

Dirección General de la Policía

MANUAL BÁSICO CONFIGURACIÓN DNIe PARA WINDOWS XP

Soporte de Atención al ciudadano



MANUAL BÁSICO CONFIGURACIÓN DNle PARA WINDOWS XP

Para la confección del presente manual, se ha utilizado Windows XP profesional Service Pack 3 con Internet Explorer 8 y prácticamente no hay diferencia sustancial, para la utilización del DNle, con respecto a otras versiones de dicho sistema operativo de Windows XP existentes en el mercado.

¿Cómo es el DNle?

El Documento Nacional de Identidad del reino de España es uno de los documentos acreditativos de la identidad más avanzados del mundo. El comúnmente conocido como DNle acredita la identidad de su titular en tres aspectos:

Primero, de forma documental: El Cuerpo Nacional de Policía es el único organismo competente para documentar la identidad de los españoles y extranjeros en España. El DNle es un soporte que acredita la identidad de todos los españoles y gracias a sus avanzadas medidas de seguridad es prácticamente infalsificable.

Segundo, de forma biométrica: Al realizar el DNle se capturan algunas huellas dactilares de cada ciudadano. Esto produce una identificación inequívoca e indisoluble entre el documento y su titular. Esta relación impide usurpar la identidad de su titular, pues permite a los cuerpos policiales realizar una prueba biológica irrefutable a la hora de atribuir la identidad de una persona.

Tercero, de forma electrónica: Este es el auténtico avance tecnológico de nuestro DNle. El DNle es un documento que permite certificar la identidad del ciudadano no sólo en el mundo físico, sino también ante transacciones y comunicaciones telemáticas, permitiendo firmar todo tipo de documentos electrónicos. Para ello se utiliza un dispositivo de creación de firma. La firma electrónica que se efectúe mediante un DNle tendrá efectos equivalentes a los de una firma manuscrita.

Este avance permite al ciudadano realizar trámites administrativos, comerciales o de cualquier índole posible de forma telemática, siempre y cuando las administraciones, empresas y comercios estén abdeheridos a esta tecnología. Esto reporta una gran comodidad al ciudadano al dar la posibilidad a este de hacer ciertas gestiones sin tener que desplazarse físicamente, evitándose colas y esperas innecesarias.

¿Que riesgos tiene?

Lo que se intenta garantizar con el DNle es que, en las comunicaciones telemáticas, quien se identifica con los certificados electrónicos de su DNle es quien dice ser.

Esto se consigue de la siguiente manera:

El chip de nuestro DNle alberga en su interior el certificado de autenticación, (con el cual nos identificamos) y el certificado de firma electrónica reconocida, (con el cual damos nuestro consentimiento, como si una firma manuscrita se tratase). La única forma de acceder a ellos es a través de nuestro PIN (Clave de identificación Personal). Esto quiere decir, que alguien que de forma fraudulenta intentara hacerse pasar por nosotros necesitaría estar en posesión de nuestro DNle y de nuestro PIN. Si le faltase alguna de estas dos cosas sería imposible que usurpara nuestra identidad, pero con ambas, podría hacerse pasar por nosotros y causarnos un perjuicio grave. Por este motivo, recomendamos a todos los poseedores de un DNle que no faciliten su PIN a nadie, que al generar su PIN en un Punto de Actualización configuren una clave que no esté compuesta por datos reflejados en el soporte de

su DNle, que la misma sea tan compleja como les sea posible y que comuniquen inmediatamente a las autoridades el extravío o sustracción de su DNle, para revocar inmediatamente el mismo.

Otro de los problemas que tenemos en internet es saber a quien tenemos al otro lado. Los usuarios de internet tienen que ser conscientes en todo momento que el **utilizar el DNle no da ninguna garantía extra para que no puedan ser estafados**. Los cuerpos policiales tienen grandes dificultades a la hora de perseguir este tipo de delitos, ya que los mismos, se pueden cometer desde cualquier punto del mundo mientras que, la jurisdicción de los cuerpos policiales se reduce a su territorio nacional. En estos casos, la acción de los cuerpos policiales debe ser principalmente preventiva, suministrando a nuestros ciudadanos consejos de seguridad en sus transacciones y comunicaciones por internet. Ahí van algunos de ellos:

Verificar la legitimidad de una página:

Para verificar la legitimidad de una página es necesario comprobar su certificado digital, elemento de seguridad por el que un tercero de confianza garantiza que la página es realmente de la entidad que dice ser.

Para que este proceso sea más intuitivo, las últimas versiones de los navegadores interpretan los certificados mediante códigos de colores, de manera que por el simple color de la barra de navegación se pueda comprobar la legitimidad de la página.

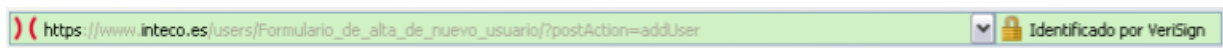
En función de este código de colores, tenemos dos niveles de confianza, que pasamos a describir a continuación.

Página confiable

Si la barra de direcciones es de color verde, se puede estar seguro de que la página es de la entidad que dice ser, ya que la empresa propietaria del navegador lo ha confirmado previamente. Cada navegador usa una forma distinta de indicárnoslo, pero para todos ellos, el color verde significa que se trata de una página confiable. Es posible que para unos navegadores una página sea confiable y para otros no, ya que como hemos dicho, cada empresa hace sus propias confirmaciones.

Internet Explorer

Fondo de la barra de direcciones en color verde. Aparece el nombre de la entidad al lado del candado, también en fondo verde.



Mozilla Firefox

En el icono de la página aparece el nombre de la entidad y todo ello con fondo verde.



Safari

Aparece el nombre de la entidad, con fondo verde cuando se pasa el cursor por encima



Página confiable si...

Si la barra de direcciones no se pone de color verde , se debe tener alguna consideración adicional.

En este caso, el tipo de certificado que usa la página no proporciona información de identidad, es decir, los propietarios del navegador no han llegado a verificar que la dirección pertenece realmente a la entidad. Por este motivo, para poder utilizar la página con unas mínimas garantías se debe estar seguro de:

La dirección de la página que se va a visitar pertenece a la entidad.

La dirección en la barra de navegación está bien escrita. En ocasiones los estafadores intentan suplantar las páginas utilizando direcciones similares y creando páginas prácticamente idénticas.

Pero si se está seguro que esa dirección pertenece a la empresa, si puede utilizarla.

Diferencia entre http y https:

El protocolo con el que funcionan las páginas webs es http, realmente este protocolo significa que una página web está enlazada con otras a través de hipervínculos, y así, conseguimos navegar por la red. Es lo que se denomina <<Hyper Text Transport Protocol>>. Cuando una web contiene https nos añade un plus de seguridad. La <<S>> es la abreviatura de <<Secure>>, y lo que nos intentan garantizar es que no hay nadie escuchando las comunicaciones entre nuestro ordenador y la web a la que estamos conectados. Es una situación de riesgo dar nuestros datos personales o nuestro número de tarjeta de crédito en una web del tipo http.

Algunos navegadores como Internet Explorer suelen añadir un candado cerrado para indicarnos que estamos ante una conexión segura. Ahora vamos a ver que información nos ofrecen los distintos navegadores en relación a este aspecto.

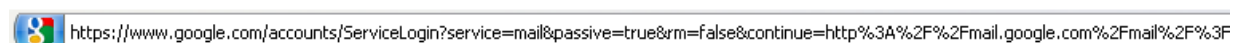
Internet Explorer

Aparece un candado con fondo azul, que al pulsarlo, nos muestra el certificado que garantiza la conexión segura y el nivel de legitimidad.



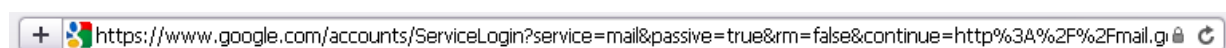
Mozilla Firefox

En el icono de la página que está a la izquierda de la barra de direcciones, aparece el nombre de la entidad y todo ello con fondo azul.



Safari

Aparece un candado en el extremo derecho de la barra de direcciones, pero no aparece el fondo verde, ni el nombre de la entidad.



Con esta información no pretendemos decir que no haya webs que sin tener este tipo de medidas de seguridad sean totalmente honestas con sus usuarios, porque puede, que por diversos motivos no tengan la capacidad suficiente de dar este tipo de garantías.

Hablar de seguridad en la red es un tema muy complejo y de continuo desarrollo. Con esta pequeña aportación intentamos dar un poco de luz a los usuarios. Para quienes quieran profundizar más en este tema recomendamos que consultes con los informes de INTECO, boletines de seguridad de la Dirección General de la Guardia Civil y de la Dirección General de la Policía.

¿Qué es lo que necesito para que funcione mi DNle?

1º Para la utilización del DNI electrónico, es necesario contar con determinados elementos de hardware y software que nos van a permitir el acceso al chip de la tarjeta y por tanto, la utilización de los certificados contenidos en él.

Estos elementos son:

-**Un Ordenador personal** (Intel -a partir de Pentium III- o tecnología similar).

-**Su DNle** (Tarjeta Inteligente con chip integrado).

-**Su PIN**. Es el número de identificación personal, se suministra en un sobre ciego cuando le entregan su DNle. Es posible, que usted haya modificado dicho PIN en un Puesto de Actualización del DNle cambiando el mismo. Tenga en cuenta que si usted ha realizado dicha operación, el PIN contenido en el sobre ciego suministrado ya no tendrá ninguna validez, siendo válida la última contraseña que usted mismo haya generado en el Puesto de Actualización del DNle. Puede recuperar su PIN acudiendo a una Oficina de Expedición del DNle, en un Puesto de Actualización del DNle sin necesidad de cita previa.

-**Un lector de tarjetas inteligentes que cumpla el estándar ISO-7816**. Existen distintas implementaciones, bien integrados en el teclado, bien externos (conectados vía USB) o bien a través de una interfaz PCMCIA.




Para elegir un lector que sea compatible con el DNI electrónico, verifique que al menos:

- Cumpla el estándar ISO 7816 (1, 2 y 3).
- Soporta tarjetas asíncronas basadas en protocolos T=0 (y T=1).
- Soporta velocidades de comunicación mínimas de 9.600 bps.
- Soporta los estándares:

- API PC/SC (Personal Computer/Smart Card)
- CSP (Cryptographic Service Provider, Microsoft)
- API PKCS#11

- **Drivers o software de instalación del lector de tarjetas inteligentes.** El cual vendrá suministrado con su producto y/o deberá ser actualizado a través de la web del fabricante.

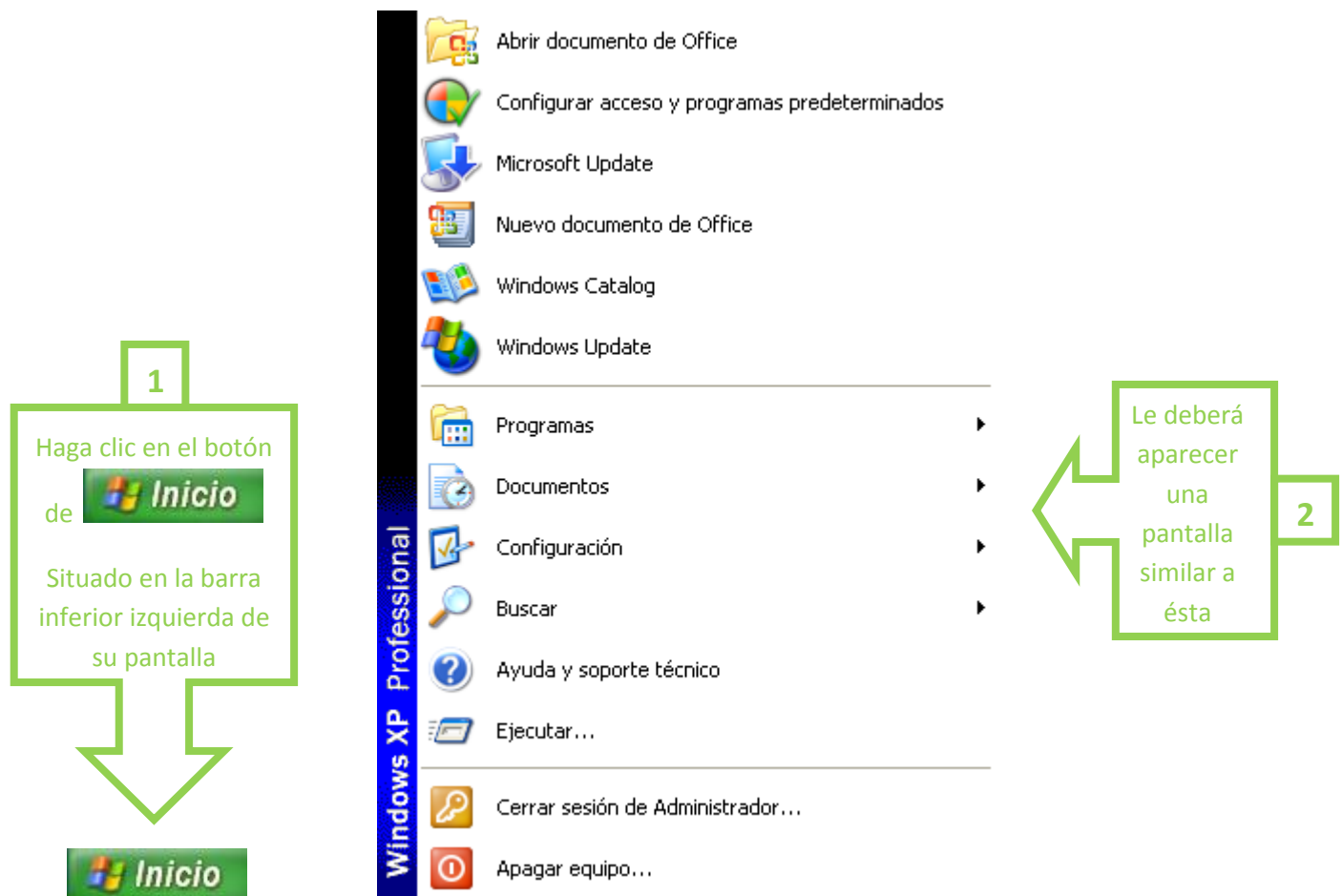
- **Drivers del módulo criptográfico del DNle.** Los cuales le enseñaremos a descargar por medio de este manual, desde la web oficial del DNle.

2º El Sistema Operativo Windows XP permite al usuario la elección de dos tipos de menús de  , el "menú de inicio" y el "menú de inicio clásico". Para comprobar que tipo de menú de inicio tiene usted haga la siguiente comprobación:

1 Ejemplo de "menú de inicio":



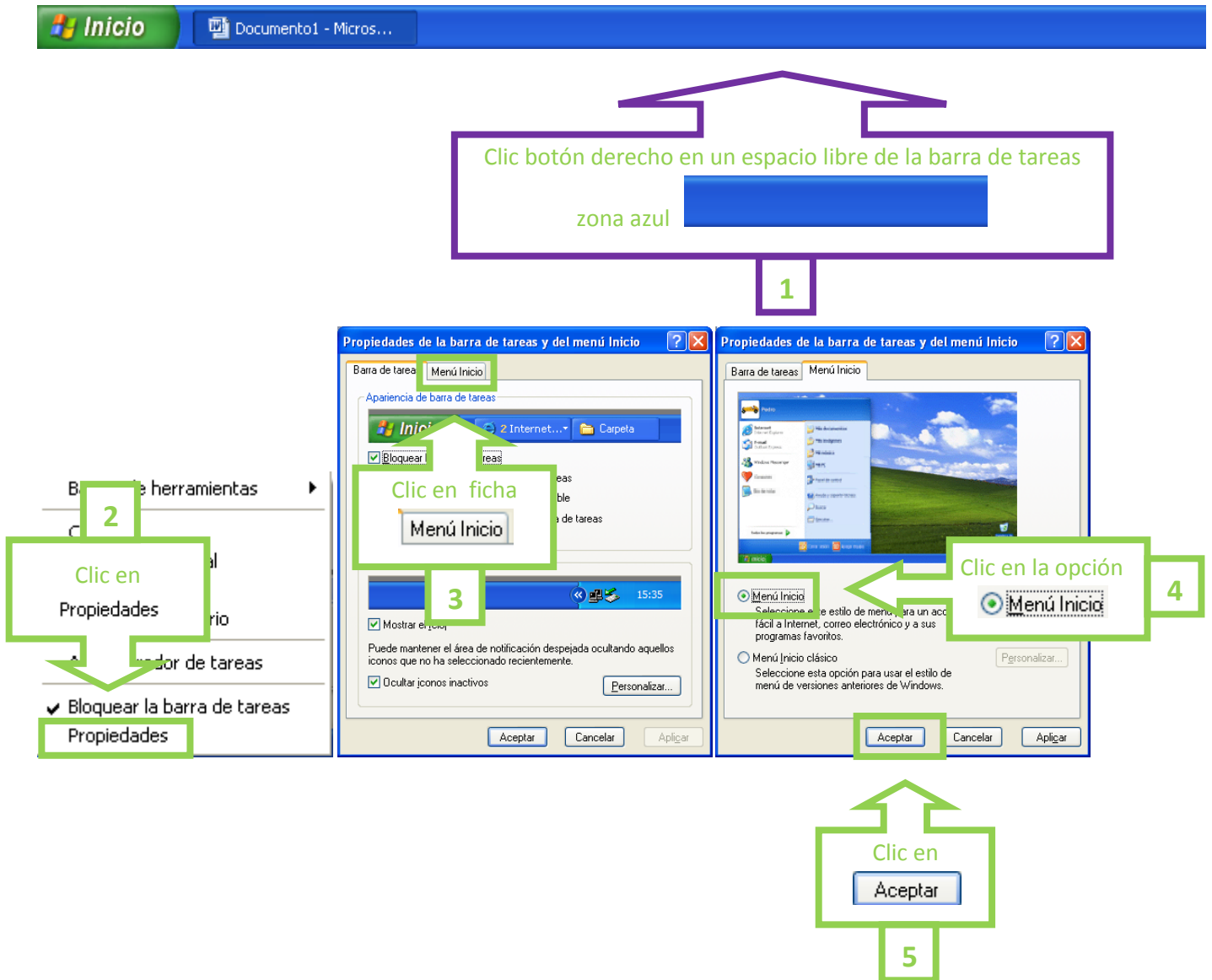
2 Ejemplo de “menú de inicio clásico”:



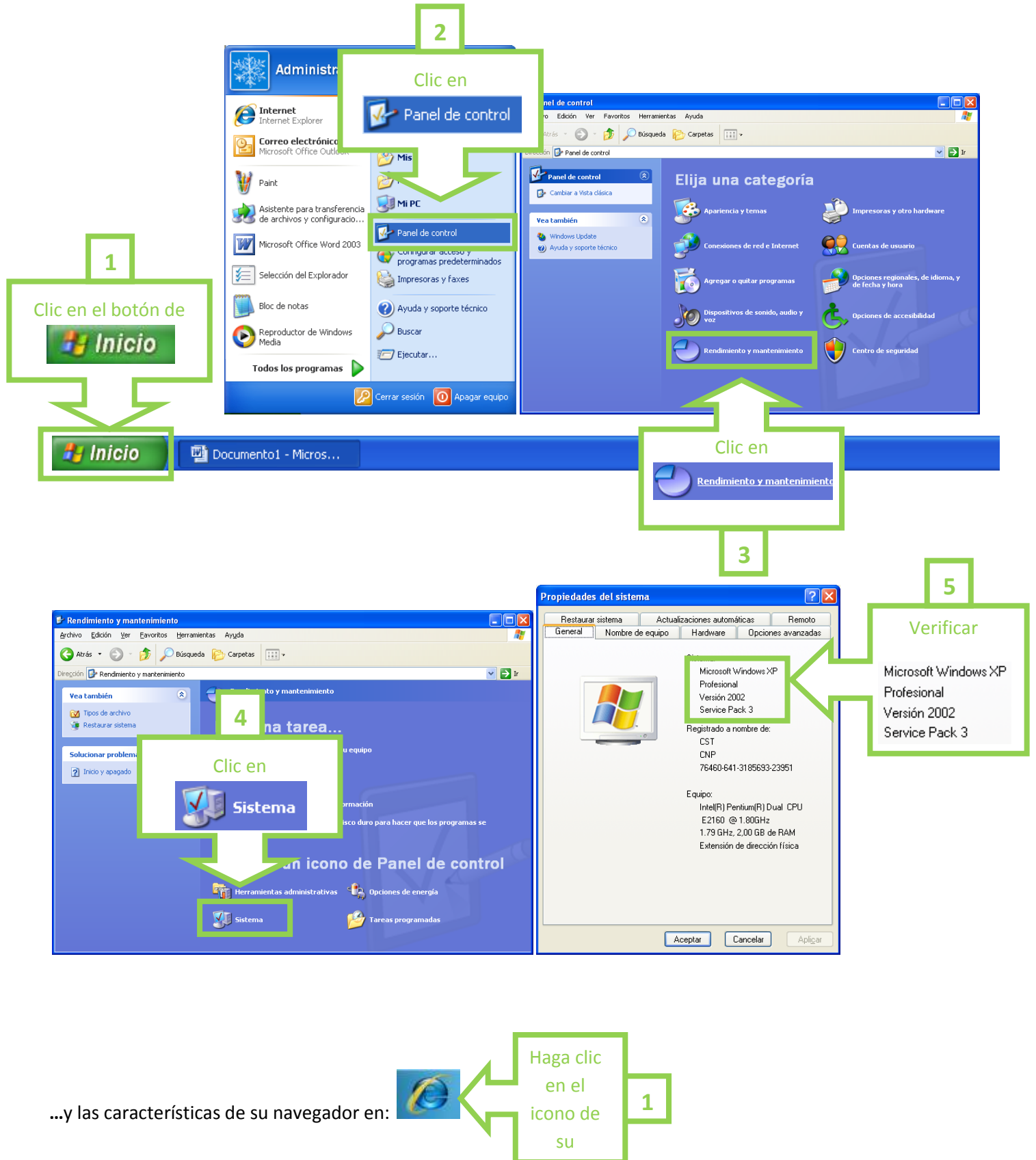
Este manual utilizará el “menú de inicio” como referencia a la hora de indicar sus instrucciones y pasos, ya que éste es el menú que utiliza Windows XP por defecto. Si usted ha comprobado que tiene configurado el “menú de inicio” del ejemplo primero, puede pasar al punto 3º del manual.

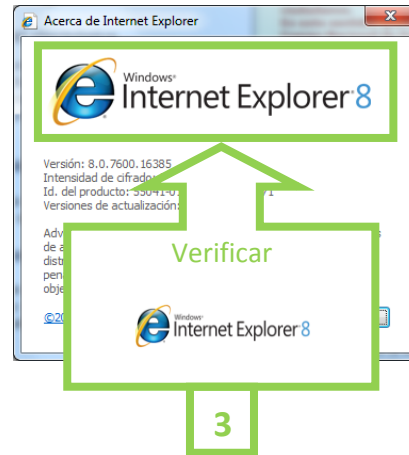
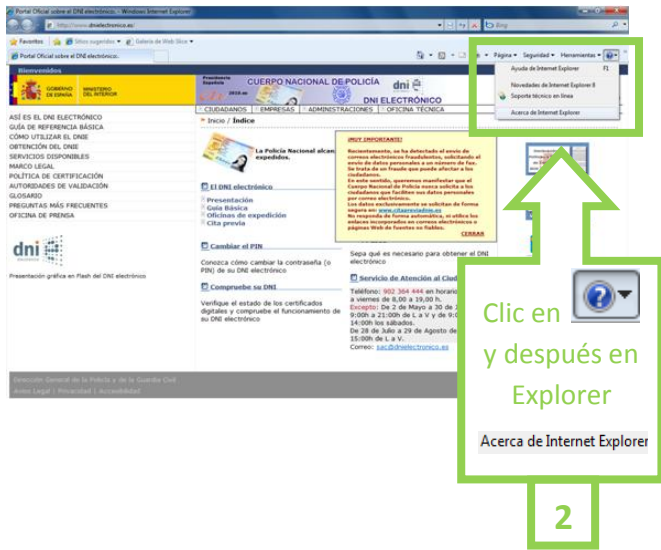
Si usted por el contrario, utiliza el “menú de inicio clásico” y no es un usuario muy avanzado, convendría que siguiese las instrucciones que le vamos a dar a continuación para modificar su “menú de inicio clásico” al “menú de inicio”. De esta forma, las pantallas, instrucciones y rutas que se establecen en este manual le resultarán más familiares. Esta acción es reversible en cualquier momento, por lo que si usted está adaptado a este tipo de menú podrá después de seguir las instrucciones del manual, volver a establecer el “menú de inicio clásico” como su menú predeterminado.

Para cambiar el menú de inicio haga lo siguiente:

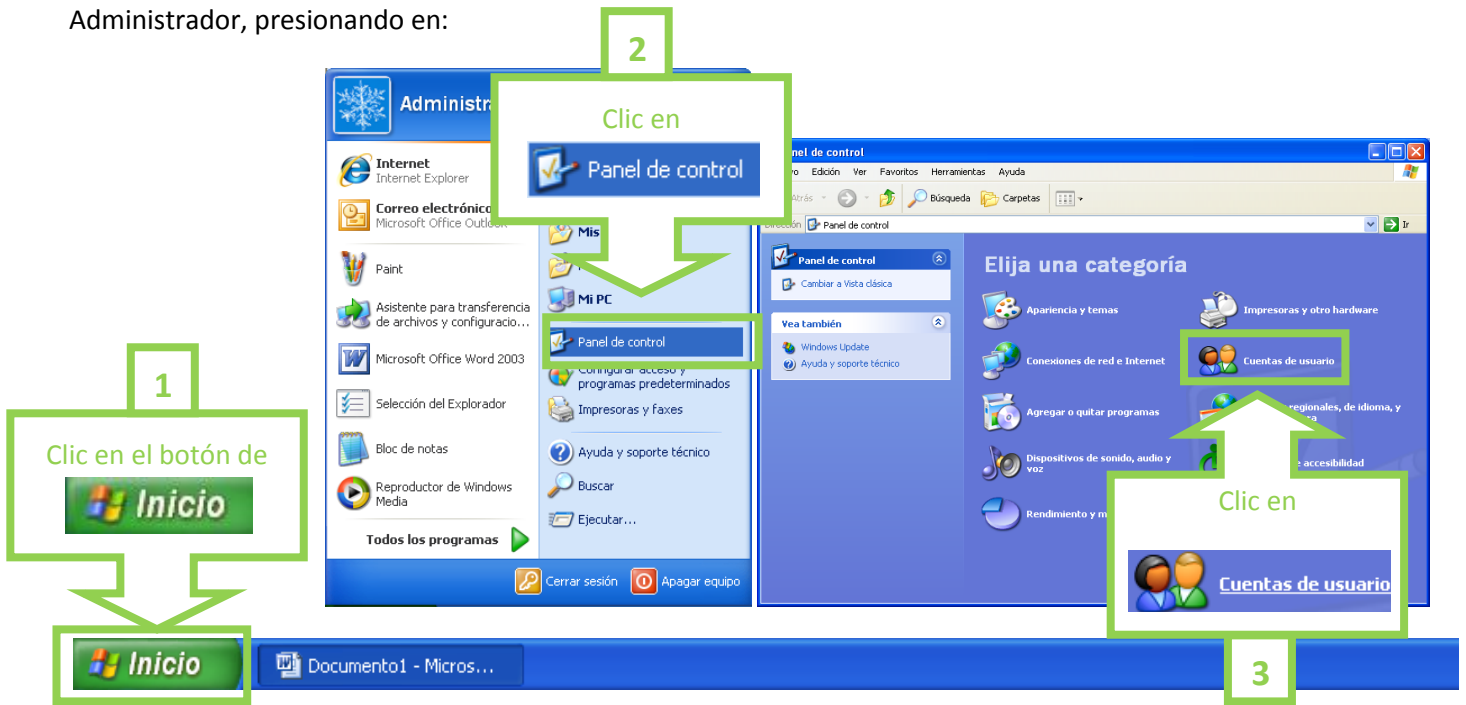


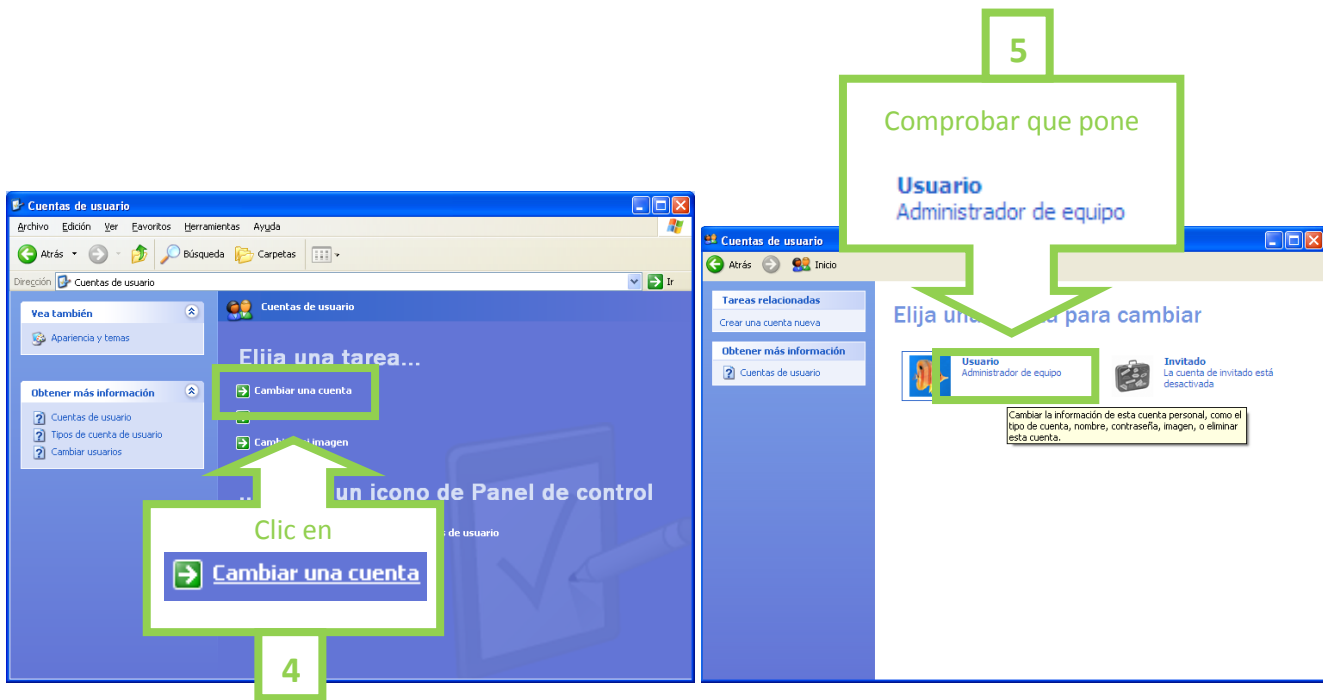
3º Usted puede averiguar cual es su sistema operativo en la siguiente ruta:





4º Al objeto de poder efectuar una serie de modificaciones, debemos asegurarnos de haber entrado como usuario Administrador, presionando en:

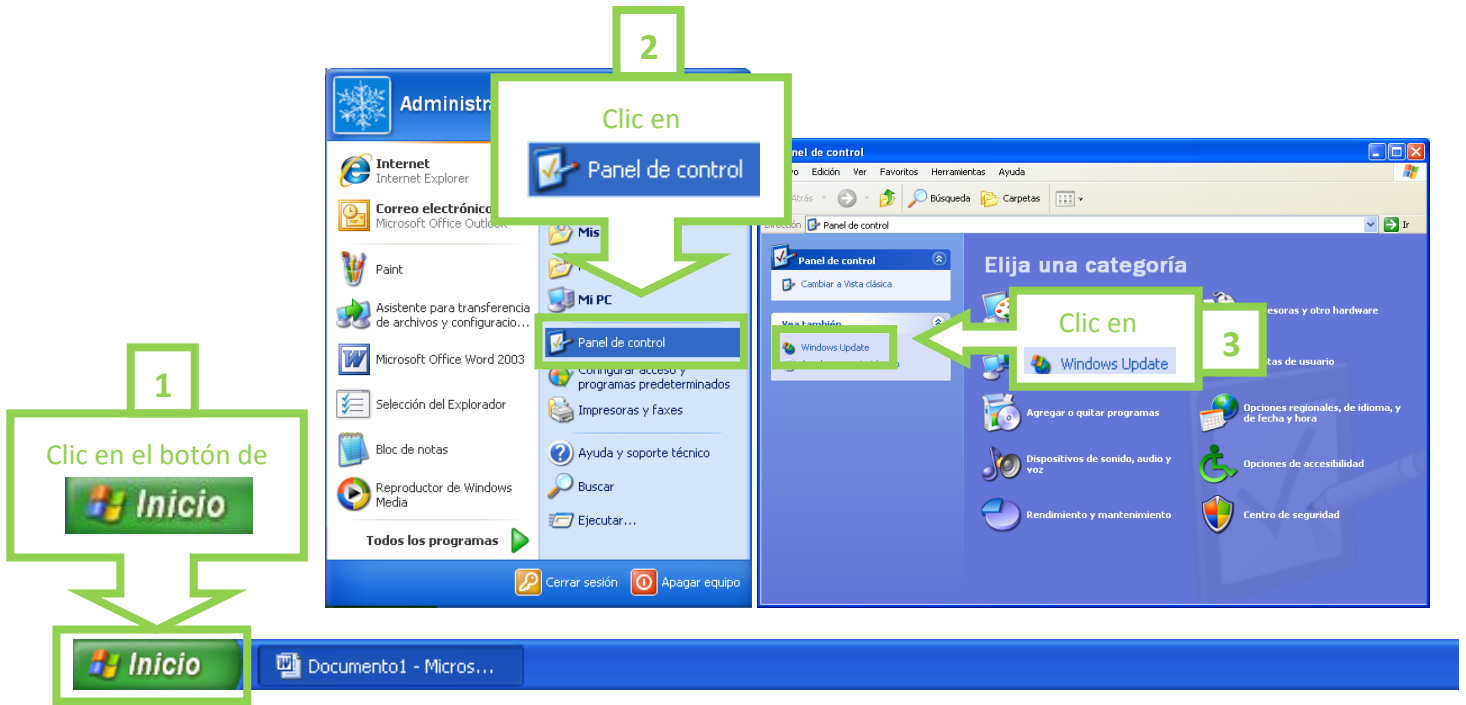




5º Como podemos ver, es un usuario “Administrador” y en el supuesto de que no sea así, deberemos reiniciar el equipo, entrando como tal. Una vez que nos aseguremos de este extremo, cerraremos la ventana, presionado en el aspa del margen superior derecho.

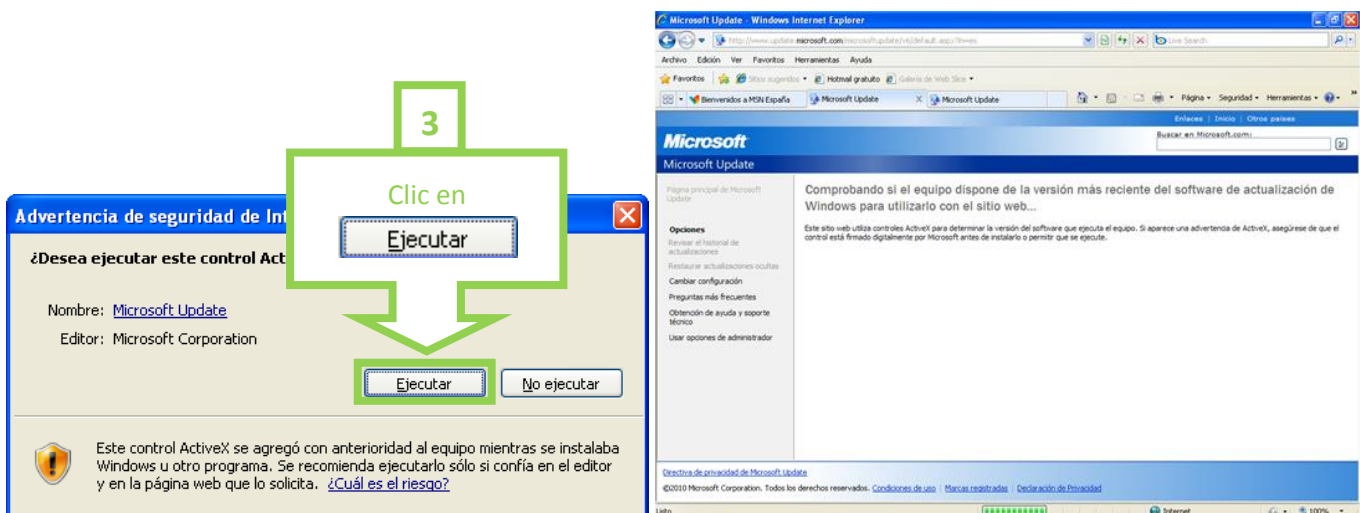
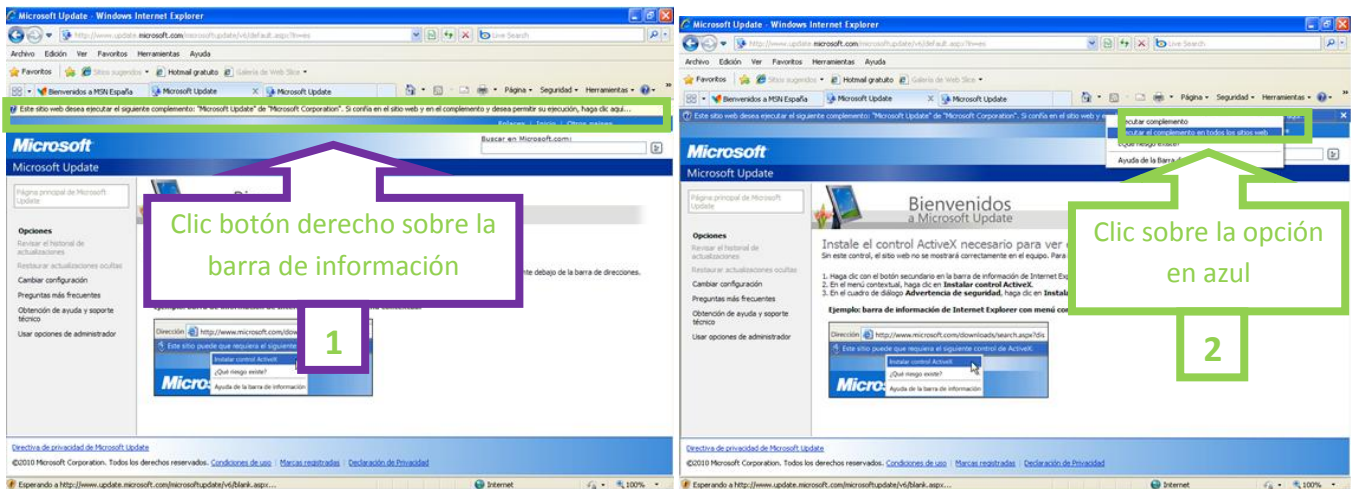


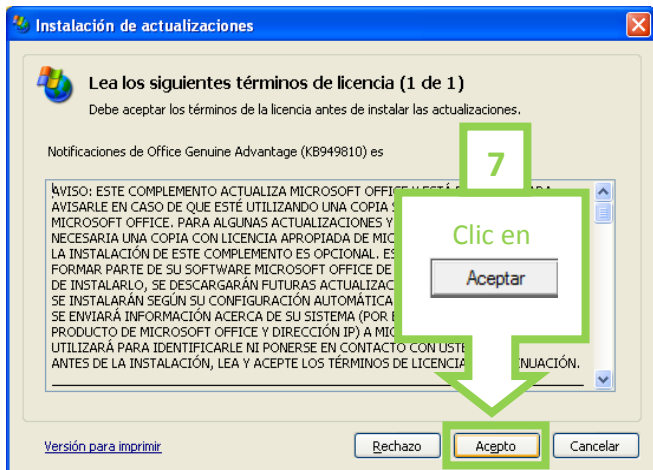
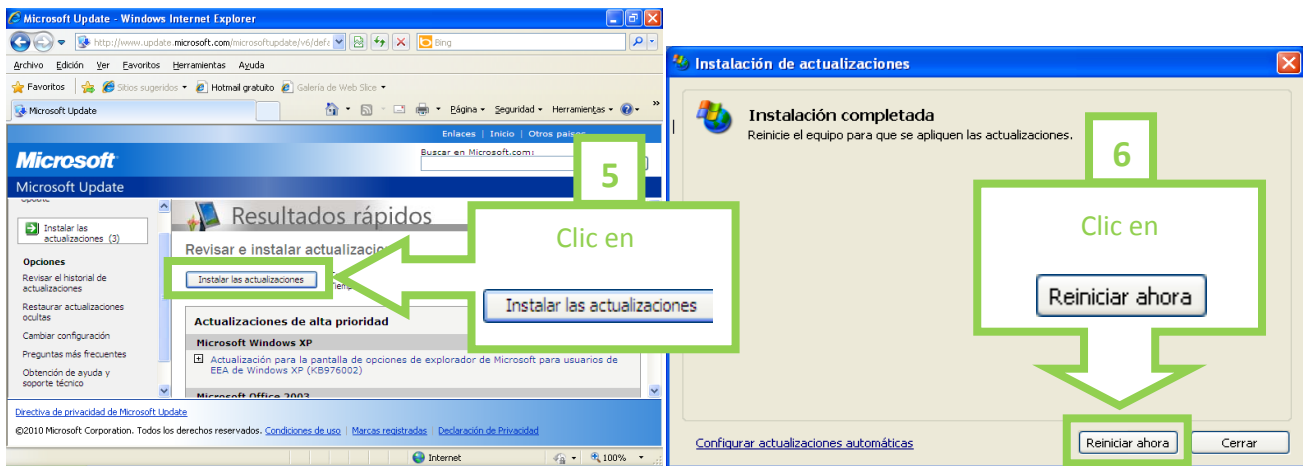
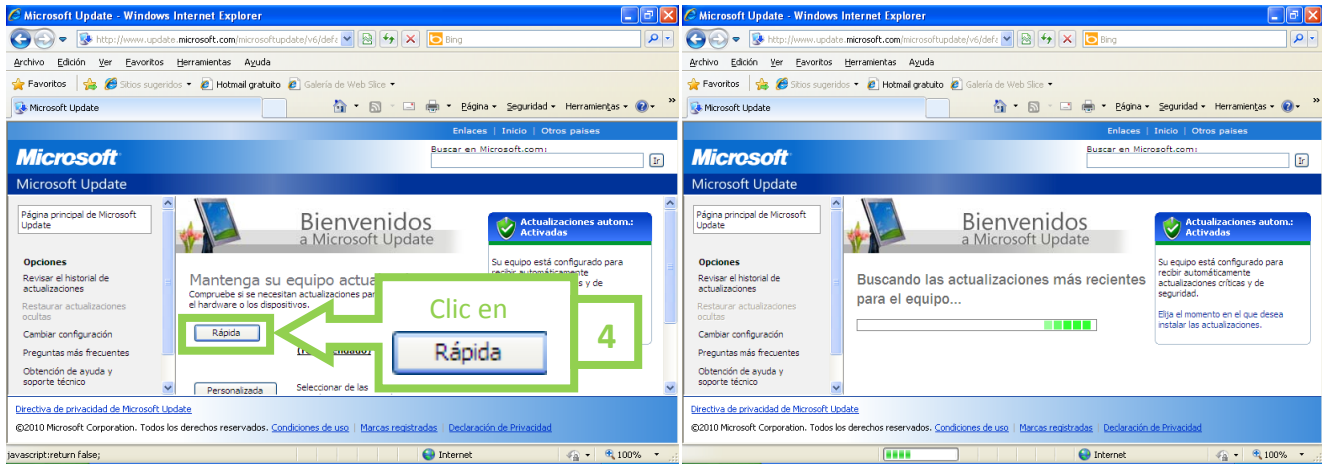
6º Para un correcto funcionamiento del sistema operativo, es conveniente tenerlo actualizado, por lo que comprobaremos que estén activadas las actualizaciones automáticas de “Windows Update”. Para ello haremos la siguiente ruta:

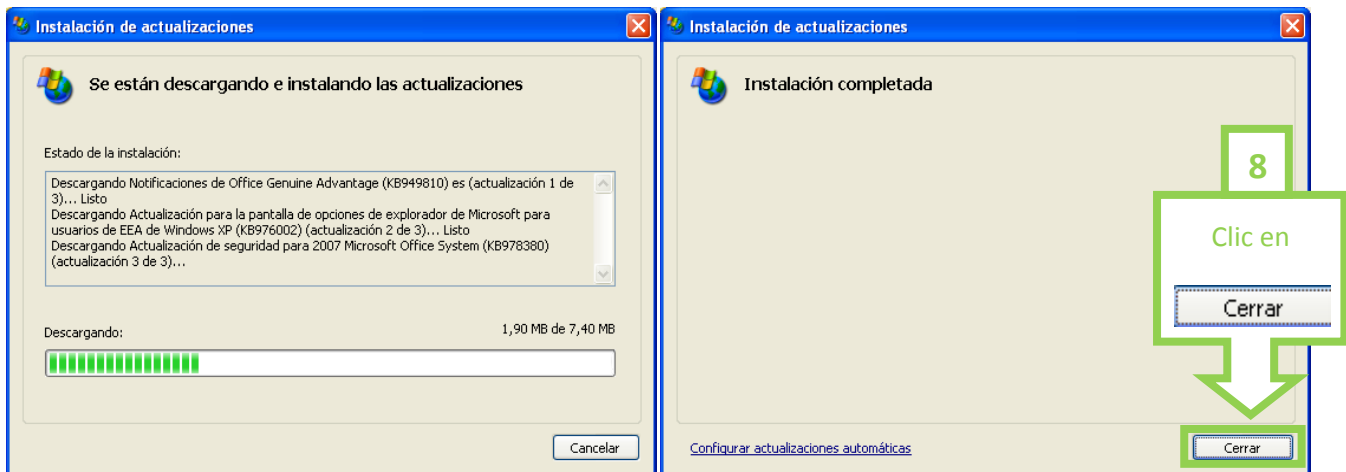


(Tenga presente, que su sistema operativo debe ser original, ya que en caso contrario no podrá realizar correctamente este punto).

Una vez se hayan instalado estas actualizaciones deberá reiniciar el equipo.



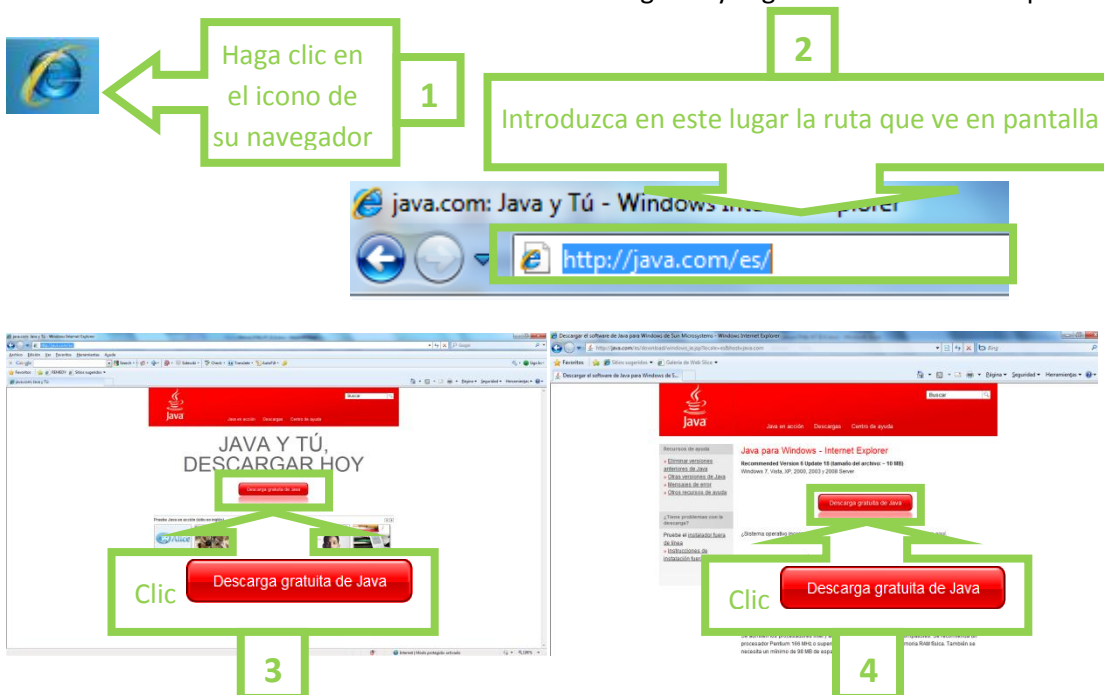


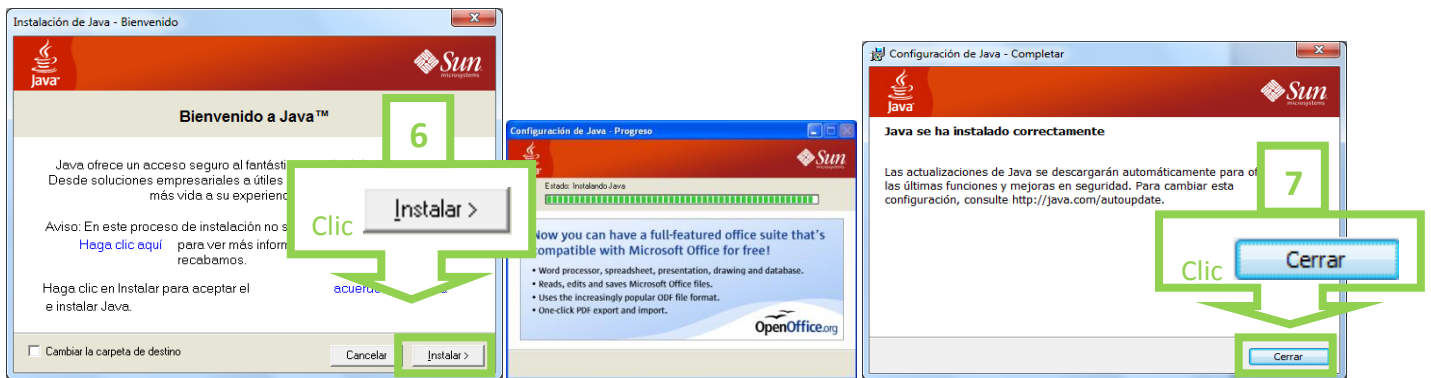
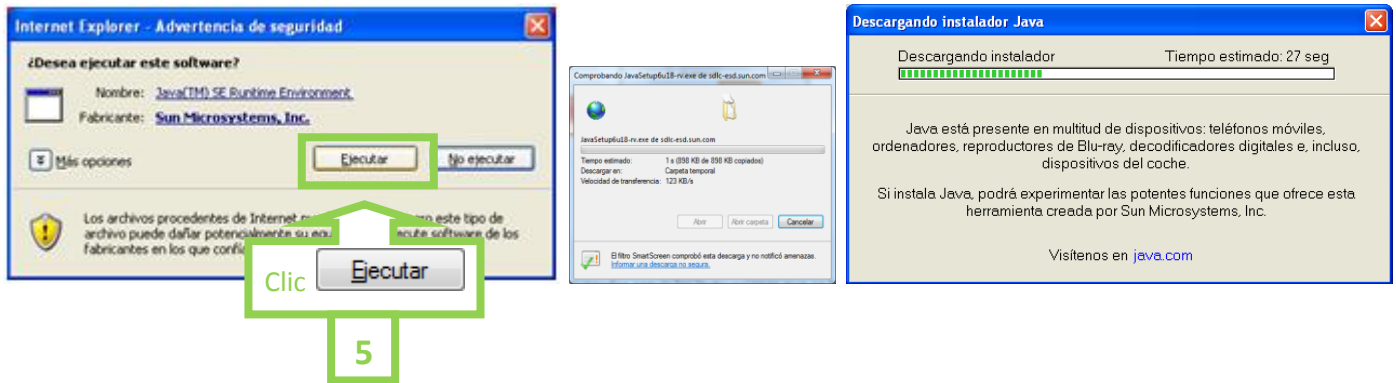


7º Para el correcto funcionamiento del DNIE, en algunas páginas web ajenas al Cuerpo Nacional de Policía, es conveniente la instalación del software Java. Dicho software lo puede descargar en la siguiente ruta:

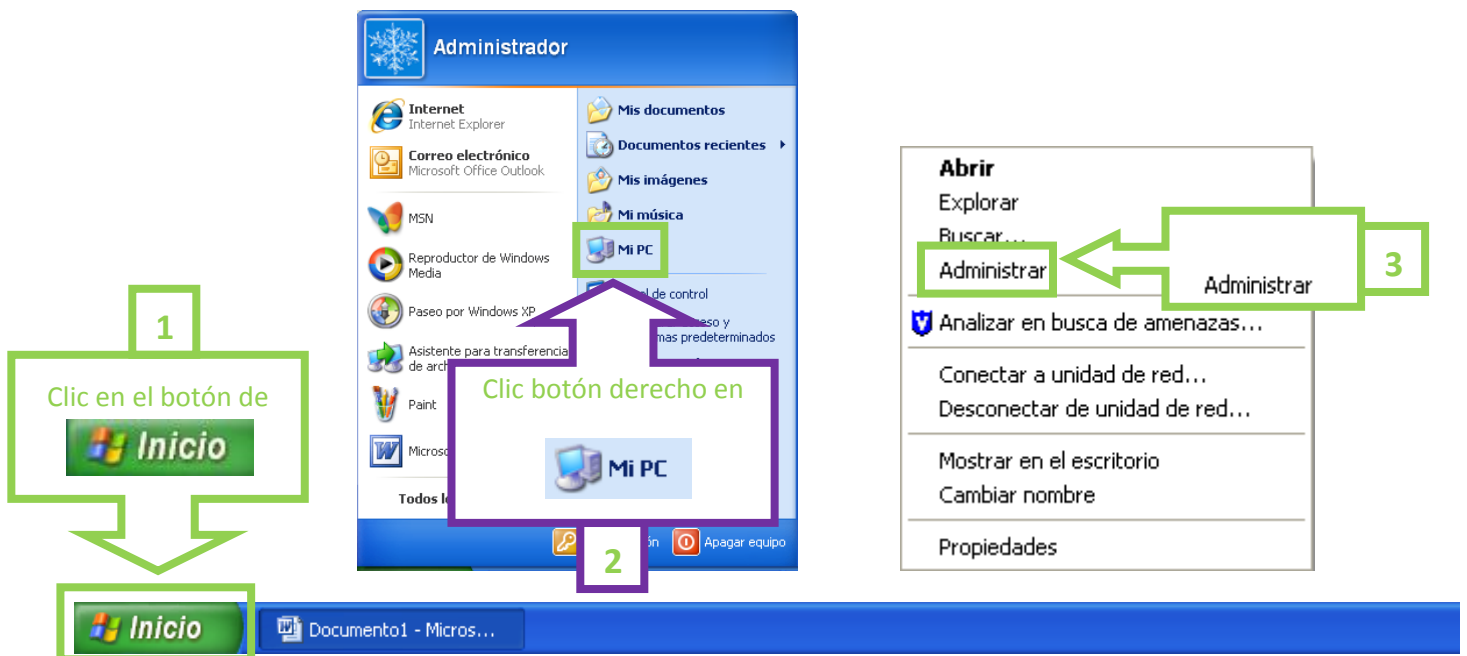
<http://java.com/es/>

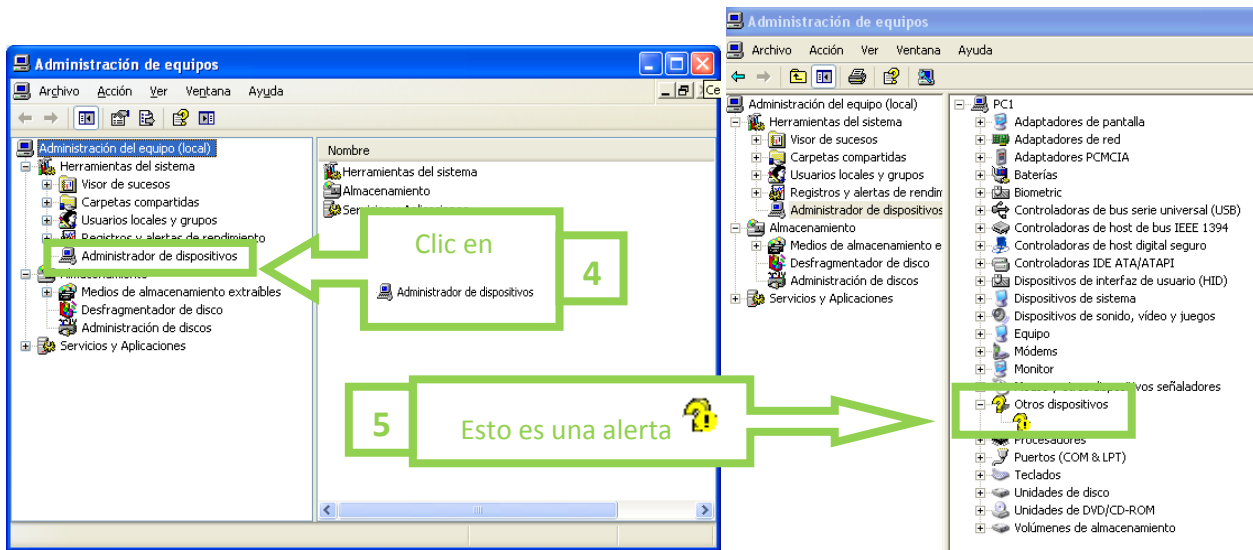
Deberá introducir esta dirección en su navegador y seguir las instrucciones que se le van a detallar.





8º Debe asegurarse que su PC no presente en el <<Administrador de dispositivos>> ningún conflicto o alerta. Para ver su estado realice lo siguiente:





Le aparecerá una pantalla similar a la anterior que no tiene porqué ser igual, ya que depende de los dispositivos que tenga instalados en su equipo.

Las alertas indican que su ordenador presenta un conflicto con alguno de los dispositivos que tiene incorporados, lo cual puede que interfiera en el funcionamiento de su DNle.

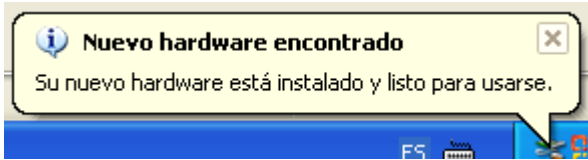
Si este tipo de alertas no quedaran solventadas después de abordar el punto 9º (sobre la instalación de lector de tarjetas inteligentes), no podremos ayudarle a resolverlas. Para solventarlas, le recomendamos que utilice las ayudas que le ofrece Windows para actualizar los controladores o que busque en Internet los drivers o controladores de los dispositivos que su PC no reconoce. En caso de no encontrarlos tendrá que ponerse en manos de algún servicio técnico de su confianza.

9º Al llegar a este punto vamos a proceder a instalar el lector de tarjetas inteligentes. Hay muchos tipos de lectores de tarjetas en el mercado, algunos vendrán integrados en su ordenador (suele ocurrir con los portátiles), otros vendrán integrados en el teclado, y la mayoría de ellos, se comunicarán con su ordenador a través de un puerto USB. Es probable que su Sistema Operativo sea capaz de reconocer su lector de tarjetas inteligentes y operar con él sin generar ningún conflicto. Si su lector de tarjetas está integrado en su equipo o en su teclado y éste no ha generado ningún tipo de alerta como los que se han especificado en el punto 8º, seguramente usted no tendrá ningún problema y no será necesario instalar ningún driver o controlador en su ordenador.

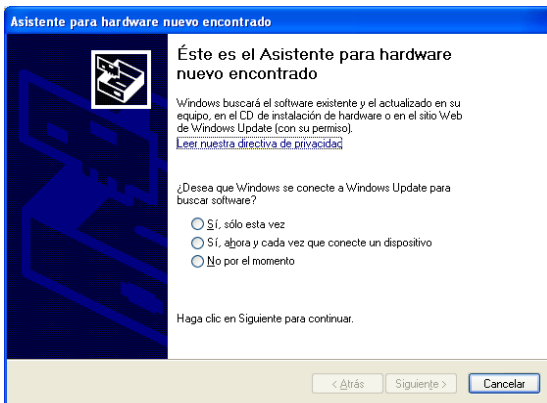
Si todavía no ha conectado su lector de tarjetas inteligentes a su ordenador, ahora es el momento de hacerlo, **hágalo siempre sin haber insertado en el mismo el DNle.** En cuanto su Sistema Operativo lo detecte emitirá un mensaje similar a éste en el margen inferior derecho de su pantalla.



En este momento su Sistema Operativo está intentado reconocer el lector de tarjetas que ha conectado a su ordenador, en el caso de que lo reconozca **emitirá un mensaje similar a éste** y significará que no necesitará instalar ningún tipo de driver o controlador.

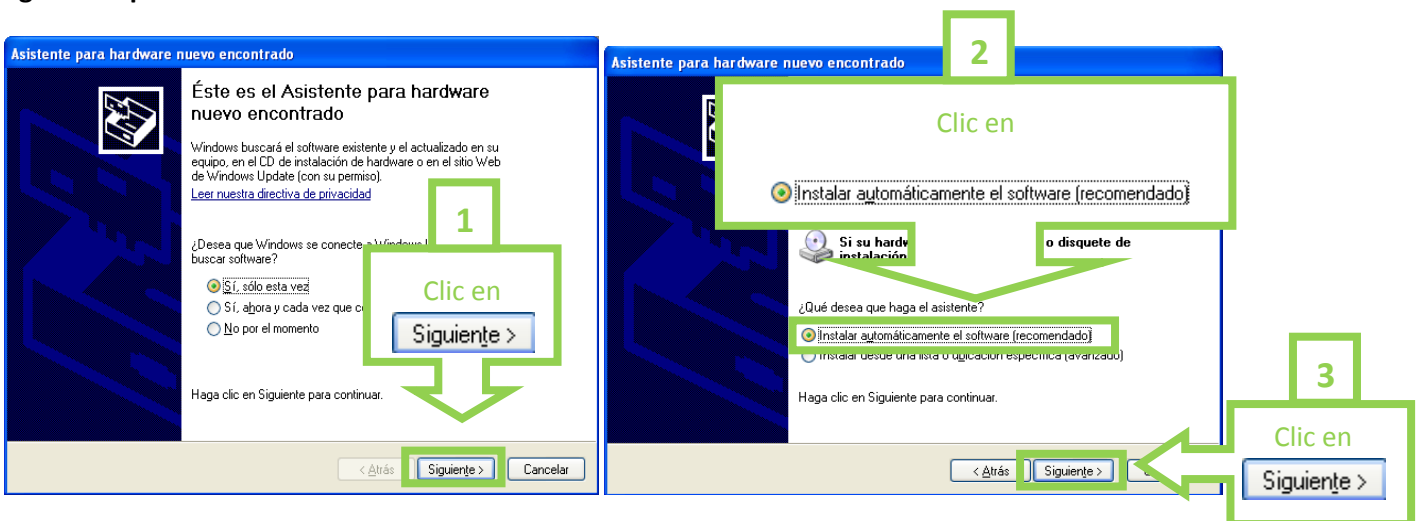


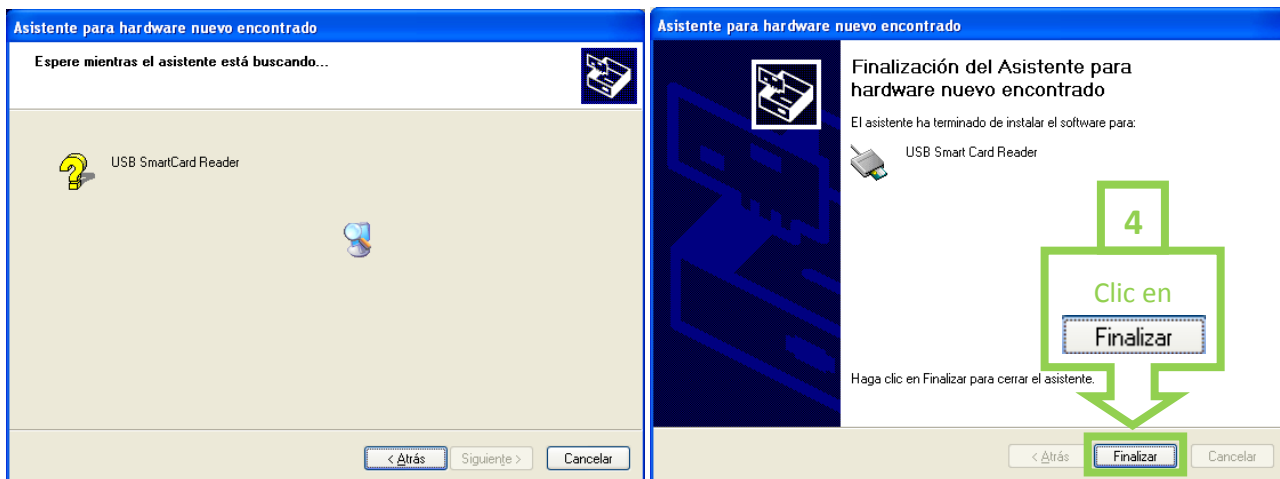
En el caso que su Sistema Operativo no sea capaz de reconocer el lector de tarjetas aparecerá un mensaje similar a éste:



Ante este mensaje, primero **debe cerciorarse que dicho lector sea compatible con el sistema operativo que utiliza su equipo y que cumpla los estándares indicados en el punto 1º.**

Si su lector de tarjetas trae consigo algún tipo de CD o software de instalación ahora es el momento de instalarlo. Siempre siguiendo las instrucciones de instalación recomendadas por el fabricante. Si no lo trae, tenemos la opción de utilizar la herramienta Windows Update para buscar el software que necesitamos. Para ello siga los siguientes pasos:

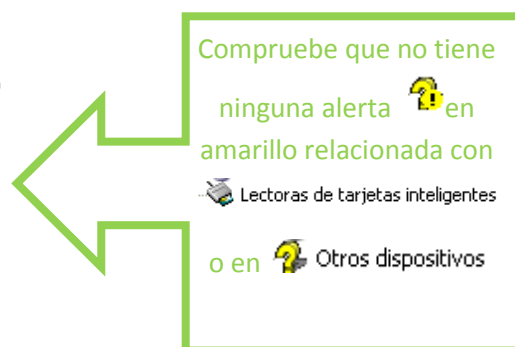
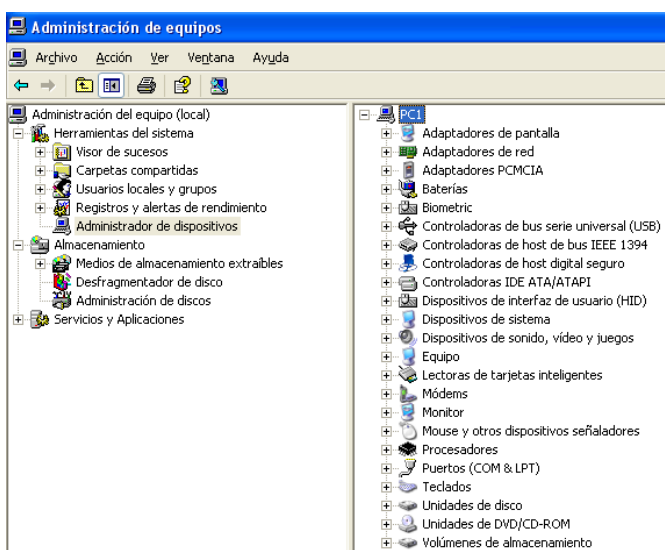







A pesar de que con la utilización del software del fabricante o con la herramienta de Windows Update hayamos conseguido que nuestro Sistema Operativo reconozca nuestro lector de tarjetas inteligentes, es recomendable consultar la web del fabricante en busca de nuevas actualizaciones de drivers/controladores, ya que muchos de los problemas de los usuarios del DNle se generan por una inadecuada instalación del lector, al necesitar éste ser actualizado.

Es vital que todas estas consideraciones se tengan en cuenta, pues la tecnología del DNle está en continuo desarrollo implementándose día a día las últimas novedades en seguridad, de ahí deriva la necesidad de actualizarse continuamente.

Una vez conectado el lector de tarjetas a su PC (importante: sin tener insertado todavía su DNle en el mismo), puede comprobar su correcta instalación **entrando de nuevo en << Administrador de dispositivos>>**, tal y como se explica en el punto 8º.



En el supuesto de que le salga alguna alerta  en el apartado  Lectoras de tarjetas inteligentes , querrá decir que su lector o los drivers/controladores del mismo no están bien. **La solución a este problema tendrá que buscarla a través del fabricante del lector.**

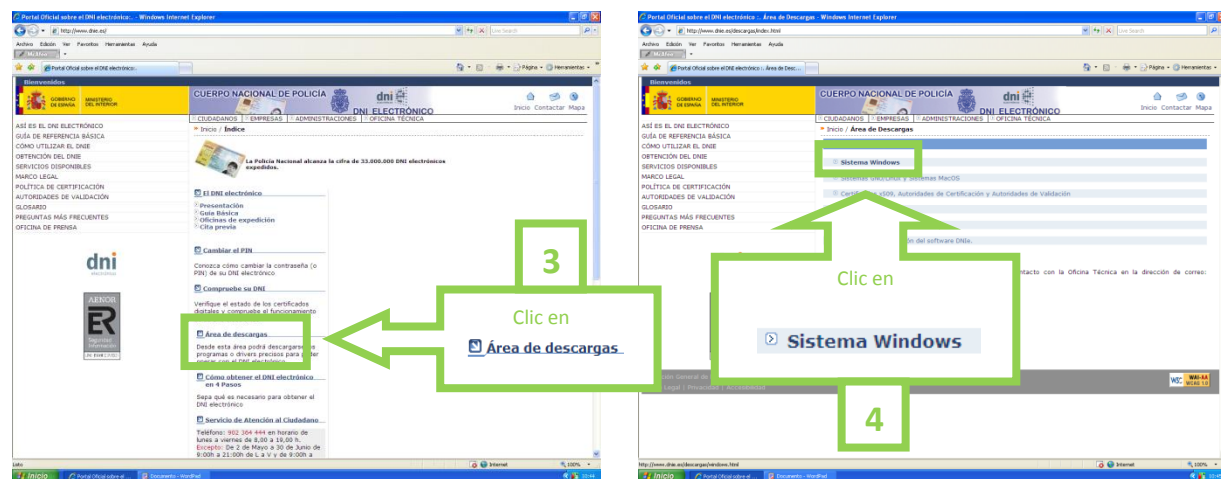
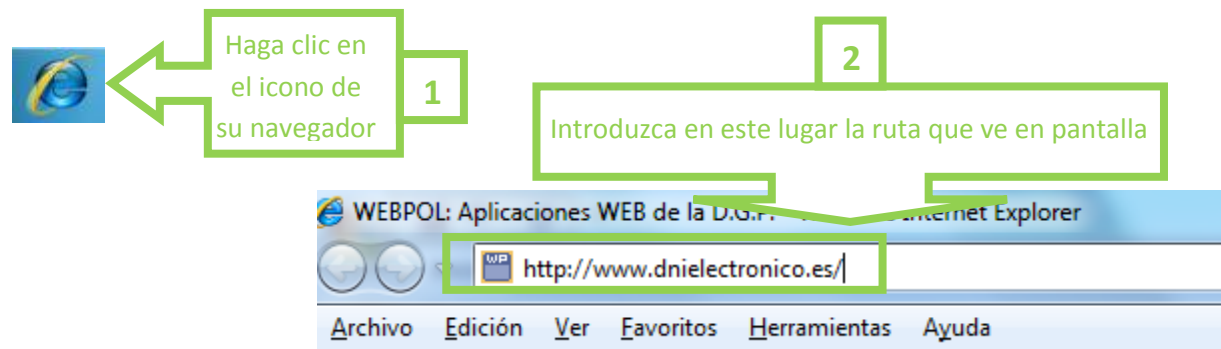
Si la alerta le surge en  Otros dispositivos puede ser debido a varios motivos:

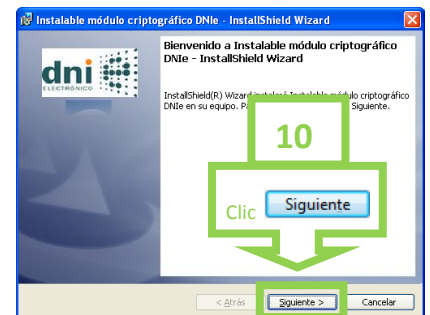
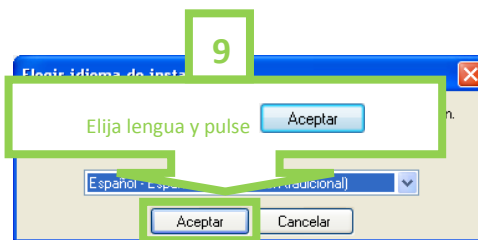
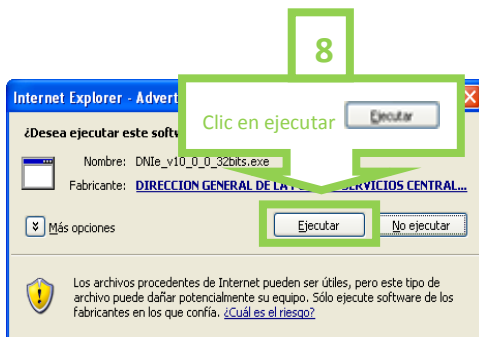
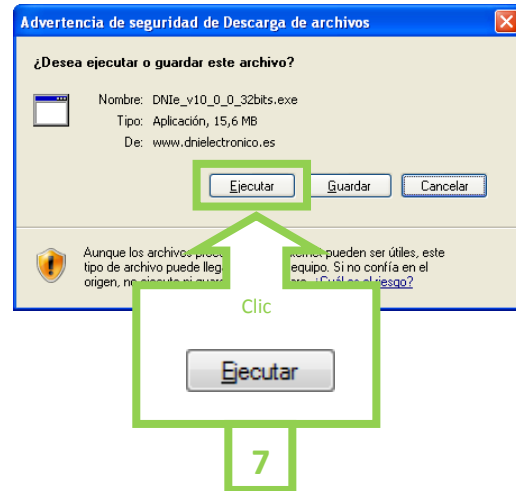
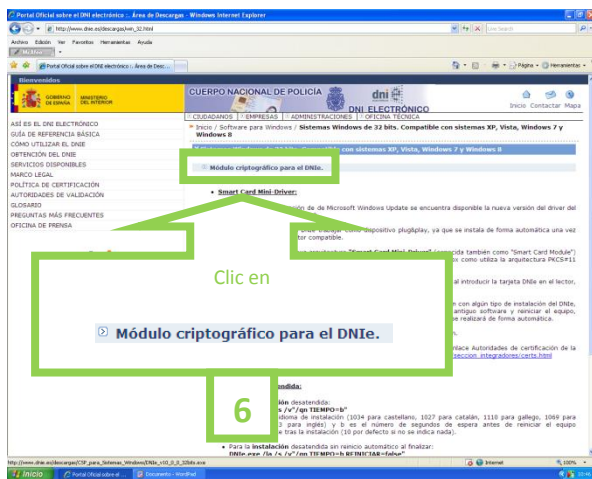
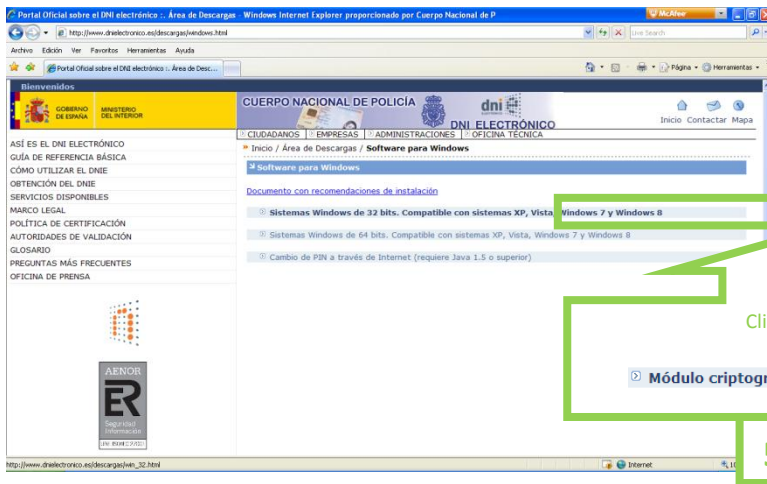
- Por la misma causa del párrafo anterior y con la misma solución.
- Por la causa referida en el punto 8º con las referencias aportadas en el mismo.
- Que tenga introducido su DNLe en el lector y por consiguiente la solución pase por extraer el mismo.

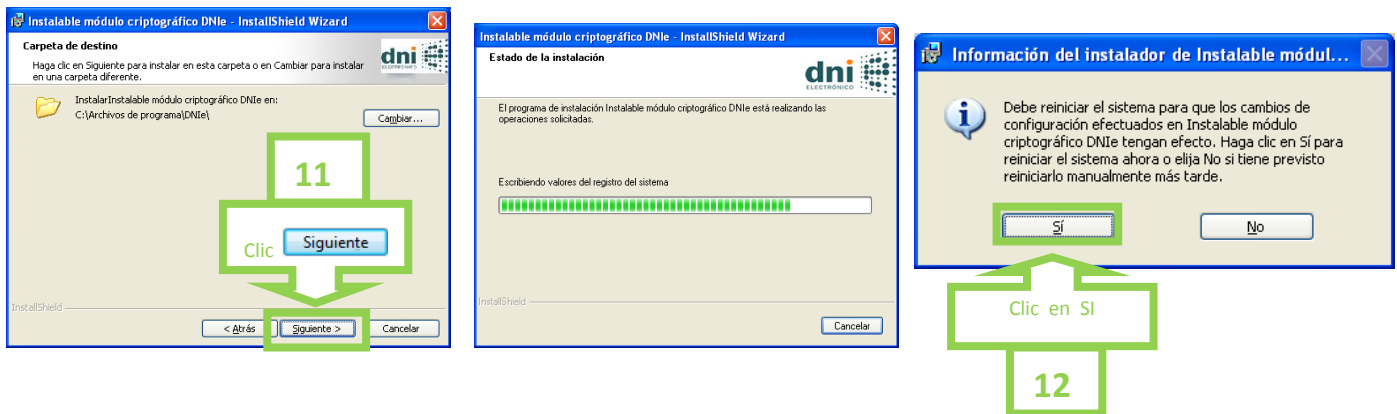
10º Ahora vamos a proceder a instalar el módulo criptográfico del DNLe, en este caso instalaremos la última versión del módulo criptográfico del DNLe que está disponible la V. 10, la cual se encuentra en la siguiente dirección:

<http://www.dnielectronico.es/>

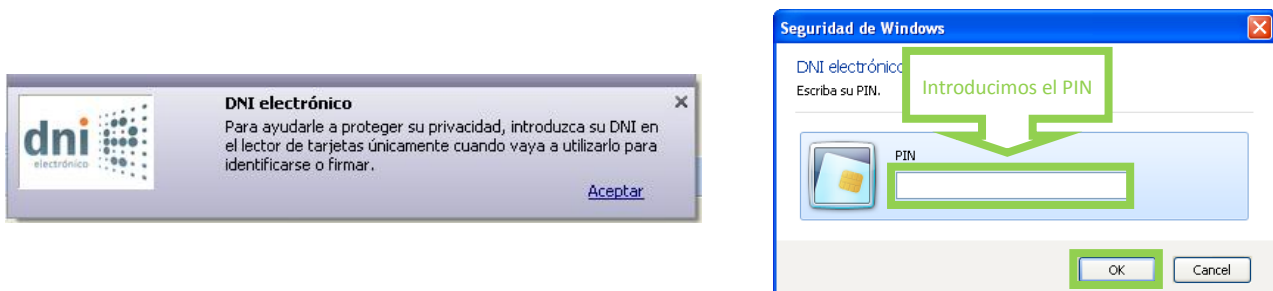
... siguiendo los pasos que se detallan a continuación.







11º Ahora vamos a hacer una comprobación para cerciorarnos de que nuestro DNIe funciona perfectamente en nuestro equipo, **para ello introduciremos correctamente el DNIe en el lector**, nos mostrará un mensaje de seguridad y solicitará el PIN del DNIe. Introdúzcalo correctamente y pulse OK:

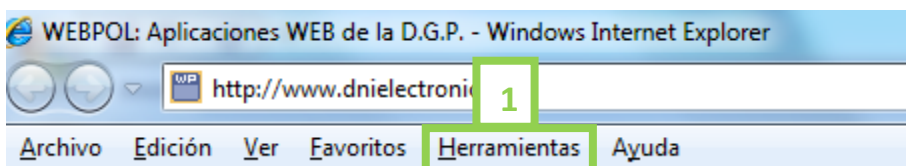


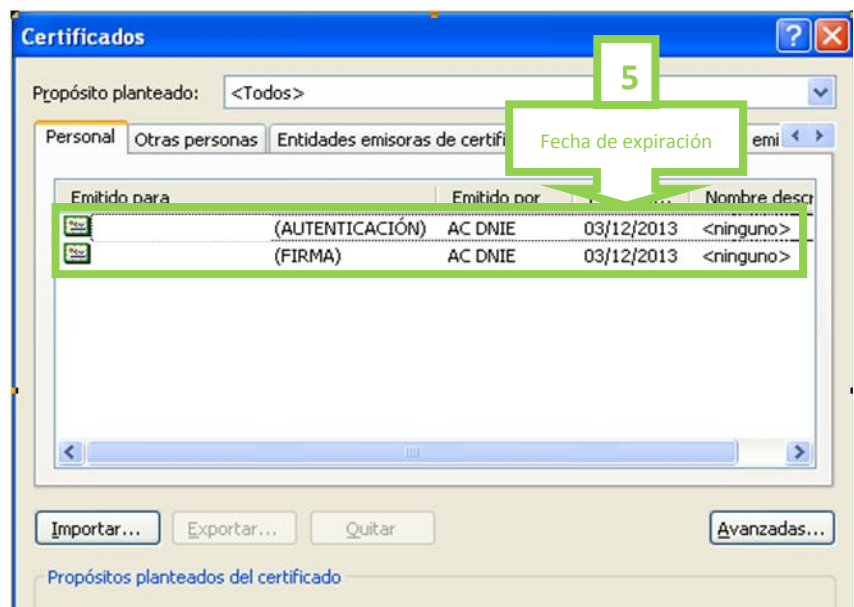
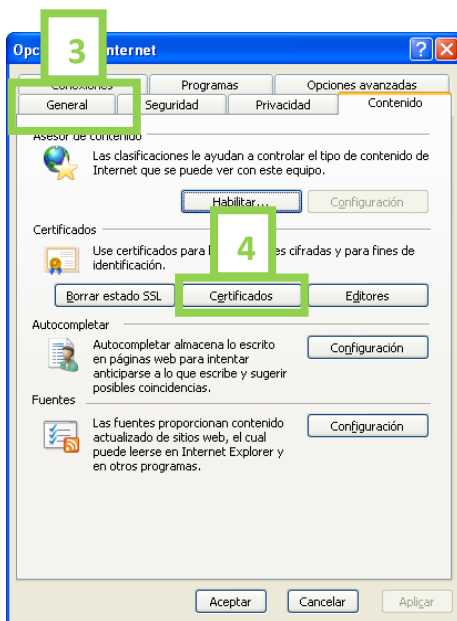
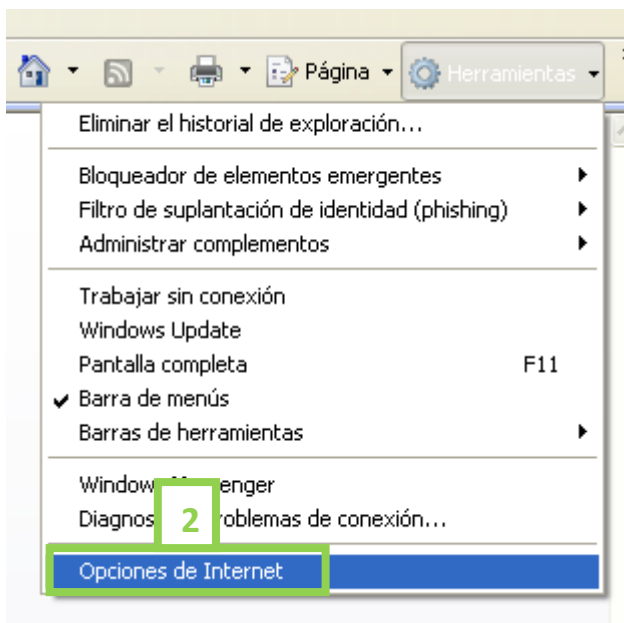
A partir de este momento podrá acceder a la clave pública de sus certificados sin necesidad de introducir constantemente el PIN, este solo volverá a solicitarse cuando sea necesario acceder a las claves privadas para realizar operaciones de Autenticación y Firma.

12º Abra una sesión del navegador:



Para acceder y ver la información de los certificados seguimos la siguiente secuencia:





Esta comprobación es muy útil pues al ver nuestros certificados nos cercioramos de que nuestro equipo es capaz de leer el chip de nuestro DNIE. También podemos comprobar si nuestros certificados han caducado fijándonos en la fecha de expiración.

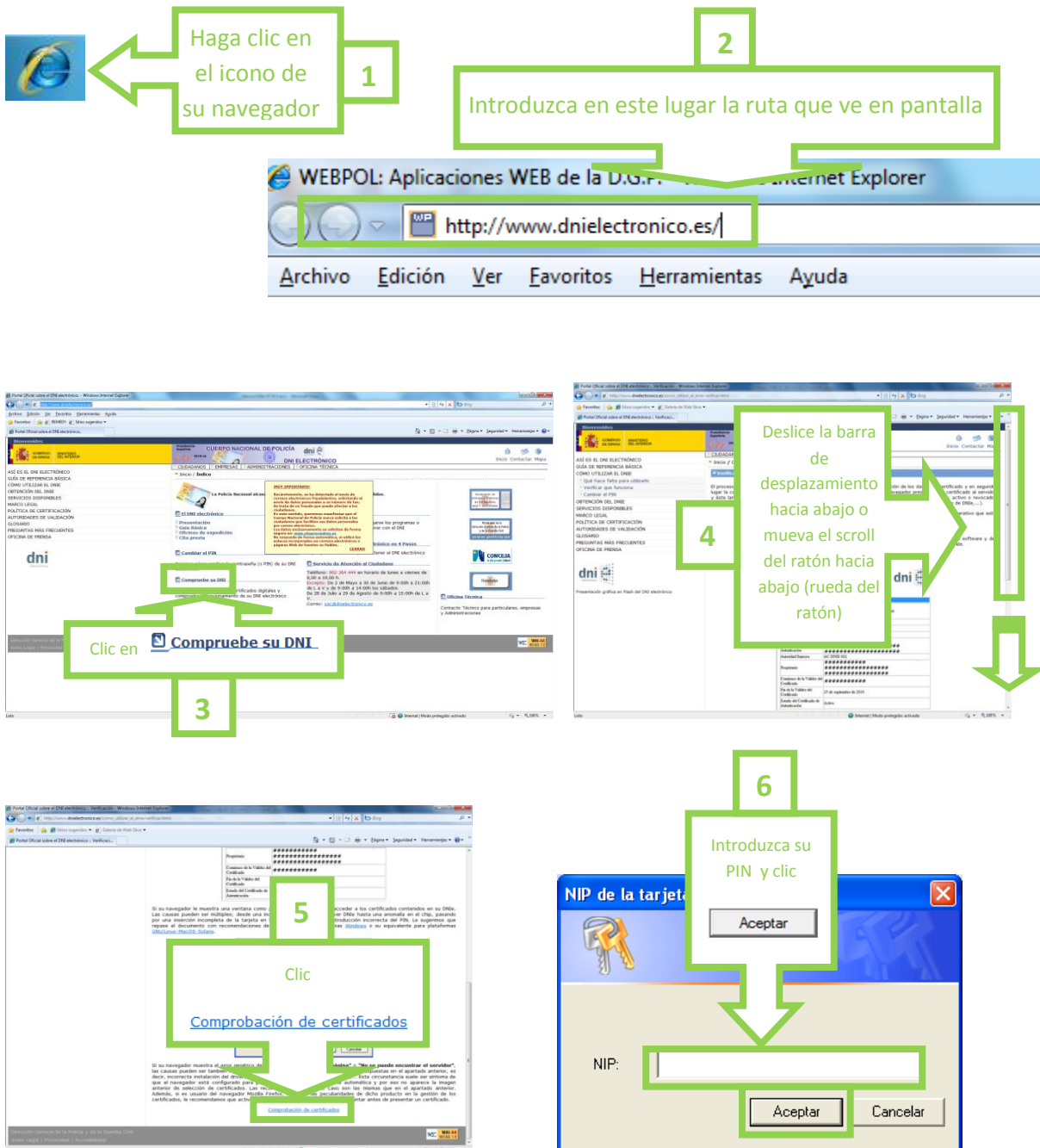
Nuestros certificados caducan cada 30 meses a diferencia de nuestro DNIE, que puede caducar cada 5 o 10 años.

Si tiene usted sus certificados caducados puede renovarlos en cualquier oficina de expedición del DNIE, utilizando un Puesto de Actualización, como es una tarea que puede realizar usted mismo no necesita cita previa para realizarlo.

Actualmente, también puede renovar sus certificados un mes antes de su fecha de expiración.

Acceda a: <http://www.dnielectronico.es/>

...y seguiremos las instrucciones siguientes:



1 Haga clic en el icono de su navegador

2 Introduzca en este lugar la ruta que ve en pantalla

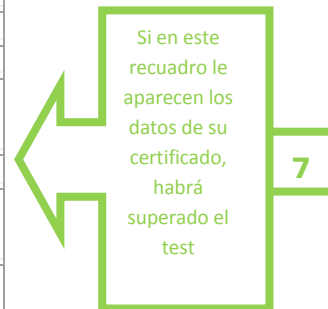
3 Clic en [Compruebe su DNI](#)

4 Deslice la barra de desplazamiento hacia abajo o mueva el scroll del ratón hacia abajo (rueda del ratón)

5 Clic [Comprobación de certificados](#)

6 Introduzca su PIN y clic **Aceptar**

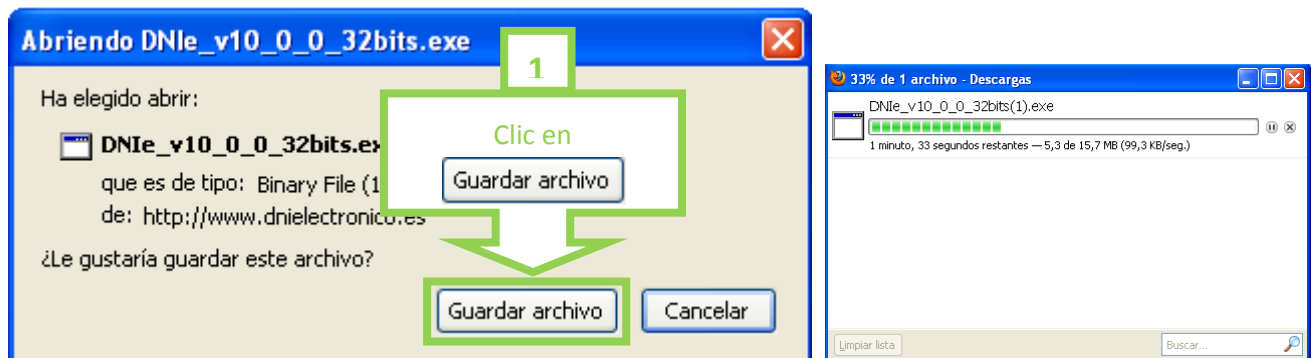
Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	XXX (AUTENTICACIÓN)
Apellidos	XXXX XXXXX
NIF	XXXXXXXX
Número de Serie del Certificado de Autenticación	xxxxxxx
Autoridad Emisora	AC DNIE 003
Propietario	CN="XXXXXXXXXX(AUTENTICACIÓN)", GIVENNAME=XXXX, SURNAME=XXXX, SERIALNUMBER=XXXXXXXX, C=ES
Comienzo de la Validez del Certificado	xx de xxxxx de 20xx
Fin de la Validez del Certificado	xx de xxxxx de 20xx
Estado del Certificado de Autenticación	Activo

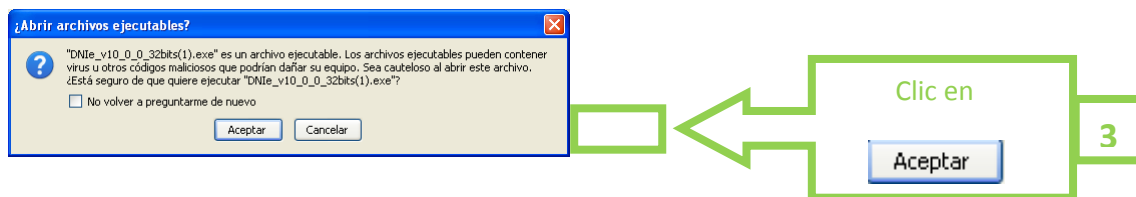
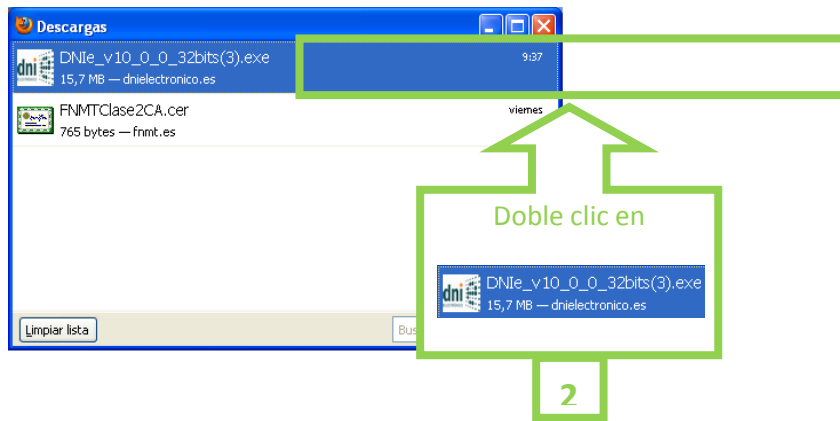


¿Qué es lo que tengo que hacer si prefiero utilizar el navegador Fire Fox?

La nueva versión DNIE v10_0_0.exe ha conseguido una instalación mucho más fácil e intuitiva del módulo criptográfico del DNIE y ya no es necesario cargar las librerías del PKCS#11, como ocurría en las anteriores versiones.

Realmente la instalación es prácticamente idéntica a como se hace si utilizásemos Internet Explorer. Por ese motivo no vamos a detallarla, si no remitir al lector a la página 19 de este manual para seguir la misma. Las únicas diferencias son:

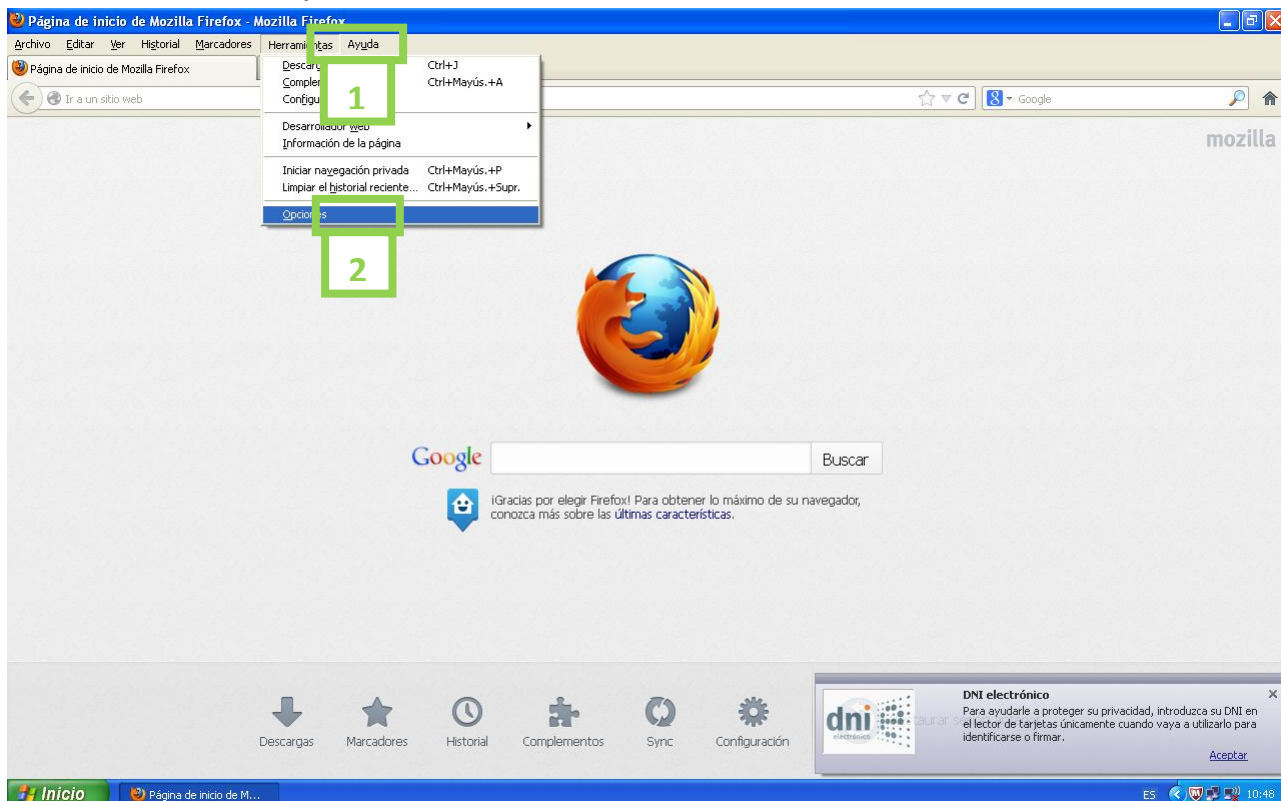


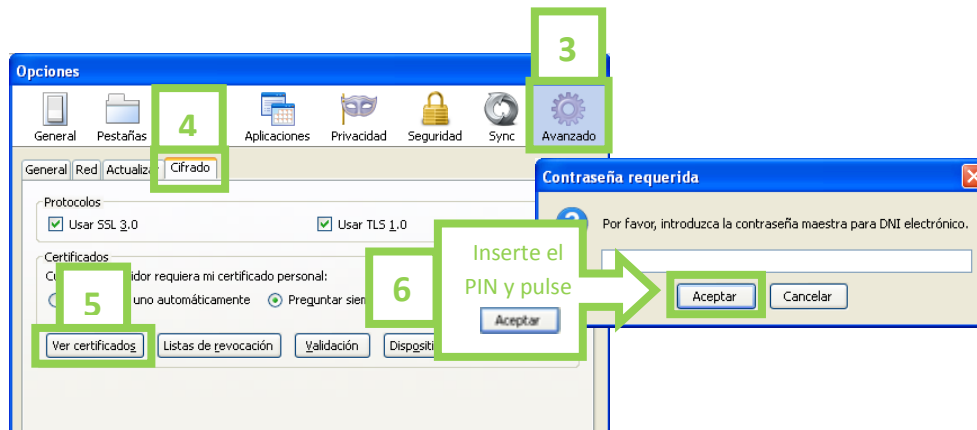


A partir de aquí la instalación es idéntica que con Internet Explorer.

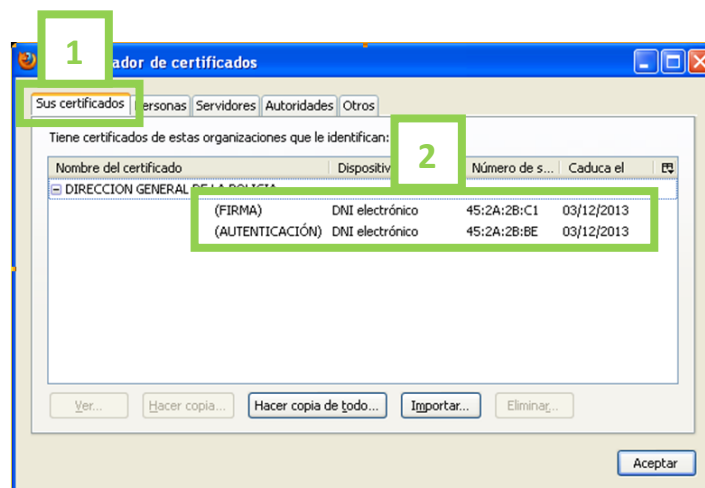
Para acceder y ver la información de los certificados en nuestro equipo seguiremos la secuencia indicada. Primero introducimos el DNIE correctamente en nuestro lector de tarjetas.

Herramientas - Opciones - Avanzado - Pestaña de Cifrado - Ver Certificados





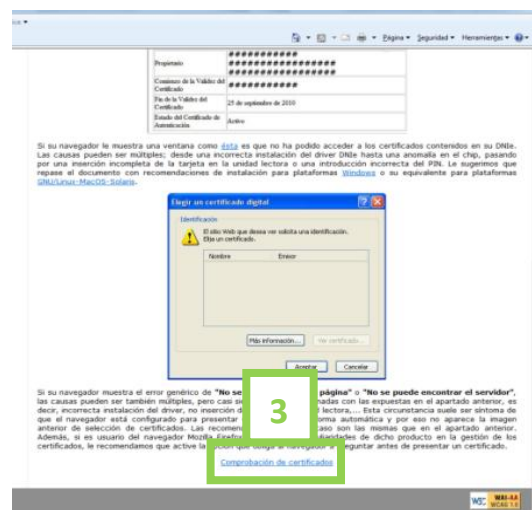
En la pestaña “Sus Certificados” mostrará la clave pública de los certificados de Autenticación y Firma. Esta comprobación es muy útil pues al ver nuestros certificados nos cercioramos de que nuestro equipo es capaz de leer el chip de nuestro DNle. También podemos comprobar si nuestros certificados han caducado fijándonos en la fecha de expiración.



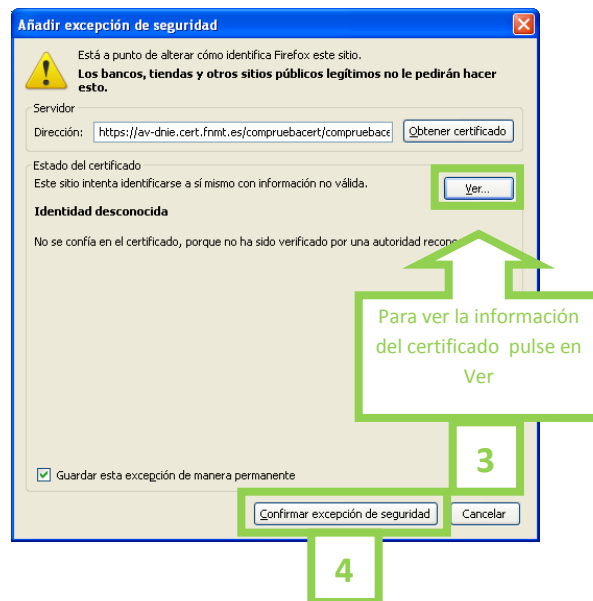
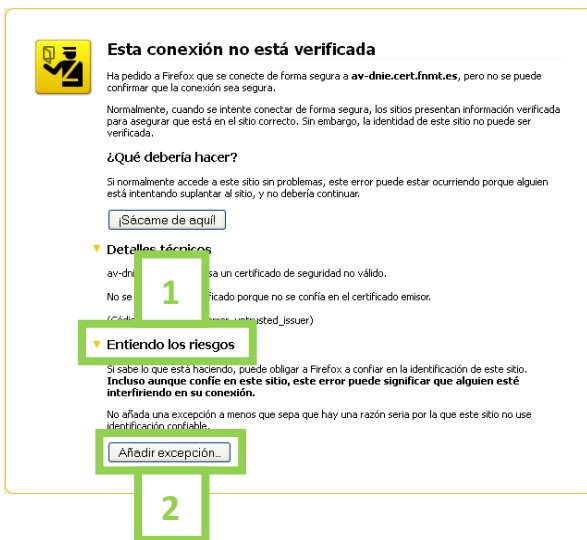
También podrá verificarlo accediendo a la página Web del DNle a través de la opción “Compruebe su DNle”. Ponga la siguiente dirección en la barra de direcciones www.dnielectronico.es

<http://www.dnielectronico.es/>

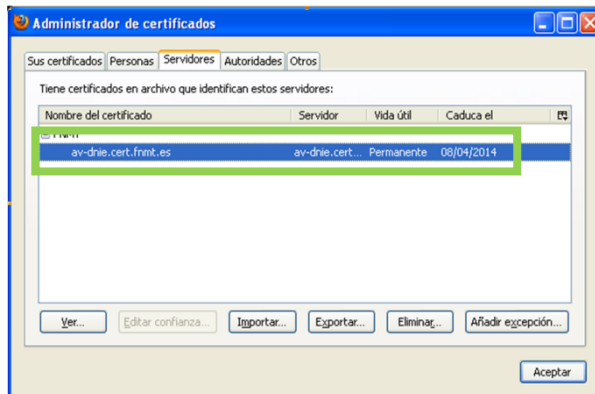
1



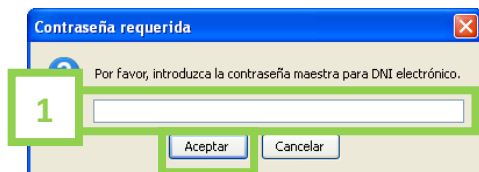
La primera vez que acceda a este servicio es posible que le muestre el mensaje que se adjunta, esto se produce porque la validación se efectúa a través de una conexión segura https (servidor **av-dnie.cert.fnmt.es** protegido por un certificado). Para efectuar la validación primero hay que confiar en este certificado. Para ello siga los siguientes pasos:



El certificado se instalará en la pestaña “Servidores” del Administrador de certificados de Firefox:

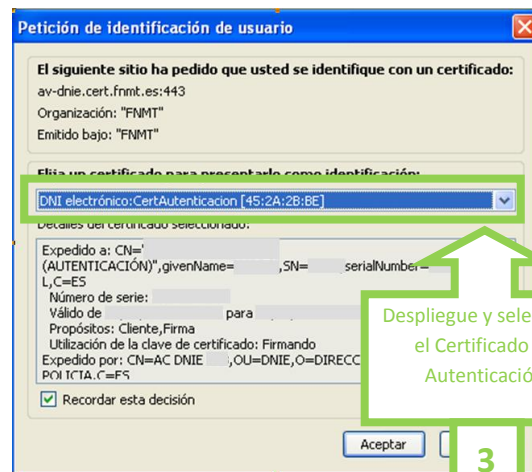


Cierre el navegador y acceda de nuevo a la comprobación de certificados, tras introducir correctamente el PIN seleccione el Certificado de Autenticación:



Inserte el PIN y pulse Aceptar

2



Despliegue y seleccione el Certificado de Autenticación

3

Identificador	Valor
INFORMACIÓN SOBRE LA IDENTIDAD	(Valores Personales)
Nombre	XXX (AUTENTICACIÓN)
Apellidos	XXXX XXXXX
NIF	XXXXXXXX
Número de Serie del Certificado de Autenticación	xxxxxxx
Autoridad Emisora	AC DNIE 003
Propietario	CN="xxxxxxxxxx(AUTENTICACIÓN)", GIVENNAME=xxxxx, SURNAME=xxxxx, SERIALNUMBER=xxxxxxxx, C=ES
Comienzo de la Validez del Certificado	xx de xxxxx de 20xx
Fin de la Validez del Certificado	xx de xxxxx de 20xx
Estado del Certificado de Autenticación	Activo

Si en este recuadro le aparecen los datos de su certificado, habrá superado el test

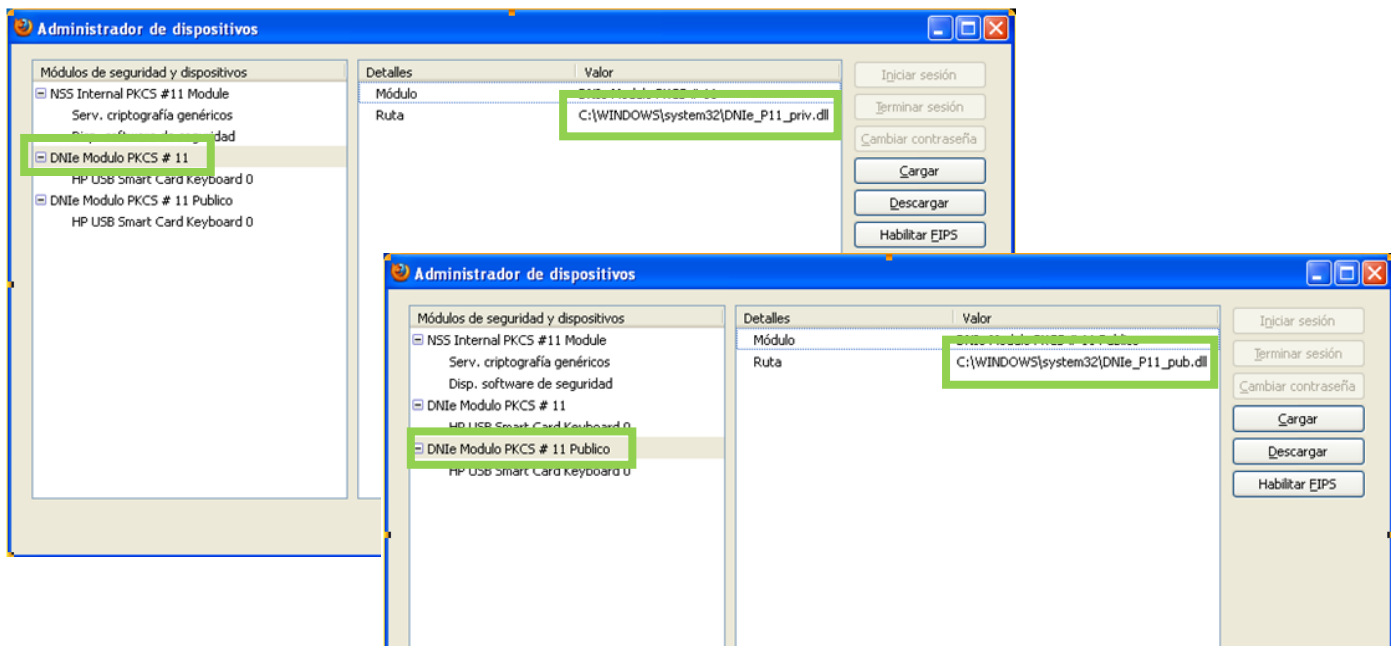
4

Información para usuarios avanzados de Mozilla Firefox:

El nuevo CSP versión DNIe v10_0_0.exe incorpora los siguientes cambios:

Sustitución de las librerías del PKCS#11 por unas de nuevo desarrollo; estas librerías se cargarán directamente en el administrador de dispositivos de Firefox durante la instalación del CSP; se realizan dos entradas:

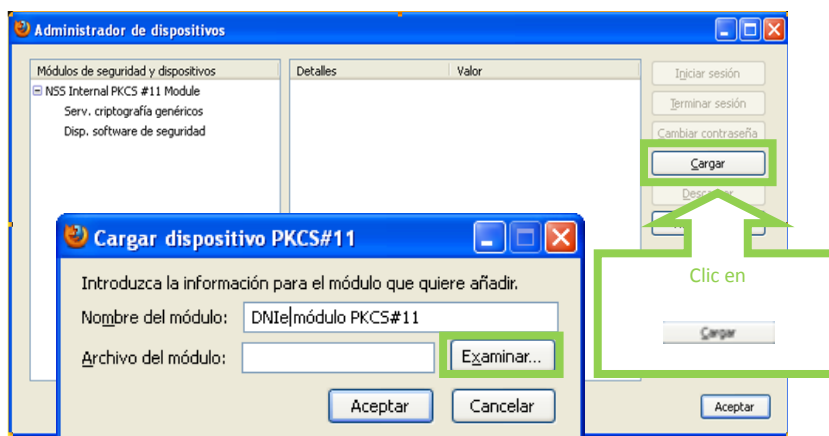
Herramientas – Opciones – Avanzado – Administrador de dispositivos

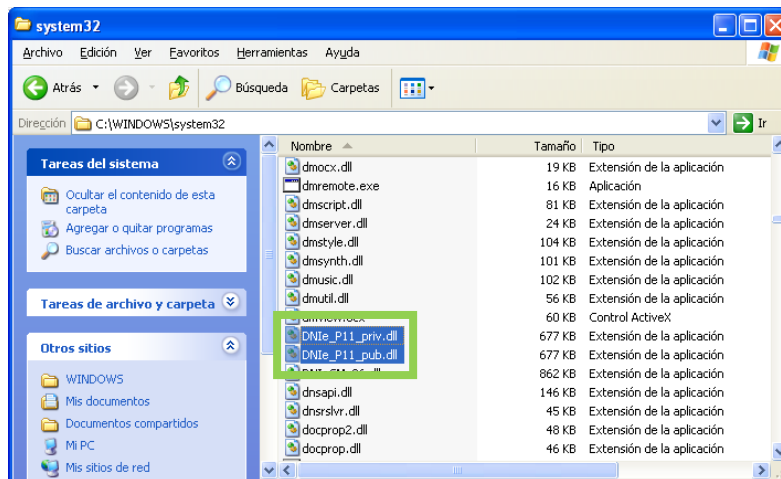


- Si fuera necesario cargarlas manualmente incorpórelas desde: **C:\WINDOWS\system32**

Dnie_p11_priv.dll

Dnie_p11_pub.dll





13º En estos momentos, el equipo está configurado para realizar gestiones con el DNle, no obstante, para su información, debe saber que hay páginas Web ajenas a este C.N.P, con las que usted puede tener problemas a la hora de operar con su DNle. En el caso de que usted tenga problemas con alguna página Web lo mejor que puede hacer es ponerse en contacto con responsables de dicho servicio.

NOTA IMPORTANTE:

Debido a las modificaciones (desarrollo webs, actualización de aplicaciones, software y hardware, etc.) que se producen frecuentemente, puede que con el paso del tiempo, alguna indicación ofrecida en este manual quede desfasada, no correspondiéndose con la realidad. No obstante, como nuestro empeño es ofrecer a todos los usuarios el mejor servicio posible, agradeceríamos que nos comunicaran cualquier incidencia que se les haya producido al respecto en la siguiente dirección: soporte.sacdni@policia.es