MANUAL

CONFIGURACIÓN CORRECTA PARA USO DE LA FIRMA DIGITAL

Versión 3.0.
Última modificación: 27/09/2016

Índice

Introducción

Para acceder a la mayoría de los servicios o procedimientos disponibles en sedes electrónicas en general, y a las de la Universidad de Granada en particular (en https://sede.ugr.es) son necesarios una serie de requisitos técnicos para permitir la identificación segura del usuario y la firma de documentos en su nombre.

El principal de esos requisitos es disponer instalado en el ordenador a utilizar un certificado digital válido que le identifique como persona o representante.

El objetivo de este manual es conocer con suficiente nivel de detalle los requisitos y recomendaciones de configuración y ayudarle a resolver las dudas y problemas que le impidan completar los trámites de su interés.

Para todo ello, se tratarán los siguientes bloques:

- El programa Autofirma
- Consideraciones previas respecto a los navegadores web
- Certificado digital
- Errores frecuentes
- Configuración de Java (opcional)

Aclaración: durante este manual se usará indistintamente el término firma digital o certificado digital por simplificar aunque técnicamente no son lo mismo.

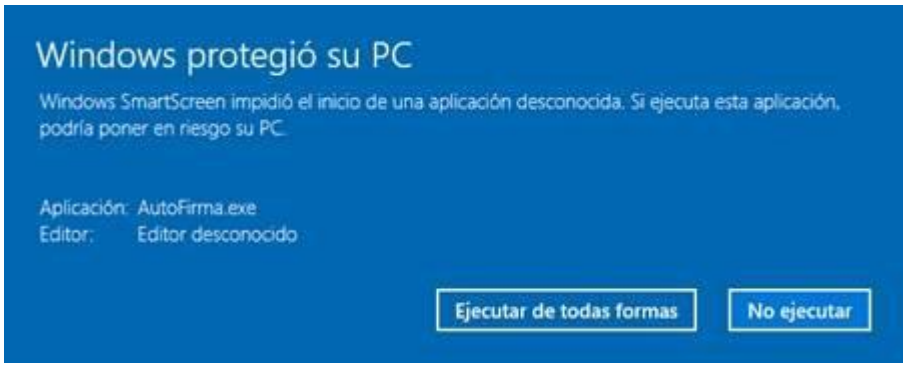
El programa Autofirma

Autofirma es una aplicación de firma realizada por el Ministerio de Hacienda y Administraciones Públicas. Su principal objetivo es ofrecer al usuario un sistema de firma de cualquier tipo de documento de manera sencilla.

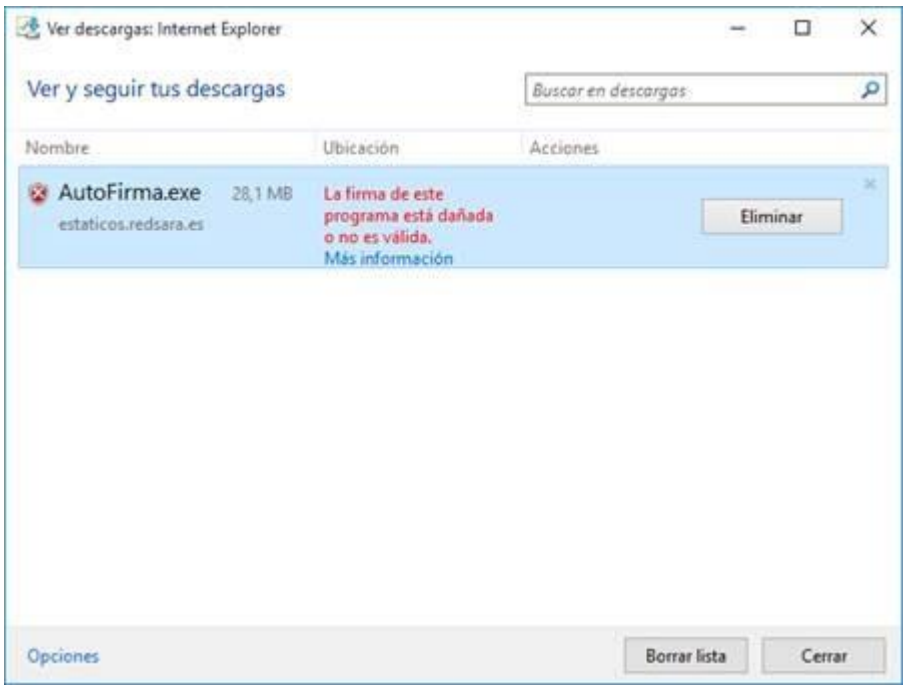
En la página de requisitos técnicos de la Sede Electrónica (https://sede.ugr.es/sede/requisitos-tecnicos/index.html) existe tanto un enlace al **manual de instalación detallado** como a la **descarga del propio programa en sí**. Es importante que el sistema operativo que se utilice esté lo más actualizado posible.

Instalación

Autofirma viene en forma de ejecutable instalable. Descárguelo y pulse el botón derecho del ratón sobre el icono del programa descargado, seleccionando la opción de **Ejecutar como administrador**. Esta forma de instalación es especialmente importante en Windows 10, ya que si intenta instalarlo haciendo doble clic en el programa instalado, Autofirma no se instalará ni siquiera indicando que continúe con la ejecución.



Asimismo, en la descarga el navegador Internet Explorer puede dar el aviso de que la firma del programa está dañada o no es válida. Ignore este aviso; la aplicación es 100% confiable.



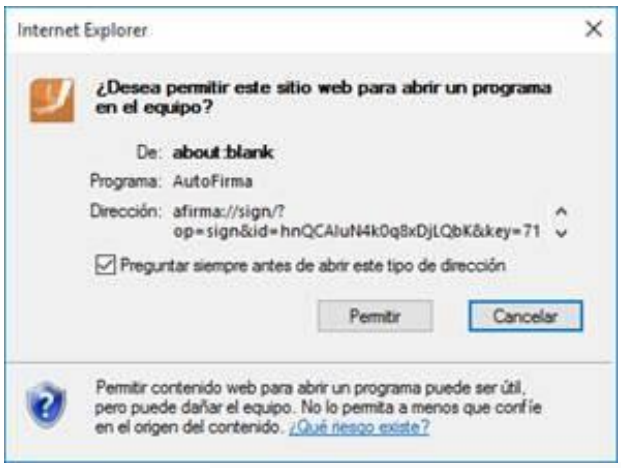
El método más simple para evitarlo es descargar a instalar con otro navegador. Si quiere seguir utilizando Internet Explorer, ejecute el navegador Internet Explorer como administrador. (Para ello acceda al disco local C:/, "Archivos de programa" o "Archivos de programa (x86)", "Internet Explorer" y sobre el archivo "iexplorer.exe", haga clic con el botón derecho del ratón y seleccione la opción "Ejecutar como administrador". Acceda a la web, descargue el fichero y ejecútelo como administrador).

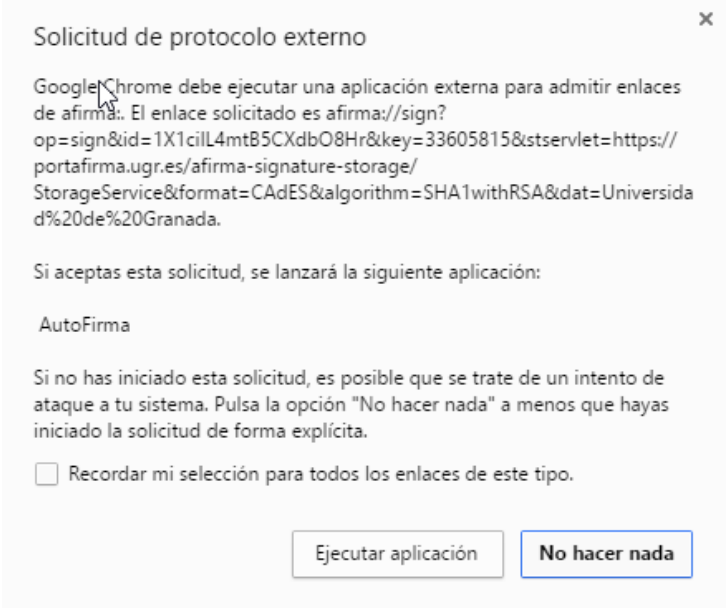
En caso de dudas sobre como completar la instalación, consulte el manual completo mencionado más arriba.

Uso

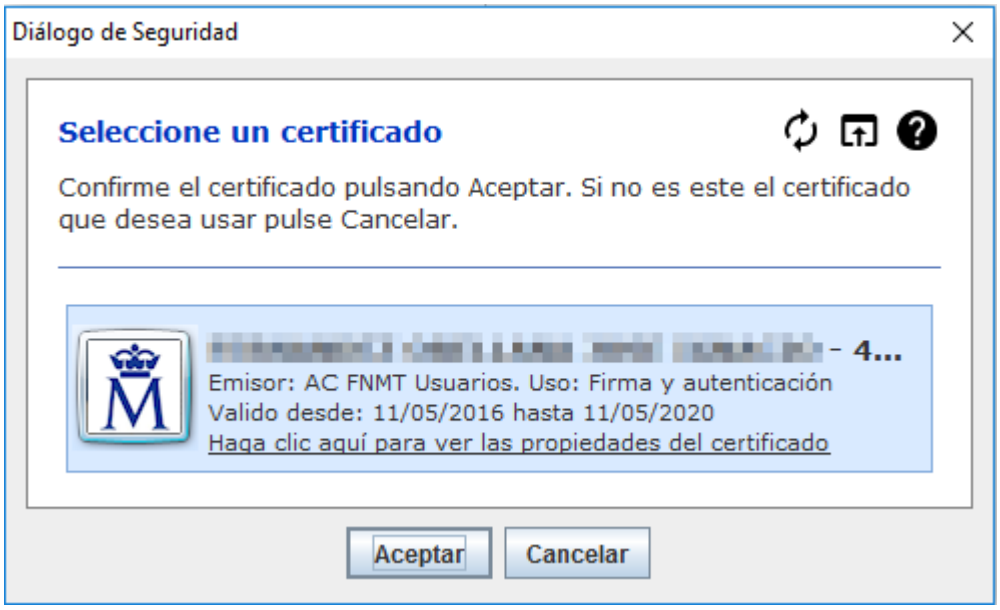
El uso del programa es automático, **no requiere intervención del usuario para iniciarse**, sino que será llamado por el navegador web que esté utilizando para acceder a la firma electrónica.

Al iniciar el proceso se mostrarán unos mensajes como los siguientes (en función de si utiliza, por este orden, Internet Explorer, Mozilla Firefox o Google Chrome), solicitando la ejecución a un programa externo a su navegador, **permita o acepte la ejecución**.



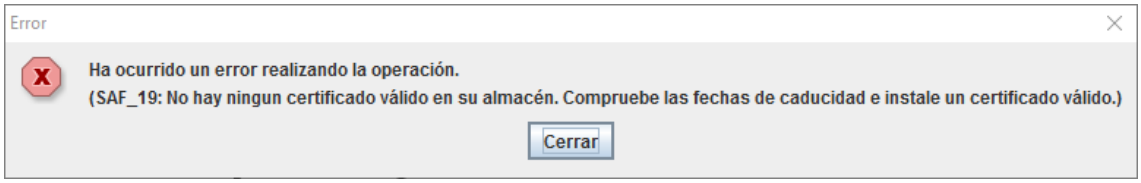


Al acceder a un procedimiento electrónico o realizar una firma, aparecerá una ventana similar a esta para elegir un certificado entre los certificados instalados en el sistema (consultar el apartado "Certificado digital" para conocer cuáles son válidos):



Tan sólo habría que elegir el certificado y aceptar.

En caso de que no aparezca ningún certificado a elegir, no dispone de un certificado válido instalado y aparecerá un mensaje de error similar al siguiente:



Este mensaje significa que el certificado incumple alguno de los requisitos necesarios o el sistema no puede localizarlo. Consulte la sección "Certificado digital" de este documento para diagnosticar y solucionar el problema.

Consideraciones previas respecto a los navegadores web

Certificados digitales

Existe una diferencia fundamental entre los navegadores web respecto a los certificados digitales:

- Google Chrome, Internet Explorer, Microsoft Edge y Safari utilizan los certificados digitales instalados en **el almacén de certificados general** del sistema operativo (bien sea Windows, Mac OS o Linux).
- Mozilla Firefox utiliza los certificados digitales instalados **dentro del propio Firefox.**

Java

Existe la siguiente diferencia entre navegadores web respecto al uso del plug-in Java de certificados digitales:

- Google Chrome y Microsoft Edge **no permiten** la ejecución de Java.
- Internet Explorer, Mozilla Firefox y Safari **permiten** la ejecución de Java, requiriendo la configuración necesaria asociada.

¿Es Java necesario?

Java **NO es necesario** para realizar el uso de la firma digital si se utiliza el programa **Autofirma**, que simplifica todo el proceso de acceso y firma con certificado digital.

En el caso de no utilizar el programa Autofirma, Java es necesario. No es recomendado ya que requiere configuración adicional para poder realizar la firma. (Ver apartado "Configuración de Java").

¿Qué navegador es el recomendado?

Dentro de lo posible, por el momento **Google Chrome** es el navegador recomendado ya que combinado con el programa **Autofirma** reduce los problemas en el proceso de instalación y firma.

Certificado digital

Es requisito imprescindible para poder realizar un procedimiento electrónico en la Sede Electrónica de la Universidad de Granada disponer de un certificado digital adecuado que le identifique.

Requisitos que debe cumplir un certificado digital para su uso en la sede

- Que haya sido **emitido por una entidad certificadora aceptada** por la UGR, como por ejemplo el Certificado de Persona Física, de Representante (empresas) o de Empleado Público de la FNMT-RCM, Fábrica Nacional de Moneda y Timbre. Puede consultar la lista de las mismas en https://sede.ugr.es/sede/requisitos-tecnicos/index.html
- Que **su estado sea válido**, es decir, que se encuentre en su periodo de validez (no caducado) y no haya sido revocado (dado de baja por algún motivo).
- Que **incluya la clave privada** que permita utilizarlo para firmar (se trata de ficheros de certificados importables tipo .pfx o .p12, más información en próximos apartados).

Adicionalmente, para que la Sede Electrónica permita utilizar el certificado digital, no es suficiente con descargarlo, sino que será necesario **instalarlo adecuadamente** como se explica más adelante.

Obtención de un certificado digital

El proceso de obtención dependerá de la entidad certificadora elegida. El proceso de solicitud siempre está documentado en la página web de la entidad.

Se recomienda el mencionado FNMT-RCM, Fábrica Nacional de Moneda y Timbre, mediante la web https://www.sede.fnmt.gob.es/, donde la información de ayuda es especialmente completa y detallada.

Importante: el certificado **raíz** de la FNMT no es un certificado personal que le identifique como usuario y por tanto NO es válido, debe obtener un certificado personal.

Una vez realizado el proceso necesario para la obtención del certificado digital, que dependerá de la entidad certificadora utilizada, como resultado se obtendrá una de las siguientes posibilidades:

a) Un fichero descargado, en formato .pfx o .p12. (Para instalarlo puede seguir los pasos indicados en el apartado Instalación de un certificado desde una copia de seguridad)
b) El certificado instalado en el navegador donde se realizó el proceso.

Importante: al instalar un certificado digital en Windows, asegúrese de seleccionar la opción "Marcar la clave como exportable" para poder realizar la copia de seguridad de la misma.

Importante: si en algún momento tiene la opción de que se seleccione el almacén de certificados automáticamente, elija esa opción.

Copia de seguridad de un certificado

Es altamente recomendado crear una copia de seguridad de un certificado digital en el momento de conseguirlo. La forma de hacerlo dependerá del resultado del apartado anterior:

a) Si dispone del fichero .pfx o .p12, simplemente copie el fichero en un almacenamiento distinto (unidad externa como disco duro externo o pendrive usb, almacenamiento en la nube como Dropbox, Drive, Documenta, etc).
b) Si dispone del certificado instalado en el navegador, deberá exportarlo a un fichero y luego proceder como en el punto a (ver sección sobre exportar un certificado).

Localizar el certificado digital

Si el certificado no está en un fichero .pfx o .p12, como ya se ha comentado anteriormente existen dos lugares posibles donde localizar el certificado digital para exportarlo:

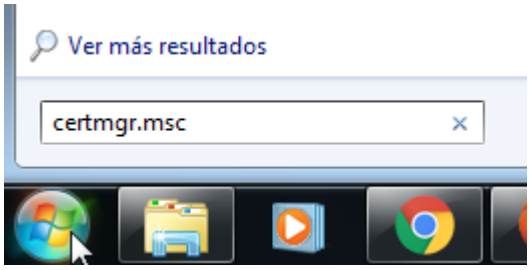
- Almacén de certificados del sistema operativo (Windows/MAC)
- Almacén de certificados propio de Firefox

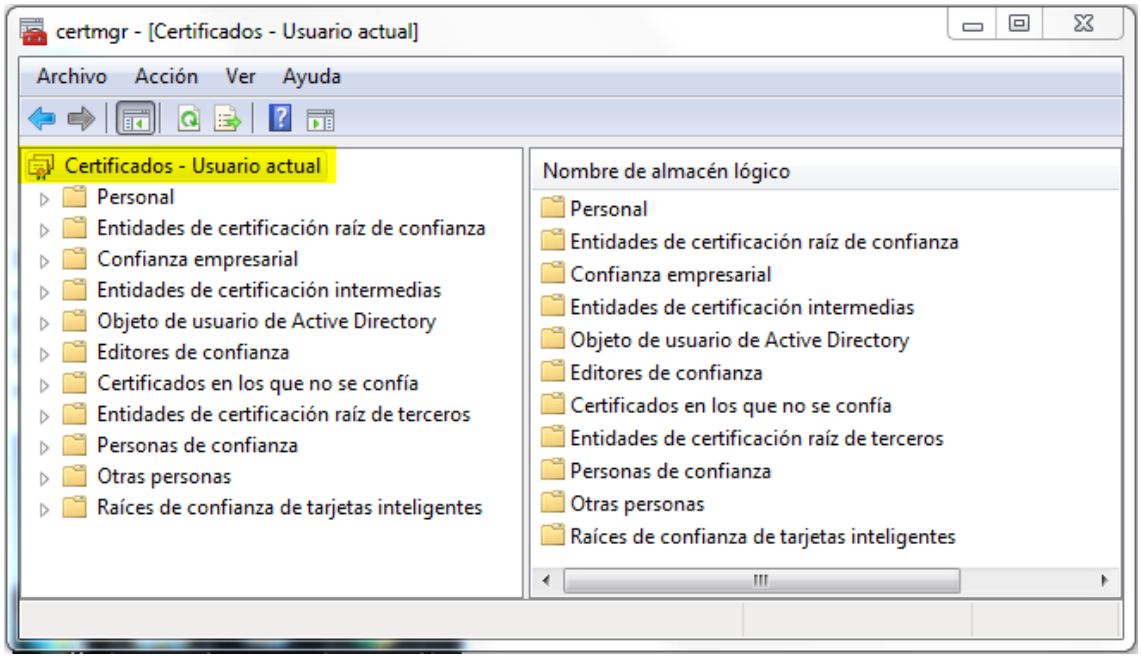
Nota: para los sistemas operativos de la familia Linux, es recomendable por su simplicidad acceder a los certificados a través del navegador web que se desee utilizar.

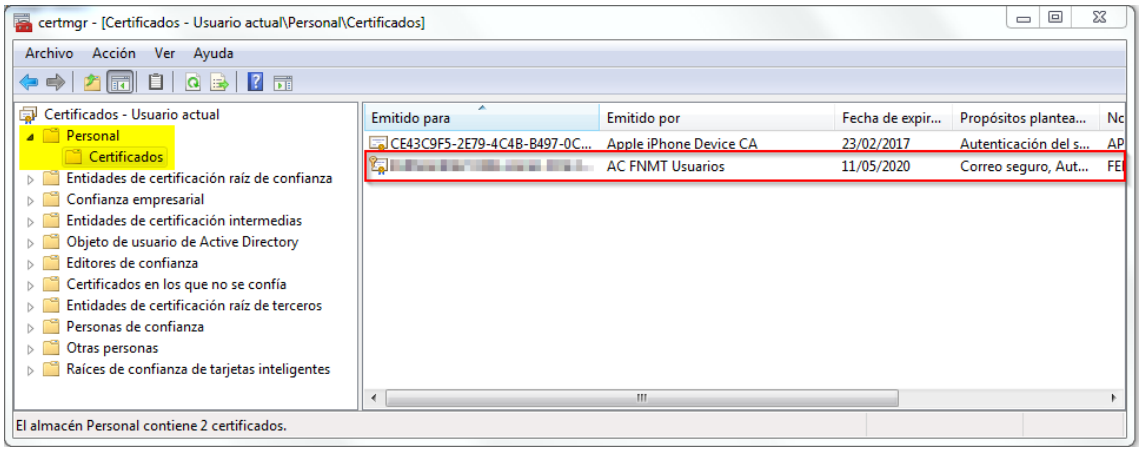
Almacén de certificados de Windows

Nota: Los certificados que se encuentran en este almacén también están accesibles desde la gestión de certificados de navegadores como Google Chrome (Menú de acciones > Configuración > Mostrar configuración avanzada… > HTTP/SSL > Administrar certificados…) o Microsoft Internet Explorer (Herramientas > Opciones de Internet > Contenido > Certificados).

Para localizar el certificado digital en el almacén de certificados de Windows, haga lo siguiente:
Botón de inicio > Abrir el administrador de certificados (Escribir en la casilla de búsqueda “certmgr.msc” y pulsar enter/intro) > Seleccionar “Certificados – Usuario actual” a la izquierda > Seleccionar “Personal” > Seleccionar “Certificados”





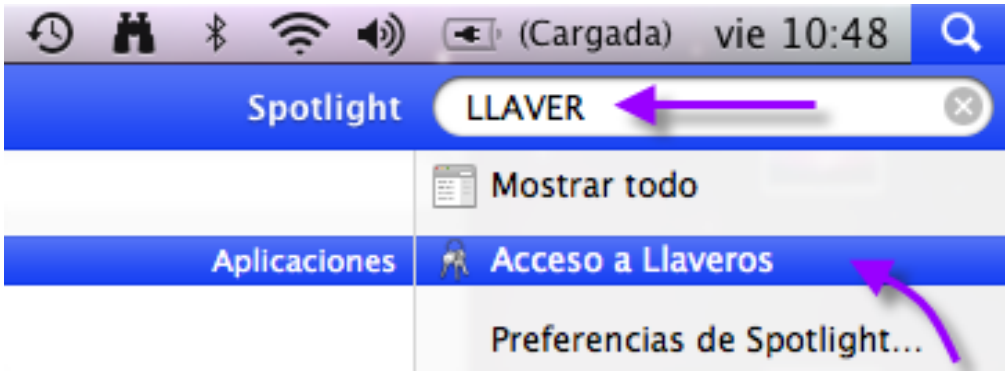


Si todo es correcto, debe disponer de al menos un certificado en esa sección "Personal", como el que se encuentra recuadrado en la captura. El icono tendrá una pequeña llave representada en su esquina superior izquierda, significando que **el certificado contiene una clave privada**. (Si el certificado no posee ese icono, es un certificado incompleto que no cumple los requisitos y no puede ser utilizado en la Sede Electrónica).

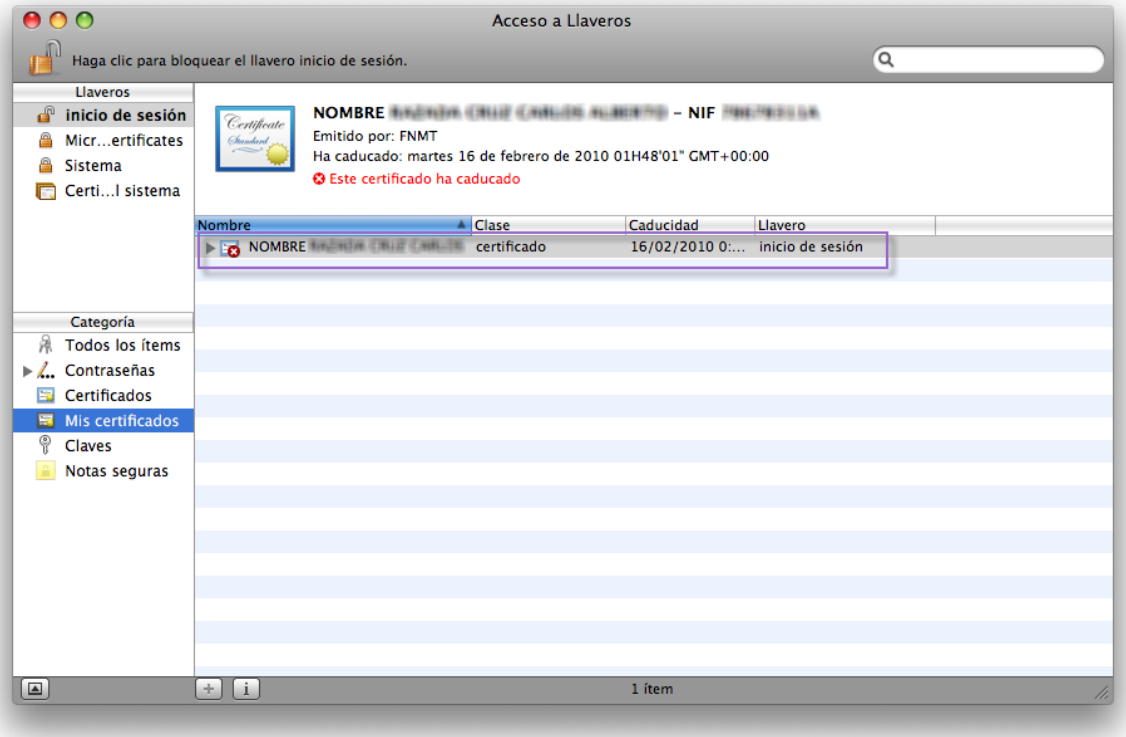
La columna "Emitido para" debe coincidir con su nombre, "Emitido por" debe tratarse de una entidad certificadora aceptada (como en este ejemplo la más usual, "AC FNMT Usuarios") y la "Fecha de expiración" no debe de haberse alcanzado.

Almacén de certificados de MAC (Acceso a llaveros)

1.- En la utilidad Spotlight de Mac OSX buscar la aplicación **Acceso a Llaveros** y pulsar en la misma.



2.- Pulsamos en la **Categoría Mis Certificados** para ver los certificados.

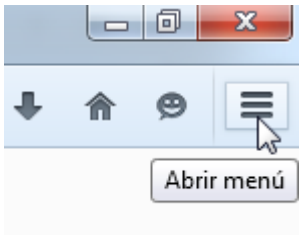


Al abrir el certificado, en el apartado “Confiar” hay que seleccionar la opción “Confiar siempre” en el primer elemento (“Al utilizar este certificado”):

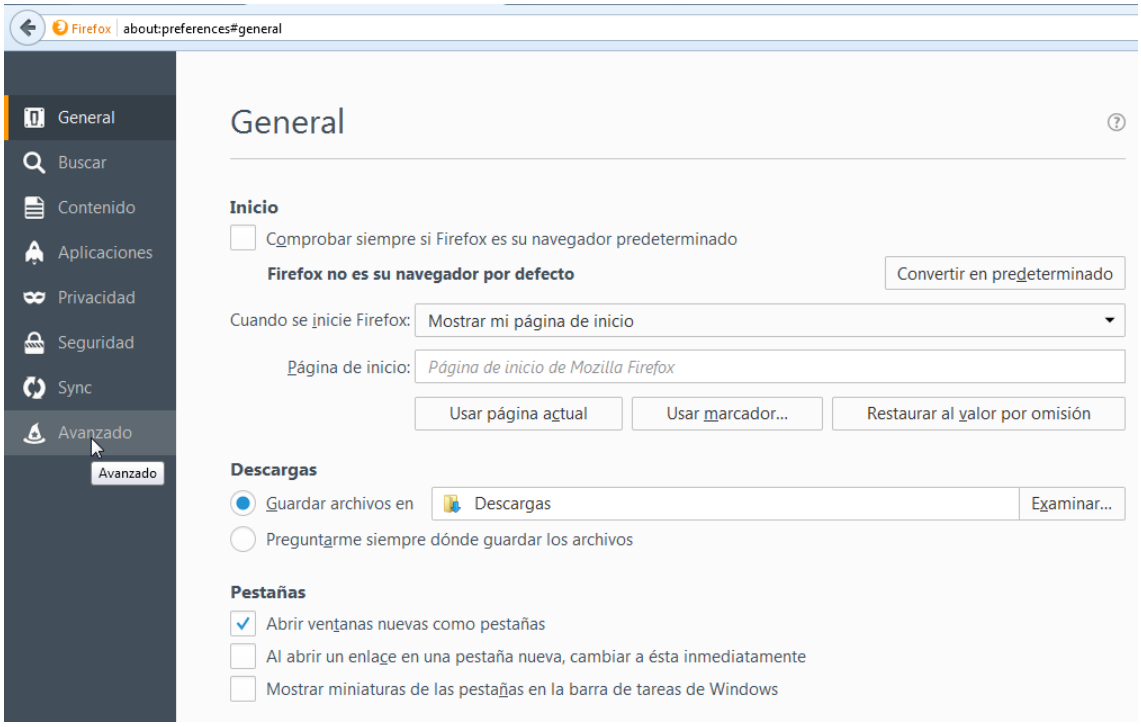
Almacén de certificados de Mozilla Firefox

Para localizar el certificado digital en el almacén de certificados de Mozilla Firefox, haga lo siguiente:

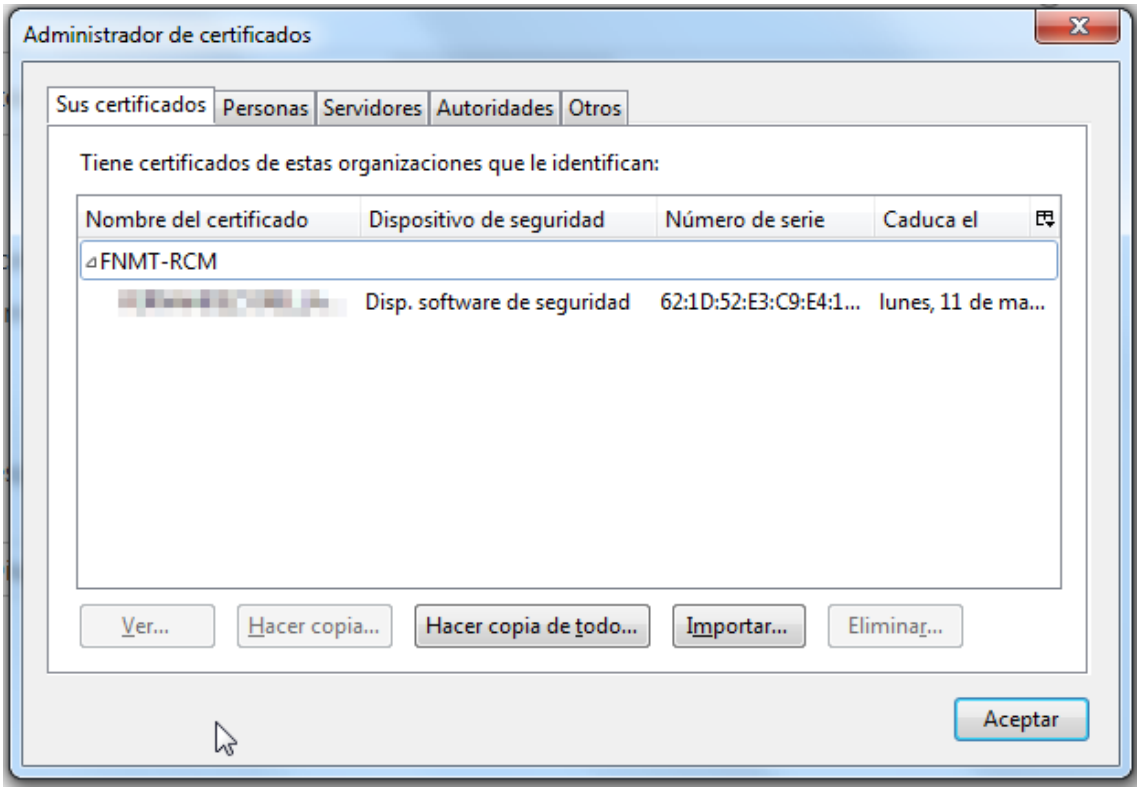
Botón “abrir menú” > Opciones > Avanzado > Botón “Ver certificados”


Abrir menú


Cortar
Copiar
Pegar
100%
Nueva ventana
Nueva ventana privada
Guardar página
Imprimir
Historial
Pantalla completa
Buscar
Opciones
Abrir opciones
Desarrollador
Conectarse a Sync
Personalizar


Firefox
about:preferences#general
General
Buscar
Contenido
Aplicaciones
Privacidad
Seguridad
Sync
Avanzado
Avanzado
General
Inicio
Comprobar siempre si Firefox es su navegador predeterminado
Firefox no es su navegador por defecto
Convertir en predeterminado
Cuando se inicie Firefox:
Mostrar mi página de inicio
Página de inicio:
Página de inicio de Mozilla Firefox
Usar página actual
Usar marcador...
Restaurar al valor por omisión
Descargas
Guardar archivos en
Descargas
Examinar...
Preguntarme siempre dónde guardar los archivos
Pestañas
Abrir ventanas nuevas como pestañas
Al abrir un enlace en una pestaña nueva, cambiar a ésta inmediatamente
Mostrar miniaturas de las pestañas en la barra de tareas de Windows


General
Buscar
Contenido
Aplicaciones
Privacidad
Seguridad
Sync
Avanzado
Avanzado
General
Elección de datos
Red
Actualizar
Certificados
Solicitudes
Cuando un servidor requiera mi certificado personal:
Seleccionar uno automáticamente
Preguntar siempre
Consultar a los servidores respondedores OCSP para confirmar la validez actual de
Ver certificados
Dispositivos de seguridad



En la pestaña “Sus certificados” debe de haber al menos un certificado a su nombre.

Exportación de un certificado digital

Es muy importante tener en cuenta que la exportación de un certificado digital debe siempre **incluir la clave privada**, por lo que en el proceso de exportación siempre debe marcar esa opción. Le pedirá una **contraseña** para añadir seguridad al proceso y que nadie que no conozca la clave pueda importar su certificado. **Importante:** Debe recordar dicha contraseña que le será requerida cada vez que quiera importar/instalar el certificado.

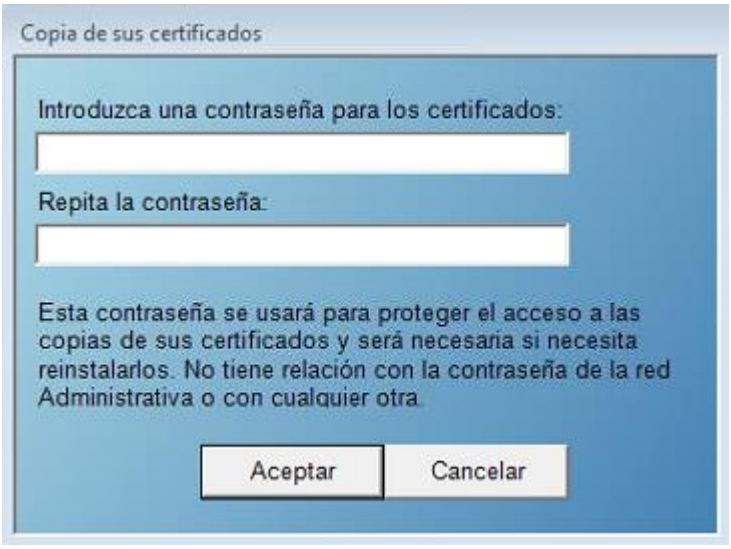
Desde el día 16/09/2016, además de la forma habitual de exportar certificados digitales, los ordenadores de la Red Administrativa disponen de una herramienta propia del CSIRC (método recomendado). A continuación se detallan ambas opciones:

Herramienta propia del CSIRC

Con objeto de facilitar las copias de seguridad de sus certificados (tanto personales como los relacionados con la gestión de UGR) y tenerlos ubicados en una carpeta fácilmente accesible (aunque perfectamente protegidos), se ha instalado un nuevo programa en la carpeta "Aplicaciones Universidad" llamado "Exportar mis certificados"

.

Al ejecutarlo saldrá una ventana solicitando una contraseña:



Dicha contraseña se usa para proteger las copias de los certificados y se le pedirá si desea instalar el certificado de nuevo. Esta contraseña no tiene por qué coincidir con ninguna otra ni tiene otro uso salvo el de proteger el acceso a las copias de sus certificados. Tras introducir la contraseña y repetirla, pulsaremos 

o la tecla [INTRO]. En ese momento, dependiendo de la configuración que eligiéramos en la instalación del certificado, nos puede salir una ventana como esta, para acceder al certificado y poder salvaguardarlo:

Si todo ha ido bien, el programa nos creará ficheros con el nombre del certificado y su fecha de caducidad y extensión .PFX en la carpeta L:\Misdocs\Certificados.backup. Recuerde la contraseña que ha elegido para sus copias, ya que la necesitará para

importarlos de nuevo.

Se recomienda ejecutar este programa cada vez que instale un nuevo certificado en su usuario.

Exportación sin la herramienta del CSIRC

El proceso de exportación en sí depende del navegador utilizado, suele ser muy simple una vez localizado el certificado y tenido en cuenta el párrafo anterior.

En función de dónde haya localizado el certificado:

- **Almacén de Windows**:
  Abra el certificado haciendo doble click sobre él.
  En la pestaña "Detalles", pulse el botón "Copiar en archivo…".
  Ejecute el asistente, **marcando la opción de "Exportar clave privada"** (deberá introducir una contraseña para proteger el archivo generado).
  Importante: Si esa opción no ha sido marcada, el certificado exportado tendrá extensión .crt o .cert en lugar de .pfx o .p12 y **será incompleto**, no siendo válido para su uso en la Sede Electrónica.
- **Almacén de Mozilla Firefox**:
  Seleccione la línea que representa el certificado y pulse el botón "Hacer copia…".
  Seleccione una ruta de destino e introduzca un nombre para el fichero resultante (tendrá extensión .p12) y pulse "Guardar".
  Introduzca y confirme una contraseña para proteger el certificado exportado, y pulse "Aceptar".
- **MAC**:
  Abra la utilidad de llaveros, para ello pulse en Ir / Utilidades / Acceso a llaveros.
  Pulse en Mis Certificados y seleccione el certificado que desea exportar.
  Pulse en Archivo - exportar elementos.
  Elija un nombre de archivo y elija la ruta donde se guardará.
  Introduzca su password y confírmela. Pulse OK.
  Su certificado será guardado con extensión .p12.

Nota: Para los sistemas operativos de la familia Linux se recomienda por simplicidad acceder a los certificados y actuar sobre ellos mediante el navegador web utilizado.

Instalación de un certificado desde una copia de seguridad

En función del lugar a instalar:

- **Almacén de Windows**:
  Busque el fichero .p12 o .pfx de copia de seguridad del certificado.

Haga doble click sobre él para abrir el "Asistente para la importación de certificados".
Escriba una contraseña para proteger la clave privada.
Importante: marque la segunda casilla de verificación "Marcar esta clave como exportable".
Complete el asistente.

- **Llavero de MAC**:
  Abra la utilidad de llaveros, para ello pulse en Ir / Utilidades / Acceso a llaveros.
  Pulse en Archivo - Importar elementos.
  Seleccione el archivo de su copia de seguridad (.pfx o .p12) y pulse Abrir.
  Introduzca la contraseña y pulse OK.
- **Almacén de Mozilla Firefox (sólo necesario si NO se utiliza Autofirma)**:
  En el "Administrador de certificados" donde se localizan los certificados, pulse el botón "Importar…".
  Seleccione el fichero .pfx o .p12 a importar.
  Introduzca la contraseña con la que protegió el fichero.
  Complete el asistente.

Si el fichero del certificado que quiere instalar tiene extensión **.crt o .cert** en lugar de .pfx o .p12, es un **certificado sin clave privada, no válido** para su uso en la Sede Electrónica. Deberá volver a exportarlo marcando la opción de "Exportar clave privada" o en el peor caso volver a realizar el proceso completo de solicitud de un nuevo certificado válido.

Más información sobre certificados digitales

Consulte https://www.sede.fnmt.gob.es/preguntas-frecuentes

Errores frecuentes

En esta sección encontrará una enumeración somera de errores frecuentes con indicaciones simples para ayudar a solucionarlos.

Problema	Sugerencia
La comprobación de requisitos técnicos muestra un error en la versión de Java y he decidido no continuar el proceso por precaución.	El aviso no implica necesariamente que no se pueda completar el proceso, pruebe a realizarlo en cualquier caso. Si su navegador es Chrome o Edge y tiene instalado Autofirma, es seguro ignorar los posibles avisos sobre Java y proceder a realizar el trámite. Si su navegador es Firefox, consulte la sección sobre Configuración de Java.
Me aparece un error del certificado digital al intentar completar un procedimiento. Al comprobar el certificado, es correcto, aunque aparece en la pestaña "Otras personas"/"Otros" en vez de en "Personal"/"Sus certificados".	El certificado instalado es incompleto, no tiene la clave privada y es insuficiente para completar los trámites. Reinstale el certificado digital desde el fichero .p12 o .pfx original o exportándolo de donde lo tenga correctamente instalado (marcando la opción de exportar incluyendo la clave privada). (Ver apartado Certificado digital)
Al ir a completar un procedimiento o firmar, la página se queda cargando sin terminar.	Compruebe que no se ha abierto una ventana emergente aparte para autorizar la ejecución de la aplicación Autofirma o elegir el certificado a utilizar (que puedan haber quedado ocultas tras alguna otra). Vaya ocultando las ventanas una a una para comprobarlo.
Al intentar instalar el programa Autofirma en mi ordenador de la Red Administrativa, me indica que no tengo permisos suficientes para instalarlo.	El programa Autofirma está instalado de inicio en los ordenadores de la Red Administrativa. Si el programa no funciona, contacte con el departamento de Microinformática.
El navegador me da un mensaje de que "La conexión no es privada" al acceder a una página de la Oficina Virtual o la Sede Electrónica.	Si la dirección de la página a la que va a acceder comienza por https y contiene .ugr.es, confíe en dicha página para acceder, la página es segura.
Utilizando el navegador Mozilla Firefox no	Determinadas versiones de dicho

consigo adjuntar un documento requerido para un procedimiento.	navegador no envían correctamente el fichero a nuestros servidores y aún no disponemos de solución. Por favor utilice un navegador alternativo para realizar el procedimiento o la versión más actualizada de Firefox.
Utilizando el navegador Mozilla Firefox, no me reconoce un documento pdf como tal aunque puedo abrirlo sin problemas con un programa lector de pdfs.	Determinadas versiones de dicho navegador muestran este problema. Por favor utilice un navegador alternativo para realizar el procedimiento o la versión más actualizada de Firefox.
Al entrar en un procedimiento lo puedo hacer sin problema seleccionando mi certificado digital y aparecen mis datos cargados, pero al ir a continuar o firmar me da un error.	El mensaje de error debería proporcionarle información suficiente para resolver el problema por la vía adecuada, en ocasiones a través de su centro (que no esté correctamente dado de alta en los sistemas de la UGR, por ejemplo). Si el mensaje es insuficiente o no hay mensaje, contacte con la Administración Electrónica indicando el procedimiento que intentaba completar, su DNI y el error que le aparece cuando exista.

Configuración de Java

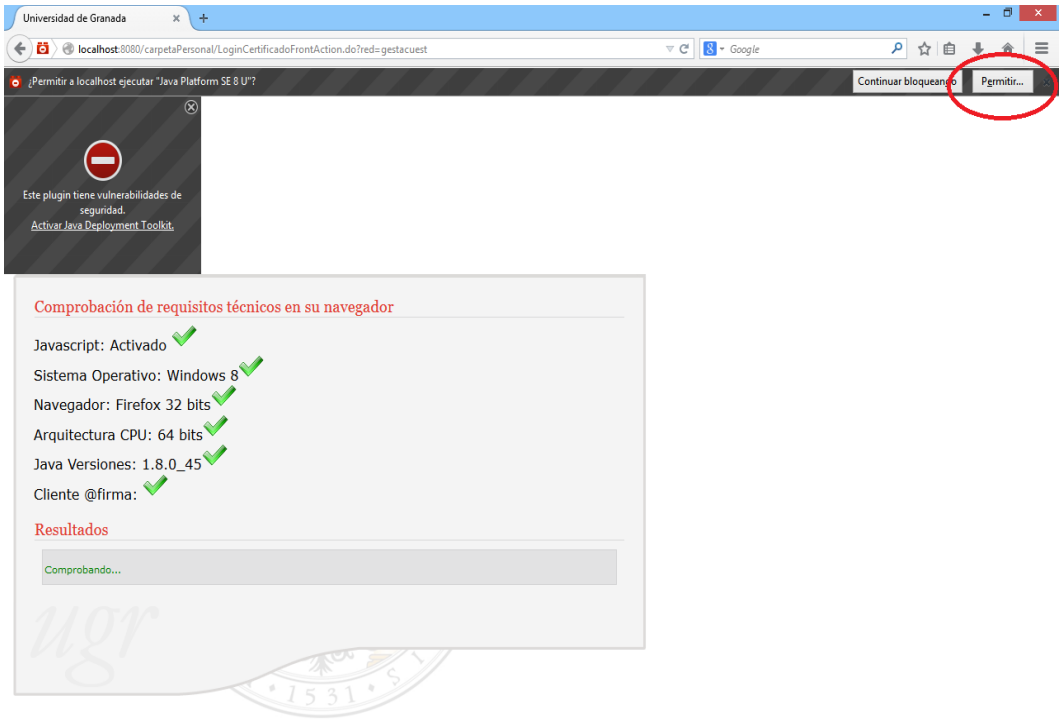
En el caso de que **no utilice la configuración recomendada** con el programa Autofirma, para el uso correcto del certificado digital necesitará la siguiente configuración adicional de los componentes o plug-in Java de firma.

Versión de Java

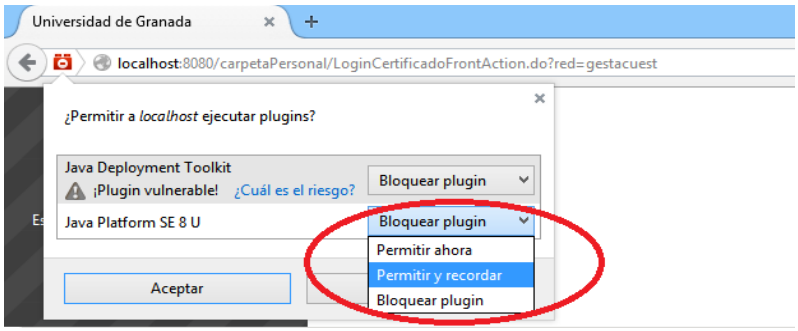
Siempre es recomendable tener la última versión de Java instalada en su sistema. Para ello acceda a la página web http://java.com y diríjase a la sección o enlace "¿Tengo Java"? donde se realizará una comprobación del estado de Java en su sistema: si está activo (si no, siga los pasos siguientes) y si es la versión recomendada.
Si la versión no es la recomendada, siga los pasos indicados en dicha web para actualizarla.

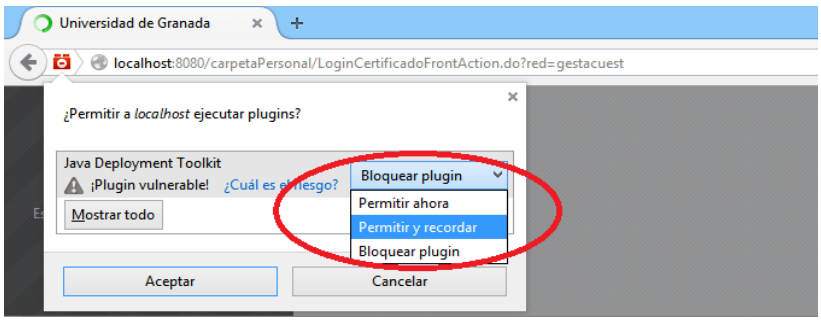
Permisos de ejecución de Java

Por defecto, los navegadores que permiten usar Java bloquean su uso por motivos de seguridad, con un mensaje como el siguiente:



Para continuar haga click en Permitir... y aparecerá un cuadro de diálogo en la parte izquierda del navegador con dos advertencias de bloqueo de dos plugin de Java, para desbloquearlo haga click en el desplegable donde pone Bloquear plugin y después seleccione la opción Permitir y recordar y pulse Aceptar. (Repita el proceso para ambos plugins).

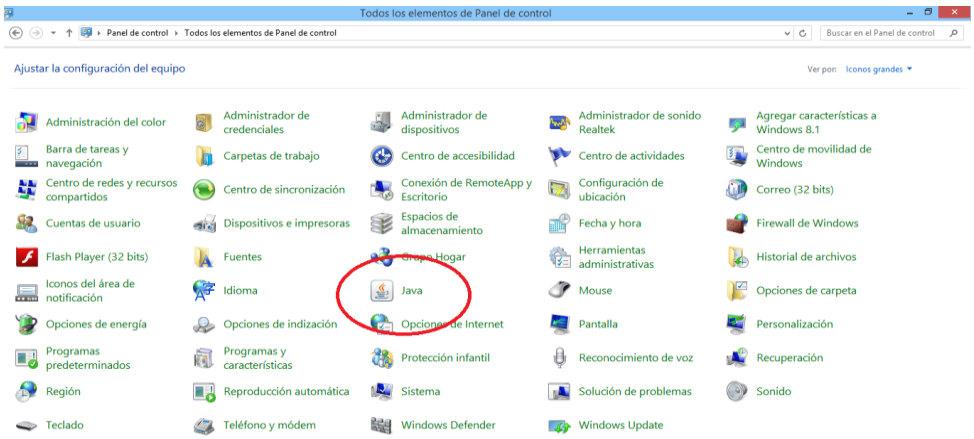




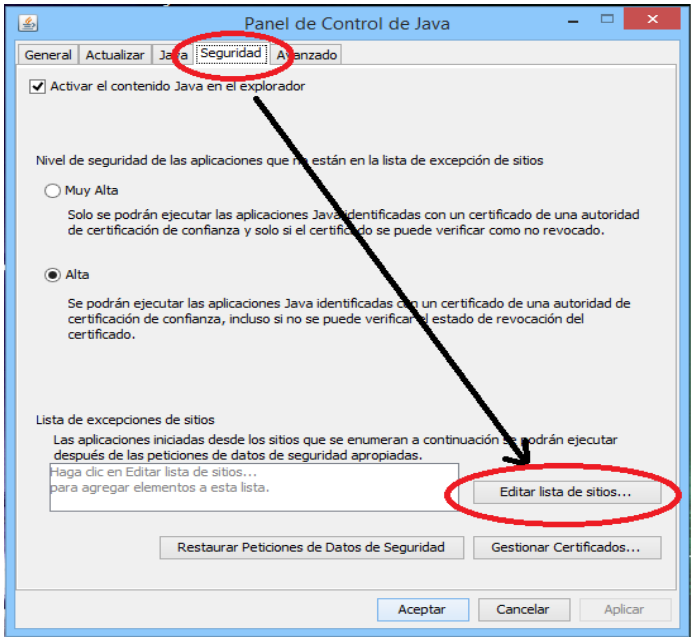
Sede Electrónica como sitio seguro

El componente Java debe además configurarse para confiar en la Sede Electrónica. Para agregar a la sede electrónica en la lista de sitios de seguros siga los siguientes pasos:

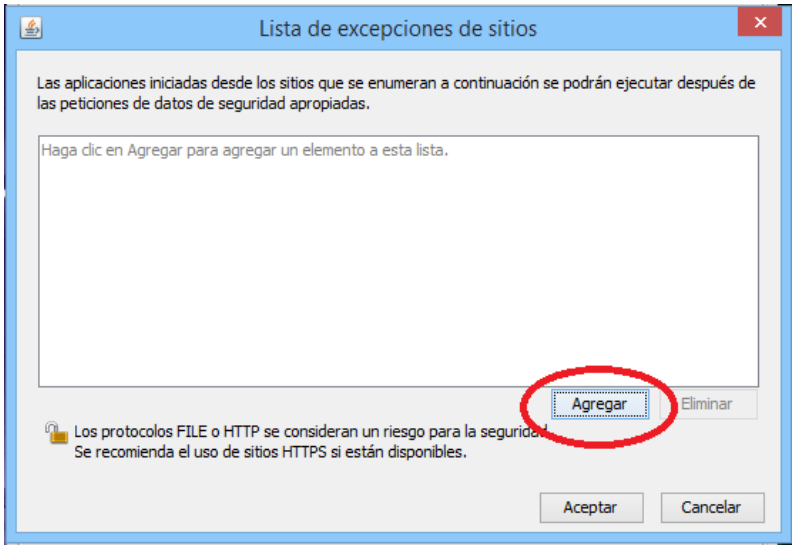
Diríjase a Inicio → Panel de Control → Java y aparecerá el Panel de Control de Java.

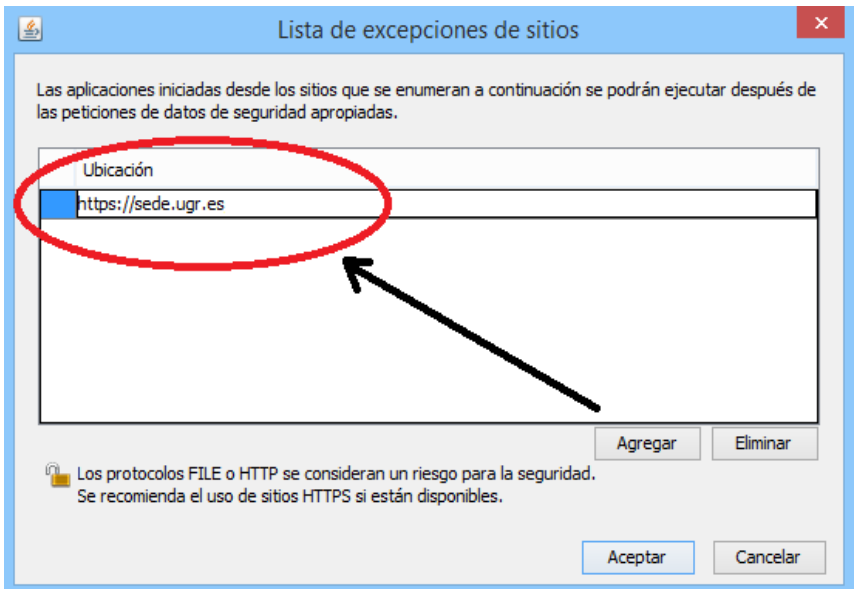


Una vez ahí vaya a la pestaña Seguridad y después abajo a la derecha haga click en Editar lista de sitios… y aparecerá una nueva ventana con el listado de excepciones de sitios.



Después haga click en Agregar y teclee en el recuadro remarcado la url de la sede electrónica https://sede.ugr.es después pulse en Aceptar para finalizar.





Importante: La información aquí referida a https://sede.ugr.es también es aplicable a otros sitios web como https://factura.ugr.es.

Ventanas emergentes

Cuando los navegadores acceden al plug-in de Java, suelen mostrarse ventanas emergentes con mensajes o preguntas que, según el momento pueden quedar en segundo plano (detrás de la ventana actualmente activa). Al producirse esto, puede parecer que el proceso está tardando excesivamente o se ha bloqueado. Por favor, en caso de aparente retraso/bloqueo asegúrese de que no está sucediendo mediante la minimización del navegador y otras ventanas para que se muestren esos mensajes o preguntas que permitan continuar.