INSTRUCCIONES PARA EL USO DE LA FIRMA ELECTRÓNICA EN LA SEDE ELECTRÓNICA DE LA AGENCIA ESTATAL DE SEGURIDAD AÉREA

Novedades

A partir del miércoles 8 de marzo de 2017, las aplicaciones de la Sede Electrónica que requieran el uso de firma electrónica podrán comenzar a utilizar el programa AutoFirma, como complemento del MiniApplet de @firma.

Se trata de un software que forma parte de la suite de @firma, y que se ejecuta en el equipo del usuario, permitiéndole la firma en las aplicaciones de la Sede Electrónica sin necesidad de que el navegador soporte la interfaz NPAPI. Ahora bien, a diferencia del MiniApplet, requiere la instalación previa del mismo para su uso.

Conviene tener presente que ambos programas pueden convivir en el mismo equipo, e incluso es posible que durante el uso de la Sede Electrónica se utilice uno u otro, en función del sistema operativo y navegador utilizado, y la instalación de AutoFirma. Esto no supone problema alguno, y las operaciones de identificación y firma se realizarán con la misma validez empleando cualquiera de los dos programas.

La versión recomendada de AutoFirma para el uso con la Sede Electrónica es la versión 1.5.

Requisitos técnicos del programa AutoFirma de @firma

El programa AutoFirma de @firma requiere la instalación previa del mismo para su uso. La última versión del instalador puede descargarse en la página web de @firma:

http://firmaelectronica.gob.es/Home/Descargas.html

En el material descargado se incluye un manual de instalación, con los detalles y características a tener en cuenta. Recuerde que para la instalación del mismo, es necesario contar con permisos de administrador del equipo en el que se quiere instalar.

A continuación le mostramos una lista de los navegadores de uso habitual y su compatibilidad:

- Microsoft Internet Explorer.

  Actualmente no se soporta. Se debe utilizar el MiniApplet de @firma

- Microsoft Edge.

  Actualmente no se soporta

- Google Chrome

  Se requiere el uso de la versión 46 o superior.

- Mozilla Firefox

CORREO ELECTRÓNICO:
cau.aesa@seguridadaerea.es

www.seguridadaerea.gob.es

AVDA. GENERAL PERÓN, 40 1ª planta
28020 MADRID
TEL: +34 91 396 8000
FAX: +34 91 770 5459

Se requiere el uso de la versión 41.0.1 o superior.

- Apple Safari

  Actualmente no se soporta

AutoFirma funciona en los sistemas operativos Microsoft Windows, Apple OS X y Linux. La versión concreta de cada uno depende también de que permitan ejecutar el navegador, la máquina Java y el software adicional que necesite para el certificado. En principio, es posible utilizarlo en los siguientes sistemas:

- Microsoft Windows 7 SP1 o superior.
- Apple OS X 10.11 o superior.
- Linux: soportado con Guadalinex y Ubuntu

AutoFirma requiere disponer de un entorno de ejecución de Java instalado en el sistema operativo Linux. Para el resto de sistemas operativos, AutoFirma dispone de su propia máquina virtual. Las versiones soportadas de la máquina virtual son:

- Oracle Java 8
- OpenJDK 8

El certificado electrónico que utilice para la firma ha de permitir realizar firmas electrónicas empleando los algoritmos SHA-2 y RSA. Si dispone de certificado en tarjeta criptográfica (por ejemplo, DNI electrónico o tarjeta criptográfica de la FNMT), debe asegurarse que tiene instalado en su equipo una versión del software que soporte los algoritmos anteriores.

- DNIe: soporta los algoritmos a partir de la versión 2.0
- FNMT: soporta los algoritmos a partir de la versión CERES v11.0.0 y TC-FNMT 2.0.0

Instalación de AutoFirma de @firma

La instalación de AutoFirma de @firma viene detallada en el manual de instalación que se facilita con el programa ejecutable. Se incluye en este apartado un breve resumen de los pasos a seguir para su instalación en Windows. En el manual de instalación puede encontrar más información, así como los pasos a seguir para instalarlo en otros sistemas operativos.

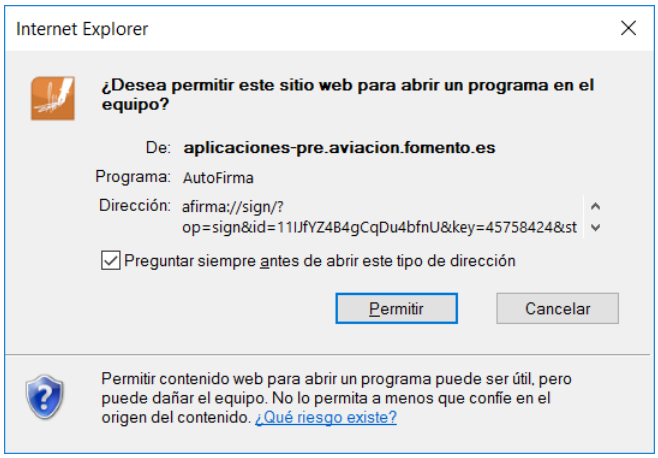
- **Proceso de instalación en Windows:**
  - Se requiere disponer de permisos de administrador en el equipo donde se va a llevar a cabo la instalación.
  - Ejecutar el fichero ejecutable de instalación (".exe"). Se iniciará un asistente que irá solicitando confirmación de los distintos pasos y selección de ruta donde instalar el programa, aunque recomendamos la ruta por defecto. Una vez escoja la ruta de instalación, pulse el botón "Instalar".
  - El programa mostrará el avance del proceso de instalación e indicará cuando haya terminado. Pulse sobre el botón "Terminar" para finalizar la instalación.

- **Una vez instalado**:
    - Cuando el programa AutoFirma de @firma se ejecute, es posible que la máquina virtual de Java que contiene solicite permisos de acceso a Internet. Se deberá conceder para que funcione correctamente.

Uso de AutoFirma

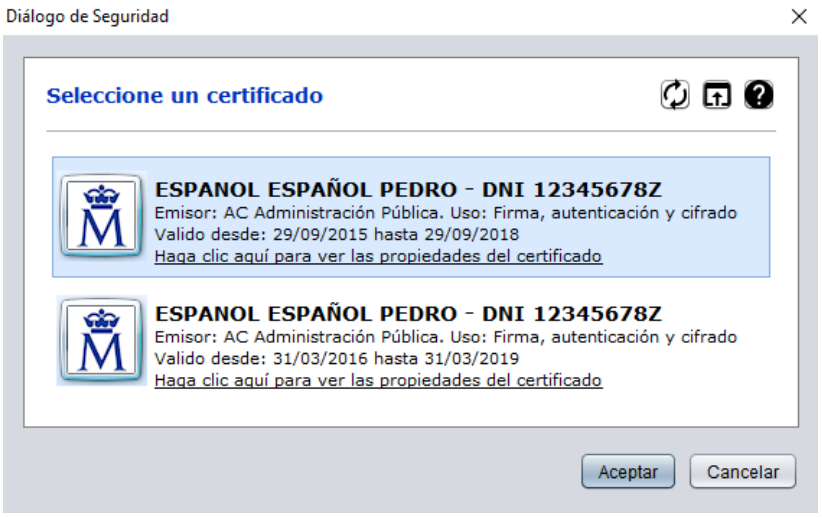
AutoFirma requiere ser instalado previamente en el equipo que vaya a ser utilizado.

Por defecto, dependiendo del navegador le preguntará con qué aplicación desea ejecutar el enlace o bien si permite la ejecución del enlace. En cada caso, debe seleccionarlo y permitirlo para poder continuar.



- Si pulsa “Cancelar” no se podrá ejecutar el componente de firma electrónica y no podrá operar con la Sede Electrónica.

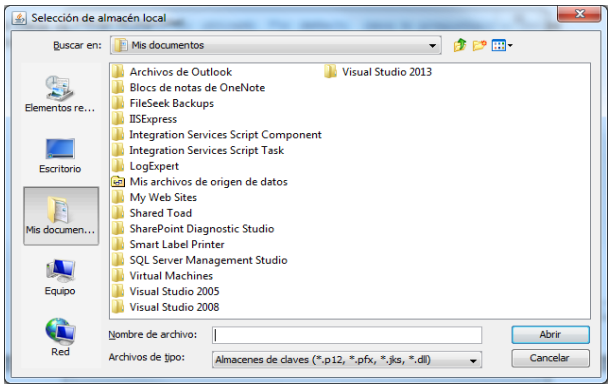
Una vez permitido, cuando vaya a llevar a cabo el proceso de firma electrónica mediante certificado al pulsar el botón “Acceder con certificado” o “Firmar”, se le mostrará un diálogo con los certificados disponibles en su equipo.



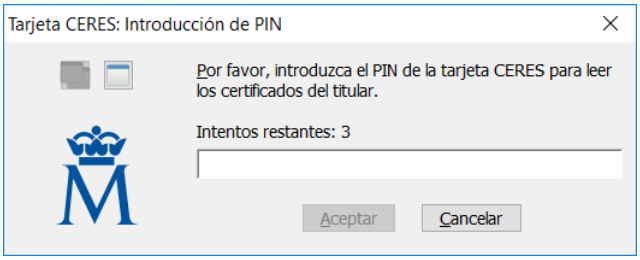
Una vez escogido el certificado, pulse el botón “Aceptar” para llevar a cabo la firma electrónica. Asegúrese que el certificado escogido no está caducado ni ha sido revocado; en caso contrario se rechazará la firma electrónica:

- Si dispone de certificado en tarjeta criptográfica, y no lo ha introducido en el lector previamente, puede realizarlo en este momento y pulsar el botón “Actualizar” para que cargue nuevamente la lista de certificados disponibles.

- Si dispone de un almacén de claves externas, puede cargarlo a través del botón “Cargar”.



En caso de que sea necesario, el programa le solicitará la contraseña necesaria para realizar la firma.

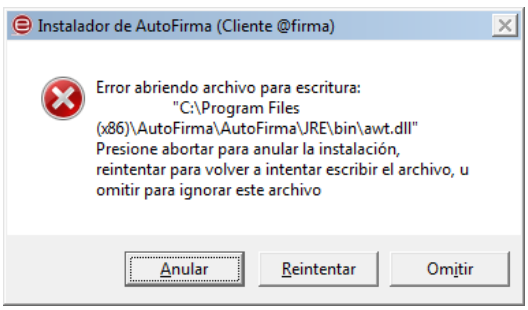


Problemas conocidos relacionados con AutoFirma de @firma

Existe una serie de problemas identificados relacionados con la instalación de AutoFirma de @firma, que se enumeran a continuación:

- “**Al instalar AutoFirma falla la instalación de los certificados de confianza SSL**: AutoFirma requiere permisos de administrador para ser instalado y para insertar el certificado de confianza SSL para el funcionamiento de la firma en los trámites online. Si no puede instalar AutoFirma o el certificado de confianza, solicite al administrador de su sistema que realice la instalación de la aplicación.

- **Al instalar AutoFirma se muestra el error: “Error abriendo archivo para escritura”**: Es posible que durante la instalación se le muestre un error como el que sigue:



Si ya tenía instalado el programa AutoFirma, compruebe que este no se está ejecutando, en cuyo caso el instalador no podrá sobrescribir los ficheros de instalación. Cierre AutoFirma y pulse el botón reintentar.

Si AutoFirma no se está ejecutando, es posible que el archivo en cuestión se encuentre bloqueado por una ejecución o intento de instalación previo. Reinicie su equipo y pruebe a instalar nuevamente la aplicación.

- **Al abrir Google Chrome después del proceso de instalación de AutoFirma se muestra un mensaje notificando que la configuración de la aplicación está corrupta:** El navegador Google Chrome incluye en su configuración un listado de protocolos que considera seguros para la llamada a aplicaciones externas. Durante el proceso de instalación de AutoFirma se registra el protocolo "afirma" en este listado seguro de Chrome para que las invocaciones desde el navegador se realicen correctamente.

  En algunas situaciones en las que el instalador podría no poder completar el proceso de registro, el fichero de configuración de Chrome podría quedar en un estado inconsistente. En estos casos, al iniciarse de nuevo el navegador, detectará el problema y anunciará al usuario esta corrupción de datos mediante una ventana de advertencia que nos permitirá restaurar las propiedades por defecto.

  Seguidamente, el navegador restaurará las propiedades de configuración y volverá a funcionar normalmente. En este caso, el usuario recibirá mensajes de advertencia al usar AutoFirma desde Chrome para realizar firmas, aunque esto no impedirá que funcione normalmente.

  Durante el proceso de desinstalación de AutoFirma se realiza el proceso inverso al de instalación y se elimina el protocolo "afirma" del listado de protocolos seguros registrados en Chrome. Este proceso podría derivar en algunas circunstancias a la misma corrupción de la configuración del navegador.

- **Cuando se instala Mozilla Firefox o se crea un nuevo perfil de usuario después de la instalación de AutoFirma, este no funciona en Firefox**: Durante el proceso de instalación de AutoFirma se genera un certificado para la comunicación entre la página web y la aplicación, y lo instala en los almacenes de confianza del sistema y de Firefox. Si se crea un perfil de usuario de Firefox o se instala el propio Firefox después de la instalación de AutoFirma, este no contará con el certificado entre los que considera de confianza. Para resolver este problema deberá desinstalar AutoFirma y volverlo a instalar. Tenga en cuenta, sin embargo, que esto implicará que se pierda la configuración personalizada establecida en AutoFirma."

Requisitos técnicos del MiniApplet de @firma

NOTA: Con la puesta en marcha de AutoFirma y la progresiva desaparición del soporte de la interfaz NPAPI en los navegadores, se recomienda la instalación de AutoFirma y su uso de manera preferente.

El MiniApplet @firma requiere el uso del plug-in de Java en su navegador. No todos los navegadores permiten la ejecución de Java o no lo permiten a través de la interfaz NPAPI, por lo que para el uso correcto de las aplicaciones es posible que tenga que utilizar un navegador diferente al que usa habitualmente.

En general, los dispositivos móviles (tabletas, teléfonos, reproductores, etc.) no soportan el plug-in de Java.

A continuación le mostramos una lista de los navegadores de uso habitual y su compatibilidad:

- Microsoft Internet Explorer: soporta Java mediante NPAPI.

Se recomienda el uso de versiones posteriores a la 8 en 32 bits. No es compatible con Internet Explorer 10 o superiores en su versión “Metro”.

- Mozilla Firefox: soporta Java mediante NPAPI en Firefox 4.0 o superior, y hasta la versión 51.

  En sistemas operativos Windows XP o Windows Server 2003, a partir de la versión 9 es necesario tener instalados los entornos de ejecución redistribuibles de Microsoft Visual C++ 2005 y Microsoft Visual C++ 2013 para la carga del almacén de claves y certificados. Si no consigue acceder al almacén necesitará descargarlos e instalarlos como administrador manualmente:

  - Visual Studio 2013, desde el siguiente enlace https://www.microsoft.com/en-us/download/details.aspx?id=40784 seleccionando el idioma y la arquitectura correspondiente para su sistema operativo.

  - Visual Studio 2005, dependiendo de la arquitectura:

    - x86: http://www.microsoft.com/download/en/details.aspx?id=3387

    - x64: http://www.microsoft.com/download/en/details.aspx?id=21254

- Google Chrome: soporta Java hasta la versión 41.

  Las versiones posteriores, a partir de septiembre de 2015, no soportan el interfaz NPAPI.

- Safari: soporta Java en sistemas operativos Mac OS X en Apple Safari 6.2 o superior y no soporta Java en sistemas operativos iOS.

- Microsoft Edge: no soporta Java.

Puede obtener más información al respecto en la web oficial de Java:

https://www.java.com/es/download/faq/index_general.xml

Existen distintas versiones de la máquina virtual Java. Para un uso correcto de la Sede Electrónica de AESA recomendamos utilizar una de las siguientes versiones:

- Oracle Java 6: actualizaciones 45 y posteriores, en arquitectura de 32 bits (x86).

- Oracle Java 7: actualizaciones 55 y posteriores.

- Oracle Java 8: actualizaciones 51 y posteriores. Se recomienda adoptar esta versión.

En los navegadores Internet Explorer y Mozilla Firefox se recomienda la versión de 32 bits en cualquier versión de Java. En los demás navegadores es posible tanto la de 32 (x86) como la de 64 (x64/AMD64) según la arquitectura del navegador a partir de Java 7.

El certificado electrónico que utilice para la firma ha de permitir realizar firmas electrónicas empleando los algoritmos SHA-2 y RSA. Si dispone de certificado en tarjeta criptográfica (por ejemplo, DNI electrónico o tarjeta criptográfica de la FNMT), debe asegurarse que tiene instalado en su equipo una versión del software que soporte los algoritmos anteriores.

- DNIe: soporta los algoritmos a partir de la versión 2.0

- FNMT: soporta los algoritmos a partir de la versión CERES v11.0.0 y TC-FNMT 2.0.0

MiniApplet funciona en los sistemas operativos Microsoft Windows, Apple OS X y Linux. La versión concreta de cada uno depende también de que permitan ejecutar el navegador, la máquina Java y el

software adicional que necesite para el certificado. En principio, es posible utilizarlo en los siguientes sistemas:

- Microsoft Windows: a partir de Windows XP SP3, aunque se recomienda el uso a partir de Windows 7 SP1.
- Microsoft Windows Server: a partir de Windows 2003 R2 SP2.
- Linux: a partir de versiones del kernel 2.6, aunque se recomienda el uso de a partir de versiones del kernel 3 o superior del núcleo.
- Apple OS X: Yosemite (10.10.5 o superior) o el Capitán (10.11.1).

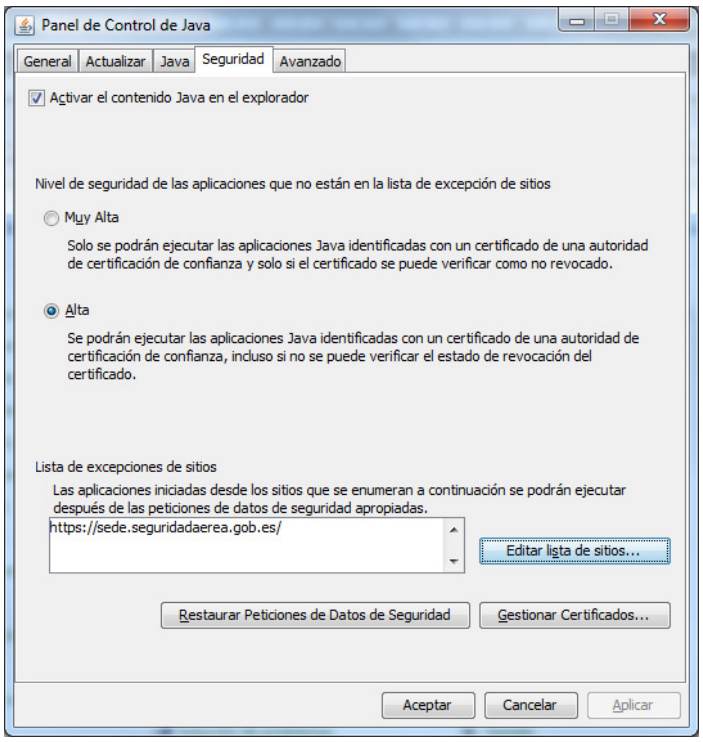
Configuración para el uso del MiniApplet @firma

De cara a utilizar el MiniApplet @firma, es necesario que configure el navegador de la siguiente manera:

- Debe permitir el uso de JavaScript.
- Debe permitir la ejecución de plug-in de Java.
- Debe permitir el acceso a su certificado electrónico.

Consulte la ayuda de su navegador para obtener más información sobre cómo habilitar las opciones anteriores.

Así mismo, es necesario que configure la máquina virtual Java para permitir ejecutarlo como plug-in, y también poder ejecutarlo en la dirección de la Sede Electrónica (https://sede.seguridadaerea.gob.es).



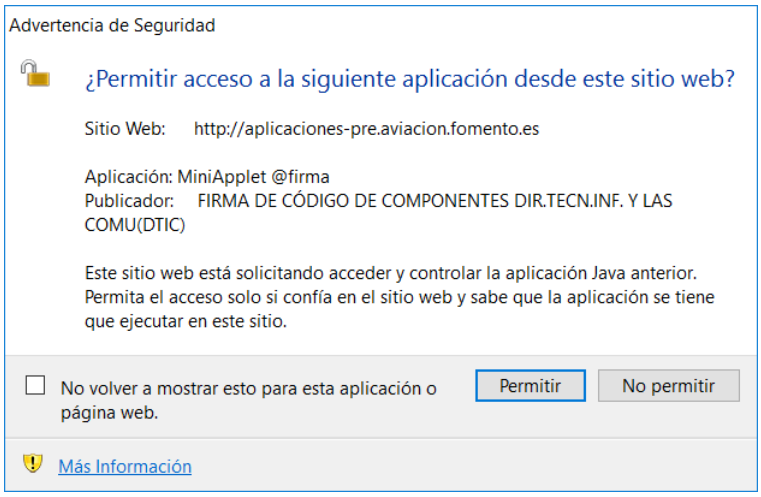
Uso del MiniApplet @firma

El MiniApplet @firma se descargará cada vez que vaya a ser utilizado. Por defecto, Java le preguntará si desea ejecutar la aplicación MiniApplet @firma, para lo cual debe pulsar el botón “Ejecutar”.

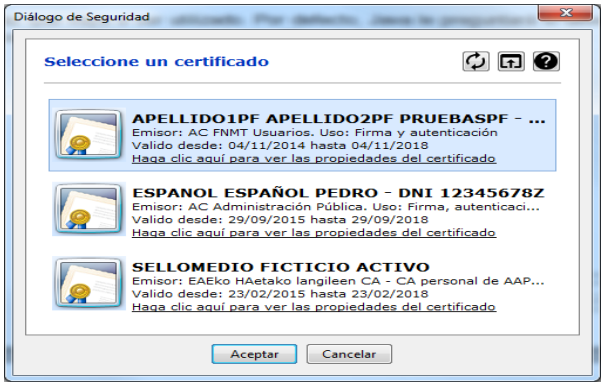
- Antes de pulsar “Ejecutar” puede marcar la casilla “No volver a mostrar…” para que no le efectúe la pregunta en futuras ocasiones.

- Si pulsa “Cancelar” no se podrá ejecutar el componente de firma electrónica y no podrá operar con la Sede Electrónica.

A continuación, es posible que su navegador le pregunte si desea permitir la ejecución de la aplicación @firma en la dirección de la Sede Electrónica (https://sede.seguridadaerea.gob.es), siendo necesario que lo permita para utilizar la firma electrónica.



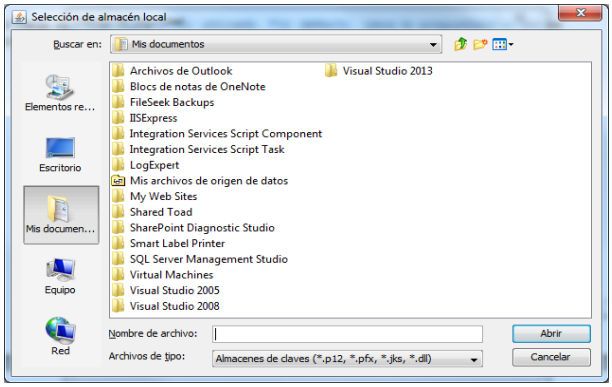
Una vez permitido, cuando vaya a llevar a cabo el proceso de firma electrónica mediante certificado al pulsar el botón “Acceder con certificado” o “Firmar”, se le mostrará un diálogo con los certificados disponibles en su equipo.



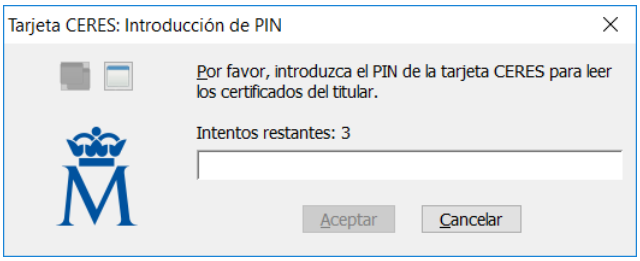
Una vez escogido el certificado, pulse el botón “Aceptar” para llevar a cabo la firma electrónica. Asegúrese que el certificado escogido no está caducado ni ha sido revocado; en caso contrario se rechazará la firma electrónica:

- Si dispone de certificado en tarjeta criptográfica, y no lo ha introducido en el lector previamente, puede realizarlo en este momento y pulsar el botón “Actualizar” para que cargue nuevamente la lista de certificados disponibles.

- Si dispone de un almacén de claves externas, puede cargarlo a través del botón “Cargar”.



En caso de que sea necesario, el programa le solicitará la contraseña necesaria para realizar la firma.



Enlaces para descargas

- AutoFirma de @firma

  http://firmaelectronica.gob.es/Home/Descargas.html

- DNI electrónico

http://www.dnielectronico.es/PortalDNIe/

- Tarjetas criptográficas FNMT

  https://www.sede.fnmt.gob.es/descargas/descarga-software

- Oracle Java

  https://www.java.com/es/download/