

# Especificación técnica para el acceso a HERA

## Índice

<b>1</b>	<b>Objetivo.....</b>	<b>2</b>
<b>2</b>	<b>Requisitos técnicos generales.....</b>	<b>2</b>
2.1	Equipo.....	2
2.2	Sistema operativo.....	2
2.3	Internet.....	2
2.4	Navegador.....	3
2.5	Nivel de seguridad del navegador.....	3
2.6	Desactivación del bloqueo de elementos emergentes.....	6
2.7	Acceso a la aplicación mediante certificado.....	7
2.8	Lector de tarjetas.....	10
<b>3</b>	<b>Requisitos técnicos para la firma electrónica.....</b>	<b>10</b>
3.1	Máquina virtual de Java.....	10
3.2	Configuración seguridad de java.....	11
3.3	Cacheo del PIN del certificado.....	13
<b>4</b>	<b>Anexo I. Accesos.....</b>	<b>14</b>
4.1	Solicitud de Acceso.....	14
4.2	Acceso al sistema HERA.....	14
4.3	Manual del usuario.....	20
4.4	Tramitación de incidencias CATS.....	20
4.5	Comprobar que la firma electrónica se ha instalado correctamente en el navegador.....	20
<b>5</b>	<b>Anexo II: Instalación de la máquina virtual de java.....</b>	<b>23</b>

## 1 Objetivo

El objeto de este documento es ayudar a configurar los equipos que accedan al sistema HERA para la gestión de la ortoprótesis de la Consellería de Sanitat.

Se recomienda leer el documento completamente antes de iniciar cualquier actuación en los equipos.

## 2 Requisitos técnicos generales

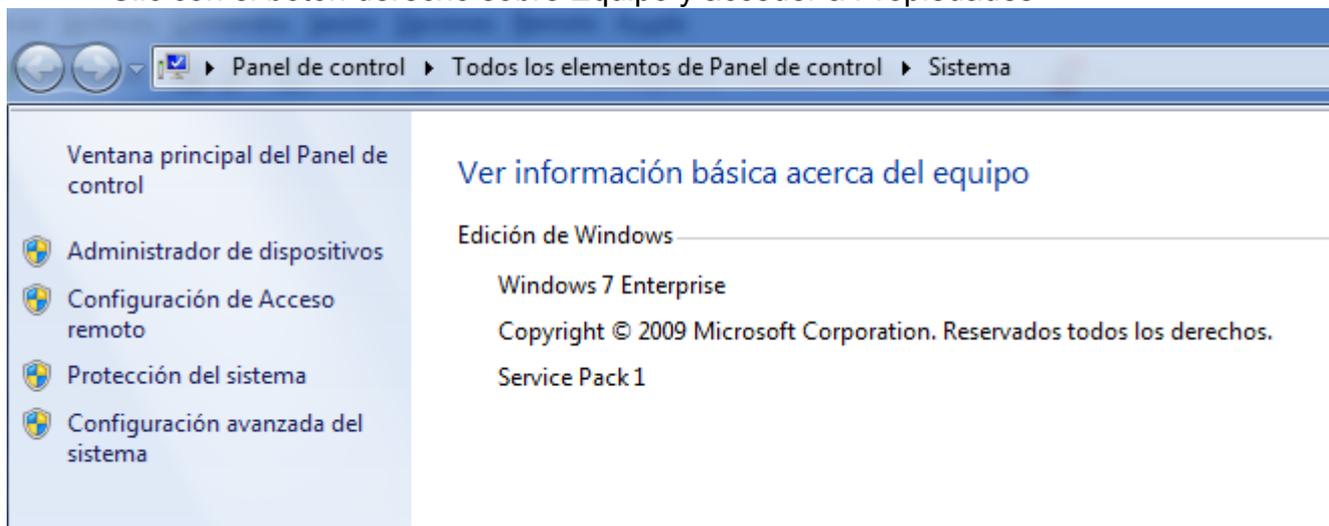
### 2.1 Equipo

Cualquiera computador actual de venta del mercado es adecuado, como mínimo se recomienda un Core i3 con mínimo 2 Gb de RAM.

### 2.2 Sistema operativo

Comprobar que tiene: Windows 7 ó Windows 10

Clic con el botón derecho sobre Equipo y acceder a Propiedades



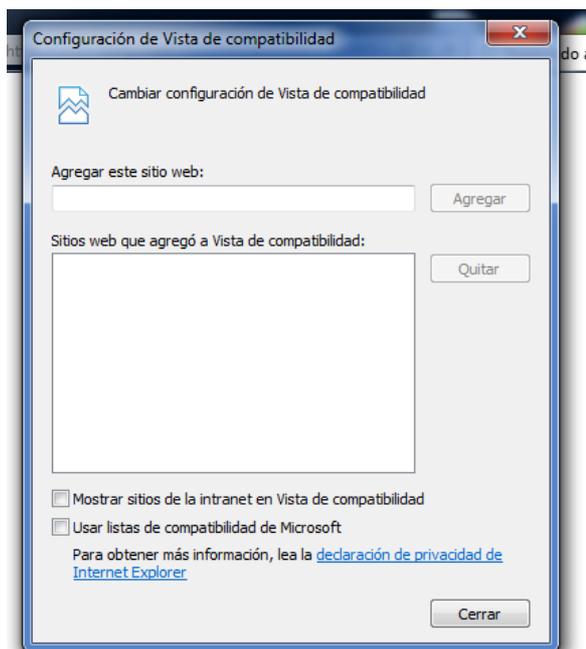
### 2.3 Internet

Los requisitos de la banda de conexión no son específicos, cualquier ADSL o fibra óptica del mercado es suficiente.

## 2.4 Navegador

**Internet Explorer**, versión 11 de 32 bits con modo de compatibilidad desactivado.

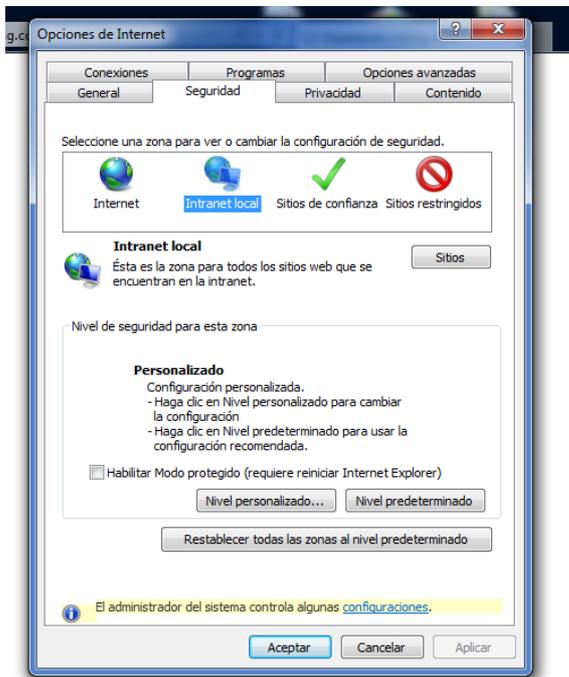
Para ello hay que acceder al menú de **Herramientas** con la opción de **Configuración de vista de compatibilidad** y comprobar que no está añadida la URL de acceso a HERA (<https://siscv.san.gva.es>).



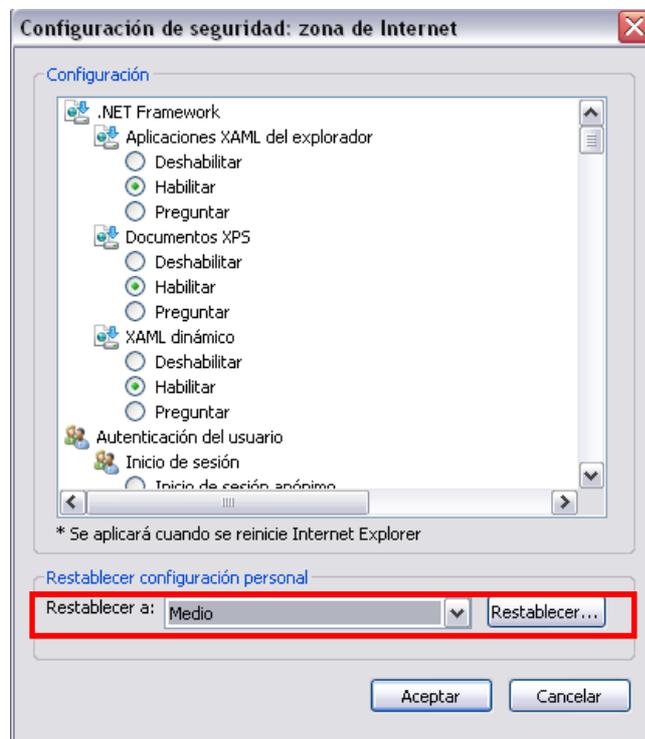
## 2.5 Nivel de seguridad del navegador

Restablecer el nivel de seguridad a MEDIO

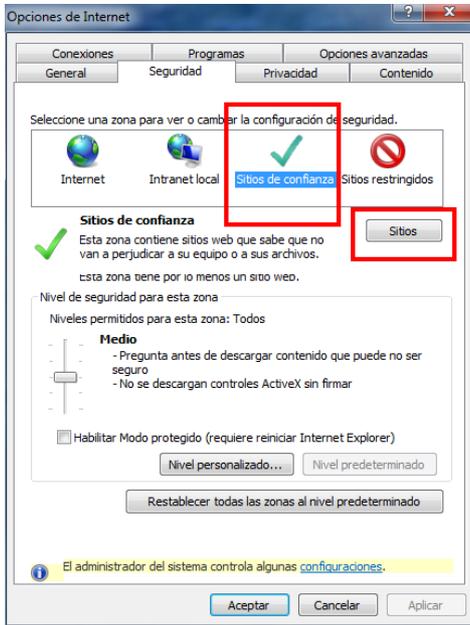
**Herramientas** Ⓞ **Opciones de Internet** Ⓞ pestaña **Seguridad** Ⓞ **Nivel personalizado...**



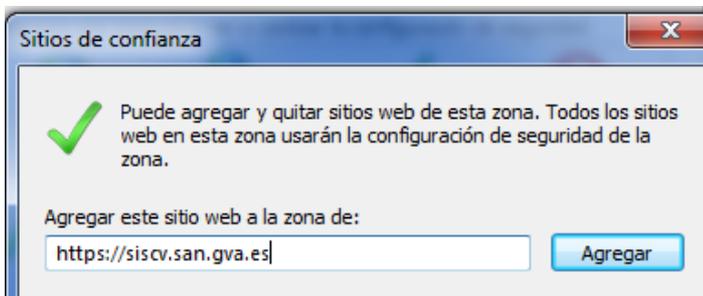
Seleccionar **Medio** y pulsar **Restablecer...**



Una vez hecho esto, dentro del apartado Seguridad seleccionar Sitios de confianza y dentro de éste Sitios



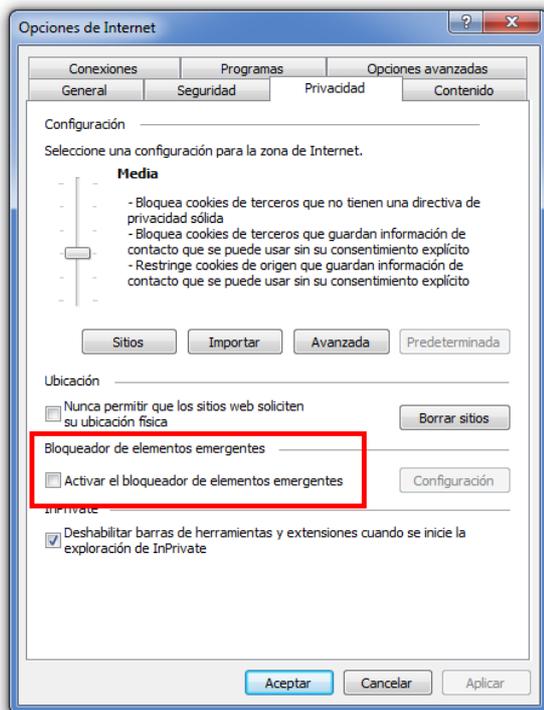
Dentro de sitios añadir la url de acceso a la aplicación <https://itsiscv.gva.es> y pulsar Agregar



**Cerrar el explorador** (todas las ventanas que tenga abiertas) y volver a abrirlo.

## 2.6 Desactivación del bloqueo de elementos emergentes

Es necesario desactivar el bloqueo de elementos emergentes del navegador desde la opción del menú **Herramientas/Opciones de Internet** de Internet Explorer. En éste menú hay que acceder a la pestaña **Privacidad** y desmarcar el check “*Bloquear elementos emergentes*” en la parte inferior.



También es posible acceder a la configuración del bloqueador para añadir los sitios en los que se permiten ventanas emergentes.

En el caso se acceda desde fuera de la red Arterias de la Consellería de Sanidad es recomendable añadir la url de acceso (<https://itsiscv.san.gva.es>) a sitios seguros de Internet.

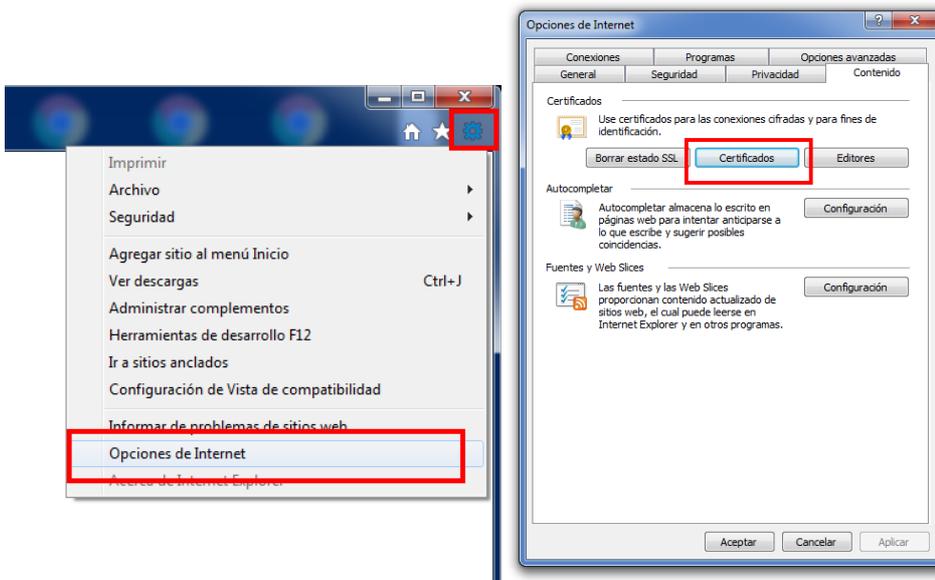
## 2.7 Acceso a la aplicación mediante certificado.

Se debe disponer de un certificado personal en soporte tarjeta expedido por la Autoridad Certificadora de la Comunitat Valenciana (ACCV). Es necesario instalar los certificados raíz válidos de la ACCV son: ACCV-CA2, ACCV-CA1, ACCV-CA120, ACCV-CA110, ACCVRAIZ1 y ROOT CA GENERALITAT VALENCIANA.

Estos certificados se expiden en puntos de registro de usuarios (PRU). Puede consultar su ubicación en la página web [www.accv.es](http://www.accv.es).

**Comprobar que tiene los certificados correctamente instalados en el navegador.**

Abrir el navegador: **Herramientas** ① **Opciones de Internet** ① **Contenido** ①  
seleccione el botón **Certificados**



## Pestaña **Entidades emisoras de certificados intermedias**

Comprobar que tiene los siguientes certificados:

- ACCV-CA110
- ACCV-CA120

ó

- ACCV-CA2
- ACCV-CA1

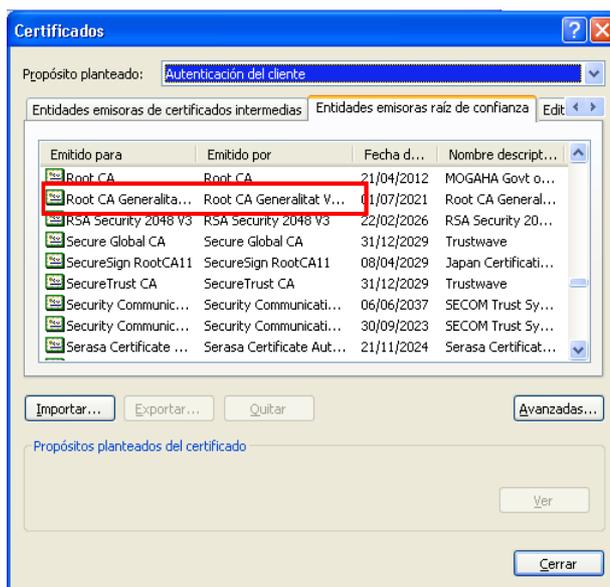
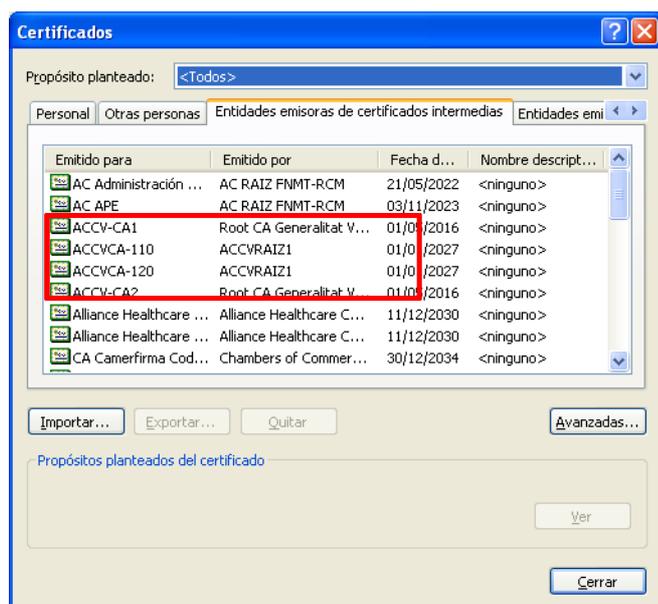
Dependiendo del certificado que se posea, si la tarjeta es emitida en 2013 o 2014, deberán instalarse ACCV-CA110 y ACCV-CA120.

NOTA: No hay ningún problema si se instalan todas

## Pestaña **Entidades emisoras raíz de confianza**

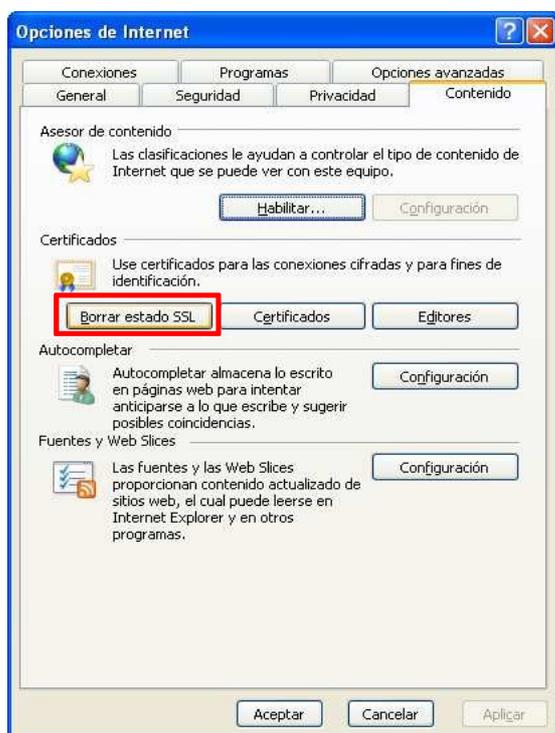
Comprobar que tiene los siguientes certificados:

- ROOT CA GENERALITAT VALENCIANA
- ACCVRAIZ1



En [www.accv.es](http://www.accv.es) están disponibles estos certificados para su descarga, así como la página de ayuda de accv.es.

NOTA: Es conveniente antes de acceder al sistema por primera vez borrar el estado SSL



## **2.8 Lector de tarjetas**

Cualquier lector disponible en el mercado es válido. Puede ser integrado en el teclado o conectado a la torre a través de un USB. El fabricante del lector le dará instrucciones para una correcta instalación. Nótese que si es un USB, dependiendo en qué puerto USB se instale, el resto de puertos pueden no reconocerlo. Confírmese la correcta instalación del lector de tarjetas en el ordenador del usuario. Para la correcta instalación de la tarjeta y el lector puede consultar la guía ofrecida por la accv: <http://www.accv.es/ayuda/manuales-de-instalacion/> (Guías de instalación de la tarjeta criptográfica y el lector).

Hay que tener en cuenta que existen 2 tipos de tarjetas, G&D y Siemens, cada una tiene sus propios drivers. Recordar que para G&D hay que descargar los driver para 32bits para el correcto uso de la aplicación.

## **3 Requisitos técnicos para la firma electrónica**

Para aquellos usuarios que realicen alguna actividad relacionada con las exoprótesis (prescripción, visado, autorización o adaptación) será necesario que dispongan de determinados requisitos técnicos para poder hacer uso de la firma electrónica en HERA.

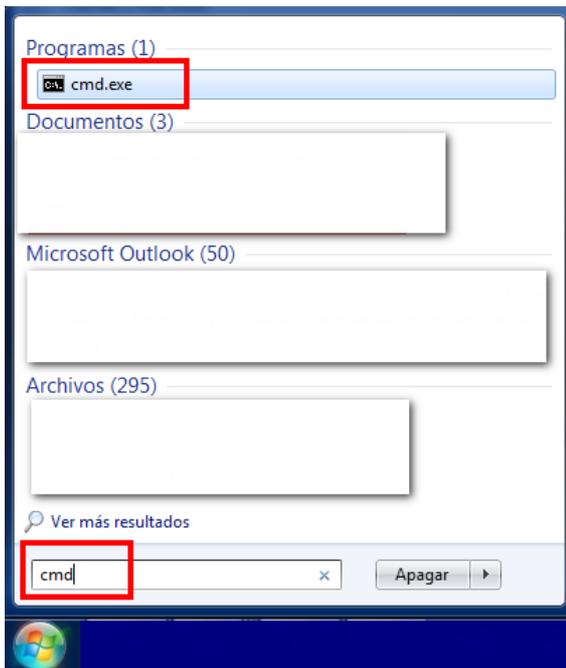
Es necesario disponer de certificados de la ACCV y lector de tarjetas descritos en los apartados anteriores.

### **3.1 Máquina virtual de Java**

Se requiere disponer de una versión de la máquina virtual de Java con la versión 1.8\_101 de 32 bits que es la homologada por la maqueta de los puestos de trabajo de la Consellería de Sanitat.

Se puede comprobar la versión de Java disponible siguiendo los siguientes pasos:

**Inicio** Ⓞ **Bucar cmd**

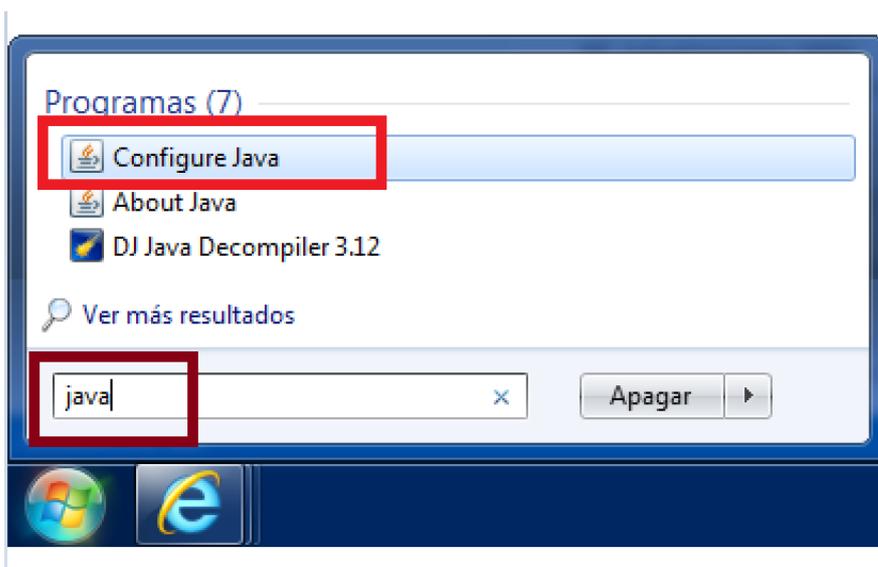


Y seleccionar cmd.exe

Ejecutar el comando: `java -version` y comprobar que java versión es “1.8.0.101”

### 3.2 Configuración seguridad de java

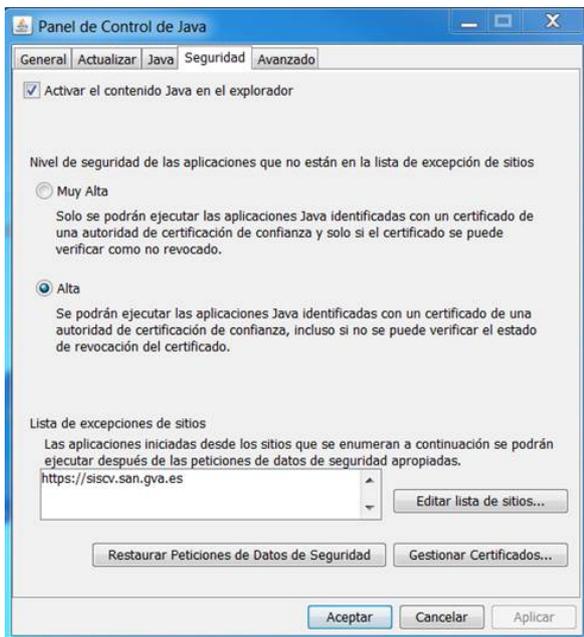
Pulsar el botón de Windows y en el buscador escribir “Java”, a continuación pulsar Configure Java



En la sección inferior muestra las excepciones de sitios, pulsar el botón “Editar lista de sitios...”

En la ventana que se abre pulsar el botón agregar y en el recuadro que se habilita introducir la siguiente dirección: <https://itsiscv.san.gva.es>

Pulsar el botón aceptar y comprobar que la lista de excepciones queda como en la imagen:



### 3.3 *Cacheo del PIN del certificado*

Si se dispone del certificado de usuario en tarjeta criptográfica Siemens, es posible configurar el cacheo del PIN para evitar que éste solicite cada vez que el usuario tenga que hacer una firma electrónica en la aplicación. Para ello, se debe disponer de la siguiente clave del registro de Windows con los valores indicados:

**HKEY\_LOCAL\_MACHINE\SOFTWARE\Siemens\CardOS API**

**CSPFlags** (REG\_DWORD) con el valor 16 (decimal)/10 (hexadecimal)

**CSPPinCacheExpirationTime** (REG\_DWORD) con el valor 0

## 4 Anexo I. Accesos

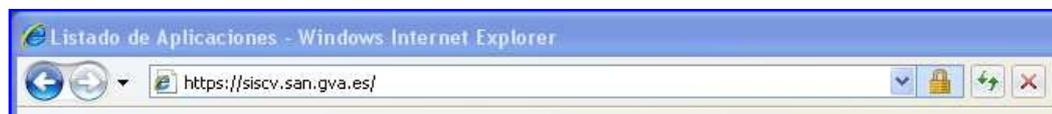
### 4.1 Solicitud de Acceso

Para acceder al sistema HERA se requiere cumplimentar y enviar la correspondiente solicitud de credencial de acceso. Éste modelo está disponible en la página web de la Consellería de Sanitar ([www.san.gva.es](http://www.san.gva.es)); ruta: Profesionales > Farmacia > HERA > Acceso.

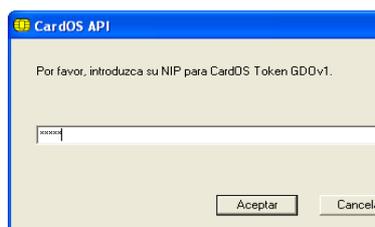
### 4.2 Acceso al sistema HERA

Aprobada la solicitud, el usuario recibirá un correo electrónico informativo del nuevo estado de alta como usuario del lugar donde consultar los manuales de usuario.

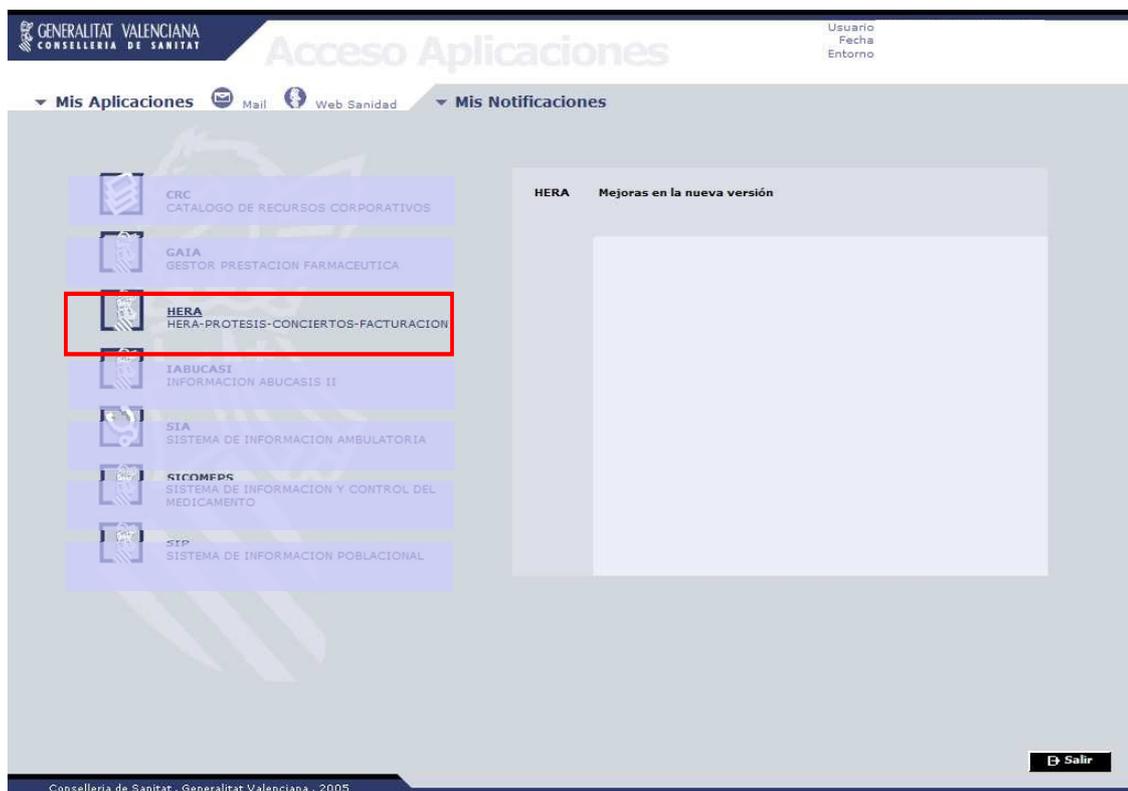
Para acceder a la aplicación, debe introducir la tarjeta ACCV en el lector. Y escribir la siguiente dirección en la barra de su navegador Internet Explorer: <https://siscv.san.gva.es>



Esta dirección le llevará al Portal de Aplicaciones de la Generalitat Valenciana. Esta página tiene el acceso restringido a usuarios, por lo que se solicita autenticación del usuario. En una ventana parecida a las que muestran en la imagen, el usuario debe introducir el PIN de su tarjeta.



En la pantalla del Portal de Aplicaciones, se visualiza el icono de HERA.  
Seleccionando dicho icono o la palabra “HERA” y se accede a la aplicación.



Si tiene algún problema con el acceso a través de esta url puede acceder la siguiente url:

[https://itsiscv.san.gva.es/hera/app/hera\\_inicio.jsp](https://itsiscv.san.gva.es/hera/app/hera_inicio.jsp)

### 4.3 Manual del usuario

Existe un manual de usuario para cada uno de los distintos perfiles de usuario existentes en HERA. Puede consultar el manual adecuado para su perfil en la página web de la Consellería de Sanitat ([www.san.gva.es](http://www.san.gva.es); ruta: Profesionales > Farmacia > HERA).

### 4.4 Tramitación de incidencias CATS

El vehículo normalizado de transmisión de incidencias con la aplicación es el Centro de Atención Telefónica Sanitaria (CATS), que tiene varios canales de contacto:

Teléfono: 902 39 39 99 / 989500

Fax: 96 348 82 32

Correo electrónico: [cats@gva.es](mailto:cats@gva.es)

Las incidencias así transmitidas se contestan en un máximo de 48h.

### 4.5 Comprobar que la firma electrónica se ha instalado correctamente en el navegador:

<http://www.accv.es/ayuda/comprobacion-de-la-firma-electronica/>



A través de este formulario puede comprobar que sus **certificados son válidos**, que están **registrados correctamente en su navegador** y que **realiza la firma electrónica correctamente**.

Recuerde que previamente debe [instalar los certificados de la Autoritat de Certificació de la Comunitat Valenciana](#) y sus [certificados de usuario](#).

Introduzca el texto a firmar:

**Firmar y Enviar** >

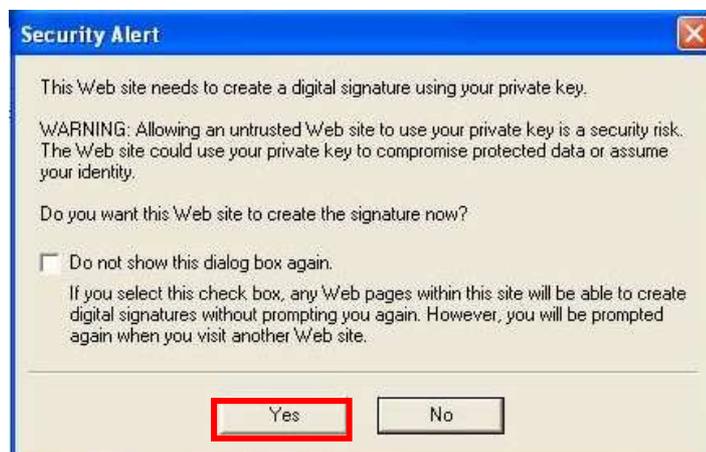
**AVISO:** Si sus certificados son en **fichero** y durante el registro definió una contraseña del sistema, a continuación deberá introducirla. Si no la definió, pulse **Aceptar**.

Introducir un texto (por ejemplo: prueba) y seleccionar '**Firmar y Enviar**':



Seleccionar el certificado de la lista (si la lista aparece vacía, remitir al usuario a la página: <http://www.accv.es/ayuda/manuales-de-instalacion/> *Guías de instalación de la tarjeta criptográfica y el lector*).

En la alerta de seguridad que aparece, seleccionar **Yes**.



Introducir el **PIN** de la tarjeta criptográfica:



Comprobar que se ha verificado la firma:

**Comprobación de la firma electrónica**

La firma del formulario se ha verificado con éxito.

**Datos del firmante:**

Nombre: [REDACTED]

NIF/NIE: [REDACTED]

**Datos del certificado:**  
EL CERTIFICADO ESTÁ REVOCADO.  
Emitido por: ACCV-CA2  
Fecha de emisión: Jueves, 29 Abril 09:39:23 CEST 2010  
Fecha de caducidad: Domingo, 28 Abril 09:49:23 CEST 2013  
Número de Serie: [REDACTED]  
Algoritmo de Firma: SHA256 con RSA

## 5 Anexo II: Instalación de la máquina virtual de java

- Acceder a la URL: \_

<http://www.oracle.com/technetwork/java/javase/downloads/java-archive-javase8-2177648.html>

- Buscamos la opción **Java SE Runtime Environment 8u101**

### Java SE Runtime Environment 8u101

You must accept the [Oracle Binary Code License Agreement for Java SE](#) to download this software.

Accept License Agreement  Decline License Agreement

Product / File Description	File Size	Download
Linux x86	54.79 MB	<a href="#">jre-8u101-linux-i586.rpm</a>
Linux x86	70.58 MB	<a href="#">jre-8u101-linux-i586.tar.gz</a>
Linux x64	52.68 MB	<a href="#">jre-8u101-linux-x64.rpm</a>
Linux x64	68.49 MB	<a href="#">jre-8u101-linux-x64.tar.gz</a>
Mac OS X	64.32 MB	<a href="#">jre-8u101-macosx-x64.dmg</a>
Mac OS X	55.99 MB	<a href="#">jre-8u101-macosx-x64.tar.gz</a>
Solaris SPARC 64-bit	52 MB	<a href="#">jre-8u101-solaris-sparcv9.tar.gz</a>
Solaris x64	49.85 MB	<a href="#">jre-8u101-solaris-x64.tar.gz</a>
Windows x86 Online	0.71 MB	<a href="#">jre-8u101-windows-i586.iftw.exe</a>
Windows x86	59.42 MB	<a href="#">jre-8u101-windows-i586.tar.gz</a>
Windows x64	59.17 MB	<a href="#">jre-8u101-windows-x64.exe</a>
Windows x86 Offline	52.63 MB	<a href="#">jre-8u101-windows-i586.exe</a>
Windows x64	62.77 MB	<a href="#">jre-8u101-windows-x64.tar.gz</a>

[Back to top](#)

- Aceptar la licencia y descargar la versión
- Solicitará que el usuario se inscriba para comenzar la descarga:

ORACLE

### Inicio de sesión

Nombre de usuario

Contraseña

[¿No tiene una cuenta en Oracle?](#)  
[Inscríbese](#) en una cuenta de Oracle Web gratuita

[¿Necesita ayuda?](#)

Powered by Oracle Access Manager 11g

Este sitio ha sido creado para el uso exclusivo de usuarios autorizados de Oracle. El uso de este sitio está sujeto a los Avisos Legales, las Condiciones de Uso y la Declaración de Privacidad publicadas en el sitio. El uso del sitio por parte de clientes y partners autorizados también está sujeto a las condiciones de su(s) contrato(s) con Oracle. El uso de este sitio por parte de los empleados de Oracle también está sujeto a las políticas de la empresa, incluido el Código de Conducta. El acceso no autorizado o el incumplimiento de estas condiciones puede dar lugar a la cancelación de su permiso para utilizar el sitio y/o a las acciones legales pertinentes.