



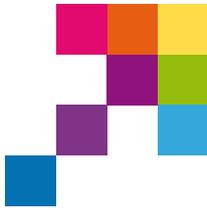
C/ Acceso Ademuz, Nº 12-1º-Pta 1 - 46980 Paterna (Valencia)  
www.ivnosys.com - Tel. 960 031 203

# DRIVER KEY CONTROLLER

## MANUAL DE INSTALACION, CONFIGURACION Y USO



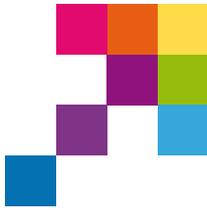




## ÍNDICE DE CONTENIDOS

<b>ÍNDICE DE CONTENIDOS</b>	<b>1</b>
<b>1. DRIVER KEYCONTROLLER PARA IVSIGN</b>	<b>2</b>
<b>2. INSTALACIÓN Y CONFIGURACIÓN ESTÁNDAR</b>	<b>3</b>
2.1. INSTALACIÓN MANUAL O ESTÁNDAR	3
2.2. CONFIGURACIÓN MANUAL O ESTÁNDAR	8
<b>3. INSTALACIÓN Y CONFIGURACIÓN DESATENDIDA</b>	<b>11</b>
3.1. INSTALACIÓN DESATENDIDA	11
3.2. CONFIGURACIÓN DESATENDIDA	13
<b>4. INSTALACIÓN DEL DRIVER MEDIANTE GPO</b>	<b>17</b>
4.1. AUTENTICACIÓN BÁSICA	21
4.2. AUTENTICACIÓN FEDERADA	23
<b>5. CONFIGURACIÓN DE ENTORNOS PKCS#11</b>	<b>26</b>
<b>6. PROCEDIMIENTO DE ACTUALIZACIÓN DE VERSIONES</b>	<b>30</b>
<b>7. GESTIÓN Y USO DE KEYCONTROLLER</b>	<b>31</b>
7.1. SISTEMA DE NOTIFICACIONES	31
7.2. PANEL DE CONTROL	32
7.3. HABILITAR/DESHABILITAR CERTIFICADOS	33





## 1. DRIVER KEYCONTROLLER PARA IVSIGN

**IvSign** es la solución para la firma electrónica segura.

Con **IvSign** no será necesario tener el certificado instalado en el propio dispositivo, gracias a que permite la centralización de todos los certificados en el propio **IvSign**.

**IvSign** consiente el almacenamiento de forma segura de los certificados digitales, para autorizar su uso en equipos de diversos usuarios, procesos y páginas web de forma centralizada y con trazabilidad de las operaciones.

Es el único medio que permite garantizar técnica y legalmente la identidad de una persona en internet, la firma electrónica de documento y cifrar las comunicaciones y contenido.

Para ello es necesaria la instalación y posterior configuración del **Driver KeyController**.



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

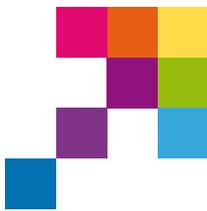


[sopORTE.ivsign@ivnosys.com](mailto:sopORTE.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia





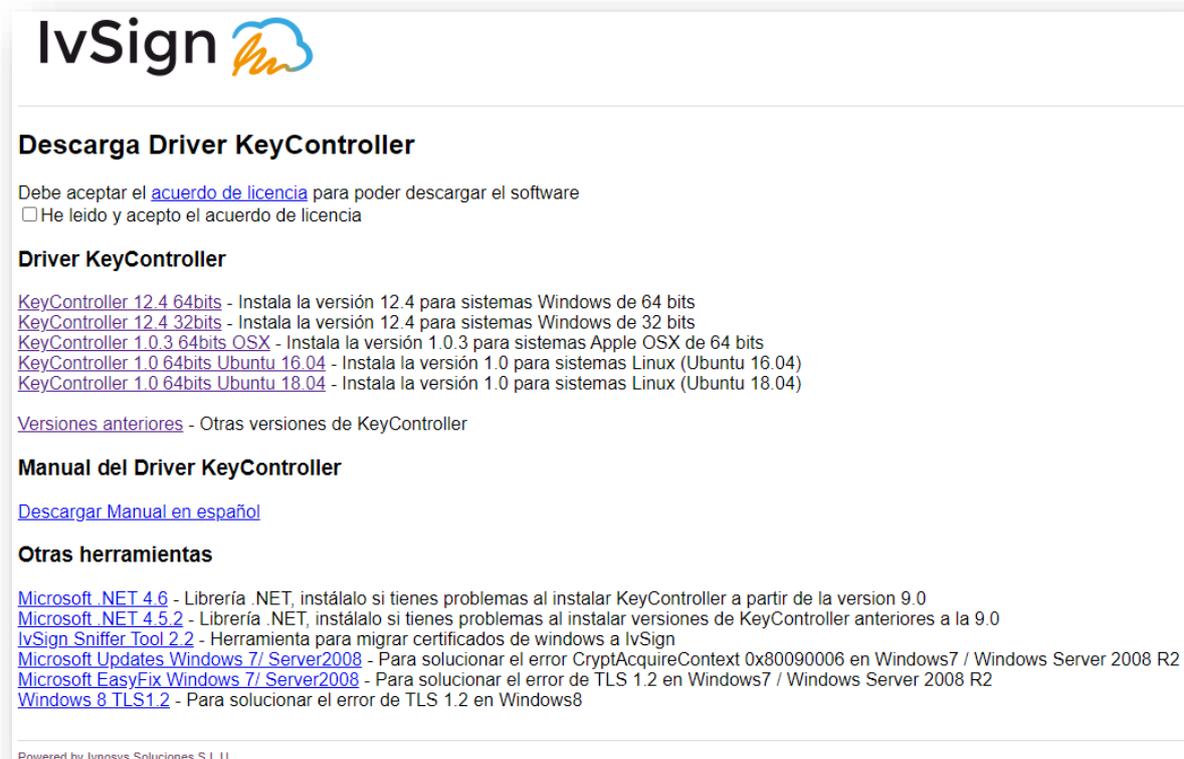
## 2. INSTALACIÓN Y CONFIGURACIÓN ESTÁNDAR

### 2.1. INSTALACIÓN MANUAL O ESTÁNDAR

Para usar el certificado con sus aplicaciones Windows, de igual modo que si se tratase de un certificado en SmartCard o Software, necesitará disponer del **Driver KeyController** que podrá descargar y configurar siguiendo estos sencillos pasos.

Accediendo a la siguiente url: <https://ivsdriver.com>

deberá leer y aceptar el acuerdo de licencia, antes de proceder a su descarga, pulsando la opción '**He leído y acepto el acuerdo de licencia**'.



**IvSign**

### Descarga Driver KeyController

Debe aceptar el [acuerdo de licencia](#) para poder descargar el software  
 He leído y acepto el acuerdo de licencia

#### Driver KeyController

[KeyController 12.4 64bits](#) - Instala la versión 12.4 para sistemas Windows de 64 bits  
[KeyController 12.4 32bits](#) - Instala la versión 12.4 para sistemas Windows de 32 bits  
[KeyController 1.0.3 64bits OSX](#) - Instala la versión 1.0.3 para sistemas Apple OSX de 64 bits  
[KeyController 1.0 64bits Ubuntu 16.04](#) - Instala la versión 1.0 para sistemas Linux (Ubuntu 16.04)  
[KeyController 1.0 64bits Ubuntu 18.04](#) - Instala la versión 1.0 para sistemas Linux (Ubuntu 18.04)

[Versiones anteriores](#) - Otras versiones de KeyController

#### Manual del Driver KeyController

[Descargar Manual en español](#)

#### Otras herramientas

[Microsoft .NET 4.6](#) - Librería .NET, instálalo si tienes problemas al instalar KeyController a partir de la versión 9.0  
[Microsoft .NET 4.5.2](#) - Librería .NET, instálalo si tienes problemas al instalar versiones de KeyController anteriores a la 9.0  
[IvSign Sniffer Tool 2.2](#) - Herramienta para migrar certificados de windows a IvSign  
[Microsoft Updates Windows 7/ Server2008](#) - Para solucionar el error CryptAcquireContext 0x80090006 en Windows7 / Windows Server 2008 R2  
[Microsoft EasyFix Windows 7/ Server2008](#) - Para solucionar el error de TLS 1.2 en Windows7 / Windows Server 2008 R2  
[Windows 8 TLS1.2](#) - Para solucionar el error de TLS 1.2 en Windows8

Powered by Ivnosys Soluciones S.L.U.

Tras pulsar sobre el enlace correspondiente, deberá ejecutar el fichero descargado y se mostrará el asistente para la instalación.



#### Nota:

Para instalar el driver es necesario tener permisos de administrador en el equipo.



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

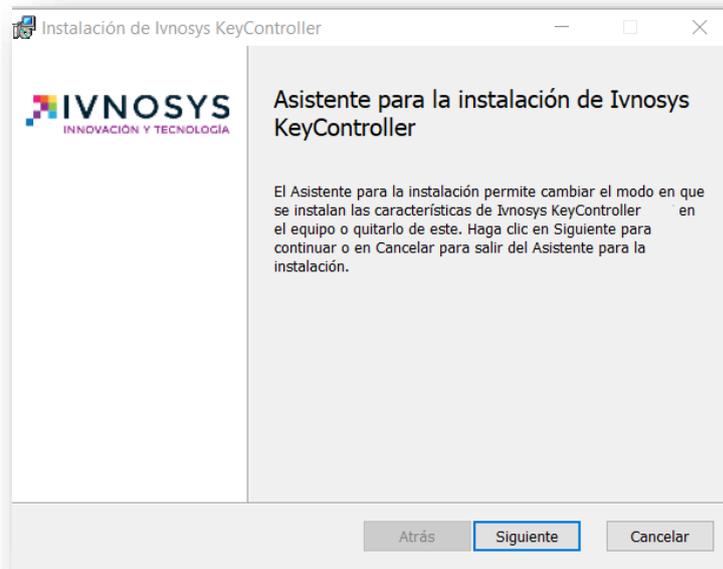
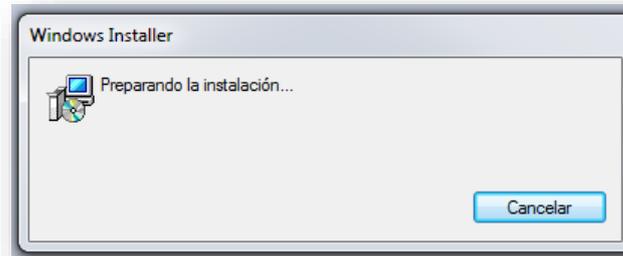
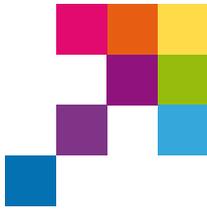


[suporte.ivsign@ivnosys.com](mailto:suporte.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia





Marca la casilla **Acepto los términos del contrato de licencia** y se activará el botón que permite iniciar la instalación.



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

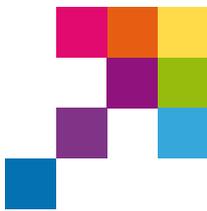


[sopORTE.ivsign@ivnosys.com](mailto:sopORTE.ivsign@ivnosys.com)



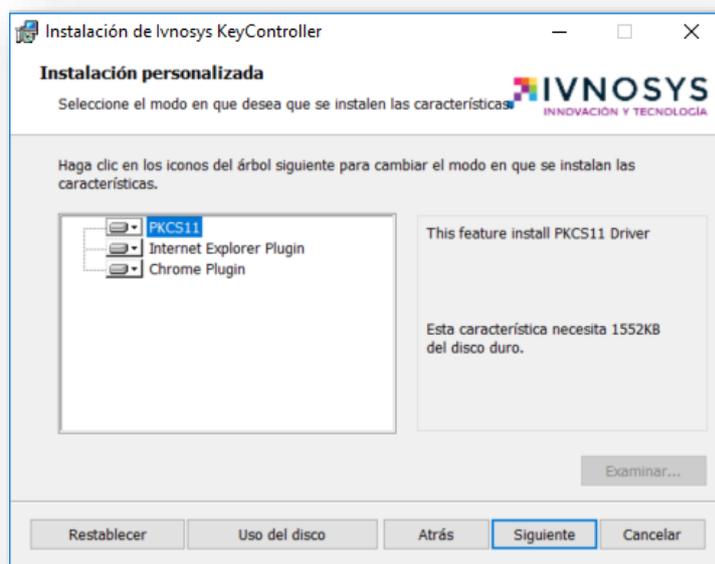
Madrid · Barcelona · Valencia





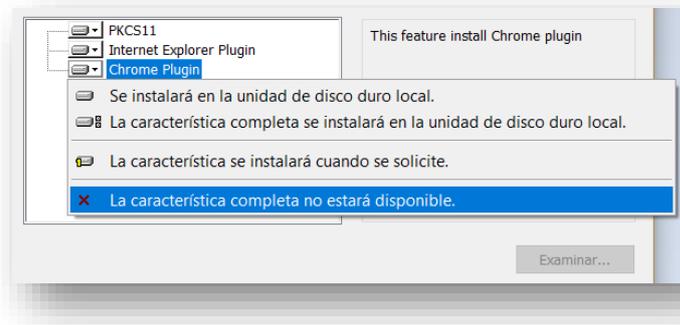
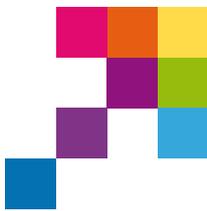
La siguiente pantalla permite seleccionar los componentes del Driver KeyController que se desea incluir en el proceso de instalación.

No obstante, la recomendación es que se mantengan los valores por defecto, manteniendo la instalación de todos los componentes.



Al pulsar sobre cada componente, se abrirá el menú contextual con todas las opciones disponibles para cada uno.

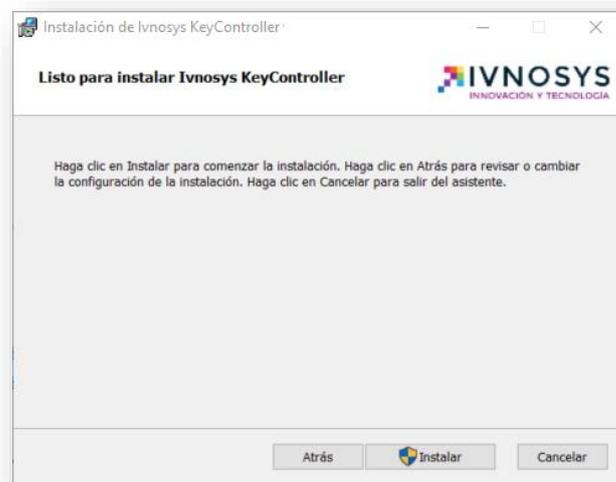




Por defecto todos los componentes vendrán marcados con la opción **Se instalará en la unidad de disco duro local**.

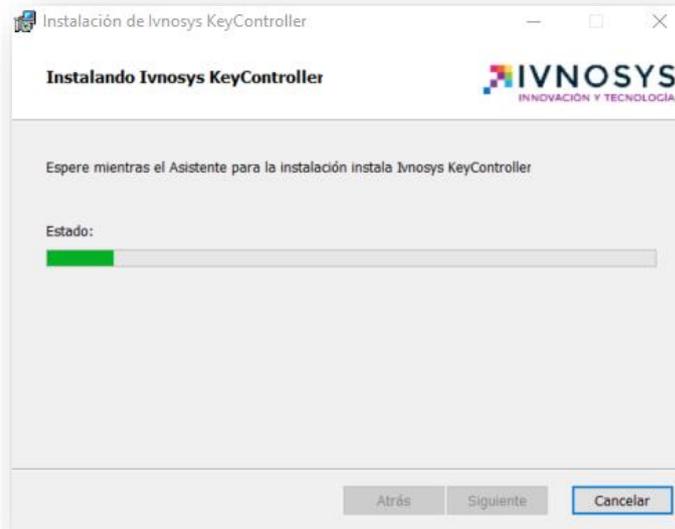
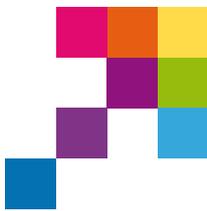
Si no se desea instalar, se deberá marcar la opción **La característica completa no estará disponible**.

Tras pulsar sobre la opción **Siguiente**, se solicitará confirmación para iniciar el proceso de instalación, en base a los parámetros seleccionados previamente.

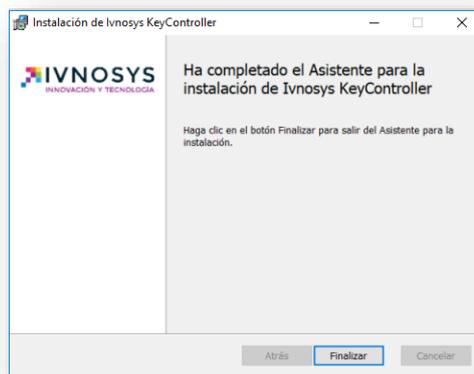


Pulsando sobre la opción **Instalar**, se mostrará la ventana que indicará el estado de la instalación, a través de la barra de progreso.

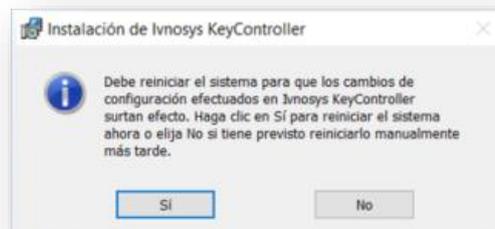




Finalizada la instalación, se pulsará el botón **FINALIZAR** para salir del asistente.



Por último, se solicitará el reinicio del equipo mediante el siguiente cuadro de diálogo:



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

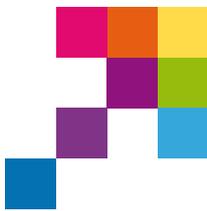


[suporte.ivsign@ivnosys.com](mailto:suporte.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia

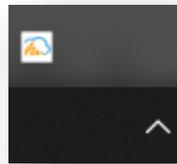




**IMPORTANTE.** El reinicio del equipo es un requisito para garantizar el correcto funcionamiento del sistema. Si no se permite o si se omite dicho reinicio, es posible que el driver no se ejecute correctamente o que presente un comportamiento inestable.

En el caso de que no sea posible reiniciar el equipo de forma inmediata, hay que asegurarse de que este reinicio se lleve a cabo a posteriori, antes de que los usuarios finales empiecen a trabajar con el driver.

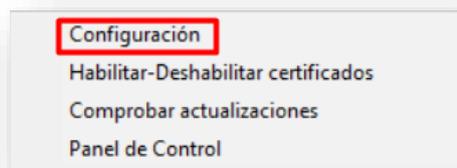
El icono del **Driver KeyController** se mostrará en la zona derecha de la barra de tareas de Windows, en el área de notificaciones.



## 2.2. CONFIGURACIÓN MANUAL O ESTÁNDAR

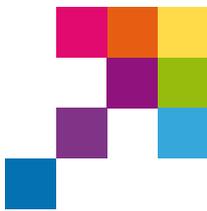
Para poder hacer uso de los certificados centralizados en **IvSign**, se deberá configurar la aplicación siguiendo los pasos indicados a continuación.

Pulsando sobre el icono del **Driver KeyController**, situado en el área de notificaciones, con el botón derecho del ratón, se mostrará el siguiente menú de opciones.



Se deberá pulsar sobre la opción **Configuración**, que deberá completarse con la siguiente información:

- **Servidor:** en este campo se introducirá el valor correspondiente a la dirección URL de la plataforma (por ejemplo, ivsign.net).
- **Autenticación:** seleccionar la opción *Autenticación integrada* o *Usuario y contraseña*, según corresponda.
  - **Autenticación integrada:** mediante esta opción, se tomarán los datos de la sesión activa de Windows, comprobando que exista el usuario en



el Directorio Activo de la organización, siempre que éste se encuentre en la misma red que el servidor de IvSign.

- **Usuario y Contraseña:** deberá indicar los datos facilitados en el correo *Bienvenido al servicio IvSign*, para acceder a la plataforma. Esta información se validará en la propia base de datos de IvSign.
- **Id Organización:** indicar el identificador de la organización, en caso de no disponer de él, póngase en contacto con su responsable de proyectos.



### NOTA

Si se ha modificado la contraseña, introduzca la nueva y no la del correo.

Podrá comprobar si las credenciales indicadas son correctas, pulsando el botón **Probar**.

Configuración

**KeyController** **IVNOSYS**  
INNOVACIÓN Y TECNOLOGÍA

Servidor: ivsign.net  
Autenticación: Usuario y contraseña  
ID Organización: organización  
Usuario: usuario  
Contraseña: \*\*\*\*\*

Probar Aceptar Cancelar

Configuración sin validar

Si las credenciales indicadas son correctas o incorrectas, se mostrará un mensaje indicándolo, en la parte inferior de la ventana de configuración.

Configuración

**KeyController** **IVNOSYS**  
INNOVACIÓN Y TECNOLOGÍA

Servidor: ivsign.net  
Autenticación: Usuario y contraseña  
ID Organización: organización  
Usuario: usuario  
Contraseña: \*\*\*\*\*

Probar Aceptar Cancelar

Error autenticando usuario

Configuración

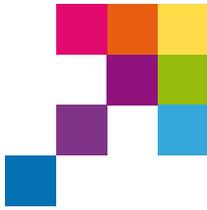
**KeyController** **IVNOSYS**  
INNOVACIÓN Y TECNOLOGÍA

Servidor: ivsign.net  
Autenticación: Usuario y contraseña  
ID Organización: organización  
Usuario: usuario  
Contraseña: \*\*\*\*\*

Probar Aceptar Cancelar

Configuración validada correctamente





Finalizadas las comprobaciones de la configuración indicada, se pulsará **Aceptar**.

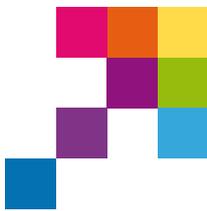
Los certificados que tuviera centralizados en **IvSign**, se mostrarán desde los navegadores y aplicaciones que hagan uso del almacén estándar de Windows.

En caso de no mostrarse de forma automática, sería recomendable reiniciar el sistema.



**NOTA.** Los certificados centralizados no pueden ser eliminados del sistema manualmente, ni tampoco podrá ser exportada su clave privada, pues en ningún caso se encuentran en el equipo donde se configuran.





## 3. INSTALACIÓN Y CONFIGURACIÓN DESATENDIDA

### 3.1. INSTALACIÓN DESATENDIDA

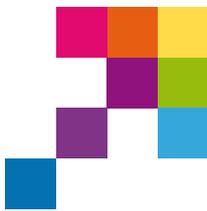
Desde la versión 5, la instalación de KeyController incorpora nuevos componentes y opciones de instalación adicionales. Por ejemplo, el sistema solicita el reinicio del equipo tras finalizar el proceso de instalación. Se trata de un requerimiento de la versión con el fin de garantizar el correcto funcionamiento del sistema.

En el caso de la instalación desatendida, este requerimiento puede ser omitido o personalizado en base a las opciones de instalación utilizadas.

En la siguiente tabla se detallan las opciones disponibles:

Opciones	Descripción
<b>Componentes</b>	<p>Para excluir todos los componentes adicionales del proceso de instalación se deben incluir los siguientes parámetros:</p> <pre>"ADDLOCAL=ALL REMOVE=PluginChrome,PluginIE,Pkcs11"</pre> <p>Por el contrario, es posible deshabilitar componentes de forma específica. Esto puede realizarse de dos formas: Bien utilizando el comando anterior (especificando solo un componente) o bien mediante la opción DISABLE y el nombre del componente, tal y como se muestra a continuación:</p> <pre>"DISABLE_PluginChrome=1"</pre> <pre>"DISABLE_PluginIE=1"</pre> <pre>"DISABLE_Pkcs11=1"</pre>
<b>Reinicio</b>	<p><b>/norestart</b> : Impide que el equipo se reinicie una vez completado el proceso de instalación.</p> <div style="border: 1px solid orange; padding: 10px; margin-top: 10px;"><p><b>NOTA:</b> de no incluir este parámetro, el ordenador se reiniciará automáticamente después de la instalación, sin posibilidad de cancelarla por parte del usuario.</p></div>





A continuación, se añaden algunos ejemplos:

**EJEMPLO.** Instalación de KeyController excluyendo todos los componentes y evitando el reinicio del equipo tras la instalación:

```
msiexec /q /i KeyController.msi ADDLOCAL=ALL REMOVE=PluginChrome,PluginIE,Pkcs11 /norestart
```

**\*Es importante que el /norestart esté al final de la línea**

**EJEMPLO:** Instalación de KeyController excluyendo tan solo el componente de Google Chrome (por el primero método) y forzando el reinicio del equipo tras el proceso de instalación:

```
msiexec /q /i KeyController.msi ADDLOCAL=ALL REMOVE=PluginChrome
```

**EJEMPLO:** Instalación de KeyController excluyendo tan solo el componente de Google Chrome (por el segundo método) y forzando el reinicio del equipo tras el proceso de instalación:

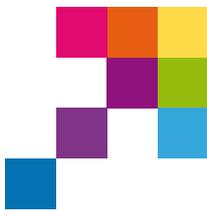
```
msiexec /q /i KeyController.msi DISABLE_PluginChrome=1
```



**IMPORTANTE:** El reinicio del equipo es un requisito para garantizar el correcto funcionamiento del driver. Si no se permite o si se omite dicho reinicio, es posible que el sistema no se ejecute correctamente o que presente un comportamiento inestable.

En el caso de que no sea posible reiniciar el equipo de forma inmediata, hay que asegurarse de que este reinicio se lleve a cabo a posteriori, antes de que los usuarios finales empiecen a trabajar con el driver.





## 3.2. CONFIGURACIÓN DESATENDIDA

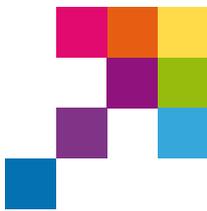
### Opción 01: configuración con parámetros por línea de comandos

El instalador MSI permite configurar el driver con valores por defecto en el momento de la instalación.

Algunos de los **parámetros** son los siguientes:

Parámetro	Descripción
<b>Server</b>	Establece el servidor configurado por defecto para nuevos usuarios.
<b>Serverfix</b>	Establece el servidor configurado de manera obligatoria para todos los usuarios (el valor no podrá ser modificado por el usuario).
<b>Auth</b>	Establece el tipo de autenticación: <ul style="list-style-type: none"><li>• pass &gt; Autenticación básica</li><li>• win &gt; Autenticación integrada</li><li>• external &gt; Autenticación externa, usando SAML</li></ul>
<b>Authfix</b>	Establece el tipo de autenticación de manera obligatoria (el valor no podrá ser modificado por el usuario).
<b>Orga</b>	Establece el código de organización de IvSign.
<b>Orgafix</b>	Establece el código de organización de forma obligatoria (el valor no podrá ser modificado por el usuario).
<b>noupdates</b>	Permite desactivar las comprobaciones de versión (usando el valor 1)
<b>nocertdisable</b>	Permite eliminar la posibilidad de habilitar-deshabilitar certificados desde el menú (usando el valor 1)
<b>acesopanel</b>	Permite habilitar la opción "Panel de control" en el menú contextual de KeyController (utilizando el valor 1)





### SSOPanel

Especifica si se permite el autologin en CertManager a través de la opción "Panel de Control" o desde una notificación (utilizando el valor 1).

Si se requiere obligatoriamente que el usuario introduzca su contraseña, se debe configurar con el valor 0.

### autoregister

Establece si KeyController debe crear la referencia del usuario en IvSign, cuando el usuario inicie sesión en el equipo (usando el valor 1).

Esta opción sólo es hábil para los sistemas de autenticación integrada.

### disabledforapps

Establece las aplicaciones para las que el driver no estará disponible. Si se configura un valor para el usuario o en fixed, este valor no será tenido en cuenta

### disabledforappsfix

Establece las aplicaciones para las que el driver no estará disponible. Si se configura este valor, SIEMPRE será tenido en cuenta, sin importar lo que tenga el usuario o el default

El listado de variables indicado en la tabla anterior no quiere indicar que solo se pueda configurar una vez se instala. Dichas variables son modificables desde el registro de Windows, en caso de disponer de permisos para su edición.

En el caso de que alguna configuración anterior se haya realizado en la organización de IvSign, prevalecerá dicha configuración en vez de la configurada en el propio equipo.



#### NOTA IMPORTANTE.

Hay que tener en cuenta que para realizar la instalación desatendida con el parámetro **/q**, se debe de ejecutar la consola en modo administrador.



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

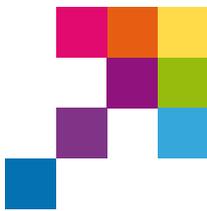


[suporte.ivsign@ivnosys.com](mailto:suporte.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia





A continuación, se añaden algunos ejemplos:

**EJEMPLO:** Ejemplo básico de instalación en el que se permite al usuario editar los campos del formulario y se deshabilita la comprobación de actualizaciones.

```
msiexec /q /i KeyController.msi server=ivsign.net auth=win orga=XXXX noudates=1 nocertdisable=1
```

**EJEMPLO:** A continuación, se repite el ejemplo anterior, pero restringiendo / bloqueando los campos para el usuario.

```
msiexec /q /i KeyController.msi serverfix= ivsign.net authfix=win orgafix=XXXX noudates=1 nocertdisable=1
```

## Opción 02: Configuración mediante el registro de Windows

Es posible modificar la configuración por defecto y obligatoria del servidor y método de autenticación del driver de un equipo mediante modificaciones en el registro.

Las **entradas del registro** disponibles son:

Entradas del registro	Descripción
[HKEY_CURRENT_USER\Software\Ivnosys\KeyController]	Establece la configuración específica para un usuario
[HKEY_LOCAL_MACHINE\SOFTWARE\Client\KeyController\fixed]	Establece valores obligatorios de todos los usuarios sin posibilidad de modificación.
[HKEY_LOCAL_MACHINE\SOFTWARE\Client\KeyController\default]	Contiene los valores de configuración por defecto.  KeyController utiliza estos valores si no encuentra información de configuración disponible en las dos rutas o paths anteriores.



www.ivnosys.com



96 003 12 03

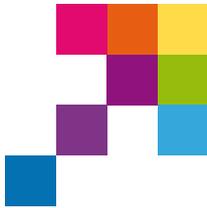


soporte.ivsign@ivnosys.com



Madrid · Barcelona · Valencia





**EJEMPLO:** Pongamos un ejemplo de configuración en el que se utilice ivsign.net y autenticación integrada de manera forzada. El archivo **reg** a ejecutar sería el siguiente:

```
-----  
Windows Registry Editor Version 5.00
```

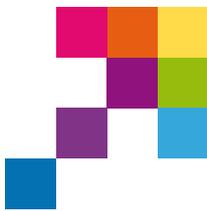
```
[HKEY_LOCAL_MACHINE\SOFTWARE\Clients\KeyController\fixed]  
"server"=" ivsign.net"  
"auth"="win"  
-----
```

**EJEMPLO:** Adicionalmente se incluye un ejemplo con autenticación federada de manera pre-determinada:

```
-----  
Windows Registry Editor Version 5.00
```

```
[HKEY_LOCAL_MACHINE\SOFTWARE\Clients\KeyController\default]  
"server"=" ivsign.net"  
"auth"="federated"  
"fedcode"="XXXXXXXXXXXX"  
-----
```





## 4. INSTALACIÓN DEL DRIVER MEDIANTE GPO

Para poder disponer del driver KeyController, en todos los equipos requeridos, se debe realizar una instalación a través de las políticas del dominio.

El primer paso es ubicar en un recurso compartido, accesible por todos los puestos, y con permisos para todos los usuarios, los ficheros de instalación (tanto para arquitecturas de 32 bits como para 64).

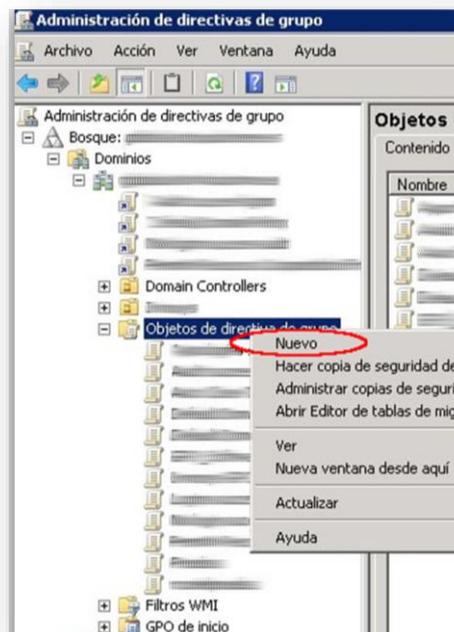


### NOTA IMPORTANTE.

Es importante que los instaladores sean MSI.

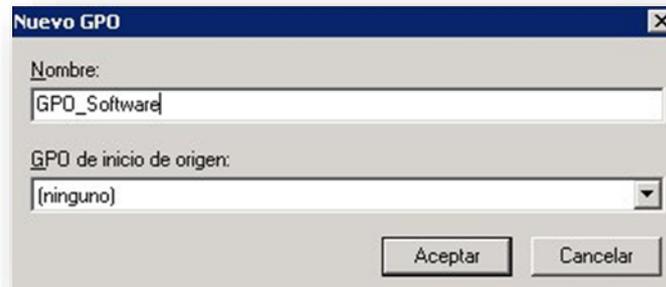
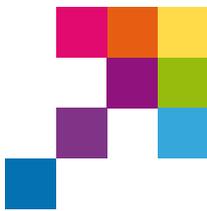
### PASOS A SEGUIR

Para generar la directiva encargada de realizar la instalación desatendida se lleva a cabo a través del **Administrador de directivas de grupo**. Para acceder a este panel, desde el controlador de dominio, se debe ejecutar el comando "gpmc".

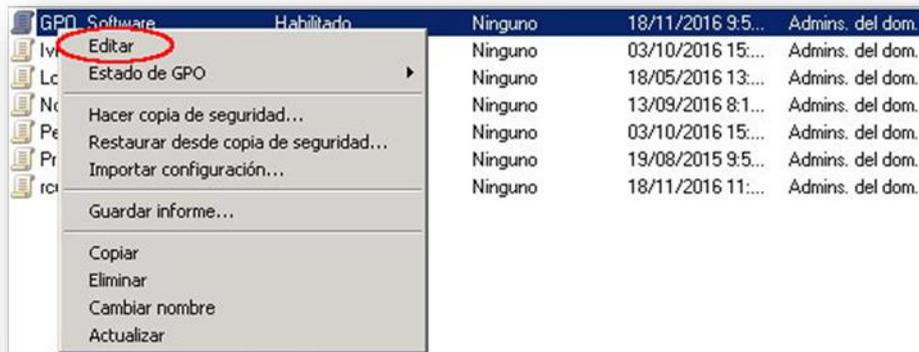


Dentro de este panel, desplegando el dominio empleado, y en **Objetos de directiva de grupos**, se debe crear uno nuevo.

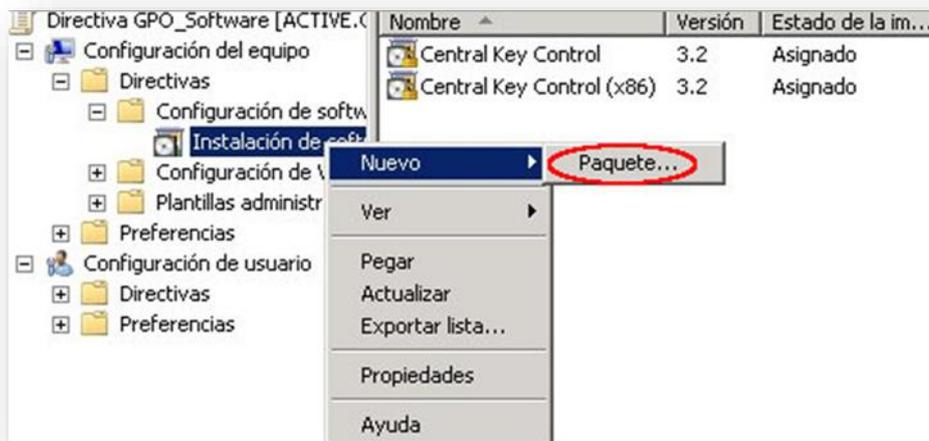


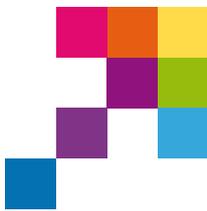


Edita la política creada.



En la nueva ventana sigue la ruta: **Configuración del equipo > Directivas > Configuración de software > Instalación de software**. En este último apartado, se creará un nuevo paquete por cada MSI.



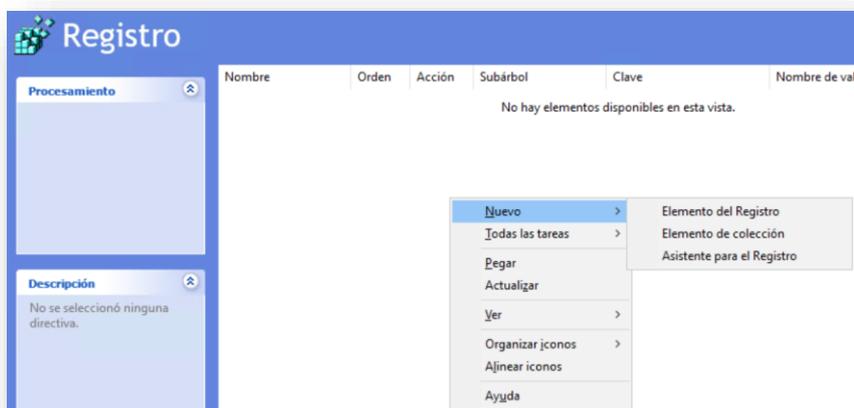


Una vez se dispongan de los paquetes de 32 y 64 bits, el siguiente paso consiste en configurar las variables del driver, para acceder a la siguiente ruta:

### Configuración del equipo > Preferencias > Configuración de Windows > Registro



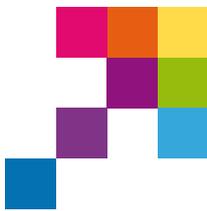
Se configurarán las variables haciendo click derecho con el ratón sobre la ventana de Registro > **Nuevo > Elemento del Registro.**



#### **NOTA IMPORTANTE.**

Las variables dependen de la configuración, para más información consulta con tu gestor de proyectos.

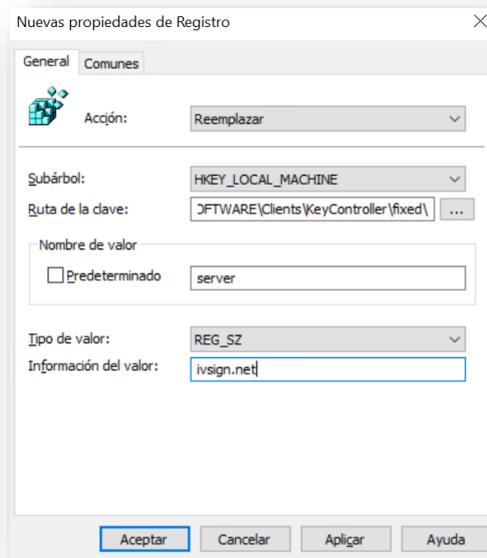




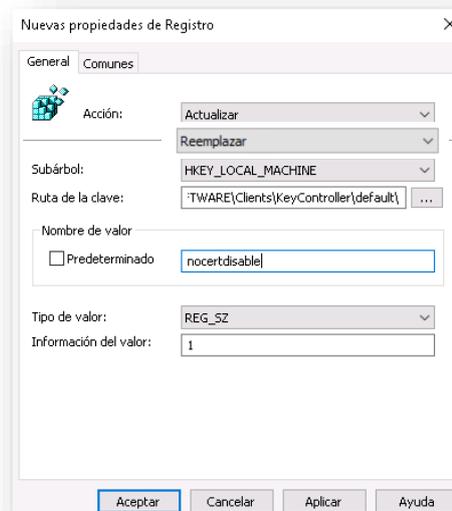
En las opciones de parametrización de KeyController, existen determinados campos que pueden bloquearse para que los usuarios no modifiquen su valor.

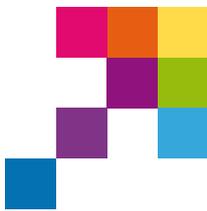
Revisa el apartado de [configuración con parámetros por línea de comandos](#) para ver el.

Como ejemplo de configuración de variables fijas y editables revisa las imágenes de ejemplo:  
Campo fijo o no editable por el usuario (**fixed**).



### 1. Campo editable por el usuario (**default**).





### NOTA IMPORTANTE.

Es importante que en el campo "**Acción**" contenga el valor de "**Reemplazar**" para evitar problemas de configuración.

A continuación, se detallan varias **configuraciones recomendadas** (según el método de autenticación) para instalaciones definitivas en puestos de cliente (en producción).

## 4.1. AUTENTICACIÓN BÁSICA

La siguiente tabla indica la configuración recomendada con autenticación básica en la cual se encuentran los campos *noupdates* y *nocertdisable* como bloqueados.

Parámetro	Config (editable o bloqueado)	Valor
<b>server</b>	fixed	*
<b>auth</b>	fixed	pass
<b>orga</b>	fixed	**
<b>noupdates</b>	default	1
<b>nocertdisable</b>	default	1

\***server**: Contiene la url de IvSign

\*\***orga**: Establece el código de organización de IvSign.

*[Si no dispone de estos datos, deberá solicitárselos a su Responsable de Proyecto]*

Como resultado de la configuración anterior, el driver quedará configurado de la siguiente manera:



www.ivnosys.com



96 003 12 03

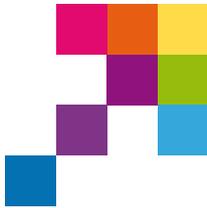


soporte.ivsign@ivnosys.com



Madrid · Barcelona · Valencia





Configuración

**KeyController**  INNOVACIÓN Y TECNOLOGÍA

Servidor:

Autenticación:

ID Organización:

Usuario:

Contraseña:

**Configuración sin validar**



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

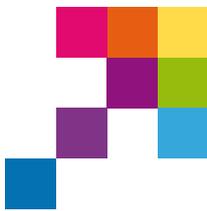


[soporte.ivsign@ivnosys.com](mailto:soporte.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia





## 4.2. AUTENTICACIÓN FEDERADA

Esta configuración establece la configuración recomendada con autenticación federada en la cual se encuentran los campos *noupdates* y *nocertdisable* como bloqueados.

Parámetro	Config (editable o bloqueado)	Valor
<b>server</b>	fixed	*
<b>auth</b>	fixed	federated
<b>fedcode</b>	fixed	**
<b>orga</b>	fixed	***
<b>noupdates</b>	default	1
<b>nocertdisable</b>	default	1

\***server**: Contiene la url de IvSign

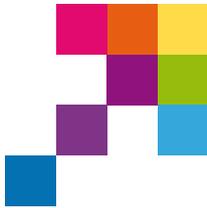
\*\***fedcode**: Código de federación. Requerido para el uso de autenticación federada y proporcionado al inicio del proyecto.

\*\*\***orga**: Establece el código de organización de IvSign.

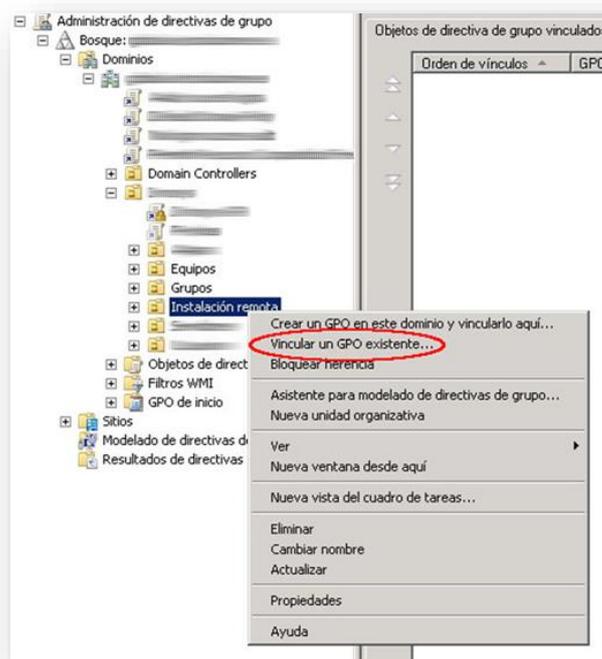
*[Si no dispone de estos datos, deberá solicitárselos a su Responsable de Proyecto]*

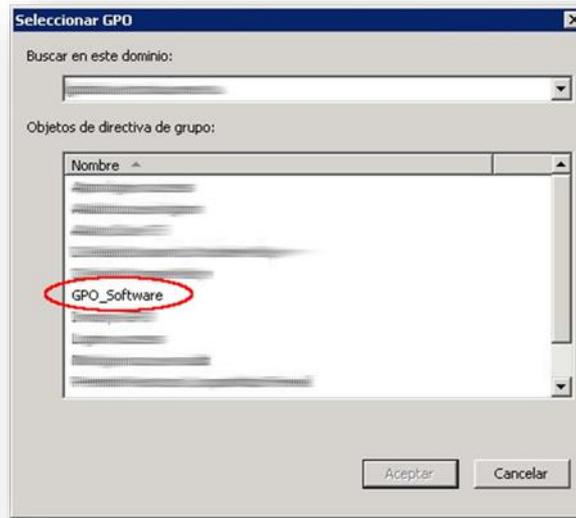
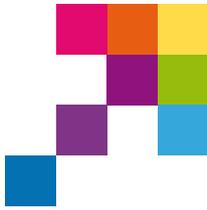
Como resultado de la configuración anterior, el driver quedará configurado de la siguiente manera:





Por último, en el Administrador de directivas de grupo, se debe seleccionar la unidad organizativa que contenga los equipos sobre los que se quiere realizar la instalación del driver, y se aplicará la GPO configurada en los pasos anteriores seleccionando Vincular un GPO existente.





Para que la instalación se haga efectiva, se puede esperar a que los equipos en cuestión sean reiniciados, o bien forzar una actualización de las directivas de grupo mediante el comando **"gpupdate /force"** (este comando debe ser lanzado en cada equipo cliente).



[www.ivnosys.com](http://www.ivnosys.com)



96 003 12 03

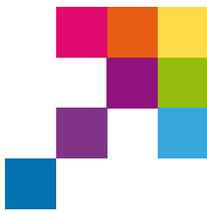


[sopORTE.ivsign@ivnosys.com](mailto:sopORTE.ivsign@ivnosys.com)



Madrid · Barcelona · Valencia

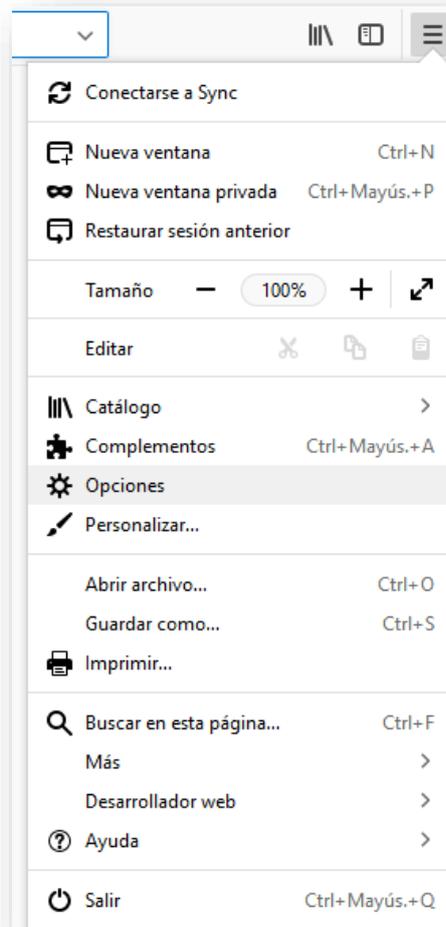


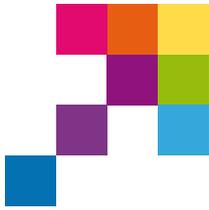


## 5. CONFIGURACIÓN DE ENTORNOS PKCS#11

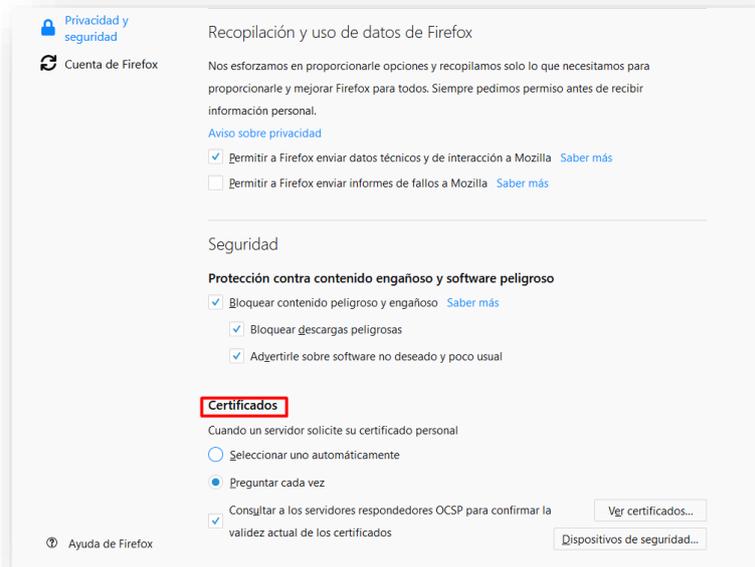
En Navegadores como Firefox u otros sistemas que necesiten de acceso estándar PKCS#11, será necesario configurar **KeyController Driver** como un proveedor criptográfico específico, como si se tratase de una SmartCard. El procedimiento es el siguiente:

1. Acceder al menú **Opciones**



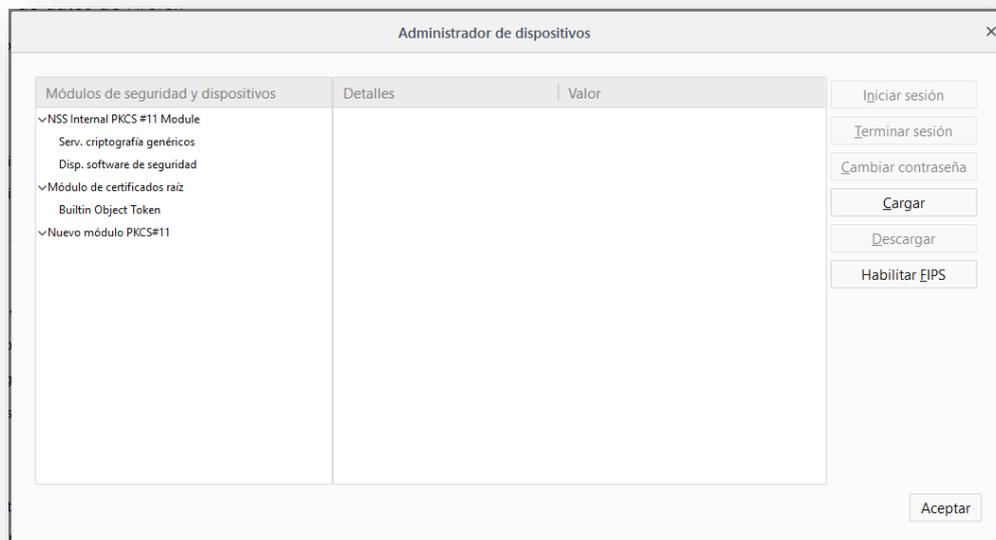


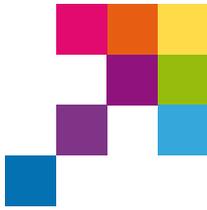
## 2. En la sección Privacidad y seguridad, buscar Certificados



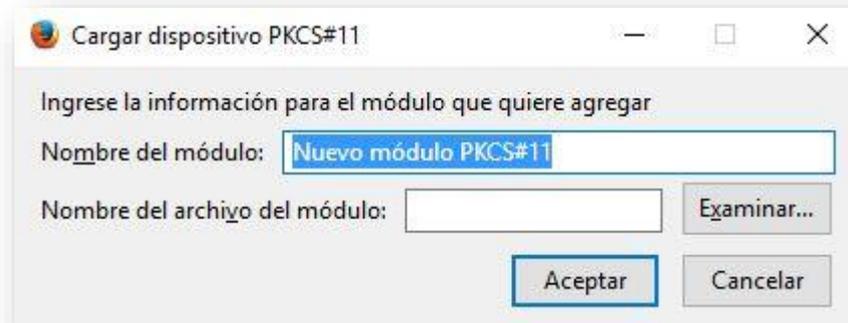
## 3. A continuación, pulsa el botón **Dispositivos de seguridad**

Aparecerá la siguiente pantalla:





#### 4. Pulsar el botón **Cargar** y seleccionar el módulo **PKCS#11**:



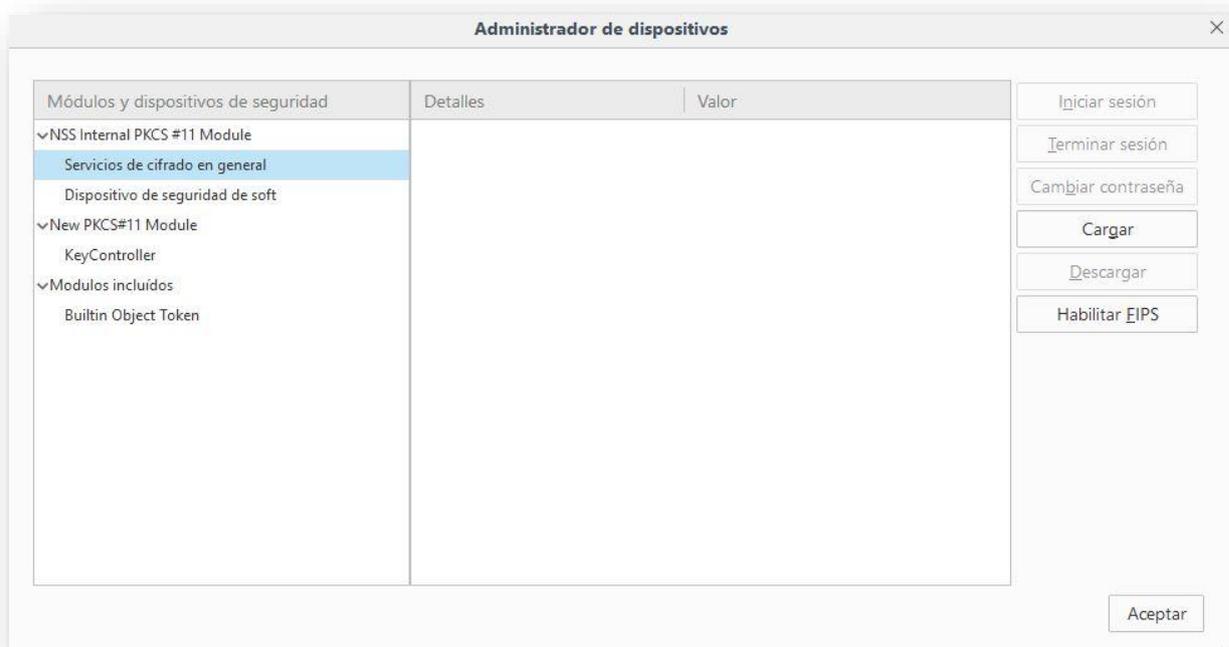
La **ubicación del driver** está por defecto en...

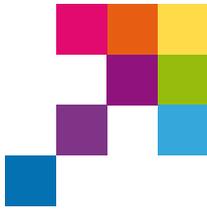
**%programFiles%\Ivnosys\KeyController**

...y en función de la plataforma del navegados, dentro del **subdirectorio x86 o x64**

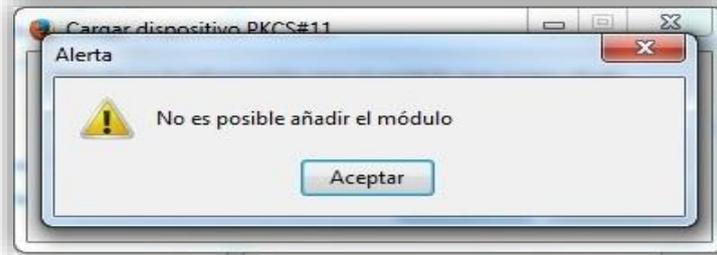
Normalmente será el directorio x86.

Si todo es correcto, debe quedar configurado del siguiente modo:

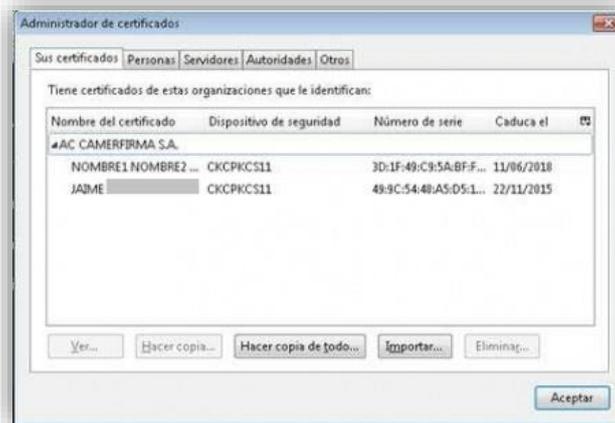


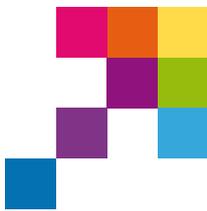


Si la ruta no es correcta o se selecciona la versión del driver que no corresponde con la arquitectura de compilación del navegador, se mostrará el siguiente aviso y no se habrá configurado correctamente:



Seguidamente **Los certificados aparecerán en Firefox** como cualquier otro certificado importado desde un p12 o en SmartCard:





## 6. PROCEDIMIENTO DE ACTUALIZACIÓN DE VERSIONES

Periódicamente, el **Driver KeyController** informará de la última versión disponible, en una ventana de aviso en la barra de notificaciones.



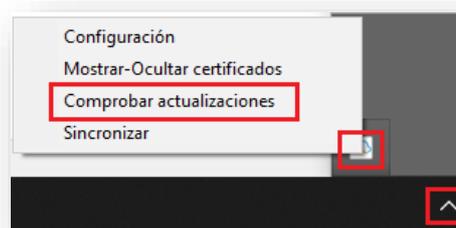
Pulsando sobre el mensaje, se descargará el fichero que deberá **EJECUTAR** para que se apliquen las actualizaciones.

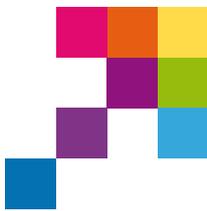


### NOTA IMPORTANTE.

Será imprescindible disponer de permisos de administrador en el equipo, para que se ejecute correctamente.

En caso de querer comprobar si está disponible alguna nueva versión sin esperar a la notificación automática, se podrá hacer la comprobación pulsando, sobre el icono situado en la barra de notificaciones, con el botón derecho del ratón, sobre la opción **Comprobar actualizaciones**.





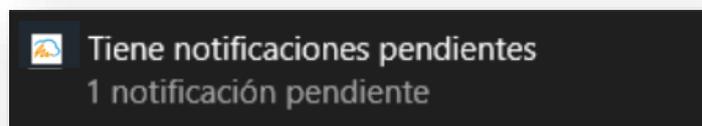
## 7. GESTIÓN Y USO DE KEYCONTROLLER

### 7.1. SISTEMA DE NOTIFICACIONES

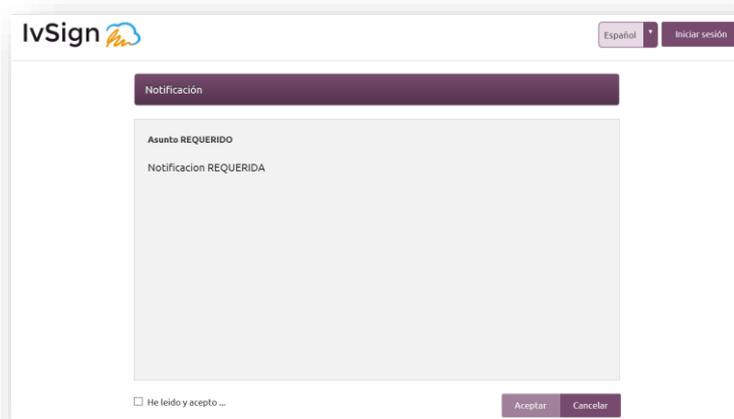
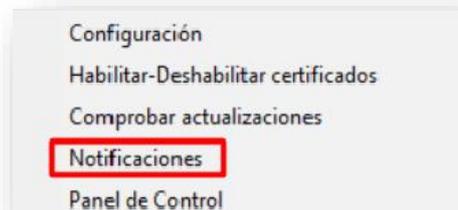
Desde la plataforma de **IvSign** se envían notificaciones informativas a los usuarios sobre las gestiones de la propia plataforma.

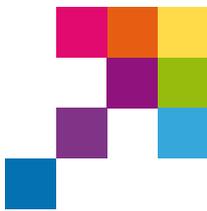
Para leer estas notificaciones hay que acceder a la plataforma de **IvSign**.

El **Driver KeyController** avisa de que hay notificaciones pendientes de leer, mostrando el siguiente mensaje:



La opción **Notificaciones** del **Driver KeyController**, aparece disponible cuando detecta que hay notificaciones pendientes de lectura. Al pulsar sobre el menú **Notificaciones**, abre el navegador enlazado a la plataforma de **IvSign**, para que el usuario pueda leer las notificaciones.

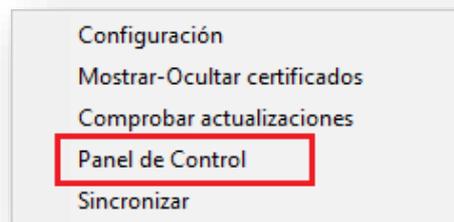




## 7.2. PANEL DE CONTROL

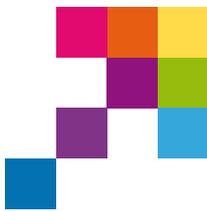
La opción del menú de “**Panel de Control**”, es un acceso directo desde el **Driver KeyController** a la plataforma de **IvSign**.

Pulsando sobre este menú, se abre el navegador y enlaza a la plataforma de **IvSign** para que el usuario se identifique pudiendo acceder a todas las opciones de la propia plataforma.



Se requiere activarlo a nivel de configuración en el equipo con la variable *accesopanel=1*, ya bien sea desde el registro de Windows o al instalarlo por línea de comandos.





### 7.3. HABILITAR/DESHABILITAR CERTIFICADOS

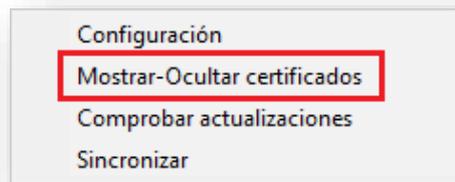


#### NOTA IMPORTANTE.

Esta opción estará disponible por defecto a no ser que al instalarse se haya incluido el valor `nocertdisable=1` para que se oculte.

En el caso de disponer de muchos certificados, para evitar que se muestren todos cada vez que necesitemos realizar alguna acción con ellos (firmar, acceder a una web,...) está disponible la opción de **Habilitar/Deshabilitar certificados**.

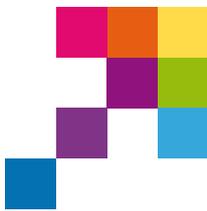
Pulsando sobre el icono del **Driver KeyController**, situado en el área de notificaciones, con el botón derecho del ratón.



Esta opción únicamente permite trabajar con los certificados que actualmente están habilitados en IvSign.

Los que dispongan del icono  en la columna OPCIONES **si se mostrarán**.





Nombre	Estado	Asunto	Certid	Opciones
Certificado	✓	Nombre Apellido Apellido	89D59944BECD	
Certificado	🔒	Nombre Apellido Apellido	89D521B893EB	

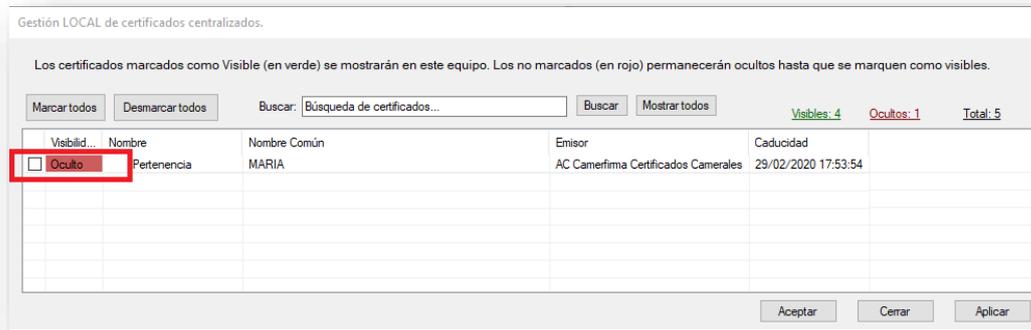
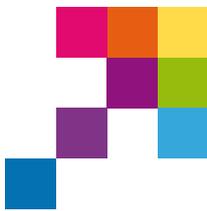
Los que se encuentren deshabilitados en IvSign (por haberse puesto mal el PIN varias veces, por haber sido deshabilitados manualmente, ...), no se mostrarán disponibles en el driver.

Los que dispongan del icono  en la columna OPCIONES **no se mostrarán**.

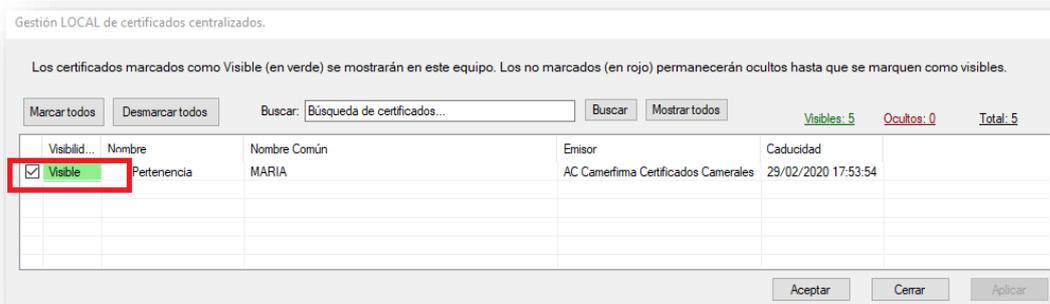
Nombre	Estado	Asunto	Certid	Opciones
Certificado	✓	Nombre Apellido Apellido	89D59944BECD	
Certificado	🔒	Nombre Apellido Apellido	89D521B893EB	

**Estas acciones de habilitar o deshabilitar, sólo afectaran al equipo desde el que se está accediendo.** Es decir, si existe un certificado delegado a otro usuario, los cambios de habilitar o deshabilitar, únicamente funcionarán en el equipo en el que se está haciendo. La persona que tenga ese certificado delegado deberá habilitar o deshabilitar los suyos en su equipo.

Para mostrar un certificado que esté oculto, se pulsará la casilla **OCULTO** de ese certificado.

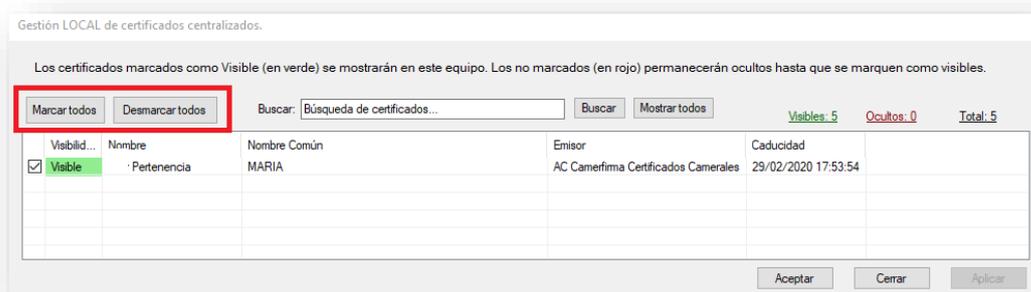


Para no mostrar un certificado que esté visible, se pulsará la casilla **VISIBLE** de ese certificado.



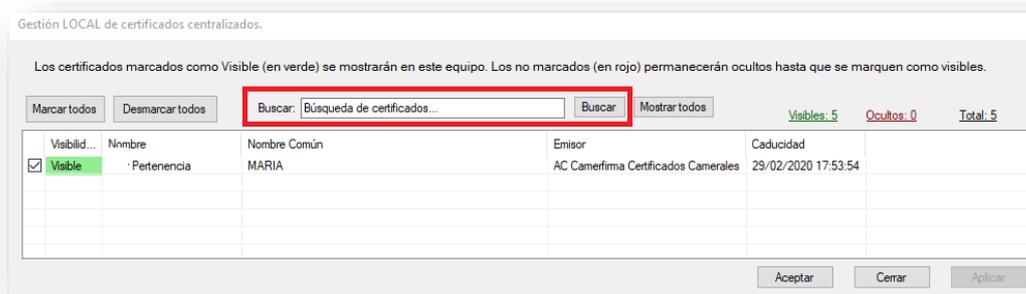
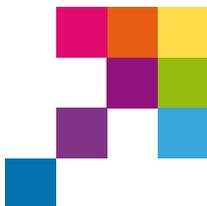
En ambos casos, la VISIBILIDAD cambiará automáticamente.

Estas acciones se podrán realizar de forma individual o de forma masiva pulsando **Marcar todos** o **Desmarcar todos**.



Se podrán filtrar los certificados por el contenido de todas las columnas (Visibilidad, Nombre, Nombre Común, Emisor o Caducidad) indicando el texto en el campo **Buscar** y pulsando INTRO o el botón **Buscar**. Se mostrarán todos los certificados que coincidan con el texto indicado.





Para volver a mostrar todos los certificados de nuevo y poder realizar otro filtro, se pulsará **Mostrar todos**.

