



# ESPUBLICO GESTIONA

Requerimientos técnicos y configuración de equipos

Septiembre de 2014

Alejandro Navarret Martínez  
anavarret@espublico.com

## 1. Requerimientos técnicos

- [Java Runtime Environment](#) Página 2
- [Actualización de software para las carpetas web \(KB907306\)](#) Página 2
- [Navegador de internet Mozilla Firefox](#) Página 2
- [Adobe Flash Player](#) Página 2
- [Adobe Acrobat Reader](#) Página 2
- [Drivers del lector de tarjetas, según el modelo a utilizar](#) Página 3
- [Drivers de la tarjeta para firma digital, según el modelo a utilizar](#) Página 3
- [Suite de Ofimática Microsoft Office/OpenOffice/LibOffice](#) Página 4

## 2. Configuración de equipos:

- [Configuración Microsoft Office 2010 y 2013 para el uso con Gestiona](#) Página 5

## 3. Java Runtime Environment: Advertencias de Seguridad

- [¿Permitir acceso a la siguiente aplicación desde este sitio web?](#) Página 10
- [¿Desea ejecutar esta aplicación?](#) Página 16
- [Este plugin tiene vulnerabilidades de seguridad](#) Página 17
- [El certificado de la página web no se puede verificar / La conexión a este sitio web no es de confianza](#) Página 19



## Requerimientos técnicos

- **Java Runtime Environment**

Versión mínima: 6.31

Versión recomendada: 7.67

<http://javadl.sun.com/webapps/download/AutoDL?BundleId=95123>

- **Actualización de software para las carpetas web (KB907306)**

<http://www.microsoft.com/es-es/download/confirmation.aspx?id=15123>

- **Navegador de internet Mozilla Firefox**

Versión mínima: 12.0

Versión recomendada: última versión 32.0

<https://download.mozilla.org/?product=firefox-32.0-SSL&os=win&lang=es-ES>

- **Adobe Flash Player**

Versión recomendada: última version 15.0.0.152 (Win IE); 14.0.0.152 (Plugin-based browsers)

[http://download.macromedia.com/get/flashplayer/current/licensing/win/install\\_flash\\_player\\_15\\_active\\_x.exe](http://download.macromedia.com/get/flashplayer/current/licensing/win/install_flash_player_15_active_x.exe)

[http://download.macromedia.com/get/flashplayer/current/licensing/win/install\\_flash\\_player\\_15\\_plugin.exe](http://download.macromedia.com/get/flashplayer/current/licensing/win/install_flash_player_15_plugin.exe)

- **Adobe Acrobat Reader**

Versión mínima: 9.5

Versión recomendada: última versión 11.0.08

[ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.07/es\\_ES/AdbeRdr11007\\_es\\_ES.exe](ftp://ftp.adobe.com/pub/adobe/reader/win/11.x/11.0.07/es_ES/AdbeRdr11007_es_ES.exe)



- **Drivers del lector de tarjetas, según el modelo a utilizar**

- Lector tarjeta criptográfica OKU 3021 y OKU 3121

<http://www.accv.es/fileadmin/Archivos/software/OKU3121-3021.zip>

- Lector tarjeta criptográfica SCM SCR3310

[http://www.accv.es/fileadmin/Archivos/software/SCR3xxx\\_DriversOnly\\_V8.40.exe](http://www.accv.es/fileadmin/Archivos/software/SCR3xxx_DriversOnly_V8.40.exe)

- Lector tarjeta criptográfica integrado en teclado Cherry G83-6644 (RS 6600)

[http://www.accv.es/fileadmin/Archivos/software/CherrySmartCard-Setup\\_31\\_ES.zip](http://www.accv.es/fileadmin/Archivos/software/CherrySmartCard-Setup_31_ES.zip) (Instalador oficial)

<https://www.dropbox.com/s/j6rohjjcmwpxfi5/Driver%20Lector%20Tarjetas%20Gen%C3%A9rico%20Windows.zip>  
(Este driver genérico omite el software PinPad incluido en el instalador oficial)

- Lector tarjeta criptográfica MiniLector EVO EsPublico

[http://www.bit4id.com/es/index.php?option=com\\_zoo&task=callelement&format=raw&item\\_id=33&element=f85c494b-2b32-4109-b8c1-083cca2b7db6&method=download&args\[o\]=715db963d0e337129ebf1b1ee69068e0&Itemid=535](http://www.bit4id.com/es/index.php?option=com_zoo&task=callelement&format=raw&item_id=33&element=f85c494b-2b32-4109-b8c1-083cca2b7db6&method=download&args[o]=715db963d0e337129ebf1b1ee69068e0&Itemid=535)

- Lector tarjeta criptográfica LTC31, LTC32, LTC36

<https://www.c3po.es/wp-content/drivers/usb/instalador.exe>

- **Drivers de la tarjeta para firma digital, según el modelo a utilizar**

- Documento nacional de identidad electrónico (DNIe)

[http://www.dnielectronico.es/descargas/CSP\\_para\\_Sistemas\\_Windows/DNIe\\_v11\\_1\\_o\\_\(32bits\).exe](http://www.dnielectronico.es/descargas/CSP_para_Sistemas_Windows/DNIe_v11_1_o_(32bits).exe)

[http://www.dnielectronico.es/descargas/CSP\\_para\\_Sistemas\\_Windows/DNIe\\_v11\\_1\\_o\\_\(64bits\).exe](http://www.dnielectronico.es/descargas/CSP_para_Sistemas_Windows/DNIe_v11_1_o_(64bits).exe)

- Tarjeta criptográfica Autoritat de Certificació de la Comunitat Valenciana (ACCV)

[http://www.accv.es/fileadmin/Archivos/software/ACCV\\_instal\\_Tarjeta.exe](http://www.accv.es/fileadmin/Archivos/software/ACCV_instal_Tarjeta.exe)

- Tarjeta criptográfica Fábrica Nacional de Moneda y Timbre WG10-CERES (FNMT)

[https://www.sede.fnmt.gob.es/documents/11614/70993/TC\\_FNMT\\_v4\\_o\\_o\\_32bits.exe/ef185385-aabo-40cc-aa07-eoddf33aeeaa](https://www.sede.fnmt.gob.es/documents/11614/70993/TC_FNMT_v4_o_o_32bits.exe/ef185385-aabo-40cc-aa07-eoddf33aeeaa)

[https://www.sede.fnmt.gob.es/documents/11614/70993/TC\\_FNMT\\_v4\\_o\\_o\\_64bits.exe/ofcddb40-d2ae-4db4-94eg-ed91a979f3eb](https://www.sede.fnmt.gob.es/documents/11614/70993/TC_FNMT_v4_o_o_64bits.exe/ofcddb40-d2ae-4db4-94eg-ed91a979f3eb)



- **Suite de Ofimática Microsoft Office/OpenOffice/LibreOffice**

Versión recomendada: Microsoft Office 2003/2007, OpenOffice 3.3.0, Libre Office 4.3.1

- LibreOffice 4.3.1

[http://donate.libreoffice.org/es/dl/win-x86/4.2.4/es/LibreOffice\\_4.2.4\\_Win\\_x86.msi](http://donate.libreoffice.org/es/dl/win-x86/4.2.4/es/LibreOffice_4.2.4_Win_x86.msi)

- OpenOffice 3.3.0

[http://archive.apache.org/dist/incubator/ooo/localized/es/3.3.0/OOo\\_3.3.0\\_Win\\_x86\\_install\\_es.exe](http://archive.apache.org/dist/incubator/ooo/localized/es/3.3.0/OOo_3.3.0_Win_x86_install_es.exe)

*Versiones posteriores, de OpenOffice a la recomendada pueden no funcionar correctamente a la hora de editar documentos web.*

*Para la configuración de Microsoft Office 2010 y 2013 ver anexo "Configuración Microsoft Office 2010 y 2013 para el uso con Gestiona"*



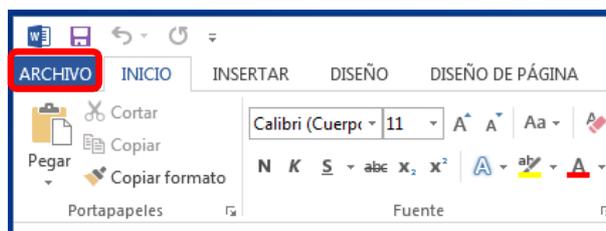
## Configuración Microsoft Office 2010 y 2013 para el uso con Gestiona

Recordar que adicionalmente a la configuración descrita en este documento debemos tener instalado el plugin *Actualización de software para las carpetas web (KB907306)* que se puede descargar desde la siguiente URL:

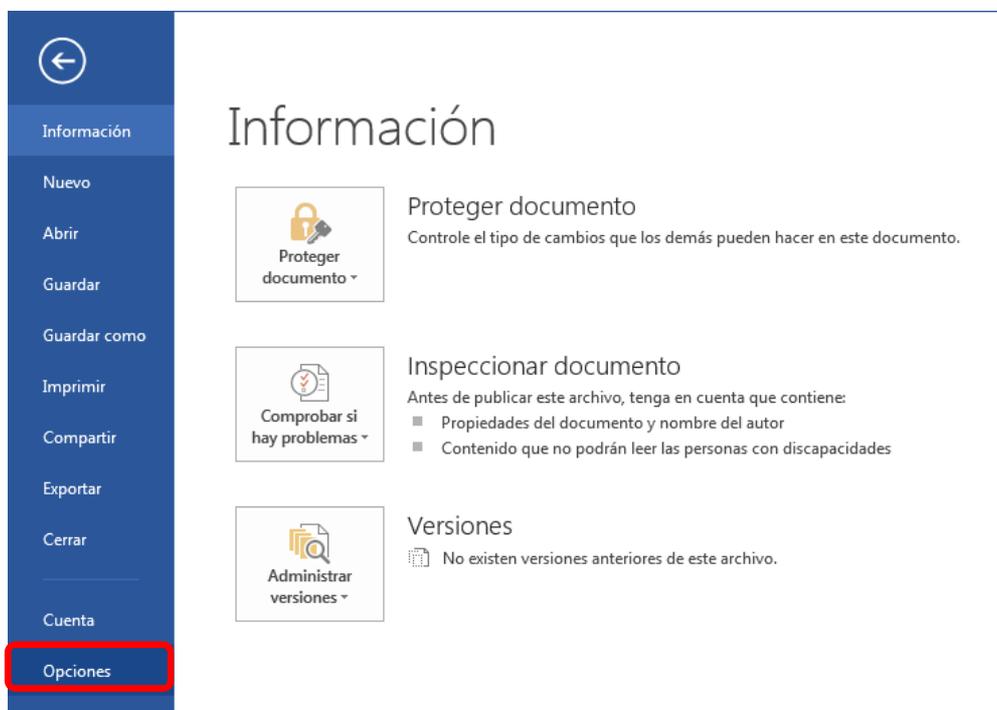
<http://www.microsoft.com/es-es/download/details.aspx?id=15123>

Abrimos cualquier software contenido en la suite de ofimática a utilizar, Microsoft Office 2010 o 2013, independientemente de si es 32 o 64 bits. Por ejemplo Microsoft Word.

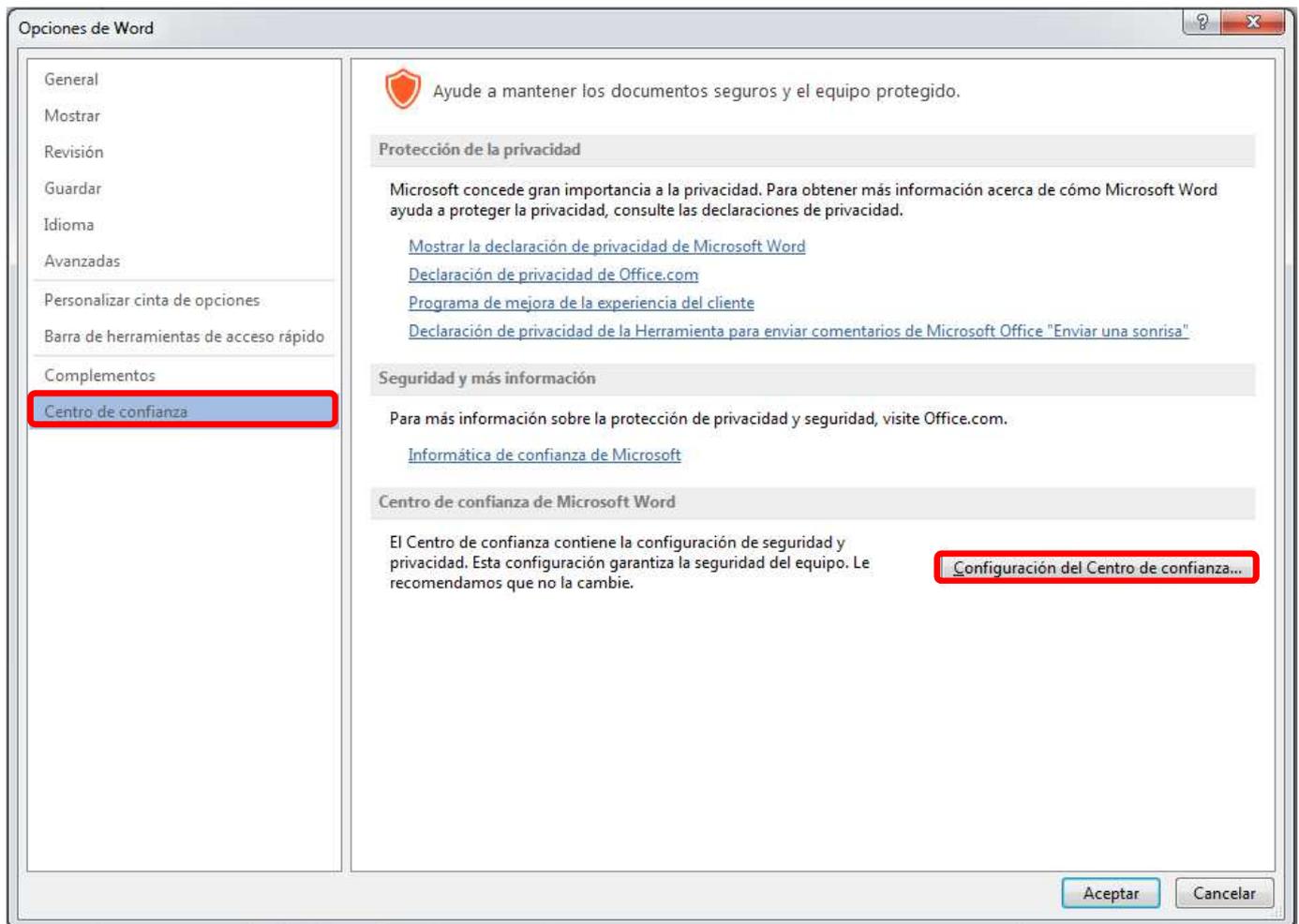
Buscamos en la parte superior izquierda la pestaña **ARCHIVO** y pulsamos sobre ella.



En la pantalla que se nos muestra a continuación buscaremos en el menú izquierdo la palabra **Opciones** y pulsamos sobre ella.

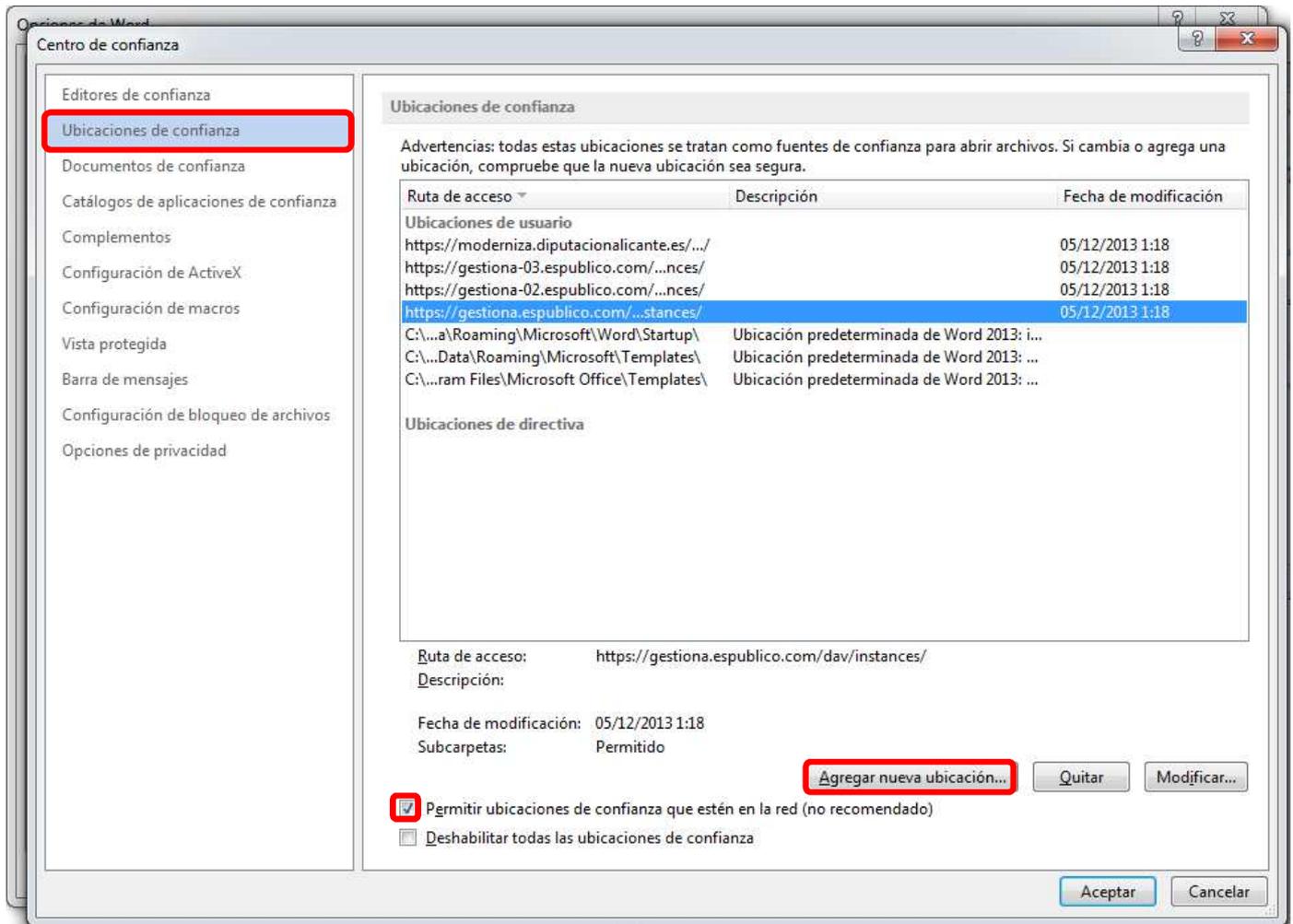


Se nos abre una nueva ventana con título **Opciones de Word** en la que seleccionaremos en el menú izquierdo la opción **Centro de confianza**, al mostrarse el contenido de dicho apartado pulsamos sobre el botón **Configuración del Centro de confianza**.



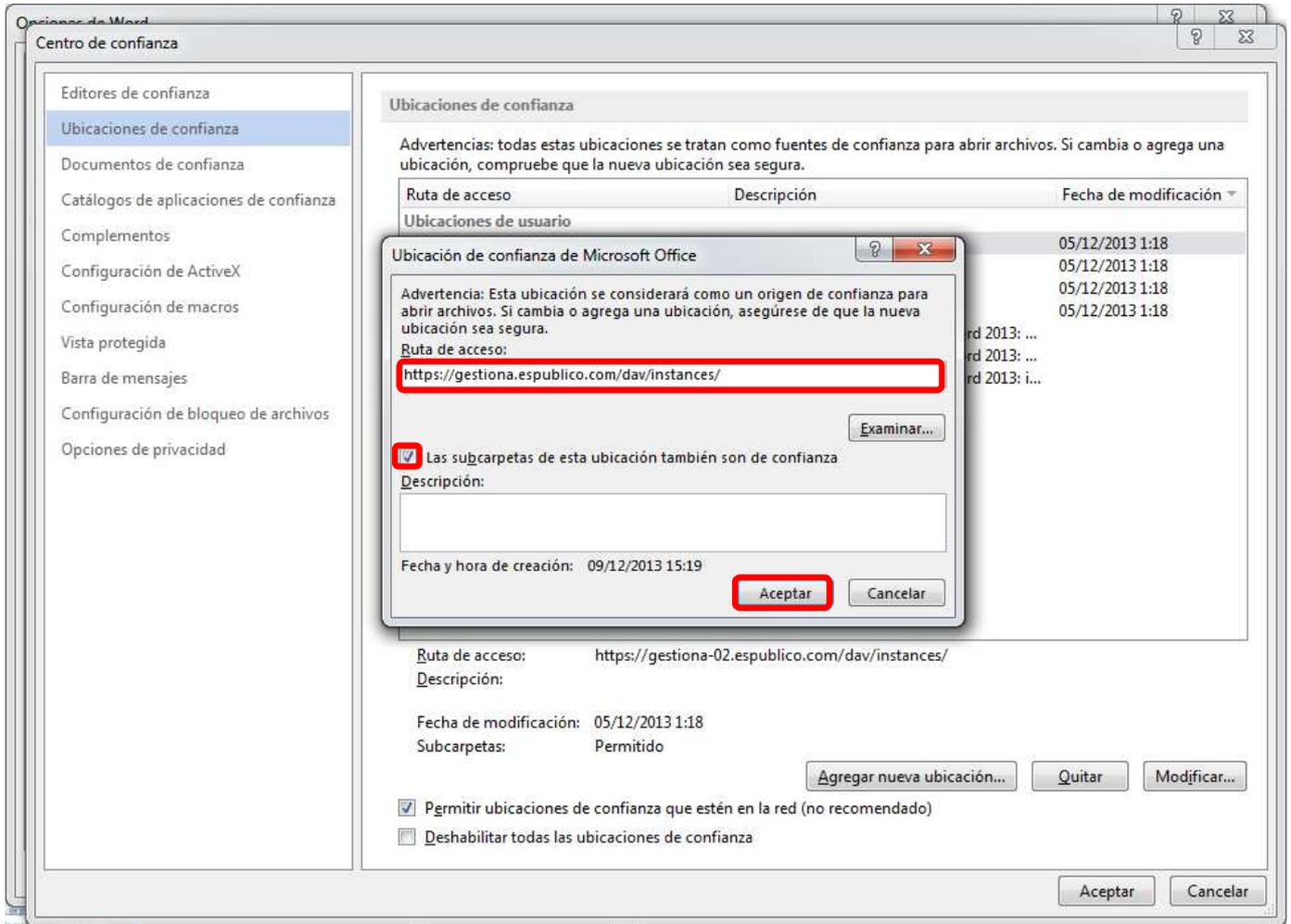
Se abre una nueva ventana con título **Centro de confianza** en la que seleccionaremos en el menú izquierdo la opción **Ubicaciones de confianza**, al mostrarse el contenido de dicho apartado debemos marcar la casilla que tiene como enunciado el texto **Permitir ubicaciones de confianza que estén en la red (no recomendado)** y pulsamos sobre el botón **Agregar nueva ubicación**.





Se nos abre una nueva ventana con título **Ubicación de confianza de Microsoft Office** en la que escribimos, en el campo de texto enunciado como **Ruta de acceso**, la URL de acceso a Gestiona seguido de **/dav/instances/** a continuación, marcamos la casilla que tiene como enunciado **Las subcarpetas de esta ubicación también son de confianza** y pulsamos el botón Aceptar.





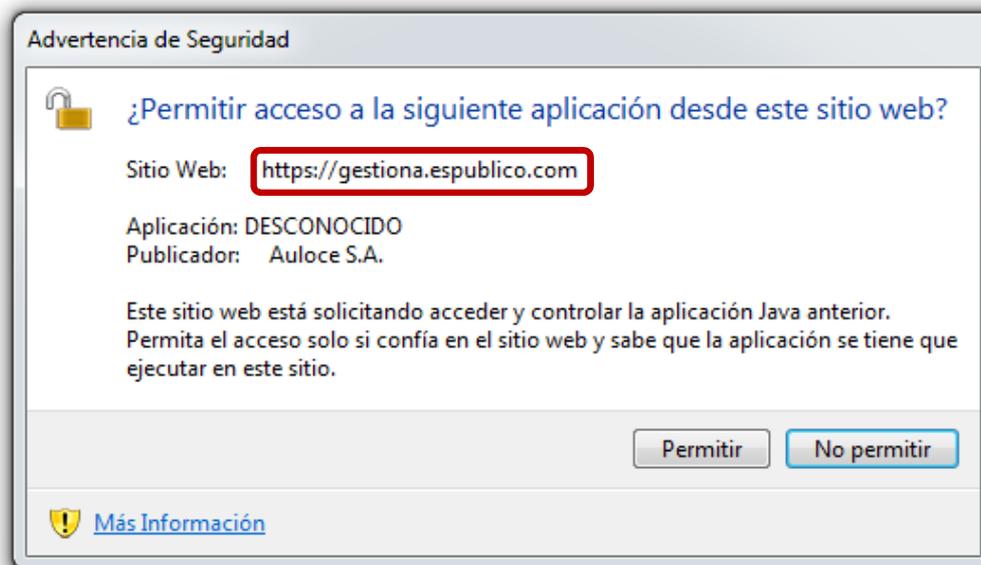
En el ejemplo nuestra URL de acceso a Gestiona es <https://gestiona.espublico.com> y hemos agregado la dirección <https://gestiona.espublico.com/dav/instances/> como ubicación de confianza.

Al agregar la ubicación ya podemos pulsar **Aceptar** en la ventana de **Centro de confianza** y **Opciones de Word** para terminar la configuración.



## Java Runtime Environment: Advertencias de Seguridad

- ¿Permitir acceso a la siguiente aplicación desde este sitio web?



En **Sitio Web** nos aparecerá el pool de conexión a través del cual conectamos a Gestiona, en este ejemplo nosotros accedemos a Gestiona a través de la dirección **https://gestiona.espublico.com**.

- **COMPORTAMIENTO DE LA ADVERTENCIA**

Esta ventana de **Advertencia de Seguridad** nos aparece al tratar de editar un documento en el apartado **DOCUMENTOS** de un expediente, o al tratar de firmar un documento desde nuestro portafirmas.

Esta **Advertencia de Seguridad** nos aparecerá la primera vez que intentemos realizar alguna de las dos acciones comentadas por primera vez en la actual sesión de nuestro navegador de internet, recordando la decisión seleccionada hasta que cerremos el navegador. Al abrir el navegador, y entrar de nuevo en Gestiona, nos vuelve a aparecer la ventana de nuevo.



- **SOLUCIÓN**

Para solucionar dicha advertencia deberemos tener instalada, como mínimo, la versión de Java 7 Update 51.

<http://javadl.sun.com/webapps/download/AutoDL?BundleId=83383>

Debemos acceder al panel de control de Java, el cual localizaremos, en función de nuestro sistema operativo, de la siguiente forma:

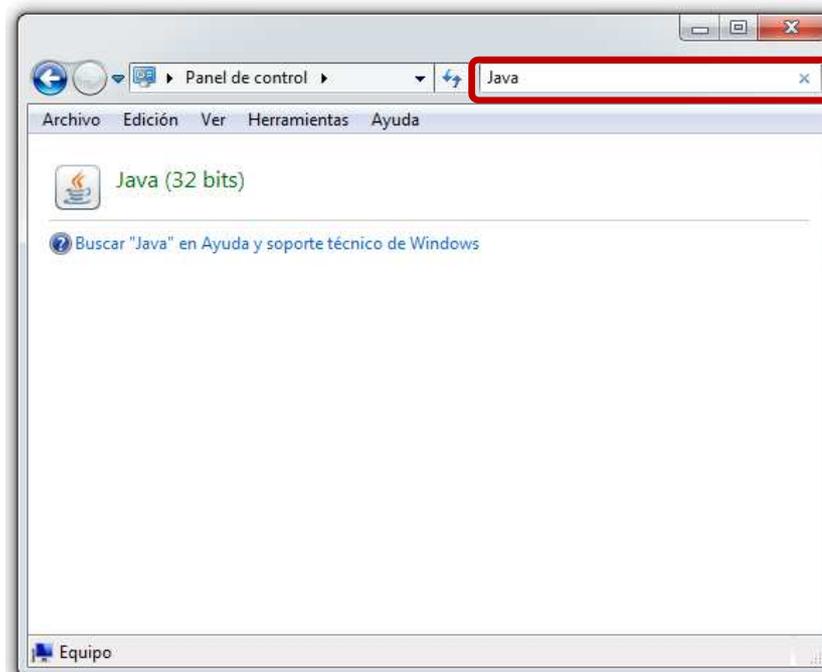
#### **Windows 8**

Utilice la búsqueda para encontrar el panel de control

- Pulse la **tecla con el logotipo de Windows + W** para abrir el **acceso a Buscar** y buscar la configuración, o bien arrastre el puntero del mouse hasta la esquina inferior derecha de la pantalla y luego haga clic en el icono **Buscar**.
- En el cuadro de búsqueda, escriba **Panel de control de Java**
- Haga clic en el icono de Java para abrir el panel de control de Java.

#### **Windows 7, Vista**

- Haga clic en el botón **Inicio** y, a continuación, en la opción **Panel de control**.
- En el **cuadro de búsqueda del panel de control**, escriba **Java**.



## Windows XP

- Haga clic en el botón **Inicio** y, a continuación, en la opción **Panel de control**.
- Haga doble clic en el icono de Java para abrir el panel de control de Java.

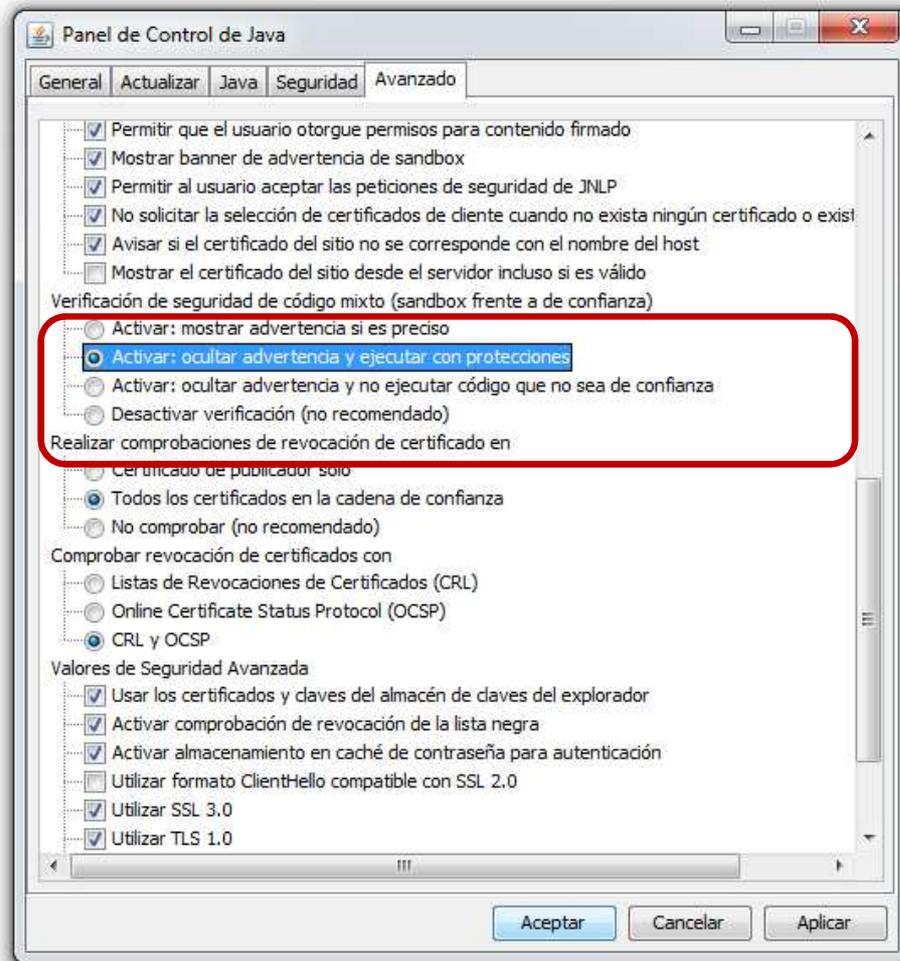
Una vez abierto el **Panel de Control de Java** vamos a abrir la pestaña **Avanzado**.



Navegaremos entre las opciones disponibles en hasta localizar una que se llama **Verificación de seguridad de código mixto (sandbox frente a de confianza)**.

Ampliamos la opción **Verificación de seguridad de código mixto (sandbox frente a de confianza)** de la sección **Seguridad** y seleccionamos la opción **Activar: ocultar advertencia y ejecutar con protecciones**.





Una vez marcada la opción vamos a abrir la pestaña **Seguridad**.

Desde la pestaña **Seguridad** localizaremos un apartado enunciado como **Listado de excepciones de sitios**, en el que se describe "Las aplicaciones iniciadas desde los sitios que se enumeran a continuación se podrán ejecutar después de las peticiones de datos de seguridad apropiadas".

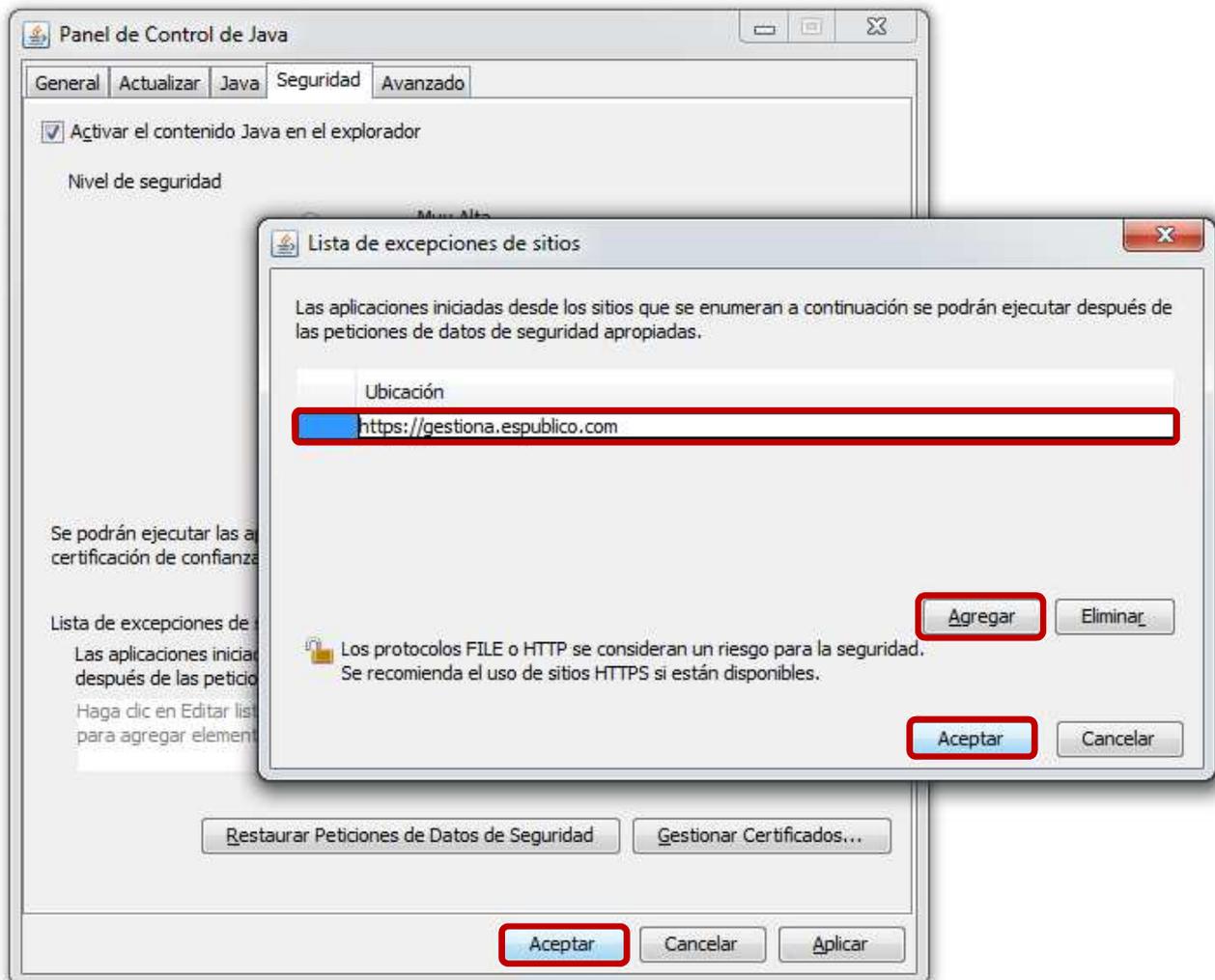


A continuación de la descripción encontraremos el botón **Editar lista de sitios**, pulsamos sobre él para añadir como excepción nuestro pool de conexión habitual para el acceso de Gestiona, en nuestro caso de ejemplo <https://gestiona.espublico.com>.



En la nueva ventana que se nos abre al pulsar sobre **Editar lista de sitios**, pulsamos sobre el botón agregar e introducimos el pool de conexión que nos aparecía en **Sitio Web** en nuestra **Advertencia de Seguridad**, una vez añadido pulsaremos **Aceptar** en la ventana actual y **Aceptar** en la ventana del **Panel de Control de Java**.

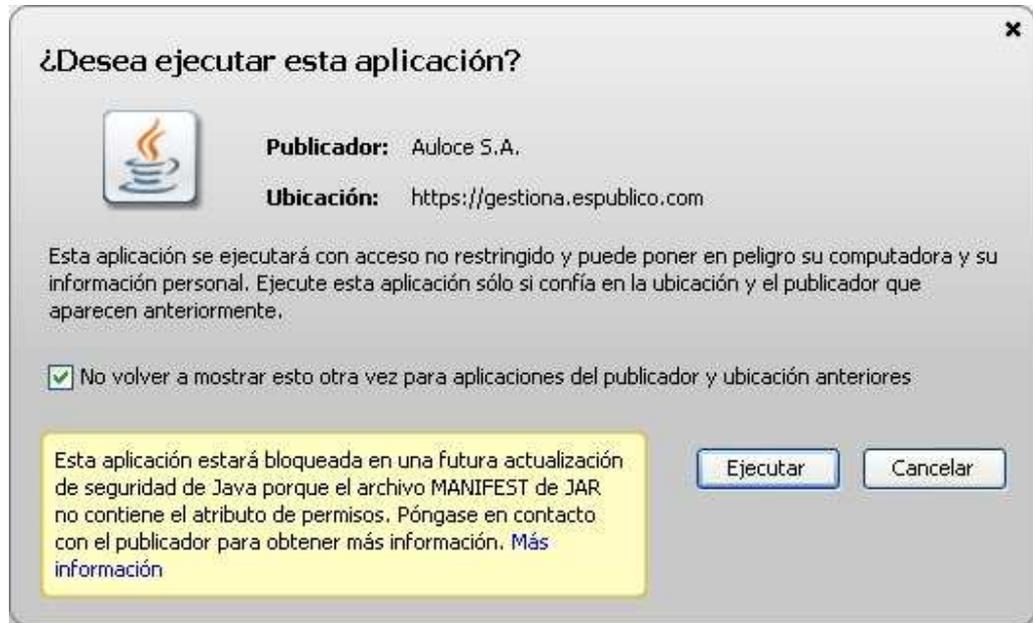




Quando volvamos a utilizar GestionA, cerrar el navegador y volver a abrirlo si este se encontraba abierto durante el proceso de configuración que hemos seguido, no deberían de volver a mostrarse estas advertencias de seguridad al funcionar con GestionA.



- ¿Desea ejecutar esta aplicación?



En **Ubicación** nos aparecerá el pool de conexión a través del cual conectamos a Gestiona habitualmente, en este ejemplo nosotros accedemos a Gestiona a través de la dirección <https://gestiona.espublico.com> utilizando el navegador Mozilla Firefox.

- **COMPORTAMIENTO DE LA ADVERTENCIA**

Esta ventana nos aparece al acceder a Gestiona por primera vez solicitándonos permiso para la ejecución de Java.

- **SOLUCIÓN**

Para solucionar esta advertencia simplemente deberemos marcar la casilla **No volver a mostrar esto otra vez para aplicaciones del publicador y ubicaciones anteriores**, como se aprecia en la imagen superior, y seguidamente pulsaremos el botón **Ejecutar**.

Según el navegador que estemos utilizando para acceder a Gestiona, y la versión del mismo, las ventanas de advertencia pueden ser diferentes. Las advertencias del ejemplo se corresponden con el uso del navegador Mozilla Firefox.

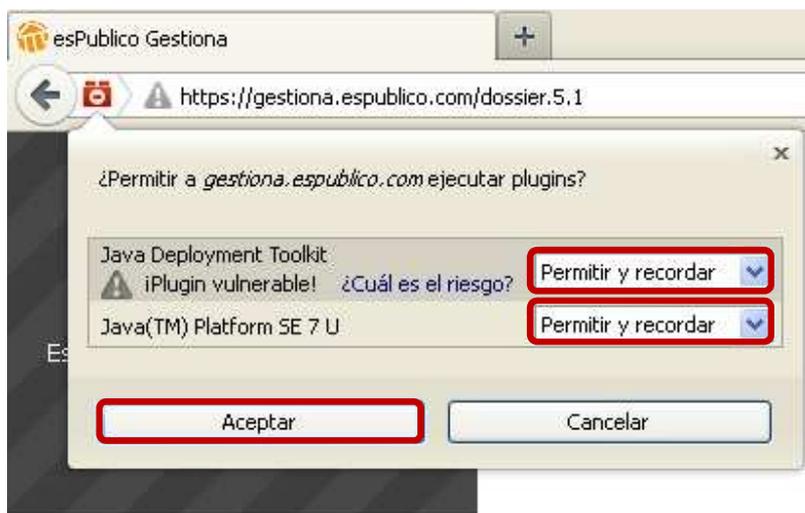


- Este plugin tiene vulnerabilidades de seguridad

Si al ejecutarse Java en Gestiona la versión de Java que tenemos instalada tiene vulnerabilidades de seguridad, bien porque se han detectado y aún no hay una actualización de Java que lo solvete o porque estemos trabajando con una versión de Java desactualizada, nos aparecerá una advertencia indicándonoslo, en este ejemplo nosotros accedemos a Gestiona a través de la dirección <https://gestiona.espublico.com> y la advertencia es sobre Java 7 al acceder a Gestiona utilizando el navegador Mozilla Firefox.



Para permitir la ejecución de Java, a pesar de las vulnerabilidades detectadas, deberemos pulsar el botón **Permitir**, o en el icono de la advertencia, resaltado en la imagen sobre este párrafo.



Se nos mostrará un desplegable en el cual deberemos seleccionar la opción **Permitir y recordar** en las cajas de selección que se nos mostrarán, de lo contrario nos los preguntará cada vez que accedamos a Gestiona, y a continuación pulsar sobre **Aceptar**.

Según el navegador que estemos utilizando para acceder a Gestiona, y la versión del mismo, las ventanas de advertencia pueden ser diferentes.



- El certificado de la página web no se puede verificar /  
La conexión a este sitio web no es de confianza

Este error ocurre en el pool de <https://moderniza.diputacionalicante.es> al utilizarse la ACCV como entidad certificadora.

Esta **Advertencia de Seguridad** aparece al acceder a Gestiona y podemos encontrarnos con dos casos diferenciados en función de la versión de Java instalada en el equipo.



- **COMPORTAMIENTO DE LA ADVERTENCIA (JAVA 6)**

Esta ventana nos aparece al acceder a Gestiona por primera vez solicitándonos permiso para continuar con la ejecución de Java a pesar de no poder verificarse el certificado de la página web.

- **SOLUCIÓN (JAVA 6)**

Nos aparece la **Advertencia de Seguridad** y nos permite marcar la casilla **Confiar siempre en el contenido de este editor**, lo cual instalará el certificado de la ACCV utilizado para la certificación de este pool en el repositorio de certificados de Java como **Sitio Seguro**. Una vez este certificado se encuentra entre los certificados de Java no se volverá a mostrar dicha advertencia, independientemente de que actualicemos a Java 7 o no.





- **COMPORTAMIENTO DE LA ADVERTENCIA (JAVA 7)**

Esta ventana nos aparece al acceder a Gestiona por primera vez solicitándonos permiso para continuar con la ejecución de Java a pesar de no poder verificarse el certificado de la página web.

Nos aparece la **Advertencia de Seguridad** y NO nos permite marcar ninguna opción para confiar siempre en el contenido del editor, como ocurría en Java 6, por lo que no llega a incorporarse el certificado en los repositorios de Java y la alerta aparecerá cada vez que abramos el navegador y accedamos a Gestiona, recordando la decisión que tomemos sobre dicha advertencia mientras mantengamos abierto el navegador y olvidándola a su cierre.

- **SOLUCIÓN (JAVA 7)**

La solución pasa por instalar de forma manual el certificado de la ACCV que está utilizando el pool de **https:moderniza.diputacionalicante.es** como Sitio Seguro en los repositorios de certificados de Java. Una vez este certificado se encuentra entre los certificados de Java no se nos volverá a mostrar dicha advertencia, independientemente de que actualicemos a Java 7 o no.

Para añadir el certificado deberemos debemos acceder al **Panel de Control de Java**, el cual localizaremos, en función de nuestro sistema operativo, de la siguiente forma:

#### **Windows 8**

Utilice la búsqueda para encontrar el panel de control

- Pulse la **tecla con el logotipo de Windows + W** para abrir el **acceso a Buscar** y buscar la configuración, o bien arrastre el puntero del mouse hasta la esquina inferior derecha de la pantalla y luego haga clic en el icono **Buscar**.



- En el cuadro de búsqueda, escriba **Panel de control de Java**
- Haga clic en el icono de Java para abrir el panel de control de Java.

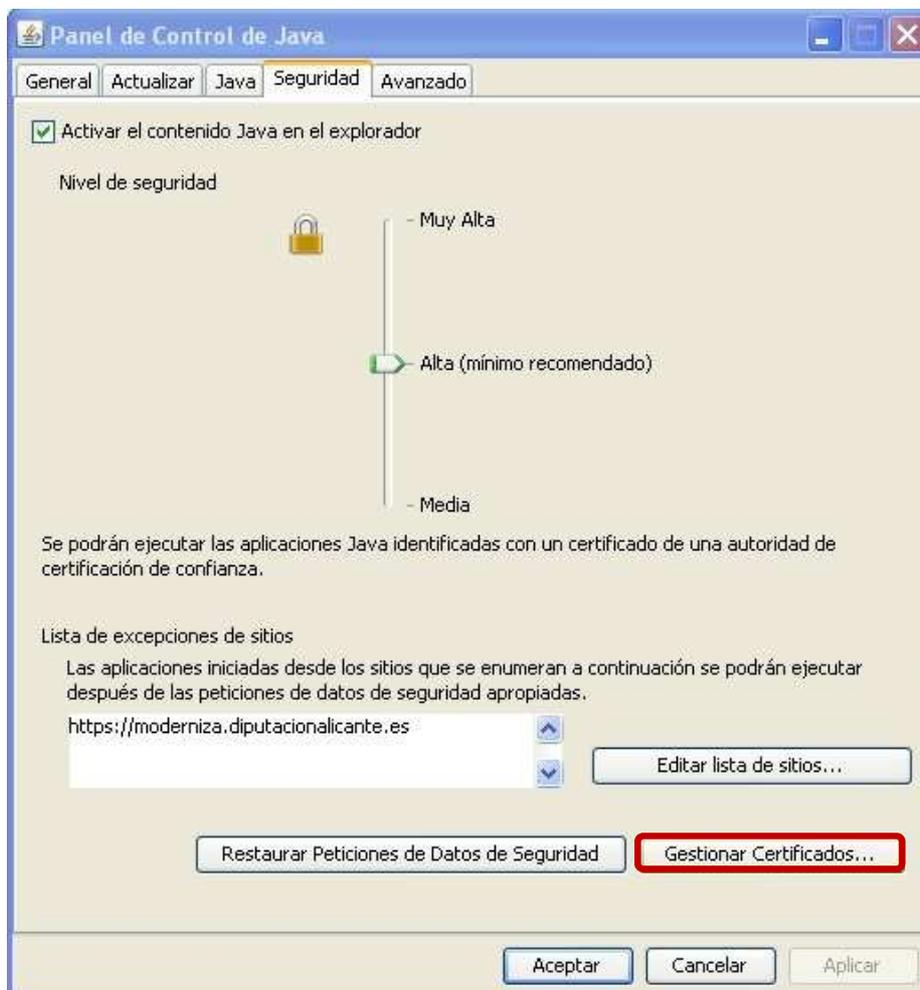
### Windows 7, Vista

- Haga clic en el botón **Inicio** y, a continuación, en la opción **Panel de control**.
- En el **cuadro de búsqueda del panel de control**, escriba **Java**.
- Haga clic en el icono de Java para abrir el panel de control de Java.

### Windows XP

- Haga clic en el botón **Inicio** y, a continuación, en la opción **Panel de control**.
- Haga doble clic en el icono de Java para abrir el panel de control de Java.

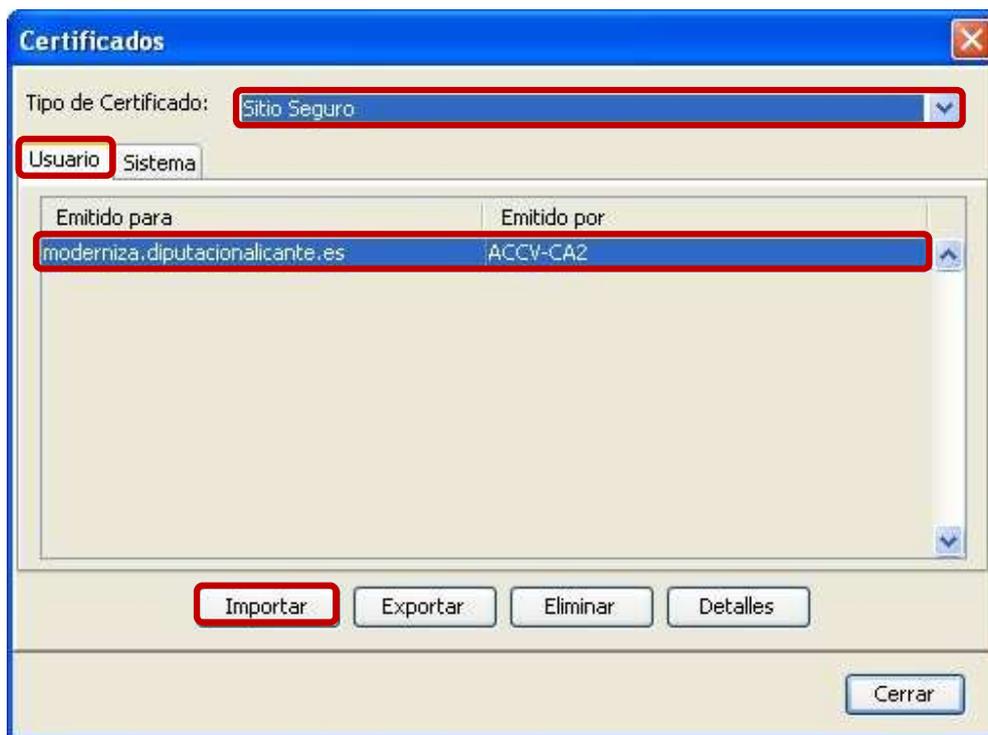
Una vez abierto el **Panel de Control de Java** vamos a abrir la pestaña **Seguridad**.



Pulsamos el botón **Gestionar Certificados** y, en la nueva ventana que se nos abre, seleccionamos como **Tipo de Certificado** en las pestaña de **Usuario**, como en la imagen, **Sitio Seguro**, a continuación pulsamos el botón **Importar** e indicaremos la localización dónde tengamos descargado el certificado correspondiente. Debería quedar importado como en la imagen.

Podéis descargaros el certificado desde el siguiente enlace:

<https://www.dropbox.com/s/73psym5zjubeorb/moderniza.diputacionalicante.es%20ACCV-CA2.csr>



Para terminar pulsamos el botón **Cerrar** y en la ventana principal del **Panel de control de Java**, pulsamos **Aceptar**.

