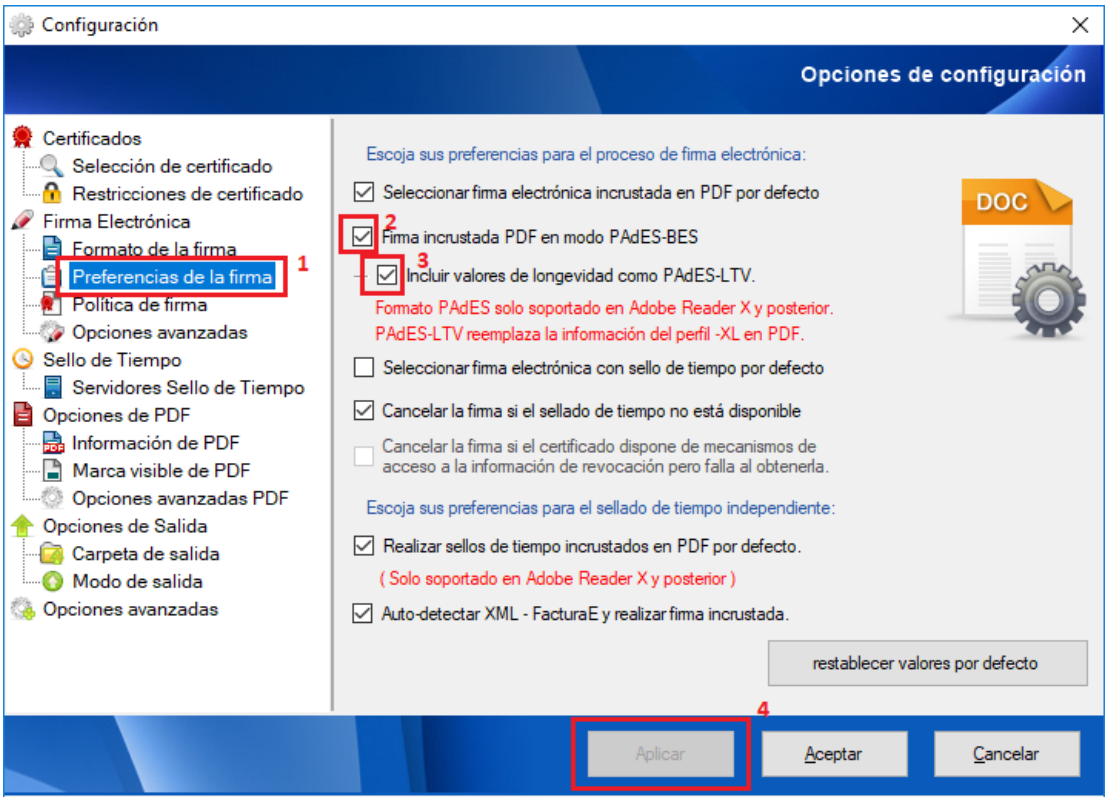


Se abrirá la pantalla de firma de documentos donde estableceremos, sólo hay que hacerlo una vez, la marca de visible que aparecerá en el documento PDF enlazada a su certificado. Para ello pinchamos en Firma visible



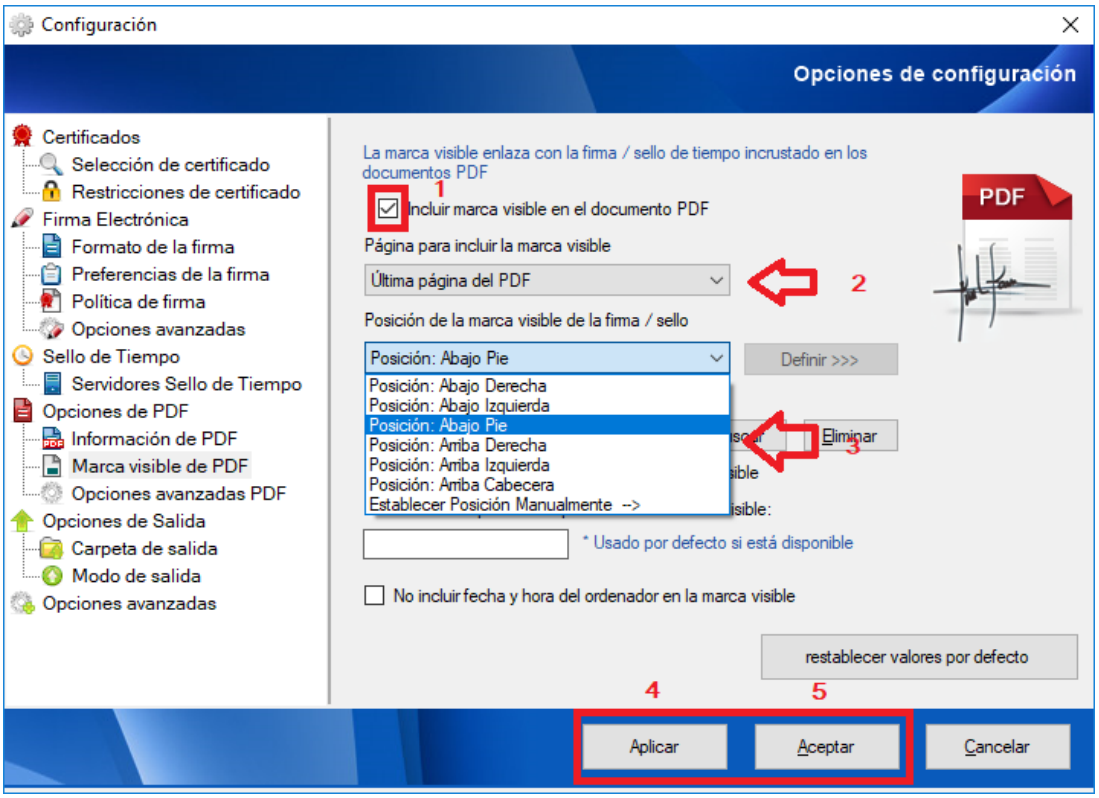
Configuramos el formato de la firma:

1. Seleccionamos "Preferencias de la firma" (1)
2. Marcamos la casilla "Firma incrustada PDF en modo PAdES-BES".
3. Marcamos la casilla "Incluir valores de longevidad como PAdES-LTV".
4. Aplicamos y Aceptamos los cambios.



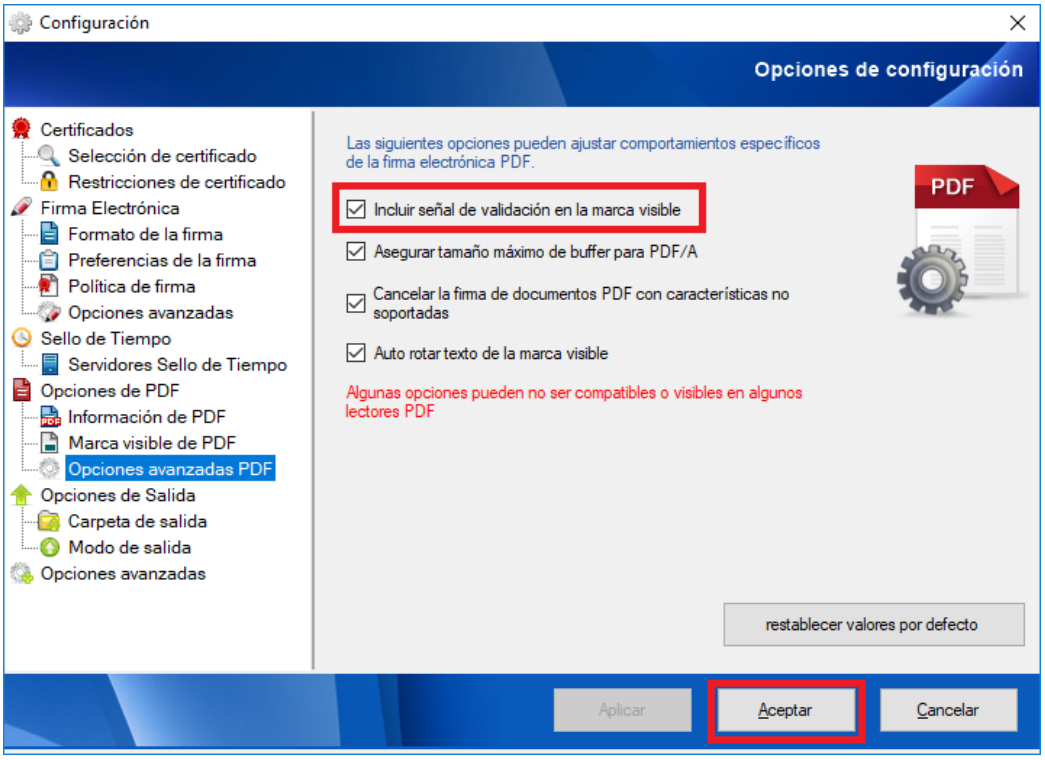
Configuramos la posición de la marca visible:

5. Marcamos “Incluir marca visible…”
6. Especificamos en qué página se insertará la marca visible (normalmente en la última página).
7. Seleccionamos la posición dentro de la página (normalmente al pie).
8. Aplicamos y Aceptamos los cambios.

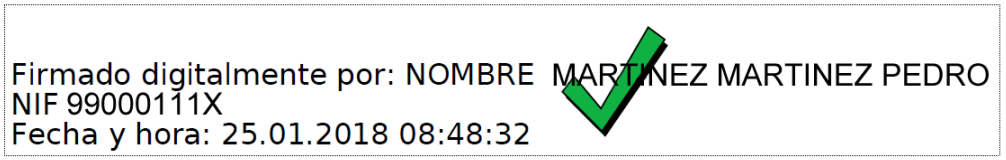


Si lo deseamos, también podemos incluir una marca de verificación junto con la marca visible:

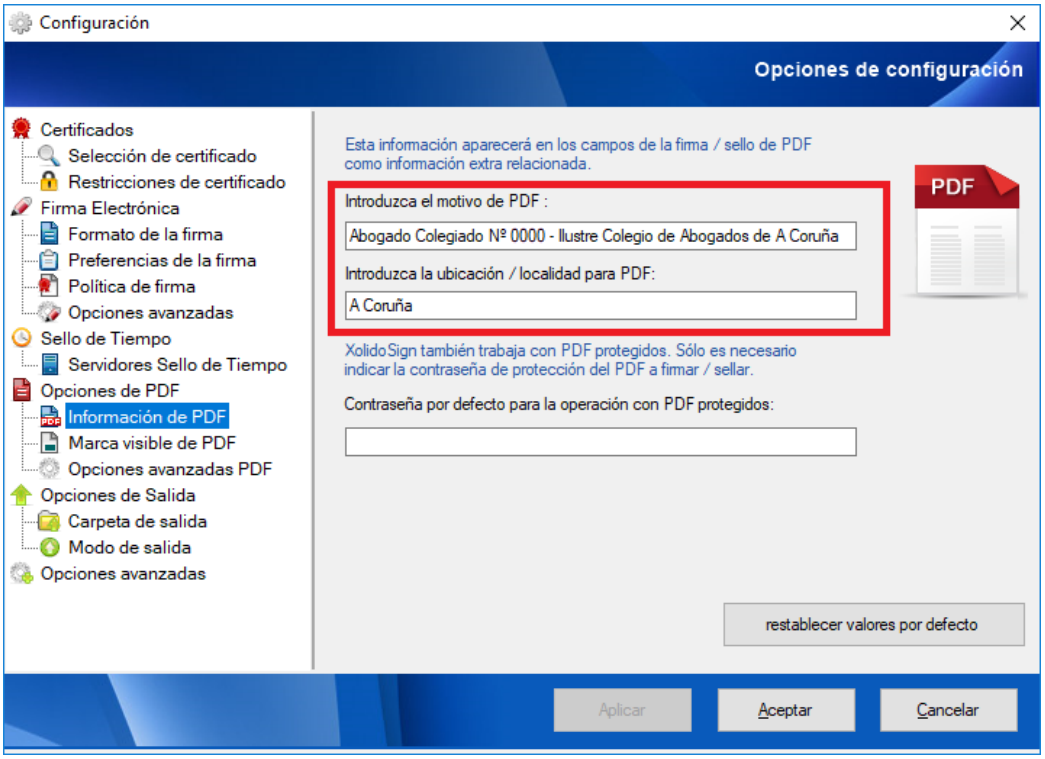
1. Dentro de configuración, seleccionamos “Opciones avanzadas PDF”
2. Marcamos la opción “Incluir señal de validación en la marca visible”
3. Aceptamos los cambios



Apariencia de la Firma visible en un documento PDF, junto con la marca de verificación, tras el proceso de firma:



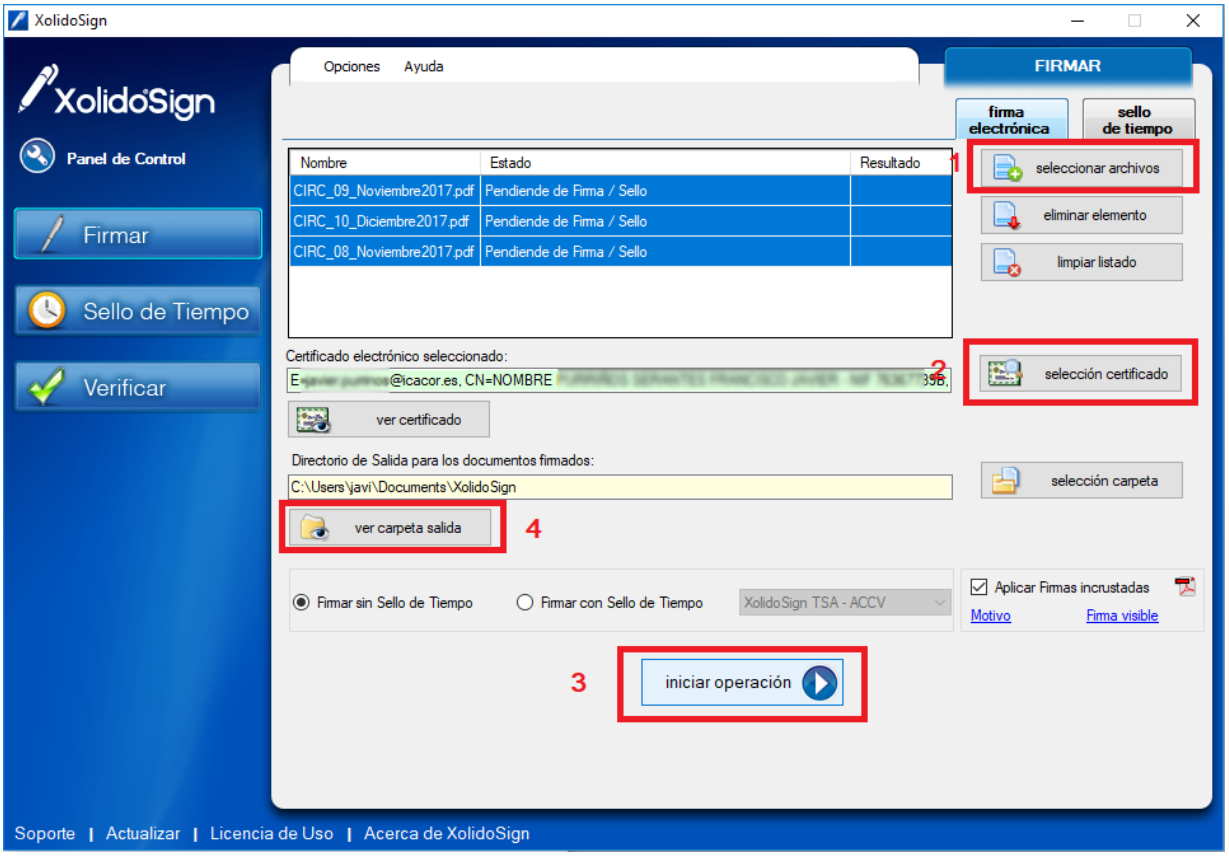
También es posible añadir al texto de la firma un motivo o descripción y la localidad. Esto se haría en el menú Opciones de PDF -> Información de PDF, dentro de las Opciones de configuración.



4.- Firma de documentos PDF:

Pasos para la firma de uno o varios documentos PDF.

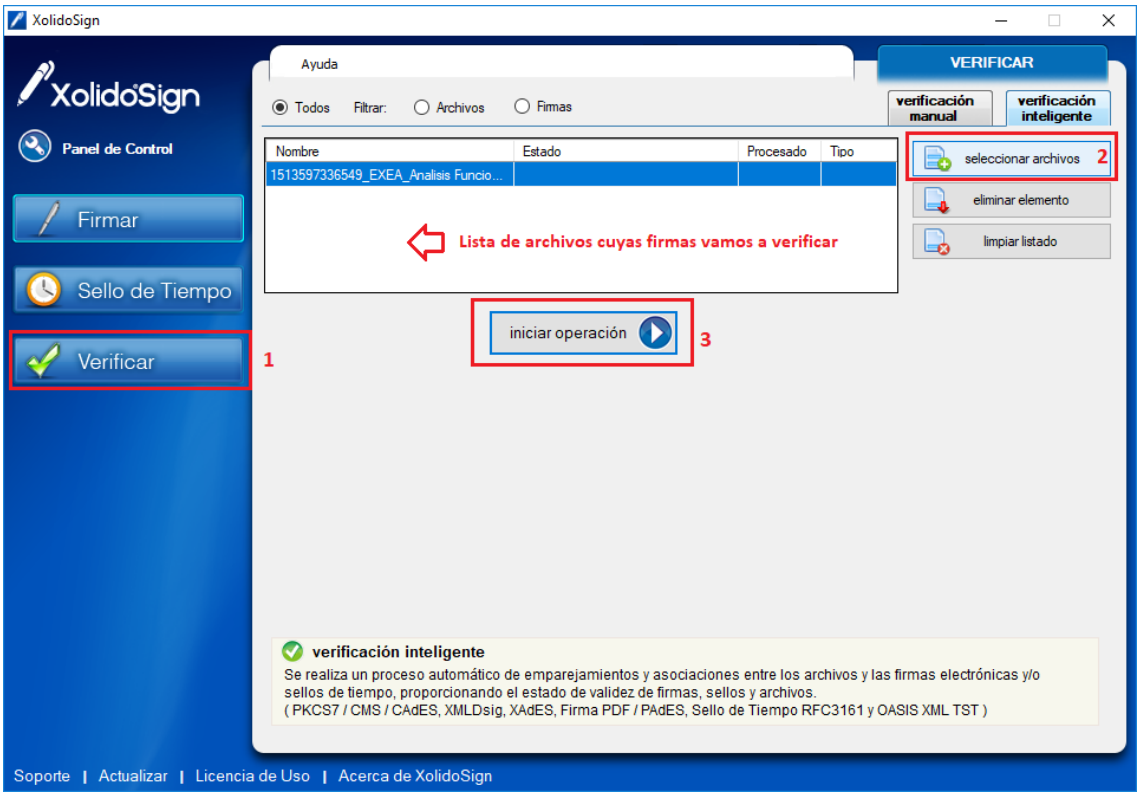
1. Seleccionamos tantos ficheros PDF como deseemos firmar. Los ficheros se irán agregando al listado de documentos pendientes de Firma.
2. Seleccionamos el certificado ACA o DNIe (LexNet no admite la firma con certificados instalables FNMT). Una vez seleccionado el certificado, Xolido verificará automáticamente que el certificado es válido (no está caducado ni revocado).
3. Iniciamos la operación de Firma. Nos pedirá el PIN de la tarjeta y firmará uno a uno los documentos.
4. Los documentos firmados se guardarán, por defecto, en la carpeta de firma de XolidoSign. Esta carpeta se crea automáticamente dentro de la carpeta "Documentos" de Windows.
   Aviso: XolidoSign no permite reemplazar el documento original con el firmado, ni guardar el documento firmado en la misma carpeta que el documento original. El PDF original y el firmado, por tanto, deben ubicarse siempre en carpetas distintas.



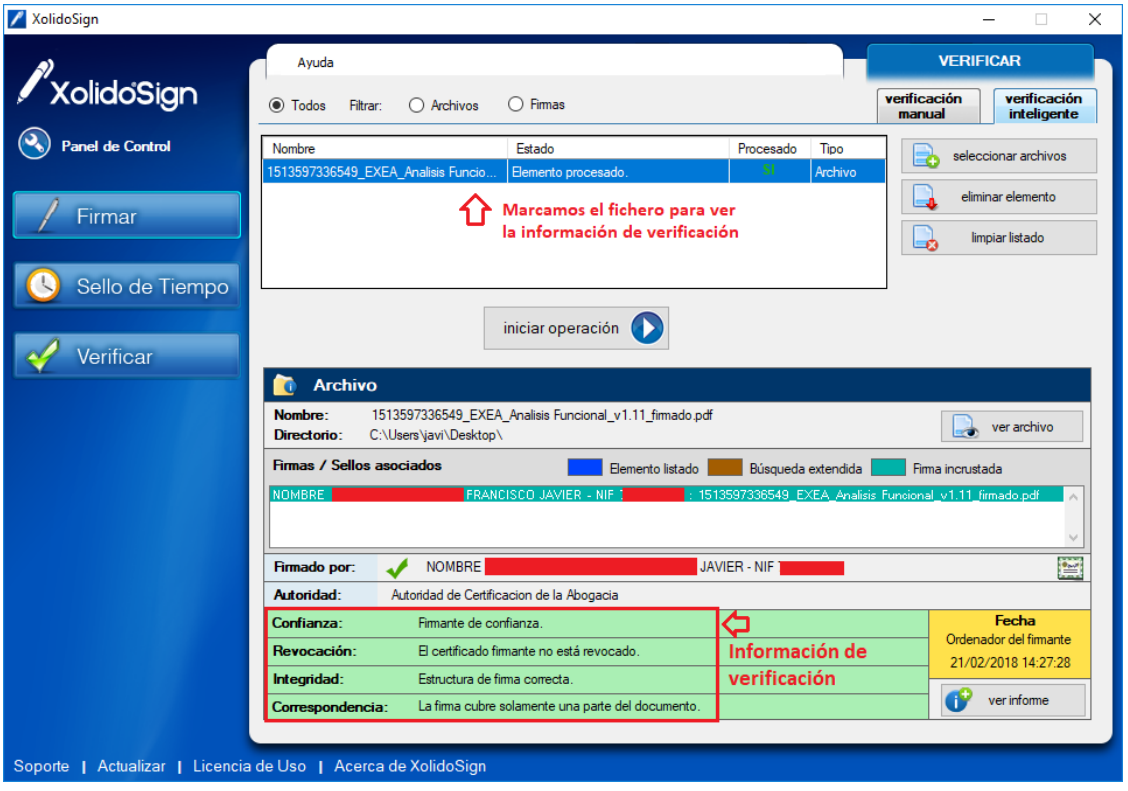
5.- Verificación de las firmas de documentos PDF:

Pasos para verificar la firma de uno o varios documentos PDF.

1. Pinchamos en el botón "Verificar" (1) en el menú de la izquierda.
2. A continuación, con el botón "seleccionar archivos" (2), seleccionamos tantos ficheros PDF como deseemos verificar. Los ficheros se irán agregando al listado de documentos pendientes de verificación.
3. Iniciamos la operación de Verificación pinchando en el botón "iniciar operación" (3).



Al seleccionar un fichero de la lista se visualizará la información de verificación correspondiente en el panel inferior.



6.- Actualizaciones:

XolidoSign debe estar actualizado para su correcto funcionamiento. Si en algún momento deja de detectar el certificado o de firmar correctamente lo primero que deberá hacer es verificar que no existe ninguna actualización pendiente. Pinchando en el enlace Actualizar de la aplicación se buscarán posibles actualizaciones, que dado el caso habrá que instalar obligatoriamente: