

UNIVERSIDAD DE
MURCIA



Manual de usuario para el uso del certificado electrónico en la Universidad de Murcia

Versión: 3.1



Contenido

Contenido	2
1 ¿Qué puedo encontrar en este manual?.....	4
2 Uso del certificado electrónico desde la tarjeta universitaria.....	5
2.1 Introducción	5
2.2 Tarjeta universitaria	6
2.3 Software de la TUI.....	6
2.3.1 Instalación mediante el instalador.....	8
2.3.1.1 Windows	9
2.3.1.2 Linux	12
2.3.1.3 Mac OSX	13
2.3.2 Desinstalación del Software TUI.....	16
2.3.2.1 Windows	16
2.3.3 Configuración de los módulos PKCS#11 para Firefox y Thunderbird (y Chrome/Chromium en Linux)	18
2.3.3.1 Configuración de los módulos PKCS#11 de forma manual	19
2.3.3.1.1 Mozilla Firefox.....	19
2.3.3.1.2 Mozilla Thunderbird.....	25
2.3.3.1.3 Configuración del módulo “TUI R5 PKCS#11”	29
2.3.3.1.4 Configuración del módulo “TUI R7 PKCS#11”	29
2.3.4 Gestor de certificado en tarjeta	30
2.3.4.1 Windows	30
2.3.4.1.1 Gestor de certificados para la Tarjeta Universitaria Inteligente (TUI) Optelio Card Santander (TUI R5), Classic Client Toolbox.	31
2.3.4.1.1.1 Contenido tarjeta	32
2.3.4.1.1.1.1 Certificados.....	32
2.3.4.1.1.1.1.1 Importar un certificado	32
2.3.4.1.1.1.1.2 Ver detalle de certificado	35
2.3.4.1.1.1.1.3 Eliminar certificados.....	36
2.3.4.1.1.1.2 Propiedades tarjeta.....	37
2.3.4.1.1.2 Administración tarjeta	39
2.3.4.1.1.2.1 Administración de NIP	39





2.3.4.1.1.2.1.1	Cambio de NIP.....	39
2.3.4.1.1.2.1.2	NIP de desbloqueo	39
2.3.4.1.2	Gestor de certificados para la Tarjeta Universitaria Inteligente (TUI) Optelio R7 (TUI R7), IDGo800UserTool.....	40
2.3.4.1.2.1	Certificados	40
2.3.4.1.2.1.1	Ver datos de un certificado	41
2.3.4.1.2.1.2	Eliminar certificado	42
2.3.4.1.2.1.3	Exportar certificado	43
2.3.4.1.2.1.4	Importar certificado	43
2.3.4.1.2.2	Gestión del PIN (PIN Management)	43
2.3.4.1.2.2.1	Cambiar PIN de usuario.....	44
2.3.4.1.2.2.2	Desbloquear PIN de usuario	44
2.3.4.1.2.3	Reciclar tarjeta (Recycle Card)	44
2.3.4.2	Linux y Mac	45
2.3.4.2.1	Importación de certificados	45
2.3.4.2.2	Borrado de certificados	52
3	Uso del certificado electrónico instalado en el equipo	57
3.1	Introducción	57
3.2	Instalación de componentes para la firma electrónica en aplicaciones de correo.....	58
4	Configuración y uso de la firma electrónica en aplicaciones de correo	59
4.1	Introducción	59
4.2	Microsoft Outlook.....	60
4.3	Mozilla Thunderbird	64
4.3.1	Importar los certificados de CA y modificar las configuraciones de confianza.	64
4.3.2	Seleccionar el certificado para firmar los correos del usuario.	67
4.4	Apple Mail	71



1 ¿Qué puedo encontrar en este manual?

En este manual se detallan los pasos necesarios para poder utilizar un certificado electrónico en los procedimientos de administración electrónica de la Universidad de Murcia.

Este manual diferencia dos posibles escenarios:

- [Uso del certificado electrónico desde la tarjeta universitaria.](#)
- [Uso del certificado electrónico instalado en el equipo.](#)

Cada uno de estos escenarios requiere pasos diferentes, por lo que el usuario deberá acudir al apartado del manual que se aplique a su caso.

Además existe un apartado para ayudar en la [configuración y uso de la firma electrónica en aplicaciones de correo.](#)

Cualquier duda o sugerencia sobre este manual, el software, o cualquier aspecto relacionado, le rogamos que consulte primero la Sede Electrónica de la Universidad de Murcia: <https://sede.um.es/sede/soporte/firmaCertificado.seam>.

IMPORTANTE: Guarde todos los documentos y cierre todas las aplicaciones que tenga abiertas antes de realizar cualquiera de los procedimientos descritos a continuación, para evitar pérdidas de información y posibles errores. Si la utiliza, desconecte también la tarjeta universitaria del lector.





2 Uso del certificado electrónico desde la tarjeta universitaria

2.1 Introducción

Para poder hacer uso de un certificado electrónico desde la tarjeta universitaria, han de cumplirse una serie de requisitos previos:

- Tener correctamente instalado y configurado en su equipo, un lector de tarjetas inteligentes compatible con el estándar PCSC.
- Poseer una tarjeta universitaria apta para albergar el certificado de usuario.
- Tener emitido un certificado electrónico por alguna de las entidades admitidas por la Universidad de Murcia.
- Tener un certificado electrónico instalado dentro de la tarjeta.

Para todos estos requisitos previos, por favor acuda a la Web de la Sede Electrónica de la Universidad de Murcia: <https://sede.um.es/sede/soporte/firmaCertificado.seam>.

Además de estos requisitos previos, se requiere:

- Instalar el software necesario para hacer uso de la tarjeta, que se describe a continuación en el apartado [Software para la TUI](#).

Para saber si su sistema operativo o aplicación puede ser utilizada con el software de la Universidad de Murcia, por favor consulte la Sede Electrónica de la Universidad de Murcia: <https://sede.um.es/sede/soporte/software.seam>.

Si va a utilizar el DNIe, deberá a su vez instalar el software desarrollado por la Dirección General de la Policía. Más información en <http://www.dnielectronico.es>.

Si va a hacer uso de la firma electrónica en páginas Web, también se requiere tener instalada la aplicación AutoFirm@. Más información en <https://sede.um.es/sede/soporte/software.seam>.

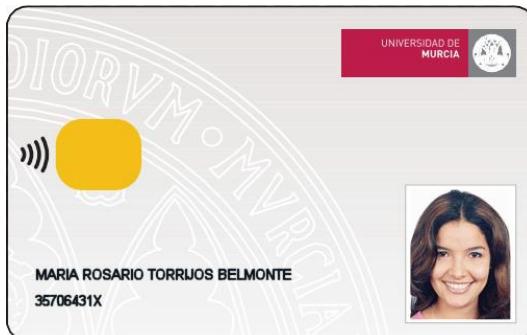




2.2 Tarjeta universitaria

Desde el curso 2012/2013, la Universidad de Murcia dispone de la Tarjeta Universitaria Inteligente (TUI), que incorpora capacidades criptográficas y puede ser utilizada en los servicios ofrecidos por la Universidad de Murcia.

Tarjeta Universitaria Inteligente (TUI)



2.3 Software de la TUI

Para posibilitar el acceso al certificado electrónico almacenado en la tarjeta universitaria, así como importar o exportar un certificado, es necesaria la instalación del software de la TUI.

Este software lo constituyen, principalmente, los siguientes módulos:

- **CSP: Módulo criptográfico para entornos Windows** que permite el uso del certificado desde la tarjeta, en programas como Internet Explorer, Google Chrome, Outlook Express, Microsoft Outlook y Windows Live Mail.
- **PKCS#11: Módulo criptográfico para entornos de software libre**, que permite el uso del certificado desde la tarjeta en programas como **Mozilla Firefox** y **Mozilla Thunderbird** en **Windows**, **Debian/Ubuntu** y **Mac OSX**.
- **Gestor de certificado en tarjeta**: Este programa permite la **importación** (mediante archivos PKCS#12) y **borrado del certificado** en la tarjeta.

En las páginas que siguen se detalla la [Instalación del Software de la TUI mediante el instalador](#), sin embargo puede que quiera realizar otras operaciones como:

- [Configuración de los módulos PKCS#11 para Firefox y Thunderbird](#).
- [Uso del gestor de certificado en tarjeta](#).





Dados los diferentes sistemas operativos soportados, por favor **acuda al apartado adecuado a su sistema operativo** para cada una de las operaciones descritas.



2.3.1 Instalación mediante el instalador

Dados los diferentes sistemas operativos soportados, por favor descargue el instalador del Software de la TUI acorde a su sistema operativo, desde la página Web de software en la Sede Electrónica de la Universidad de Murcia: <https://sede.um.es/sede/soporte/software.seam>, y guarde y cierre todas las aplicaciones que tenga abiertas antes de continuar.

Debe desinstalar las versiones previas del programa, así como el antiguo UMU-Crypto.

Una vez haya finalizado el proceso, puede que sea necesario reiniciar el equipo. Si su sistema no reconoce el dispositivo lector o no muestra el certificado electrónico presente en la tarjeta, por favor reinicie y pruebe de nuevo.

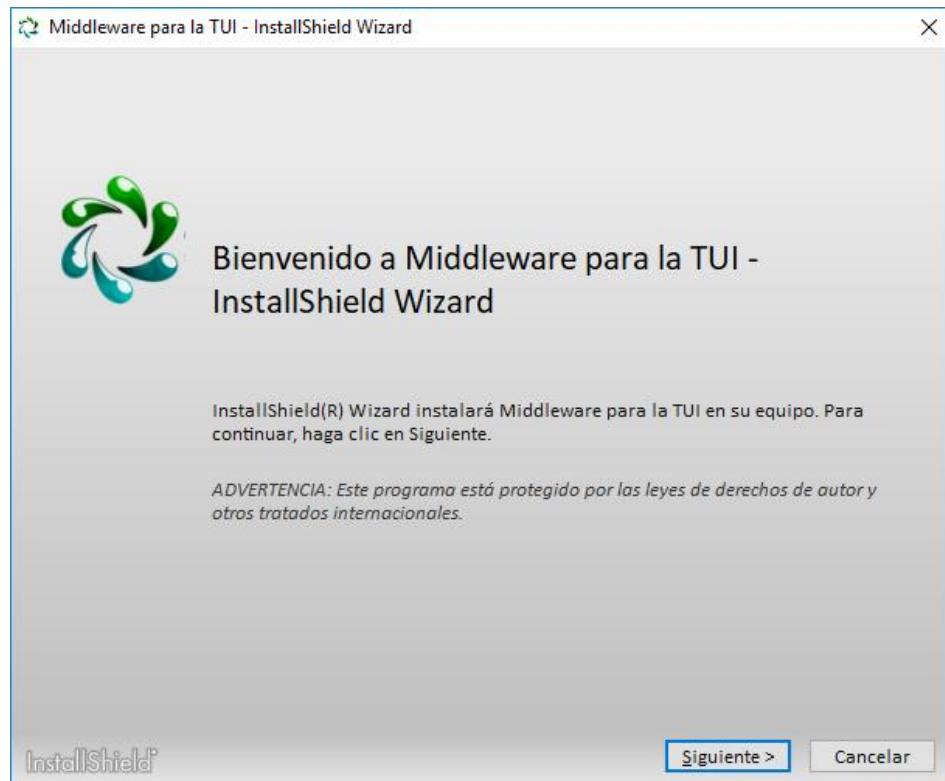




2.3.1.1 Windows

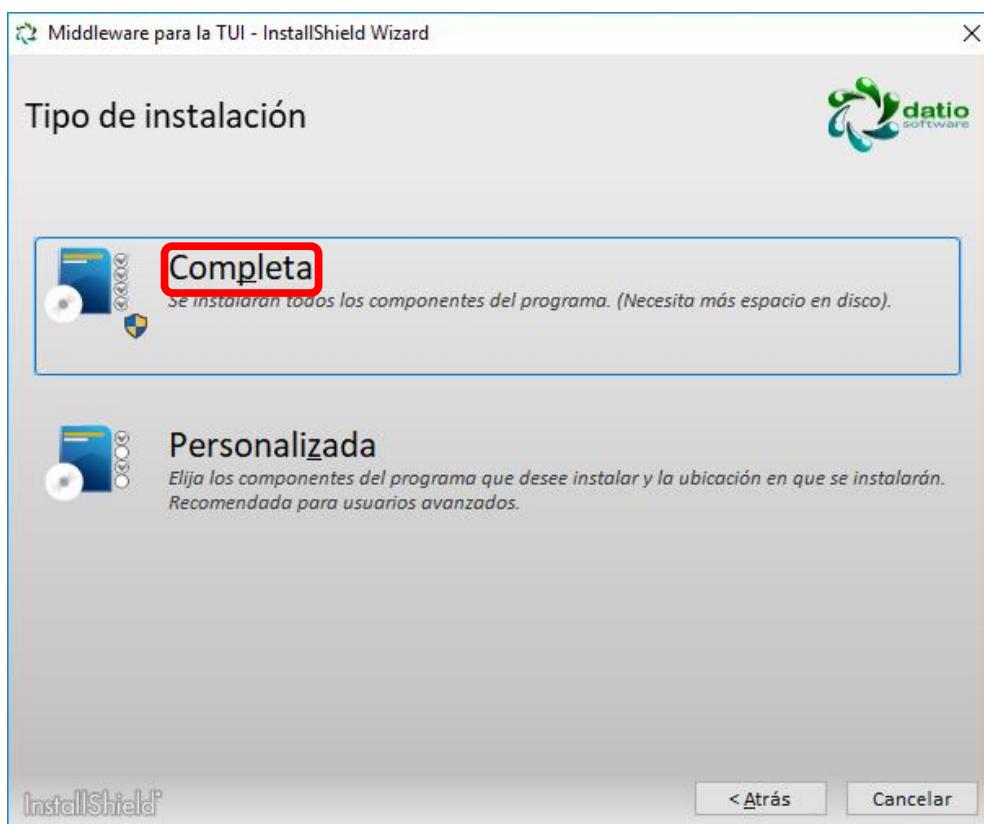
Antes de continuar, es necesario que desinstale manualmente UMU-Crypto, así como las versiones antiguas del Software de la TUI (en el caso de que tenga alguna instalada).

Para iniciar el proceso de instalación, haga doble clic sobre el archivo ejecutable instalador de la aplicación. Podrá ver la siguiente pantalla:





En cualquier momento se puede pulsar el botón **Cancelar** para salir de la instalación.
Al pulsar **Siguiente** debería aparecer la siguiente pantalla:

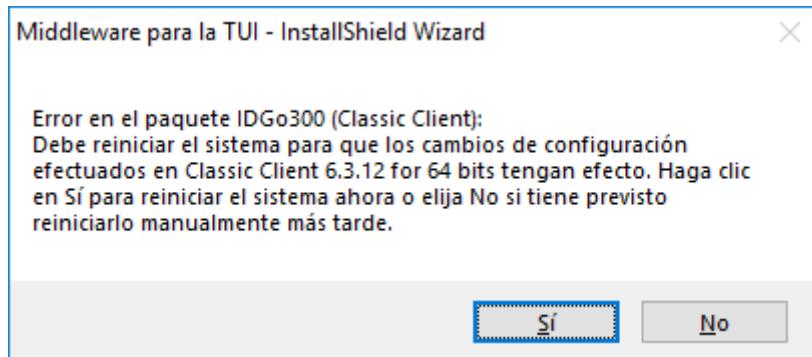


Si quiere seguir con la instalación, pulse sobre la opción “Completa”. De lo contrario, pulse **Cancelar** y saldrá del instalador.

En el caso de que pulse **Instalar**, espere a que se instale todo el software necesario. El proceso de instalación puede tardar unos minutos.

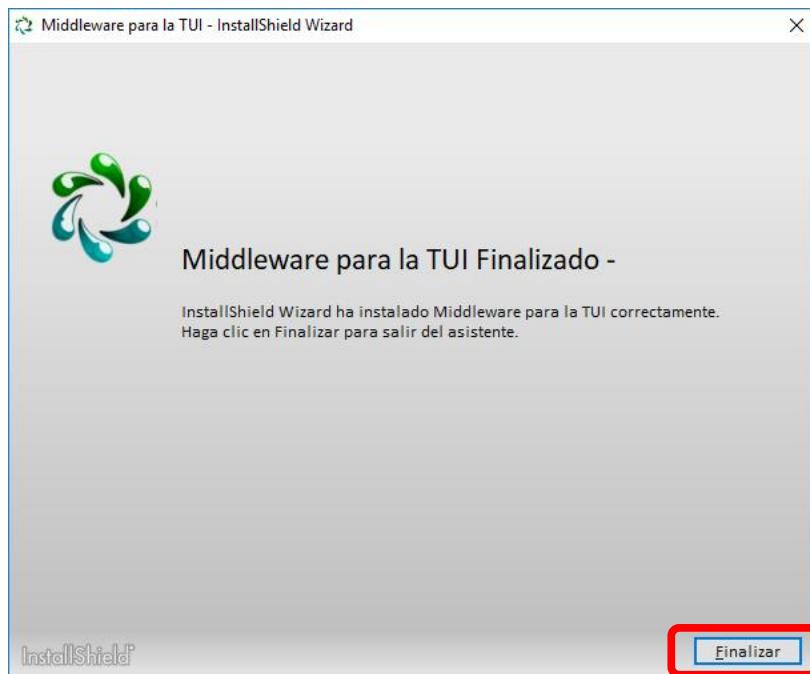


Durante la instalación del software aparecerá el siguiente mensaje indicándonos que hay que reiniciar. Debemos cerrar todas las aplicaciones guardando los trabajos y pulsar en **Sí**:



Tras el reinicio requerido el instalador se ejecutará automáticamente y continuará con la instalación hasta finalizar.

Una vez que haya terminado el proceso de instalación, pulse el botón **Finalizar**. Es probable que requiera el reinicio del equipo, para que todo funcione correctamente.

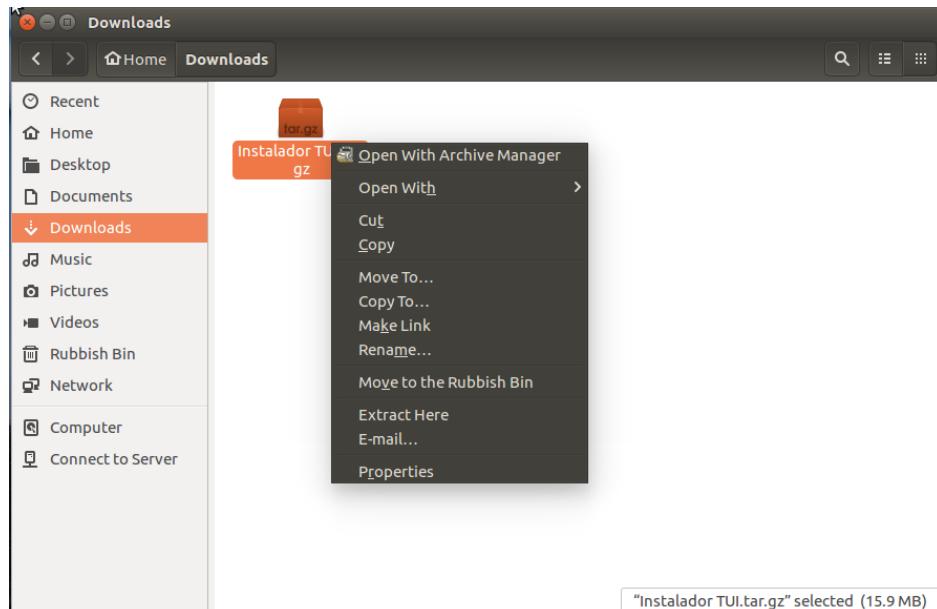




2.3.1.2 Linux

Descargar el software apropiado para nuestro sistema operativo de [esta página](#). Una vez descargado, tenemos que:

1. Descomprimir el fichero.



2. Ejecutar el script como *sudo* (o como *superusuario*) de instalación e instalar.

```
osboxes@osboxes: ~/Downloads/Instalador TUI
osboxes@osboxes:~$ cd Downloads/Instalador\ TUI/
osboxes@osboxes:~/Downloads/Instalador TUI$ sudo ./instaladorTUI.sh
```



2.3.1.3 Mac OSX

Descargar el software apropiado para nuestro sistema operativo de [esta página](#). Una vez descargado, descomprima el fichero.

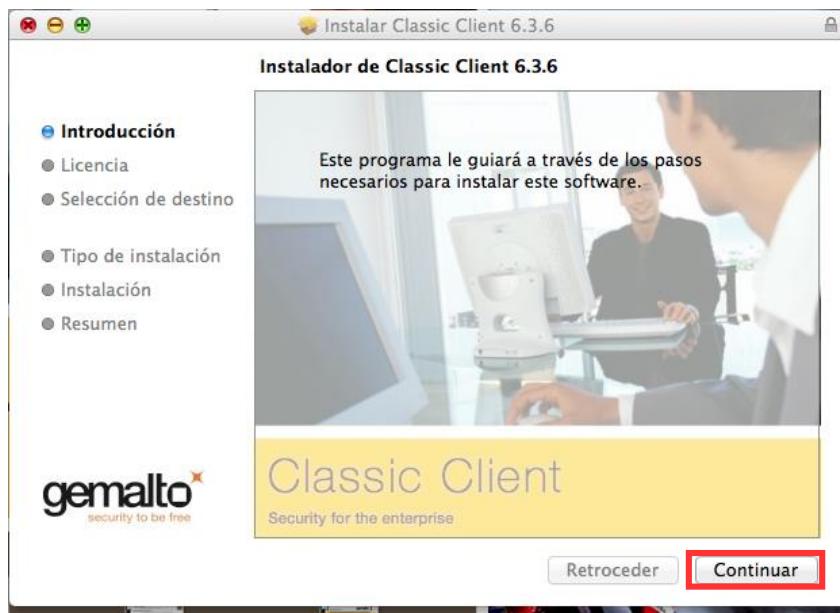
A continuación, debe montar las imágenes (ficheros .dmg) e instalarlas como se muestra a continuación.

1. Monte la imagen .dmg y ejecute el paquete del instalador.





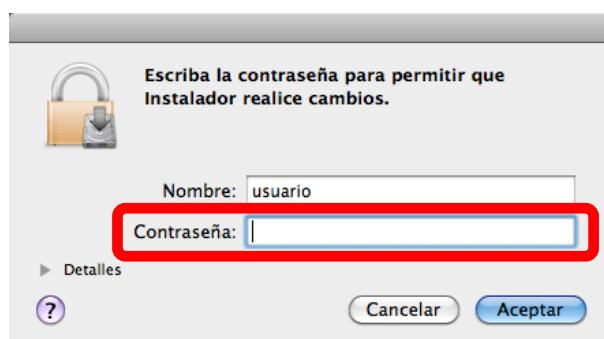
2. En la primera ventana pulse **Continuar**.



Pulse **Continuar** para iniciar el asistente de instalación o, en cualquier momento, cierre el instalador haciendo clic en la esquina superior izquierda para cancelar la instalación.

Lea el contrato de licencia, y si está conforme pulse **Continuar**. En caso contrario, cierre el instalador. Si continúa, se le mostrará un mensaje emergente para confirmar que acepta los términos del contrato. Pulse **Acepto**. A continuación, pulse **Instalar** para iniciar el proceso de instalación.

Puede que en este momento se le solicite una clave de administrador con privilegios para poder instalar software en el equipo. Introduzca la contraseña y pulse **Aceptar**.



Cuando la instalación haya finalizado, se le mostrará una ventana informando que la instalación se ha completado correctamente. Pulse **Cerrar** para terminar la instalación y salir del asistente.





3. Repita los mismos pasos para el resto de imágenes contenidas en el fichero descargado.

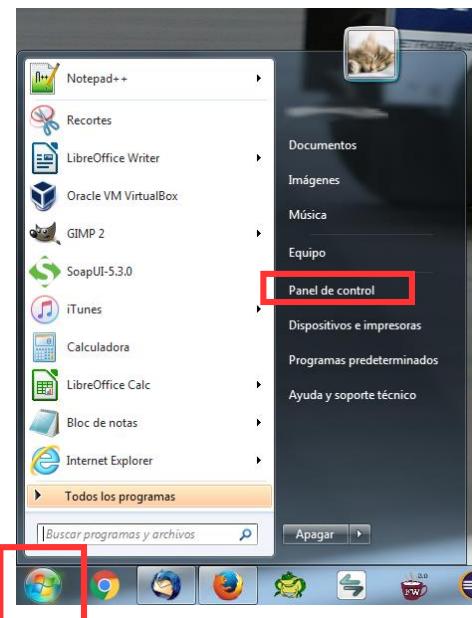


2.3.2 Desinstalación del Software TUI

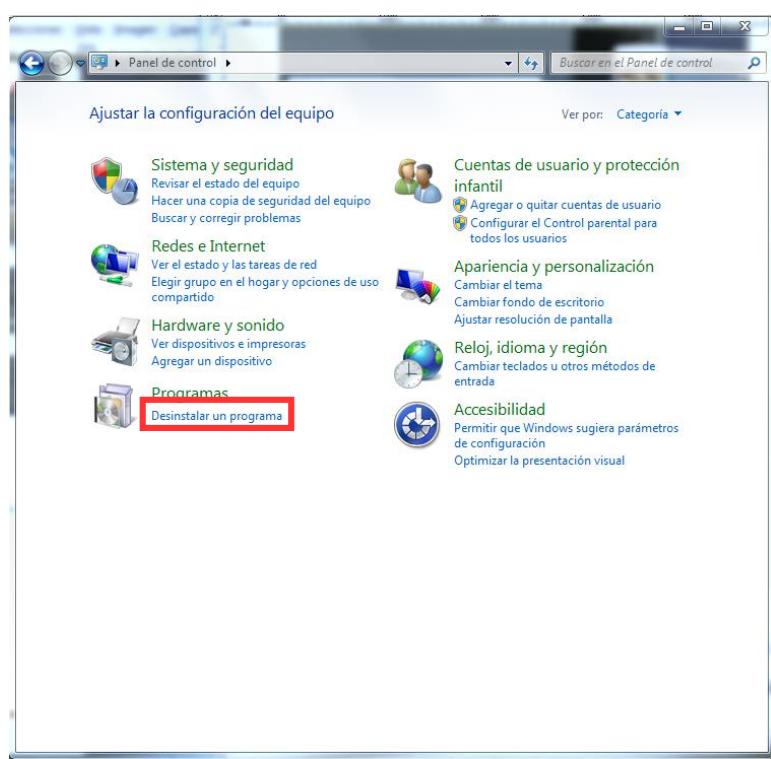
2.3.2.1 Windows

Para desinstalar el Software para la TUI en un sistema Windows, debe llevar a cabo la secuencia de pasos que se indica a continuación. Dependiendo de la versión del sistema operativo que tenga instalada, la apariencia de las ventanas puede variar.

1. Ir a Menú de Inicio → Panel de control.

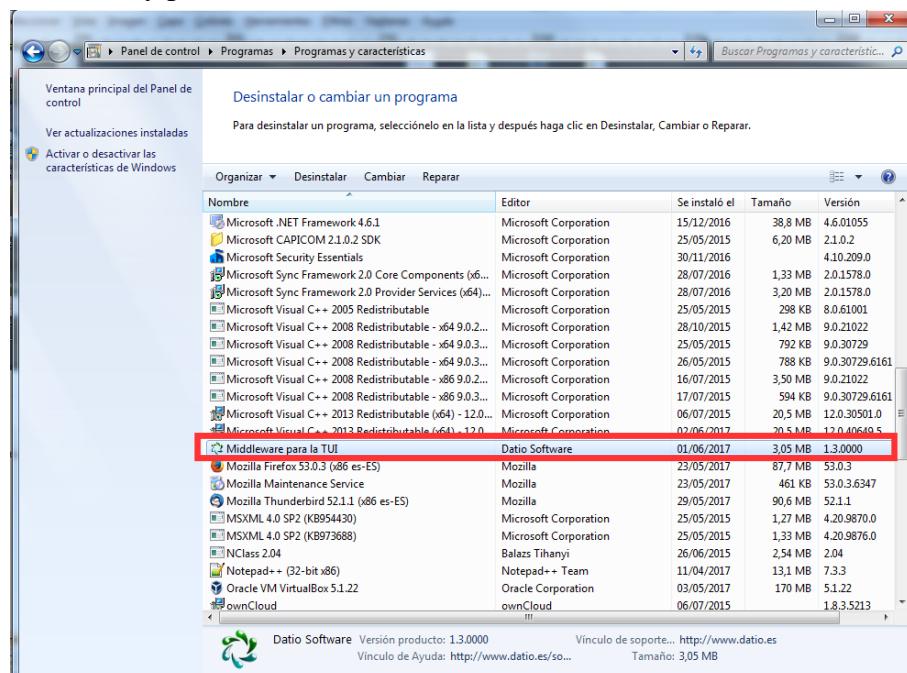


2. En Programas, seleccionar Desinstalar un programa.





3. En la lista de programas instalados, buscar **Middleware para la TUI**, seleccionar y pulsar el botón **Desinstalar**.





2.3.3 Configuración de los módulos PKCS#11 para Firefox y Thunderbird (y Chrome/Chromium en Linux)

Para poder hacer **uso de un certificado electrónico desde la tarjeta universitaria** en Firefox y Thunderbird (además de Chrome/Chromium en Linux) es necesario configurar, en las aplicaciones mencionadas, los módulos PKCS#11.

Cuando se realiza la instalación del **software de la TUI** en Windows, esta configuración de los módulos PKCS#11 se realiza de forma automática para el usuario que haya ejecutado el instalador.

Si se desea configurar el módulo en Firefox, Thunderbird (y Chrome/Chromium en Linux) para otros usuarios del equipo, puede [configurar el módulo de forma manual](#).

Una vez esté configurado, debería consultar el apartado de [configuración y uso de la firma electrónica en aplicaciones de correo](#).



2.3.3.1 Configuración de los módulos PKCS#11 de forma manual

Si ha habido problemas en la configuración durante el proceso de instalación, existen problemas al utilizarlo o no existen en su plataforma, puede configurar los módulos PKCS#11 de forma manual, siguiendo los pasos que se describen a continuación.

2.3.3.1.1 Mozilla Firefox.

Ejecute el navegador Mozilla Firefox y abra la ventana de opciones o preferencias del mismo:

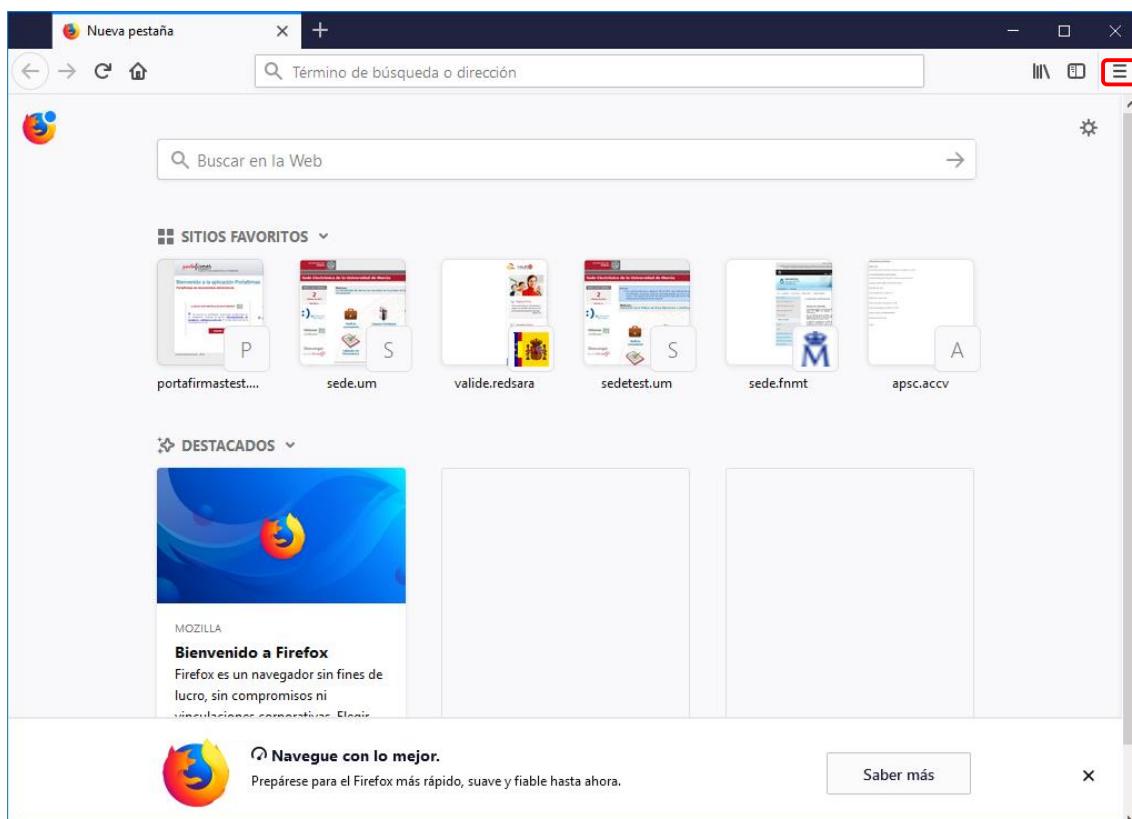


Ilustración 1: Botón de menú de Firefox 58 en Windows.

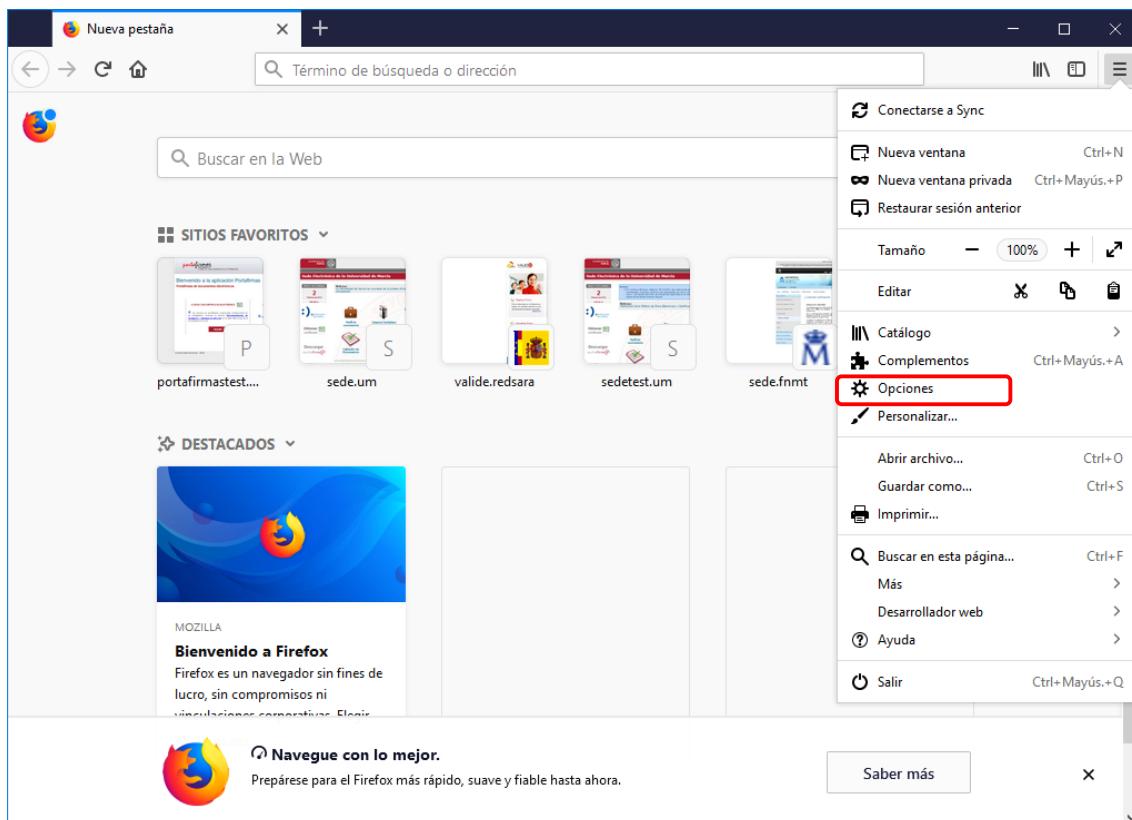


Ilustración 2: Menú opciones en Firefox 58.



En la ventana que se abre, pulse en la categoría **Privacidad y seguridad**:

The screenshot shows the Firefox 'Opciones' (Options) window with the URL 'about:preferences#privacy'. On the left, there is a sidebar with several categories: General, Buscar, **Privacidad y seguridad** (which is highlighted with a red arrow), and Cuenta de Firefox. The main content area is titled 'Privacidad del navegador' and contains sections for 'Formularios y contraseñas' (with checkboxes for 'Recordar nombres de usuario y contraseñas de los sitios web' and 'Uso de una contraseña maestra'), 'Historial' (with a dropdown menu set to 'Recordar el historial'), and 'Barra de direcciones' (with checkboxes for 'Historial de navegación', 'Marcadores', and 'Abrir pestanas').

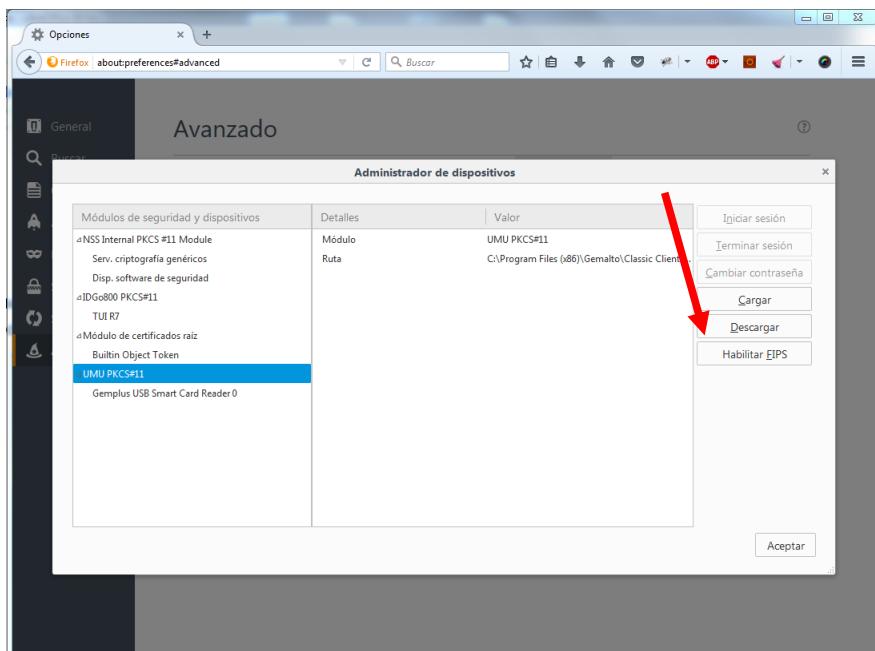
Desplace la pantalla hasta abajo y pulse sobre **Dispositivos de seguridad**:

The screenshot shows the same Firefox 'Opciones' window. The sidebar now includes 'Seguridad' instead of 'Privacidad y seguridad'. The main content area has a section titled 'Protección contra contenido engañoso y software peligroso' with checkboxes for 'Bloquear contenido peligroso y engañoso', 'Bloquear descargas peligrosas', and 'Advertir sobre software no deseado y poco usual'. Below this is a 'Certificados' section. Under 'Certificados', there are options for selecting a certificate: 'Seleccionar uno automáticamente' (radio button unselected) and 'Preguntar cada vez' (radio button selected). A checkbox 'Consultar a los servidores respondedores OCSP para confirmar la validez actual de los certificados' is checked. At the bottom right of this section is a button labeled 'Ver certificados...' and next to it, another button labeled 'Dispositivos de seguridad...' which is highlighted with a red box and a red arrow.





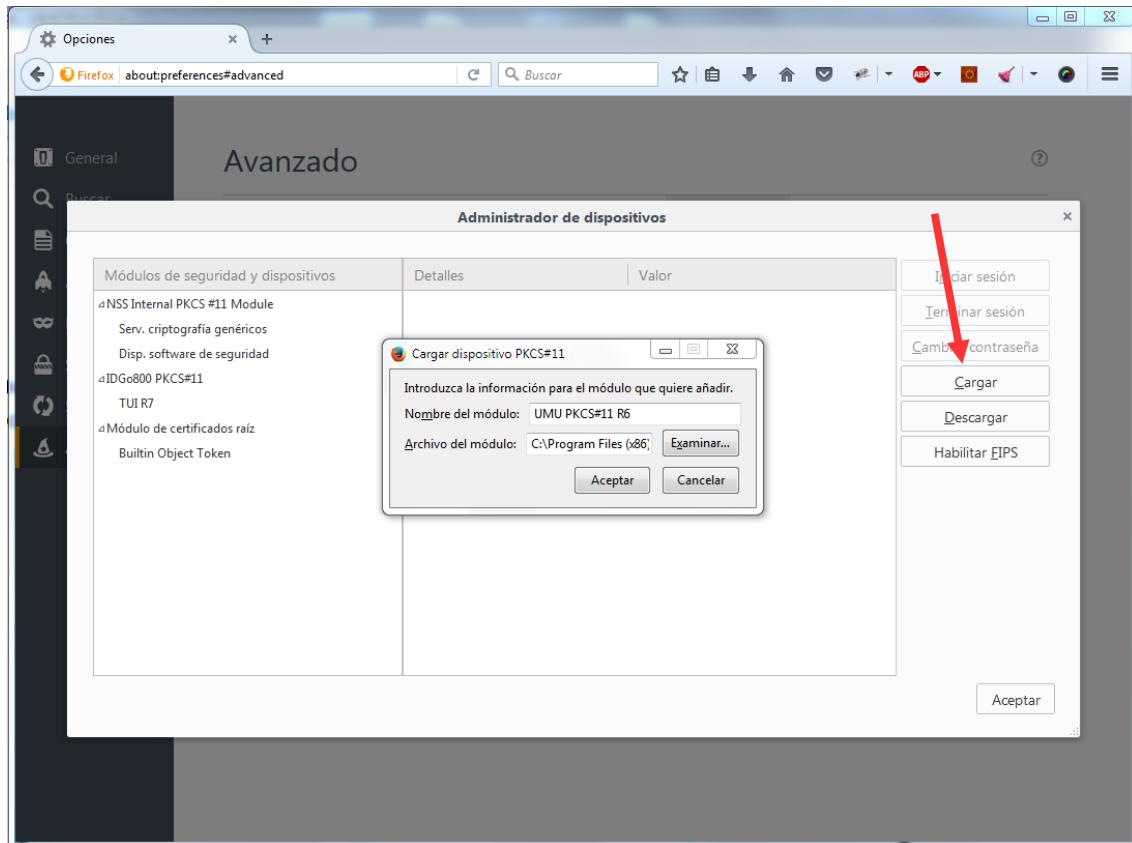
En la ventana que se abre, se mostrarán los dispositivos de seguridad que tiene instalados en su navegador. Si aparecen dispositivos con el nombre "UMU", selecciónelos y pulse el botón **Descargar**:



IMPORTANTE: En caso de haber eliminado algún módulo criptográfico, **será necesario que reinicie el navegador** antes de continuar el proceso.



Para agregar el nuevo módulo, pulse el botón **Cargar**:



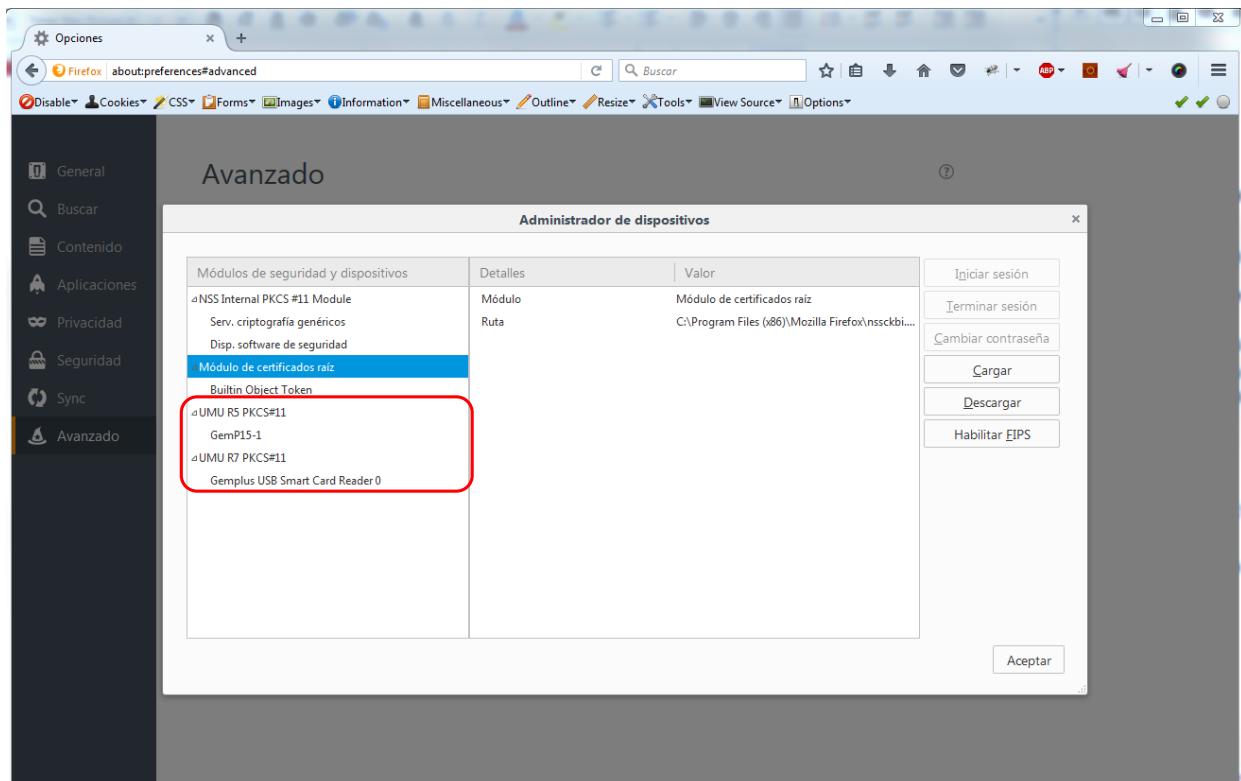
Llegados a este punto, debe cargar dos módulos: el módulo “**TUI R5 PKCS#11**” y el módulo “**TUI R7 PKCS#11**”. A continuación, se indica cómo cargar cada uno de estos módulos, en función del sistema operativo:

- [Configuración del módulo “TUI R5 PKCS#11”](#)
- [Configuración del módulo “TUI R7 PKCS#11”](#)





- Una vez se ha pulsado **Aceptar**, y si no se han producido errores, deberían verse los nuevos módulos de seguridad. En caso de tener una tarjeta introducida en el lector, podrá ver, además, información relativa a la misma.



Pulse el botón **Aceptar** y cierre la ventana del **Administrador de dispositivos** de seguridad.

En este punto, **los módulos criptográficos se encuentran configurados y listos para su uso**.

En caso de tener una tarjeta universitaria de la Universidad de Murcia **y un certificado emitido por la FNMT**, puede proceder a realizar una prueba, validando el estado de su certificado.

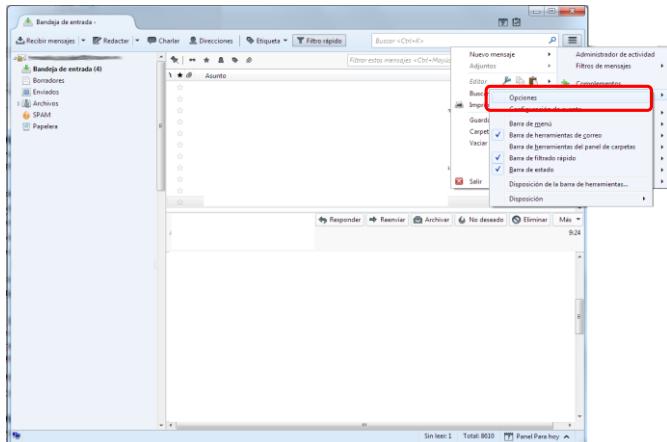
Introduzca la tarjeta universitaria y acceda a la siguiente URL para verificar el estado de su certificado: <https://www.sede.fnmt.gob.es/certificados/persona-fisica/verificar-estado/solicitar-verificacion>

Si dispone de AutoFirm@ instalada en su ordenador, también puede hacer una prueba de firma en la Sede Electrónica de la Universidad de Murcia: <https://sede.um.es/sede/soporte/test.seam>.

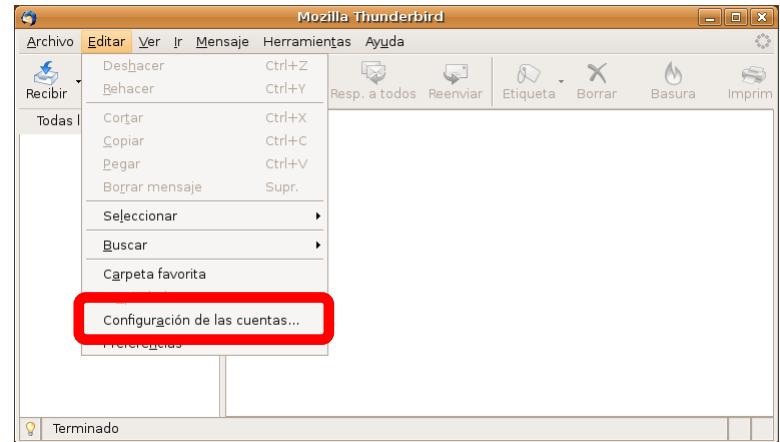


2.3.3.1.2 Mozilla Thunderbird.

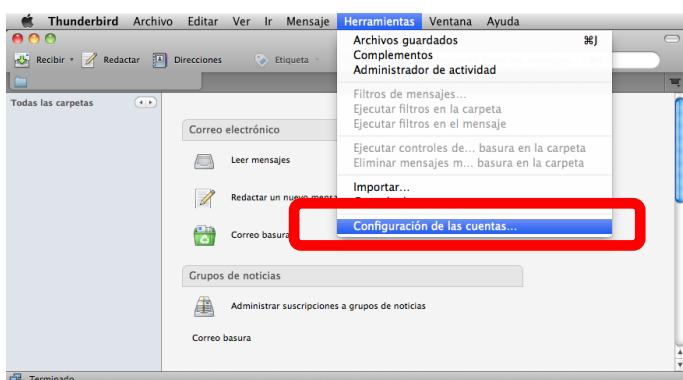
Ejecute Thunderbird y abra el menú de configuración de las cuentas:



Menú de configuración de cuentas en Windows.

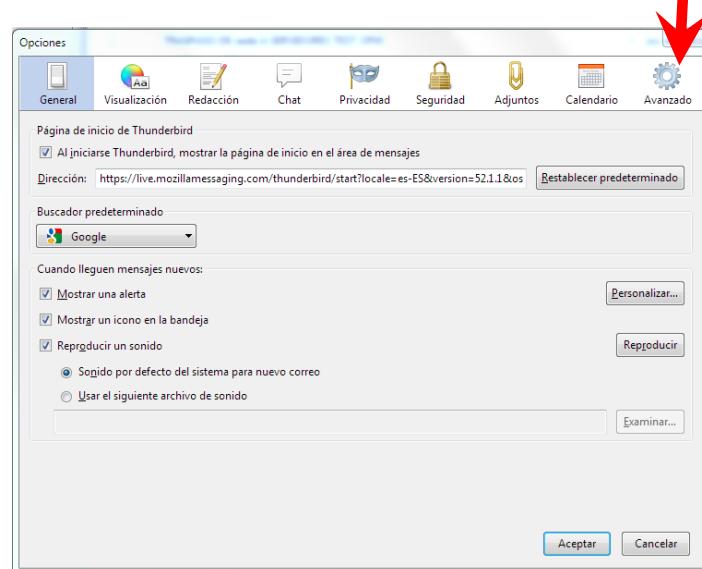


Menú de configuración de cuentas en Linux



Menú de configuración de cuentas en Mac OSX

Una vez que se abra la venta de *Opciones*, tenemos que pulsar sobre la última opción, *Avanzado*.

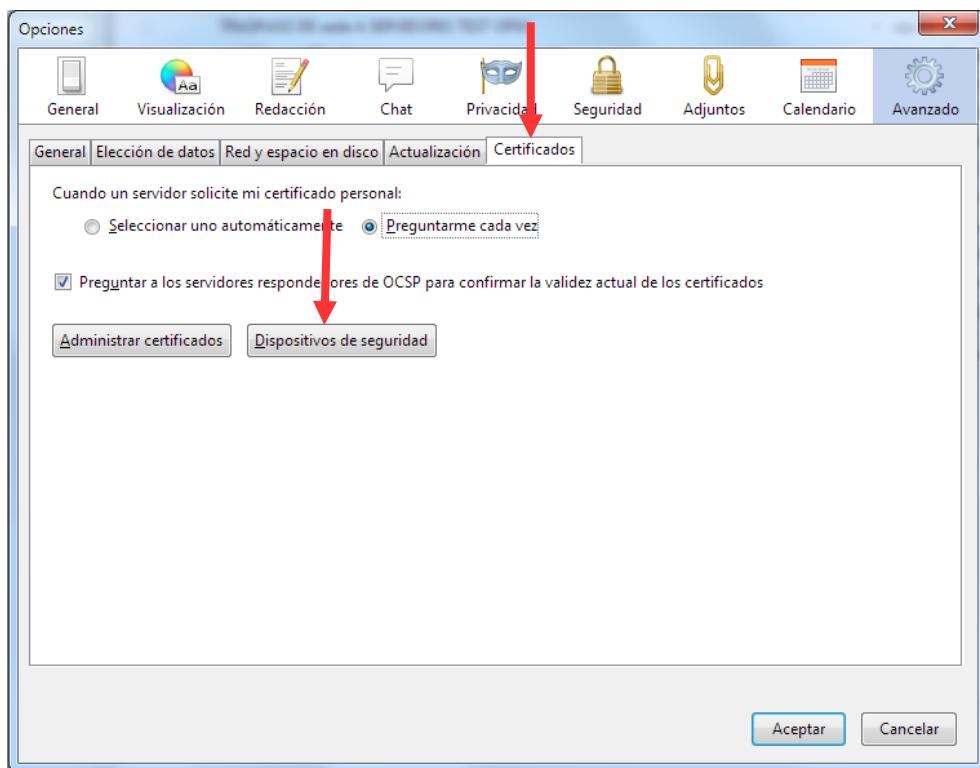


Área de Tecnologías de la Información y las Comunicaciones Aplicadas
Servicio de Desarrollo, Aplicaciones y Metodología

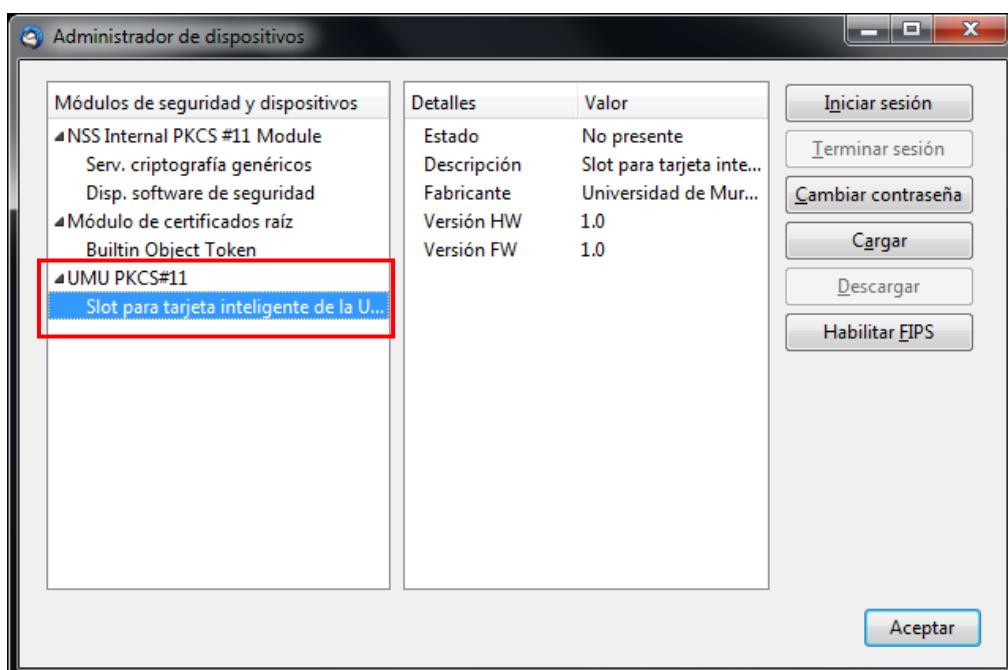
Campus Universitario de Espinardo. 30100 Murcia
T. 86 8884222 – F. 86 8888337 – www.um.es/atica



En las opciones *Avanzado*, tenemos que pulsar en la última pestaña, *Certificados*. Una vez que estemos en la pestaña *Certificados*, pulsar el botón *Dispositivos de seguridad*:



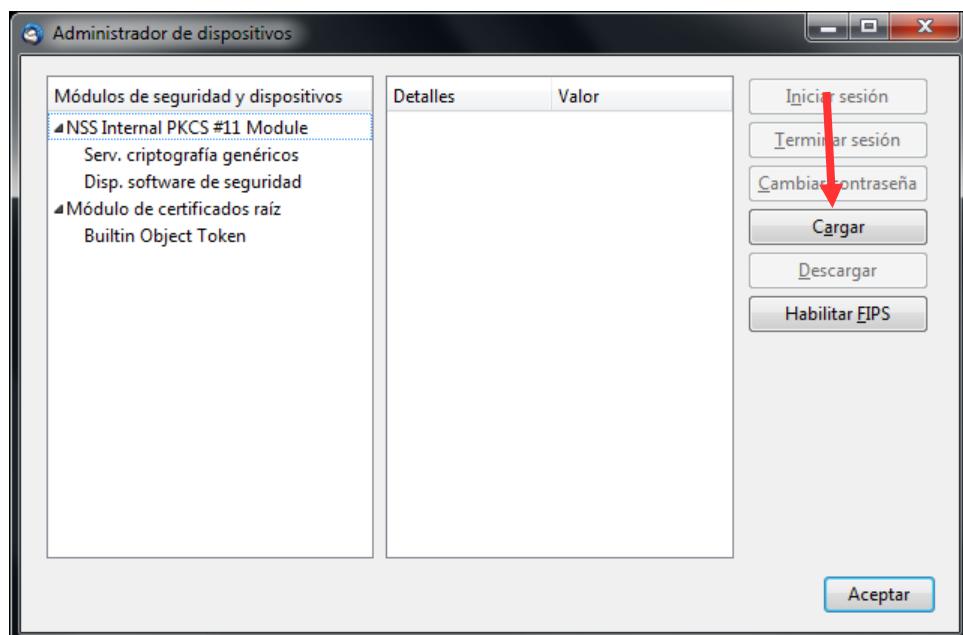
En la ventana que se abre, se mostrarán los dispositivos de seguridad que tiene instalados en su navegador. Seleccione aquellos en los que aparezca el nombre “**UMU**” y pulse el botón *Descargar*:





IMPORTANTE: En caso de haber eliminado algún módulo criptográfico, **será necesario que reinicie el programa** antes de continuar el proceso.

Para agregar el nuevo módulo, pulse el botón **Cargar**:

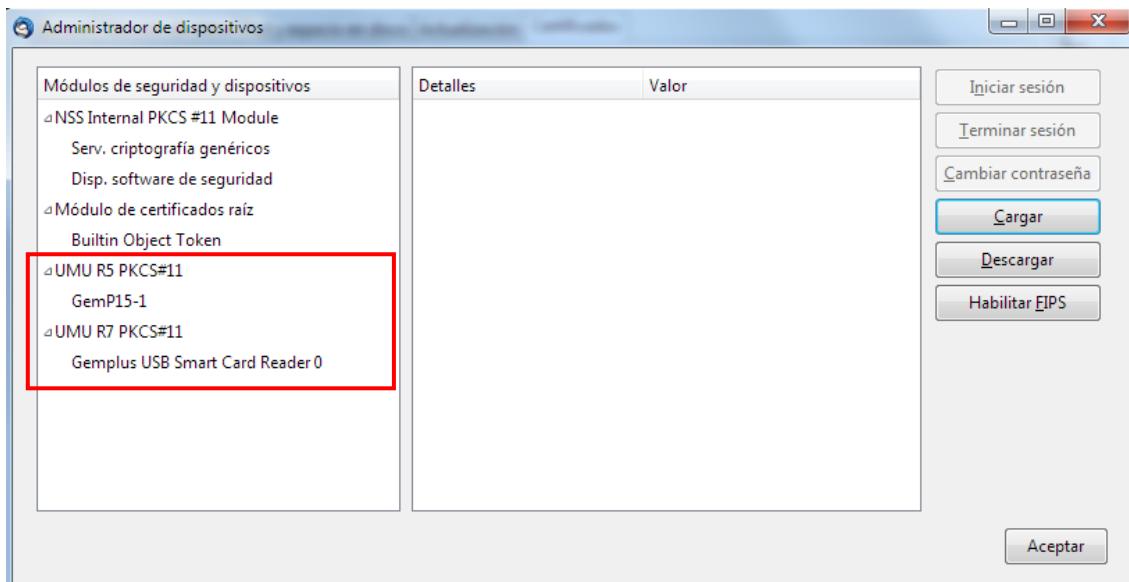


Llegados a este punto, debe cargar dos módulos: el módulo “**TUI R5 PKCS#11**” y el módulo “**TUI R7 PKCS#11**”. A continuación, se indica cómo cargar cada uno de estos módulos, en función del sistema operativo:

- [Configuración del módulo “TUI R5 PKCS#11”](#)
- [Configuración del módulo “TUI R7 PKCS#11”](#)



- Una vez se ha pulsado **Aceptar**, y si no se han producido errores, deberían verse los nuevos módulos de seguridad. En caso de tener una tarjeta introducida en el lector, se podrá ver además información relativa a la misma.



Pulse el botón **Aceptar** y cierre la ventana del Administrador de dispositivos de seguridad.

En este punto, **ya tiene instalado los componentes para hacer uso del certificado almacenado en la tarjeta**.

Debería leer el apartado de [configuración y uso de la firma electrónica en aplicaciones de correo](#), para poder hacer uso del certificado en la firma de sus correos electrónicos.





2.3.3.1.3 Configuración del módulo “TUI R5 PKCS#11”

Utilice como Nombre: “**UMU R5 PKCS#11**” y como archivo de módulo, el especificado según la plataforma, tal y como se indica en la siguiente tabla.

Sistema Operativo	Versión	Ruta del archivo del módulo PKCS#11 para TUI R5		
Windows	32 bits	C:\Program Files\Gemalto\Classic Client\BIN\gclib.dll		
	64 bits	Navegador 32 bits	C:\Program Files (x86)\Gemalto\Classic Client\BIN\gclib.dll	
		Navegador 64 bits	C:\Program Files\Gemalto\Classic Client\BIN\gclib.dll	
Linux		/usr/lib/ClassicClient/libgclib.so		
Mac OS X	Todos	/Library/Frameworks/GemaltoClassicClient.framework/GemaltoClassicClient		
	El Capitán y Sierra	/usr/local/lib/ClassicClient/libgclib.dylib		
	Versiones antiguas	/usr/lib/ClassicClient/libgclib.dylib		

2.3.3.1.4 Configuración del módulo “TUI R7 PKCS#11”

Utilice como Nombre: “**UMU R7 PKCS#11**” y como archivo de módulo, el especificado según la plataforma, tal y como se indica en la siguiente tabla.

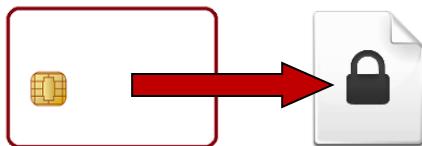
Sistema Operativo	Versión	Ruta del archivo del módulo PKCS#11 para TUI R7		
Windows	32 bits	C:\Program Files\Gemalto\IDGo 800 PKCS#11\IDPrimePKCS11.dll		
	64 bits	Navegador 32 bits	C:\Program Files (x86)\Gemalto\ IDGo 800 PKCS#11\IDPrimePKCS11.dll	
		Navegador 64 bits	C:\Program Files (x86)\Gemalto\ IDGo 800 PKCS#11\IDPrimePKCS1164.dll	
Linux		/usr/lib/pkcs11/libidprimepkcs11.so		
Mac OS X		/usr/lib/pkcs11/libidprimepkcs11.dylib		



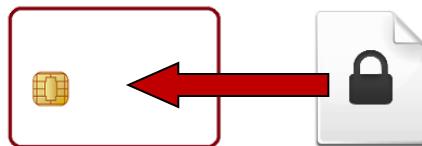


2.3.4 Gestor de certificado en tarjeta

El gestor de certificado en tarjeta permite importar y exportar el certificado desde y hacia la tarjeta universitaria y un fichero PKCS#12.



Exportar desde la tarjeta a un fichero



Importar desde un fichero a la tarjeta

Además, permite eliminar los certificados incluidos en la tarjeta universitaria.

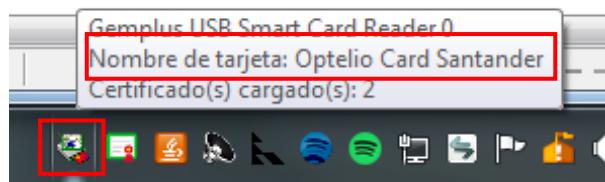
IMPORTANTE: La Tarjeta Universitaria Inteligente (TUI) NO PERMITE EXPORTAR los certificados completos a un fichero por motivos de seguridad. Solamente permite exportar la parte pública del certificado.

2.3.4.1 Windows

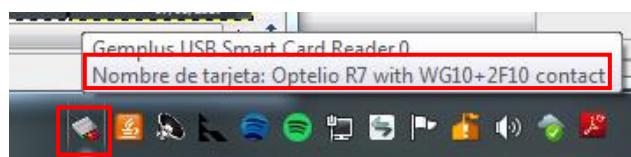
La Universidad de Murcia, en la actualidad, cuenta con dos modelos diferentes de Tarjeta Universitaria. En función del modelo que tengamos, tendremos que hacer uso de un software para la gestión de los certificados en nuestra tarjeta u otro.

Para saber el tipo de tarjeta que tenemos, tenemos que ir al *área de notificaciones* de Windows, y poner el ratón sobre el icono que se muestra a continuación:

- Optelio Card Santander (TUI R5):



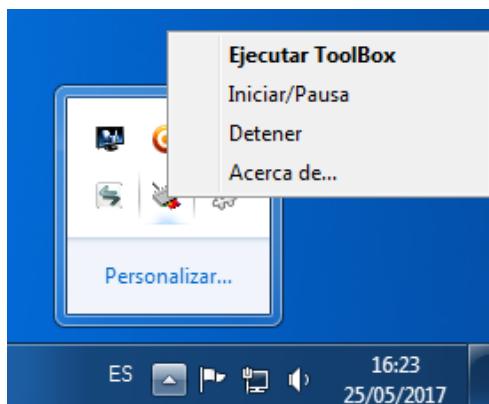
- Optelio R7 (TUI R7):



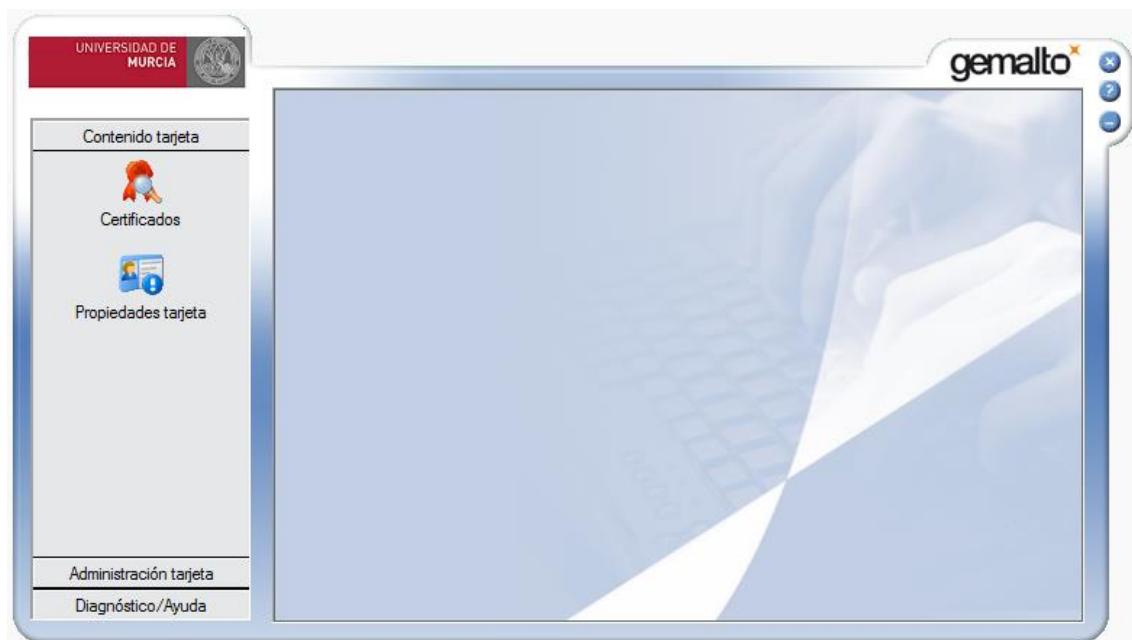


2.3.4.1.1 Gestor de certificados para la Tarjeta Universitaria Inteligente (TUI) Optelio Card Santander (TUI R5), Classic Client Toolbox.

Para abrir la aplicación navegue a **Inicio > Todos los programas > Gemalto > Classic Client > Classic Client Toolbox**. También es posible el acceso haciendo clic con el botón derecho del ratón sobre el ícono  de la bandeja de entrada, y haciendo clic en **Ejecutar toolbox**.



Se nos abrirá el gestor de certificados, cuya apariencia es la que se muestra a continuación:





Las herramientas disponibles se encuentran agrupadas en el panel lateral izquierdo, según su uso.

Contenido tarjeta



Certificados. Permite ver los certificados contenidos en la tarjeta inteligente.



Propiedades tarjeta. Permite ver la información asociada a la tarjeta inteligente.

Administración tarjeta



Administración de NIP. Permite realizar cambios en el NIP asociado a la tarjeta inteligente.

Diagnóstico/Ayuda



Herramienta diagnóstico. Se utiliza para examinar todos los componentes instalados y determinar si existe algún problema.



Documentación. Contiene la documentación disponible para el usuario.

A continuación, se comentan las herramientas más relevantes.

2.3.4.1.1.1 Contenido tarjeta

Este menú contiene las herramientas asociadas con la visualización e interacción con el contenido de la tarjeta inteligente. Estas herramientas son **Certificados** y **Propiedades tarjeta**.

2.3.4.1.1.1.1 Certificados

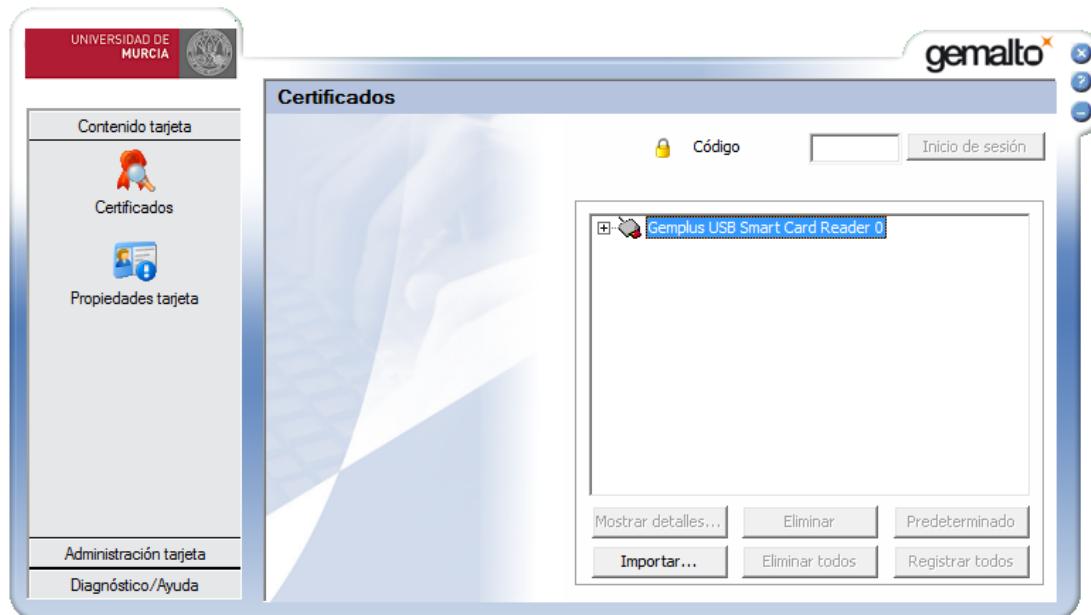
La herramienta **Certificados** permite gestionar los certificados contenidos en la tarjeta inteligente. A continuación, se incluyen las opciones disponibles junto con las acciones a realizar para cada una de ellas.

2.3.4.1.1.1.1.1 Importar un certificado

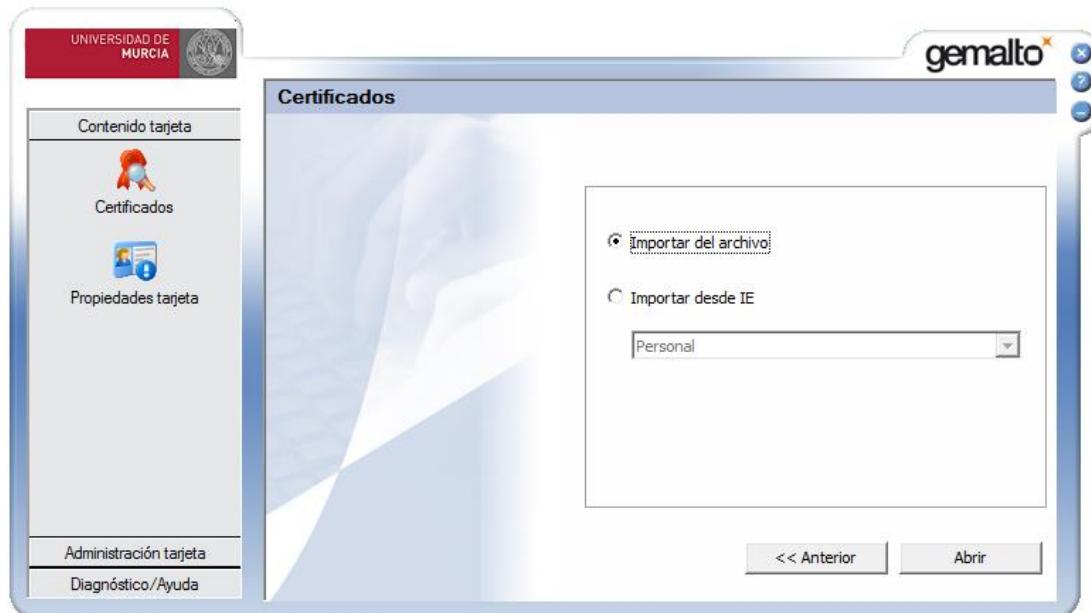
Es posible importar un certificado en la tarjeta inteligente, tal y como se indica a continuación.

1. Haga clic en **Contenido tarjeta > Certificados**. Asegúrese previamente que la tarjeta en la que importar el certificado está correctamente conectada.





2. Habilite el acceso a la tarjeta, introduciendo el Código (PIN la tarjeta) y haciendo clic en **Inicio de sesión**.
3. Seleccione el lector de tarjetas inteligentes para activar el botón **Importar**.
4. Haga clic en **Importar** (también puede hacer un clic derecho en el lector y seleccionar **Importar** desde el menú contextual).

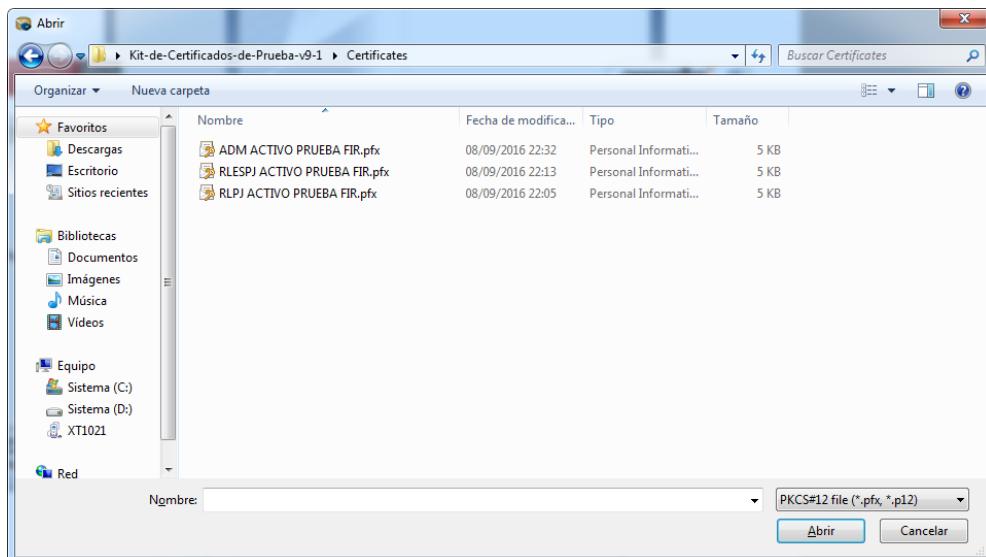


5. De las dos opciones que ofrece, elija **Importar del archivo**. Para importar el certificado desde un archivo, ir a [Importar certificado desde un archivo](#).
6. Una vez importado el certificado, es necesario extraer la tarjeta del lector, y volver a introducirla para que el certificado importado esté disponible en los almacenes de claves.

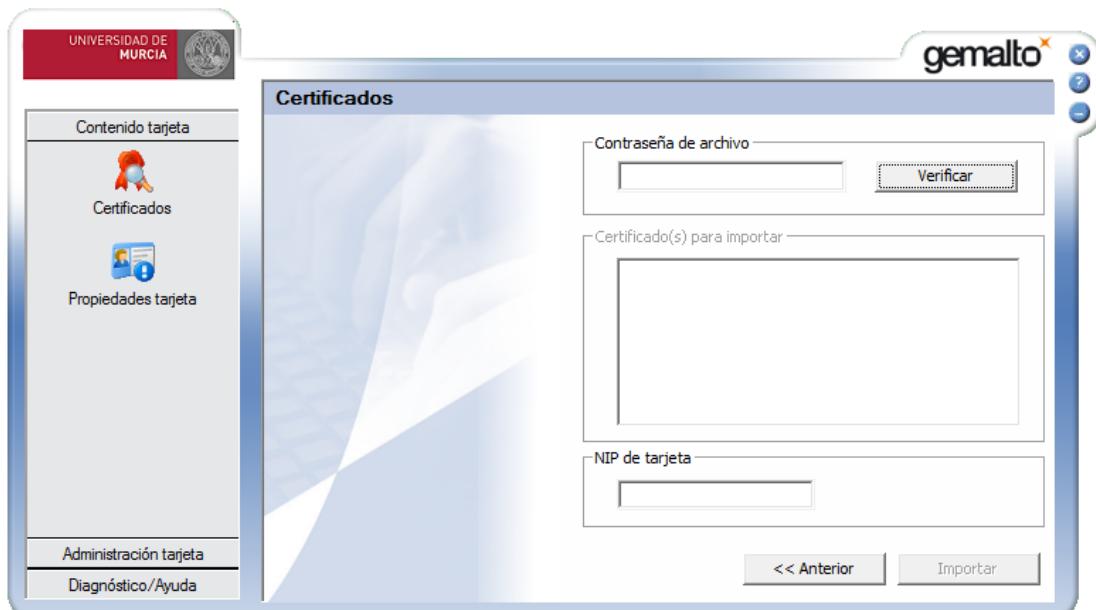


Importar certificado desde un archivo

1. Seleccione la opción **Importar del Archivo** y haga clic en **Abrir**. Se muestra la venta de Windows *Abrir*.

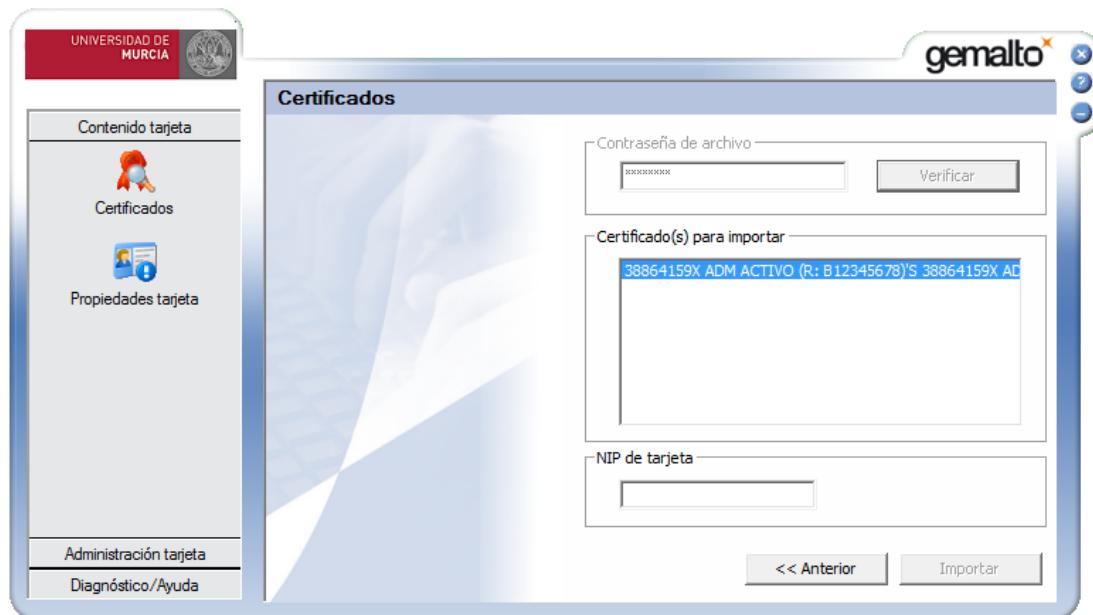


2. En la ventana anterior seleccione el archivo PKCS#12 (*.pfx, *.pf12) que contiene el certificado a importar.
3. Este archivo requiere el conocimiento de una contraseña para poder trabajar con los certificados o claves que contiene. Para ello, seleccione el archivo a importar y haga clic en **Abrir**. Se mostrará la siguiente ventana.





4. Introduzca la contraseña del archivo y haga clic en **Verificar**. Si la contraseña es correcta, se mostrarán todos los certificados que contiene el archivo, en **Certificado(s) a importar**.



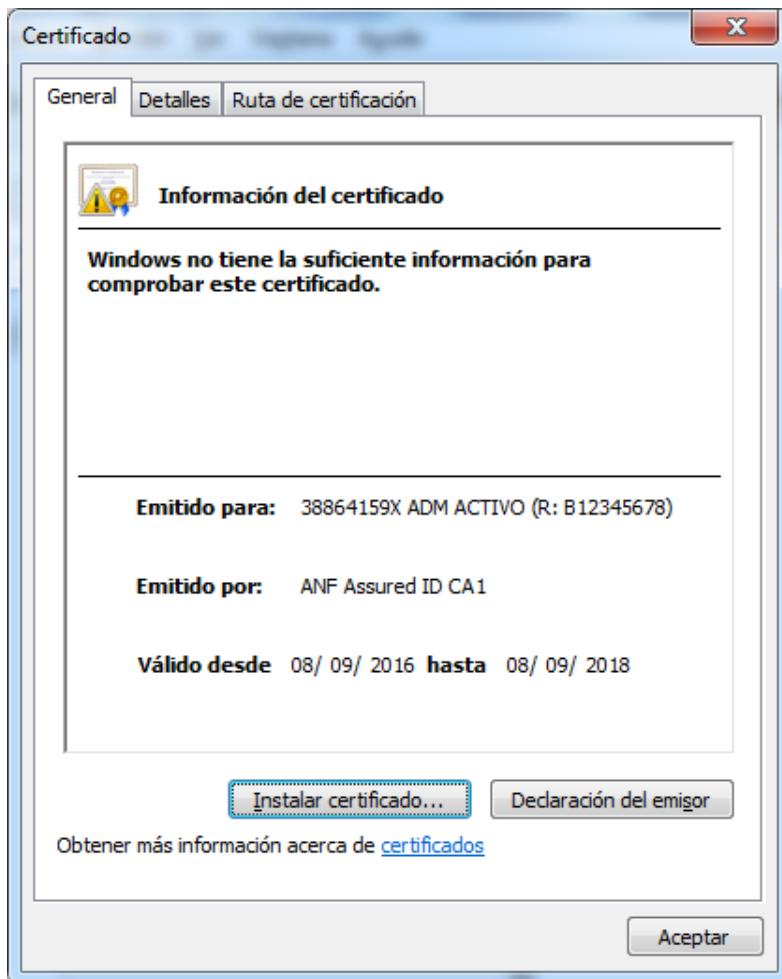
5. En **Certificado(s) a importar**, seleccione el certificado que quiera importar.
6. Una vez que introduzca el PIN de la tarjeta, haga clic en **Importar**. Si el NIP es correcto, se muestra una ventana que indica que el certificado ha sido correctamente importado.

2.3.4.1.1.1.2 Ver detalle de certificado

Es posible ver la información de todos certificados contenidos en la tarjeta inteligente.

1. Haga clic en **Contenido tarjeta > Certificados**. Asegúrese previamente que la tarjeta en la que importar el certificado está correctamente conectada.
2. Habilite el acceso a la tarjeta, introduciendo el Código (NIP la tarjeta) y haciendo clic en **Inicio de sesión**.
3. Seleccione el certificado del cual visualizar la información.
4. Haga doble clic en el certificado o clic en **Mostrar detalles**, y el visor de certificados de Microsoft se abrirá.





2.3.4.1.1.1.3 Eliminar certificados

Es posible eliminar todos certificados contenidos en la tarjeta inteligente o un certificado individual. Esta funcionalidad es útil si no existe espacio disponible en la tarjeta inteligente y es necesario añadir nuevos certificados.

2.3.4.1.1.1.3.1 Eliminar todos los certificados

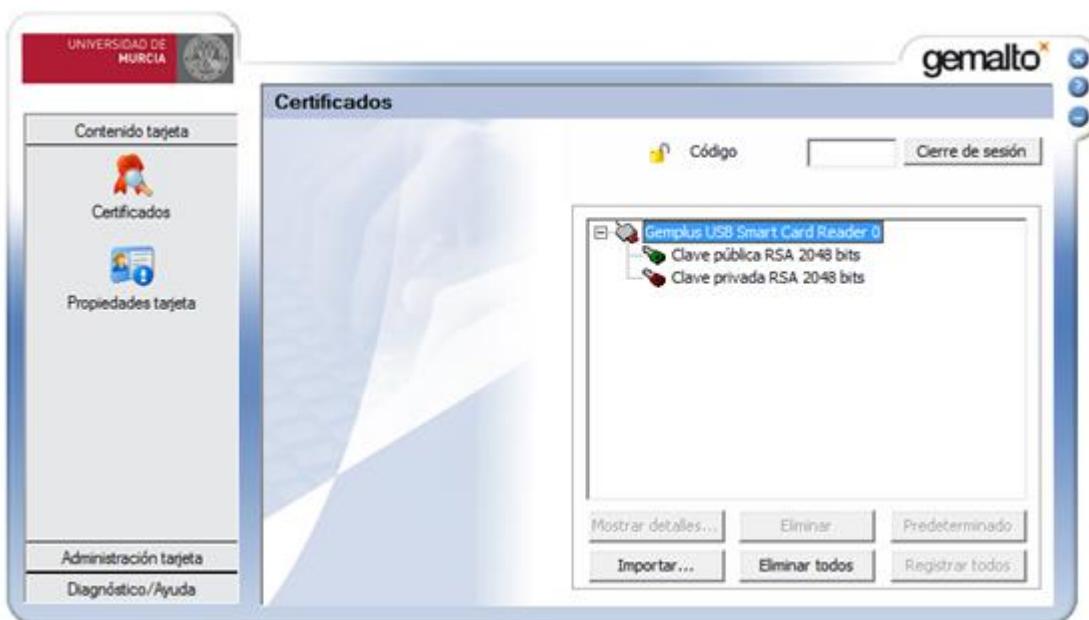
1. Haga clic en **Contenido tarjeta > Certificados**. Asegúrese previamente que la tarjeta de la que eliminar los certificados está correctamente conectada.
2. Habilite el acceso a la tarjeta, introduciendo el Código (NIP la tarjeta) y haciendo clic en **Inicio de sesión**.
3. Seleccione el lector de tarjetas inteligentes para activar el botón **Eliminar todos**.
4. Haga clic en **Eliminar todos**. Se mostrará una ventana de confirmación.





2.3.4.1.1.1.3.2 Eliminar certificado individual

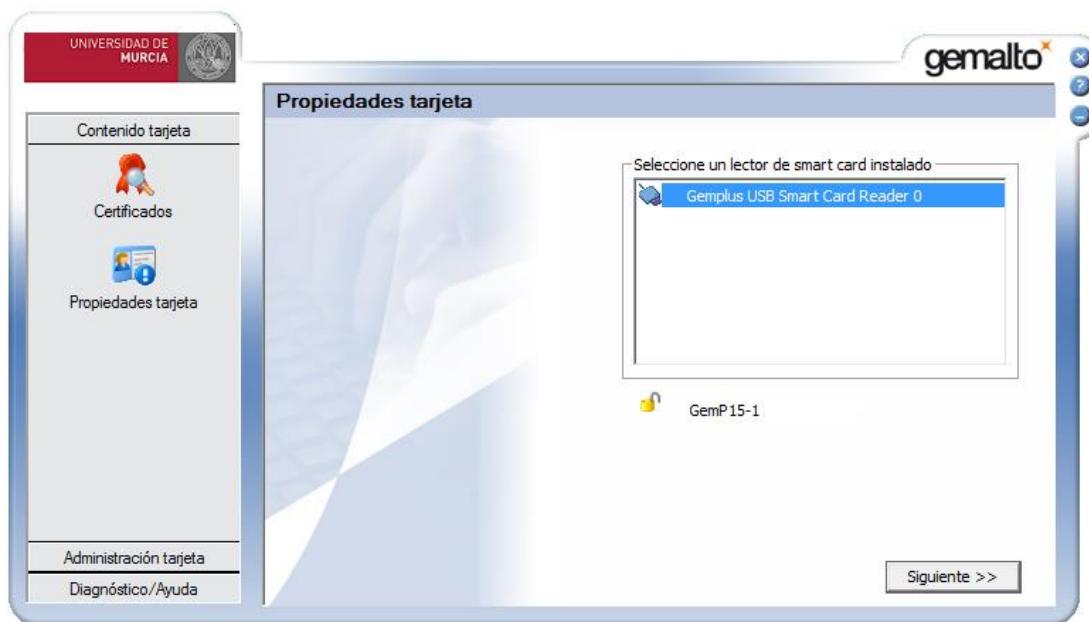
1. Haga clic en **Contenido tarjeta > Certificados**. Asegúrese previamente que la tarjeta de la que eliminar el certificado está correctamente conectada.
2. Habilite el acceso a la tarjeta, introduciendo el Código (NIP la tarjeta) y haciendo clic en **Inicio de sesión**.
3. Seleccione el certificado a eliminar y haga clic en **Eliminar**. Se mostrará una ventana de confirmación.
4. Además del certificado, es necesario eliminar la clave pública y privada asociadas al certificado. Para ello seleccionar cada una de las claves y hacer clic en **Eliminar**.



2.3.4.1.1.1.2 Propiedades tarjeta

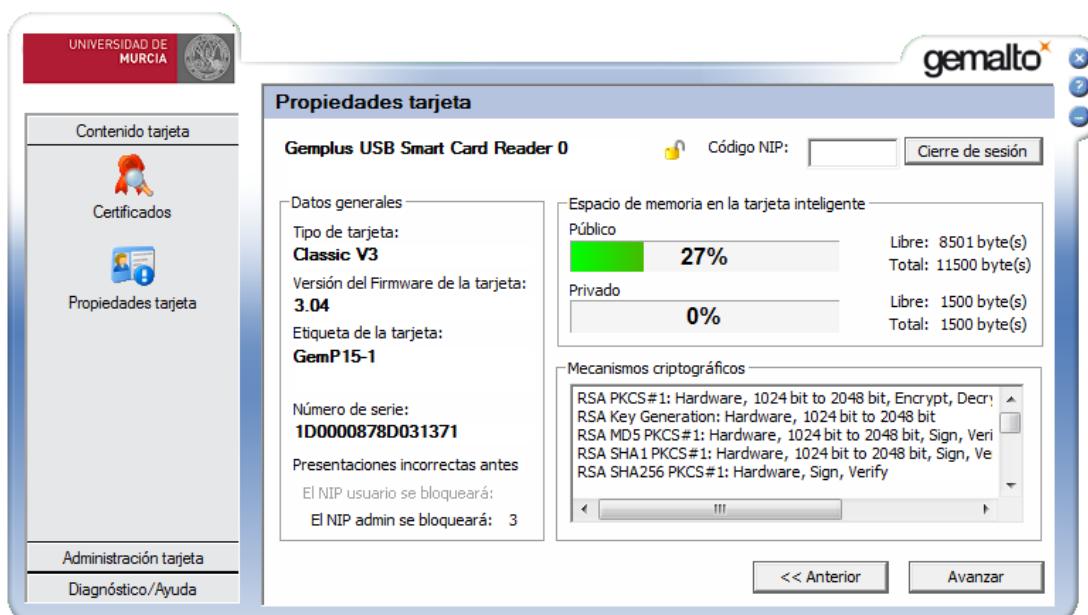
La herramienta **Propiedades tarjeta** permite visualizar información asociada con la tarjeta inteligente, que se encuentra disponible en el lector de tarjetas configurado.





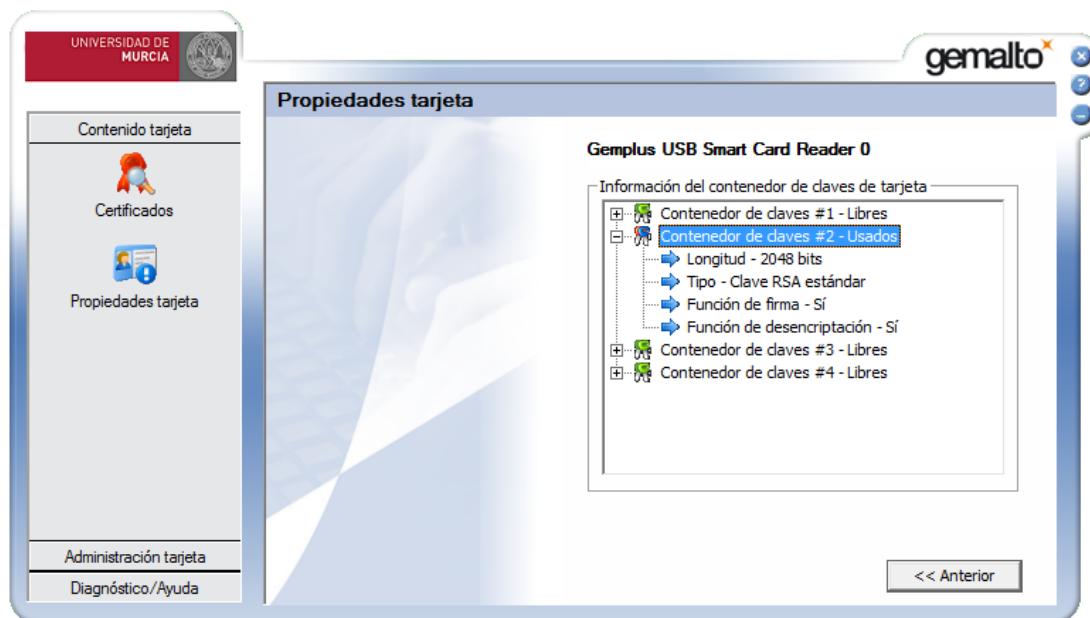
Para visualizar la información contenida en la tarjeta inteligente.

1. Seleccione el lector de tarjeta inteligente instalado y haga clic en **Siguiente**. Se mostrará la información de la tarjeta inteligente.



2. Habilite el acceso a la tarjeta, introduciendo el Código (NIP la tarjeta) y haciendo clic en **Inicio de sesión**, para que se active el botón **Avanzar**.
3. Haciendo clic en **Avanzar**, se mostrarán todas las claves contenidas en la tarjeta. Se podrá ver información adicional haciendo clic en el símbolo más, para expandir el contenedor de claves.





2.3.4.1.1.2 Administración tarjeta

Este menú contiene la herramienta **Administración de NIP**.

2.3.4.1.1.2.1 Administración de NIP

La herramienta **Administración de NIP** permite modificar el PIN asociado a una tarjeta inteligente. Además, permite ver las reglas para la generación del NIP, así como desbloquear el NIP.

Esta opción no se encuentra activada.

2.3.4.1.1.2.1.1 Cambio de NIP

Puede modificar el PIN de su tarjeta, desde una Secretaría Virtual (TPS) disponible en la gran mayoría de los centros o acudiendo a un punto de atención al carné inteligente.

2.3.4.1.1.2.1.2 NIP de desbloqueo

Para desbloquear el PIN de la tarjeta, diríjase a Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA) en el Campus de Espinardo o al Campus de La Merced (frente Biblioteca Nebrija).

También puede cambiarlo desde cualquier Secretaría Virtual autenticándose con tu cuenta de correo@um.es.

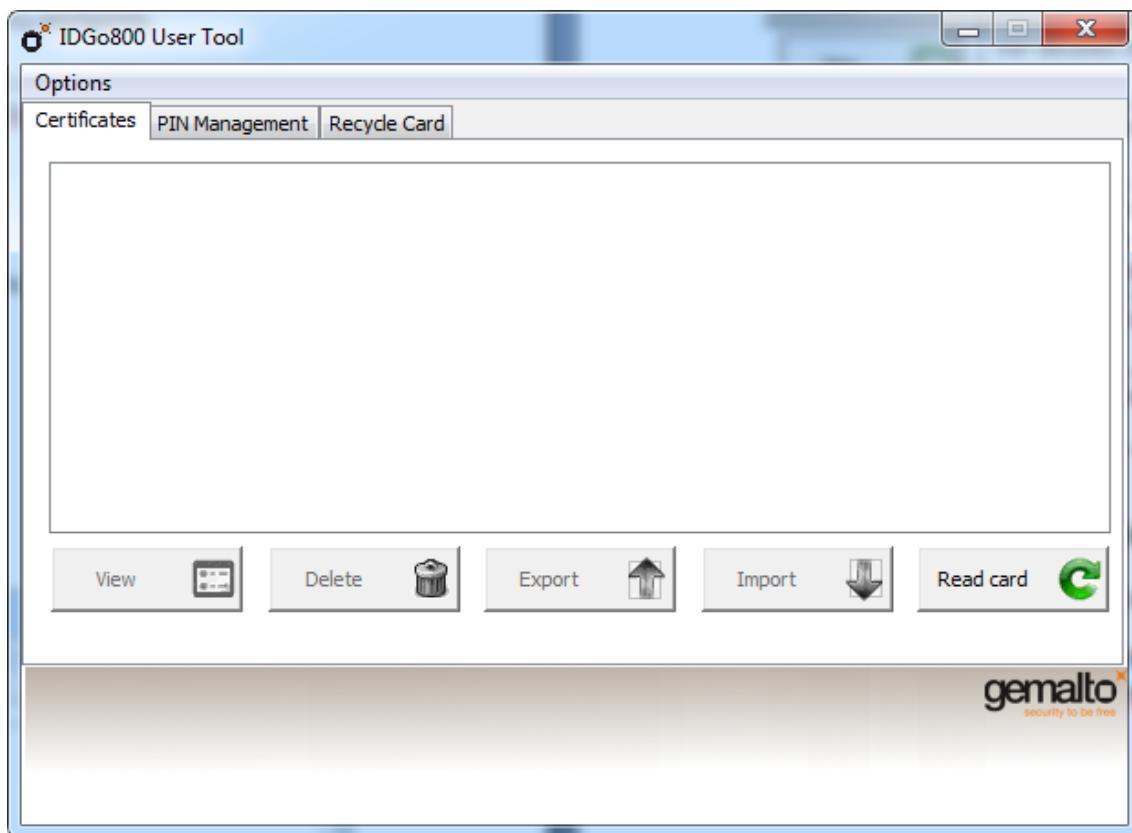




2.3.4.1.2 Gestor de certificados para la Tarjeta Universitaria Inteligente (TUI) Optelio R7 (TUI R7), IDGo800UserTool.

Para abrir la aplicación en un sistema Windows, navegue a **Inicio > Todos los programas > Datio Software > Middleware para la TUI > IDGo800UserTool**.

Para poder realizar cualquier acción, es necesario, que una vez introducida la tarjeta inteligente en el lector se establezca la conexión con ésta, para ello haga clic en **Read Card**.



2.3.4.1.2.1 Certificados

Si la tarjeta inteligente contiene certificados, la lista de certificados contenidos se muestra en la pestaña **Certificates**.

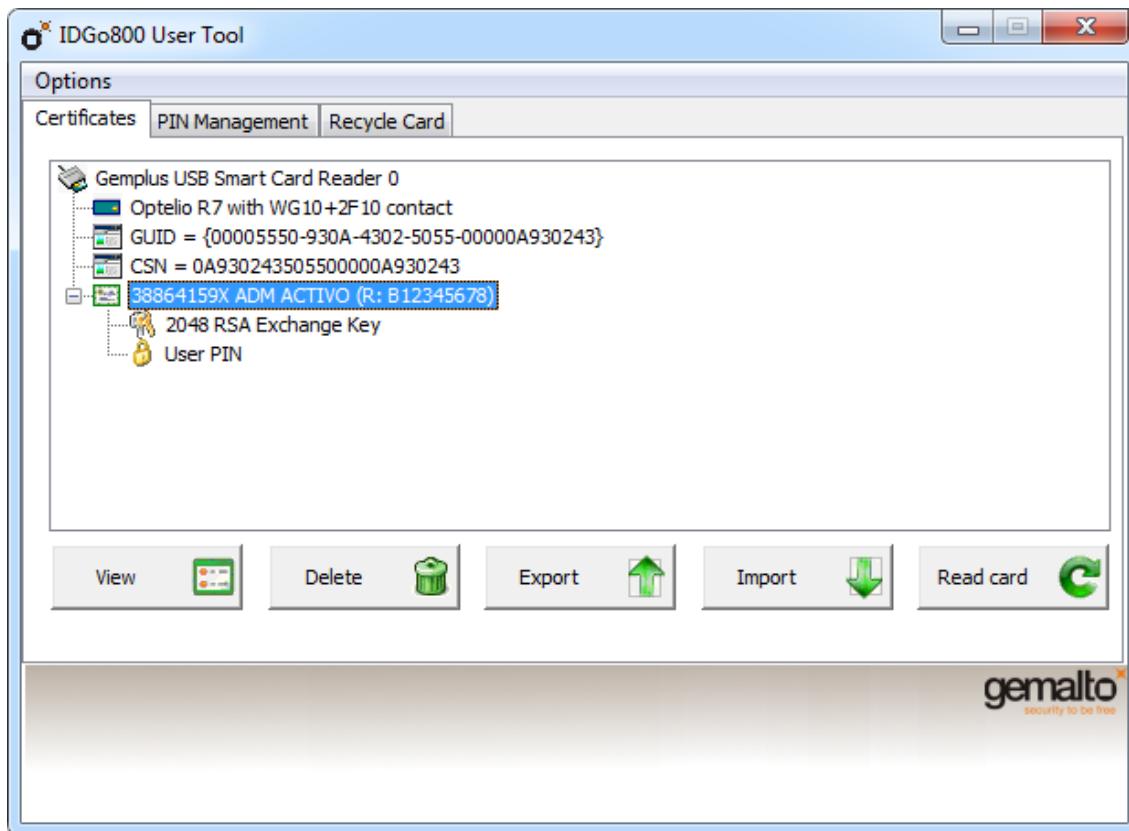
La información que se puede ver es la siguiente:

- Tipo de tarjeta (Card Type).
- Identificador único de la tarjeta (GUID).
- Número de serie (CSN).
- Certificados de usuario junto con claves privadas.





- Certificados de CA.



Las siguientes opciones están disponibles desde la pestaña **Certificates**.

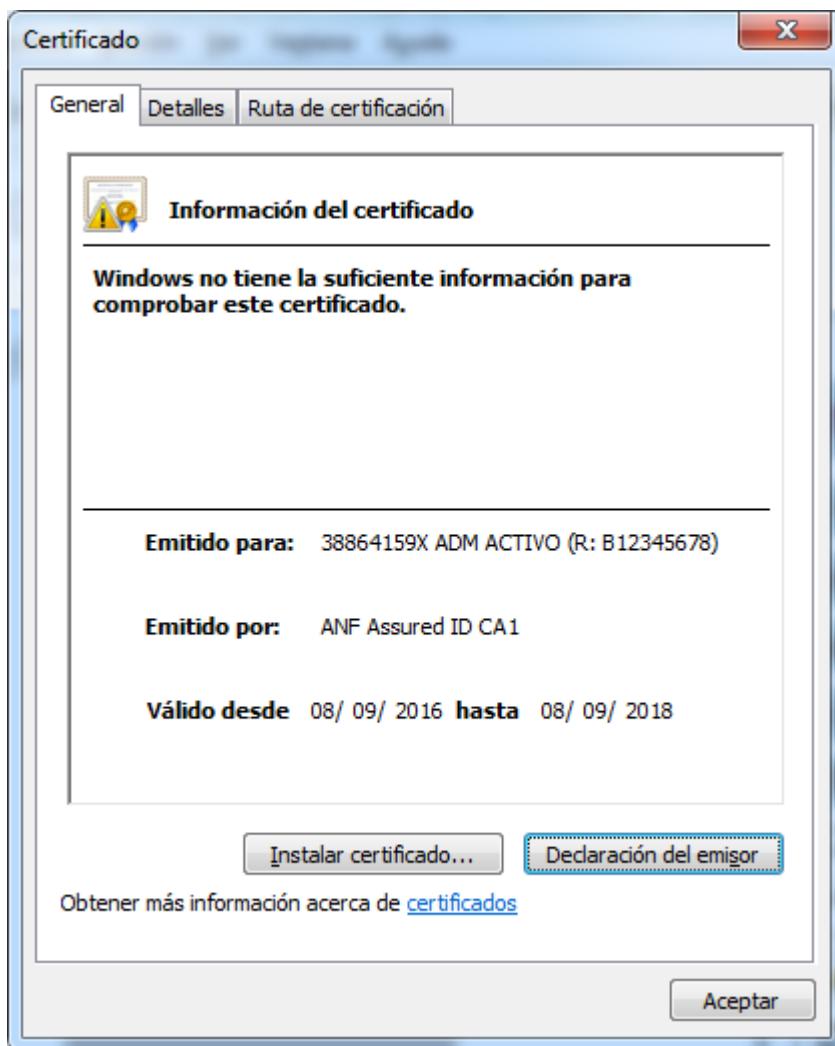
Función	Descripción
	Ver detalles de un certificado.
	Elimina el certificado seleccionado de la tarjeta inteligente.
	Exporta el certificado seleccionado desde la tarjeta inteligente. La clave privada no es posible exportarla, únicamente se puede exportar la parte pública del certificado.
	Importar un certificado a la tarjeta inteligente.
	Lee la información almacenada en la tarjeta.

2.3.4.1.2.1.1 Ver datos de un certificado

Para ver los datos de un certificado.

1. Seleccione la pestaña **Certificates** y haga clic en el certificado cuyos datos se quieren consultar.
2. Haga clic en **View**.



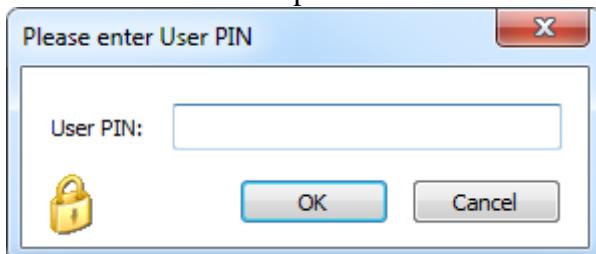


2.3.4.1.2.1.2 Eliminar certificado

Para eliminar un certificado, debe llevar a cabo los siguientes pasos:

1. Seleccione la pestaña **Certificates** y haga clic en el certificado que se quiere eliminar.
2. Haga clic en **Delete**.

Se muestra la ventana para introducir el **PIN** de la tarjeta.



3. Introduzca el **PIN** y haga clic en **OK**.
4. El certificado seleccionado es eliminado.

Se muestra un mensaje indicando que el proceso se ha completado correctamente.





2.3.4.1.2.1.3 Exportar certificado

Para exportar la parte pública de un certificado, debe realizar los siguientes pasos:

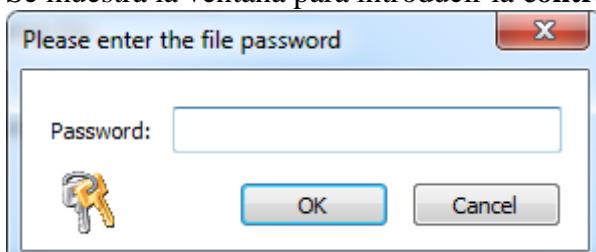
1. Seleccione la pestaña **Certificates** y haga clic en el certificado que se quiere exportar.
2. Haga clic en **Export**. Se muestra la ventana **Guardar** de Windows.
La clave privada no es posible exportarla, únicamente se puede exportar la parte pública del certificado.
3. Seleccione la localización en la que almacenar el certificado, introduzca el nombre del fichero y haga clic en **OK**.

2.3.4.1.2.1.4 Importar certificado

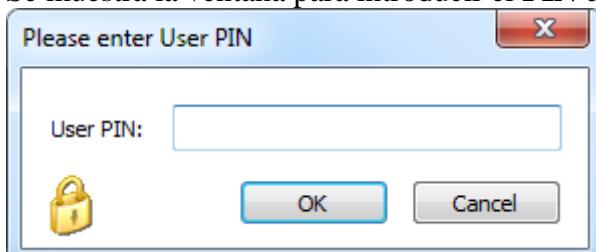
Cuando se importa un certificado, la clave privada y el certificado correspondiente son importados a la tarjeta inteligente. Se solicita al usuario la contraseña que protege al fichero que contiene el certificado.

Para importar un certificado.

1. Seleccione la pestaña **Certificates** y haga clic en **Import**.
2. Seleccione el archivo PKCS#12 (.pfx ó .p12) que contiene el certificado a importar, y haga clic en **Abrir**.
Se muestra la ventana para introducir la **contraseña** del certificado.



3. Introduzca la **contraseña** del certificado y haga clic en **OK**.
Se muestra la ventana para introducir el **PIN** de la tarjeta.



4. Introduzca el **PIN** de la tarjeta y haga clic en **OK**.
5. El certificado seleccionado es importado.
Se muestra un mensaje indicando que el proceso se ha completado correctamente.
6. Una vez importado el certificado, es necesario extraer la tarjeta del lector, y volver a introducirla para que el certificado importado esté disponible en los almacenes de claves.

2.3.4.1.2.2 Gestión del PIN (PIN Management)

Permite realizar acciones sobre el PIN de la tarjeta.





IMPORTANTE: Aunque el gestor de certificados permite modificar o desbloquear el PIN de la tarjeta, **está completamente desaconsejado su uso. La aplicación de estas opciones podría invalidar la tarjeta.**

ES RESPONSABILIDAD DE LA PERSONA USUARIA CUALQUIER PROBLEMA DERIVADO DE HACER CASO OMISO A ESTA RECOMENDACIÓN.

2.3.4.1.2.2.1 Cambiar PIN de usuario

Puede modificar el PIN de su tarjeta, desde una Secretaría Virtual (TPS) disponible en la gran mayoría de los centros o acudiendo a un punto de atención al carné inteligente.

2.3.4.1.2.2.2 Desbloquear PIN de usuario

Para desbloquear el PIN de la tarjeta, diríjase a Área de Tecnologías de la Información y las Comunicaciones Aplicadas (ATICA) en el Campus de Espinardo o al Campus de La Merced (frente Biblioteca Nebrija).

También puede cambiarlo desde cualquier Secretaría Virtual autenticándose con tu cuenta de correo@um.es.

2.3.4.1.2.3 Reciclar tarjeta (Recycle Card)

Permite eliminar todos los objetos presentes en la tarjeta.

IMPORTANTE: Aunque el gestor de certificados permite modificar o desbloquear el PIN de la tarjeta, **está completamente desaconsejado su uso. La aplicación de estas opciones podría invalidar la tarjeta.**

ES RESPONSABILIDAD DE LA PERSONA USUARIA CUALQUIER PROBLEMA DERIVADO DE HACER CASO OMISO A ESTA RECOMENDACIÓN.





2.3.4.2 Linux y Mac

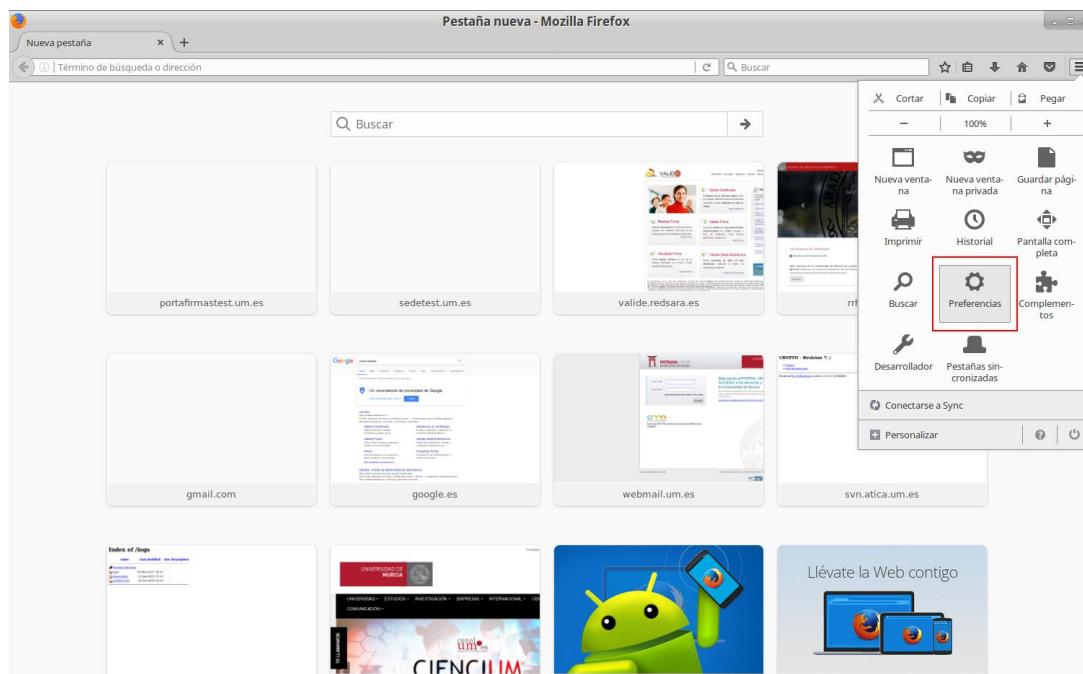
Tanto la importación de certificados a la tarjeta universitaria como el borrado de los certificados en la misma se llevará a cabo usando el navegador **Mozilla Firefox**. Para ello, tenemos que tener correctamente configurados los [módulos PKCS#11 en el navegador](#).

La información sobre como configurar correctamente **Mozilla Firefox** la podemos encontrar [aquí](#).

2.3.4.2.1 Importación de certificados

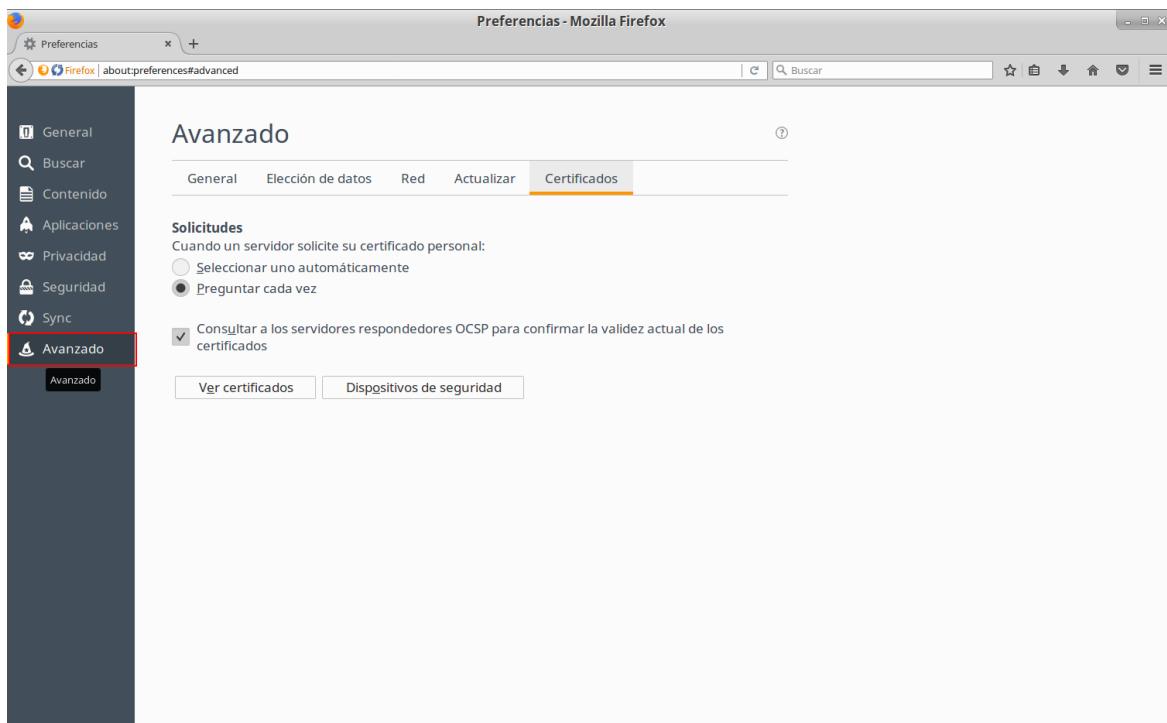
Los pasos que hay que realizar para la importación son los siguientes:

1. Abrir el navegador **Mozilla Firefox** e ir a las preferencias.

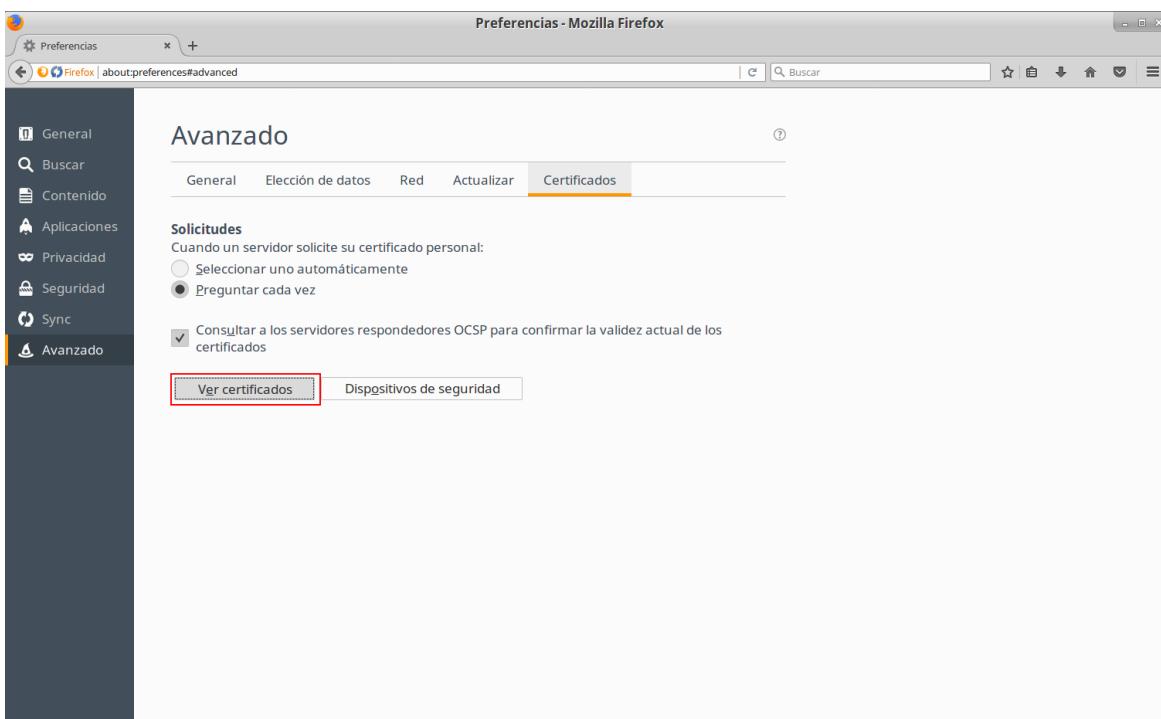




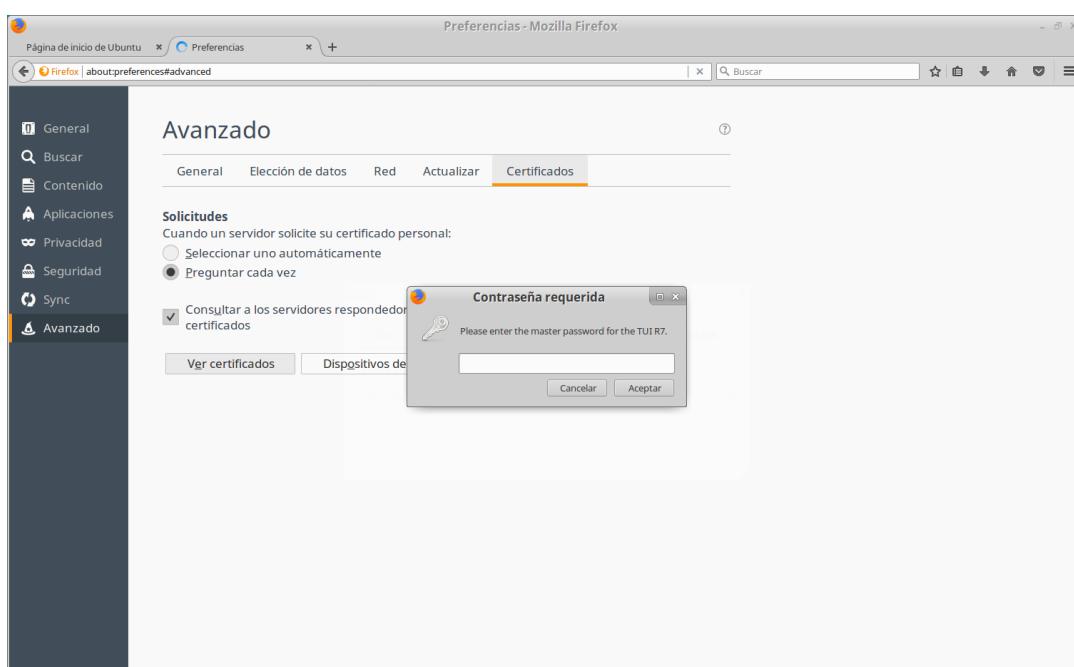
2. En las preferencias del navegador, ir a la última opción, *Avanzado*. Una vez que estemos en dicha opción, tenemos que ir a la última pestaña, *Certificados*.



3. Una vez que estemos en la pestaña *Certificados*, pulsar el botón *Ver certificados*.

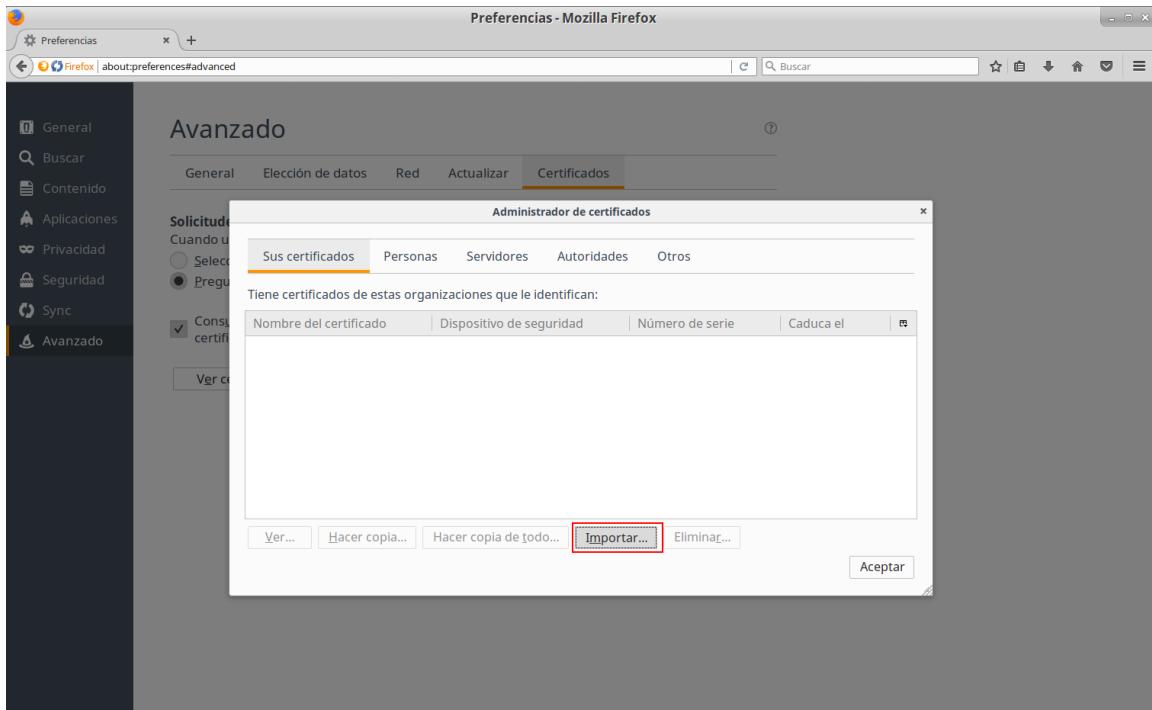


4. Si es la primera vez que intentamos acceder a los certificados desde que hemos arrancado **Firefox**, nos pedirá el **PIN** de la tarjeta, para poder leer los posibles certificados que tenga.

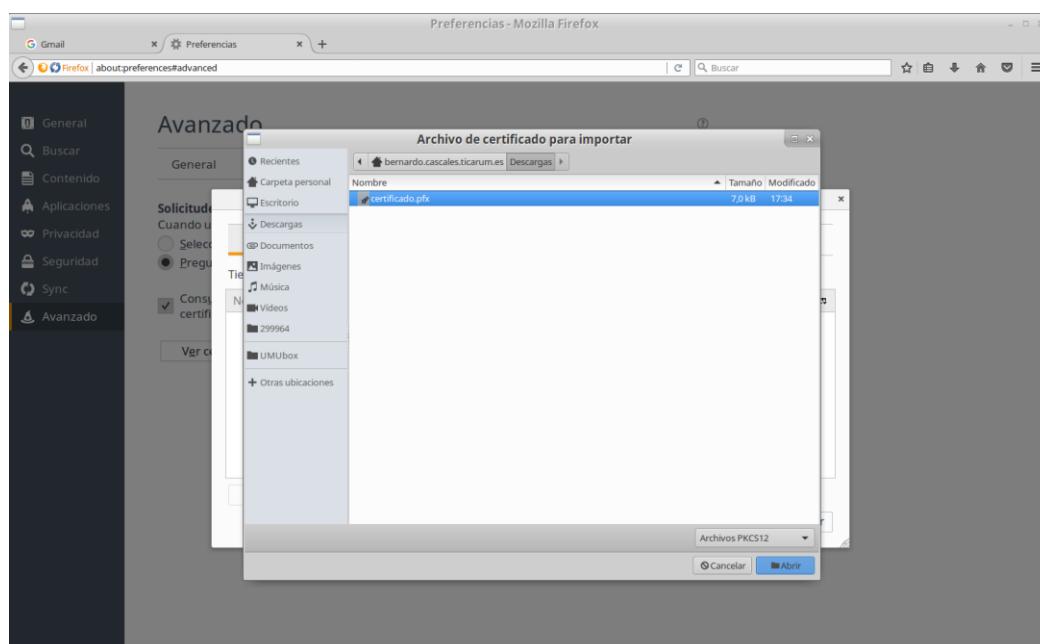




5. Una vez que se abra la ventana **Administrador de certificados**, estando en la pestaña **Sus certificados**, pulsamos sobre el botón **Importar**.

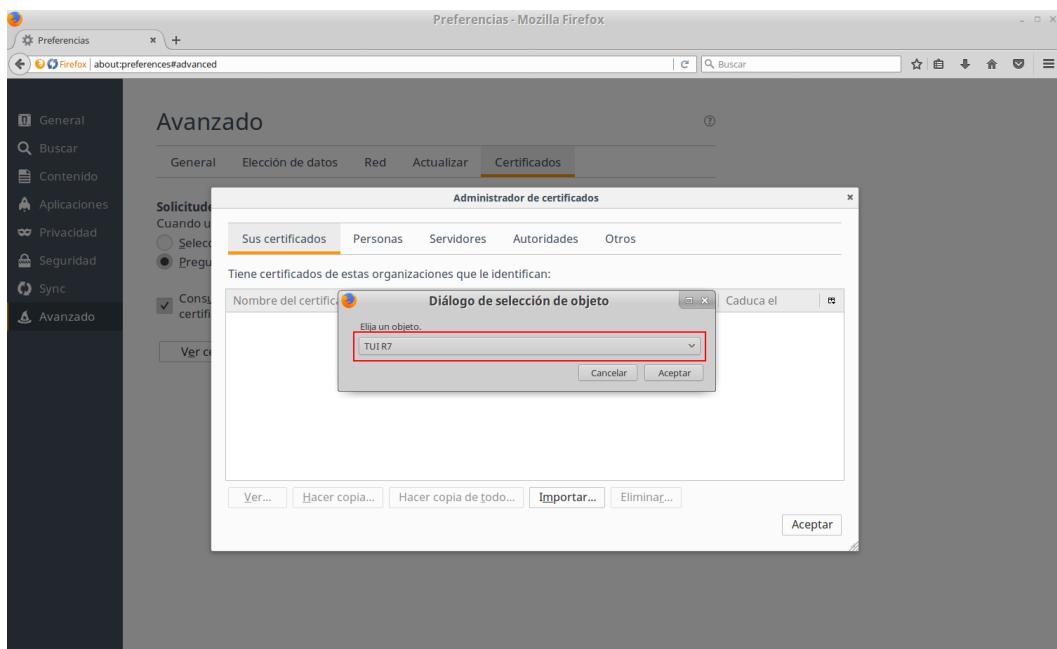


6. Tras pulsar sobre el botón **Importar**, se abrirá el explorador de ficheros. Tenemos que buscar el fichero (.p12 o .pfx) que contiene al certificado a importar. Una vez localizado, seleccionar el fichero y pulsar el botón **Abrir**.

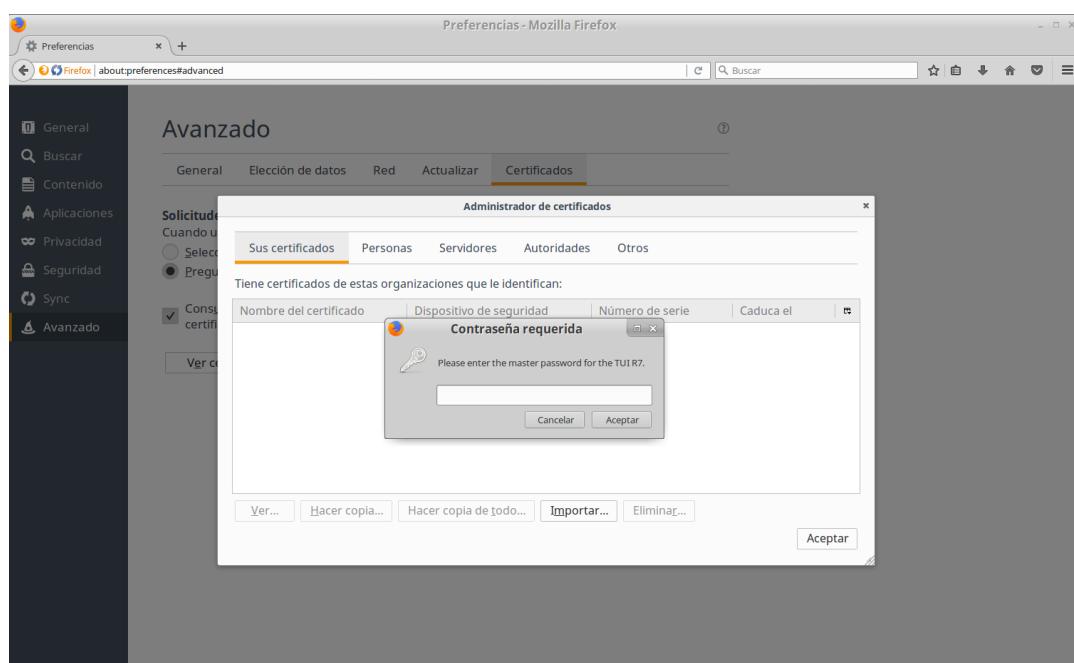




7. Una vez que pulsemos *Abrir*, nos preguntará dónde queremos importar el certificado. Tenemos que seleccionar, de las opciones disponibles, la opción **TUI R7 o GemP15-1** (dependerá del modelo de TUI que tengamos).

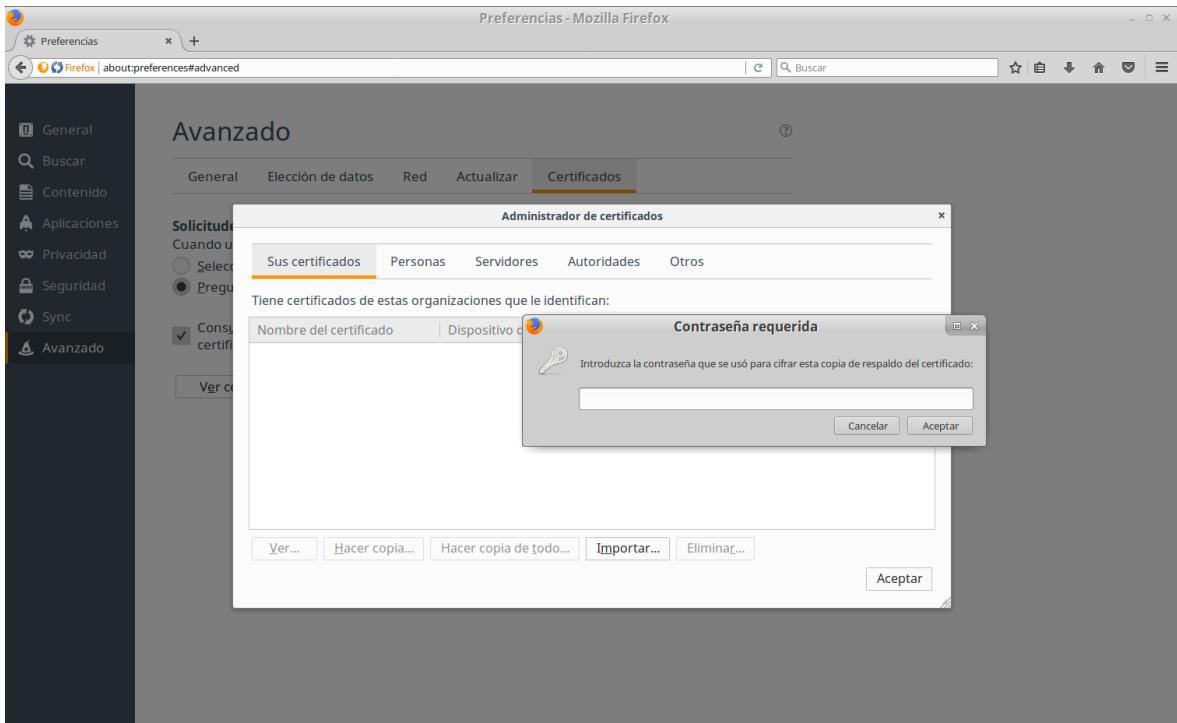


8. Una vez que hemos seleccionado el certificado a importar, se nos pedirá el **PIN** de la tarjeta. Introducir el **PIN** y pulsar *Aceptar*.

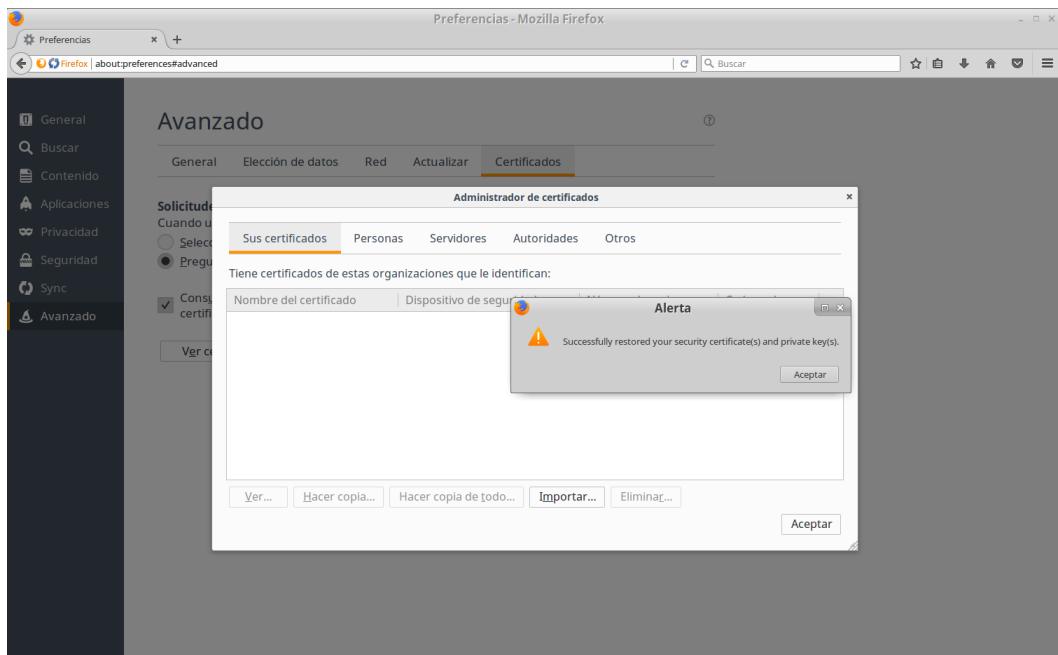




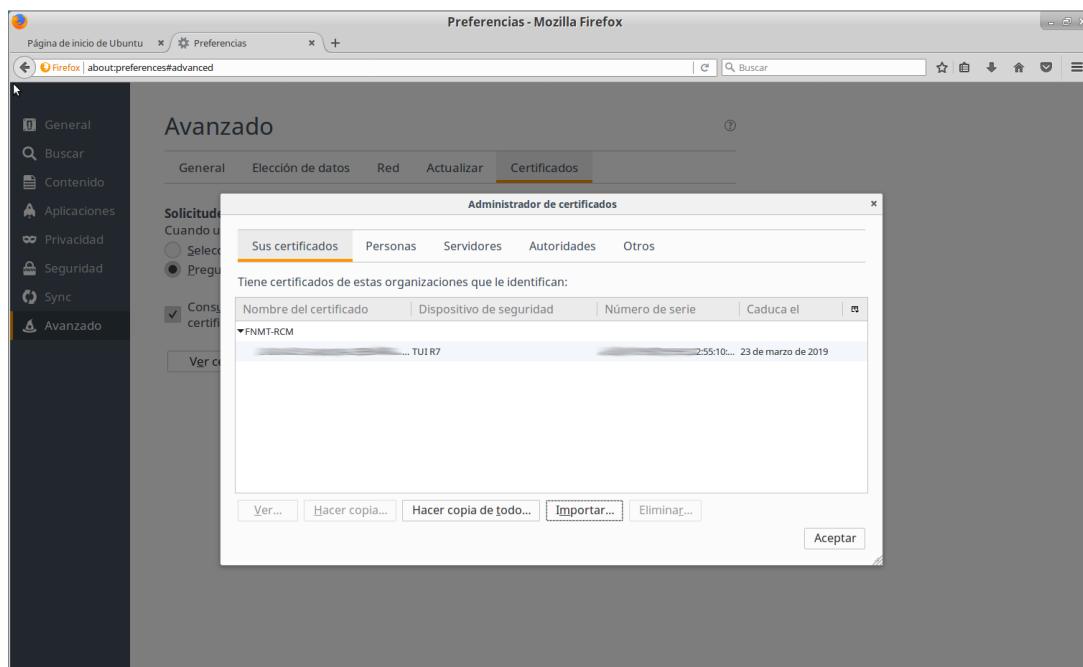
9. Tras introducir el PIN de la tarjeta, se mostrará un nuevo diálogo, en el cual, se nos pide la contraseña del certificado. Introducir dicha contraseña y pulsar **Aceptar**.



10. Tras introducir la contraseña, si la hemos puesto correctamente, se mostrará la siguiente imagen, indicándonos que todo ha ido bien. Pulsar sobre el botón **Aceptar**.



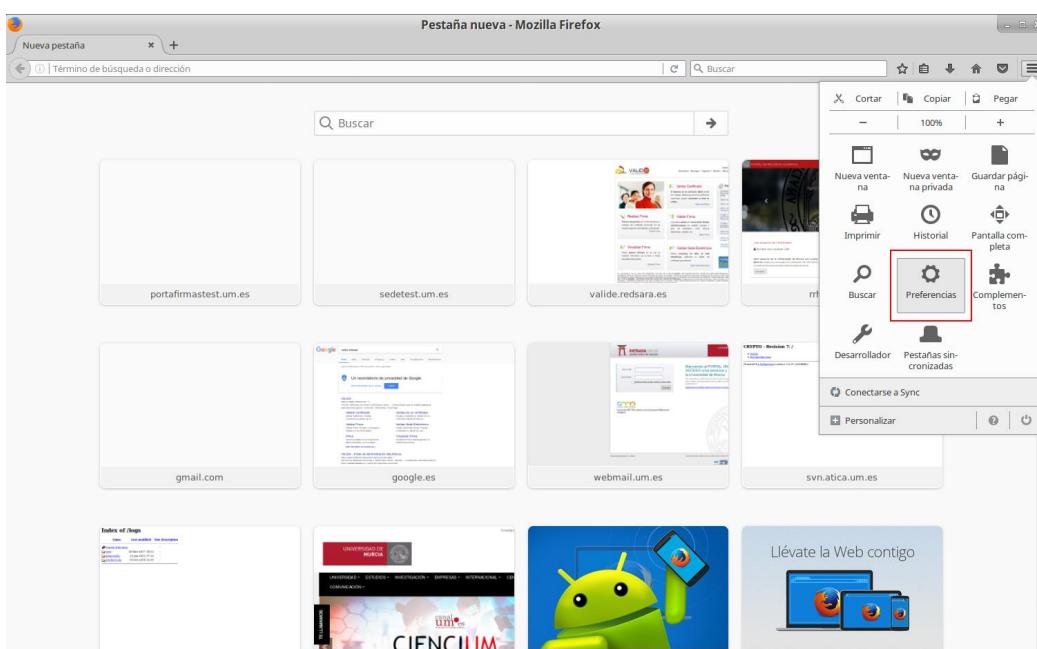
11. Una vez que hemos importado correctamente el certificado, podremos verlo en la pestaña *Sus certificados*.



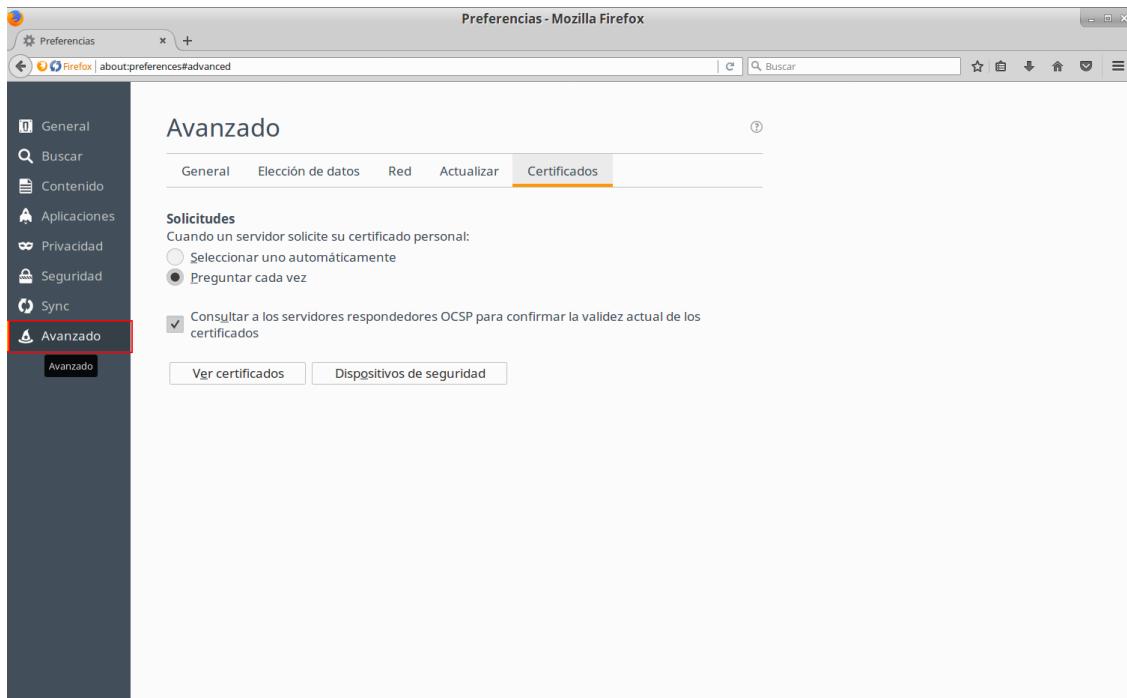


2.3.4.2.2 Borrado de certificados

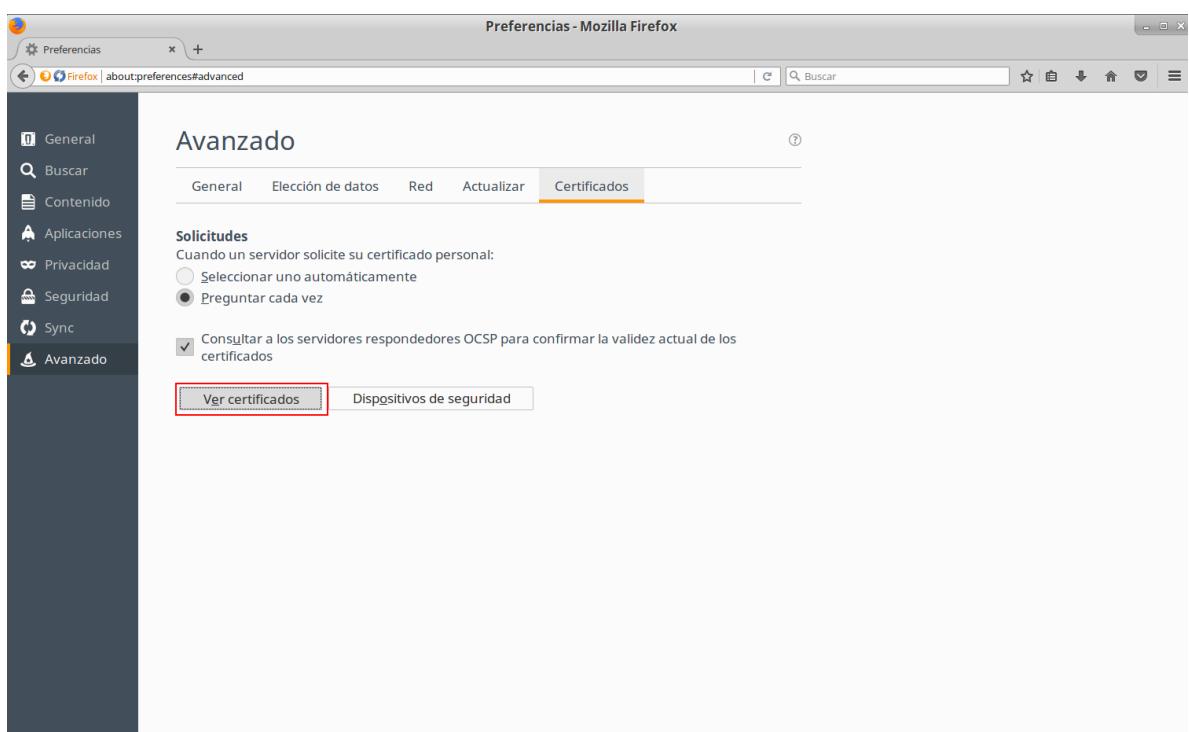
1. Abrir el navegador **Mozilla Firefox** e ir a las preferencias.



2. En las preferencias del navegador, ir a la última opción, **Avanzado**. Una vez que estemos en la opción **Avanzado**, tenemos que ir a la última pestaña, **Certificados**.

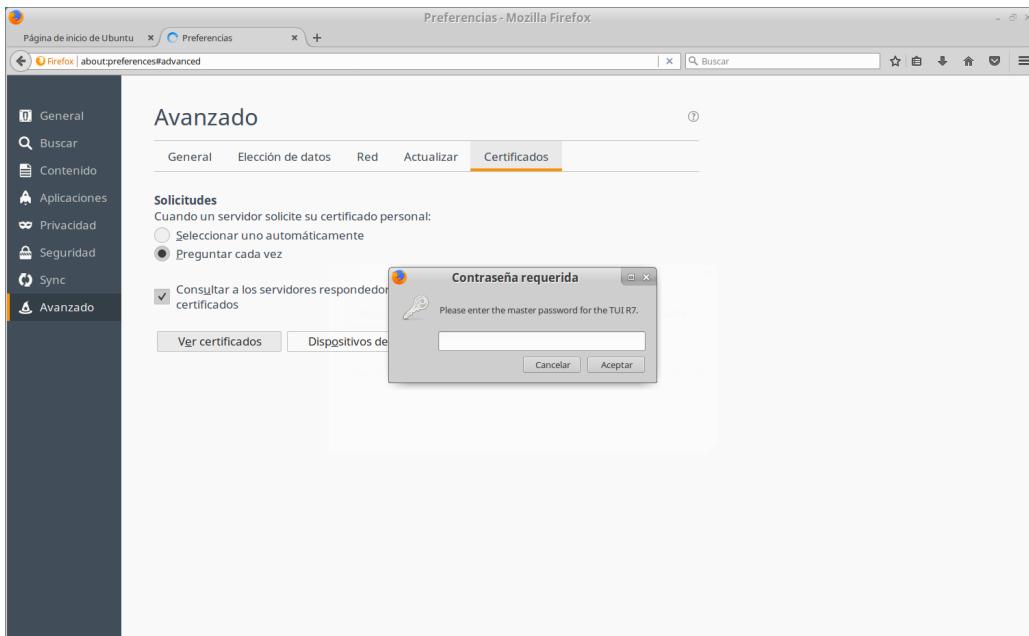


3. Una vez que estemos en la pestaña *Avanzado*, pulsar el botón **Ver certificados**.

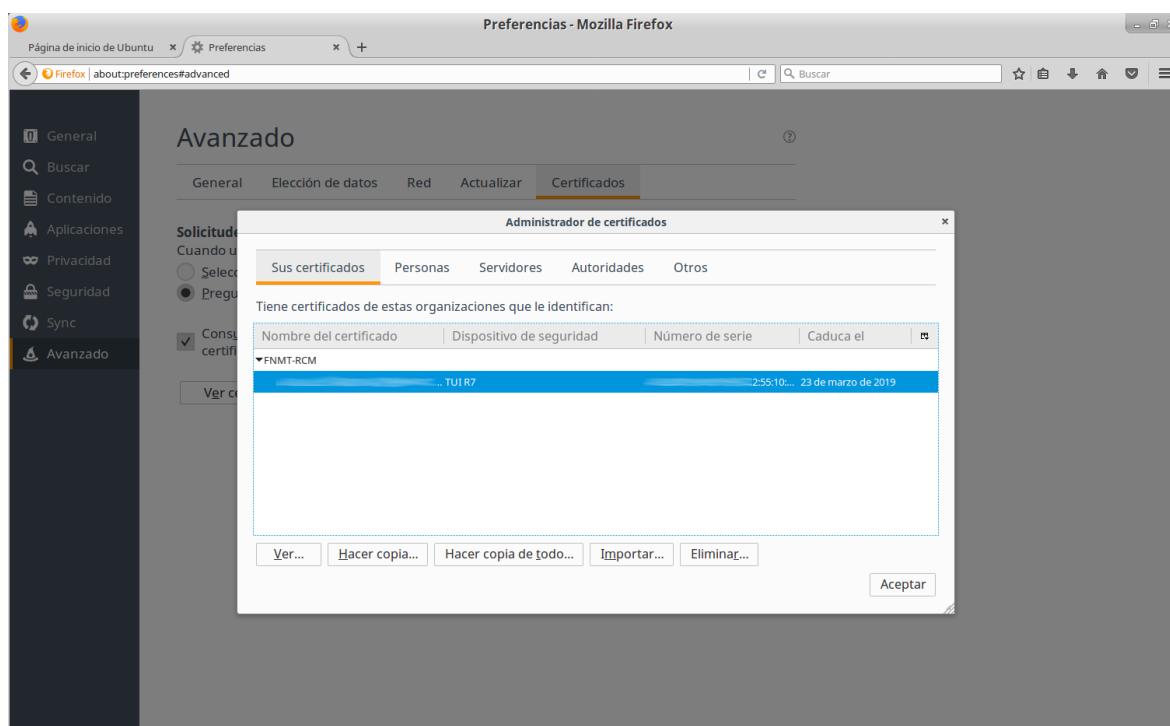




- Si es la primera vez que intentamos acceder a los certificados desde que hemos arrancado **Mozilla Firefox**, nos pedirá el **PIN** de la tarjeta, para poder leer los posibles certificados que tenga.

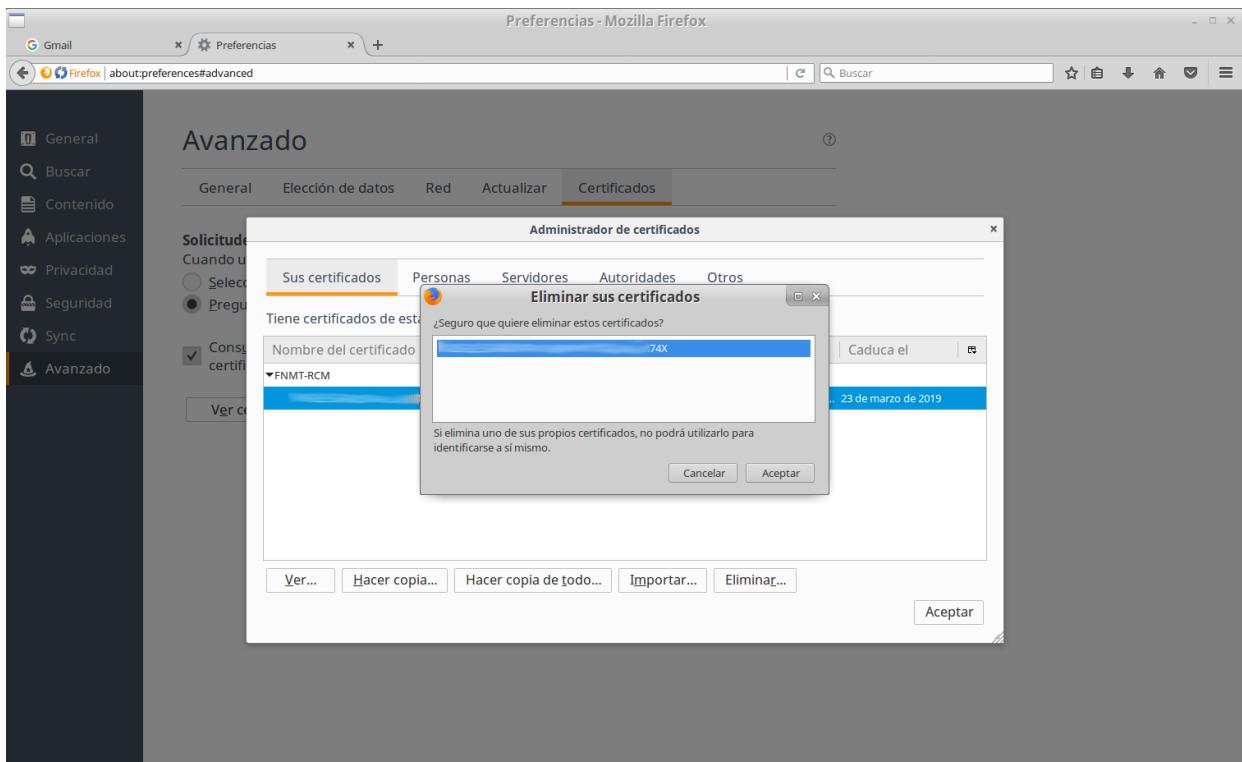


- Una vez que se abra la ventana de los certificados, desde la pestaña **Sus certificados**, seleccionamos el certificado que queremos eliminar, y pulsamos sobre el botón **Eliminar**.

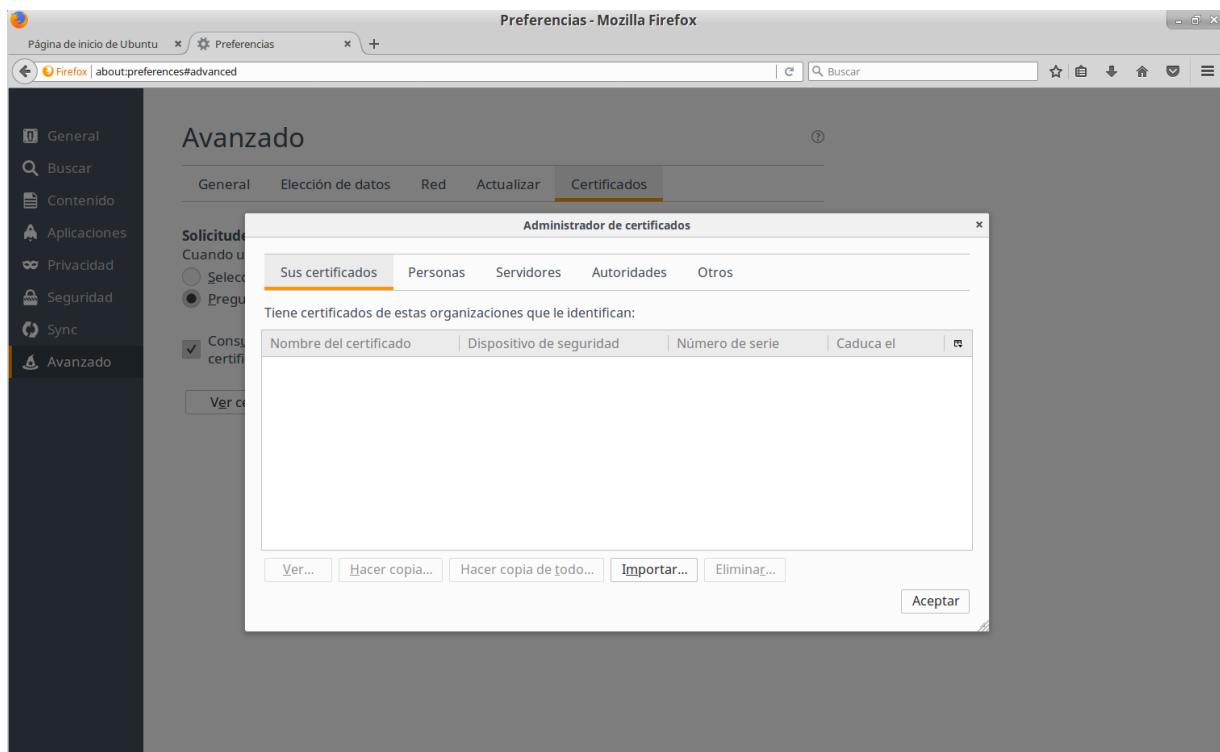




6. Tras pulsar el botón **Eliminar**, se mostrará un diálogo. Seleccionar el certificado a borrar de la tarjeta, como se muestra en la siguiente imagen.



7. Tras eliminarlo, se volverá a mostrar la pantalla de certificados. Podemos comprobar que ya no aparece el certificado eliminado.





3 Uso del certificado electrónico instalado en el equipo

3.1 Introducción

Para poder hacer uso del certificado electrónico instalado en su equipo, han de cumplirse una serie de requisitos previos:

- Tener emitido un certificado electrónico por alguna de las entidades admitidas por la Universidad de Murcia.
- Tener instalado el certificado en el almacén de certificados del sistema
 - o
 - Tener instalado el certificado en el almacén de la aplicación concreta, en el caso de Mozilla Firefox, Mozilla Thunderbird (y Google Chrome/Chromium en Linux).

Para todos estos requisitos previos, por favor acuda a la Web de la Sede Electrónica de la Universidad de Murcia: <https://sedetest.um.es/sede/soporte/firmaCertificado.seam>.

Si se van a utilizar los servicios de firma electrónica desde páginas Web, es necesario tener instalado en su equipo la aplicación AutoFirm@. Puede obtener más información en la Sede Electrónica de la Universidad de Murcia: <https://sedetest.um.es/sede/soporte/software.seam>.

Si se desea hacer uso de la firma electrónica en aplicaciones de correo, deberá consultar el apartado sobre [instalación del componente para la firma electrónica en aplicaciones de correo](#).

Cuando haya finalizado este último apartado, puede que le interese consultar la [configuración y uso de la firma electrónica en aplicaciones de correo](#).



3.2 Instalación de componentes para la firma electrónica en aplicaciones de correo

La firma de correos electrónicos en Windows está soportada de forma nativa para aplicaciones Microsoft.

Para programas de terceros, como Mozilla Thunderbird, no es necesaria la instalación de ningún componente, sin embargo sí es necesario que siga los pasos descritos en el apartado [configuración y uso de la firma electrónica en aplicaciones de correo](#).



4 Configuración y uso de la firma electrónica en aplicaciones de correo

4.1 Introducción

En el siguiente apartado se describe cómo configurar diversas aplicaciones de correo para que hagan uso del certificado electrónico.

Se presupone que se cumplen los siguientes requisitos previos:

- Disponer de un certificado electrónico ya sea instalado en el equipo, o utilizando la tarjeta universitaria
- Tener una cuenta de correo correctamente configurada.

Si no cumple estos requisitos, acuda a la Web de la Sede Electrónica de la Universidad de Murcia <https://sedetest.um.es/sede/soporte/firmaCertificado.seam>.



4.2 Microsoft Outlook

Para configurar el certificado electrónico con el que firmar los correos de su cuenta, es necesario que modifique la configuración de seguridad de la misma.

En Outlook 2010 y 2007 vaya al menú **Archivo** -> **Opciones** -> **Centro de confianza** -> **Configuración del centro de confianza** -> **Seguridad del correo electrónico**.

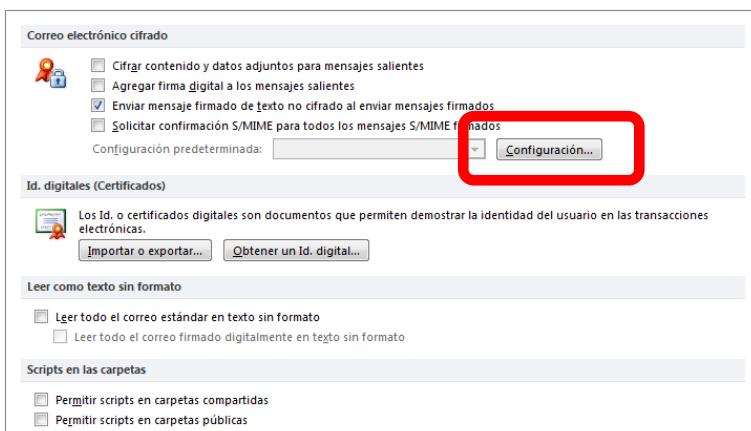
The screenshot shows five windows illustrating the steps to reach the 'Seguridad del correo electrónico' (Email Security) settings in Microsoft Outlook 2010:

- Step 1:** The main Outlook window with the ribbon menu open. The 'Archivo' tab is selected. A red box highlights the 'Archivo' tab and the 'Nuevo mensaje de correo electrónico' button.
- Step 2:** The 'Archivo' tab is still selected. A red box highlights the 'Opciones' button in the ribbon.
- Step 3:** The 'Opciones de Outlook' dialog box is open, showing the 'General' tab. A red box highlights the 'Centro de confianza' (Trust Center) link under 'Complementos'.
- Step 4:** The 'Centro de confianza de Microsoft Outlook' (Microsoft Trust Center) page is displayed. A red box highlights the 'Configuración del Centro de confianza...' (Configure Trust Center...) button.
- Step 5:** The 'Edificadores de confianza' (Trust Builders) dialog box is open, showing the 'Seguridad del correo electrónico' (Email Security) section. A red box highlights the 'Permitir descargas de imágenes en mensajes de correo electrónico...' (Allow download of images in email messages...) checkbox.

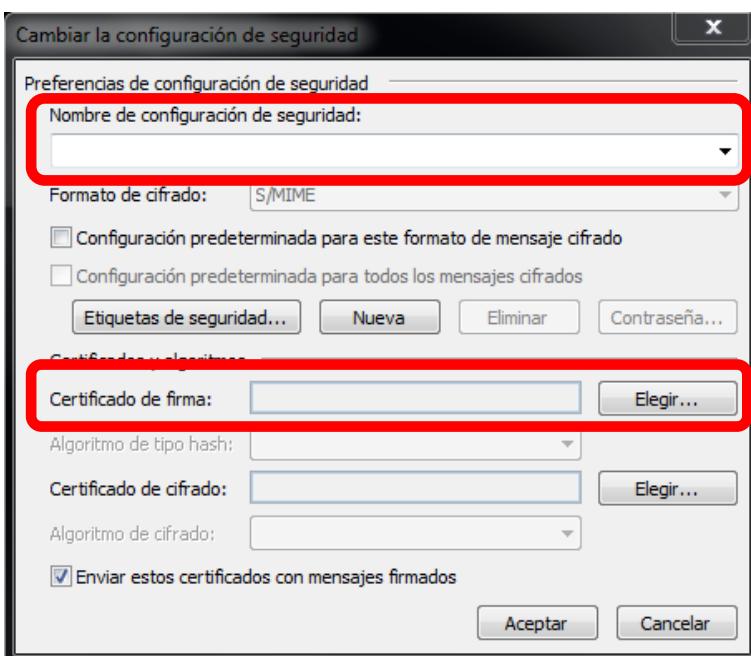


En versiones anteriores de Microsoft Outlook, esta ventana de configuración puede abrirse de la siguiente forma: Acceda al menú **Herramientas -> Opciones**. Seleccione la pestaña **Seguridad**.

Se le mostrará una ventana como la siguiente:



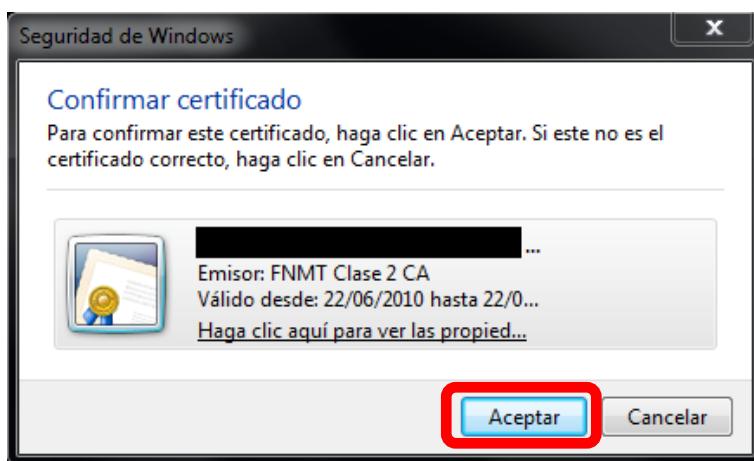
Pulse el botón **Configuración** dentro del grupo *Correo electrónico cifrado* y se abrirá la siguiente ventana:



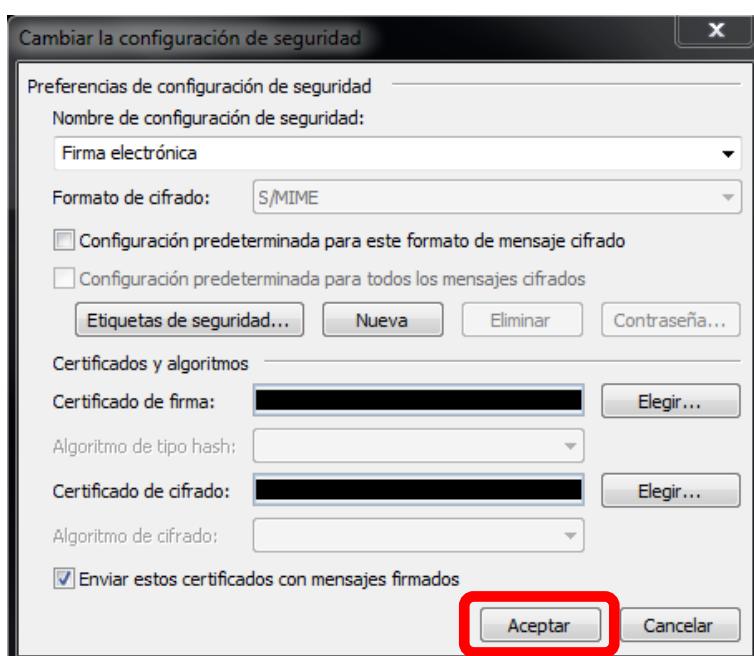
Introduzca un **nombre de configuración de seguridad** si no tiene ninguno y pulse el botón **Elegir**.



Se le mostrará una ventana donde deberá elegir qué certificado usar para la firma. Elija el certificado que desee usar y pulse **Aceptar**.

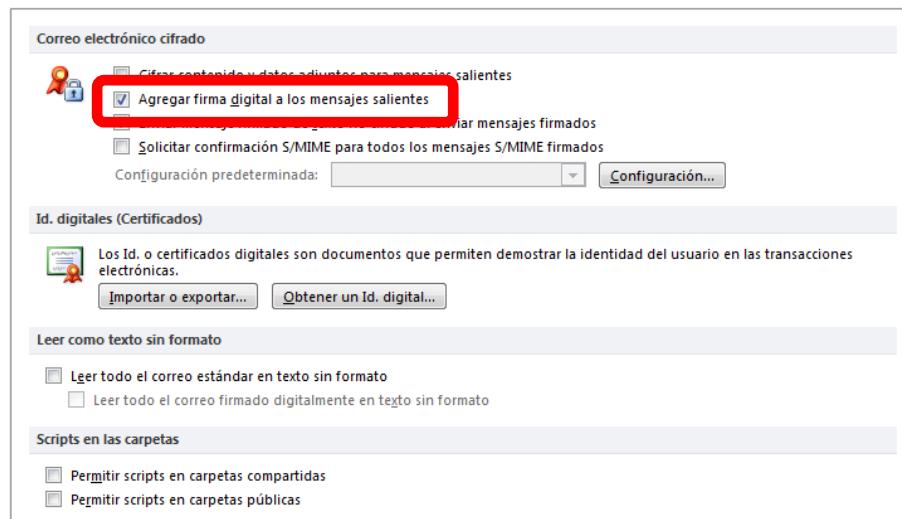


Se habrán asignado unos certificados para la firma y el cifrado. Es importante destacar que actualmente **no se soporta la funcionalidad de cifrado**. Pulse **Aceptar**.



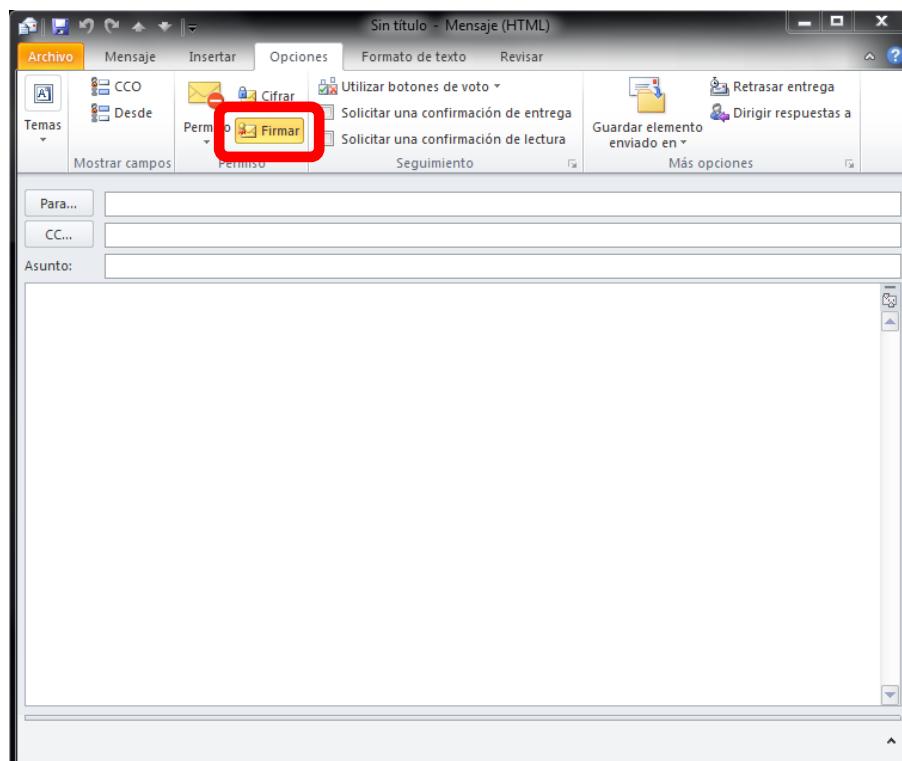


Para establecer esta configuración como predeterminada para todos los correos, marque la casilla Agregar firma digital a los mensajes salientes en la ventana que se muestra.



Acepte y cierre todas las ventanas que haya abierto durante el proceso.

Ya ha configurado la firma electrónica para su cuenta de correo. Para modificar de forma específica la firma electrónica para un correo acceda a la pestaña opciones y utilice el botón **Firmar**.

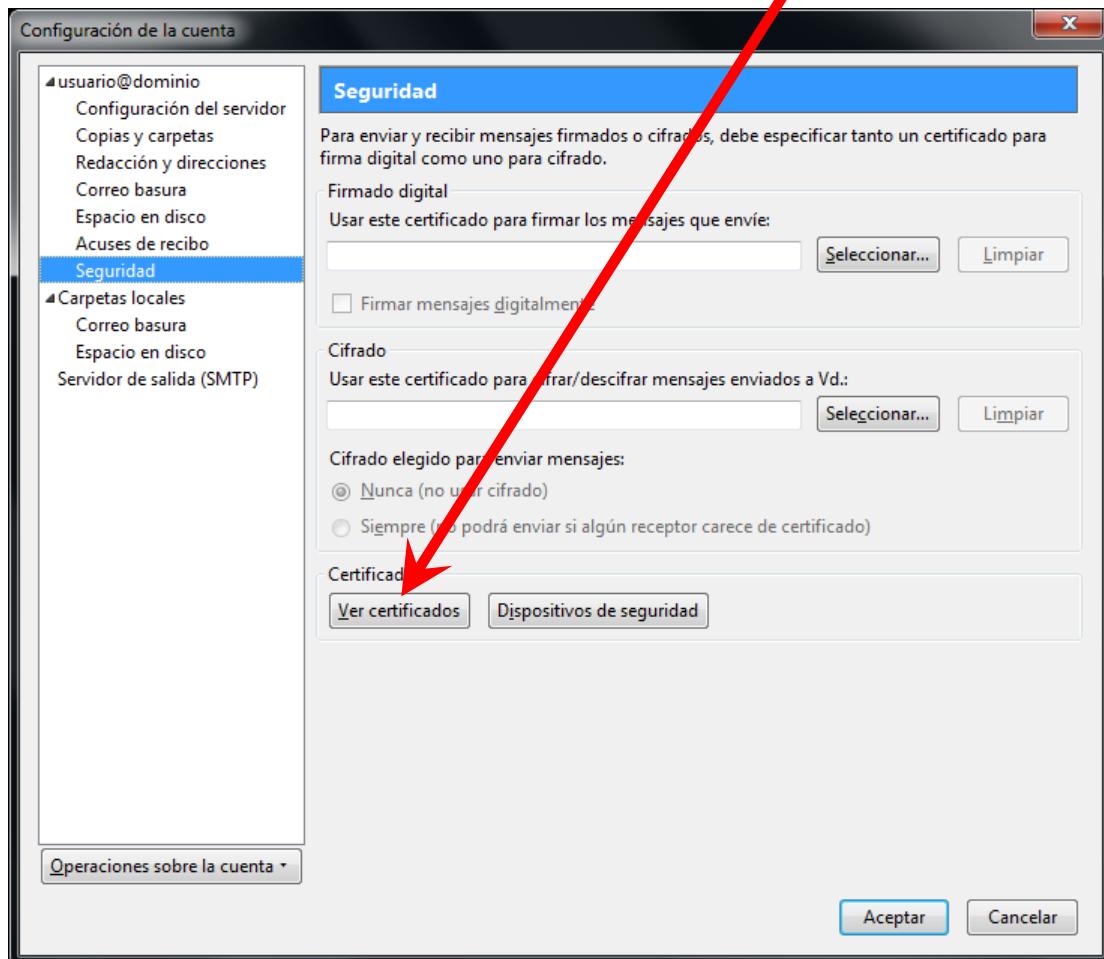




4.3 Mozilla Thunderbird

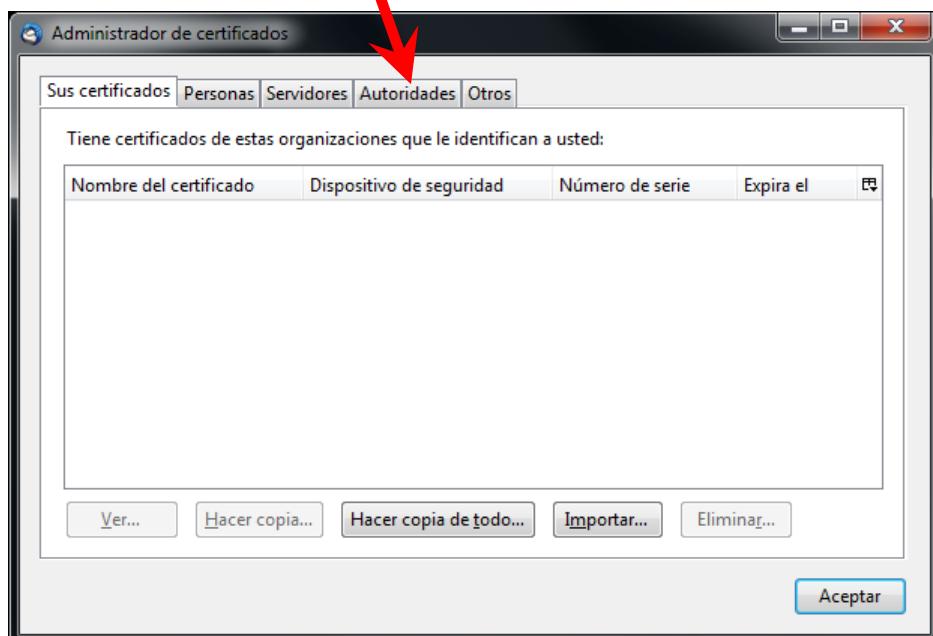
4.3.1 Importar los certificados de CA y modificar las configuraciones de confianza.

Abra la configuración de cuentas de Mozilla Thunderbird, y, para la configuración de la cuenta asociada al certificado, pulse el botón *Ver certificados*:

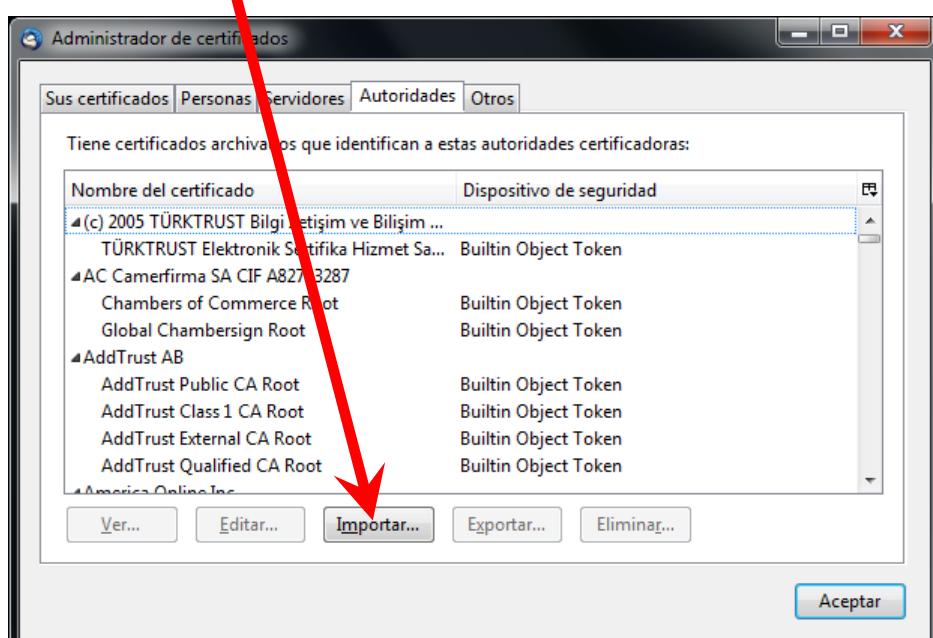




Seleccione la pestaña *Autoridades*:



Pulse el botón **Importar**:

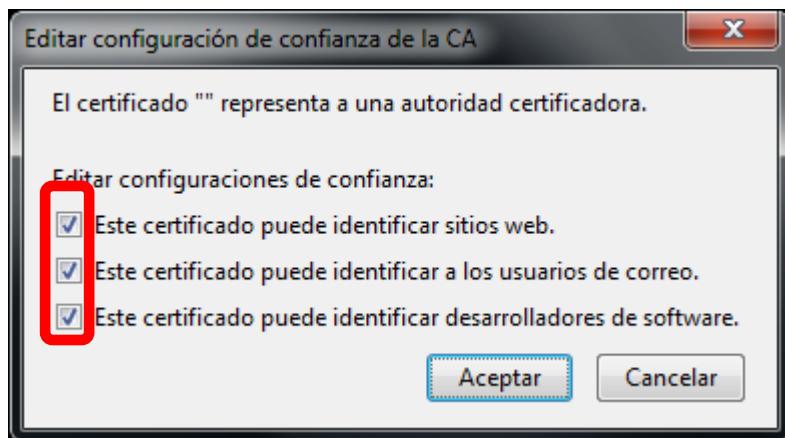




Descargue el certificado FNMT-Clase 2 desde aquí:

http://www.cert.fnmt.es/content/pages_std/certificados/FNMTClase2CA.cer

Seleccione el certificado ***FNMT Clase 2 CA*** y pulse ***Editar***: Marque las tres casillas y pulse ***Aceptar***:



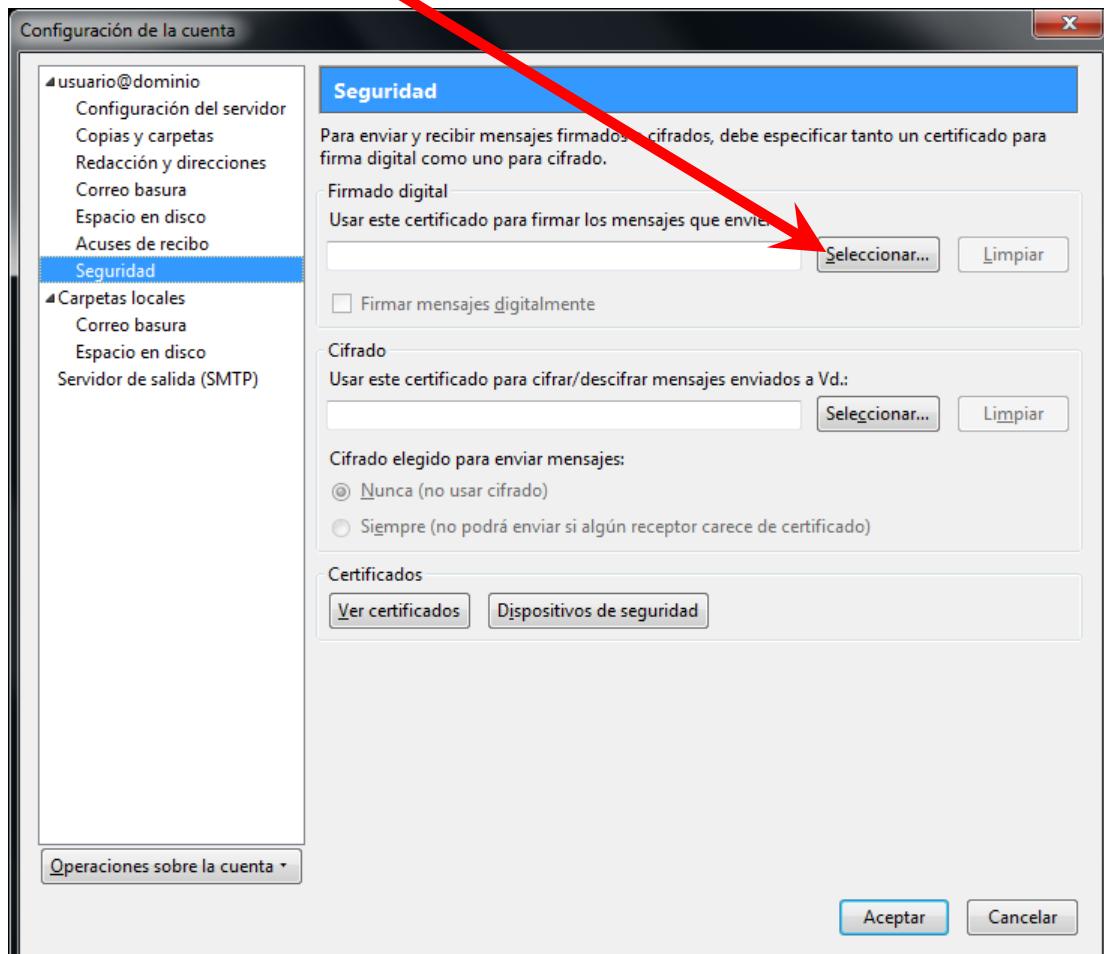
Pulse ***Aceptar*** para cerrar el administrador de certificados.



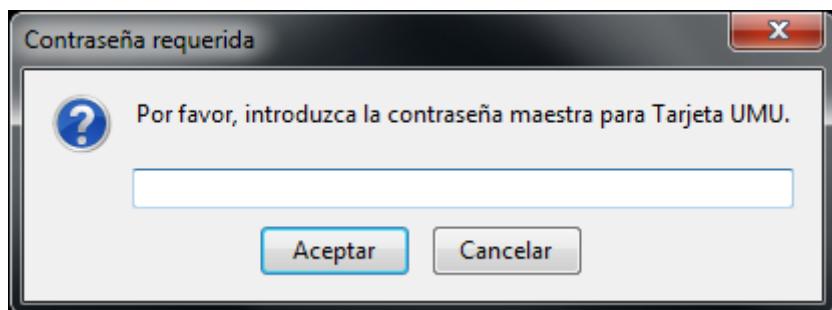


4.3.2 Seleccionar el certificado para firmar los correos del usuario.

Pulse el botón *seleccionar*:



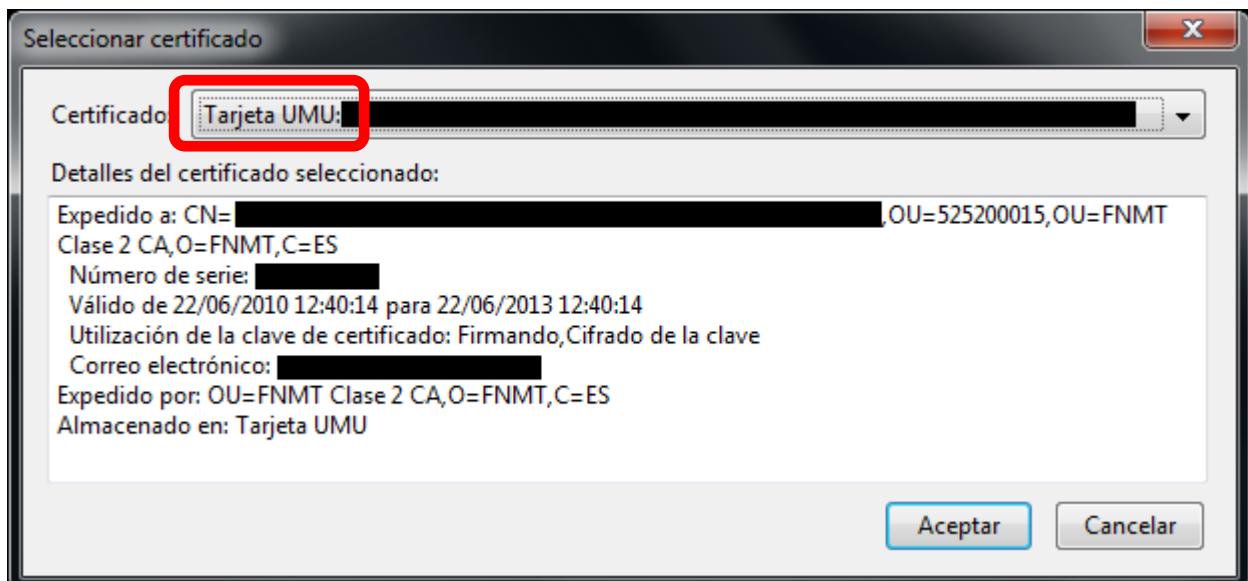
Si utiliza la tarjeta, puede que se le muestre la siguiente ventana que le solicita el PIN:



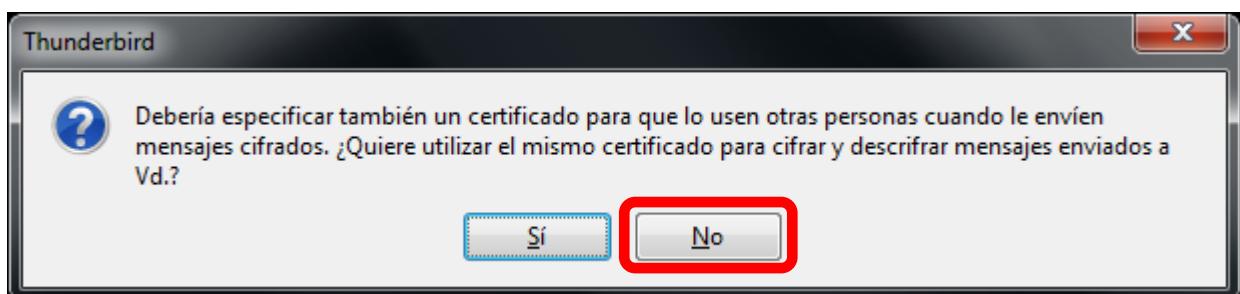


A continuación, debería aparecer una ventana con todos los certificados disponibles para firma. Si hace uso de la Tarjeta Universitaria Inteligente (TUI), el nombre del certificado estará precedido por “**TUI R7**” o “**GemP15-1**”.

Seleccione el certificado con el que firmar y pulse **Aceptar**:

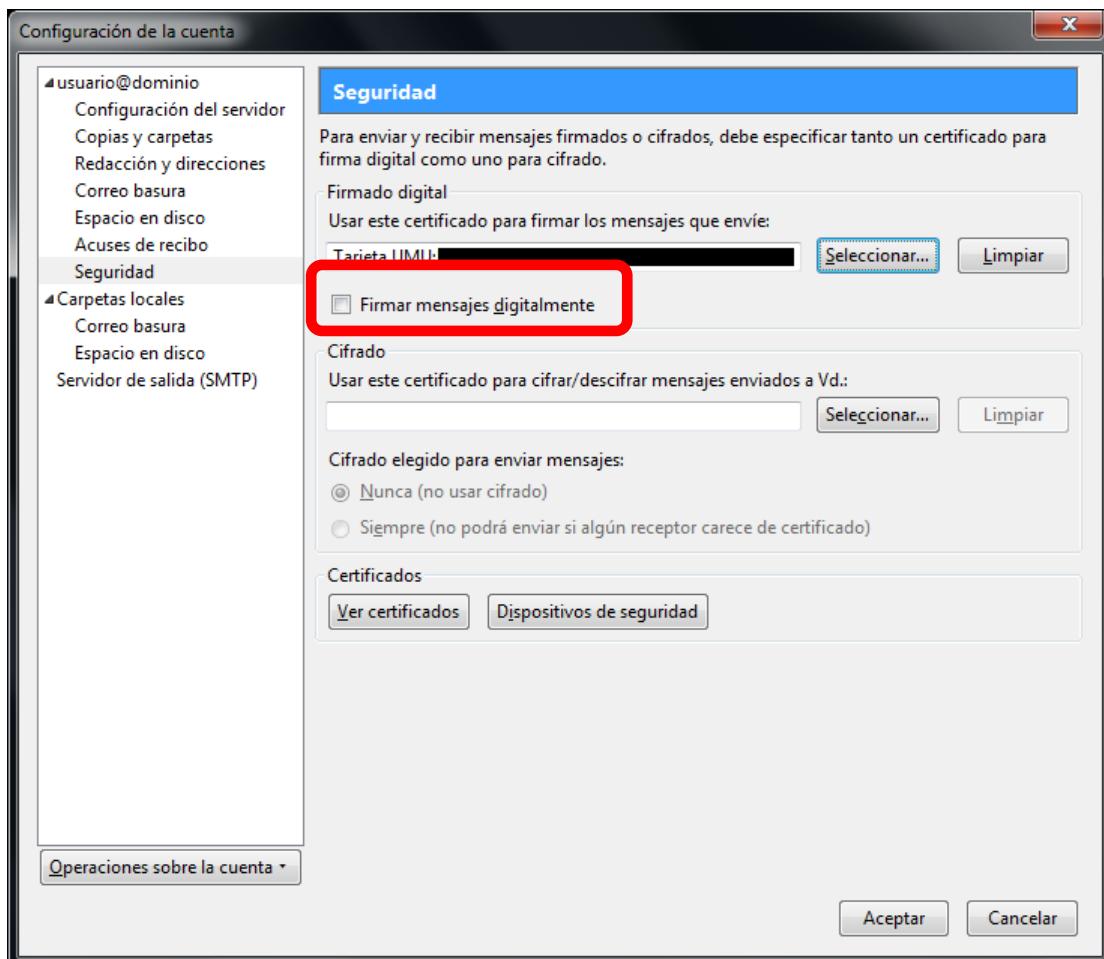


Se puede mostrar a continuación una ventana de diálogo solicitando un certificado para cifrar y descifrar. Actualmente no se soporta cifrado, así que deberá seleccionar **No**:





Puede además indicar que la firma de mensajes se haga de forma **predeterminada**, marcando si lo desea la casilla de *Firmar mensajes electrónicamente*:

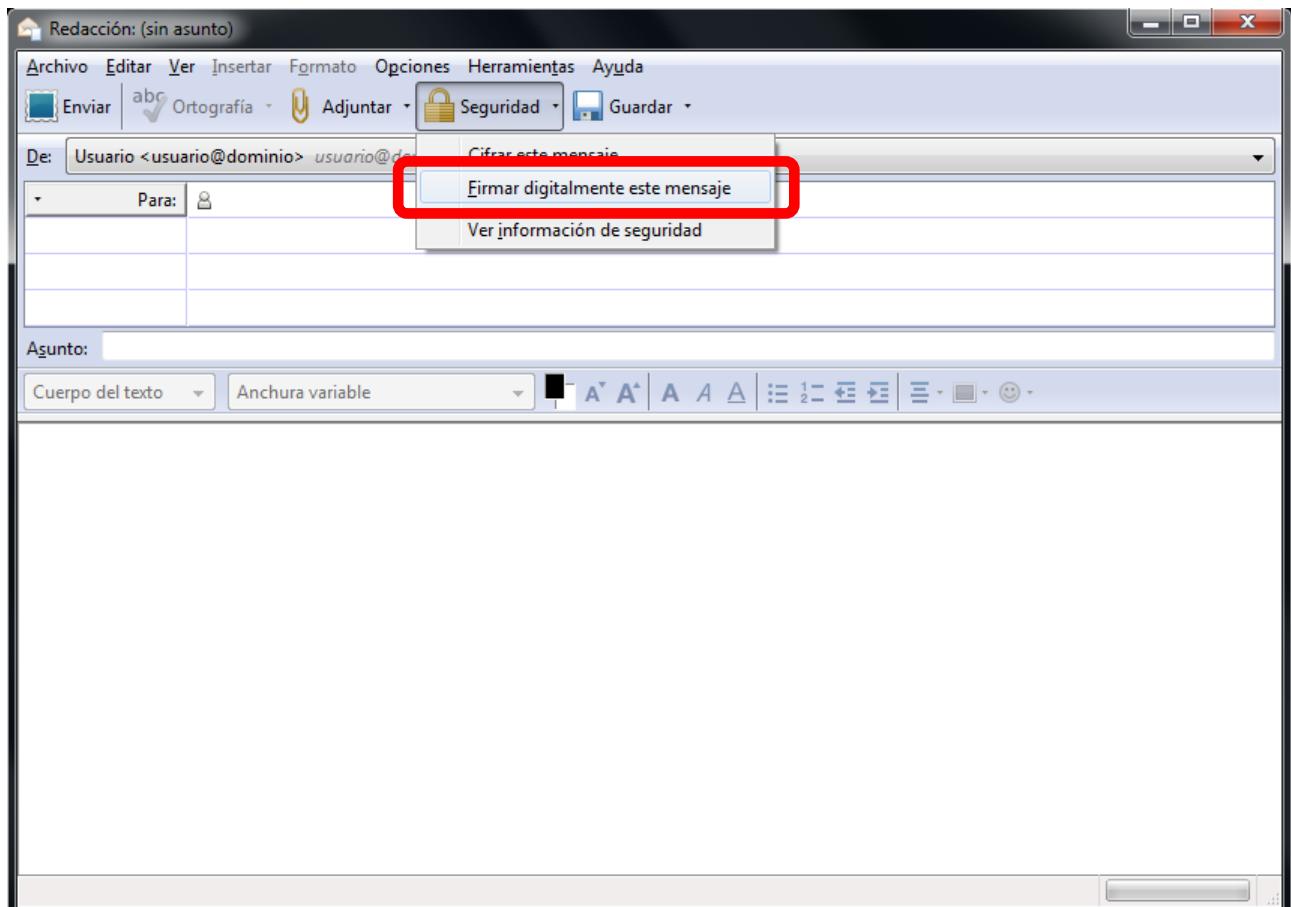


Pulse **Aceptar** para salir de la configuración de la cuenta.





Ya ha configurado la cuenta para firmar electrónicamente los correos con su certificado. Para seleccionar excepcionalmente si desea firmar o no, cuando escriba un correo puede seleccionar la opción que deseé en el menú *Seguridad*:





4.4 Apple Mail

Apple Mail hace uso del almacén de certificados del sistema de Mac OSX, conocido como *Keychain*.

Una vez se encuentre instalado el certificado en su equipo, Mail debería reconocer el mismo y posibilitar su uso sin necesidad de ninguna configuración especial. Para hacer esto, Mail busca y asocia certificados almacenados cuyo correo electrónico coincide con la cuenta de correo electrónico configurada.

Se ha encontrado un fallo por el cual, Mail solo asocia un certificado con la cuenta, cuando el correo electrónico está escrito *exactamente* en el formato en el que se encuentra en el certificado, **incluyendo mayúsculas y minúsculas**.

Para determinar cómo debe escribir la dirección de correo electrónico puede realizar los siguientes pasos:

Vaya a *Aplicaciones* -> *Utilidades* -> *Acceso a llaveros*. En la parte izquierda seleccione el llavero *Inicio de sesión*.

Seleccione el certificado deseado y pulse la opción *Obtener información* del menú secundario. Se le mostrarán los detalles del mismo. En esta lista de detalles busque el atributo *Nombre RFC 822*.

Algoritmo de firma SHA-1 con encriptación RSA (1 0 840 103049 0 0 5)
Parámetros ninguno
No válido antes de miércoles 24 de febrero de 2010 06:41:24 p.m. España (Madrid)
No válido después de domingo 24 de febrero de 2013 06:41:24 p.m. España (Madrid)

Información de la clave pública
Algoritmo Encriptación RSA (1 0 040 100549 1 0 1)
Parámetros ninguno
Clave pública 128 bytes: 00 A8 00 00 A8 A8 2F ... ⓘ
Exponente 65537
Tamaño de la clave 1024 bits
Uso de la clave Verificar, Ajustar
Firma 128 bytes: 00 4D 00 00 1A 1A 00 81 ... ⓘ

Extensión Uso de la clave (2 0 29 10)
Crítico NO
Uso Firma digital, Encriptación de la clave

Extensión Restricciones básicas (0 5 09 10)
Crítico NO

Autoridad de certificación NO

Extensión Identificador de clave del sujeto (0 5 20 14)
Crítico NO
Nombre de la clave 2E AF 00 00 C2 4E 00 DC 22 1F 00 FF EB AD 00 58 00 72 AB 00

Extensión Identificador de clave de entidad emisora (0 5 09 30)
Crítico NO
Nombre de la clave 00 9A 76 00 97 74 07 C4 AC 00 CB 00 8D 00 3A 45 7C 00 D7 00

Extensión Nombre alternativo del sujeto (2 0 00 07)
Crítico NO
Nombre RFC 822 USUARIO@DOMINIO.COM

EXACTAMENTE ESE TEXTO Y EN ESE FORMATO deberá ser el que utilice para la dirección de Correo en Apple Mail.



Para determinar si firmar un correo, active o desactive la casilla que aparece encima del cuerpo del mensaje.

