

Instrucciones para la configuración del acceso a SIA-GAIA

Configuración hardware del puesto.

- Configuración mínima del PC:
 - Procesador Intel® Pentium Dual Core
 - 2 Gb de memoria RAM
 - Teclado con lector Tarjeta CHIP + Banda Magnética. El lector de tarjeta chip es necesario para leer el certificado en tarjeta para la identificación del usuario que accede al sistema y la firma digital de los actos médicos. El lector de banda se utiliza para la lectura de las tarjetas SIP. El sistema sólo permite acceder introduciendo por teclado el nº SIP del paciente un nº limitado de veces.
 - Adaptador de red.
 - Windows XP Professional con Service Pack 3.
 - Internet Explorer 6 ó 7. Cualquier referencia en la documentación anexa a IE6 será extensible a IE7.
- Impresora local, compartida o de red. Deberá disponer de dos bandejas más una manual. Como por ejemplo la: Brother 5350DNLT, Brother HL-5150D, Brother HL-5250DN, Brother HL-6050D/DN, Epson LQ-850... Puede estar conectada como local, de red o compartida. Ver **Anexo3.- Configuración de la impresora del puesto de trabajo**
- **Acceso a Internet desde el puesto.**

Configuración software de los PC's.

- Instalación de los certificados de la ACCV (Root CA.crt, ACCV-CA1.crt y ACCV-CA2.crt) Si desea instalar para un usuario concreto basta con hacer doble click sobre el archivo del certificado y aceptar las opciones por defecto presentadas hasta finalizar su instalación. Para instalar los certificados en una estación de trabajo y **permitir que el certificado esté disponible para cualquier usuario** seguir el procedimiento indicado en **Anexo 1.- Instalación de certificados**.
- Instalación del driver de la tarjeta. Descargar el instalador de:
http://www.accv.es/fileadmin/Archivos/software/Siemens-Microsoft_Windows.zip

Tras la instalación puede aparecer un mensaje cada vez que se inicie sesión solicitando una modificación del registro:

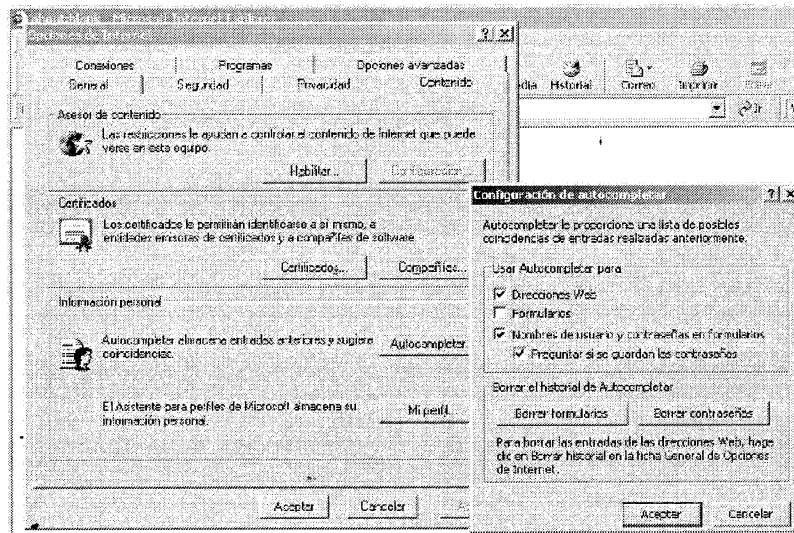
The Microsoft build-in certificate propagation is currently enabled.
It is not recommended to use the Microsoft build-in propagation an CardOS API propagation in parallel.
Microsoft build-in propagation can be disabled by setting
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\ScCertProp\Enabled\nto0.
Continue anyway? Si - No

Para solucionarlo se puede modificar la entrada indicada del registro (Inicio-> Ejecutar -> regedit) o bien ejecutar desde la línea de comando: (Inicio -> Ejecutar -> cmd) el comando:

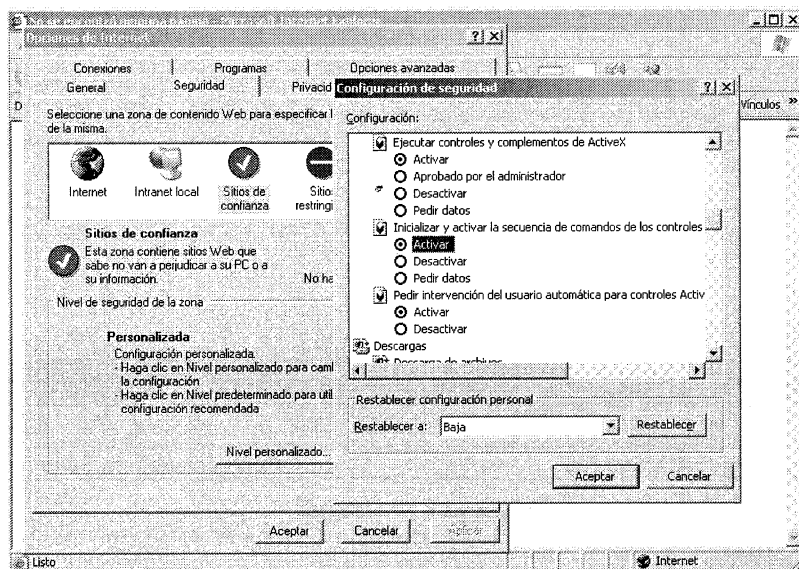
```
REG ADD "HKLM\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\Notify\ScCertProp" /V Enabled /T REG_DWORD /D 0 /F
```

- Instalación y configuración de la última versión de máquina virtual de Java homologada por la CS/AVS (Actualmente es la JRE 1.5.0_11 y hay que instalarla en C:\Archivos de Programa) Seguir procedimiento según el **Anexo 2.- Procedimiento manual de configuración de la plataforma JRE versión 1.5 en puestos de trabajo**
- Instalar las librerías de Firma Digital. Para ello es necesario copiar la librería capicom.dll al directorio c:\windows\system32\ y registrarla mediante el comando *regsvr32.exe*.
- Instalación de Acrobat Reader 9.
- Instalación del Adobe Flash Player 10.1

- Configuración de Internet Explorer para cada perfil de usuario que utilice el puesto con las siguientes características:
 - En Herramientas → Opciones de Internet → Contenido, en el apartado de Configuración personal, sobre el botón Autocompletar, desmarcar Formularios



- En la pestaña Seguridad, en Sitios de confianza > Nivel personalizado > Controles y complementos de ActiveX > Inicializar y activar la secuencia de comandos de los controles ActiveX no marcados como seguros, marcar la opción Activar.



- En el menú Archivo > Configurar página borrar lo que hay en los campos Encabezado y Pie de página y poner 11 mm en los márgenes Izquierdo y Derecho.

Anexo 1.- Instalación de certificados.

En este documento se detalla el procedimiento a seguir para la renovación de los certificados necesarios para utilizar las aplicaciones con firma electrónica. Se contempla la importación de certificados para Internet Explorer.

Instalación certificados en Internet Explorer

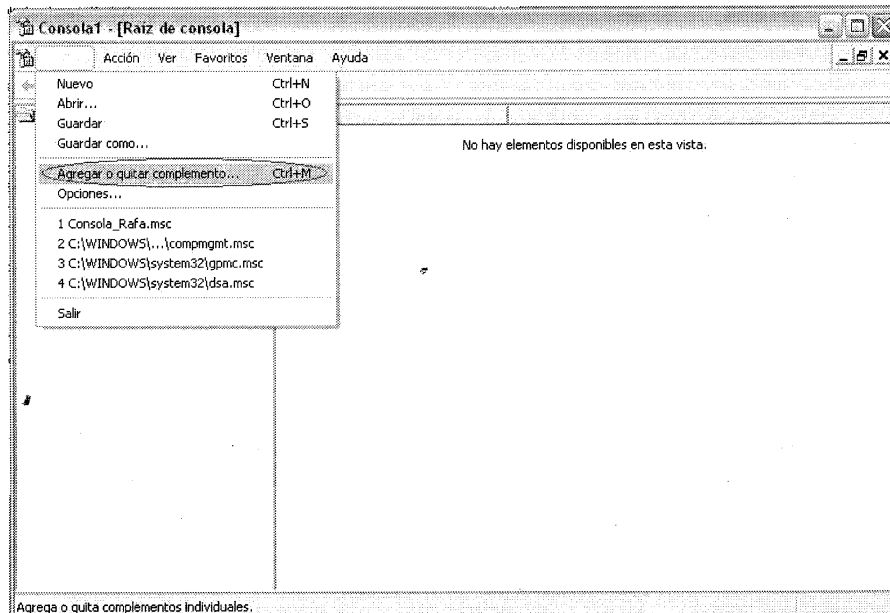
La instalación de los certificados: **RootCA** (Certificado de la Autoridad de Certificación Raíz), **ACCV-CA1** (Certificado de la Autoridad de Certificación de certificados para personas jurídicas) y **ACCV-CA2** (Autoridad de Certificación de certificados para personas físicas y otros usos) en Internet Explorer, se realiza desde la consola de administración siguiendo los siguientes pasos.

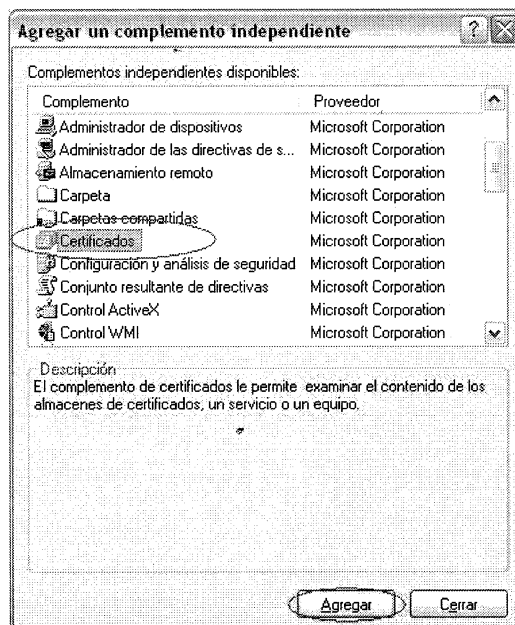
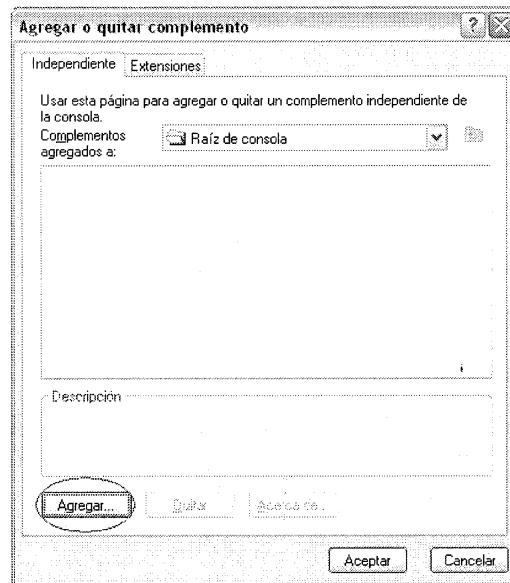
Para instalar los certificados en una estación de trabajo y **permitir que el certificado esté disponible para cualquier usuario** que inicie sesión en el equipo, se ha de utilizar la consola MMC e importar los certificados en **la cuenta de equipo**.

El primer paso a seguir es ejecutar la consola de administración para poder gestionar los certificados del equipo

Ir a Inicio-Ejecutar y escribir mmc con un usuario administrador local.

Archivo, Agregar o quitar complemento...





Complemento de certificados

Este complemento administrará siempre certificados de:

Mi cuenta de usuario

Cuenta de servicio

Cuenta de equipo

< Atrás Siguiete > Cancelar

Seleccionar equipo

Seleccione el equipo que desea que administre este complemento.

Este componente administrará siempre:

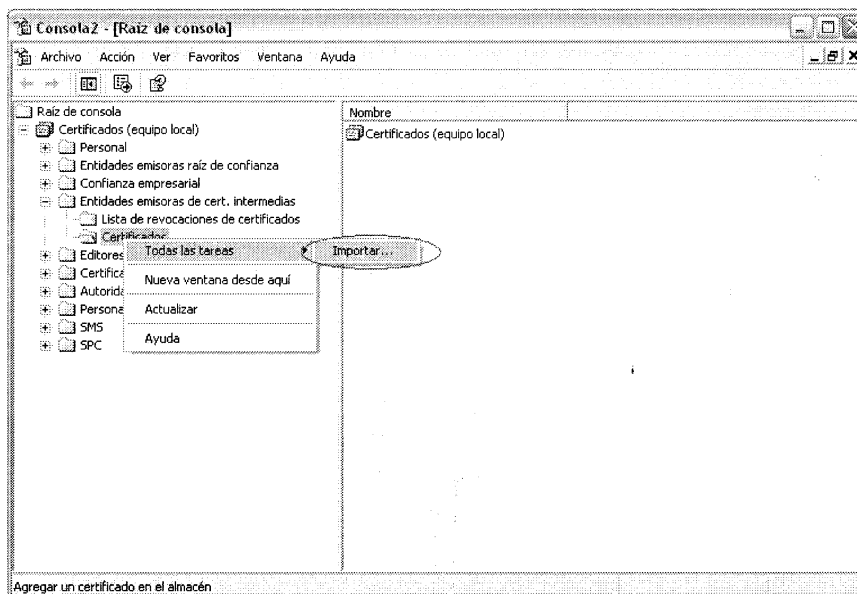
Equipo local: (el equipo en el que se está ejecutando esta consola)

Otro equipo: Examinar...

Permitir cambiar el equipo seleccionado al iniciar desde la línea de comandos. Esto sólo es aplicable si ha guardado la consola.

< Atrás Finalizar Cancelar

Una vez tenemos la consola de administración lista para gestionar los certificados, pasamos a la importación de los mismos:



Nota: estos certificados tienen que ser importados como "Certificados de entidades emisoras de cert. intermedias".

Una vez dentro del Asistente de importación de certificados, hay que seguir los siguientes pasos:



Asistente para importación de certificados

Archivo para importar
Especifique el archivo que desea importar.

Nombre de archivo:

Nota: se puede almacenar más de un certificado en un mismo archivo en los siguientes formatos:

- Intercambio de información personal: PKCS #12 (.PFX, .P12)
- Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)
- Almacén de certificados en serie de Microsoft (.SST)

< Atrás Siguiente > Cancelar

En *Nombre de archivo* hay que poner la ruta completa de la ubicación del archivo que contiene el certificado.

Asistente para importación de certificados

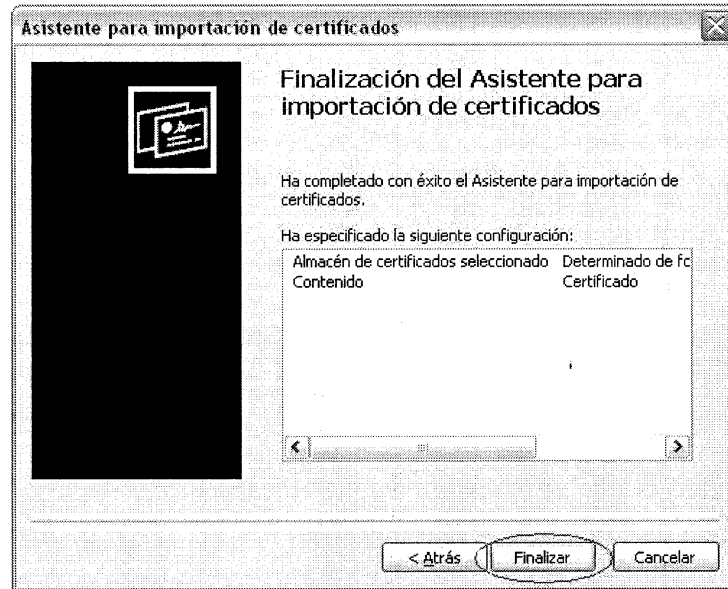
Almacén de certificados
Los almacenes de certificados son áreas del sistema donde se guardan los certificados.

Windows puede seleccionar automáticamente un almacén de certificados, o bien es posible especificar una ubicación para el certificado.

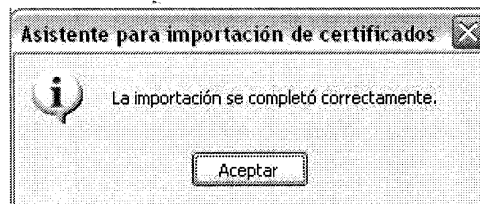
- Seleccionar automáticamente el almacén de certificados en base al tipo de certificado
- Colocar todos los certificados en el siguiente almacén:

Almacén de certificados:

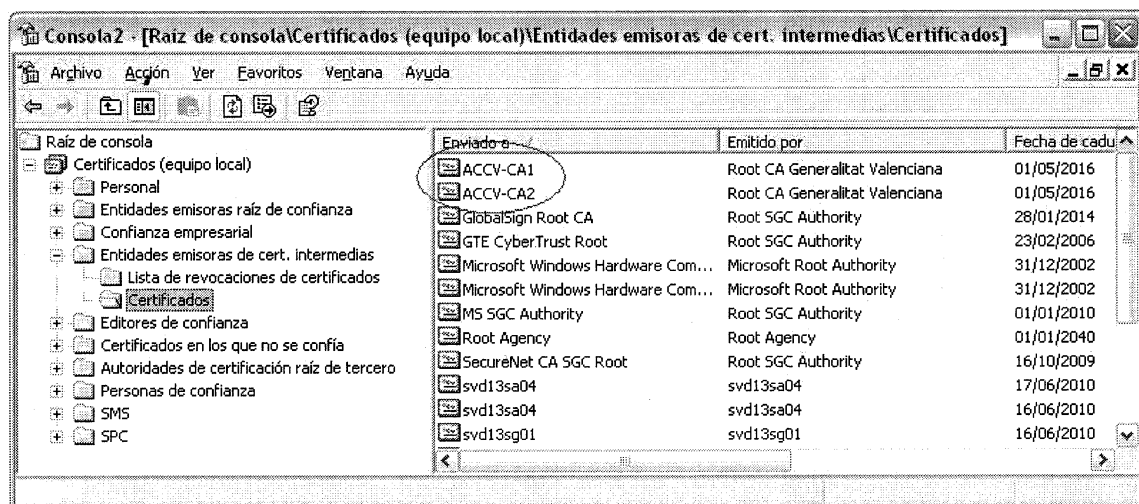
< Atrás Siguiente > Cancelar



Si la importación se realizó con éxito, se abrirá la siguiente ventana:

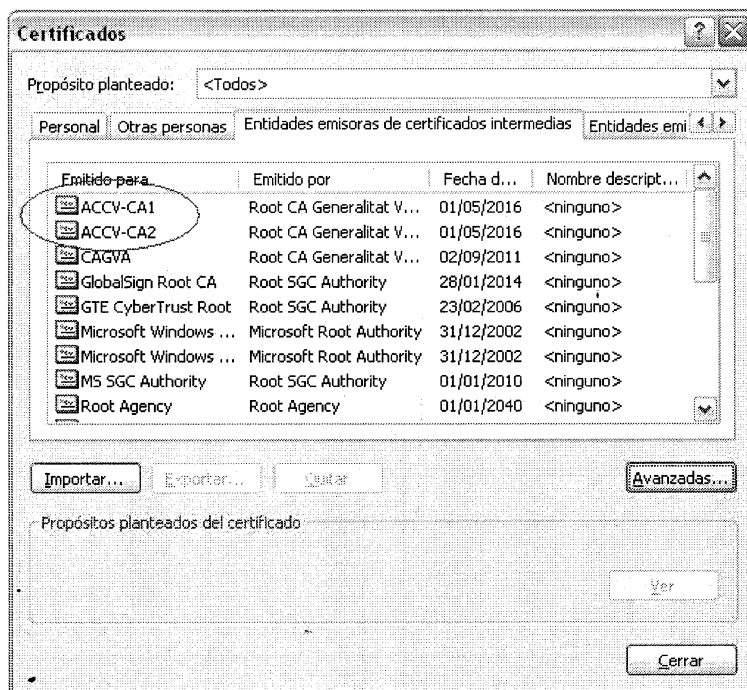


Estos pasos se tienen que realizar para cada uno de los certificados. Finalmente, comprobamos desde la consola que los certificados se han instalado correctamente en *Entidades emisoras de cert. Intermedias, Certificados*, tal y como muestra la siguiente figura:



También podemos comprobar en Internet Explorer que los certificados se han importado correctamente, desde *Herramientas, Opciones de Internet, Contenido, Certificados*,

Entidades emisoras de certificados intermedias, tal y como muestra la siguiente imagen:



Anexo 2.- Procedimiento manual de configuración de la plataforma JRE versión 1.5 en puestos de trabajo

Este anexo muestra como instalar y configurar la máquina JRE de la familia 1.5.0_11 para poder trabajar con las aplicaciones corporativas.

Instalación manual de la máquina JRE versión 1.5

La versión de la familia 1.5 consensuada con la Conselleria de Sanidad es la JRE 1.5.0_11. Para la instalación manual de esta plataforma se seguirán los siguientes pasos:

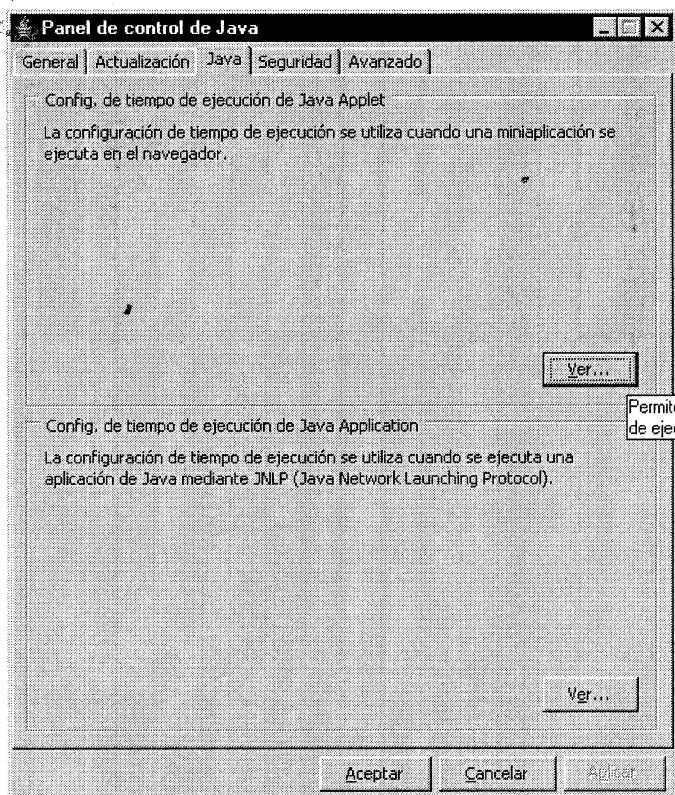
1. Como paso previo hay que verificar qué aplicaciones del puesto a instalar utilizan la máquina virtual de Java

Nota: Este paso es necesario ya que existen aplicaciones NO corporativas como el visor PACS que utilizan Java y NO están homologadas para la familia 1.5.

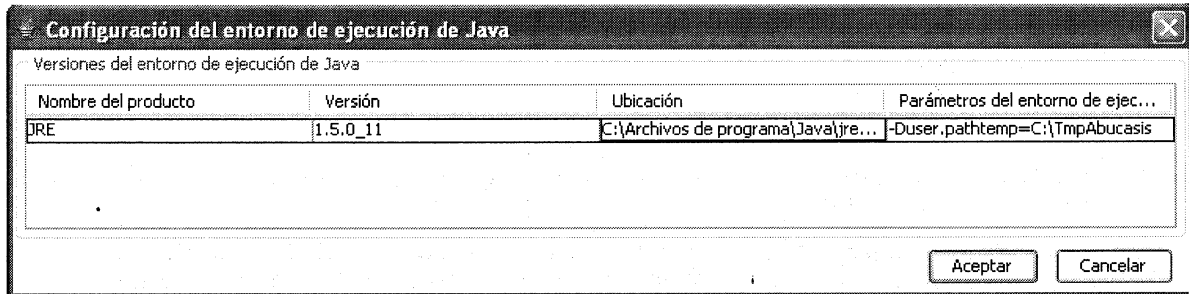
2. Instalar la máquina java **JRE 1.5.0_11** (a descargar desde el centro de descargas de SUN) desde una cuenta con privilegios de administrador.

Ir a la ruta **C: | Documents and Settings | Administrador | Datos de programa | Sun | Java | Deployment** y renombrar el fichero **deployment.properties** a **deployment.properties.old**.

4. Abrir la consola de java desde el panel de control y entrar a al pestaña **java** → **config. de tiempos de ejecución de java applet** y pulsar en la opción **Ver**.

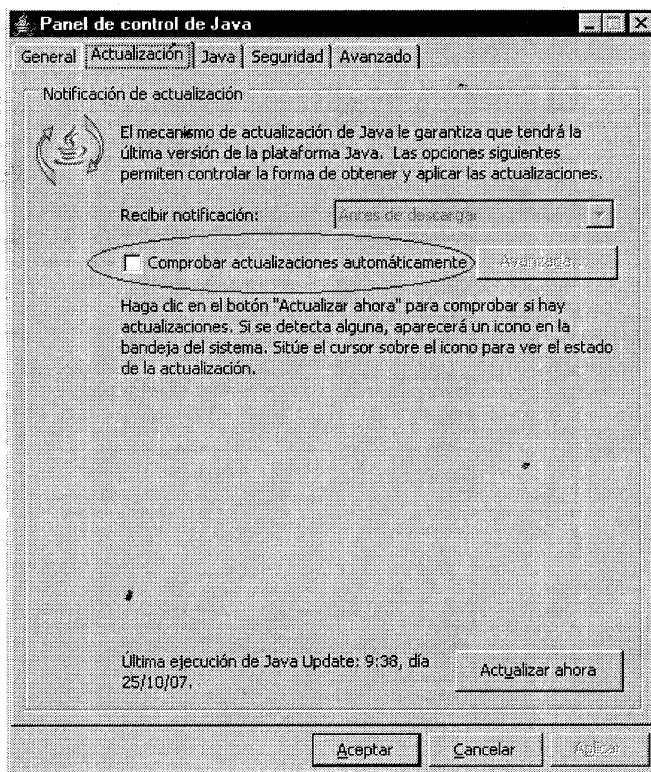


En la columna **Parámetros del entorno de ejec...** escribir: -
Duser.pathtemp=c:\TmpAbucasis.

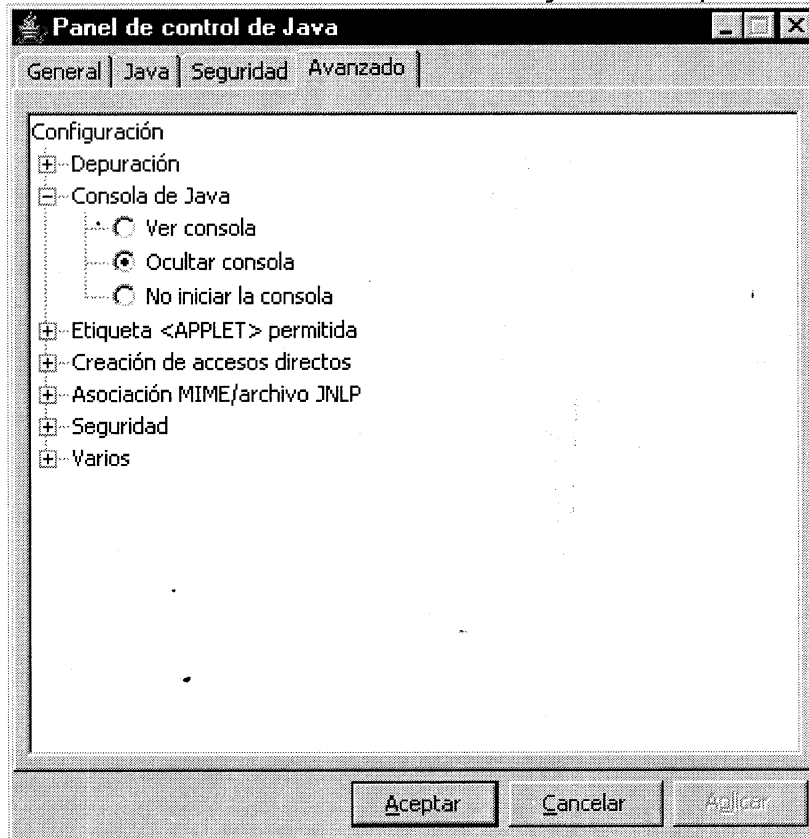


Deberemos crear dicha carpeta en el PC. Además copiaremos sobre ella el archivo de fuentes: **abucasis.ttf**.

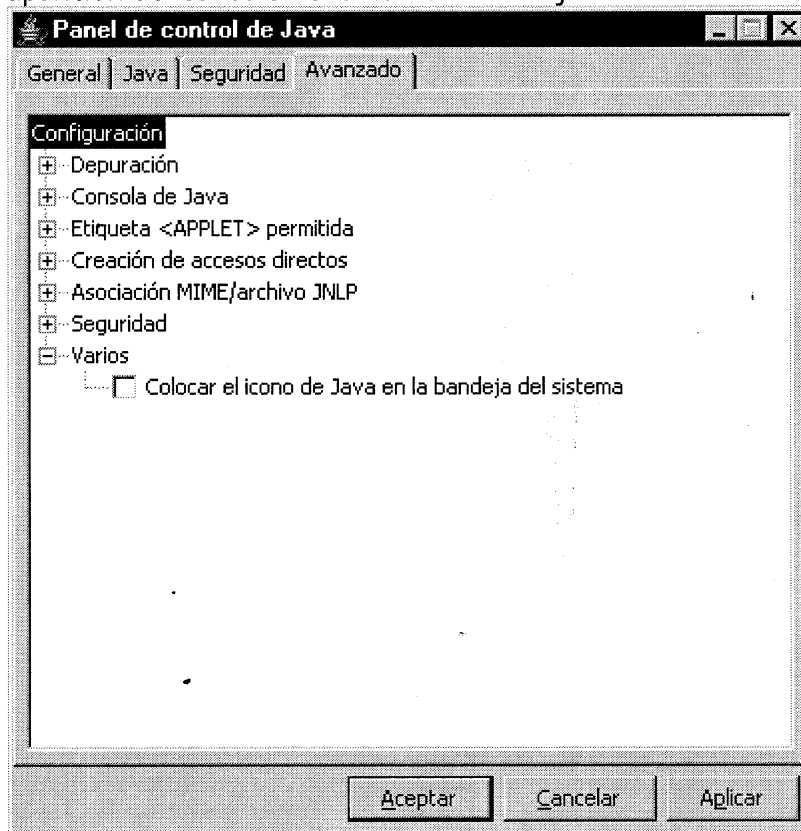
5. En la pestaña de **actualización** desmarcar la comprobación automática de descarga de actualizaciones.



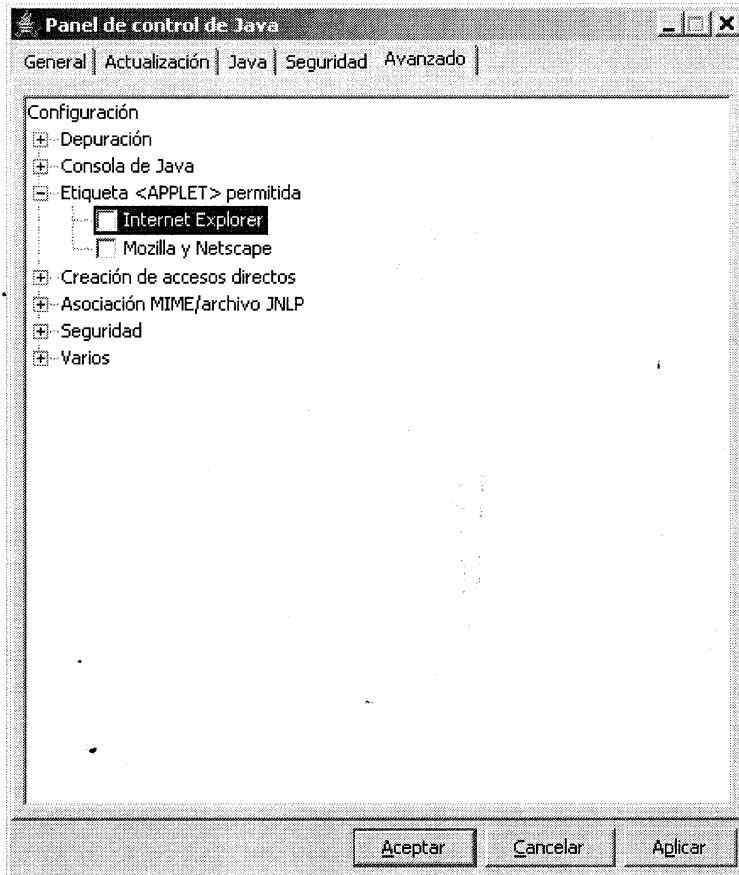
6. Activar el check de ocultar consola, para evitar que la consola de java se abra automáticamente a los usuarios cuando ejecuten la aplicación.



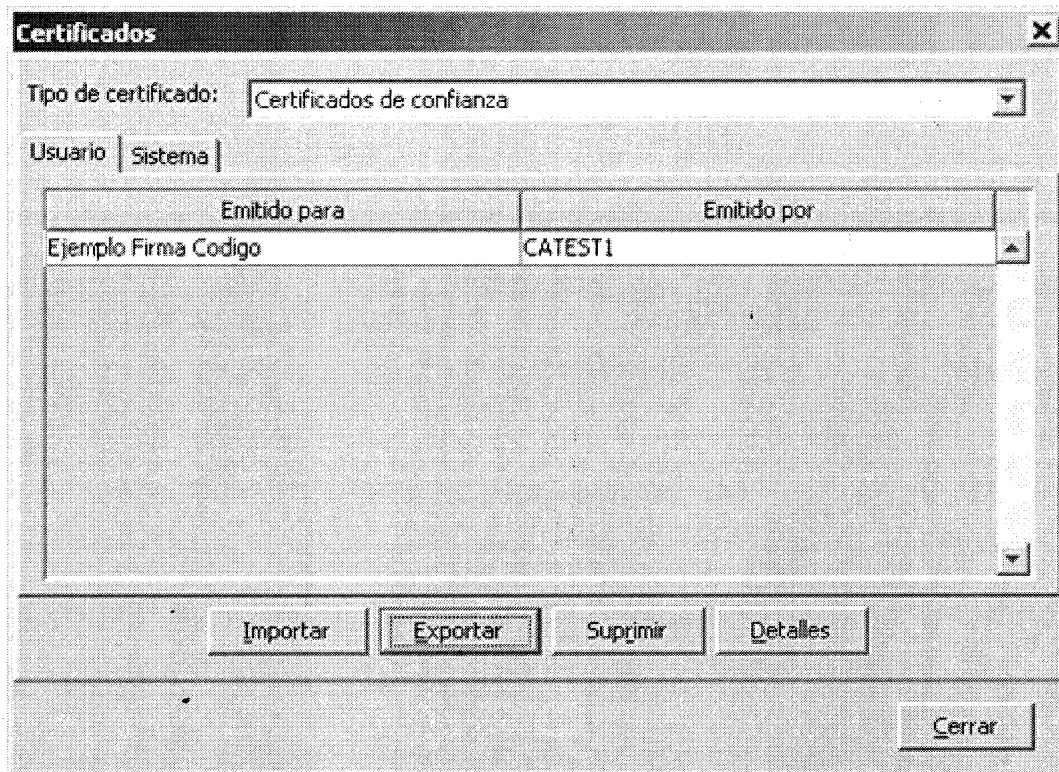
7. Desactivar el check de colocar un icono de java en la bandeja del sistema para evitar la aparición de iconos en el entorno de trabajo del usuario.



8. Deshabilitar la opción de Internet Explorer de **Etiqueta <APPLET> permitida:**



9. Importar el archivo **Ejemplo Firma Codigo** desde Java Plugin de la JRE 1.5.0_11.



10. Copiar la carpeta **C:\Documents and Settings\UsuarioAdministrador\Datos de programa\Sun** a la ruta **C:\Documents and Settings\Default user\Datos de programa**. Consiguimos que cualquier usuario nuevo que no ha iniciado sesión en el puesto coja las propiedades del **Default User**.

Si queremos que estas propiedades se apliquen a usuarios que ya habían iniciado sesión habría que copiar la carpeta sobre cada perfil local en **C:\documents and settings**.

Nota: El fichero **deployment.properties** define las propiedades que hay definidas en Panel de Control-Java Plugin en un fichero.

11. Copia del fichero actualizado de políticas **Java.policy** en la ruta → C:\Archivos de Programa\java\jre_1.5.0_11\lib\security
12. Copia del fichero almacén de certificados **cacerts** en la ruta → C:\Archivos de Programa\java\jre_1.5.0_11\lib\security

Anexo 3.- Configuración de la impresora del puesto de trabajo

En este anexo detallaremos la configuración de la impresora del puesto de trabajo que podrá estar conectada como impresora local, compartida o de red. Deberá disponer de dos bandejas más una manual. La primera, que denominaremos "ARRIBA", apuntará a la primera de las bandejas donde se colocarán las recetas verdes. La segunda, denominada "ABAJO", apuntará a la segunda bandeja y contendrá las recetas rojas. La tercera, con el nombre "MANUAL", apuntará a la bandeja manual donde se situaran las recetas sin financiación y papel blanco para cualquier tipo de informe.

En primer lugar procederemos a la instalación de la impresora con sus drivers. A continuación, procederemos a definir tres impresoras sobre el puerto en el que tengamos definida la impresora, cada una con un nombre determinado con un origen de papel diferente. Por último, se elegirá la impresora predeterminada y se limpiará cualquier otra impresora que se pueda haber creado de forma automática (Plug&Play).

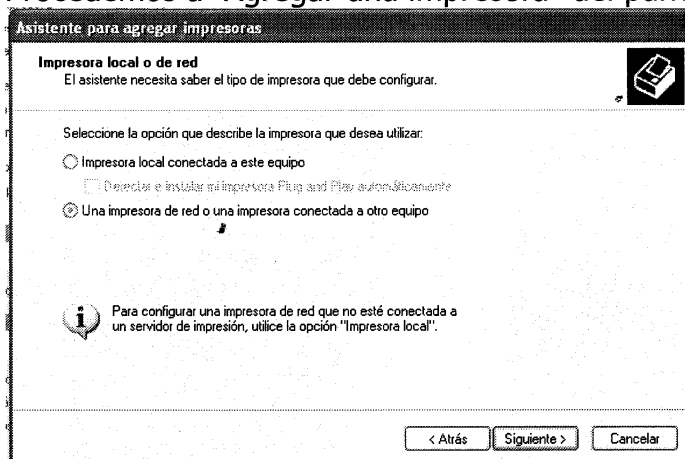
Instalación de la impresora y sus drivers.

No se detalla este apartado ya que dependerá del modelo seleccionado y del tipo de conexión empleado.

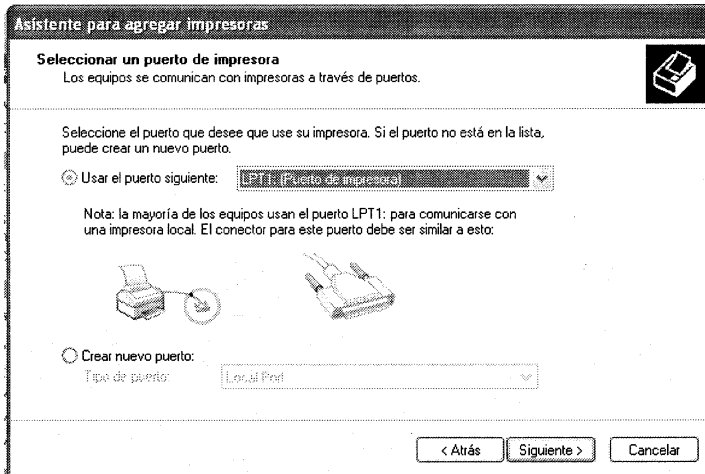
Definición de las tres impresoras de trabajo.

Tendremos que definir ahora tres impresoras denominadas "ARRIBA", "ABAJO" y "MANUAL" que compartan el mismo puerto, el definido en el paso anterior, y que ataquen a cada una de las bandejas de la impresora.

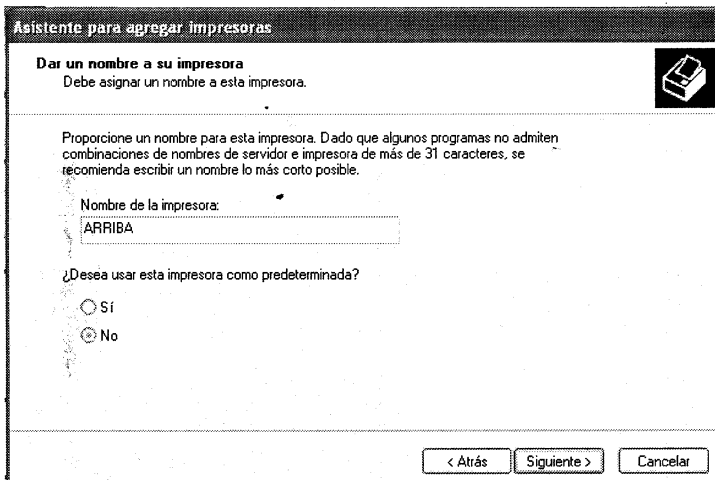
Procedemos a "Agregar una impresora" del panel de "Impresoras y faxes".



Si la impresora es local o de red, seleccionamos de la lista el puerto definido en el apartado anterior. Si la impresora es local, será un puerto de tipo "Virtual printer for USB" y si es de red, será de tipo "Standard TCP/IP Port".



En caso de ser compartida, deberemos buscar el equipo que la sirve y seleccionarla. Deberemos renombrarla como "ARRIBA".



A continuación, seleccionamos la impresora recién definida, "ARRIBA", y accedemos a "propiedades", "Opciones avanzadas", "Valores predeterminados de impresión". Buscamos y cambiamos el "origen/fuente del papel" a la primera de las bandejas. Repetimos el proceso para las otras impresoras, "ABAJO" y "MANUAL" haciendo que el origen del papel de cada una de ellas sea la segunda bandeja y la manual por este orden.

Selección de la impresora predeterminada.

Por último, MUY IMPORTANTE, seleccionaremos la impresora "MANUAL" como la predeterminada.

Si la impresora es local, también procederemos a eliminar la impresora "Plug & Play" que se pudiera haber instalado de forma automática al conectarla.

El aspecto final del panel de impresoras debería ser:

