Dr.WEB®
CureNet!

Proteja lo que crea

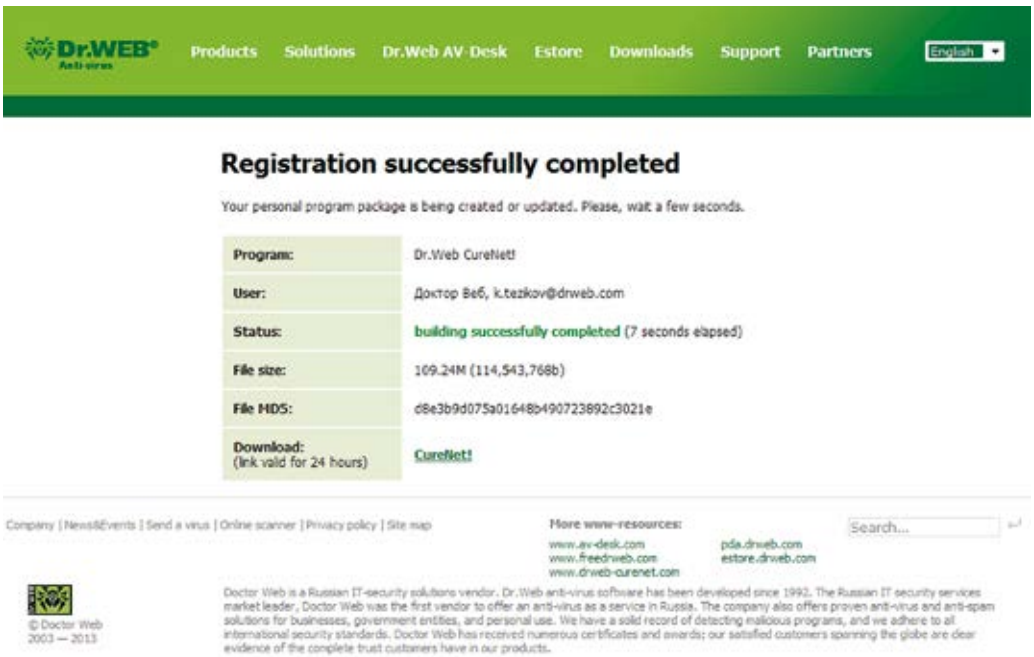
Guía rápida de configuración e inicio

Dr.Web CureNet! Está diseñado para el análisis antivirus centralizado de los equipos de la red sin necesidad de instalar el antivirus en los equipos remotos. Dr.Web CureNet! permite analizar estaciones de trabajo y servidores con un sistema operativo de Microsoft® Windows® independientemente de la configuración de la red local a la que pertenecen.

¡Atención! Dr.Web CureNet! NO ESTA DISEÑADO para la protección permanente de la red local o equipos independientes, ya que durante los intervalos entre los análisis pueden estar infectados con malware. Para obtener una protección segura de los equipos de la red local se recomienda utilizar productos, tales como Dr.Web Security Space Pro o Dr.Web Enterprise Security Suite.

Obtener la distribución de Dr.Web CureNet!

Para obtener la distribución, es necesario registrar su número de serie en la página http://products.drweb.com/register/. Al finalizar el registro se formará su distribución personal del producto, disponible para la descarga desde el Área Personal.



Se puede acceder al Área Personal desde el programa o introduciendo el número de serie en la página http://support.DrWeb.com/get+Cabinet+Link/.

Si el número de serie de Dr.Web CureNet! ya está registrado, solo tiene que acceder al Área Personal de

Dr.Web CureNet! y descargar la última versión del programa.

Requisitos del sistema

Para un análisis remoto de los equipos con Dr.Web CureNet! es necesario cumplir los siguientes requisitos:

- los equipos analizados deben ser accesibles dentro de la red;
- la cuenta del usuario, que se utiliza por Dr.Web CureNet! para conectar a los equipos analizados, debe existir y tener los privilegios administrativos necesarios;
- los puertos 139 y 445 de los equipos analizados deben estar abiertos.

Para realizar el análisis con la herramienta antivirus Dr.Web CureNet! Es necesario tener los derechos de administrador para las estaciones de trabajo y servidores correspondientes. El análisis remoto no requiere ninguna configuración adicional de los equipos, si forman parte del dominio y utilizan una cuenta de administrador del dominio. Si el equipo remoto no forma parte del dominio o se utiliza una cuenta local, algunas versiones de Windows requerirán una configuración adicional del equipo remoto. Los ajustes de Windows detallados se describen en la sección **Requisitos del sistema** de esta guía. También puede ver los videos formativos.

Debido, a que la configuración del análisis remoto puede reducir la seguridad del equipo remoto, se recomienda encarecidamente estudiar la asignación de ajustes indicados antes de realizar cambios en el sistema, o renunciar al análisis remoto y realizar el análisis antivirus expresamente en el equipo remoto fuera del dominio o utilizando una cuenta local.

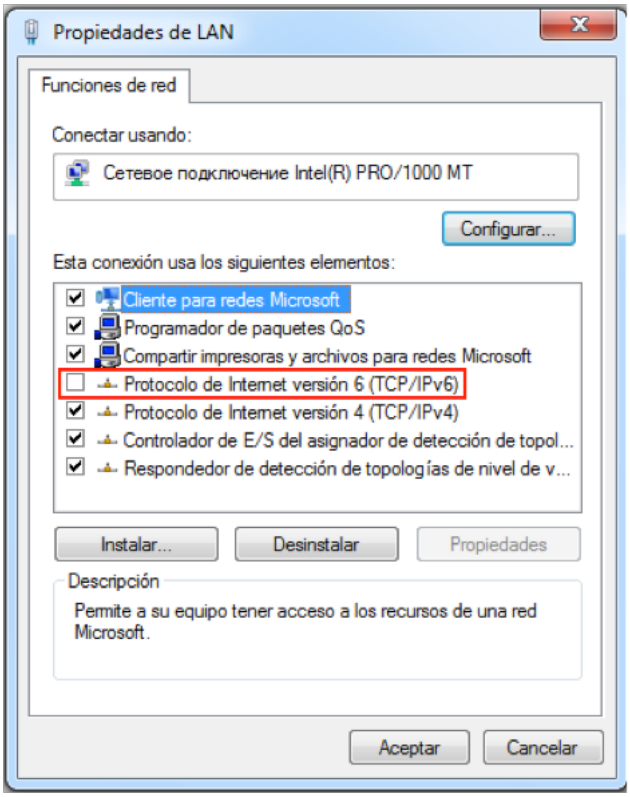
Configuración de Windows para la ejecución del Asistente

El Asistente que forma parte de la distribución de Dr.Web CureNet! es compatible con las siguientes versiones de Windows:

- Windows 2000 (Professional, Server, Advanced Server, Datacenter Server)
- Windows XP (Starter, Professional, Home Edition, Media Center Edition)
- Windows Server 2003 (Standard Edition, Enterprise Edition, 64-Bit Enterprise Edition, Datacenter Edition)
- Windows Vista (Starter, Home Basic, Home Premium, Business, Ultimate, Enterprise)
- Windows Server 2008 (Standard Edition, Enterprise Edition, Datacenter Edition)
- Windows 7 (Starter, Home Basic, Home Premium, Professional, Ultimate, Enterprise)
- Windows Server 2008 R2 (Standard, Enterprise, Datacenter)
- Windows 8, Windows 8 Professional
- Windows Server 2012 (Foundation, Essential, Standard, Datacenter)

Para el correcto funcionamiento del Asistente, es necesario cumplir dos condiciones:

1. Ausencia de caracteres del alfabeto nacional en la ruta a la carpeta de trabajo de Dr.Web CureNet!
2. Si el asistente se ejecuta en el entorno del sistema operativo Windows Vista, Windows 7, Windows 8, Windows Server 2008, Windows Server 2008 R2 o Windows Server 2012, es necesario desconectar el protocolo IPv6 en la configuración del adaptador de red. Para eso, haga clic en el botón **Inicio**, seleccione **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador**. Seleccione una conexión de red y haca clic en el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**. Desmarque la casilla de **Protocolo de Internet versión 6**.

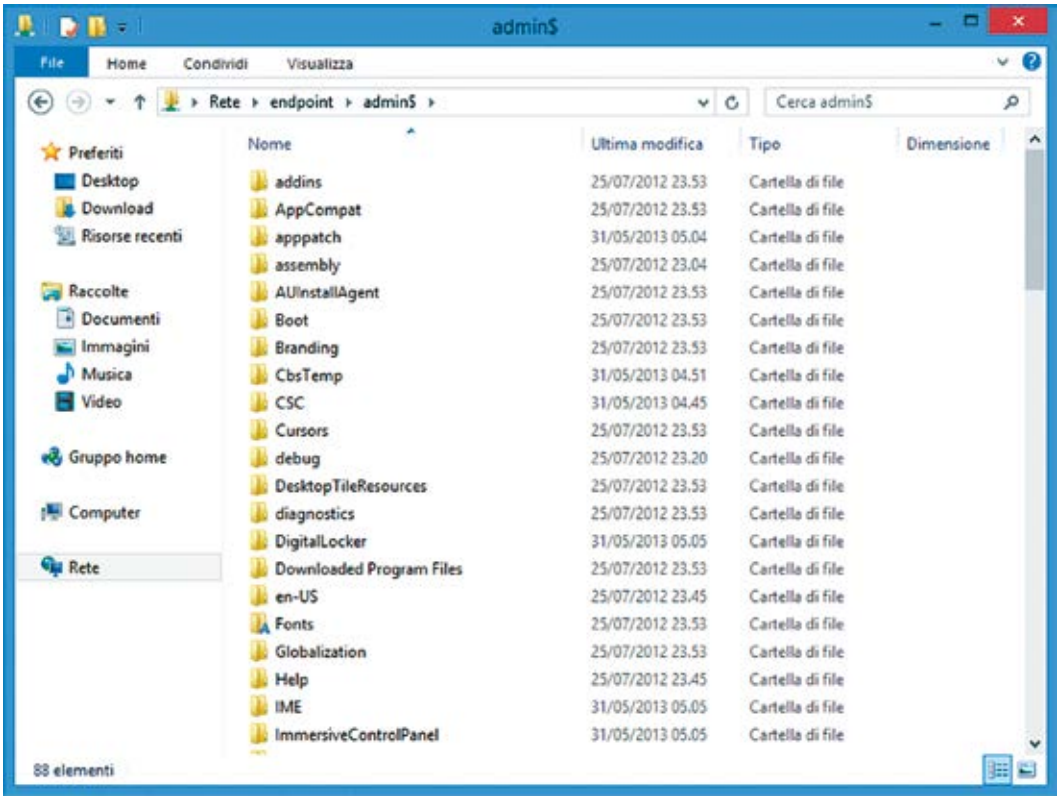


Haga clic en el botón **Aceptar**.

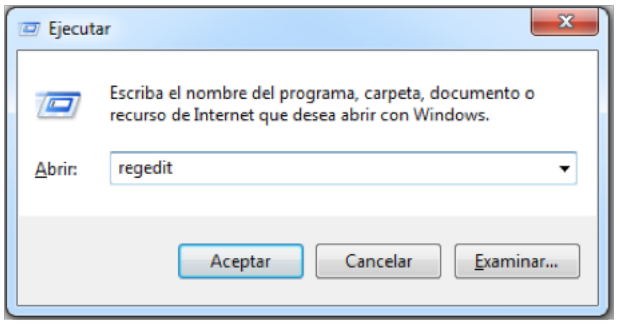
Configuración de Windows para la ejecución remota del escáner Dr.Web

Configuración general para Windows 2000 – 8, Windows Server 2003/2008/2012

Asegúrese de que los recursos administrativos generales están disponibles en el equipo. Para eso, diríjase a la carpeta de red `admin$` en el equipo remoto. Dependiendo de la configuración de Windows, posiblemente tendrá que introducir el nombre de usuario y la contraseña para iniciar la sesión como administrador. Esto abrirá una carpeta de red (ver fig. abajo).

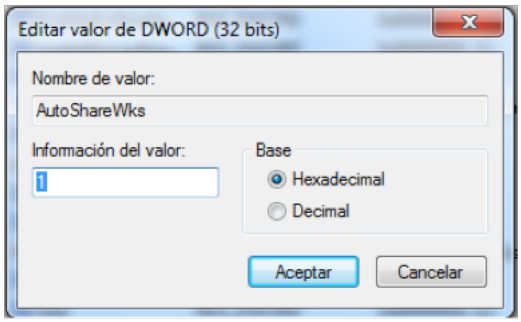


Si los recursos administrativos generales no están disponibles, es necesario realizar los siguientes ajustes en el equipo. Abre el Editor de Registro (regedit)



y seleccione `[HKEY_LOCAL_MACHINE\SYSTEM\CURRENTCONTROLSET\SERVICES\LANMANSERVER\PARAMETERS]`

Es necesario crear un valor tipo DWORD (32bits) **AutoShareWks** (sin comillas) y en el campo **Información del valor** introducir uno (1).



Reinicie el equipo. Los recursos administrativos generales estarán activados.

Configuración de Windows 2000

1. Inicio de la cuenta del administrador.
2. Configuración de componentes de red.

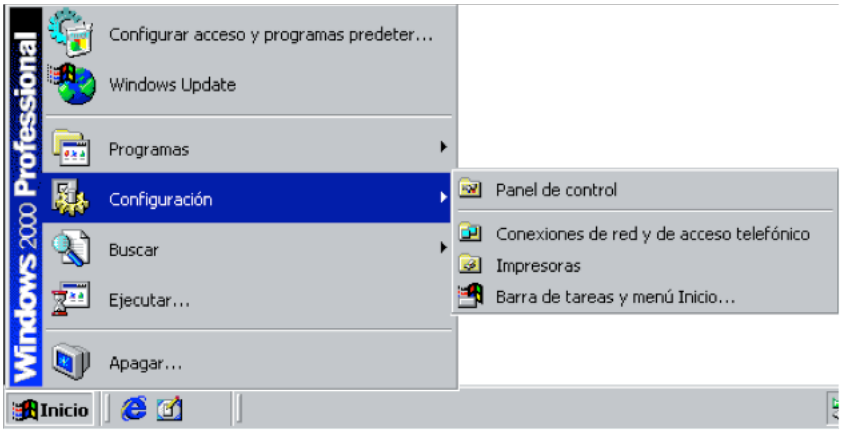
Importante! El sistema debe tener instalado Service Pack 4 + Rollup 1.

Descargar Service Pack 4 para Windows 2000:
http://www.microsoft.com/ru-ru/download/details.aspx?id=4127

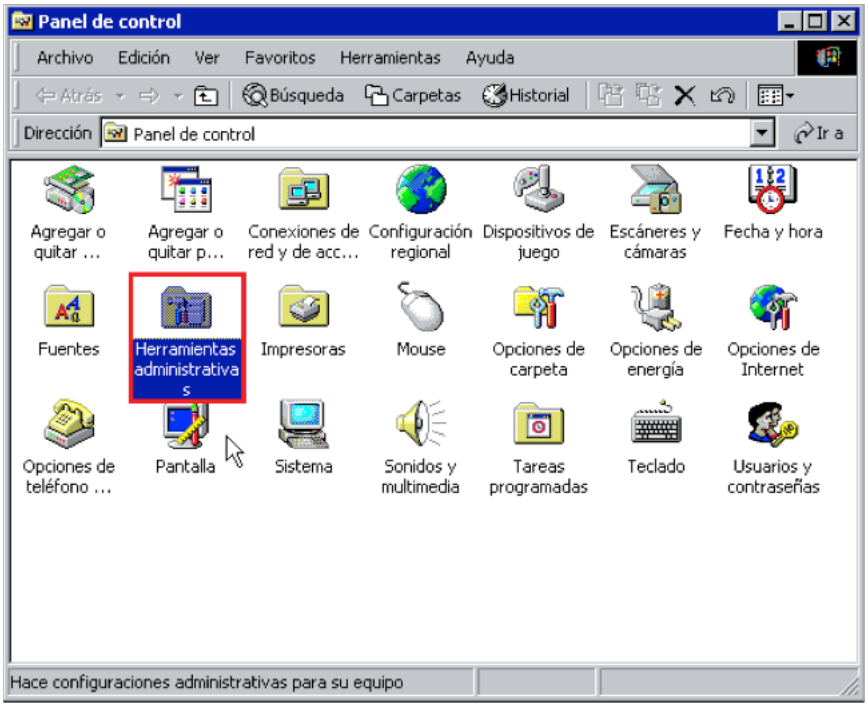
Descargar Rollup 1 para Windows 2000 Service Pack 4:
http://www.microsoft.com/ru-ru/download/details.aspx?id=18997

1. Inicio de la cuenta del administrador.

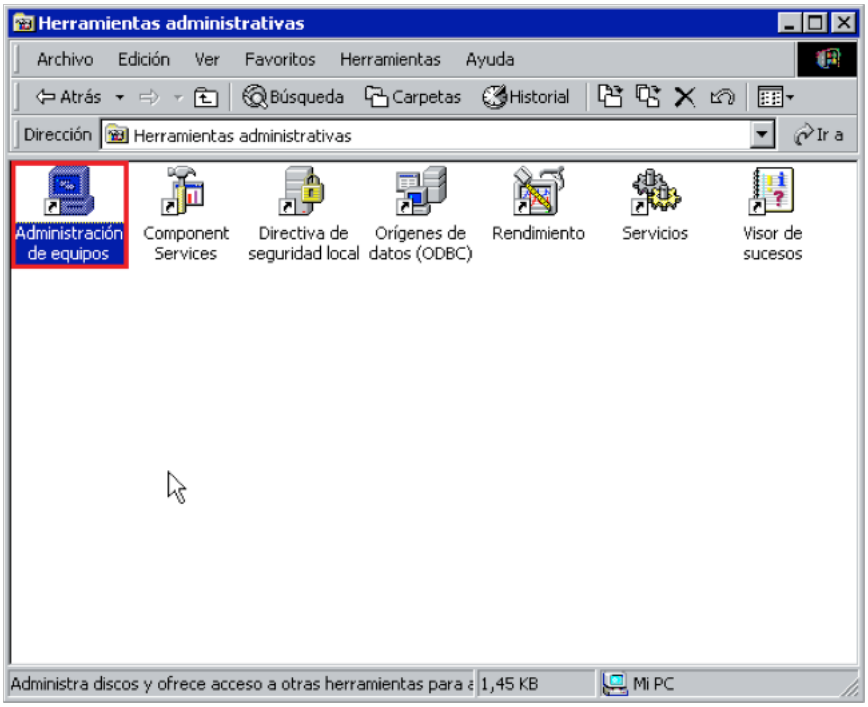
Haga clic en el botón **Inicio**, seleccione el menú **Configuración** → **Panel de Control**



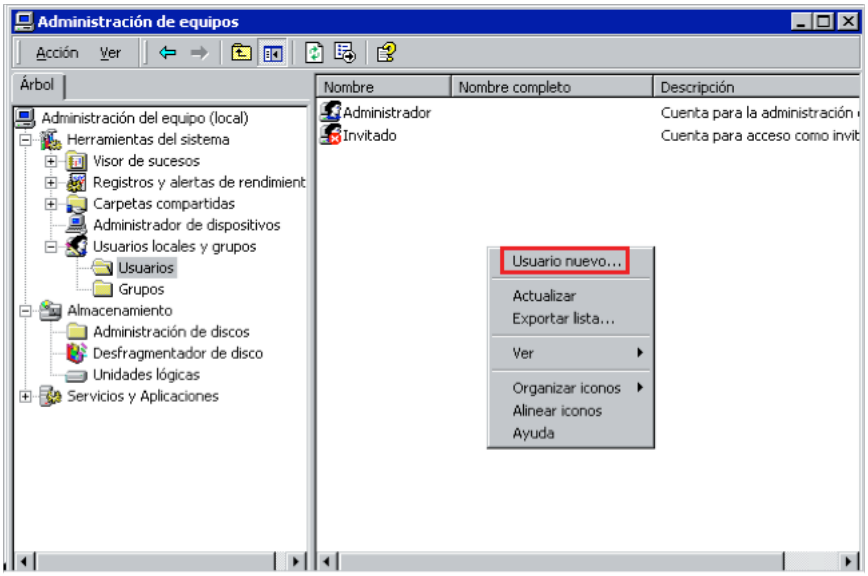
→ Herramientas administrativas



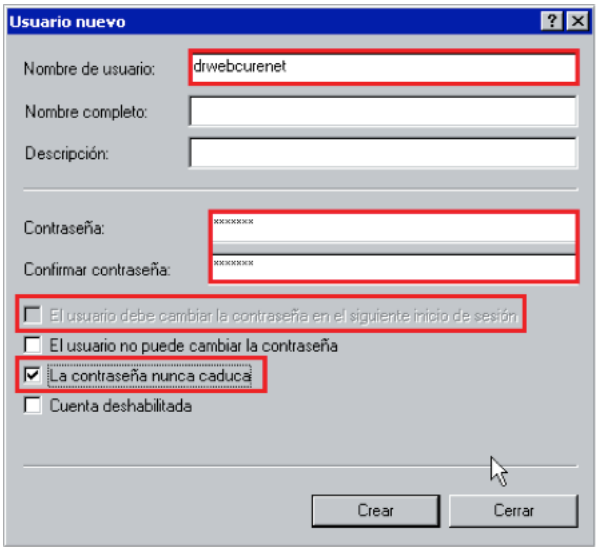
→ Administración de equipos



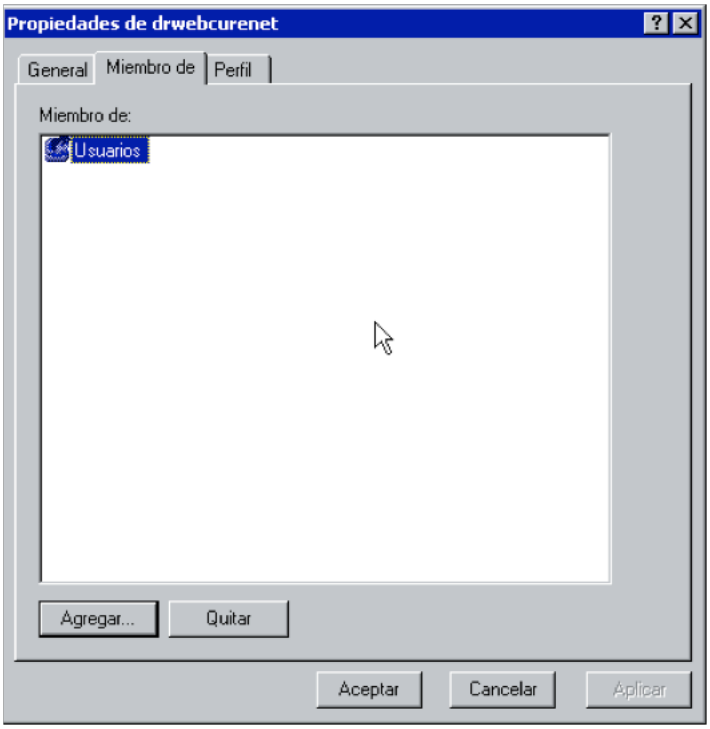
→ **Usuarios locales y grupos** → **Usuarios**. Ahora puede seguir trabajando con la cuenta de administrador, pero para aumentar la privacidad es aconsejable crear una cuenta de administrador alternativa. Para eso haga clic en el botón derecho del ratón y en el menú contextual que aparece seleccione la opción **Usuario nuevo**.



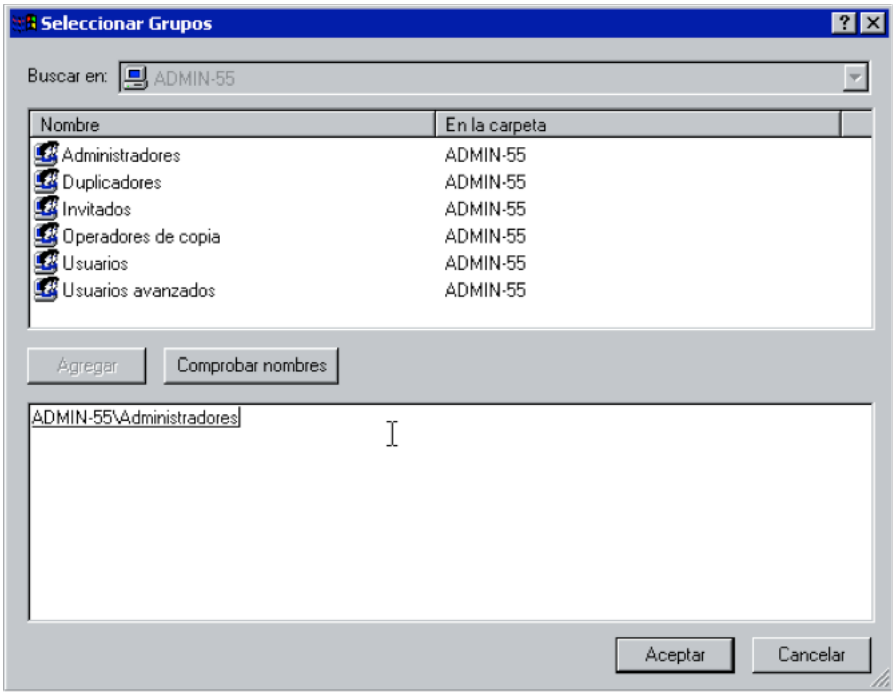
Introduzca el nombre de usuario: DrWebCurenet. En los campos **Contraseña** y **Confirmar contraseña** introduzca una contraseña segura. Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Marque la casilla **La contraseña nunca caduca**.



Haga clic en el botón **Crear** y luego en **Cerrar.** Con el botón izquierdo del ratón haga doble clic en la cuenta creada - DrWebCurenet y diríjase a la pestaña **Miembro de**. Seleccione **Usuarios** y haga clic en el botón **Quitar**.



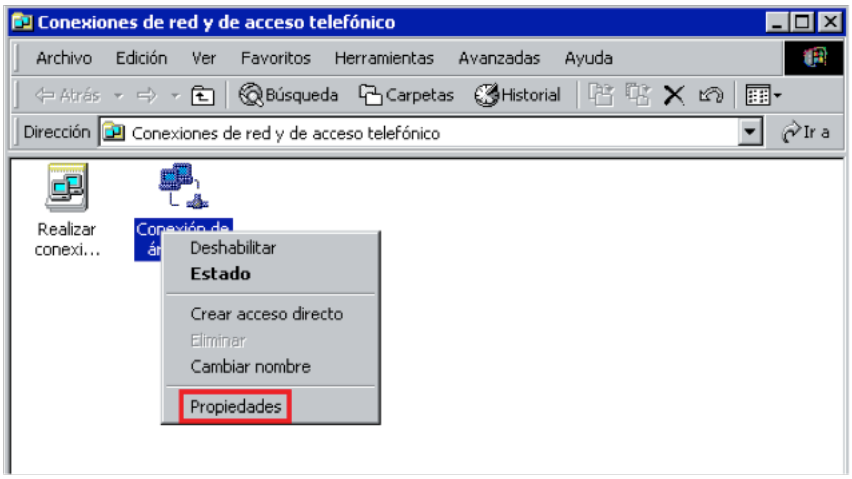
A continuación, haga clic en el botón **Agregar**. Aparecerá la ventana de **Seleccionar Grupos**, en la parte superior haga clic en **Administradores**, y a continuación en **Agregar** u **Aceptar**.



En la ventana de **Propiedades de DrWebCurenet** haga clic en **Aplicar** y a continuación en **Aceptar**. Cierre la ventana de **Administración de equipos**.

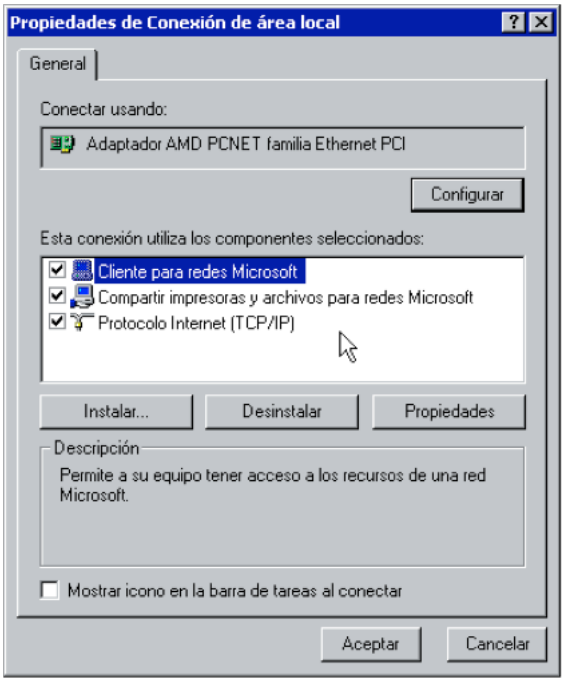
2. Configuración de componentes de red.

Haga clic en el botón **Inicio** y seleccione **Configuración → Conexiones de red y de acceso telefónico**. Seleccione una conexión de red u haga clic en el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**.



Asegúrese de que los siguientes componentes están activados:

- Cliente para redes Microsoft
- Compartir impresoras y archivos para redes Microsoft
- Protocolo Internet (TCP/IP)



Haga clic en el botón **Aceptar**. Si está utilizando un firewall, es necesario abrir los puertos 139 y 445.

Configuración de Windows XP y Windows Server 2003

1. Inicio de la cuenta del administrador.
2. Configuración de uso compartido de archivos (no se requiere para Windows 2003)
3. Configuración de directiva de seguridad local
4. Configuración del Firewall de Windows
5. Configuración de componentes de red.

Importante! El sistema operativo Windows XP debe tener instalado el Service Pack 2 o 3.

Descargar Service Pack 2 para Windows XP:
http://www.microsoft.com/ru-ru/download/details.aspx?id=28

Descargar Service Pack 3 para Windows XP (recomendado):
http://www.microsoft.com/ru-ru/download/details.aspx?id=24

Versiones compatibles:

- Windows XP Professional

Las siguientes versiones no son compatibles:

- Windows XP Starter
- Windows XP Home Edition

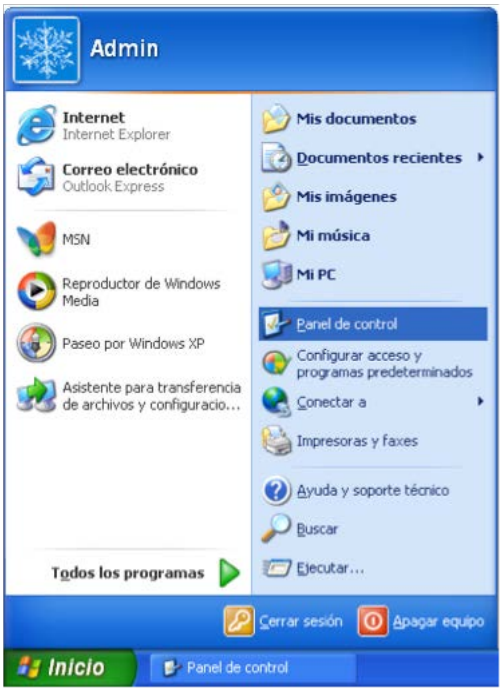
El sistema operativo Windows 2003 debe tener instalado el Service Pack 1 o 2.

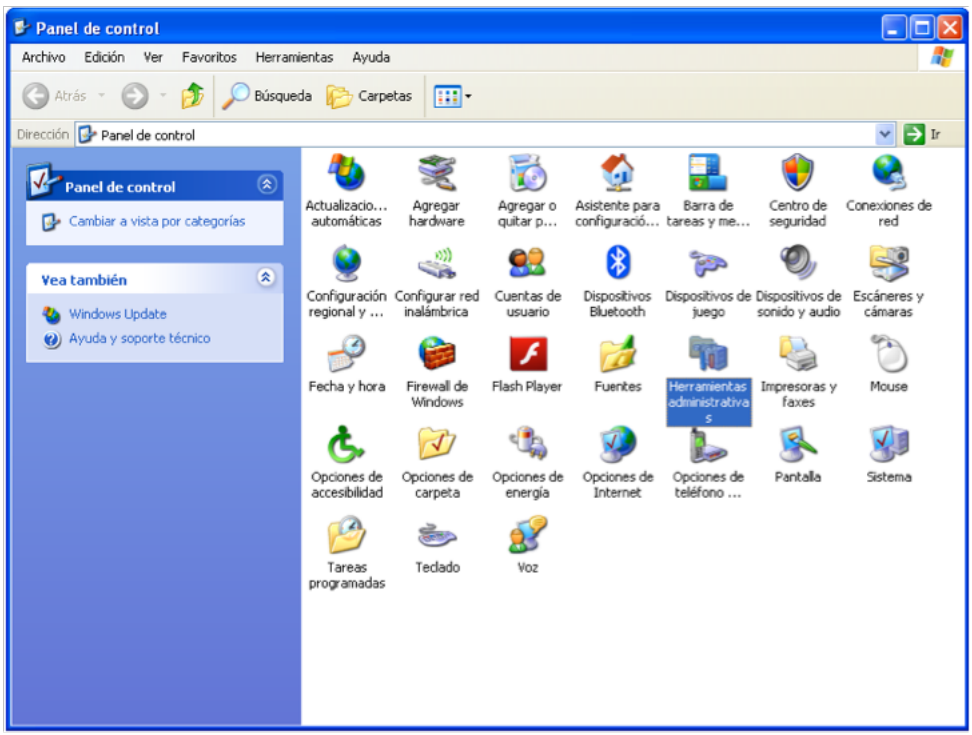
Descargar Service Pack 1 para Windows 2003:
http://www.microsoft.com/ru-ru/download/details.aspx?id=11435

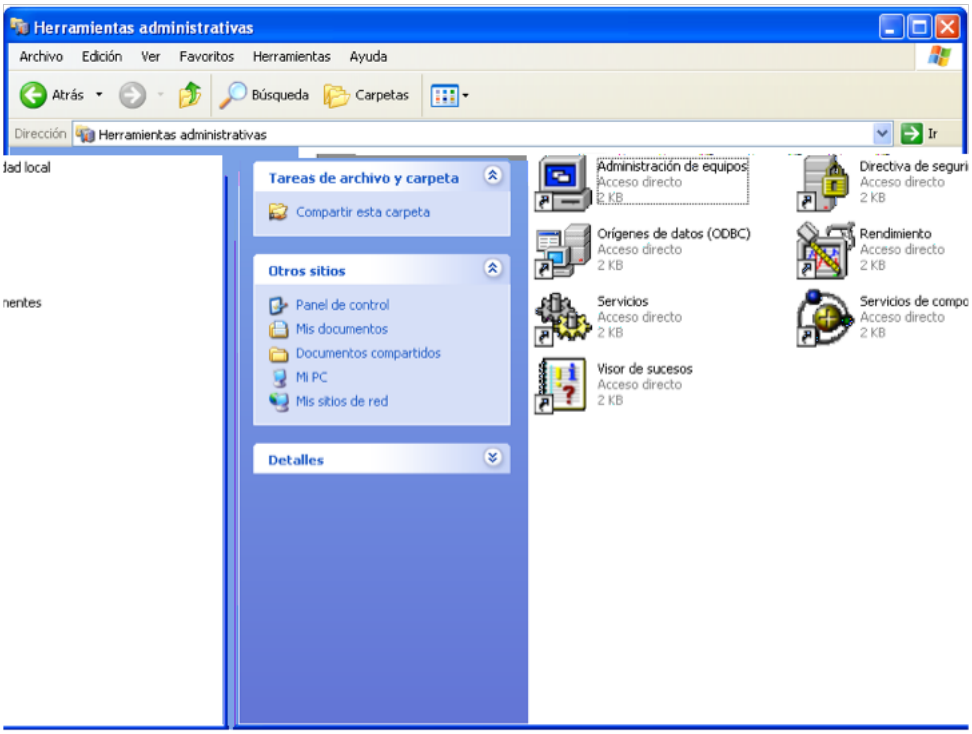
Descargar Service Pack 2 para Windows 2003 (recomendado):
http://www.microsoft.com/ru-ru/download/details.aspx?id=41

1. Inicio de la cuenta del administrador.

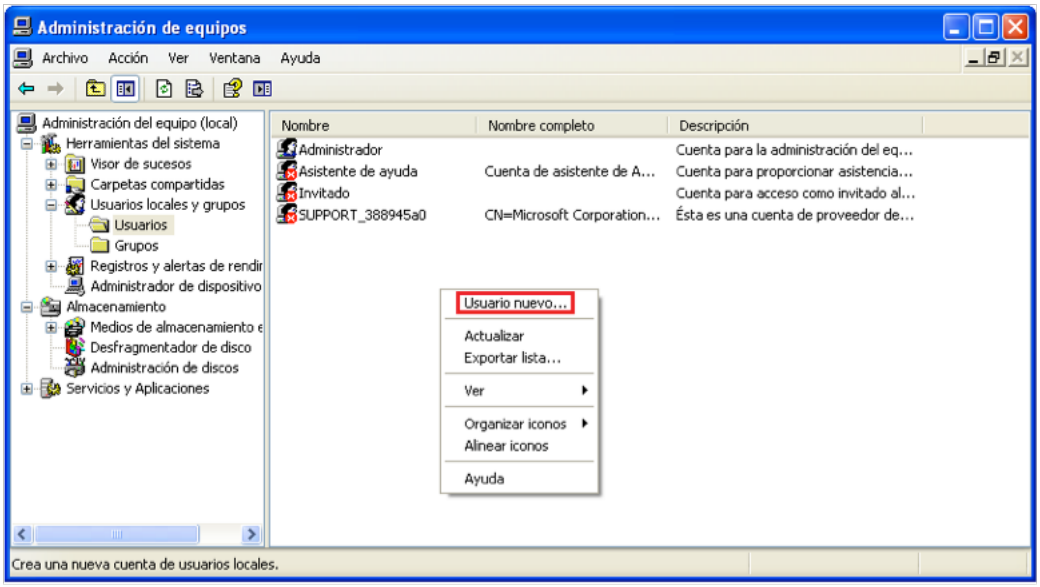
Haga clic en el botón **Inicio**, seleccione **Panel de control** → **Herramientas administrativas** → **Administración de equipos** → **Usuarios locales y grupos** → **Usuarios**.



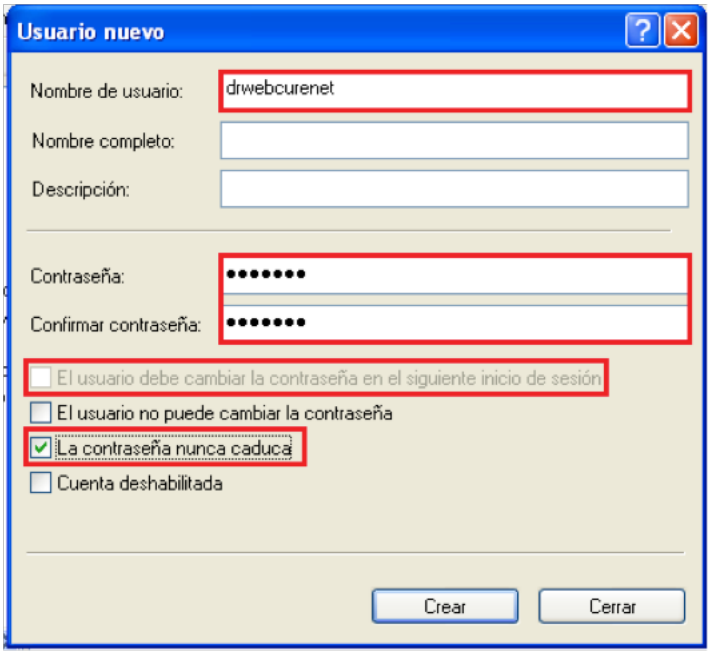




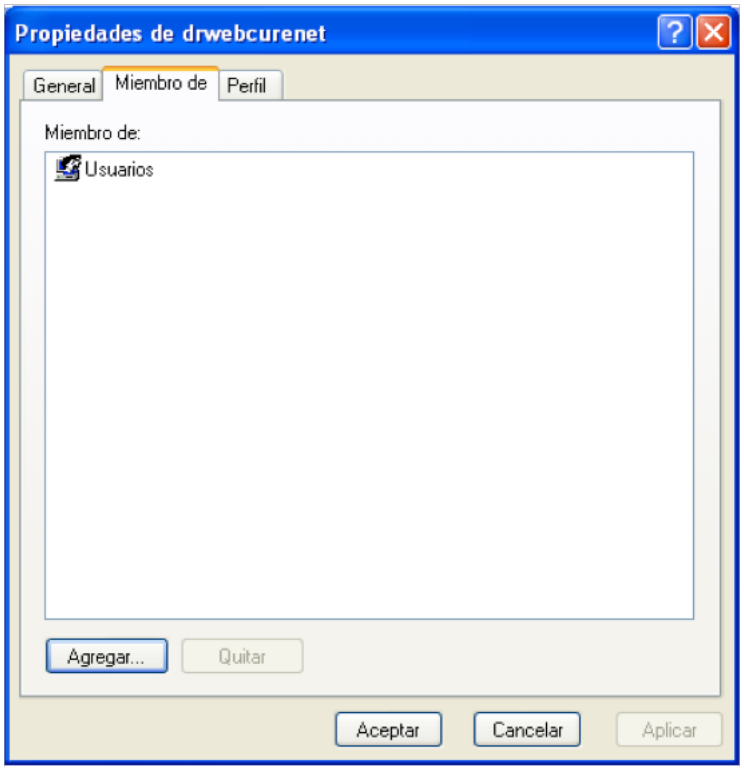
Ahora puede seguir trabajando con la cuenta de **Administrador**, pero para aumentar la privacidad es aconsejable crear una cuenta de administrador alternativa. Para eso haga clic en el botón derecho del ratón y en el menú contextual que aparece seleccione la opción **Usuario nuevo**.



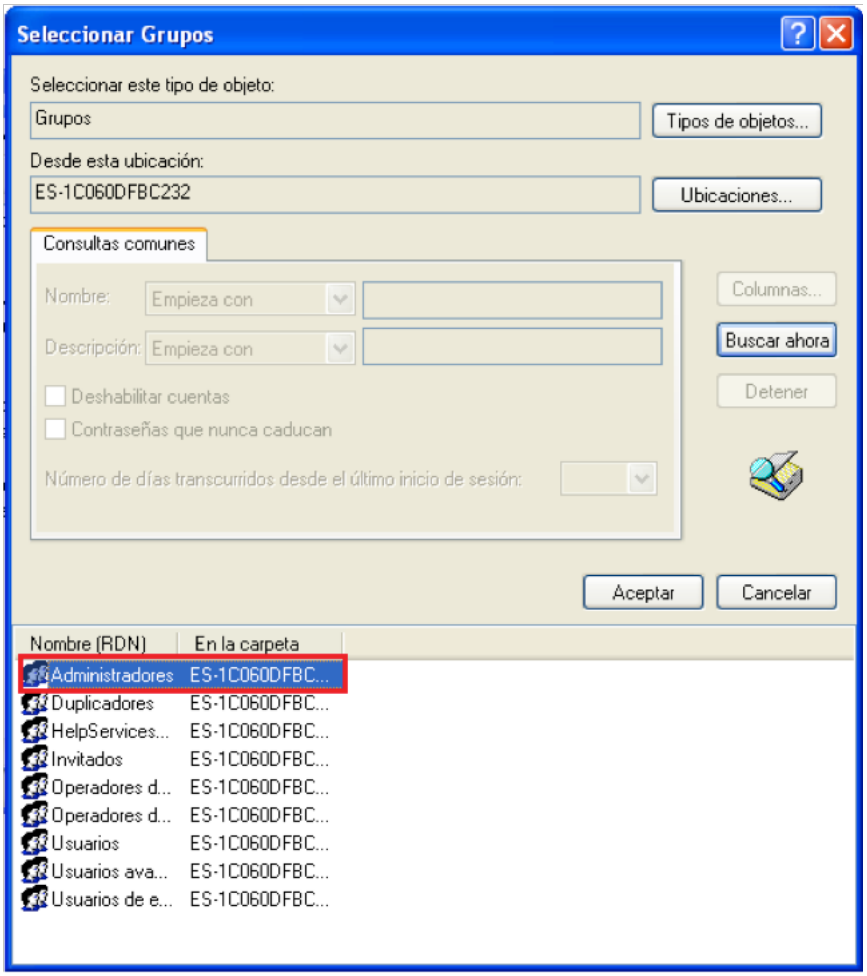
Introduzca el nombre de usuario - DrWebCureNET, en los campos **Contraseña** y **Confirmar contraseña** introduzca una contraseña segura. Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Habilite la opción **La contraseña nunca caduca**. Haga clic en el botón **Crear**, y luego - en el botón **Cerrar**.

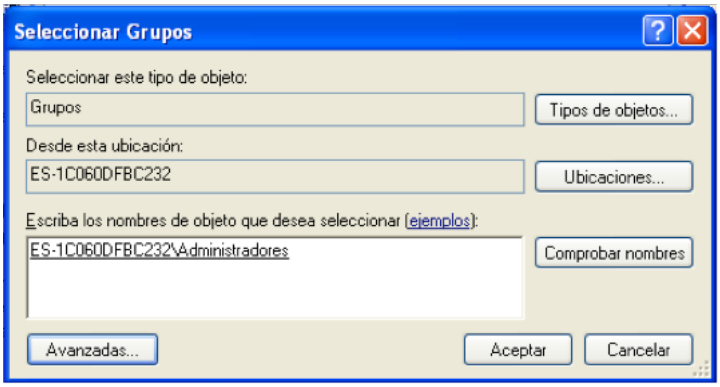


Haga doble clic en la cuenta creada – DrWebCurenet. Se abrirá la ventana de **Propiedades de DrWebCurenet**. Haga clic en la pestaña **Miembro de**.



En la ventana **Miembro de** seleccione **Usuarios** y haga clic en el botón **Quitar**. A continuación, haga clic en el botón **Agregar**. Aparecerá la ventana de **Seleccionar Grupos**. Haga clic en el botón **Avanzadas**, y luego - en el botón Buscar ahora. En la lista generada, seleccione **Administradores**, haga clic en el botón **Aceptar** y, a continuación - haga clic en el botón **Aceptar** en la ventana de **Seleccionar Grupos**.

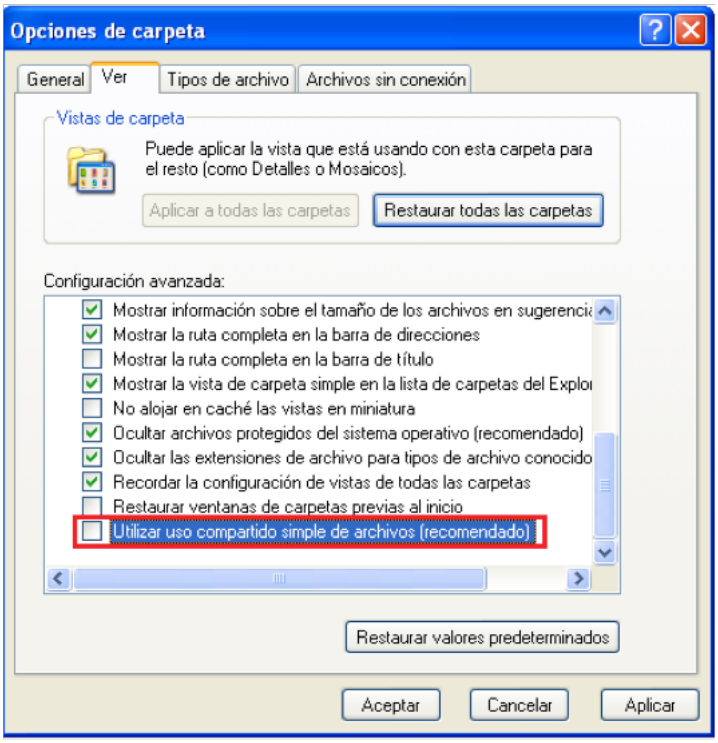




En la ventana de **Propiedades: Dr.WebCurenet** haga clic en **Aplicar** y luego en **Aceptar**.

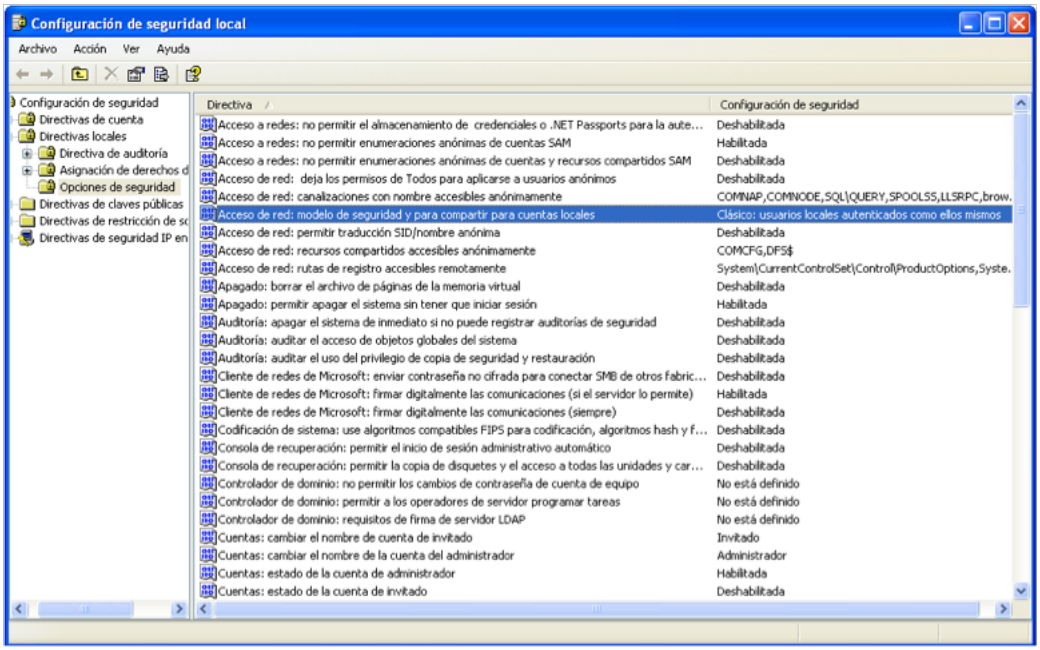
2. Configuración de uso compartido de archivos.

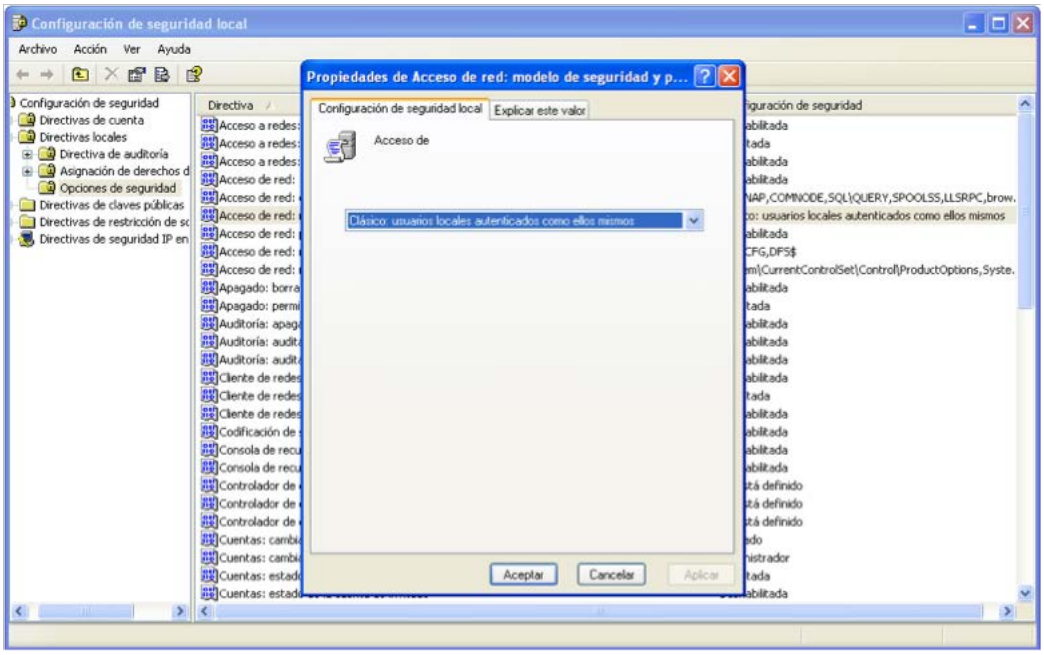
Haga clic en el botón **Inicio**, seleccione **Panel de control → Cambiar a vista clásica → Opciones de carpeta**. Aparecerá la ventana de **Opciones de carpeta**. Diríjase a la pestaña **Ver**. Desactive la opción **Utilizar uso compartido simple de archivos**. Haga clic en **Aplicar** y luego en **Aceptar**.



3. Configuración de directiva de seguridad local.

Diríjase al **Panel de control → Herramientas administrativas → Directiva de seguridad local → Directivas locales → Opciones de seguridad**. Seleccione con el cursor la política **Acceso de red: Modelo de seguridad y para compartir para cuentas locales** y haga doble clic con el botón izquierdo del ratón. Se abrirá la ventana de **Propiedades**. Seleccione la opción **Clásico**.

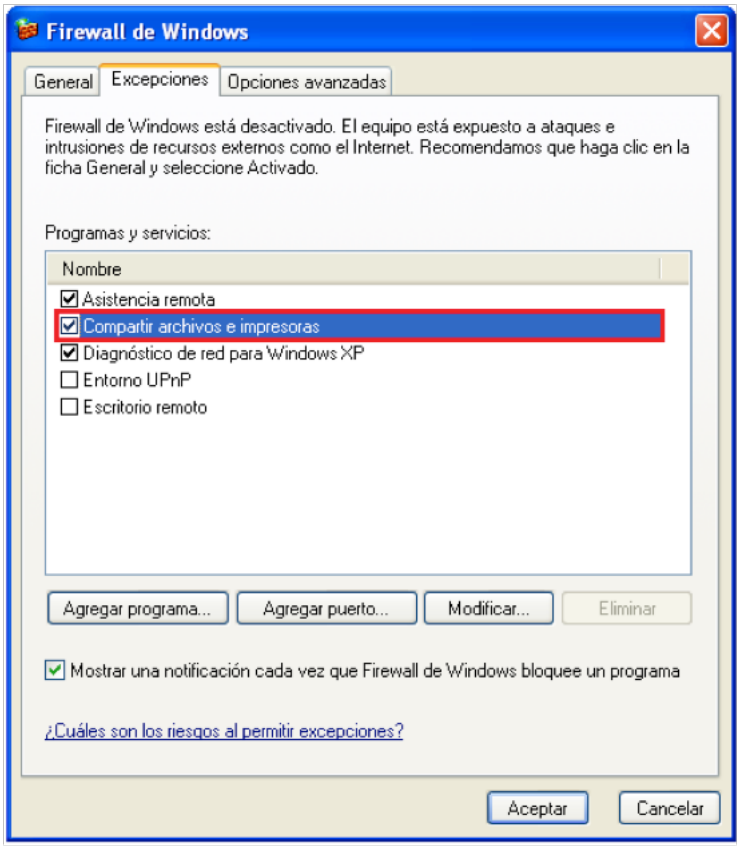




Haga clic en el botón **Aplicar** y luego en **Aceptar**. Cierre la ventana de **Configuración de seguridad local**.

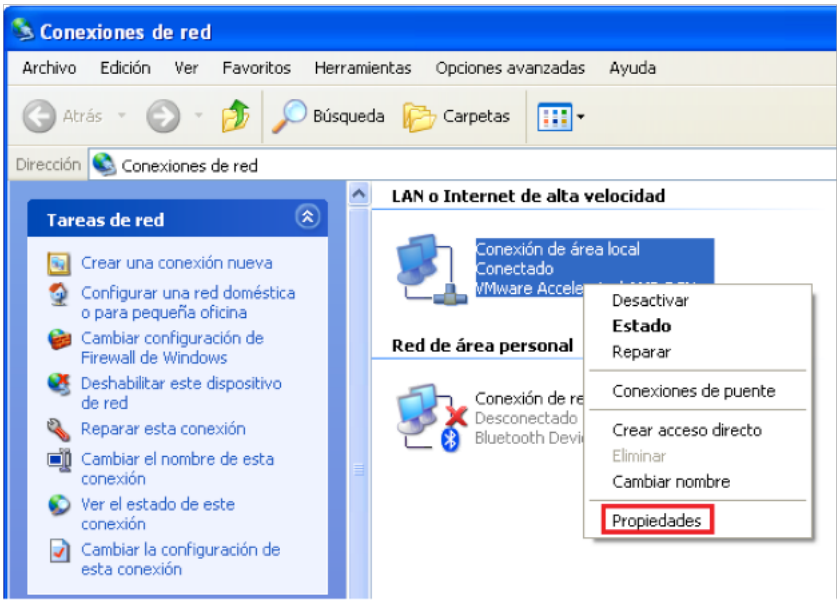
4. Configuración del firewall.

Si está utilizando un firewall de terceros, es necesario abrir los puertos 139 y 445. Si el firewall que utiliza es de Windows, hay que configurar lo siguiente: Haga clic en el botón **Inicio**, seleccione **Panel de control → Firewall de Windows**. Se abrirá la ventana **Firewall de Windows**. Diríjase a la pestaña **Excepciones**. Habilite la opción **Compartir archivos e impresoras**. Haga clic en el botón **Aceptar**.



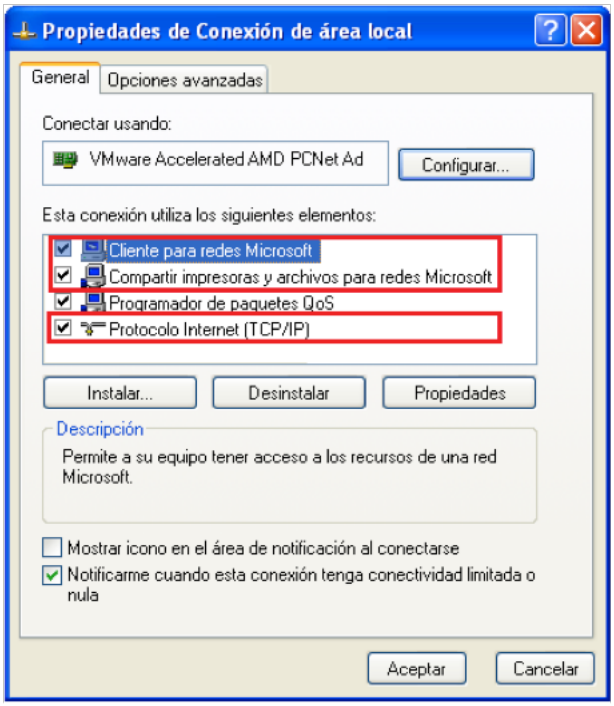
5. Configuración de componentes de red.

Haga clic en el botón **Inicio**, seleccione **Panel de control** → **Conexiones de red**. Seleccione una conexión de red y haga clic en el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**. Aparecerá una ventana de Propiedades de conexión.



Diríjase a la pestaña **General**. Asegúrese de que los siguientes componentes están activados:

- Cliente para redes Microsoft
- Compartir impresoras y archivos para redes Microsoft
- Protocolo Internet (TCP/IP)



Haga clic en el botón **Aceptar**.

Configuración de Windows Vista y Windows Server 2008

1. Configuración de control de cuentas de usuario (para Windows Vista)
2. Configuración de parámetros de acceso compartido
3. Inicio de la cuenta del administrador
4. Configuración del Firewall de Windows
5. Configuración de componentes de red
6. Configuración de directiva de seguridad local

Importante! El sistema debe tener instalado:

- Para Windows Vista - Service Pack 1 ó 2.
- Para Windows Server 2008 - Service Pack 2.

Descargar Service Pack 1 para Windows Vista:
http://www.microsoft.com/ru-ru/download/details.aspx?id=910

Descargar Service Pack 2 para Windows Vista (recomendado):
http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

Descargar Service Pack 2 para Windows Server 2008:
http://www.microsoft.com/ru-ru/download/details.aspx?id=15278

Versiones compatibles:

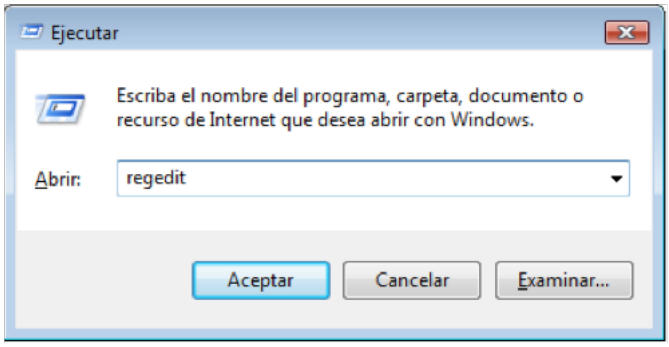
- Windows Vista Business
- Windows Vista Enterprise
- Windows Vista Ultimate

Las siguientes versiones no son compatibles:

- Windows Vista Starter
- Windows Vista Home Basic
- Windows Vista Home Premium

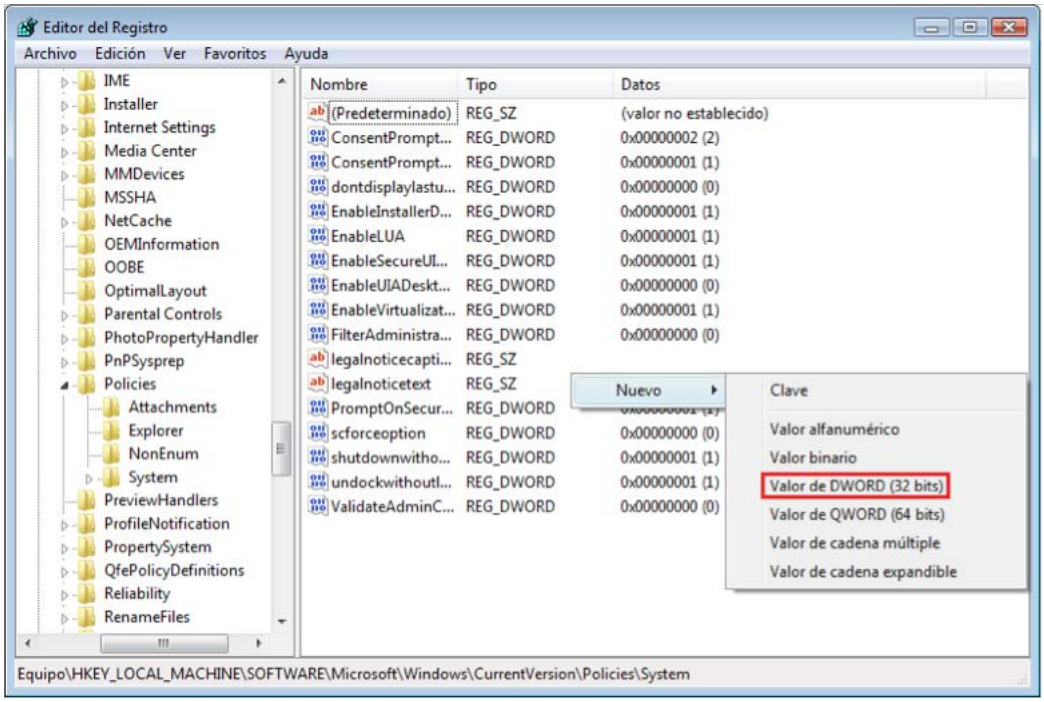
1. Configuración de Control de cuentas de usuario (para Windows Vista).

Pulse las teclas **Windows + R**.

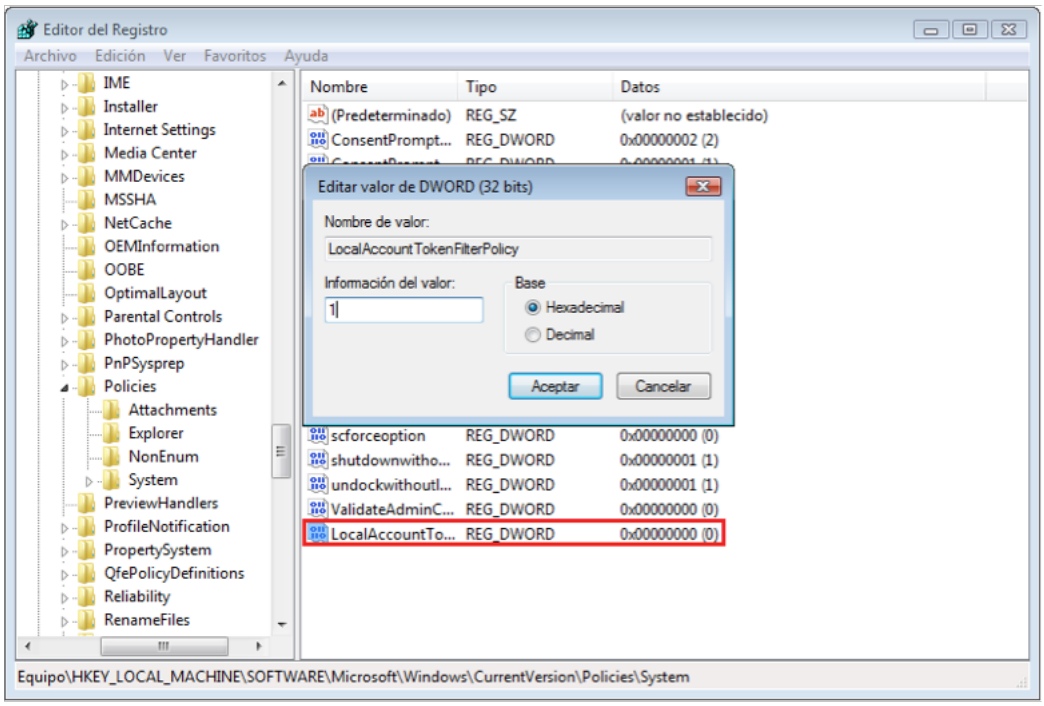


En la ventana que se abre introduzca **regedit**. Aparecerá la ventana del Editor del registro de Windows. Seleccione `[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]`

Diríjase a la parte derecha de la ventana del Editor de registro de Windows, haga clic con el botón derecho del ratón y en el menú contextual seleccione **Nuevo → Valor de DWORD (32 bits)**.



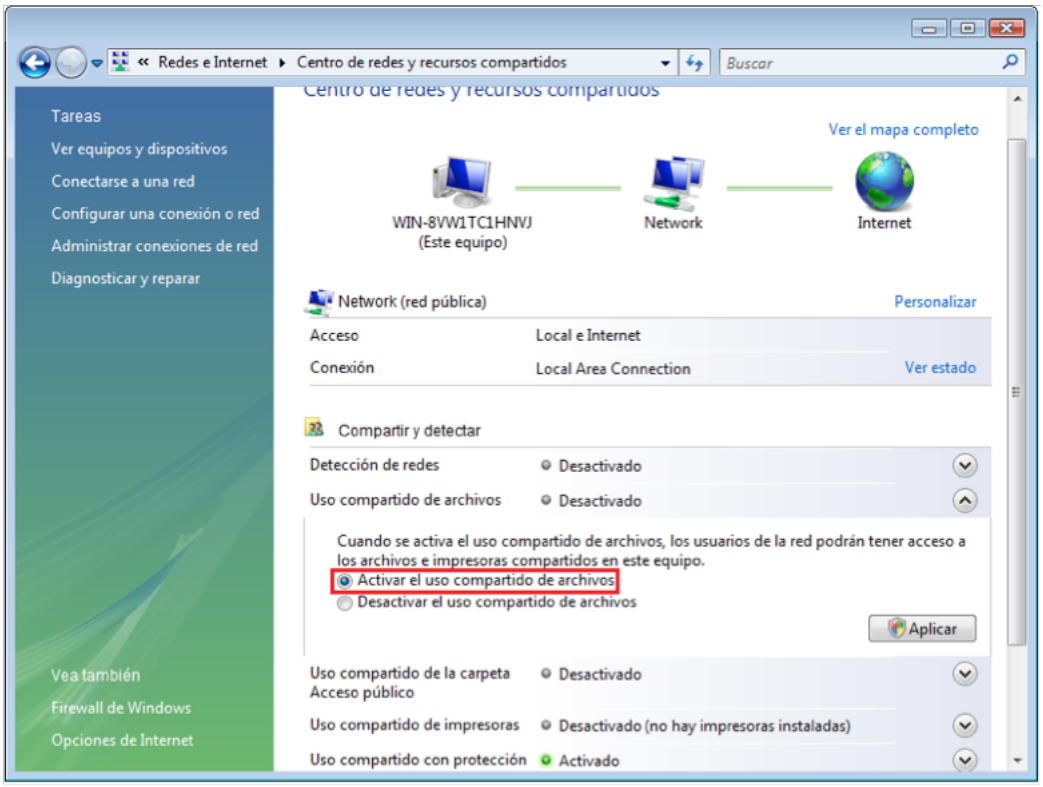
Establezca el nombre del parámetro LocalAccountTokenFilterPolicy. Haga doble clic en el parámetro creado con el botón izquierdo del ratón. Se abrirá la ventana de **Editar valor DWORD (32 bits)**. En el campo **Información del valor** introduzca el valor 1 y haga clic en **Aceptar**.



Cierre el Editor del registro de Windows. Realice los demás ajustes (párrs. 2-6) y reinicie el equipo.

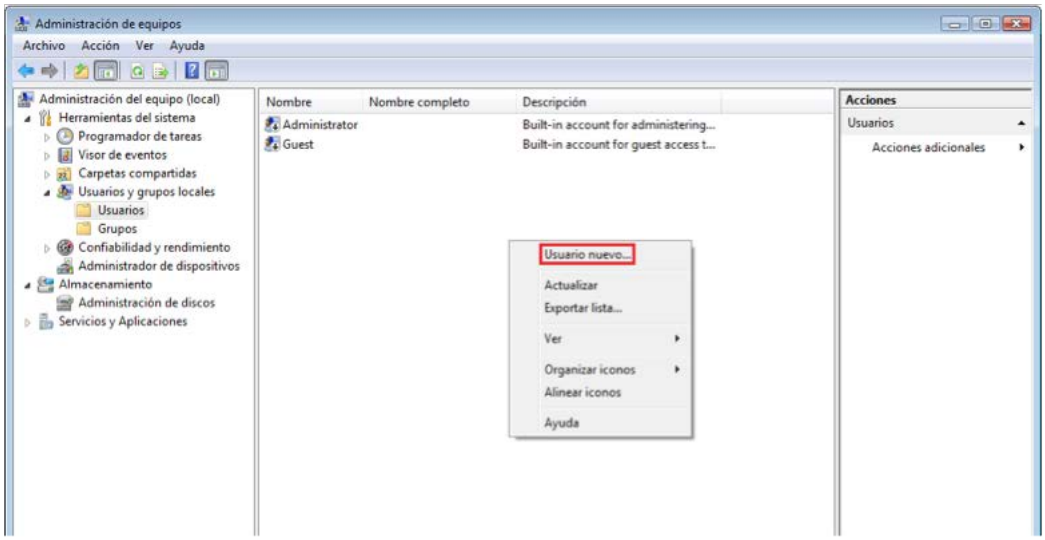
2. Configuración de parámetros de acceso compartido.

Haga clic en el botón **Inicio**, seleccione **Panel de control → Redes e Internet → Centro de redes y recursos compartidos**. En el grupo **Compartir y detectar** active la opción **Uso compartido de archivos** Haga clic en el botón **Aplicar**.

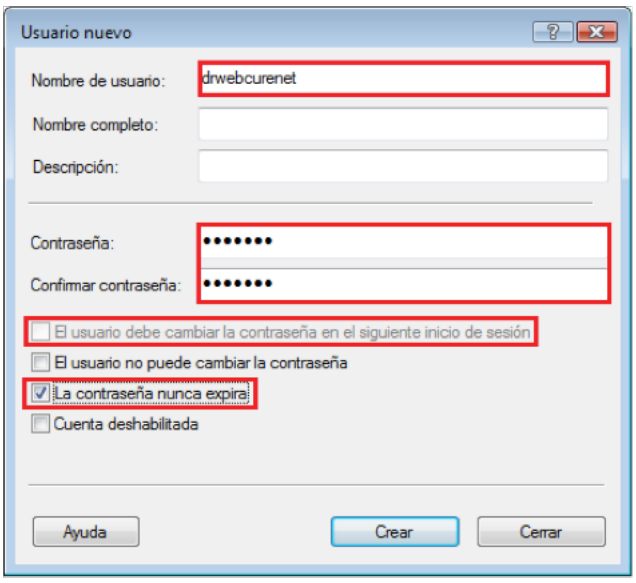


3. Inicio de la cuenta del administrador.

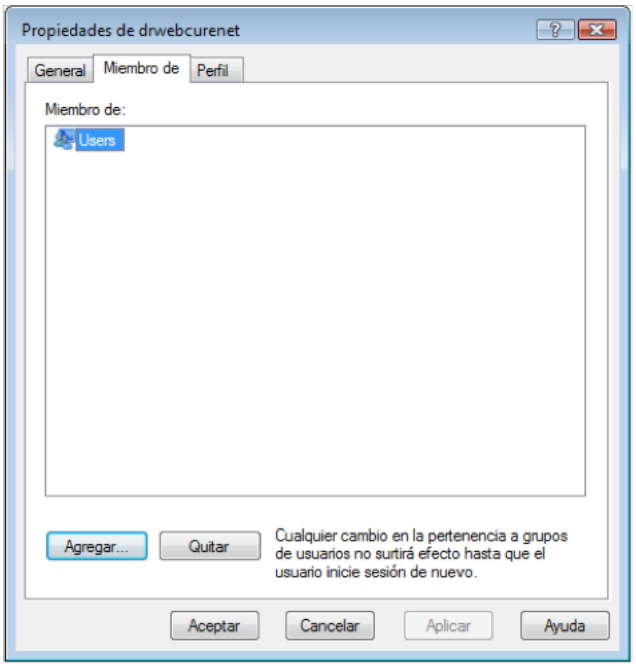
Haga clic en el botón **Inicio**, seleccione **Panel de control → Sistema y mantenimiento → Herramientas administrativas → Administración de equipos → Usuarios y grupos locales → Usuarios**. Ahora puede seguir trabajando con la cuenta de **Administrador**, pero para aumentar la privacidad es aconsejable crear una cuenta de administrador alternativa. Para eso haga clic en el botón derecho del ratón y en el menú contextual que aparece seleccione la opción **Usuario nuevo**.



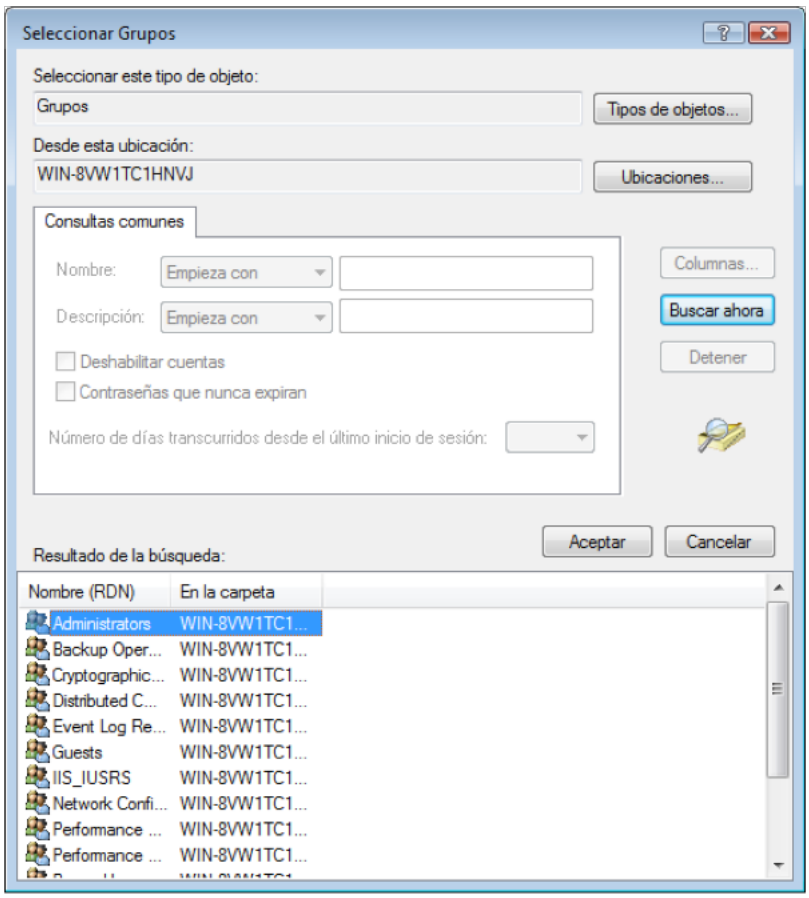
Introduzca el nombre de usuario - DrWebCurenet. En los campos **Contraseña** y **Confirmar contraseña** introduzca una contraseña segura. Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Marque la casilla **La contraseña nunca expira.**



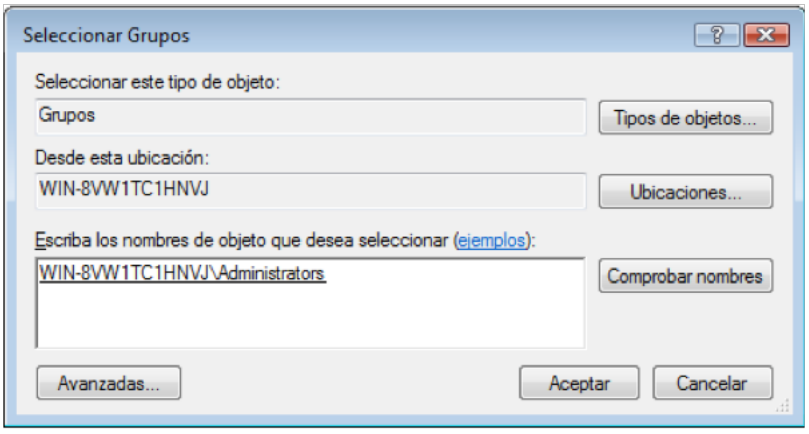
Haga clic en el botón **Crear** y luego en **Cerrar**. Con el botón izquierdo del ratón haga doble clic en la cuenta creada - DrWebCurenet y diríjase a la pestaña **Miembro de**.



Seleccione **Usuarios** y haga clic en el botón **Quitar**. A continuación, haga clic en el botón **Agregar**. Aparecerá la ventana de **Seleccionar Grupos**. Haga clic en el botón **Avanzadas**, y luego - en el botón **Buscar ahora**. En los resultados de búsqueda, seleccione la opción **Administradores** y haga clic en **Aceptar**.



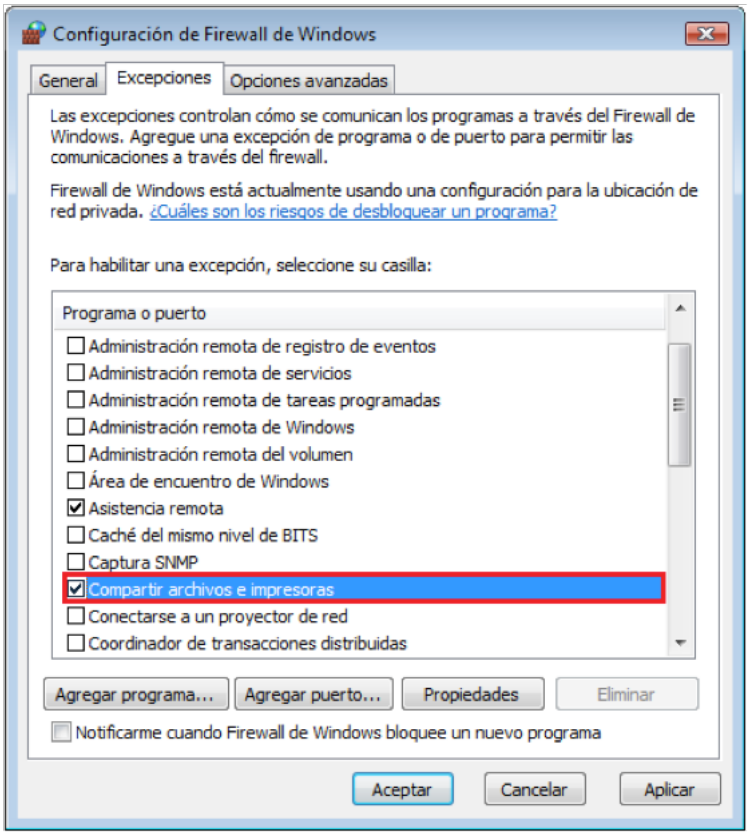
En la ventana de **Seleccionar Grupos** haga clic en el botón **Aceptar**.



En la ventana de **Propiedades de DrWebCurenet** haga clic en el botón **Aplicar** y luego en **Aceptar**:

4. Configuración del firewall.

Si está utilizando un firewall de terceros, es necesario abrir los puertos 139 y 445. Si el firewall que utiliza es de Windows, hay que configurar lo siguiente: Haga clic en el botón **Inicio**, seleccione **Panel de control → Seguridad → Firewall de Windows**. Diríjase al enlace **Activar o desactivar Firewall de Windows**. En la ventana de **Configuración de Firewall de Windows**, haga clic en la pestaña **Excepciones**. Seleccione la casilla **Compartir archivos e impresoras**.

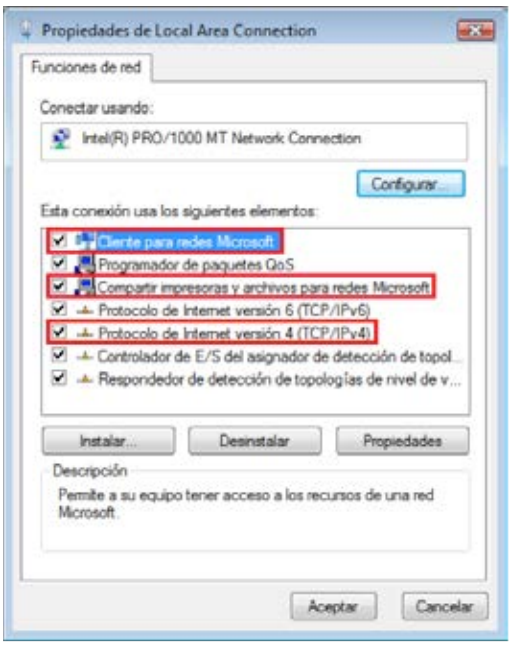


Haga clic en el botón **Aceptar**.

5. Configuración de componentes de red.

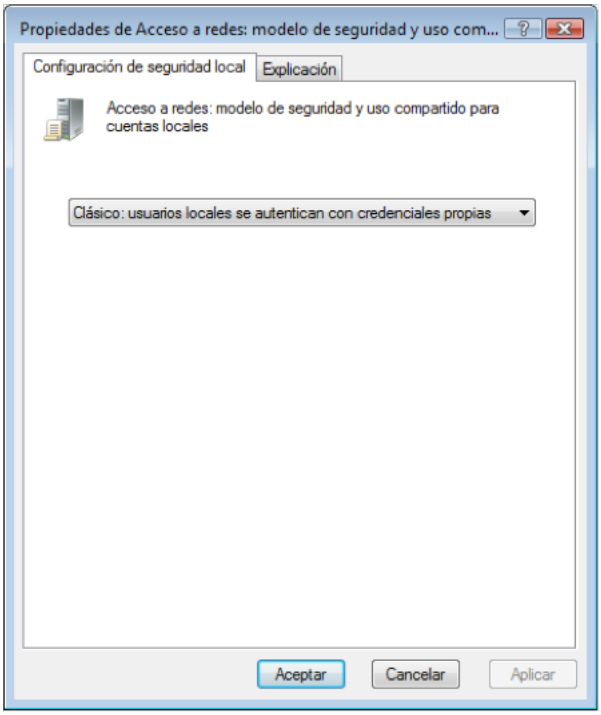
Haga clic en el botón **Inicio**, seleccione **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Administrar conexiones de red**. Seleccione una conexión de red, y haga clic en el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**. Asegúrese de que los siguientes componentes están activados:

- Cliente para redes Microsoft
- Compartir impresoras y archivos para redes Microsoft
- Protocolo de Internet Versión 4



6. Configuración de la directiva de seguridad local.

Haga clic en el botón **Inicio**, seleccione **Panel de control** → **Sistema y Mantenimiento** → **Herramientas administrativas** → **Directiva de seguridad local** → **Directivas locales** → **Opciones de seguridad**. Seleccione con el cursor del ratón la directiva **Acceso a redes: modelo de seguridad y uso compartido para cuentas locales**. Haga doble clic en el botón izquierdo del ratón. Se abrirá la ventana de **Propiedades**. Seleccione la opción Clásico y haga clic en **Aceptar**.



Configuración de Windows 7, Windows 2008 R2

1. Configuración del control de cuentas de usuario (para Windows 7).
2. Configuración parámetros de acceso compartido.
3. Inicio de la cuenta del administrador.
4. Configuración del Firewall de Windows.
5. Configuración de componentes de red.
6. Configuración de directiva de seguridad local.

Importante! Versiones compatibles:

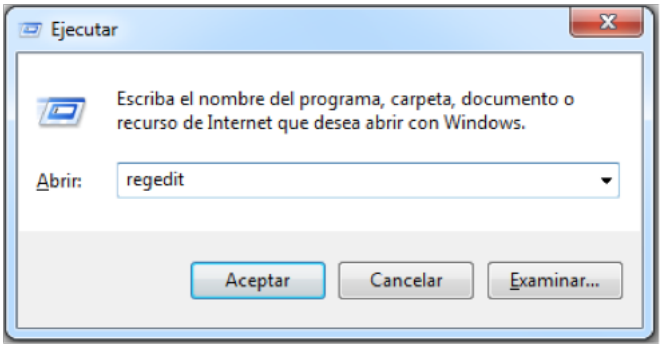
- Windows 7 Professional.
- Windows 7 Enterprise.
- Windows 7 Ultimate.

Las siguientes versiones no son compatibles:

- Windows 7 Starter.
- Windows 7 Home Basic.
- Windows 7 Home Premium.

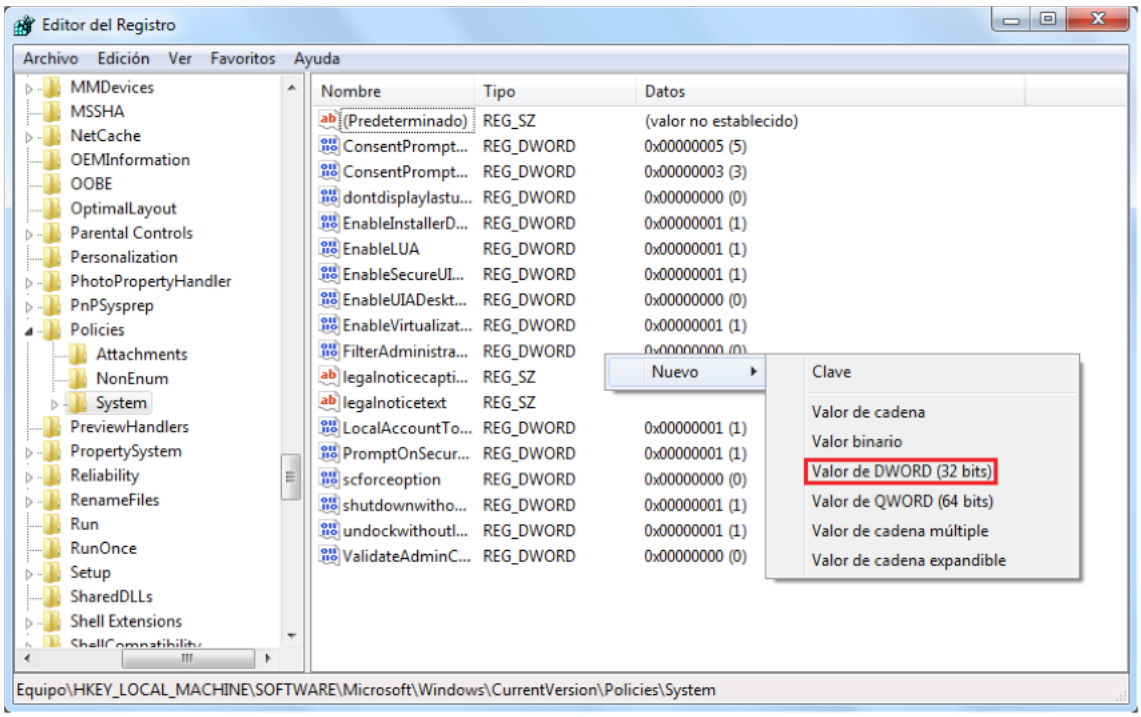
1. Configuración del control de cuentas de usuario

Pulse las teclas **Windows + R**.

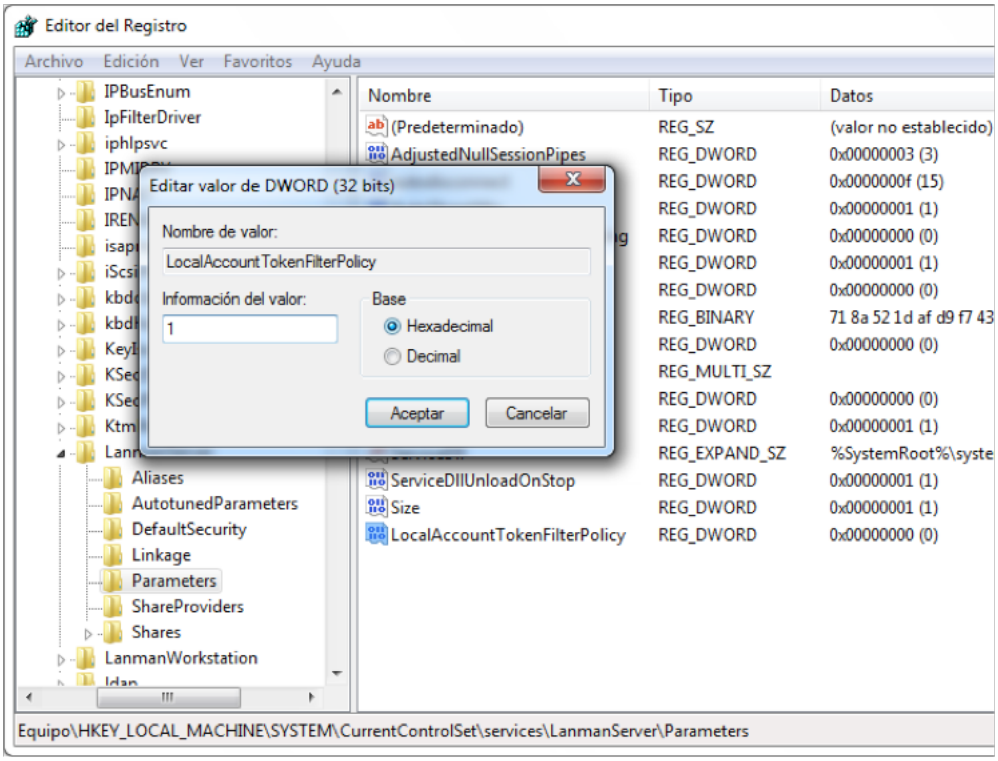


En la ventana que se abre introduzca **regedit**. Aparecerá la ventana del Editor del registro de Windows. Seleccione `[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]`

Diríjase a la parte derecha de la ventana del Editor de registro de Windows, haga clic en el botón derecho y en el menú contextual seleccione la opción **Nuevo → Valor de DWORD (32 bits)**.



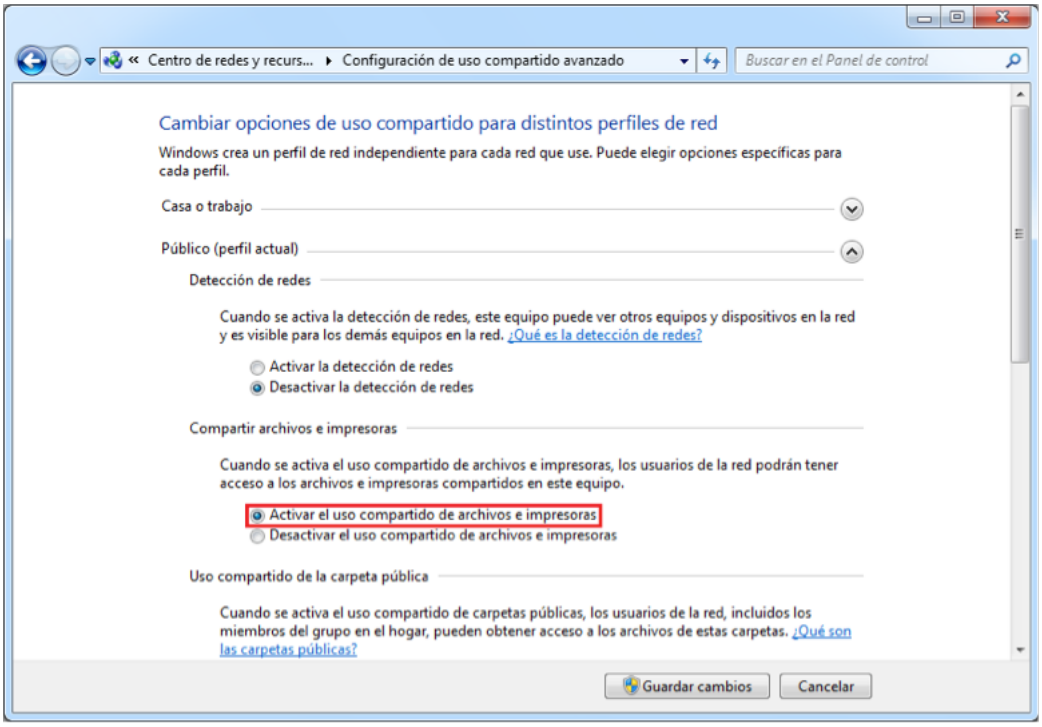
Establezca el nombre del parámetro LocalAccountTokenFilterPolicy. Haga doble clic en el parámetro creado con el botón izquierdo del ratón. Se abrirá la ventana de **Editar valor DWORD (32 bits)**. En el campo **Información del valor** establezca el valor 1 y haga clic en Aceptar.



Cierre el Editor del Registro. Realice los demás ajustes (párrs. 2-6) y reinicie el equipo.

2. Configuración de parámetros de acceso compartido.

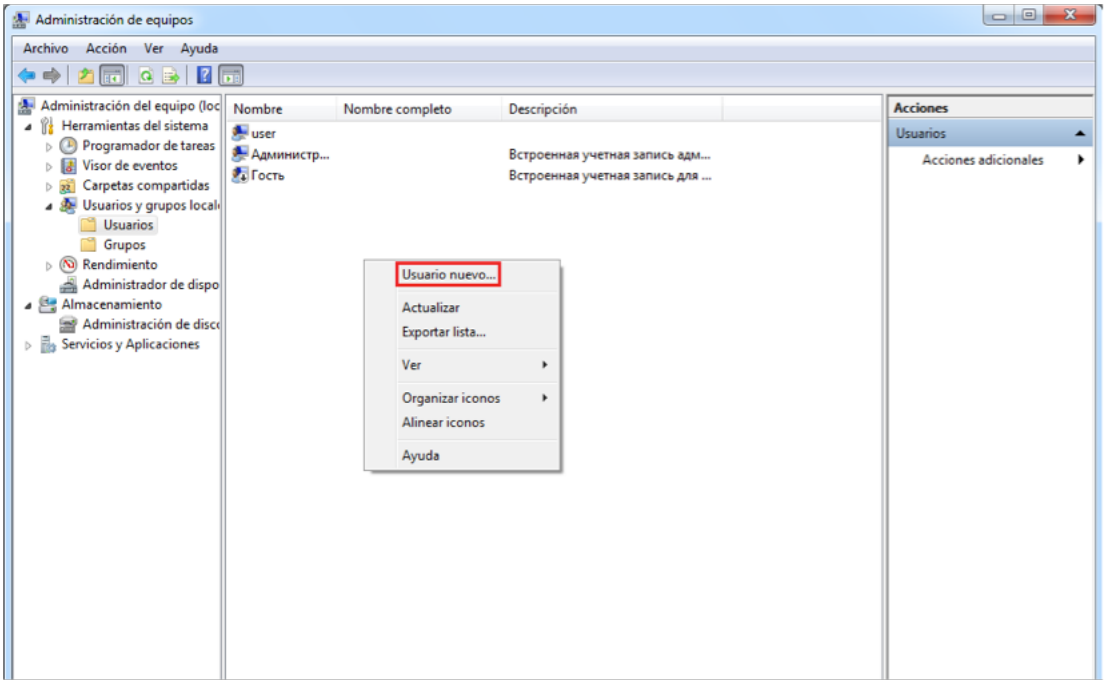
Haga clic en el botón **Inicio**, seleccione **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración de uso compartido avanzado**. En el perfil de red general seleccione la opción **Activar el uso compartido de archivos e impresoras**.



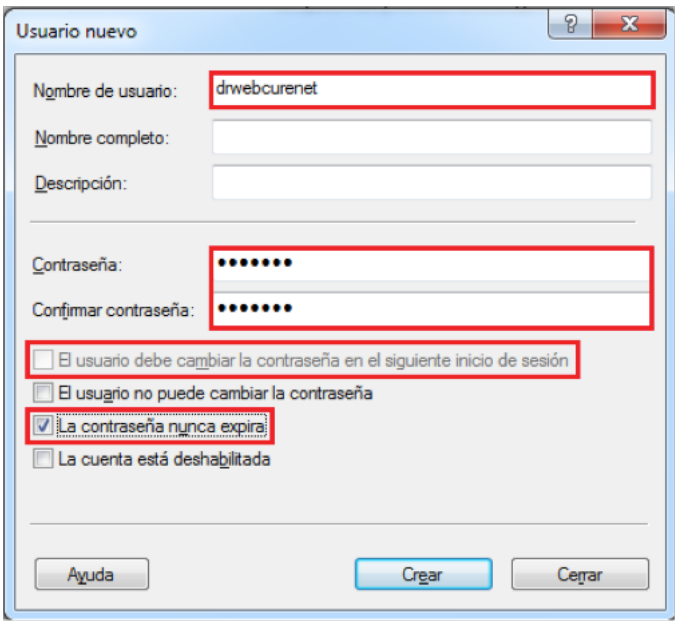
Haga clic en el botón Guardar cambios.

3. Inicio de la cuenta del administrador.

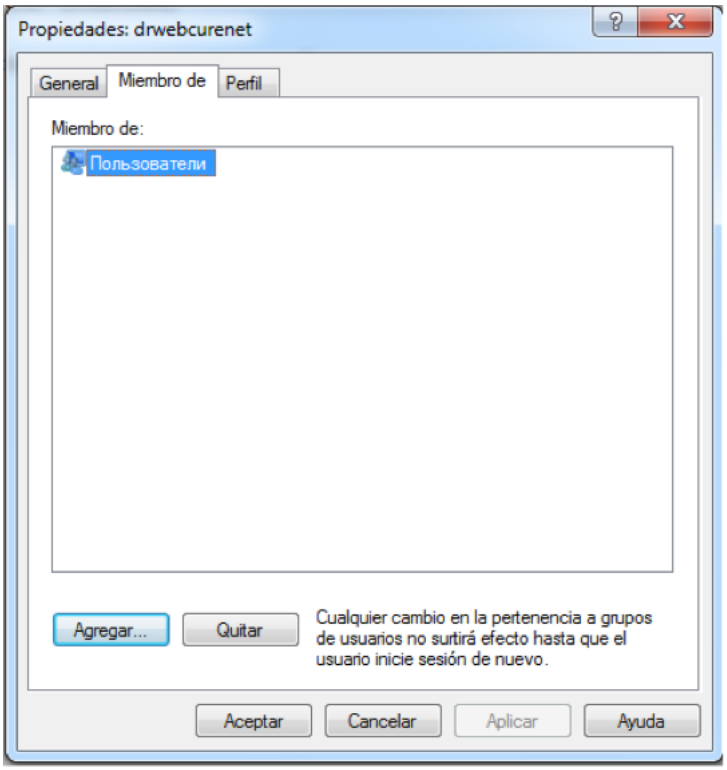
Haga clic en el botón **Inicio**, seleccione **Panel de control → Sistema y seguridad → Herramientas administrativas → Administración de equipos → Usuarios y grupos locales → Usuarios**. Ahora puede seguir trabajando con la cuenta de **Administrador**, pero para aumentar la privacidad es aconsejable crear una cuenta de administrador alternativa. Para eso haga clic en el botón derecho del ratón y en el menú contextual que aparece seleccione la opción **Usuario nuevo**.



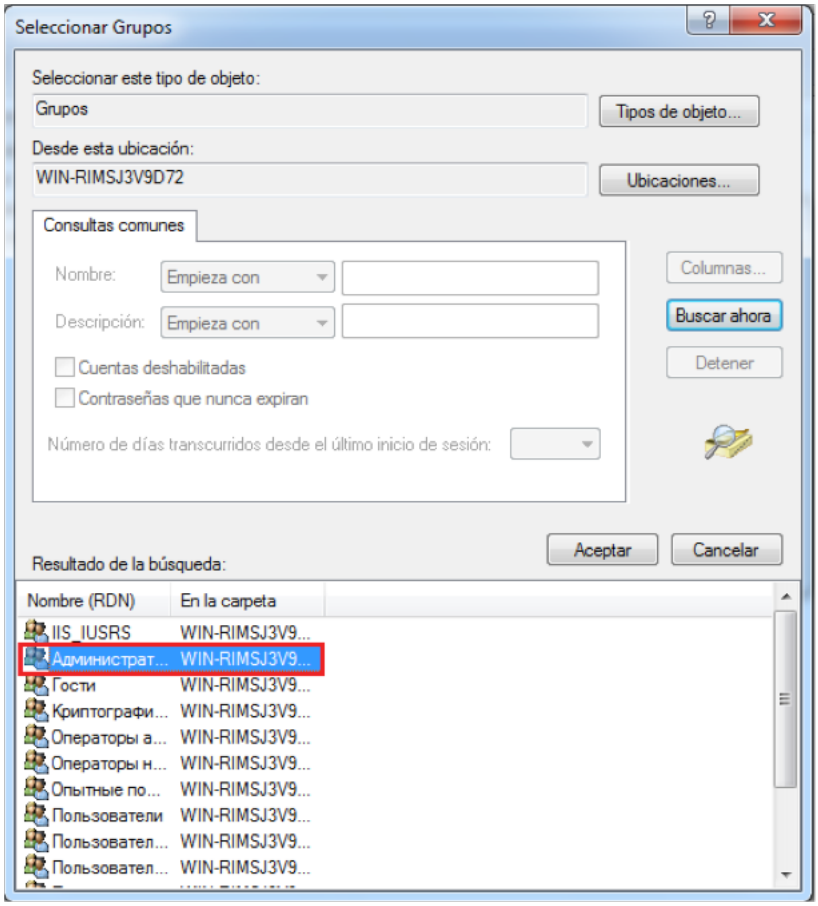
Introduzca el nombre de usuario - DrWebCurenet. En los campos **Contraseña** y **Confirmar contraseña** introduzca una contraseña segura. Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Marque la casilla **La contraseña nunca expira**. Haga clic en el botón **Crear** y luego en **Cerrar**.



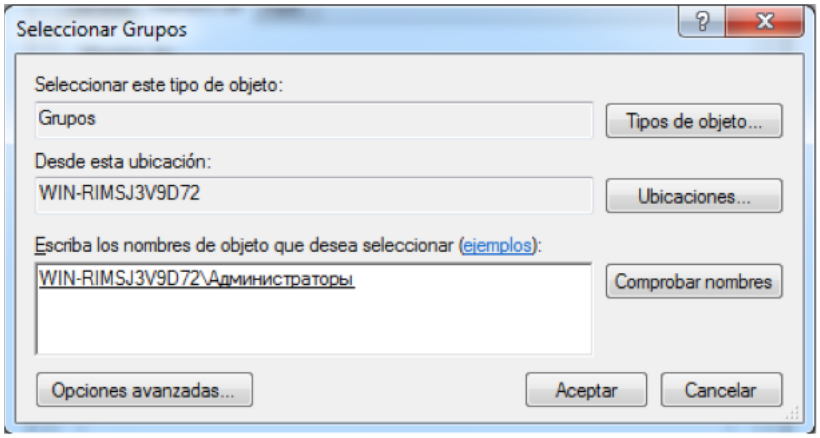
Con el botón izquierdo del ratón haga doble clic en la cuenta creada - DrWebCurenet y diríjase a la pestaña **Miembro de**. Seleccione **Usuarios** y haga clic en el botón **Quitar**.



A continuación, haga clic en el botón **Agregar**. Aparecerá la ventana de **Seleccionar: Grupos**. Haga clic en el botón **Opciones avanzadas**, y luego - en el botón **Buscar ahora**. En los resultados de búsqueda, seleccione la opción **Administradores** y haga clic en **Aceptar**.



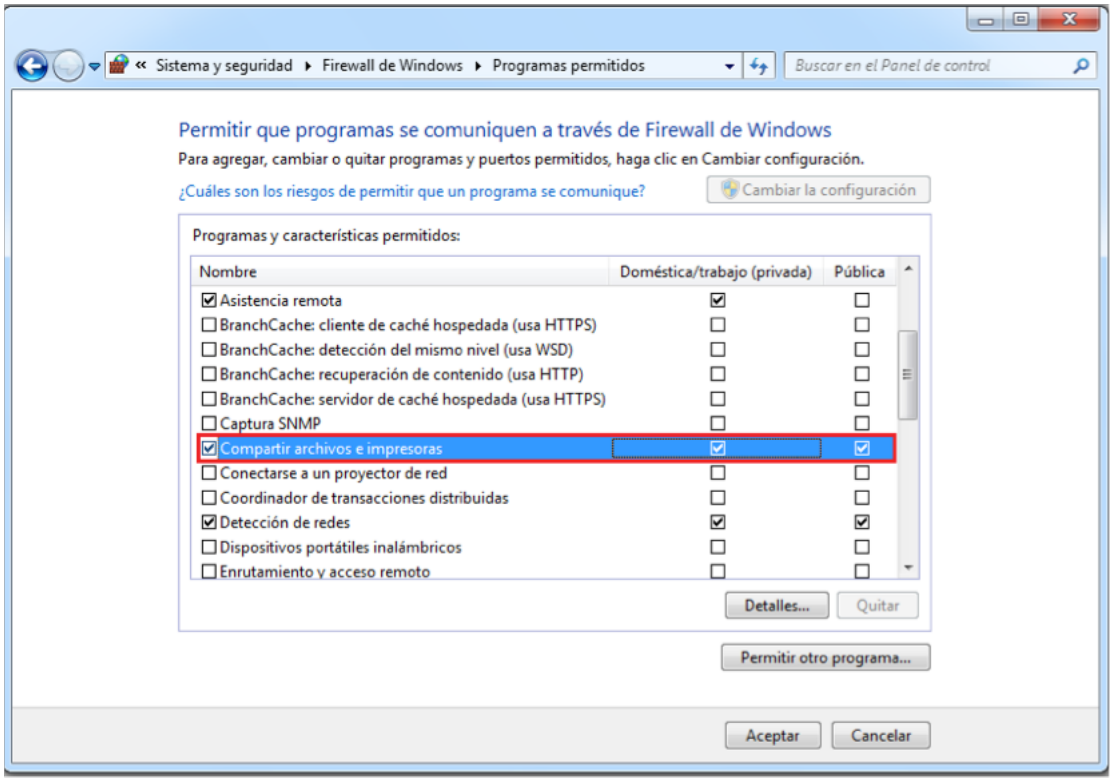
En la ventana de **Propiedades: Grupo** haga clic en el botón **Aceptar**.



Ahora, en la ventana de **Propiedades: Dr.WebCurenet** haga clic en **Aplicar** y luego en **Aceptar**.

4. Configuración del firewall.

Si está utilizando un firewall de terceros, es necesario abrir los puertos 139 y 445. Si el firewall que utiliza es de Windows, hay que configurar lo siguiente: Haga clic en el botón **Inicio**, seleccione **Panel de control → Sistema y Seguridad → Firewall de Windows → Permitir un programa o una característica a través de Firewall de Windows**. Haga clic en el botón **Cambiar la configuración**. Marque la casilla **Compartir archivos e impresoras**.

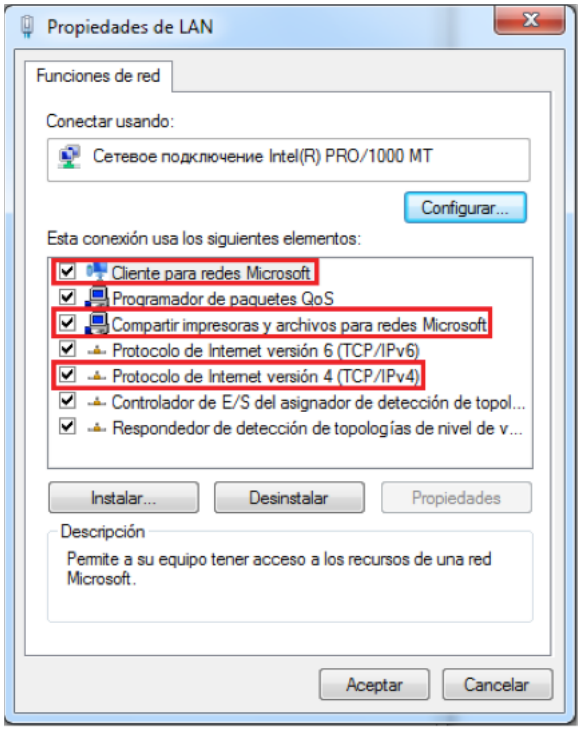


Haga clic en el botón **Aceptar**.

5. Configuración de componentes de red.

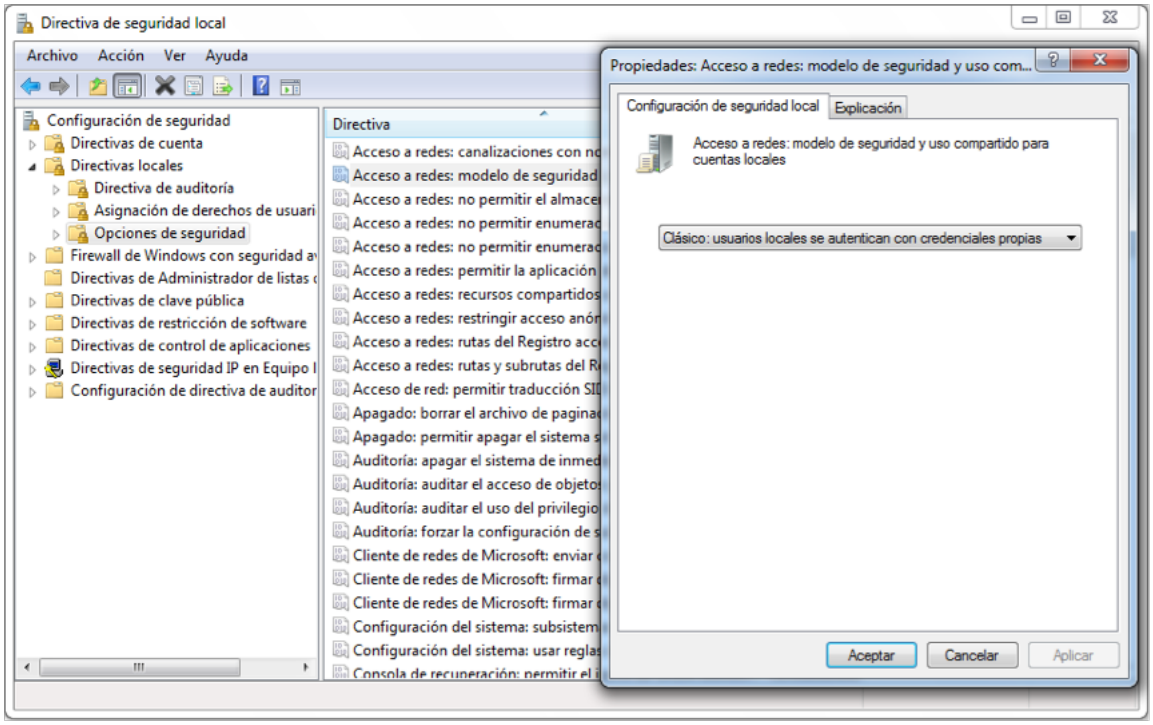
Para eso, haga clic en el botón **Inicio**, seleccione **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador**. Seleccione una conexión de red y haga clic con el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**. Asegúrese de que los siguientes componentes están activados:

- Cliente para redes Microsoft
- Servicio de acceso a los archivos e impresoras de redes Microsoft
- Protocolo de Internet versión 4 (TCP/IP v4)



6. Configuración de la directiva de seguridad local.

Haga clic en el botón **Inicio**, seleccione **Panel de control** → **Sistema y seguridad** → **Herramientas administrativas** → **Directiva de seguridad local** → **Directivas locales** → **Opciones de seguridad**. Seleccione la directiva **Acceso a redes: modelo de seguridad y uso compartido para cuentas locales**. Haga doble clic en el botón izquierdo del ratón. Se abrirá la ventana de **Propiedades**. Seleccione la opción **Clásico** y haga clic en **Aceptar**.

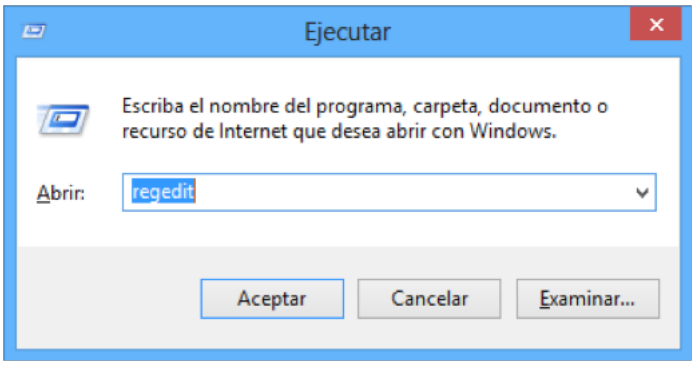


Configuración de Windows 8, Windows Server 2012

1. Configuración del control de cuentas de usuario.
2. Configuración parámetros de acceso compartido.
3. Inicio de la cuenta del administrador.
4. Configuración del Firewall de Windows.
5. Configuración de componentes de red.
6. Configuración de directiva de seguridad local.

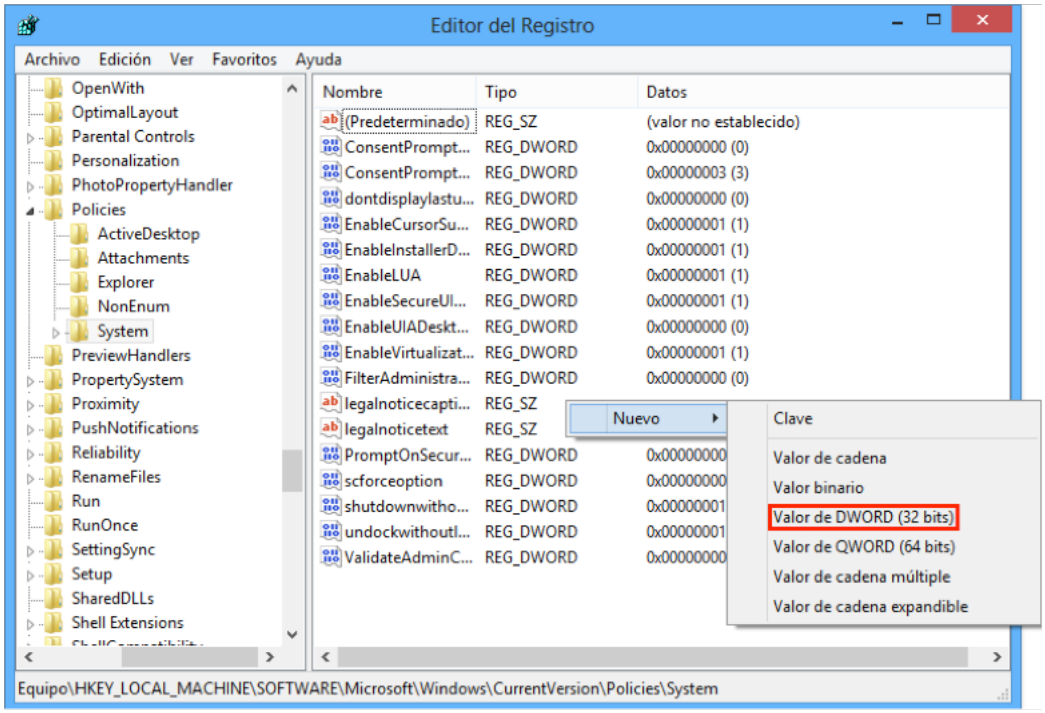
1. Configuración del control de cuentas de usuario.

Pulse las teclas **Windows + R**.

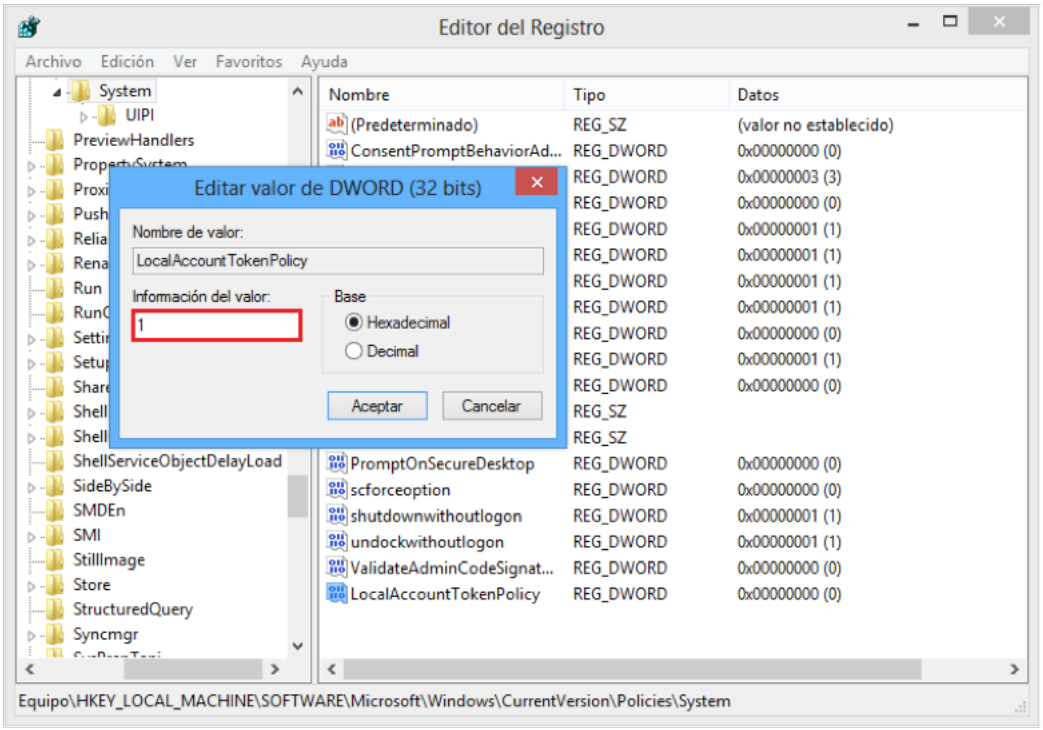


En la ventana que se abre introduzca **regedit**. Aparecerá la ventana del Editor del registro de Windows. Seleccione `[HKEY_LOCAL_MACHINE\SOFTWARE\MICROSOFT\WINDOWS\CURRENTVERSION\POLICIES\SYSTEM]`

Diríjase a la parte derecha de la ventana del Editor de registro de Windows, haga clic en el botón derecho y en el menú contextual seleccione la opción **Nuevo → Valor de DWORD (32 bits)**.



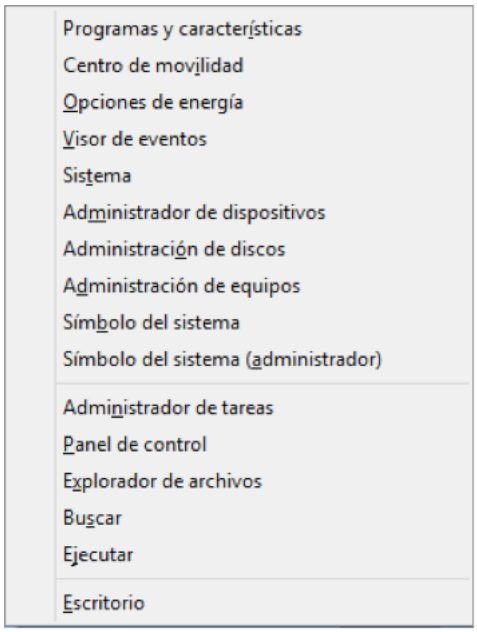
Establezca el nombre del parámetro LocalAccountTokenFilterPolicy. Haga doble clic en el parámetro creado con el botón izquierdo del ratón. Se abrirá la ventana de **Editar valor DWORD (32 bits)**. En el campo **Información del valor** establezca el valor 1 y haga clic en **Aceptar**.



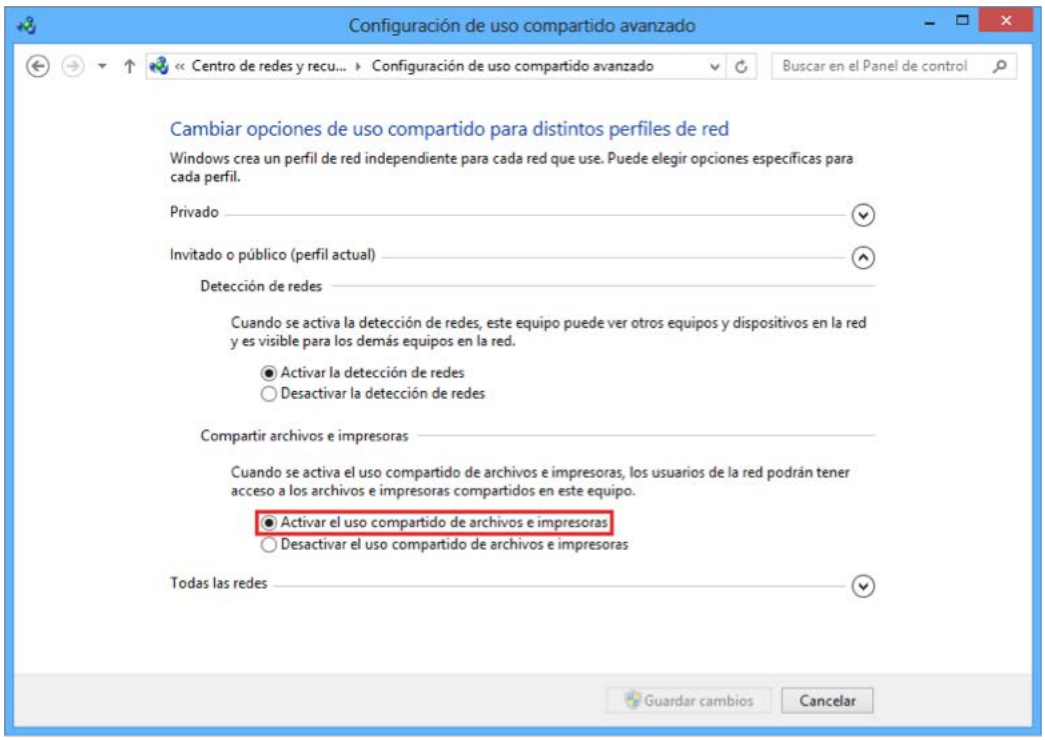
Cierre el **Editor del Registro**. Realice los demás ajustes (párrs. 2-6) y reinicie el equipo.

2. Configuración de parámetros de acceso compartido.

Pulse las teclas **Windows + X**.



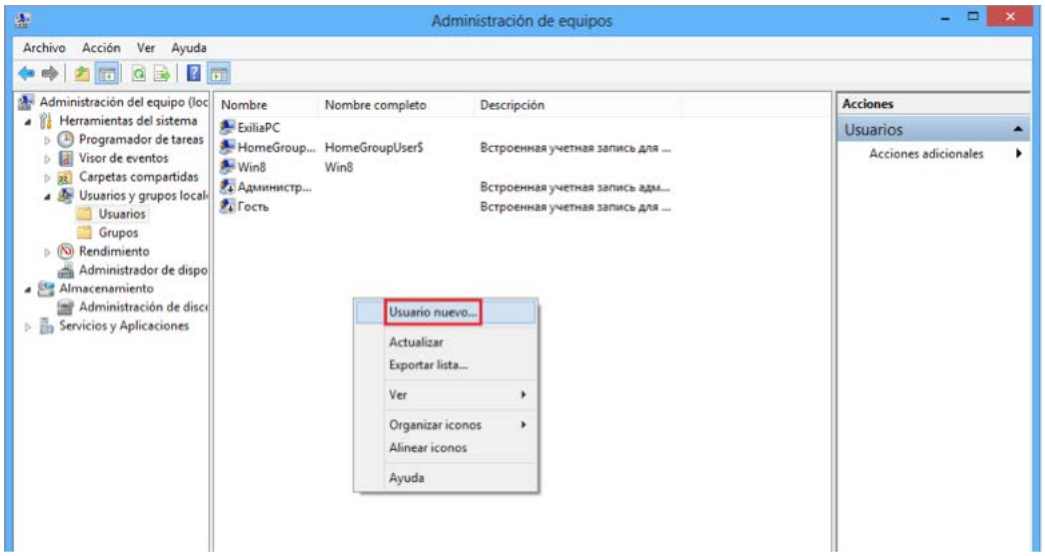
En el menú contextual que aparece, seleccione la opción **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración de uso compartido avanzado**. En el perfil de red **Invitado o público** seleccione la opción **Activar el uso compartido de archivos e impresoras**.



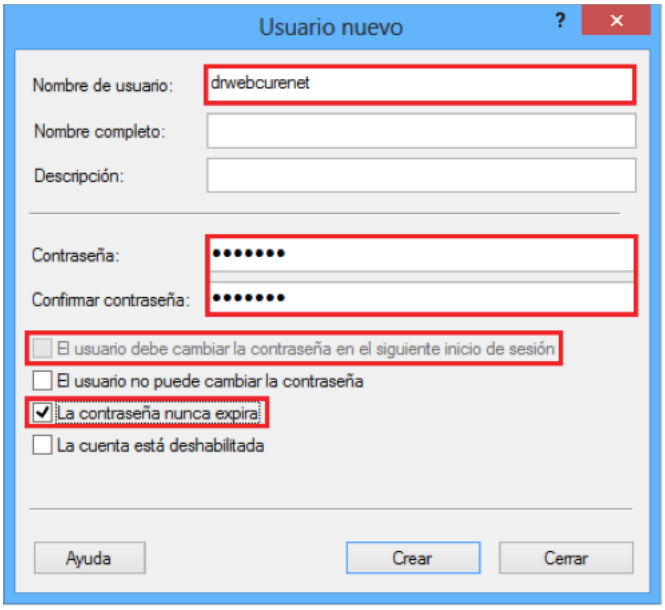
Haga clic en el botón **Guardar cambios**.

3. Inicio de la cuenta del administrador.

Pulse las teclas **Windows + X**. En el menú contextual que aparece seleccione la opción **Panel de control → Sistema y Seguridad → Herramientas administrativas → Administración de equipos → Usuarios y grupos locales → Usuarios**. Ahora puede seguir trabajando con la cuenta de **Administrador**, pero para aumentar la privacidad es aconsejable crear una cuenta de administrador alternativa. Para eso haga clic en el botón derecho del ratón y en el menú contextual que aparece seleccione la opción **Usuario nuevo**.

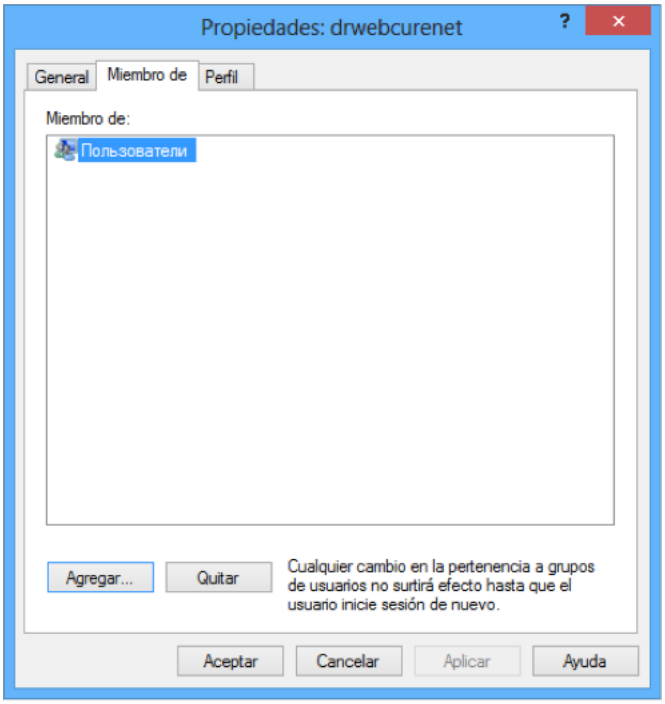


Introduzca el nombre de usuario - DrWebCurenet. En los campos **Contraseña** y **Confirmar contraseña** introduzca una contraseña segura. Desactive la opción **El usuario debe cambiar la contraseña en el siguiente inicio de sesión**. Marque la casilla **La contraseña nunca expira.**



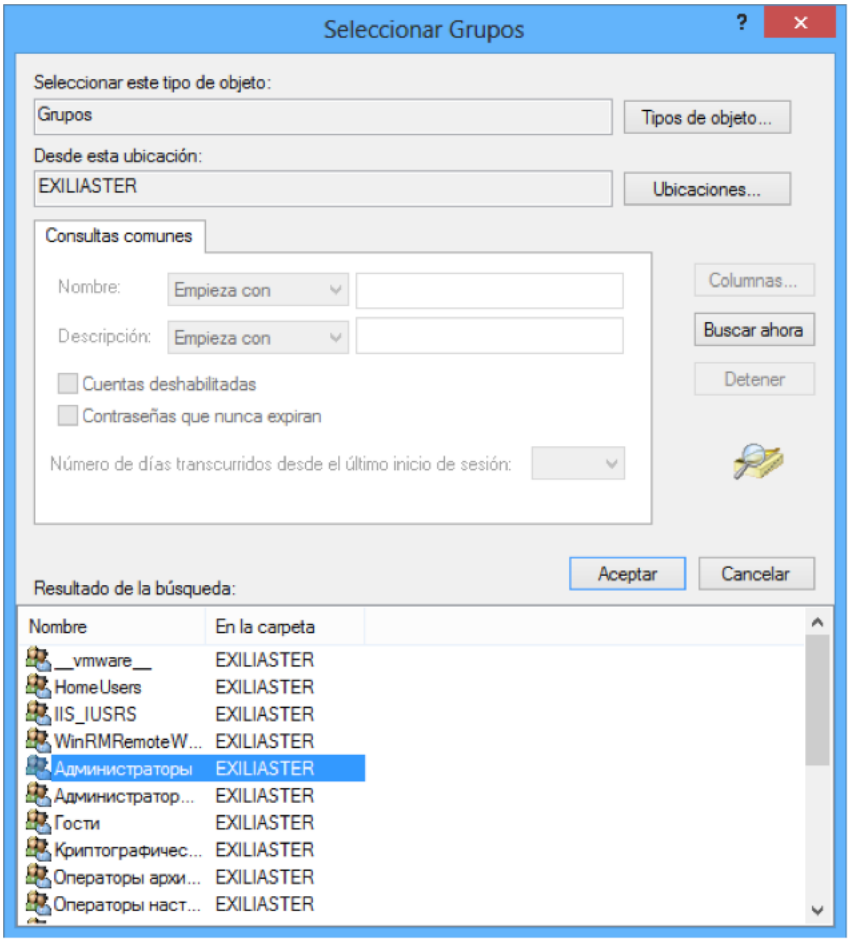
Haga clic en el botón **Crear** y luego en **Cerrar**.

Con el botón izquierdo del ratón haga doble clic en la cuenta creada - DrWebCurenet y diríjase a la pestaña **Miembro de**.

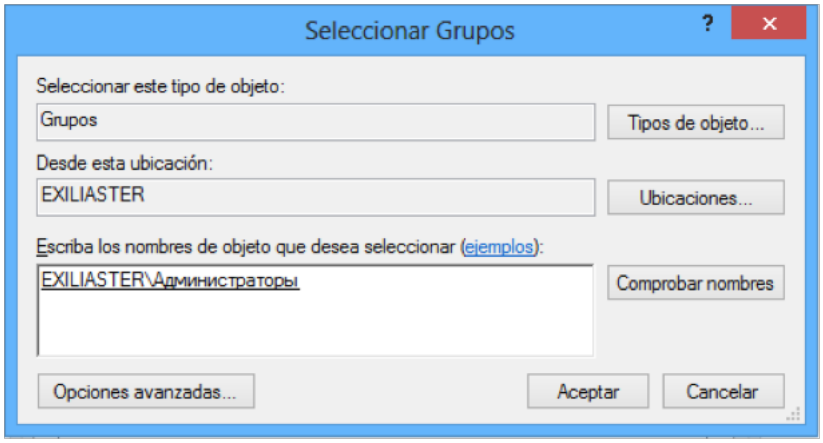


Seleccione **Usuarios** y haga clic en el botón **Quitar**.

A continuación, haga clic en el botón **Agregar**. Aparecerá la ventana de **Seleccionar Grupos**. Haga clic en el botón **Opciones avanzadas**, y luego - en el botón **Buscar ahora**. En los resultados de búsqueda, seleccione la opción **Administradores** y haga clic en **Aceptar**.



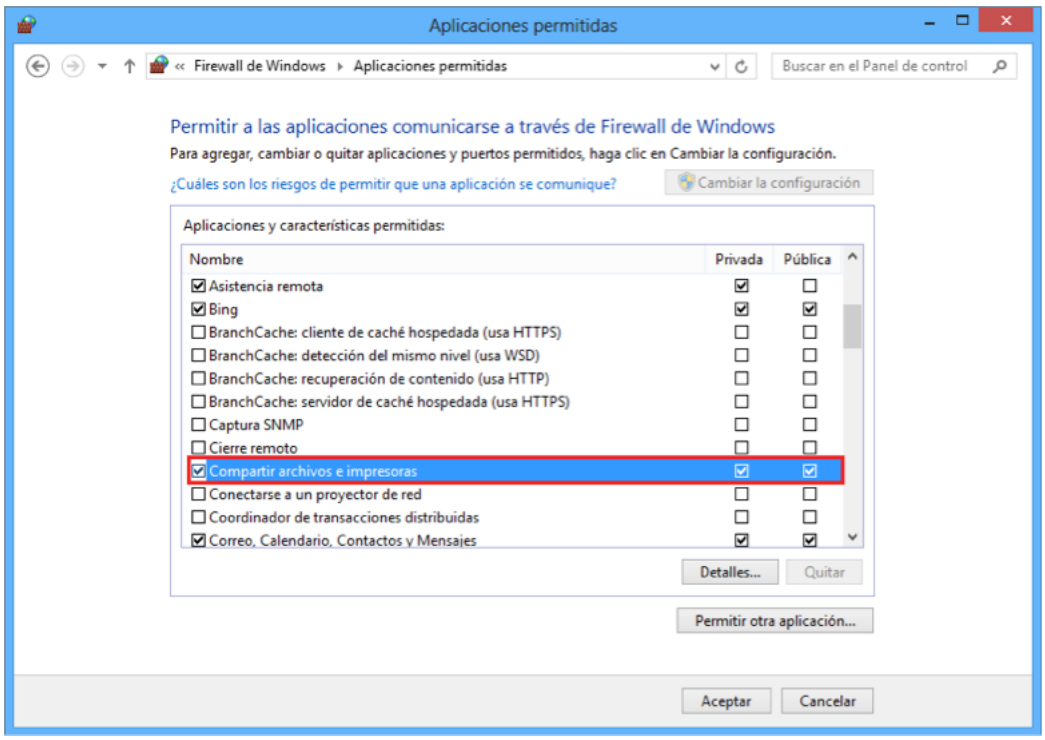
En la ventana de **Seleccionar Grupos** haga clic en el botón **Aceptar**.



Ahora, en la ventana de **Propiedades: Dr.WebCurenet** haga clic en **Aplicar** y luego en **Aceptar**.

4. Configuración del firewall.

Si está utilizando un firewall de terceros, es necesario abrir los puertos 139 y 445. Si el firewall que utiliza es de Windows, hay que configurar lo siguiente: Pulse las teclas **Windows + X**. En el menú contextual que aparece seleccione la opción **Panel de control → Sistema y Seguridad → Firewall de Windows → Permitir un programa o una característica a través de Firewall de Windows**. Haga clic en el botón **Cambiar la configuración**. Marque la casilla **Compartir archivos e impresoras**.



Haga clic en el botón **Aceptar**.

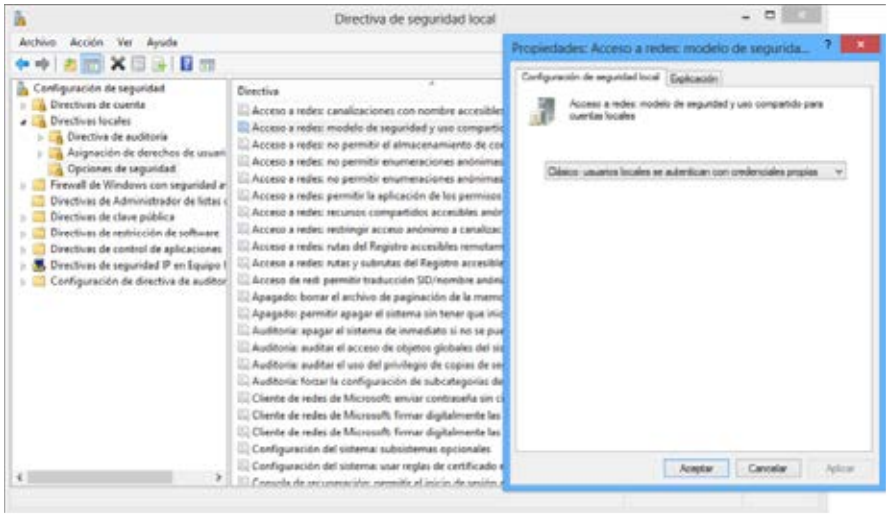
5. Configuración de componentes de red.

Pulse las teclas **Windows + X**. En el menú contextual que aparece seleccione la opción **Panel de control → Redes e Internet → Centro de redes y recursos compartidos → Cambiar configuración del adaptador**. Seleccione una conexión de red y haga clic con el botón derecho del ratón. En el menú contextual que aparece seleccione la opción **Propiedades**. Asegúrese de que los siguientes componentes están activados:

- Cliente para redes Microsoft
- Servicio de acceso a los archivos e impresoras de redes Microsoft
- Protocolo de Internet versión 4 (TCP/IP v4)

6. Configuración de la directiva de seguridad local.

Pulse las teclas **Windows + X**. En el menú contextual que aparece seleccione la opción **Panel de control → Sistema y Seguridad → Herramientas administrativas → Directiva de seguridad local → Directivas locales → Opciones de seguridad**. Seleccione la directiva **Acceso a redes: modelo de seguridad y uso compartido para cuentas locales**. Haga doble clic en el botón izquierdo del ratón. Se abrirá la ventana de **Propiedades**. Seleccione la opción Clásico y haga clic en **Aceptar**.



Ejecución de Dr.Web CureNet

1. Ejecute su distribución de `CureNet!.exe`.

   ¡Atención! El procedimiento de posteriores ejecuciones de Dr.Web CureNet! se describe a continuación.

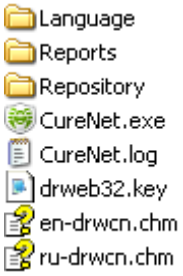
   ¡Atención! Aunque Dr.Web CureNet! es compatible con los productos antivirus de otros fabricantes, para acelerar el proceso del análisis es recomendable prohibir su funcionamiento durante el uso de Dr.Web CureNet!

2. Para continuar, haga clic en el botón **Instalar**.

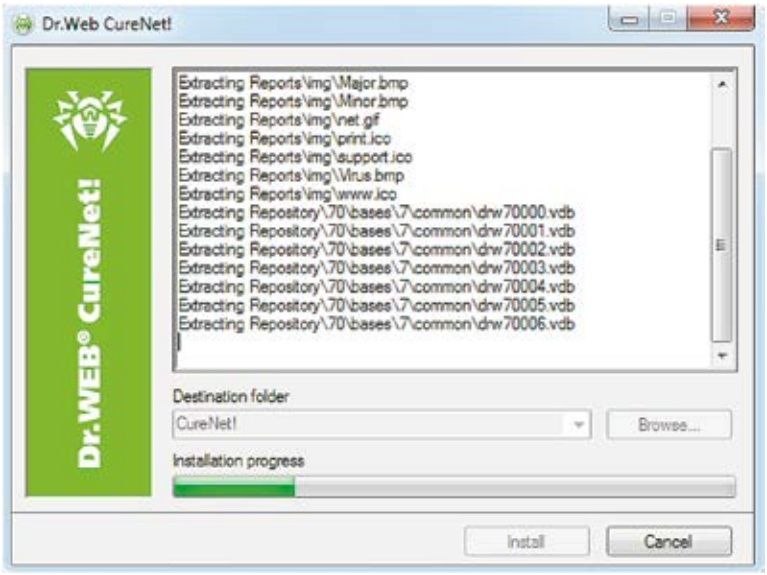
3. Si desea guardar los archivos de Dr.Web CureNet! para su uso posterior en una carpeta distinta a la carpeta predeterminada, selecciónela haciendo clic en **Examinar**.

   `CureNet!.exe` es un archivo de extracción automática, por lo tanto el producto no requiere instalación. Sólo es necesario seleccionar la ubicación para extraer los archivos. El nombre predeterminado de la carpeta es CureNet, pero puede especificar cualquier otro nombre. Si va a extraer el archivo en una unidad USB o cualquier dispositivo similar, siempre tendrá Dr.Web CureNet! a mano en caso de situaciones imprevistas.

   En la carpeta creada al extraer estarán ubicados los archivos del repositorio del producto y el archivo clave.



   Para continuar la instalación, haga clic en **Instalar**.



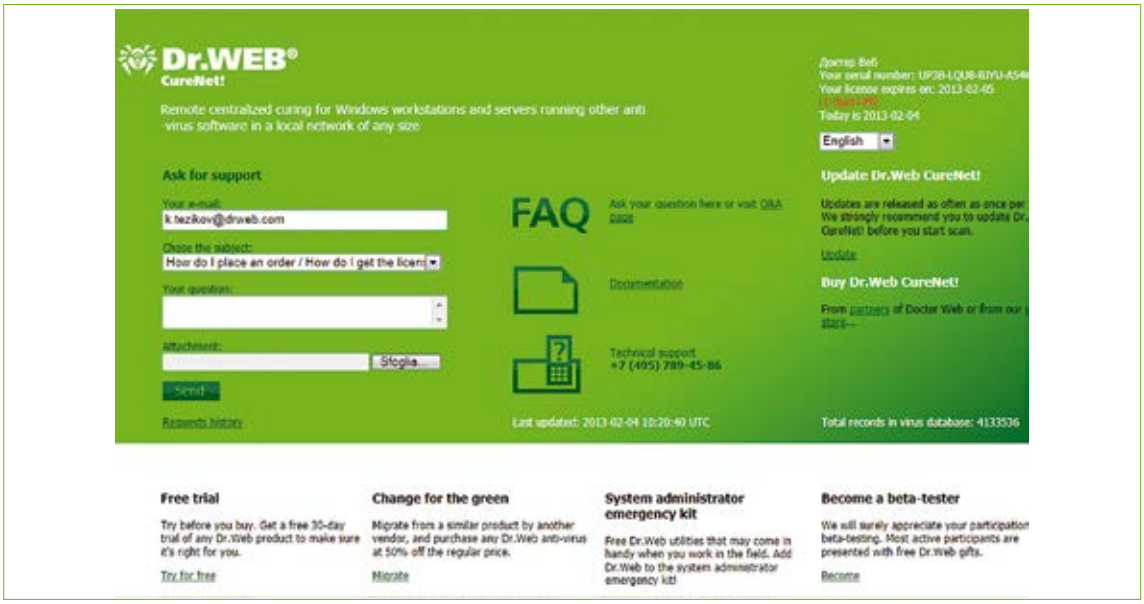
4. En la ventana que aparece, puede seleccionar el idioma de localización, pulsando el botón en la esquina superior derecha.

Si esta utilizando una versión española del sistema operativo, asegúrese de que tiene instalados todos los componentes para la visualización de símbolos españoles.

En el caso de que haya guardado los ajustes del análisis anterior, puede ejecutarlos, pulsando el botón **Perfil estándar** en la esquina superior derecha.

Si usted tiene alguna pregunta, haga clic en el botón . Seleccione Ayuda en el menú contextual para estudiar la Guía del usuario. Seleccione Mi Dr.Web para acceder a su área personal, donde puede crear una consulta al Soporte Técnico.

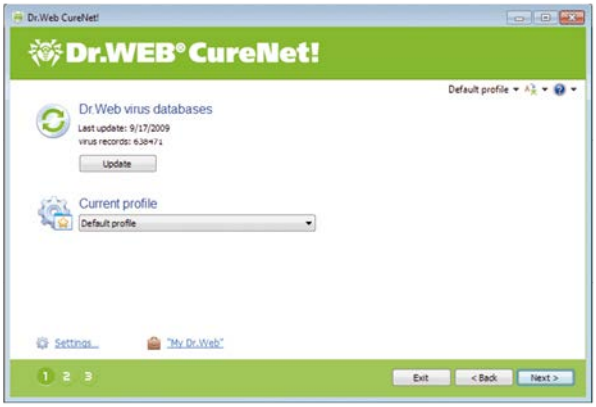
Además, puede pulsar el botón **Acerca de** para ver la información de su licencia.



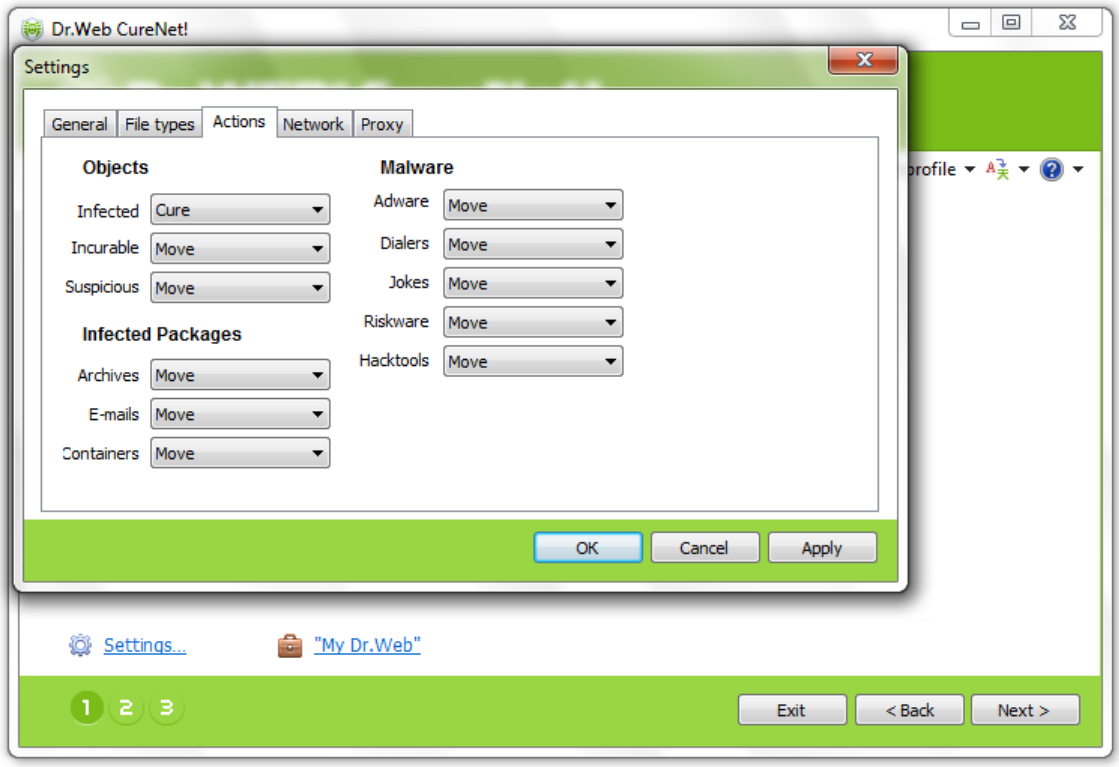
Para continuar, haga clic en **Siguiente**.

Para actualizar las bases de firmas de virus, haga clic en el botón **Actualizar**.

¡Atención! Para detectar y eliminar los virus con éxito, es importante que las bases de firmas de virus siempre estén actualizadas, por eso se recomienda actualizarlas cada vez al iniciar el equipo.



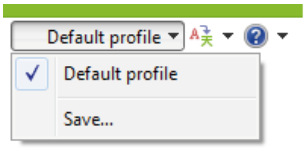
Si desea cambiar la configuración predeterminada, haga clic en **Configuración**.



En la pestaña Acciones, puede seleccionar las acciones que se aplicarán a los objetos malware de varios tipos. El valor predeterminado para la mayoría de los objetos es la acción **Mover**.

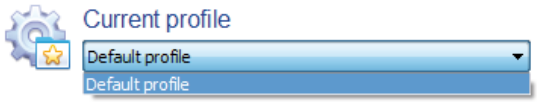
Cabe señalar que la lista de posibles acciones varía para diferentes tipos de objetos. Por lo tanto, las acciones disponibles para archivos infectados son Desinfectar, Eliminar, Cambiar nombre y Mover, pero para archivos incurables la acción Desinfectar no está disponible.

¡Atención! La desinfección de la mayoría de los virus requiere reinicio, aunque la opción de **Reiniciar estación** (Pestaña General) no está seleccionada por defecto, ya que puede perjudicar el trabajo de los usuarios. Por eso, al detectar un virus dentro de la red local, se recomienda realizar su análisis completo, notificando a los usuarios. Para guardar los ajustes, seleccione el Perfil estándar y en el menú que aparece seleccione la opción **Guardar**.



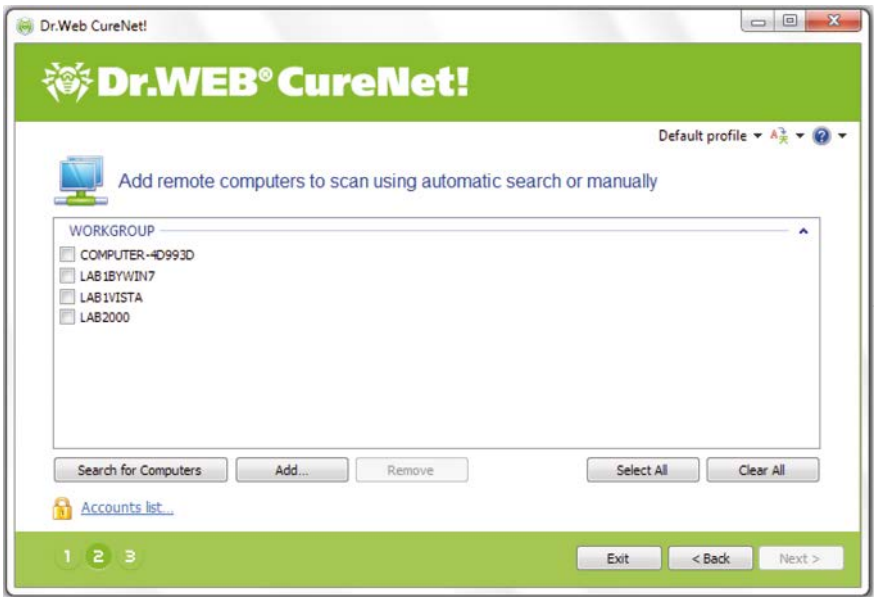
¡Atención! Se recomienda utilizar la configuración predeterminada, ya que todos los productos de la empresa "Doctor Web" se suministran con la configuración, adaptada para un trabajo confortable.

En caso, si ya tiene guardados los perfiles, haga clic en **Perfil actual** y seleccione el perfil que quiere utilizar.

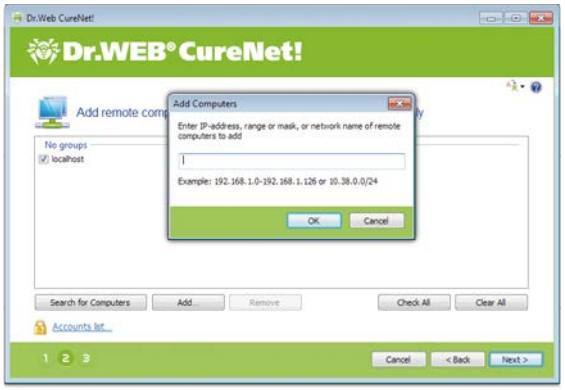


Para continuar, haga clic en siguiente.

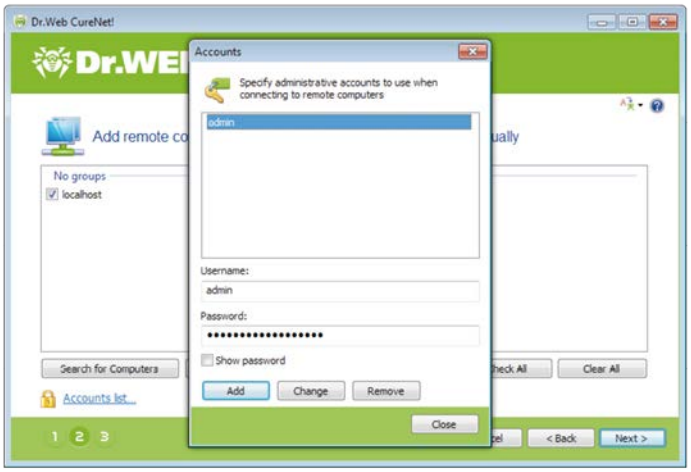
5. En la ventana que aparece, hay que crear la lista de estaciones para realizar el análisis antivirus.



Para encontrar los equipos de la red, haga clic en **Buscar automáticamente**. En caso, si desea crear una lista manualmente, haga clic en el botón **Agregar** y en la ventana que aparece introduzca la dirección de un equipo o el rango de red a analizar.



En caso, si la red que se analiza no tiene estructura del dominio, haga clic en el botón Contraseñas para conectar y en la ventana que aparece introduzca las contraseñas de acceso para los equipos analizados.



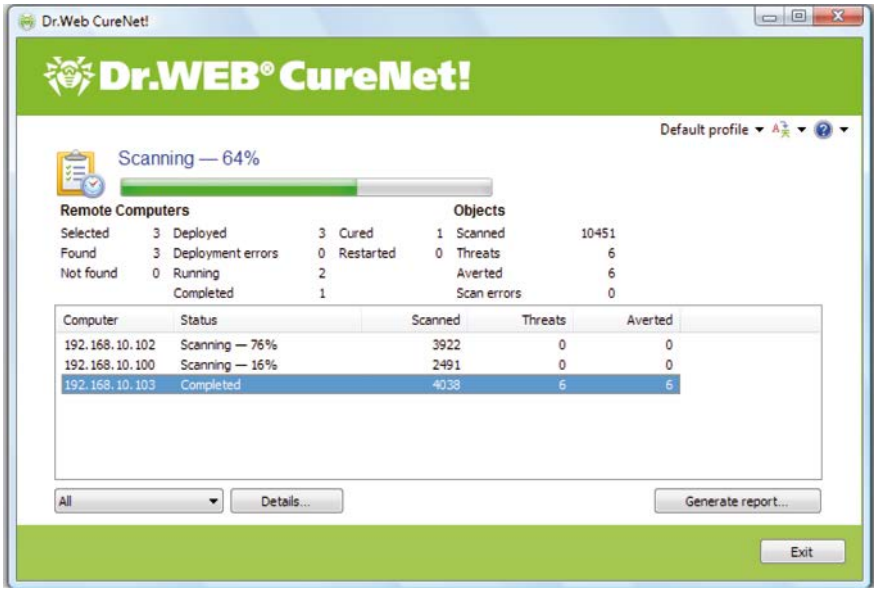
Para continuar, haga clic en siguiente.

En la ventana que aparece, seleccione el tipo del análisis - Completo o Rápido.

¡Atención! Durante el análisis rápido, se analizan únicamente las áreas del sistema y los procesos en ejecución, por lo

tanto este tipo del análisis no puede garantizar una desinfección completa de sus equipos. En particular, debido a que los virus en ejecución pueden infectar los archivos ya analizados (limpios).

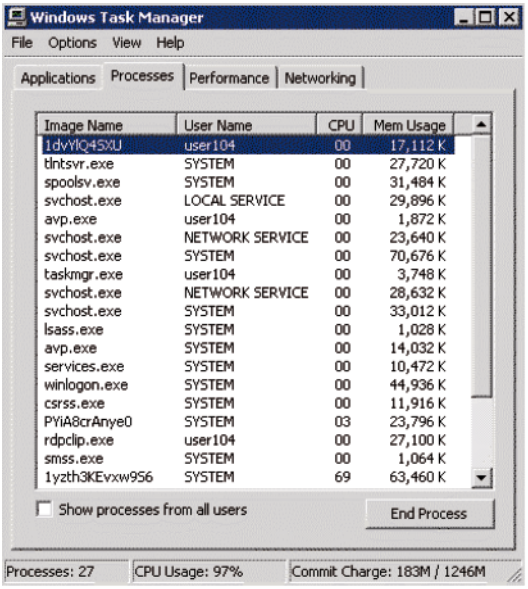
Para continuar, haga clic en el botón **Analizar**.



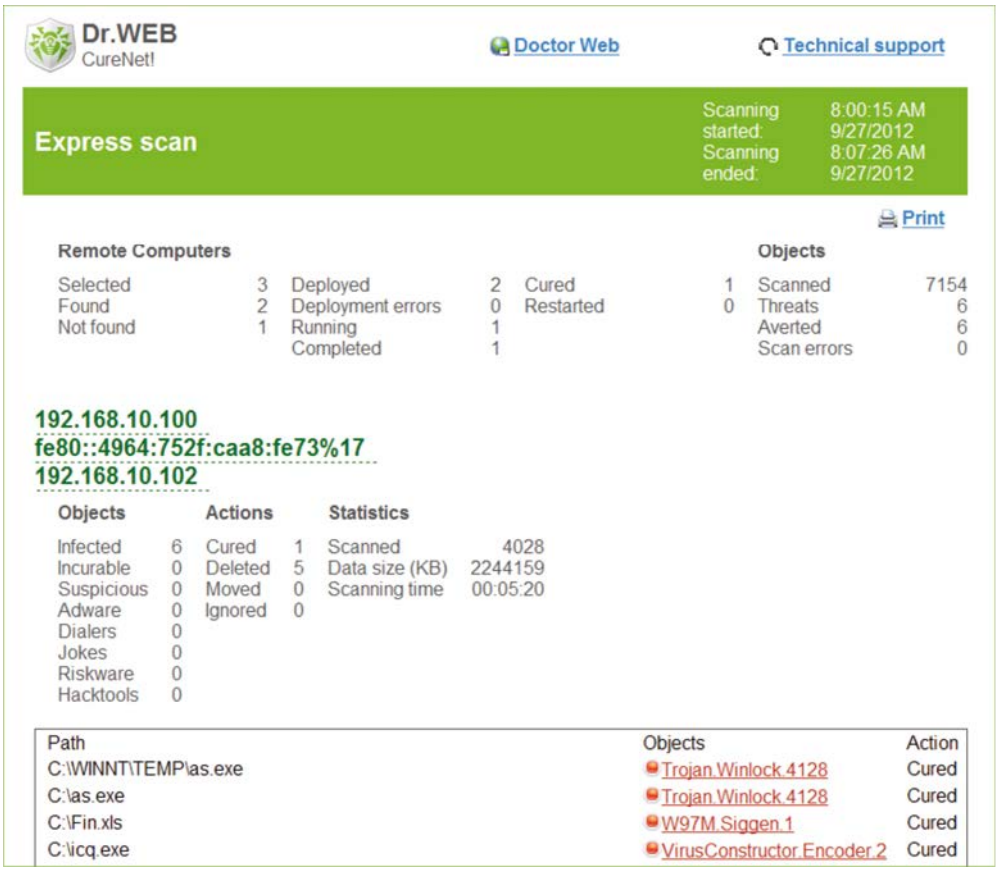
Esta página muestra el progreso y los resultados del análisis de los equipos remotos de la red. Las estadísticas proporcionadas no dependen de la calidad de conexión entre los equipos. Incluso si se interrumpe la conexión, Dr.Web CureNet! actualizará las estadísticas al recuperarla.

¡Atención! No se recomienda interrumpir el análisis.

Los procesos del análisis en ejecución utilizan mecanismos de autoprotección contra acciones de programas malware.



Puede crear un informe del análisis, al hacer clic en el botón **Crear informe**.



PPara terminar el trabajo, haga clic en el botón **Salir**.

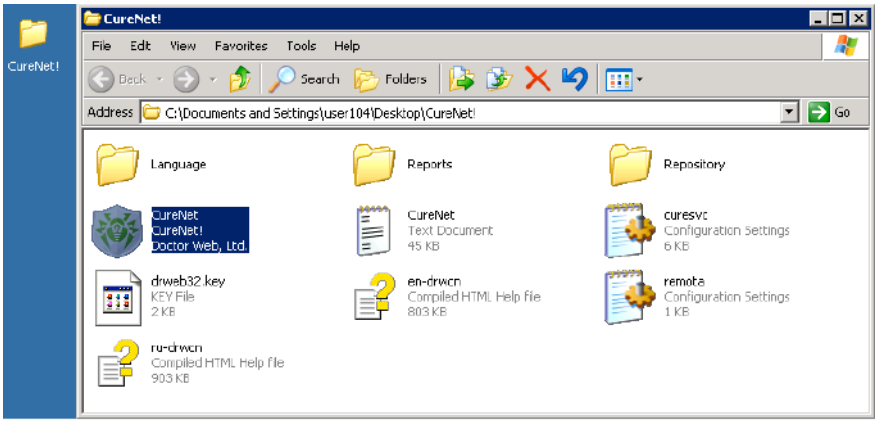
Las instrucciones detalladas para la utilización del producto, configuración del análisis y creación de perfiles están disponibles en la Guía del administrador de Dr.Web CureNet!.

Uso de Dr.Web CureNet

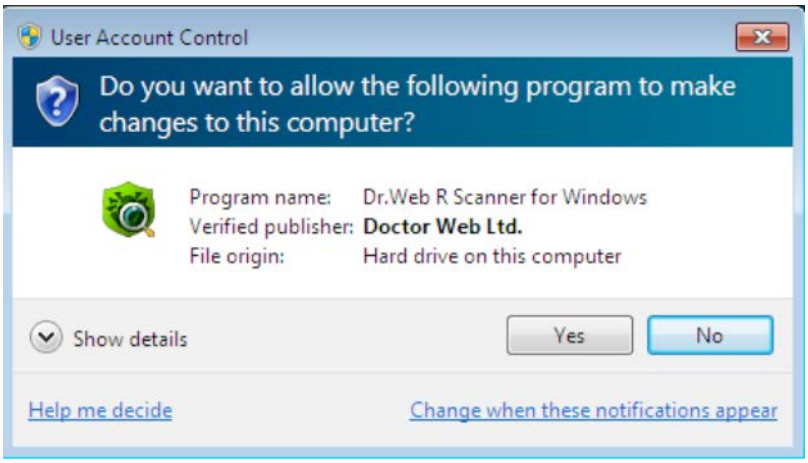
Se recomienda realizar el análisis antivirus del sistema regularmente. En particular, debido al hecho de que el monitor de archivos y los archivos grabados en el disco pueden contener virus, desconocidos en el momento del análisis.

Para analizar su sistema:

Abre la carpeta con los archivos de Dr.Web CureNet! guardados tras primera ejecución (Por defecto es la carpeta CureNet en el Escritorio) y ejecute el archivo CureNet.



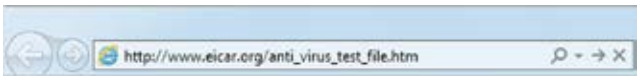
1. Si está utilizando Windows 7, es necesario confirmar la ejecución del programa, haciendo clic en el botón **Aceptar**.



El posterior procedimiento de trabajo con el programa es igual al arriba mencionado.

Verificación de operatividad del producto

2. Para obtener un virus de prueba, abre su navegador e introduzca esta dirección



3. En la página que aparece busque el texto

Download area using the standard protocol http			
eicar.com 68 Bytes	eicar.com.txt 68 Bytes	eicar_com.zip 184 Bytes	eicarcom2.zip 308 Bytes

   y seleccione uno de los archivos para descargar, por ejemplo el primero eicar.com.

4. Guarde el archivo recibido en el escritorio del equipo analizado.

   ¡Atención! Si está utilizando Dr.Web CureNet! como adición a los productos antivirus de otros fabricantes, desconéctelos antes de guardar el archivo de prueba.

5. Ejecute Dr.Web CureNet! para realizar el análisis antivirus.

125124, Rusia, Moscú, C./ 3ª Yamskogo Polya, nº2, entrada 12A.
Teléfono: +7(495) 789-45-87 (multicanal)
Fax: +7 (495) 789-45-97
www.drweb.com
www.freedrweb.com
www.av-desk.com
www.drweb-curenet.com

Última actualización: 04.07.2013