# LAS HERRAMIENTAS DEL SISTEMA

## Introducción a las herramientas del sistema

En este capítulo descubriremos el sistema operativo para conocer los principales engranajes. Una buena manera de abordar este aspecto del ordenador es explicar el funcionamiento de herramientas que deberá dominar: el símbolo del sistema, Windows PowerShell, los permisos NTFS, el Registro de Windows, los diarios de eventos, el Administrador de tareas y, finalmente, un vistazo rápido de las herramientas Sysinternals.

## El Símbolo del sistema

La línea de comandos Windows, que antes se ejecutaba en una máquina virtual llamada VDM (*Virtual Dos Machine*), comunica, desde Windows 7, con el núcleo del sistema operativo por medio del proceso padre **conhost.exe**. Para abrir una ventana de Símbolo del sistema en Windows 10, siga las siguientes instrucciones.

### 1. Ejecutar el Símbolo del sistema

Existen dos formas de lanzar el Símbolo del sistema en Windows: ya sea en modo estándar (con un token de usuario) o como administrador.

En Windows 10, dispone de varios métodos de acceso al Símbolo del sistema:

- En la zona de búsqueda de la barra de tareas, introduzca directamente la palabra clave **cmd** o **Símbolo del sistema**.
- También puede hacer clic en el menú **Inicio** y a continuación en el enlace **Todas las aplicaciones**. Vaya hasta la carpeta **Sistema de Windows** y haga clic en esta carpeta. Verá el icono de la aplicación.

Para los usuarios de Windows 8, desde la pantalla de inicio de la interfaz de usuario, coloque el ratón en un espacio vacío, es decir, donde no haya ningún icono. Haga clic con el botón derecho: aparecerá la barra de comandos de aplicación. Haga clic en el botón **Todas las aplicaciones**.
A continuación, tanto en Windows 8 como en Windows 10, haga clic con el botón derecho en el icono **Símbolo del sistema** y a continuación, en la barra de comandos, seleccione la opción **Ejecutar como administrador**. El control de cuenta de usuario le pide autorizar la ejecución de la aplicación. Haga clic en **Sí**.

En la práctica, siempre deberá ejecutar el Símbolo del sistema como administrador.

Hay una consideración importante que debemos tener en cuenta: si quiere modificar archivos de sistema desde el Símbolo del sistema, deberá activar la visualización de archivos y carpetas ocultos en el Explorador de Windows.

### 2. Utilizar el Símbolo del sistema

En la ventana de Símbolo del sistema introduzca: **help** o el nombre del comando seguido del modificador: **/?**. Si desea obtener la sintaxis completa del comando clip, introduzca lo siguiente: **clip /?**.

Si la salida de pantalla sobrepasa la dimensión de la ventana, introduzca: **dir /? | more**.

Para desplazarse dentro de los árboles de directorio, utilice el comando **cd**. Puede acceder directamente a una unidad introduciendo la letra de esta seguida de dos puntos: **e:**, **f:**, etc.

Podemos encontrar la carpeta principal utilizando el comando: **cd **.

Puede dejar que el sistema complete los comandos que usted ha introducido. Teclee: **cd d** y, a continuación, pulse la tecla [Tab] del teclado. El sistema le mostrará todos los directorios que empiezan por la letra D (por ejemplo, en Windows Vista, la carpeta *Documentos*). También funciona con los archivos, sea cual sea su extensión.

- El método abreviado de teclado [Ctrl]+C le permitirá anular el comando en todo momento.
- El método abreviado de teclado [Ctrl]+S le permitirá pausar un comando.

Pulse cualquier tecla para volver a iniciar la ejecución del comando en curso.

En Windows 10, la arquitectura del Símbolo del sistema se ha renovado profundamente por primera vez desde hace mucho tiempo. El modo de edición también se ha mejorado para aportar una buena experiencia de usuario y una mejor interactividad con, por ejemplo, la implementación de las teclas de edición. Este nuevo modo de funcionamiento, que carga una nueva DLL en la ejecución del proceso conhost.exe, se puede activar o desactivar a través de la ventana de configuración de las propiedades de la consola. Para ello, active o desactive la opción **Usar la consola heredada** en la pestaña **Opciones**.

En esta ventana, dispone de otras opciones para personalizar el comportamiento de la consola como por ejemplo el control de la opacidad de la consola en la pestaña **Colores**.

## 3. Utilizar las variables de entorno

Cuando introduce un comando, se efectúan tres operaciones:

Si el comando señala la ubicación de un archivo ejecutable, el intérprete de comandos comprobará si el archivo ejecutable existe en el directorio especificado. En caso de que no sea así, se encontrará con este tipo de error: "'Nombre del programa' no se reconoce como comando interno o externo, un programa o un archivo por lotes ejecutable".

Si el comando no contiene la ubicación exacta del archivo ejecutable introducido, el intérprete de comandos comprobará si el archivo ejecutable existe en el directorio actual. Si no es el caso, intentará encontrar el programa en todas las ubicaciones definidas por la variable de entorno "Path" y en el orden asignado en los datos de este valor. Cada vez que descarga una herramienta, puede optar por guardar el archivo ejecutable en una de las ubicaciones ya establecidas por la variable de entorno "Path", o bien añadir esta nueva ubicación a la misma variable de entorno. Algunos programas lo hacen automáticamente. De lo contrario, el procedimiento a seguir es el siguiente:

En el **Panel de control**, en la sección **Sistema y seguridad**, seleccione la opción **Sistema/Cambiar configuración**.
Haga clic en el vínculo **Opciones avanzadas** y a continuación en el botón **Variables de entorno**.

En el apartado **Variables del sistema**, haga clic en **Path** y después en el botón **Editar**.
Escriba las diferentes ubicaciones de los archivos ejecutables.

Tenga en cuenta que es más fácil crear un directorio exclusivo. Cada comando debe separarse por punto y coma.

Por defecto, existen variables creadas por el sistema operativo. Hay dos tipos de variables:

- Las variables de usuario que corresponden a la cuenta en la cual abre sesión.
- Las variables de sistema que se aplican al conjunto de usuarios del ordenador.

Para llegar a un directorio de sistema directamente es posible utilizar el nombre de la variable. Abra un Símbolo del sistema y a continuación ejecute uno de los siguientes comandos: **explorer %windir%** o **explorer %userprofile%**.

¿Cuál es la función de las variables? Una variable permite efectuar una operación sin importar el contexto de usuario o equipo en los que se ejecuta. Veamos dos ejemplos: la variable %USERPROFILE% se dirigirá al directorio de usuario, sea cual sea el usuario conectado: C:\Users\Juan o C:\Users\Isabel.

La variable %windir% remitirá al directorio de Windows, sin importar la letra de la unidad en la que esté instalado el sistema operativo: C:\Windows, D:\Windows, etc.

# Introducción a Windows PowerShell v5

PowerShell es la nueva interfaz en línea de comandos y el nuevo lenguaje de scripts dedicado a la administración de sistemas Windows. PowerShell está orientado a objetos y utiliza el framework Microsoft .NET para la ejecución de herramientas de línea de comandos llamadas cmdlets o commandlets. Estos comandos permiten administrar los sistemas Windows locales o remotos. El formato abierto de PowerShell permite desarrollar y añadir cmdlets de terceros en forma de módulos portables para enriquecer el entorno estándar. Microsoft pone igualmente a su disposición numerosos ejemplos de scripts PowerShell desde el sitio https://code.msdn.microsoft.com/

Windows 8 y Windows Server 2012 integran de forma nativa la versión 3.0 de PowerShell.

Windows 10 integra de forma nativa la versión 5 de Microsoft PowerShell

## 1. Windows Remote Management (WinRM)

Este servicio implementa el protocolo WS-Management que utiliza PowerShell para la administración remota de sistemas Windows en un modo de conexión cliente-servidor. El protocolo WS-Management es un Web Service estándar de tipo SOAP. El servicio WinRM actúa como un listener (servicio de escucha) del lado servidor. La herramienta de línea de comandos Winrs.exe permite lanzar comandos remotos en el lado cliente que son recibidos por el servicio WinRM. PowerShell utiliza el servicio WinRM para la ejecución de scripts remotos.

Antes de poder lanzar comandos remotos y utilizar el servicio WinRM, deberá configurar el servicio.

Usando el comando **services.msc**, abra el administrador de servicios. Compruebe la configuración del servicio **Administración remota de Windows (WS-Management)** y arránquelo si no estuviera funcionando. Configure el servicio para que arranque automáticamente al iniciar la sesión.
En el lado servidor, abra un Símbolo del sistema en modo administrador y ejecute el comando **WinRM quickconfig** para lanzar la configuración del servicio **WinRM**.
Teclee **y** para confirmar la configuración del servicio como listener (servicio de escucha).

Teclee **y** para confirmar la configuración del cortafuegos de Windows.

El servicio WinRM está configurado para la ejecución de comandos remotos.

Del lado cliente, abra un Símbolo del sistema en modo administrador.
Ejecute un comando con la siguiente sintaxis **winrs -r%servername% remote command**, por ejemplo **winrs -r:SRVDC01 ipconfig/all** como en la siguiente pantalla:

## 2. Ejecución de PowerShell

Para ejecutar el anfitrión PowerShell, introduzca el comando Windows Powershell en el cuadro **Buscar** a la derecha del menú Inicio.

En los resultados, haga clic en **Windows PowerShell**. Observe la presencia de Windows PowerShell ISE; este entorno gráfico, que aparece con Windows 7, permite escribir, ejecutar y probar scripts de PowerShell.

En Windows 8, la herramienta PowerShell ISE está disponible en las herramientas de administración del sistema. En el **Panel de control**, sección **Sistema y seguridad**. Para visualizar las herramientas desde la interfaz de usuario, consulte el capítulo Mantenimiento del sistema.

PowerShell asegura la compatibilidad con los comandos DOS a través de los alias, la lista de los cuales está disponible ejecutando el comando **Get-Alias**. Puede utilizar PowerShell para la ejecución de comandos DOS estándar, como por ejemplo el comando **DIR**.

## 3. Utilización de los cmdlets estándares

El cmdlet, llamado ”Command-let”, es un comando batch especializado en la ejecución de una funcionalidad única para el contexto de la interfaz de comando activa. La ejecución de un cmdlet no crea de nuevo procesos en el sistema anfitrión.

El cmdlet **get-command** permite retornar la lista de los cmdlets. No podrá recordar todos los cmdlets disponibles para el entorno de ejecución PowerShell, ya que son demasiados. Por el contrario, debe poder encontrarlos y determinar la sintaxis principal. Los principales cmdlets que debe conocer son los siguientes:

- **get-command**: este comando lista el conjunto de cmdlets disponibles en el entorno de ejecución de PowerShell. El comando **get-command -noun process** permite listar los cmdlets relativos a la gestión de procesos.
- **get-help**: este comando permite obtener información detallada sobre la utilización de cmdlets, como el nombre y la descripción de la sintaxis del cmdlet. El comando **get-help ls** permite listar la información detallada del cmdlet que hace referencia al alias ”ls”.
- **get-member**: este comando permite obtener información sobre los objetos y listas de objetos de los cmdlets. La lista de comandos siguientes permite listar los objetos adjuntos a un objeto del sistema operativo, como el directorio Windows, y visualizar el contenido de un objeto de tipo propiedad.

Observe que se puede acceder al histórico de comandos con la tecla [F7].

Ejemplo de utilización del comando **get-member**:

## 4. Ejemplos de comandos para solucionar problemas con PowerShell

Si aprende los muchos comandos PowerShell, ganará mucho tiempo en las tareas de mantenimiento habituales que a menudo suelen ser repetitivas.

Por ejemplo, puede visualizar los errores del diario de eventos **Application** con el siguiente comando:

```
Get-EventLog -LogName "application" -Newest 20 -EntryType error |
fl EntryType,Category,CategoryNumber,Source,Message
```

También puede volver a desplegar las aplicaciones descargadas desde Windows Store con el siguiente comando:

```
Get-AppXPackage -AllUsers | Foreach {Add-AppxPackage
-DisableDevelopmentMode -Register
"$($_.InstallLocation)\AppXManifest.xml"}
```

Este comando es útil si una o varias aplicaciones descargadas desde la tienda Windows Store tienen problemas de funcionamiento o de arranque en su entorno.

Otro comando interesante es el comando **repair-volume**, que equivale al comando **chkdsk**.

Por ejemplo, puede ejecutar el siguiente comando para escanear el disco c:\

```
Repair-Volume c -Scan
```

Observe que Windows 10 integra nuevos comandos PowerShell para la gestión de paquetes de aplicaciones o, por ejemplo, para administrar Windows Defender.

En la web TechNet de Microsoft puede encontrar los cientos de comandos PowerShell para la gestión y la administración de los sistemas Windows. Puede acceder a esta lista en la siguiente dirección: https://technet.microsoft.com/en-us/library/mt156946.aspx

# Los permisos NTFS

Cada vez que abre sesión, la información de identificación utilizada por el usuario (nombre de usuario y contraseña) se transfiere a un monitor de seguridad local que accede al Administrador de seguridad (SAM de *Security Account Manager*). Este último, asignará un token de acceso que determinará los derechos de acceso que posee ese usuario para todos los objetos "asegurables" (claves del Registro, archivos, carpetas, servicios, procesos, etc.) Este descriptor de seguridad revisa dos informaciones:

- El SID del usuario.
- La lista DACL del objeto al que intenta acceder el usuario.

A continuación, explicaremos estas dos nociones.

## 1. Los SID de usuarios

Un SID (*Security IDentifier*) es una manera única de identificar a un usuario o grupo de usuarios. Podemos encontrar estos identificadores en los token de acceso, en las ACL (*Access Control List*) y en las bases de seguridad de cuentas. Diríjase al apartado siguiente para ver una descripción completa sobre el mecanismo de las ACL.

Los SID son datos de longitud variable que forman una representación jerárquica del actor designado: S-R-I-XXX-XXX-XXX.

- S: la letra S (para recordar que se trata de un SID).
- R: el número del formato binario de SID.
- I: número entero que identifica la autoridad que ha emitido el SID.
- XXX-XXX-XXX: serie de longitud variable, formada de identificadores de subautoridad o identificadores relativos (*Relative IDentifier* o RID).

Puede visualizar los SID de esta manera:

En la línea de comandos, teclee: **whoami /all**.

Se muestra la información siguiente:

- El SID correspondiente al grupo Administradores es S-1-5-32-544.
- La autoridad que ha emitido este SID tiene como identificador el número 5.
- La subautoridad tiene como identificador el número 32.
- 544 es el RID del grupo Administradores.

Puede comprobar los resultados mostrados con los siguientes comandos:

- **whoami**
- **whoami /user /priv**
- **whoami /groups**

Se mostrarán los privilegios del usuario que está conectado en ese momento. Puede obtener algunos SID de usuarios o entidades de seguridad abriendo este árbol de Registro: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\ProfileList.

Finalmente, los SID de algunas entidades se muestran en este otro árbol: HKEY_USERS.

## 2. Las listas de control de acceso

Una lista de control de acceso discrecional (DACL o *Discretionary Access Control Lists*, comúnmente llamadas ACL) es un mecanismo que permite proteger recursos como los archivos y las claves del Registro. Las DACL contienen las entradas de control de acceso (ACE o *Access Control Entry*) que funcionan como registros para cada usuario o grupo de usuarios que su SID señala. Estas entradas asocian una entidad de seguridad (una cuenta de usuario, un grupo de cuentas, una entidad de sistema) con una regla que define el uso del recurso. Las DACL y las ACE permiten aceptar o rechazar los privilegios de acceso a los recursos según los permisos que usted quiera darle a las cuentas de usuario. También puede crear una ACE y aplicarla a la DACL de un archivo para impedir que nadie, salvo un administrador, pueda modificar el archivo.

Una lista de control de acceso de sistema (SACL o "ACE de auditoría") es un mecanismo que controla los mensajes de auditoría asociados a un recurso. Las SACL contienen ACE que definen las reglas de auditoría para un recurso determinado.

Así pues, podrá utilizar las DACL para asegurarse de que solo un administrador puede modificar un archivo y las SACL para asegurarse de que se guarden todos los intentos conseguidos de apertura del archivo. Es posible distinguir las ACE positivas y ACE negativas:

En el Explorador de Windows, abra su directorio de usuario.
Cree una nueva carpeta llamada *Prueba*.
Haga clic con el botón secundario del ratón en el submenú **Propiedades**.
Haga clic en la pestaña **Seguridad**.

Tenga en cuenta que las ACE o autorizaciones visibles aparecen en gris, ya que heredan de la carpeta padre.

De hecho, la carpeta que acaba de crear ha heredado los permisos en vigor de la carpeta principal. Este mecanismo de encadenamiento se conoce como "herencia" y lo primero que haremos será desactivarlo.

Haga clic en el botón **Opciones avanzadas**.
Haga clic en el botón **Deshabilitar herencia** y a continuación en el vínculo **Convertir los permisos heredados en permisos explícitos en este objeto**.
Haga clic en **Aceptar**.

A continuación, haga clic en **Aceptar**.
Haga clic en el botón **Editar**.
Seleccione su nombre de usuario.

Ahora puede seleccionar las casillas **Denegar** para configurar una ACE negativa.

Cuando el sistema inicia una comprobación de acceso, empezará de manera sistemática, por las ACE negativas. Así pues, los permisos "Denegar" siempre tienen prioridad sobre los permisos "Permitir".

Último elemento, hemos visto que el principio más importante se basa en un problema de "no divulgación de la información". Existe una particularidad en los sistemas operativos NT: cuando un usuario crea un archivo, él es el propietario (owner). El SID del propietario se coloca en el descriptor de seguridad que el sistema de archivos NTFS tiene para el objeto correspondiente. El propietario tiene permisos para leer el descriptor de seguridad y así, por ejemplo, modificar la ACL de un archivo. Para conocer el propietario de la carpeta que acaba de crear, haga clic en la pestaña **Seguridad**, después en el botón **Opciones avanzadas**.

Se visualiza directamente el propietario de la carpeta. Puede hacer clic en el enlace **Modificar** para cambiar de propietario.

El propietario de un objeto siempre tiene permisos para leer y modificar la DACL de los objetos que él ha creado, motivo por el que el control de acceso se califica de discrecional (está a discreción del propietario).

## 3. Tomar posesión de un objeto

Haga clic en el botón **Opciones avanzadas**.

Se visualiza directamente el propietario de la carpeta en los parámetros de seguridad avanzados de la propia carpeta.

Por defecto, será su cuenta de usuario la que aparezca como el propietario del recurso. Esto se puede cambiar rápidamente de la siguiente manera:

Haga clic en el enlace **Cambiar**.

Debe buscar o directamente introducir la cuenta o grupo de usuarios que desea definir como propietarios. Puede añadir otros grupos de usuarios haciendo clic en el botón correspondiente.

Seleccione el grupo de administradores y haga clic en **Aplicar**.
Si desea que esta operación se aplique a todos los objetos secundarios, seleccione la casilla **Remplazar el propietario en subcontenedores y objetos**.

Un cuadro de diálogo le avisará de que tendrá que cerrar las propiedades del objeto para que el cambio de propietario sea efectivo.

## 4. Utilizar los permisos NTFS

Pongamos ahora el ejemplo de un administrador llamado Juan que desea compartir una carpeta con permiso de escritura con un usuario llamado Marcos y con permiso de solo lectura con otra usuaria llamada Ana.

Primero cree una carpeta llamada *Prueba*, dentro de la carpeta *Users\Public\Documents*.
Dentro de esta, cree el archivo que deberá ser visible, lo puede llamar *Fichero.txt*.

Cualquier usuario tendrá acceso a la carpeta y podrá modificar el documento, ya que la entidad de sistema INTERACTIVE posee las autorizaciones especiales para el contenido de esta carpeta. La entidad reúne a todos los usuarios que han abierto una sesión interactiva en Windows.

Empiece por desactivar el mecanismo de herencia, copiar los permisos y eliminar el grupo INTERACTIVE.

La carpeta ya no será accesible para los usuarios Marcos y Ana.

Hay que señalar que debido a que usted forma parte del grupo de administradores, no tendrá ningún problema de acceso a la carpeta.

Una vez que ha realizado este primer paso, añada el usuario llamado Ana.

Ana podrá visualizar el contenido del archivo, pero no podrá eliminarlo, modificarlo ni crear otros documentos.

Por defecto, las tres autorizaciones genéricas que se han añadido son las siguientes: **Lectura y ejecución - Mostrar el contenido de la carpeta - Lectura**.

Ahora añada el usuario llamado Marcos.
Haga clic en el botón **Opciones avanzadas**, y seleccione el usuario **Marcos**.

Haga clic en el botón **Modificar**, y a continuación en el enlace **Mostrar permisos avanzados**.

Seleccione estas cuatro casillas:

- **Crear archivos / escribir datos**
- **Crear carpetas / anexar datos**
- **Escribir atributos**
- **Escribir atributos extendidos**

Por lo que respecta al usuario, este puede editar el contenido del archivo y añadir otros documentos, pero en ningún caso podrá:

- Cambiar el conjunto de permisos NTFS.
- Tomar posesión de la carpeta.
- Eliminar la carpeta o el archivo.

## 5. Tomar posesión de un directorio

El comando TakeOwn permite a un administrador (en Windows) recuperar el acceso que se le ha denegado a un archivo al haberse cambiado el propietario del archivo.

La sintaxis es la siguiente:

```
TAKEOWN [/S sistema] [/U usuario [/P contraseña]]] /F nombre_de_archivo
[/A] [/R [/D linea_de_comandos]]
```

Los modificadores son:

- **/s**: indica el sistema remoto al que conectarse.
- **/u: [dominio\]usuario**: especifica el contexto de usuario en el que el comando debe ejecutarse. Este modificador no puede utilizarse sin /s.
- **/p: [contraseña]**: define la contraseña del contexto de un usuario determinado.
- **/f : nombre_de_archivo**: indica el nombre del archivo o directorio. Puede utilizar el carácter genérico * para englobar varios archivos.
- **/a**: asigna la posesión al grupo de administradores y no al usuario actual. Este modificador no es específico, la posesión del archivo se asignará al usuario conectado en ese momento.
- **/r**: trata el comando en modo recursivo. La operación se realizará en un conjunto de directorios y subdirectorios.
- **/d: línea_de_comandos**: permite definir una respuesta predeterminada que se utilizará aunque el usuario actual no posea el permiso "mostrar lista de carpetas" en un directorio. Esto se produce durante el proceso recursivo (/R) de subdirectorios. Utilice los valores "O" para tomar posesión o "N" para ignorar.

Aquí le mostramos un ejemplo de uso. Después de una instalación de Windows, algunos directorios situados en otra partición ya no son accesibles, ni siquiera desde una cuenta de usuario con privilegios de administrador. La explicación es sencilla: las ACL se configuran en función del SID que ya no existe en el sistema. En este caso, puede utilizar estos dos comandos:

- **takeown /f Nombre_del_directorio /r /d o**. Un mensaje le avisará: "CORRECTO: el archivo (o carpeta): ubicación y Nombre_de_archivo" es propiedad del usuario "PC\Nombre_de_usuario".
- **icacls Nombre_del_directorio /grant administradores:f /t**

¡El acceso al directorio será entonces posible! Tenga en cuenta que deberá ejecutar el Símbolo del sistema como administrador, de lo contrario aparecerá un mensaje que indica que el acceso ha sido denegado. Vea otro ejemplo de comandos que le permitirán tomar posesión del archivo Hosts:

- **takeown /f c:\windows\system32\drivers\etc\hosts**
- **icacls c:\windows\system32\drivers\etc\hosts /grant juanki:f**

Más adelante explicaremos la sintaxis de icacls.

## 6. Modificar las listas de control de acceso

Mediante el Símbolo del sistema, puede modificar las ACL de los archivos utilizando una herramienta llamada icacls. Aquí le mostramos las diferentes sintaxis posibles:

```
Icacls Nombre /save Nombre_de_archivo [/T] [/C] [/L]
```

Almacena las listas de control de acceso para todos los archivos coincidentes en Nombre_de_archivo. Este comando le permitirá utilizar luego el parámetro /restore.

```
icacls Nombre_de_directorio [/substitute Antiguo_SID Nuevo_SID [...]]
/restore Nombre_de_archivo [/C] [/L]
```

Aplica las listas de control de acceso guardadas en los archivos actuales del directorio.

```
icacls Nombre /setowner usuario [/T] [/C] [/L]
```

Cambia el propietario de todos los archivos coincidentes.

```
icacls Nombre /findsid SID [/T] [/C] [/L]
```

Busca todos los archivos correspondientes que contienen una lista de control de acceso donde se menciona el SID de manera explícita.

```
icacls Nombre /verify [/T] [/C] [/L]
```

Busca todos los archivos cuya lista de control de acceso no esté en formato canónico o cuya longitud no sea coherente con el número de entradas de control de acceso.

```
icacls Nombre /reset [/T] [/C] [/L]
```

Reemplaza las listas de control de acceso por las listas heredadas de manera predeterminada por todos los archivos correspondientes.

```
icacls Nombre [/grant[:r] SID:autorización[...]]
```

Concede los derechos de acceso al usuario especificado.

- Con el modificador :r, los permisos reemplazan cualquier permiso explícito concedido previamente.
- Sin el modificador :r, los permisos se agregan a cualquier permiso explícito concedido anteriormente.

```
icacls Nombre /deny ISD:autorización
```

Deniega de manera explícita los derechos de acceso al usuario especificado. Se agrega a los permisos indicados una entrada de control de acceso de denegación explícita y se eliminan los mismos permisos de cualquier concesión explícita.

```
icacls Nombre /remove[:[g|d]] SID
```

Suprime todas las repeticiones de SID en la lista de control de acceso.

- Con el modificador :g, se eliminan todas las repeticiones de derechos concedidos a este SID.
- Con el modificador :d, se eliminan todas las repeticiones de derechos denegados a este SID.

```
icacls Nombre /setintegritylevel [(CI)(OI)]
```

Este nivel añade de forma explícita una ACE de integridad (un nivel de integridad) a la carpeta correspondiente. El nivel puede ser:

- **L[ow] - Bajo**
- **M[edium] - Medio**
- **H[igh] - Alto**

Las opciones de herencia para la ACE de integridad pueden preceder al nivel y se aplican solo a los directorios.

Los SID pueden especificarse con un formato numérico o un nombre descriptivo. Si utiliza un formato numérico, agregue un asterisco al principio del SID.

- **/T** indica que esta operación se realiza en todos los archivos o directorios coincidentes que se encuentran en los directorios especificados en el nombre.
- **/C** indica que esta operación continuará en todos los errores de archivo. Se seguirán mostrando los mensajes de error.
- **/L** indica que esta operación se realiza directamente en el vínculo simbólico en lugar de en su destino.

No dude en consultar el archivo de ayuda de este comando para obtener más información.

## 7. Utilizar icacls

De la misma manera que antes, cree un fichero llamado *Prueba* en el directorio del usuario. Visualice la lista de las ACL utilizando el siguiente comando: **icacls Prueba.txt**.

Tres usuarios o grupos de usuarios aparecerán en una lista: usted, el grupo SISTEMA y el grupo Administradores.

- Todos poseen control total sobre el directorio: (F).
- La ACL es heredada: (I).

Para salvar la máscara de permisos, teclee: **icacls prueba.txt /save "Permisos del archivo Prueba"**

El archivo se puede abrir con el Bloc de notas de Windows y enumera los SID de usuario y la lista de permisos mediante la sintaxis SDDL.

# El Registro de Windows

El Registro juega un papel clave en la configuración del sistema operativo. No es simplemente un conjunto de datos estáticos existentes en el disco duro, sino también, mediante una arquitectura compleja de información dinámica, una ventana abierta al corazón del sistema.

El Editor del Registro es una utilidad que permite visualizar y editar todas las informaciones contenidas en los archivos de subárbol. Los archivos de subárbol son los archivos que contienen los parámetros del sistema operativo y de las aplicaciones y constituyen lo que llamamos Registro.

## 1. Ejecutar el Registro

En el cuadro de texto **Buscar en el web y en Windows** situado a la derecha del menú **Inicio**, introduzca: **regedit**. Para abrir varias ventanas de registro, introduzca el modificador **-m**: **regedit -m**. Puede hacerlo tantas veces como desee. Simplemente recuerde que los cambios realizados en una de las ventanas no repercutirán en la otra, a menos que seleccione una ventana y la actualice pulsando la tecla [F5].

## 2. Actualizar el Registro

En Windows 10 y Windows 8, cuando realiza un cambio en el Registro o en el Editor de objetos de directiva de grupo, los cambios están activos de manera inmediata (salvo algunas excepciones).

## 3. Los valores y la información del valor

Hay cinco ramas visibles que se pueden expandir de diferentes formas:

- Haciendo clic en la flecha pequeña de la izquierda.
- Haciendo doble clic en una de las ramas.
- Haciendo clic con el botón secundario del ratón y seleccionando la opción **Expandir**.

Verá que en el interior de cada una de las ramas hay un árbol de claves y subclaves. Las claves son una manera de organizar los datos presentes y clasificarlos por temas.

Si selecciona una de las claves, aparecerán algunos datos en la ventana de la derecha. Estos son los valores y están formados por tres informaciones:

- nombre del valor
- tipo del valor
- datos inscritos en el valor llamados "Datos del valor"

Cada una de las claves puede contener uno o más valores.

No es posible modificar las ramas principales, pero puede realizar todo tipo de operaciones en las claves, valores y datos del valor.

## 4. Estructura del Registro

Las claves raíz visibles son cinco.

- **HKEY_CLASSES_ROOT**: contiene principalmente la información de asociación de archivos, componentes COM y la información de registro de objetos.
- **HKEY_CURRENT_USER**: contiene los datos correspondientes al usuario que está conectado en ese momento.
- **HKEY_LOCAL_MACHINE**: contiene los datos correspondientes al sistema.
- **HKEY_USERS**: contiene los datos correspondientes al conjunto de usuarios del equipo.
- **HKEY_CURRENT_CONFIG**: contiene información del perfil físico actual.

Es habitual que algunas claves utilicen las abreviaturas siguientes:

- HKEY_CLASSES_ROOT: HKCR.
- HKEY_CURRENT_USER: HKCU.
- HKEY_LOCAL_MACHINE: HKLM.
- HKEY_USERS: HKU.
- HKEY_CURRENT_CONFIG: HKCC.

La letra H representa el identificador de Windows (Handle) de las claves (KEY).

Algunas claves funcionan como enlaces replicados que dirigen a otros árboles:

- La clave HKEY_CURRENT_CONFIG es una réplica de esta rama: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Hardware Profiles\Current.
- La clave HKEY_CLASSES_ROOT es una réplica de esta: HKEY_LOCAL_MACHINE\SOFTWARE\Classes.
- La clave HKEY_CURRENT_USER corresponde a esta: HKEY_USERS\Usuario conectado en ese momento.

En conclusión, solo las claves HKEY_USERS y HKEY_LOCAL_MACHINE poseen una existencia propia.

## 5. Los archivos de subárbol

Toda la información se extrae directamente de los archivos de subárbol que están ubicados principalmente en *\Windows\system32\config*. Presentamos aquí la lista de correspondencias:

- HKEY_LOCAL_MACHINE\BCD00000000: *\Boot\BCD*
- HKEY_LOCAL_MACHINE\COMPONENTS: *\Windows\system32\config\COMPONENTS*
- HKEY_LOCAL_MACHINE\SAM : *\windows\system32\config\SAM*
- HKEY_LOCAL_MACHINE\SECURITY: *\Windows\system32\config\SECURITY*
- HKEY_LOCAL_MACHINE\SOFTWARE: *\Windows\system32\config\SOFTWARE*

- HKEY_LOCAL_MACHINE\SYSTEM: *\Windows\system32\config\SYSTEM*
- HKEY_USERS\SID: *\Users\"Nombre_de_usuario"\ntuser.dat*
- HKEY_USERS\SID del usuario_Classes: *\Users\Juan\AppData\Local\Microsoft\Windows\UsrClass.dat*
- HKEY_USERS\.DEFAULT: *\Windows\system32\config\DEFAULT*
- HKEY_LOCAL_MACHINE\HARDWARE: subárbol volátil

Este último subárbol está ubicado exclusivamente en la memoria, así que no tiene una ruta precisa en el Explorador de Windows. Hay dos archivos de subárbol un poco particulares creados por NTDETECT.COM cada vez que el ordenador arranca:

- Servicio local: `\Windows\ServiceProfiles\LocalService\NTUSER.DAT`
- Servicio de red: `\Windows\ServiceProfiles\NetworkService\NTUSER.DAT`

Hay diferentes tipos de archivos:

- Regtrans-ms: estos archivos son diarios de transacciones que se utilizan para almacenar los cambios en bases de registro para evitar la corrupción de archivos de subárbol.
- Blf: del mismo modo, el componente Common Lof File System (CLFS) utiliza estos ficheros diarios para almacenar los cambios en bases de registro para evitar la corrupción de archivos de subárbol.
- LOG: estos archivos son archivos de registro que guardan los cambios realizados tanto en claves como en valores.

Las versiones de seguridad de los ficheros de subárbol se colocan en el directorio C:\Windows\System32\RegBack. En un principio, se trata de la mejor opción si quiere restaurar manualmente un archivo de subárbol de tipo Maquina y reemplazarlo por otra versión.

La lista de archivos de subárbol se puede obtener visualizando el contenido de esta clave de registro: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\hivelist

## 6. Manipular el registro

Existen varias maneras de crear una nueva clave. Puede, por ejemplo:

Seleccionar la clave primaria.
Hacer clic en **Edición - Nuevo - Clave**.

Aparecerá la mención *Clave nueva #1*.

Como de manera predeterminada se encuentra en modo Edición, podrá introducir directamente el nombre de la clave. Si no es así puede cambiar de nuevo al modo Edición pulsando la tecla [F2].

También puede utilizar el menú contextual accesible desde la clave que funciona como contenedor, siempre y cuando esta última esté seleccionada, o puede activar el menú contextual haciendo clic en la ventana de la derecha.

De la misma manera, también es posible eliminar ([Supr]) o renombrar una clave.

No es posible eliminar o seleccionar varias claves a la vez manteniendo presionadas las teclas [Ctrl] o [Mayús]. Sin embargo, sí puede hacerlo con los valores.

Tenga en cuenta que cada vez que cree una clave, automáticamente se creará un valor (predeterminado).

## 7. Modificar los valores

De la misma manera que antes, puede crear nuevos valores DWORD, de cadena, binario, etc. El nombre predeterminado será: Nuevo valor #1.

Para insertar los datos en la entrada que acaba de crear, haga doble clic en ella e introduzca la cadena de caracteres en el cuadro de texto **Información del valor**.

También puede hacer clic con el botón secundario del ratón en esa entrada y después en el comando **Modificar**. El mismo comando es accesible desde el menú **Edición**.

Existen dos opciones: **Modificar** y **Cambiar datos binarios**. Esta última le permite visualizar los datos en su representación hexadecimal.

Puede visualizar directamente este tipo de información si selecciona un valor DWORD o binario y hace clic en **Ver - Mostrar datos binarios**.

Por otra parte, cuando introduzca la información del valor en una entrada DWORD, podrá elegir entre utilizar la base decimal o hexadecimal. En el primer caso, solo tendrá que seleccionar la opción de botón **Decimal**. De todas maneras, la cifra o número que introduzca se mostrará en base hexadecimal.

Cuando cree un nuevo valor de cadena, los datos del valor estarán vacíos.

De manera predeterminada, al crear un valor DWORD los datos serán de valor cero y en el caso de valores binarios estos serán de longitud cero.

Cuando cree una nueva clave, el valor (predeterminado) indica que los datos no están definidos (valor no definido).

## 8. Buscar en el Registro

Para realizar una búsqueda, seleccione el árbol de partida y haga clic en **Edición - Buscar**([Ctrl]+F).
En el cuadro de texto **Buscar**, introduzca la expresión buscada.
En el apartado **Buscar en** indique si la búsqueda se realizará sobre las:

- Claves
- Valores
- Datos

Puede seleccionar la casilla **Solo cadenas completas** si prefiere encontrar los casos que corresponden exactamente a la expresión buscada (y no de manera parcial).

Para lanzar una búsqueda, haga clic en **Edición - Buscar siguiente** o pulse la tecla [F3].

En cada ocasión, la entrada o clave correspondientes se señalarán con un resaltado.

Tenga en cuenta que si la búsqueda se realiza en todo el conjunto del Registro no deberá seleccionar la rama primaria Equipo, sino la primera clave: HKEY_CLASSES_ROOT. En caso contrario, la búsqueda no dará ningún resultado.

Por otra parte, una búsqueda se inicia siempre desde la clave seleccionada. Para alcanzar rápidamente el punto de partida de la búsqueda pulse la tecla [Inicio]. La rama Equipo se resaltará automáticamente. Una vez realizado esto, solo tendrá que seleccionar la clave HKEY_CLASSES_ROOT.

## 9. Importar o exportar una clave

Esta operación permite copiar el conjunto de valores incluidos en una clave, así como la propia clave. Esto le permitirá exportar una parte del Registro procedente de un ordenador "sano" e importarlo al sistema "dañado". Es una manera rápida y segura de reparar un problema debido a entradas defectuosas en el registro.

Seleccione una de las claves del registro.
Haga clic en **Archivo - Exportar**.

También puede utilizar la opción **Exportar** que aparece en el menú contextual de la clave.

En la lista desplegable **Guardar en**, seleccione el directorio de destino.
En el cuadro de texto **Nombre**, introduzca un nombre para el archivo.

Le recordamos que el nombre que elija no tiene importancia.

En la lista desplegable **Tipo**, seleccione el formato que tendrá el archivo de rescate.

Puede elegir entre:

- **Archivo de Registro (*.reg)**: el archivo tendrá una extensión en REG que contendrá como encabezado lo siguiente: Windows Registry Editor Version 5.00. Este formato es compatible con las versiones Windows XP y posteriores.
- **Archivo de subárbol de Registro**: este archivo no tendrá ninguna extensión visible. Más adelante veremos su utilidad práctica.
- **Archivos de texto (*.*)**: el archivo tendrá una extensión TXT. Muestra el nombre de la clase así como la hora de la última escritura para cada clave o valor de la lista.
- **Archivos de Registro de Win9x/NT4 (REGEDIT4) (*.reg)**: este formato de registro es compatible con las versiones antiguas de Regedit que podemos encontrar en Windows 9X, ME y Windows NT. El encabezado del archivo será: REGEDIT4. También puede utilizar el formato de registro en los sistemas más recientes de Windows.
- **Todos los archivos**: esta posibilidad permite cambiar de manera sencilla la extensión del fichero de registro.

Esta opción necesita algunas aclaraciones: no es necesario que un archivo de registro tenga una extensión REG, ya que también funciona con archivos sin extensión que lleven una extensión que usted ha creado.

Con el fin de editar un archivo de registro REG en formato de texto, haga clic con el botón derecho en el archivo y seleccione la opción **Modificar**.

El archivo de registro se abrirá en el Bloc de notas de Windows.

También puede seleccionar abrirlo con otro programa haciendo clic en el submenú **Abrir con**.

En lo que respecta a los archivos de subárbol, describimos aquí los pasos que se deben seguir:

Haga clic con el botón secundario del ratón en el archivo y seleccione la opción **Abrir**.
En el apartado **Elija el programa que desea usar** para abrir el archivo seleccionado, utilice, por ejemplo, el Bloc de notas de Windows.

Como podrá comprobar es ilegible.

En el apartado **Intervalo de exportación**, indique si desea exportar el registro completo o simplemente el árbol que ha seleccionado. Esta última posibilidad es mucho más razonable.
Haga clic en **Guardar**.

Veamos ahora las ventajas e inconvenientes de estos dos métodos:

Un archivo de subárbol ocupa el doble que un archivo REG. Se trata de una imagen en formato binario del árbol que ha guardado. No puede exportar este archivo mediante el comando Regedit ni haciendo doble clic en el archivo de subárbol. Deberá hacer clic en **Archivo - Importar** y seleccionar el archivo de subárbol. Al contrario que un archivo *.reg*, se sobrescribirá el árbol existente y todo el contenido remplazará al archivo *.hiv*. En el caso de tratarse de un archivo REG, se conservarán los valores antiguos. Si dos valores tienen el mismo nombre, solo los datos del valor serán modificados si es preciso. Veamos un ejemplo práctico:

En el Registro, abra esta rama: HKEY_CURRENT_USER.
Cree una nueva clave llamada **Prueba**.
Seleccione esta última clave y cree un valor de cadena llamado **prueba1**.
Edite este valor e introduzca un texto cualquiera. solo es una prueba.
Exporte la clave **Prueba** como un archivo de subárbol en el formato REG.
Edite el nuevo valor **prueba1** y modifique su contenido.
Cree ahora un segundo valor de cadena llamado **prueba2**.

Abra el Explorador de Windows en la ubicación en la que haya guardado los archivos REG y de subárbol.
Haga clic con el botón secundario del ratón en el archivo REG y en la opción **Combinar**.
Confirme la combinación de los datos con los del Registro de Windows.

Después de actualizar la visualización del Registro pulsando la tecla [F5], podrá comprobar que:

- Los datos del valor prueba1 se han modificado correctamente.
- El valor test2 todavía está presente.

En el Registro, haga clic en **Archivo - Importar** y seleccione el archivo de subárbol.

En la lista desplegable situada en la parte inferior de la ventana, seleccione la opción **Archivos de subárbol de Registro (*.*)** y seleccione el archivo de subárbol.
Haga clic en el botón **Abrir**.
Confirme la sustitución de la clave.

El registro de Windows se actualizará inmediatamente y la clave prueba2 se eliminará correctamente.

Todo esto para decirle que si debe guardar claves de Registro antes de hacer una operación que le parece peligrosa, es preferible exportarlas en formato de subárbol y no en formato REG.

Hay una pregunta que nos viene a la mente: si realizamos una modificación en los permisos de una clave de Registro, ¿es posible restaurar el conjunto de permisos NTFS? En estos casos llevaremos a cabo el mismo tipo de modificación:

Seleccione la clave llamada **Prueba** y en el menú **Edición** haga clic en el submenú **Permisos**.
Haga clic en el botón **Opciones avanzadas** y a continuación en el botón **Desactivar la herencia**.
Haga clic en el enlace **Convertir los permisos heredados en permisos explícitos en este objeto**.

Seleccione el nombre de usuario que aparece en la sección **Nombres de grupos o usuarios** y haga clic en los botones **Quitar** y **Aceptar**.

De esta manera, habremos:

- Desactivado el mecanismo de herencia de los permisos NTFS.
- Eliminado su cuenta de usuario de la lista de usuarios para los que se estableció una ACE.

Con el botón secundario del ratón haga clic en el archivo de registro y, a continuación, en la opción **Combinar**.

Tenga en cuenta que también puede hacer doble clic en el archivo de registro.

Si accede otra vez al conjunto de permisos NTFS de la clave Prueba verá que la situación sigue siendo la misma.

Realice la misma modificación pero, esta vez, importe el archivo de subárbol.
Abra otra vez la ventana de permisos de la clave **Prueba**. Esta vez, el mecanismo de herencia y el conjunto de permisos han sido restaurados.

La conclusión es irrefutable: si debe realizar modificaciones en el conjunto de permisos de una clave, elija como copia de seguridad un archivo de subárbol.

## 10. Reparar un servicio utilizando las herramientas WinRE

Vamos a utilizar el mismo truco para editar el Registro de Windows. Esto supone que la opción **Última configuración válida conocida** no ha funcionado y no ha podido restaurar el ordenador a un estado anterior.

Abra una ventana de Símbolo del sistema.
Introduzca estos dos comandos y acepte después de cada uno con la tecla [Intro]:

- **\windows\inf**
- **notepad setupapi.app.log**

Cada servicio y controlador de dispositivos se clasifica por fecha.

Así pues, identifique el último controlador o servicio que haya instalado.
A continuación, introduzca el siguiente comando: **regedit**.
Cargue el subárbol SYSTEM que está accesible en esta ubicación: \Windows\System32\Config.
Dele un nombre temporal y abra este árbol: Current\ControlSetxxx_Services.
Acto seguido, localice la clave que el servicio o controlador han instalado.
Edite un valor DWORD llamado **Start** e introduzca como información del valor la cifra 4.

Haga lo siguiente para desactivarlo:

Libere el subárbol temporal y reinicie el ordenador.

# Los registros de eventos

## 1. Administrar y utilizar los registros de eventos

El visor de eventos es una de las herramientas más utilizadas por los administradores de sistemas para analizar la actividad diaria de un equipo Windows. El Visor de eventos recoge la información del sistema, así como la de los servicios y aplicaciones.

Esta herramienta se convierte en indispensable para ayudar a diagnosticar y determinar el origen de un error. Permite visualizar la actividad del sistema y encontrar códigos de error vinculados a los artículos de la base de conocimientos de Microsoft.

Windows 10, al igual que Windows 8, dispone de diferentes registros de eventos para almacenar toda la información del sistema operativo y de las aplicaciones y servicios Windows. Para saber rápidamente el estado de un sistema, puede consultar los registros Windows. Si el problema es, por ejemplo, un servicio en concreto, puede comprobar los registros de los servicios Windows. Cada servicio dispone de su propio registro de eventos.

Los registros de eventos se almacenan como ficheros de tipo *.evtx, y están ubicados en el directorio %SystemRoot%\System32\Winevt\Logs\.

Desde Windows 7, la utilización del Visor de eventos no se limita solo a la recopilación de eventos. Por ejemplo, puede utilizar los registros de eventos Windows para acciones correctivas, como activar una tarea planificada a partir de un evento de tipo error.

Para ejecutar el Visor de eventos, desde el menú **Inicio**, teclee **eventvwr.msc** en el área de búsqueda y pulse la tecla [Intro].

También puede mostrar el Visor de eventos desde las herramientas administrativas, a las que se accede desde la sección **Sistema y seguridad** del Panel de control.

La herramienta **wevutil.exe** permite administrar los registros de eventos a través de un Símbolo del sistema.

También dispone de cmdlets PowerShell para administrar y acceder a los registros de eventos como por el ejemplo el comando **Show-Eventlog**.

## 2. Filtrar los eventos de tipo error

El proceso de filtrado es el mismo sea cual sea el registro seleccionado. Para mostrar los eventos generados por los componentes del sistema Windows, en el Visor de eventos seleccione el registro **Sistema**.

Para filtrar este registro para obtener solo los eventos de tipo error y advertencia de los siete últimos días, en el panel **Acciones**, seleccione la opción **Filtrar registro actual**.
Introduzca la reglas de filtrado, en este caso los eventos de tipo **Error** y **Advertencia**. Haga clic en el botón **Aceptar** para activar la regla de filtrado. En la pantalla anterior tiene la posibilidad de definir múltiples criterios de filtrado.

Puede exportar o archivar este registro filtrado en formato *evtx o *.csv por ejemplo para explotarlo en otra herramienta.

## 3. Diagnosticar los errores de arranque de servicio

Cuando un servicio no arranque, el mensaje de error indica el código de error y le invita a que consulte el registro de eventos **Sistema**.

Tomemos por ejemplo el servicio **BranchCache**, en un equipo que no pertenece a un dominio. Intente arrancar este servicio desde la consola de administración de los servicios Windows, podrá observar que no arranca.

Si abre el registro relativo al servicio **BranchCache**, podrá visualizar los mensajes de error generados por las acciones de arranque sucesivas del servicio Windows.

Seleccione un evento de tipo error y acceda a las propiedades de este evento. En la pestaña **Detalles**puede ver la información que permite calificar el error analizado. Por ejemplo, puede ver el SID (*Security Identifier*) que corresponde a la cuenta de usuario utilizada en este contexto, en este caso la cuenta **SERVICIO DE RED**. Esta cuenta está asignada por defecto como cuenta de arranque del servicio.

En el caso del servicio BranchCache, el mensaje de error indica que el programa se ha bloqueado por una directiva de grupo. Esta directiva es obligatoria para la implementación de la funcionalidad.

Atención, algunos registros no están activos por defecto. Si quiere, por ejemplo, resolver problemas relacionados con el servicio de impresión, deberá activar el registro de tipo **Operativo** del servicio **PrintService** a través del enlace **Habilitar registro** en el panel **Acciones**.

# El administrador de tareas

## 1. Presentación

El administrador de tareas permite controlar el estado de ejecución en tiempo real de su ordenador. Por ejemplo, en esta herramienta puede visualizar los procesos ejecutados, el

rendimiento del sistema, los usuarios conectados, el estado de los servicios Windows y los detalles de los procesos que se están ejecutando. También puede acceder a las funciones avanzadas de los procesos, como por ejemplo, visualizar el árbol o modificar la prioridad de ejecución de ciertos procesos.

Para visualizar el Administrador de tareas, presione simultáneamente las teclas [Ctrl][Alt][Supr] y seleccione el Administrador de tareas. También puede, desde el menú **Inicio**, teclear el comando **taskmng.exe** en la zona de búsqueda y pulsar la tecla [Intro].

El Administrador de tareas se ejecuta en modo usuario y accede a los procesos del núcleo por medio de la función NTQuerySystemInformation de la librería NTDLL.dll. Así se beneficia de permisos extendidos en un contexto de ejecución limitada.

Para acceder a la vista completa de las pestañas y detalles del Administrador de tareas, haga clic en el enlace **Más detalles**.

Si el Administrador de tareas está desactivado, por ejemplo por un virus, puede volver a activarlo modificando la clave de registro **DisableTaskMgr** que puede encontrar en HKEY_CURRENT_USER\Software\ Microsoft\Windows\Current Version\Policies\System.

## 2. Gestión avanzada de los procesos

### Visualización de los procesos

En la vista detallada del Administrador de tareas, la pestaña **Procesos** permite visualizar los procesos por categorías:

- Las aplicaciones,
- Los procesos en segundo plano,
- Los procesos Windows

Si selecciona un proceso y hace clic con el botón derecho sobre él, se muestra un menú con las acciones disponibles para el proceso. Por ejemplo, puede hacer clic en el enlace **Abrir ubicación del archivo**para acceder al directorio de almacenamiento del fichero físico vinculado al proceso. También dispone del enlace **Ir a detalles**, que permite bascular a la pestaña **Detalle**.

Esta pestaña muestra por defecto información y detalles sobre las ocurrencias de procesos que se están ejecutando. Por ejemplo, puede visualizar el nombre, el PID o el estado de los procesos.

Si hace clic con el botón derecho sobre un proceso que no se ejecuta correctamente, puede analizar la cadena de espera para determinar el problema que bloquea la ejecución del proceso.

Observe que puede añadir columnas a la visualización propuesta por defecto para acceder a información más detallada sobre los procesos. Para visualizar columnas suplementarias, haga clic con el botón derecho en la barra de descripción de los procesos.

### Forzar la parada de un proceso

A veces es útil poder forzar la parada de una aplicación cuya ejecución está bloqueada o que no responde sin tener que reiniciar su ordenador.

En este caso, el Administrador de tareas permite forzar la parada de un proceso. Para realizar esta acción, en la pestaña **Procesos**, seleccione el proceso que quiere parar en la lista. Haga clic con el botón derecho sobre el proceso y haga clic en **Finalizar tarea**.

### Problema de arranque

La pestaña **Arranque** permite visualizar los procesos ejecutados en la fase de arranque de Windows. Añadiendo la columna **CPU al inicio** a la visualización por defecto, puede determinar el tiempo de CPU, es decir, el tiempo de procesador utilizado por un proceso. Así podrá actuar de manera más eficaz para disminuir el tiempo de latencia en el arranque de Windows.

### Controlar el rendimiento del sistema

En la pestaña **Rendimiento**, seleccione el tipo de actividad que desea supervisar. Si selecciona, por ejemplo, la actividad **Memoria**, puede ver la memoria consumida, la memoria libre y diversa información sobre el tipo y el número de ubicaciones de memoria utilizados.

Si selecciona la actividad **Ethernet**, haga clic con el botón derecho en el gráfico de actividad y a continuación haga clic en el enlace **Ver detalles de la red**.

Se pueden ver los diferentes contadores de actividad de las diferentes interfases de red del ordenador.

## Las herramientas Sysinternals

Este conjunto de herramientas, que proviene de la compra por Microsoft de Sysinternals en 2006, amplía las características de diagnóstico y reparación de las herramientas integradas por defecto en Windows que hemos visto anteriormente.

Estas herramientas están disponibles individual y gratuitamente desde la web de Microsoft. También puede obtener el conjunto de las herramientas descargando la suite Sysinternals desde la siguiente página: https://technet.microsoft.com/es-es/sysinternals/bb842062

La suite Sysinternals está compuesta por numerosas utilidades para la gestión de la seguridad, de la red, del sistema de ficheros y de los discos, así como del sistema en un sentido más amplio.

Si, tomamos como ejemplo la herramienta **Process Explorer**, aunque similar en términos de funciones al Administrador de tareas desde Windows 7, muchos administradores lo siguen utilizando para supervisar en tiempo real los rendimientos de los procesos. Permite, por ejemplo, visualizar en una única interfaz el árbol y los niveles de integridad de los procesos que se están ejecutando. También puede visualizar, como puede ver en la siguiente pantalla, si los procesos utilizan el modo de compatibilidad de control de la cuenta de usuario, es decir el concepto de virtualización del proceso.

La herramienta **Process Monitor**, que es otro ejemplo de herramienta del sistema, sobre todo se utiliza para trazar la actividad de un proceso en el Registro o en el sistema de ficheros, por ejemplo.

La multitud de herramientas ofrecidas por la suite Sysinternals facilita a menudo las operaciones de mantenimiento y reparación en el entorno Windows.

# Gestión de la Autenticación

## Las cuentas de usuario

Se puede distinguir entre las cuentas predefinidas y las cuentas interactivas, que permiten a los usuarios abrir una sesión en el equipo. Las cuentas predefinidas de tipo Administrador o Invitado le permiten sacar provecho de algunas funciones del sistema operativo. Este tipo de cuenta no corresponde pues a un usuario real. Por el contrario, una cuenta de usuario interactiva corresponde a una persona física. El sistema le da una imagen, llamada perfil, que se almacena en esta ubicación: C:\Usuarios\<Nombre Usuarios>.

Cada usuario pertenece a un grupo genérico (predefinido). Igual que se puede crear nuevos usuarios, también se puede crear nuevos grupos.

Cada grupo tiene un conjunto de permisos y restricciones. Así como el grupo de los administradores dispone de todos los permisos, el de los invitados tiene una especie de « libertad vigilada ».

Se puede acceder a la gestión de las cuentas de usuario desde el **Panel de control**, en la sección **Cuentas de usuario**. Observe que en Windows 8 y Windows 10, también puede acceder a la gestión de las cuentas de usuario desde la utilidad de gestión de configuración del PC. También puede utilizar la consola de administración avanzada de los usuarios introduciendo el comando **netplwiz** en el área de búsqueda del menú **Inicio**.

Si desea reinicializar la contraseña de una cuenta, desde la administración avanzada de usuarios, haga clic en el botón **Restablecer contraseña...**. Para acceder a las propiedades de un usuario y visualizar a qué grupo pertenece, es decir, el tipo y el nivel de acceso de la cuenta y haga clic en el botón **Propiedades**.

Seleccione la pestaña **Opciones avanzadas**, en la sección **Administración avanzada de usuarios** y haga clic en el botón **Opciones avanzadas**. Se muestra la consola de administración de las cuentas de usuario. También puede acceder a esta consola introduciendo el comando **lusrmgr.msc** en el área de búsqueda del menú **Inicio**.

Durante la instalación de Windows, hemos visto que es posible configurar una cuenta de usuario de tipo Cuenta Microsoft para integrar las funcionalidades de la nube que ofrece el sistema operativo de Microsoft, como el correo, los contactos o SkyDrive. La administración de este tipo de cuenta es idéntica a las cuentas de usuario locales del ordenador.

En Windows 10, la integración de la nube para las cuentas de usuario permite sincronizar los elementos de configuración de los parámetros personalizados.

## 1. Funcionamiento de los perfiles de usuario

Al arrancar el ordenador, se le pide que inicie su sesión. A cada nombre de sesión le corresponde un usuario. En la primera sesión de un sistema recientemente instalado, se utiliza un perfil de usuario por defecto. Este perfil está descrito en el árbol del registro: HKEY_USERS. A partir de entonces, y a medida que vaya realizando modificaciones en su entorno de trabajo, se guardarán todas las preferencias. De hecho su perfil de usuario se irá perfeccionando con el tiempo.

En los sistemas NT, se utilizan también los perfiles itinerantes (se habla sobre todo de perfiles "errantes"): en un entorno en que un usuario utiliza diversos ordenadores, podrá encontrar su mismo entorno de trabajo sea cual sea el ordenador en el que inicie una sesión.

Por otra parte, se puede asignar un perfil obligatorio para un usuario o grupo de usuarios, o modificar el perfil por defecto que se asignará a cada usuario nuevo. Dicho de otro modo, es posible copiar un perfil de usuario de una cuenta a otra del mismo modo que se pueden fabricar diferentes figuras a partir de un mismo molde.

Windows 10 introduce una nueva versión de gestión del perfil de usuario Windows. Este perfil tendrá una portabilidad superior a sus predecesores en diferentes dispositivos. La gestión de los ficheros y carpetas del perfil de usuario está ubicada por defecto en la carpeta C:\Users.

## 2. Los grupos predefinidos

Existe un cierto número de grupos de usuario que están configurados por defecto en el sistema. Nos hemos limitado a explicar los más extendidos.

### a. Las entidades de seguridad integradas

**ANONYMOUS LOGON**: representa a los usuarios y servicios que acceden a un ordenador sin utilizar un nombre de cuenta, una contraseña o un nombre de dominio.

**CREADOR PROPIETARIO**: representa al usuario que ha creado o es propietario de un objeto.

**INTERACTIVO**: representa a todos los usuarios conectados actualmente a un ordenador y que acceden a un recurso en concreto de ese ordenador (al contrario de los usuarios que acceden a un recurso de red). Cada vez que un usuario accede a un recurso específico en el ordenador en el que está conectado, se agrega automáticamente al grupo Interactivo.

**LÍNEA**: representa a cualquier usuario que está conectado al ordenador utilizando una conexión de acceso remoto.

**REMOTE INTERACTIVE LOGON**: representa a cualquier usuario que esté conectado al ordenador utilizando una conexión de Escritorio remoto.

**RED**: representa a los usuarios que acceden a un recurso específico en la red (al contrario de los usuarios que acceden a un recurso abriendo una sesión local en el ordenador que contiene este recurso). Cada vez que un usuario accede a un recurso específico de red, se agrega automáticamente al grupo Red.

**Todo el mundo**: representa a todos los usuarios de red actuales, incluidos los invitados y los usuarios de otros dominios. Cada vez que un usuario abre una sesión en la red, se agrega automáticamente al grupo Todo el mundo.

**USUARIO TERMINAL SERVER**: representa a cualquier usuario que esté conectado al ordenador utilizando una conexión de Escritorio remoto.

**Usuarios autentificados**: este grupo incluye a todos los usuarios que tienen una cuenta y una contraseña en la máquina local o en Active Directory.

**TODOS LOS PAQUETES DE APLICACIÓN**: esta entidad gestiona los permisos de acceso a los recursos del sistema para las aplicaciones Windows Store.

**PERMISOS DEL PROPIETARIO**: representa los permisos aplicados al propietario actual de un objeto.

**SYSTEM**: con esta identidad el núcleo de sistema administra el conjunto de componentes esenciales para el funcionamiento del núcleo:

- El proceso csrss.exe (*Client/Server Runtime Subsystem*) que gestiona las ventanas y los elementos gráficos de Windows.
- El proceso Lsass.exe (*Local Security Authority Subsystem Service*) que gestiona los mecanismos de seguridad local y de autentificación de los usuarios a través del servicio WinLogon.
- El proceso Lsm.exe (*Local Session Manager*) que gestiona la apertura de sesión local.
- El proceso wmiprvse.exe (*Windows Management Instrumentation*) que gestiona las funcionalidades WMI.
- El proceso Wininit.exe que gestiona el arranque de Windows.
- El proceso Winlogon.exe (*Windows Logon Process*) que gestiona la apertura y el cierre de las sesiones.
- El proceso SearchIndexer que gestiona la indexación de los ficheros para las funciones de búsqueda.
- El proceso svchost.exe que es un proceso host genérico para ejecutar servicios a partir de librerías dinámicas (DLL). Podrá ver varias instancias de este proceso que corresponden a otros tantos servicios Windows arrancados.

**SERVICIO DE RED**: esta cuenta es utilizada por los servicios que necesitan autentificarse en otros equipos de la red sin tener permisos especialmente amplios.

**SERVICIO LOCAL**: es el mismo tipo de cuenta con la diferencia que solo puede acceder a los recursos de red que permiten un acceso anónimo. Sobretodo permite la ejecución de procesos vinculados a la gestión de dispositivos y de algunos servicios de red como, por ejemplo, la resolución de nombre NetBIOS (LmHosts).

**Restricted**: permite definir una ACE en una ACL que implica un permiso de tipo Denegar para todos los tokens de acceso restringido. A esta entidad se asignará un permiso de tipo "Denegar", o de tipo "Lectura". En los dos casos, los grupos o los usuarios con restricciones no tienen acceso al recurso porque los ACE negativos van por delante de los ACE positivos. Para otras entradas, solo tendrán acceso de solo lectura.

**Trusted Installer**: la tecnología WRP (*Windows Resource Protection*) actúa como una especie de autoridad suprema que impide cualquier cambio en los ficheros, directorios y claves del Registro que se consideren necesarias para el buen funcionamiento del sistema. Solo, en ese caso, el servicio Trusted Installer puede realizar cambios en los recursos que están protegidos por este servicio.

### b. Los grupos de usuarios

**Administradores**: agrupa los miembros que poseen permisos de administrador.

**Duplicadores**: los miembros de este grupo tienen permisos para replicar ficheros en el dominio.

**IIS_IUSRS**: los miembros de este grupo predefinido tienen permisos ampliados sobre los recursos y ficheros del sistema para definir pools IIS como cuentas de servicio. Si una cuenta de servicio está asignada a un pool IIS, se convierte automáticamente en miembro de este grupo.

**Lectores del registro de eventos**: los miembros de este grupo disponen de permisos para leer los registros de eventos en el ordenador local.

**Operadores de asistencia de control de acceso**: los miembros de este grupo pueden preguntar remotamente por los recursos de sistema avanzados (permisos y autorizaciones ) en el ordenador local.

**System Managed Accounts Group**: los miembros de este grupo dedicado a las futuras funcionalidades de Windows 10 son gestionados por el sistema.

**Usuarios COM distribuidos**: los miembros de este grupo pueden ejecutar, activar y utilizar localmente los objetos COM distribuidos.

**Invitados**: los miembros del grupo Invitados tienen por defecto el mismo acceso que los miembros del grupo Usuarios, excepto la cuenta Invitado que tiene permisos restringidos.

**Operadores de configuración de red**: agrupa los miembros que tienen algunos permisos relativos a la configuración de las interfaces de red.

**Operadores de copia de seguridad**: agrupa los miembros que pueden hacer copias de seguridad y restaurar todos los ficheros de un ordenador.

**Usuarios**: los miembros de este grupo tienen un acceso limitado a los recursos y tienen un número limitado de permisos.

**Usuarios avanzados**: los miembros de este grupo pueden realizar un cierto número de tareas administrativas sin tener el control total del equipo. Este grupo está presente por razones de compatibilidad con los sistemas anteriores.

**Usuarios de escritorio remoto**: agrupa los miembros que tienen permisos de apertura de sesión remota.

**Usuarios del monitor del sistema**: agrupa los miembros que pueden visualizar los datos de rendimiento en tiempo real en el Monitor de rendimiento.

**Usuarios del registro de rendimiento**: agrupa los miembros que pueden, además de visualizar los datos de rendimiento en tiempo real, crear y modificar conjuntos de recopiladores de datos en el Monitor de rendimiento.

**Usuarios de administración remota**: agrupa los miembros que acceden a los recursos WMI a través de protocolos de comunicación compatibles.

**Administradores de Hyper-V**: agrupa los miembros que tienen permisos de administrador para las funcionalidades de Hyper-V.

**Operadores criptográficos**: agrupa los miembros que tienen permisos de implementación de operaciones de cifrado.

### c. Los usuarios predefinidos

**Administrador**: esta cuenta especial le permite liberarse del control de la cuenta de usuario. El token de acceso que se le concede es único. Por defecto está desactivada en Windows 8 y Windows 10.

**Invitado**: esta cuenta también está desactivada por defecto en Windows 8 y Windows 10. Es útil en el caso que se quiera dar acceso ocasional para un usuario que casi no tendrá permisos sobre los recursos.

**DefaultAccount**: cuenta de usuario dedicada para las futuras funcionalidades de Windows 10. Esta cuenta está gestionada por el sistema.

Puede activar estas dos cuentas siguiendo este proceso:

En el área de texto **Buscar** a la derecha del menú **Inicio**, introduzca este comando: **netplwiz**.
Haga clic en la pestaña **Opciones avanzadas** y a continuación en el botón **Opciones avanzadas**.
Abra la carpeta **Usuarios** y a continuación la cuenta que desee modificar.
Desmarque la casilla **La cuenta está deshabilitada**.

# El control de la cuenta de usuario

Windows Vista ha introdujo un nuevo concepto de seguridad llamado UAP o *User Account Protection* (en castellano, control de cuenta de usuario). Se utilizan otros términos: *Least-Privilege User Accounts* o *Limited User Accounts* (LUA). Este concepto, ahora llamado UAC (*User Account Control*), se ha conservado y mejorado en Windows 7 y después en Windows 8 y Windows 10 para que sea menos restrictivo para el usuario.

Los usuarios creados por Windows tienen estado de administrador protegido, es decir que la funcionalidad UAC está activada para estas cuentas. No es el caso de la cuenta Administrador que designa la cuenta integrada en el sistema operativo pero que, por defecto, está desactivada.

Cuando un usuario tiene permiso para interactuar sin restricción con el sistema, puede instalar una aplicación, escribir en la rama del registro HKEY_LOCAL_MACHINE, instalar dispositivos, arrancar servicios, etc.

En modo protegido, todos los procesos iniciados por un administrador se ejecutan con un mínimo de permisos. Si, por ejemplo, abre un programa desde el menú **Inicio**, la aplicación se ejecutará en un contexto limitado con los mismos permisos que se han definido previamente.

Si la aplicación, para poder ejecutarse correctamente, requiere más permisos, será necesario que la cuenta de administrador pueda ejecutar el proceso de modo no restrictivo. El proceso hereda entonces numerosos privilegios acordados por esta elevación de priviliegios (*Over The Shoulder* (OTS) *elevation*). Cuando un programa se ejecuta en modo de elevación de privilegios, un cuadro de diálogo le advierte. Por lo tanto, por defecto, no hay la posibilidad de elevar privilegios a una aplicación sin el consentimiento explícito del usuario. Vamos a ver en esta sección que ahora es posible, en Windows, desactivar la petición de confirmación del proceso de elevación de privilegios.

Tenga en cuenta de todos modos que el servicio que permanece activo incluso cuando selecciona el parámetro menos seguro para esta función.

## 1. Las cuentas de usuario

Cada vez que abre una sesión de usuario, se le asigna un token de acceso (Token). Este token contiene la lista de privilegios de que usted dispone y enumera los recursos a los que usted accede o intenta acceder. Cada recurso disponible en el sistema posee una lista de control de acceso (DACL) que contiene la lista de usuarios y servicios que pueden acceder a ella, así como el nivel de privilegios que estos poseen:

Por defecto, los administradores reciben dos tokens:

- Un token de acceso como administrador.
- Un token de acceso como usuario estándar, que es el asignado de manera predeterminada.

Durante la elevación de un proceso, un usuario recibe los mismos privilegios que los del administrador; dicho de otro modo, obtiene el mismo token de acceso. El mecanismo que le permite pasar de una identidad a otra se llama *Admin Approval Mode* (AAM).

## 2. Los niveles de integridad

El Control de integridad (MIC o *Mandatory Integrity Control*) es otro mecanismo que apareció con Windows Vista. Se le controla mediante una lista de control de acceso ACE en la lista de control de acceso del sistema (SACL) de todo objeto "asegurable" (clave de Registro, archivos, procesos, etc.).

Cada proceso tiene un nivel de integridad pero también el proceso secundario que hereda del nivel de integridad del proceso que lo ha "engendrado". Estos niveles de integridad se llaman *Integrity access Levels* o IL.

Señalemos que el nivel de integridad está asociado a la SACL y no a la DACL.

Un proceso no puede interactuar con un nivel de integridad que posea privilegios más elevados. Las interfaces de programación de aplicaciones o API (*Application Programming Interface*) no tendrán éxito desde un proceso que tiene un nivel de integridad cuando se enfrente a un proceso de integridad más elevado. Esto es así para evitar los riesgos de ataques o intrusiones malintencionadas.

Las entradas del Registro pueden escribirse solo desde un proceso con un nivel alto de integridad. Por esto mismo, Internet Explorer (un proceso de integridad bajo) solo le permite escribir en áreas mínimas del Explorador o del Registro de Windows.

Los niveles de integridad son los siguientes:

- **High (alto)**: corresponde a los privilegios de sistema de administrador. Este nivel de privilegios le da permiso para escribir en el directorio \Archivos de programa y en la rama de Registro HKEY_LOCAL_MACHINE.
- **Medium (medio)**: corresponde al nivel de Usuario. Este nivel de privilegios le permite escribir en el directorio de usuario y en la rama de Registro HKEY_CURRENT_USER.
- **Low (bajo)**: este nivel solo le permite escribir en las zonas sin nivel de privilegios como la clave HKEY_CURRENT_USER\Software\LowRegistry o los directorios llamados LOW, que están presentes en el Explorador de Windows. Por otra parte, una función llamada "aislamiento de privilegios en interfaz de usuario" (*User Interface Privilege Isolation* o UIPI) se utiliza para reforzar este dispositivo con el fin de prevenir ataques de tipo "shatter".

Windows 8 añade a los niveles de integridad anteriores el nivel de aislamiento **AppContainer**. Este nivel de aislamiento se utiliza por defecto para la ejecución de las aplicaciones Windows Store.

## 3. La elevación de privilegios

Algunas operaciones no están adaptadas para utilizar listas de control de acceso. Imaginemos que un usuario tiene la necesidad de realizar una copia de seguridad de un grupo de archivos. Es mucho más fácil darle el permiso para realizar copias de seguridad independientemente

de los permisos NTFS asociados a los archivos, que modificar una a una la máscara de permisos de cada uno de los recursos a los que puede acceder. Se le puede dar una elevación de privilegios a un proceso en las siguientes circunstancias:

- Si el programa está en una plataforma de instalación como Windows Installer o Install Shield.
- Si el programa posee una entrada en la capa de compatibilidad de aplicaciones o en la base de datos de compatibilidad de aplicaciones.

En el primer caso, aparecerá una entrada en este árbol de Registro: HKEY_CURRENT_USER\Software\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store.

En el segundo caso, el ejecutable CompatAdmin.exe creará un archivo con la extensión *.sdb*.

- Si el archivo manifiesto de la aplicación contiene una solicitud de nivel de ejecución que indica que la aplicación requiere un nivel de privilegios elevados.

También puede elevar los privilegios seleccionando la casilla **Ejecutar como administrador** en el menú contextual de la aplicación o acceso directo. Veamos cómo hacerlo:

Con el botón derecho del ratón haga clic en uno de los programas existentes en el menú **Iniciar**.
Seleccione la opción **Ejecutar como administrador**.

Para automatizar este proceso, siga el siguiente procedimiento:

Haga clic con el botón derecho del ratón en el programa que aparece en la lista del menú **Iniciar** y, a continuación, haga clic en el submenú **Propiedades**.
Haga clic en la pestaña **Compatibilidad** y active la casilla **Ejecutar este programa como administrador**.

Si se realiza en un acceso directo el procedimiento es un poco diferente:

Haga clic con el botón derecho del ratón en el acceso directo y seleccione la opción **Propiedades**del menú contextual.
Haga clic en la pestaña **Acceso directo** y en el botón **Opciones avanzadas...**.
Active la casilla **Ejecutar como administrador**.

He aquí otra posibilidad:

En el cuadro de texto **Iniciar búsqueda**, situado encima del menú **Iniciar**, introduzca: **cmd**.
Haga clic con el botón derecho del ratón en la opción **cmd.exe** y en la opción **Ejecutar como administrador**.

A partir de aquí, todos los comandos que ejecute desde el símbolo del sistema se ejecutarán con permisos de administrador.

Existen otras dos situaciones que permiten una elevación de privilegios:

- Cuando un programa se ejecuta desde un proceso que ya ha recibido esta elevación de privilegios. Un buen ejemplo es el hecho de que muchas herramientas se deben lanzar desde una ventana de Símbolo de sistema en modo administrador.
- Cuando un programa se lanza desde el Administrador de tareas:

Desde el área de búsqueda a la derecha del menú **Inicio** introduzca: **taskmgr**.
Haga clic en el enlace **Más detalles**.
Haga clic en **Archivo** - **Ejecutar nueva tarea**.

Sepa que también puede hacer clic con el botón derecho del ratón en la barra de tareas y después en la opción correspondiente.

Active la casilla **Crear esta tarea con privilegios administrativos**.

En este caso, el Administrador de tareas inicia los procesos mediante la API CreateProcess y no CreateRestrictedProcess.

## 4. El proceso de virtualización

Un proceso iniciado por una cuenta de usuario estándar no puede escribir en la rama del Registro HKEY_LOCAL_MACHINE. Evidentemente, esta particularidad va a provocar problemas ya que, en muchas ocasiones, la aplicación no podrá funcionar con normalidad. Para salvar esta dificultad, Windows Vista creó un mecanismo llamado Virtualización. Cuando un proceso con privilegios bajos debe escribir en una zona protegida del Registro o del Explorador, los datos se transfieren de manera instantánea a una zona exclusiva del usuario. Estas zonas de "Usuario" toman prioridad frente a las zonas de "Equipo".

Cuando un proceso no puede escribir en la rama HKEY_LOCAL_MACHINE\ Software las escrituras que faltan se escriben en HKEY_CURRENT_USER\ Software\Classes\VirtualStore\MACHINE\Software.

El proceso de virtualización de los archivos realiza, él mismo, este tipo de sustitución: %perfil de usuario%\AppData\Local\VirtualStore\Program Files para %Archivos de programa%, %Perfil de usuario%\AppData\Local\Virtual Store\Windows para %Windir%, etc.

Los procesos son virtuales, excepto en los casos siguientes:

- Los que son lanzados con privilegios de administrador.
- El archivo ejecutable que contiene un manifiesto llamado requestedExecutionLevel.
- Los que conciernen a las operaciones que no se inician desde una sesión interactiva.

## 5. El control de cuentas de usuario

Cuando una aplicación no le pregunta automáticamente si desea lanzarla como administrador, es posible:

- Acceder al menú contextual del acceso directo o archivo ejecutable y hacer clic en la opción **Ejecutar como administrador**.
- Ejecutar la aplicación desde otra que haya sido ejecutada como administrador.

Cuando desde una cuenta de administrador usted abre una aplicación que necesita una elevación de privilegios, verá este tipo de cuadro de diálogo: "Windows necesita su permiso para continuar".

Desde una cuenta de usuario estándar, se le pedirá la contraseña de una cuenta con privilegios de administrador para poder continuar.

Los pasos son los siguientes:

- El sistema operativo analiza la aplicación.
- Si el editor es Microsoft, el sistema le indicará que Windows necesita su autorización para continuar (bandera azul).
- Si el editor no es Microsoft, pero la aplicación está firmada digitalmente, le indicará que Windows necesita su permiso para continuar (bandera gris).
- Si la aplicación no está firmada digitalmente, significa que un programa no identificado quiere acceder a su ordenador (bandera naranja).

Además, en la interfaz gráfica existe una serie de indicadores que señalan que una acción necesita una elevación de privilegios:

Haga clic en el reloj situado en el área de notificación.
Haga clic en el enlace **Cambiar la configuración de fecha y hora**.

El botón **Cambiar fecha y hora** está acompañado del escudo del Centro de seguridad.

Haga clic en ese botón.

Puede hacer clic en el botón **Mostrar detalles** para saber cuáles son los archivos de sistema que se ejecutarán.

## 6. Desactivación del Control de cuentas de usuario

Desde el **Panel de Control**, en la sección **Cuentas de usuario y protección infantil** - **Cuentas de usuario**, seleccione la opción **Cambiar configuración de Control de cuentas de usuario**.
Configure la funcionalidad desplazando el cursor a la opción **No notificarme nunca**. Haga clic en el botón **Aceptar** para validar el nuevo parámetro.

Puede usar también la utilidad de configuración del sistema:

En el cuadro de texto **Buscar** situado a la derechea del menú **Inicio**, introduzca: **msconfig**.
Haga clic en la pestaña **Herramientas**.
Seleccione **Cambie la configuración del Control de cuentas de usuario** y a continación haga clic en el botón **Iniciar**.
Atención, el control de cuentas de usuario no está totalmente desactivado, aunque seleccione la opción **No notificarme nunca**. No obstante, si desea desactivarlo totalmente, debe configurar el valor EnableLUA a 0 en la clave del registro: HKEY_LOCAL_MACHINE\SOFTWARE\Windows\CurrentVersion\Policies\System.
Tenga cuidado: la desactivación completa del control de cuentas de usuario tiene un impacto en el funcionamiento de aplicaciones de Windows Store, ya que en esos casos no se podrá ejecutar ninguna aplicación.

## 7. Configuración del control de cuentas de usuario

A continuación, examinaremos los diferentes parámetros que tiene a su disposición mediante el Editor de objetos de directiva de grupo, para lo que deberá abrir el siguiente árbol:

Configuración del equipo/Configuración de Windows/Configuración de seguridad/Directivas locales/Opciones de seguridad. Hemos señalado cada uno de los cambios correspondientes en el Registro, ya que el Editor de objetos de directiva de grupo no está instalado en muchas versiones de Windows.

## Control de cuenta de usuario: ejecutar las cuentas de administradores en modo de aprobación de administrador

Si esta directiva está deshabilitada, el tipo de usuario del modo de aprobación de administrador y todas las demás directivas UAC relacionadas también estarán deshabilitadas. En otras palabras, supone eliminar el Control de cuentas de usuario. Una vez desactivada la directiva, reinicie el ordenador.

- Si pulsa el botón **Aplicar**, un mensaje le indicará que la tarea se creará con permisos de administrador.
- Si abre el Centro de seguridad de Windows, un mensaje le avisará de que el control de cuentas de usuario se ha deshabilitado.

Esto corresponde a la siguiente manipulación del Registro de Windows:

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: EnableLUA
- Información del valor: 0.

## Control de cuenta de usuario: comportamiento del indicador de elevación para los administradores en modo de aprobación de administrador

Esta directiva le permite configurar el comportamiento del cuadro de diálogo cuando se lanza una solicitud de elevación de privilegios desde una cuenta con privilegios de administrador. Hay seis opciones:

- **Petición de credenciales en el escritorio seguro**: se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que introduzca su nombre de usuario y su contraseña.
- **Petición de confirmación en el escritorio seguro**: se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que seleccione Autorizar o Rechazar.
- **Petición de credenciales**: se le pedirá al administrador que introduzca un nombre de usuario y una contraseña directamente en el escritorio activo.
- **Petición de confirmación**: se le pedirá al administrador que seleccione Autorizar o Rechazar en el escritorio activo.
- **Petición de confirmación para los ejecutables no Windows**: para las aplicaciones externas, se le pedirá al administrador en el escritorio seguro (entorno de escritorio atenuado) que seleccione Autorizar o Rechazar.
- **Elevar sin preguntar**: no se pedirá ninguna confirmación al administrador.

En este último caso, el Control de cuentas de usuario estará activo, pero no aparecerá ningún cuadro de diálogo que interrumpa las tareas de mantenimiento.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

- Valor DWORD: ConsentPromptBehaviorAdmin

Los valores posibles son:

- 0: Elevar sin preguntar
- 1: Petición de credenciales en el escritorio seguro
- 2: Petición de confirmación en el escritorio seguro
- 3: Petición de credenciales
- 4: Petición de confirmación
- 5: Petición de confirmación para los ejecutables no Windows

### Control de cuenta de usuario: cambio a Escritorio seguro cuando se pida confirmación de elevación

Esta directiva determina si la solicitud de elevación se efectuará en el Escritorio de usuarios interactivos o en el Escritorio seguro. Este parámetro evita el efecto retardado cuando se realiza una petición de privilegios.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: PromptOnSecureDesktop

### Control de cuenta de usuario: utilizar el modo de aprobación de administrador para la cuenta de administrador integrado

Esta directiva determina el comportamiento del modo de aprobación de administrador para la cuenta de Administrador integrado. El Administrador integrado abrirá una sesión en modo de aprobación de administrador y deberá dar su consentimiento para todas las acciones que requieran una elevación de privilegios. Si esta directiva se encuentra deshabilitada, el Administrador podrá ejecutar todas las aplicaciones con privilegios de administración completos. Si utiliza a menudo la cuenta de Administrador, le resultará interesante utilizar esta directiva.

- Clave: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System
- Valor DWORD: FilterAdministratorToken

## Introducción a Windows Hello

Windows Hello es una nueva funcionalidad de Windows 10 cuyo objetivo es poner a disposición de los usuarios funciones de autentificación biométrica. Esta funcionalidad es el resultado de la implementación del framework FIDO 2.0.

El uso de contraseñas representa un riesgo, ya que no se respetan lo suficiente las buenas prácticas en cuanta la longitud, la duración y el almacenamiento de estas.

Windows Hello responde a las exigencias de los estándares de seguridad actuales.

Microsoft ha anunciado que esta funcionalidad soportará tres tipos de capturas biométricas diferentes. De hecho, puede abrir una sesión a través de dispositivos de lectura de huellas digitales, de reconocimiento facial o de reconocimiento de iris.

De todos modos tenga en cuenta disponer de un dispositivo compatible con Windows Hello para evitar cualquier problema de reconocimiento del mismo.

Para la lectura de huellas digitales, el sistema soporta la utilización de dispositivos existentes. Las restricciones de este tipo de dispositivos son limitadas. Por el contrario, para el reconocimiento facial hay que disponer de un lector de infrarrojos adaptado como la cámara RealSense 3D de Intel.

El radio de acción de Windows Hello no se limita solo a la autentificación en el equipo local, sino que también puede autentificar en aplicaciones y servicios web a través de Microsoft Passport.

Esta solución utiliza una autentificación de doble factor con la implementación de claves de cifrado asimétricas y la utilización de un código PIN asociado. Este modo de funcionamiento asegura que la información de identificación del usuario no se almacenará en un servidor distinto y es compatible con las especificaciones de la alianza FIDO. Esto garantiza la compatibilidad de la solución con algunos de los principales actores de la Web como Google, PayPal, MasterCard y Visa.

# Trucos de las cuentas de usuario

A continuación le explicamos dos trucos útiles.

## 1. Inicio de sesión automático en Windows

En el área de búsqueda introduzca: **netplwiz**.
Desmarque la casilla **Los usuarios deben escribir su nombre y contraseña para usar el equipo**.

Haga clic en **Aceptar**.
Si es preciso cambie el nombre de usuario.
Introduzca la contraseña y confírmela.
Haga clic de nuevo en **Aceptar**.

Vamos a explicar dos cosas que deberá tener en mente:

- Necesita una contraseña para evitar cualquier intento de conexión remota.
- Si su ordenador es accesible físicamente para otras personas, el conjunto de datos también lo es.

Este truco no es válido para Windows 10.

## 2. Restablecer una contraseña olvidada

Puede parecer curioso, pero esta herramienta funciona con una memoria USB externa, una tarjeta de memoria e incluso un iPod (si no tiene una unidad de disquete). A continuación, le explicamos cómo crear un disco de emergencia:

Desde el **Panel de control**, seleccione la sección **Cuentas de usuario y protección infantil** y abra la sección **Cuentas de usuario**.
Haga clic en el enlace **Crear un disco para restablecer contraseñas**.

Haga clic en **Siguiente**.
Seleccione el disco extraíble que desee y haga clic en **Siguiente**.

En algunas versiones de Windows la letra de la unidad no aparece, así que deberá encontrar la ubicación correcta probando.

Introduzca la contraseña y haga clic en **Siguiente**.

Se iniciará el proceso de creación del archivo.

Haga clic en los botones **Siguiente** y **Finalizar**.

El archivo creado llevará el nombre de: *userkey.psw*.

A continuación, lo podrá copiar en otro disco de emergencia.

### 3. Reparar una cuenta de administrador

Puede que accidentalmente haya dañado la cuenta, que haya cambiado a una cuenta de usuario estándar o que esta ya no aparezca en la pantalla de inicio de sesión. La única solución consiste en abrir una sesión utilizando la cuenta de Administrador y, desde esta, reparar la cuenta de usuario.

Una manera sencilla de hacerlo es utilizando las herramientas de WinRE y abriendo una ventana de Símbolo de sistema. A continuación, ejecute el Editor de Registro y cargue el subárbol SAM. Solo le quedará examinar este árbol hasta: \Domains\Users\000001F4. Edite un valor binario llamado F y modifique el dígito número 57a. Escriba el número 10 en lugar del 11.

## Los archivos de consola

El método consiste en crear una consola en la que pueda añadir complementos, como por ejemplo, el Editor de objetos de directiva de grupo.

### 1. Creación de un archivo de consola

Pulse las teclas [Windows] + R.
Introduzca el siguiente comando: **mmc**.
Haga clic en **Archivo** - **Guardar**.

Por defecto, el directorio de almacenamiento de archivos de consola es el siguiente: *Herramientas administrativas*.

Haga clic en **Ver** - **Personalizar...** para activar o desactivar algunos elementos de la consola.

Ahora veamos cómo añadir complementos.

### 2. Añadir un complemento

Haga clic en **Archivo** - **Agregar o quitar complemento...**.
Seleccione el complemento **Editor de objetos de directiva de grupo** y haga clic en el botón **Agregar**.

Se muestra el asistente de configuración de la herramienta de administración de las directivas de grupo. Haga clic en el botón **Examinar...**.

Puede elegir entre:

- Otro equipo.
- Un tipo de usuarios.

Haga clic en la pestaña **Usuarios**.

Tiene la posibilidad de:

- Elegir un usuario en particular.
- Elegir entre el grupo de administradores o no administradores.

Haga clic en **Aceptar**, **Finalizar** y **Aceptar**.

En nuestro ejemplo, hemos escogido el ordenador local y el grupo de los no administradores. Puede ver la etiqueta **Directiva Equipo local\No administradores**.

Abra esta rama.

Solo será accesible la **Configuración de usuario**.

Vuelva a realizar las mismas operaciones, pero seleccionando esta vez la opción **Equipo local**; tendrá acceso a la configuración del equipo y usuarios.

Puede guardar los cambios realizados en los dos archivos de consola y guardarlos con el nombre: **ConsolaEquipo** y **ConsolaNoAdministradores**

# El Editor de objetos de directiva de grupo

Este componente permite, en particular, la manipulación de un gran número de configuraciones del Registro. Veamos cómo utilizarlo.

## 1. Utilizar el Editor de objetos de directiva de grupo

Veamos un ejemplo sencillo:

Abra el siguiente árbol: **Directiva Equipo local/Configuración del Equipo/Plantillas administrativas/Componentes de Windows/Grabadora de sonidos**.
Abra la siguiente directiva: **No permitir que se ejecute la grabadora de sonidos**.

Seleccione el botón de acción **Habilitada** y haga clic en **Aceptar**.
Intente abrir la grabadora de sonidos mediante el siguiente comando: **soundrecorder.exe**.

Un mensaje le indicará que no es posible abrir este programa porque está protegido por una directiva de restricción de software.

Puede deshabilitar la directiva o eliminarla marcando el botón de acción **No configurada**.

Vuelva a realizar las mismas operaciones en el árbol **Equipo local/No-administradores**.

Podrá abrir la grabadora de sonidos, pero si intenta realizar esta misma acción desde una cuenta de usuario sin privilegios de administrador, le aparecerá el mismo mensaje de error que antes.

Desactive la directiva otra vez.

Abra el árbol **Directiva Equipo local/Configuración del usuario/Plantillas administrativas/Componentes de Windows/Grabadora de sonidos**.

Active la misma directiva e intente abrir la grabadora de sonidos.

Le aparecerá el mismo mensaje de error y lo mismo ocurrirá en una cuenta de usuario.

Así pues, podemos concluir que no puede aplicar directivas de Equipo que hagan distinción entre los usuarios que abran una sesión local. Es posible filtrar estas directivas de la siguiente manera:

Abra una de las ramas existentes.

Haga clic con el botón derecho del ratón sobre ella y luego sobre la opción de submenú **Ver** y **Opciones de filtro...**.

Puede:

- **Filtrar por el tipo de directiva a visualizar**: le permite listar únicamente las directivas habilitadas.
- **Filtrar por palabra clave**: permite listar solo las directivas que contienen una o varias palabras clave en el título, la descripción o el comentario asociado.
- **Filtrar por requisitos**: permite listar solo las directivas que se aplican con uno u otro sistema operativo o con una u otra aplicación.

En un principio, esta opción solo incumbe a las directivas que usted podrá modificar con la creación de archivos ADMX personalizados.

Los archivos ADMX son la versión de plantillas administrativas (*.adm) en vigor en Windows XP. Son archivos de plantillas en formato XML que contienen información y configuraciones del Registro pertenecientes a cada una de las directivas listadas en el Editor de objetos de directiva de grupo.

Sepa que las ramas del registro modificables son principalmente cuatro:

- HKEY_LOCAL_MACHINE\SOFTWARE\Policies
- HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies
- HKEY_CURRENT_USER\Software\Policies
- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies

Para desactivar el conjunto de directivas que ha configurado, haga clic con el botón derecho del ratón en el nodo de **Directiva Equipo local** y en el submenú **Propiedades**.

Seleccione una u otra, o incluso las dos opciones siguientes:

- **Deshabilitar los parámetros de configuración del equipo**.
- **Deshabilitar los parámetros de configuración de usuario**.

## 2. Aplicar una directiva a todos los usuarios del equipo

Abra una sesión con su cuenta.

Active las directivas en el árbol **Configuración de usuario**.
Cierre y abra de nuevo la sesión interactiva.
Compruebe que las directivas que ha configurado funcionan correctamente con su cuenta.

También puede comprobar su eficacia desde las demás cuentas de usuario.

Copie el archivo \Windows\System32\GroupPolicy\User\Registry.pol en su carpeta de usuario.
Abra otra vez el Editor de objetos de directiva de grupo y deshabilite todas las directivas que había activado previamente.

Puede resultar más fácil activar el filtro que permite visualizar únicamente las directivas configuradas.

Cierre el Editor de objetos de directiva de grupo.
Copie en su directorio de origen el archivo que guardó y confirme que desea reemplazar el archivo existente.
Cierre y vuelva a abrir la sesión de usuario.

Podrá comprobar que las directivas habilitadas ya no se aplican a su cuenta.

Abra una sesión con las otras cuentas de usuario para comprobar que las directivas funcionan bien en ellas.

## 3. Restablecer las directivas locales originales

Elimine el archivo *Registry.pol*.
Abra el Editor de objetos de directivas de grupo y configure todas las estrategias en el modo **No configurado**.
Cierre y vuelva a abrir las sesiones de usuarios.

Todas las directivas se habrán deshabilitado.

## 4. Mostrar las directivas resultantes

Esta herramienta le permite ver rápidamente las directivas que pueden resultar de un objeto de directiva de grupo o GPO (*Group Policy Object*) propio de un dominio, red local, grupo de usuarios o de un usuario y le ayudará a detectar posibles problemas o a planificar nuevas configuraciones.

Agregue el siguiente componente de software: **Conjunto resultante de directivas**.
Haga clic con el botón derecho del ratón en el componente y, a continuación, en la opción del submenú **Generar datos RSoP**.
Pulse dos veces en **Siguiente**.

Puede elegir entre:

- **Mostrar las directivas en este equipo u otro equipo**.
- **Mostrar solo la configuración de la directiva del usuario**.

En este último caso, seleccione el botón de acción **Usuario actual** o seleccione uno de los usuarios de la lista de debajo.

Acepte lo demás.

Podrá ver las directivas que se aplican al usuario seleccionado.

CAPÍTULO 5

# Mantenimiento del Sistema

# La interfaz de usuario de Windows 10

La interfaz de usuario, ampliamente modificada en Windows 8, ha sufrido en esta última versión de Windows nuevas y numerosas adaptaciones. Se ha restaurado el menú Inicio y, en un ordenador de sobremesa, es el modo de acceso a las aplicaciones definido por defecto. El escritorio de inicio estilo ”Modern UI” sigue estando accesible si lo desea, a través de la configuración del sistema operativo. En un dispositivo de tipo tableta o smartphone, se da prioridad al escritorio de inicio.

La gran cantidad de iconos que se pueden asociar a los accesos directos puede llegar a hacer difícil la visibilidad de la página de inicio, y solo algunas aplicaciones están directamente disponibles desde ella.

Para visualizar todas las aplicaciones disponibles desde la interfaz de usuario de Windows 10:

Desde el escritorio Windows haga clic en el menú Inicio.
Haga clic en el enlace **Todas las aplicaciones**.

## Gestión de la configuración del ordenador

Observe que, en el menú Inicio, dispone de un acceso directo a la pantalla de configuración del ordenador. Esta pantalla se ha ampliado mucho respecto a los elementos de configuración presentes en Windows 8. Por ejemplo, puede modificar la configuración del sistema como las aplicaciones utilizadas por defecto o la configuración de asociación de tipos de fichero. También en esta pantalla, en la sección **Personalización**, puede configurar todos los elementos relacionados con colores, con la visualización y con el comportamiento de la pantalla de bloqueo.

Para mostrar funcionalidades de la pantalla de configuración del ordenador, también puede utilizar la combinación de teclas [Windows] + I, incluso si se puede acceder a ella a través del menú Inicio.

También puede acceder al Panel de control desde el menú Inicio - **Todas las aplicaciones** - **Sistema de Windows**.

## Gestión personalizada de los iconos

Es posible configurar la apariencia del menú Inicio así como la organización de los iconos a través de la creación de grupos. Para ello, simplemente desplace hacia abajo el icono que desea insertar en un nuevo grupo. Sobre el icono desplazado, haga clic en el icono que representa dos barras paralelas y ponga nombre a su nuevo grupo.

## Gestión de los escritorios virtuales - task view

Es una las grandes novedades de la interfaz de Windows 10. Gracias a esta funcionalidad puede crear diferentes escritorios o entornos para organizar su espacio de trabajo de manera

más flexible y eficiente. Esta funcionalidad existía desde hace muchos años en los sistemas Linux.

Observe que la personalización de los escritorios no se conserva si apaga y reinicia su ordenador.

El icono **Task view** está situado en la barra de tareas a la derecha del área de búsqueda. Haga clic en este icono; en la parte inferior derecha de la pantalla puede ver un botón con el símbolo **+** para crear un nuevo escritorio.

También puede utilizar la combinación de teclas [Windows][Ctrl][D] para crear directamente un nuevo escritorio o la combinación de teclas [Windows][Ctrl][F4] para cerrar el escritorio en el que se encuentra.

Puede utilizar la teclas [Windows][Ctrl][Cursor izquierdo] o [Windows][Ctrl][Cursor derecho] para ir de un escritorio a otro.

## El Explorador de Windows

Como en Windows 8, también en Windows 10 tenemos a nuestra disposición el explorador de Windows. Se accede a los comandos del explorador a través de una cinta como en Microsoft Office.

En Windows 8, el explorador está disponible desde el escritorio. Si la cinta no aparece en el explorador, utilice la combinación de teclas [Ctrl][F1]. Encontrará en los diferentes menús de la cinta las funciones clásicas del explorador de Windows.

En Windows 10, podemos acceder al Explorador de Windows de diferentes maneras:

- Haga clic con el botón secundario del ratón en el botón **Inicio** y luego seleccione la opción **Explorador de archivos**.
- Utilice la combinación de teclas [Windows] + E.
- Haga clic en el botón **Inicio** y a continuación seleccione el enlace **Todas las aplicaciones**. En la lista de aplicaciones, seleccione la aplicación **Documentos**.

Existen dos operaciones que debe hacer obligatoriamente antes de poder resolver un problema de software en el ordenador.

- Activar la opción de mostrar los archivos y carpetas ocultos.
- Activar la opción de mostrar las extensiones de archivo para tipos de archivo conocido.

Pulse las teclas [Ctrl][F1] para ver la cinta del Explorador de archivos de Windows.

Haga clic en el menú **Vista** y a continuación en el botón **Opciones**.

Seleccione la opción **Ver**.

Si es preciso, haga doble clic en la rama **Archivos y carpetas ocultos**.

Seleccione el botón de acción **Mostrar todos los archivos y carpetas ocultos**.

Un poco más abajo, desmarque la casilla **Ocultar archivos protegidos del sistema operativo (recomendado)**.

No existe ninguna diferencia entre estas dos opciones, excepto que se anulan mutuamente.

Acepte el mensaje de aviso que aparece y pulse en **Aplicar**.

De la misma manera, desactive la casilla **Ocultar las extensiones de archivo para tipos de archivo conocido**.

Si no lleva a cabo la primera manipulación antes de cualquier intento de reparación, no podrá encontrar en el Explorador de Windows los archivos que necesitará modificar.

El segundo truco le permitirá cambiar más fácilmente el nombre de los archivos o su extensión.

## Buscar archivos y carpetas

Windows 10 utiliza el motor Windows Search para la búsqueda y la indexación de ficheros. Windows Search arranca como servicio y es accesible a través de la consola de servicios Windows. Los procesos que utiliza Windows Search son los siguientes: **SearchIndexer.exe**, **SearchFilterHost.exe** y **SearchProtocolHost.exe**.

La indexación de ficheros y carpetas es necesaria si desea resultados rápidos y precisos en sus búsquedas. En Windows 10, los elementos indexados por defecto son las bibliotecas, el correo electrónico y los ficheros sin conexión.

Para abrir las opciones de indexación, en la barra de tareas, teclee el texto **opciones de indización**en la zona de búsqueda y pulse la tecla [Entrar].

Haga clic en el botón **Modificar** si desea añadir nuevas carpetas a los elementos indexados por defecto.
Haga clic en el botón **Opciones avanzadas** para visualizar los tipos de ficheros indexados.

Para lanzar una búsqueda en el disco de sistema, en el Explorador de Windows, seleccione el disco de sistema **C:**. En la zona de búsqueda, introduzca los elementos a buscar. La búsqueda se inicia automáticamente. Puede ver el resultado de su búsqueda en el panel central.

Observe la aparición de menús específicos para la búsqueda en la cinta del Explorador de Windows. Por ejemplo, puede afinar su resultado seleccionando filtros de búsqueda adicionales. También puede guardar su búsqueda en un fichero *.search-ms.

Para efectuar una búsqueda en un conjunto de carpetas distintas, debe crear una biblioteca. Una biblioteca representa una carpeta virtual vinculada a una o varias ubicaciones.

## Cambiar la extensión de un archivo

Ya hemos visto cómo debe activar la opción para mostrar las extensiones de archivo para tipos de archivo conocido. Si desea guardar un archivo con otra extensión que la que tiene asignada por defecto, solo tendrá que seleccionar en la lista desplegable **Archivos de tipo** esta opción: **Todos los archivos**. De este modo, podrá añadir una extensión adicional (*.bak*, *.bck*, etc.) o cambiar la extensión existente y puede hacerlo con el fin, por ejemplo, de desactivar un archivo ejecutable. El sistema no lo reconocerá como un tipo de archivo válido y simplemente tendrá que reemplazar la extensión *.exe* por *.bak* o cualquier otra expresión de carácter mnemotécnico.

Por ejemplo, la siguiente búsqueda permite visualizar los ficheros con la extensión *.log que contienen la palabra clave setup.

## Solucionar problemas del motor de búsqueda

En caso de que las consultas de búsqueda se ralenticen mucho, una de las principales soluciones es eliminar y reconstruir el índice.

Para ello, en las **Opciones de indización** del motor de búsqueda, haga clic en **Opciones avanzadas**. Dentro de la pestaña **Configuración del índice**, haga clic en **Reconstruir**. Finalmente, haga clic en **Aceptar** para eliminar y reconstruir el índice.

Otra opción para optimizar es excluir la base de datos local utilizada por el motor de búsqueda del antivirus en tiempo real.

Esta base de datos local es una base de datos de tipo EDB (*Extensible Database File*) que está en la carpeta C:\Program Data\Microsoft\Search\Data\Applications\Windows.

Observe que la carpeta ProgramData está oculta por defecto.

Les aconsejo excluir la carpeta entera del antivirus.

## Las tareas de mantenimiento habituales

En este apartado vamos a ver dos herramientas que nos permiten liberar espacio del disco duro y optimizar el lugar que ocupan los datos.

### 1. Limpieza del disco duro

Se puede acceder a esta utilidad desde las herramientas administrativas del panel de control o desde la cinta del Explorador de Windows en el menú **Administrar** cuando selecciona el disco C:\. Se trata de una etapa indispensable antes de realizar la desfragmentación de un disco. Su manejo no tiene ninguna dificultad.

También podemos encontrarnos con este tipo de error: "Cleanmgr.exe ha encontrado un problema y debe cerrarse".

En el Explorador de Windows, abra la siguiente ruta: Usuarios\Nombre_Usuario\AppData\local\Temp.
Con la ayuda del método abreviado de teclado [Ctrl]+E, seleccione todos los archivos y carpetas presentes y elimínelos.
Elimine también todos los archivos temporales de Internet Explorer haciendo clic en **Herramientas - Opciones de Internet** y en el botón **Eliminar archivos...**.

La herramienta **Liberador de espacio en disco** calculará el espacio que es posible liberar en el disco y mostrará los archivos que puede eliminar.

## 2. Desfragmentación del disco duro

En Windows 10 y Windows 8, la interfaz está pensada para que nada (o casi nada) sea visible. El proceso de desfragmentación se activa automáticamente cada cierto tiempo (cuando las tareas programadas detectan que el sistema está inactivo), ya mantiene el equipo dentro de un nivel de fragmentación aceptable.

Para entender esto, siga los siguientes pasos:

En el Panel de control, haga clic en el enlace **Sistema y seguridad**. En las **Herramientas administrativas** haga clic en el **Programador de tareas**.
Abra las ramas de **Biblioteca del programador de tareas - Microsoft - Windows** y **Defrag**. La tarea ScheduleDefrag lanza cada semana la desfragmentación de los discos de su equipo.

El proceso de desfragmentación utiliza los recursos del disco y del procesador en modo "Prioridad Baja". Gracias a ello, el proceso de desfragmentación no le molestará mientras realiza su trabajo.

Por último, sepa que este programa desfragmenta todos los volúmenes existentes en el disco duro.

Existe otra manera de iniciar el programa:

Ejecute el Símbolo del sistema como administrador.

De lo contrario, aparecerá este mensaje de error: "Este programa se necesita ejecutar con permisos administrativos. Use un Símbolo del sistema de administrador y después ejecute el programa de nuevo".

Introduzca el comando **defrag** para ver una lista de todos los modificadores válidos.

Ejecute por ejemplo este comando: **defrag c: /A /U**.

Al cabo de unos segundos podrá ver el resultado del análisis y del proceso de desfragmentación propiamente dicho.

## 3. La Herramienta de configuración de sistema

En Windows, la Herramienta de configuración de sistema se puede definir como un tipo de navaja suiza que ofrece un acceso rápido a una gran variedad de herramientas e información. Puede acceder a ella ejecutando el siguiente comando desde el símbolo del sistema: **msconfig**.

La pestaña **Servicios** le permite visualizar el conjunto de servicios instalados en el sistema. Bajo ninguna circunstancia debe configurar los servicios de Windows desde aquí, sino que debe hacerlo siempre desde el Administrador de servicios (accesible desde el comando "services.msc"). Sin embargo, si marca la casilla **Ocultar todos los servicios de Microsoft**, podrá ver de manera rápida los servicios que terceras aplicaciones han instalado.

A partir de ahora, nada le impedirá aligerar el proceso de inicio del sistema desmarcando las casillas situadas al lado de los nombres de servicios que no quiere que se inicien automáticamente cada vez que abre sesión.

Desde Windows 8, las funciones de la pestaña **Arranque** no están disponibles en esta herramienta aunque la pestaña sigue existiendo. Puede encontrar estas funciones en el Administrador de tareas. Vaya al capítulo relativo a las herramientas del sistema de este libro para ampliar detalles sobre esta funcionalidad.

La pestaña **Herramientas** permite acceder rápidamente a las principales funcionalidades de configuración del ordenador. También se puede visualizar el comando que se ejecuta para cada utilidad.

La pestaña **Arranque** permite acceder a la configuración del fichero Boot. Sobretodo puede configurar las opciones de arranque avanzadas de este fichero, como el límite de recursos de CPU y memoria que el sistema puede utilizar. Si activa la opción **Arranque a prueba de errores**, el próximo arranque será en modo seguro. Active la opción **Red** si desea poder conectarse a la misma.

Observará que la pestaña **General** permite elegir entre un inicio selectivo o un inicio con diagnósticos. Esta última opción corresponde al inicio en modo seguro.

# Administración de procesos

Resulta indispensable comprender el funcionamiento de los procesos antes de poder resolver gran número de los problemas que se presentan.

## 1. ¿Qué es un proceso?

A menudo, los usuarios ejecutan varios programas simultáneamente, pero debe saber que un procesador solo puede ejecutar un proceso a la vez. Así pues, los programas se administran de una manera secuencial y discontinua. Se puede definir la prioridad de un proceso como la atención que el procesador dirige a un programa determinado. Es una manera de decir que el procesador solo ve el proceso correspondiente de la aplicación. Los subprocesos son un tipo de procesos más ligeros que se utilizan para efectuar tareas en paralelo.

Para que lo comprenda mejor, siga los siguientes pasos:

Acceda al Administrador de tareas de Windows haciendo clic con el botón secundario del ratón en la barra de tareas y seleccionando la opción correspondiente.
Vaya a la pestaña **Procesos**.

Para determinar el proceso asociado a una aplicación, haga clic derecho en el proceso de la aplicación y, a continuación, haga clic en el comando **Ir a detalles**.

El proceso correspondiente aparecerá automáticamente resaltado. Los demás nombres de procesos están presentes en la lista pero se encargan, por su parte, de otras funciones del sistema (Explorador de archivos, acceso telefónico a redes, etc.). Algunos programas como los servicios Windows son ejecutados por un proceso host. Por ello puede visualizar diversas instancias del proceso Svchost.exe, por ejemplo.

## 2. El proceso Svchost.exe

Los procesos llamados Svchost.exe ("Service Host Process") son procesos genéricos que permiten lanzar aplicaciones cuyo funcionamiento recae en las bibliotecas de vínculo dinámico (DLL). Todos ellos están listados en esta rama del Registro: HKEY_LOCAL_MACHINE\Software\Microsoft\WindowsNT\ CurrentVersion\Svchost.

Cada valor de cadenas múltiples contiene una lista de servicios extraída de la clave HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ <Nombre abreviado de este servicio>.

Para tener una idea más precisa siga estas instrucciones:

Ejecute el Administrador de tareas y haga clic en la pestaña **Detalles**.
Haga clic en el encabezado de columna **Nombre de usuario** para clasificar los procesos en función de la entidad que los ha lanzado.

Podemos aprovechar nuestra ventaja un poco más:

En el Administrador de tareas, haga clic con el botón derecho colocando el ratón en la barra de los encabezados de columna. Haga clic en el enlace **Seleccionar columnas**.
Seleccione la casilla **Identificador de proceso (PID)** y haga clic en **Aceptar**.

Aparecerá el PID de cada uno de los procesos de la lista.

Abra una ventana de Símbolo del sistema.
Sabiendo que el PID de un proceso Svchost.exe es: 1000, teclee el comando: **tasklist /svc /fi "pid eq 1000"**.

Frente al nombre de la imagen aparecerán el o los servicios dependientes.

# Los servicios de Windows

En la zona de búsqueda del menú **Iniciar** o desde el símbolo de sistema, introduzca: **services.msc**. Seleccione este programa para acceder al Administrador de servicios.

Un servicio es una capa de software del sistema operativo o de una aplicación que se ejecuta en segundo plano y que permite el funcionamiento de los programas, algunos controladores y de los componentes de Windows.

Haga doble clic en un servicio llamado "Examinador de equipos". El nombre del servicio es: "Browser". Este es el nombre real del servicio que le permitirá identificar si realiza tareas de mantenimiento desde el Símbolo del sistema, la consola de recuperación o desde las herramientas de WinRE.

La propiedad **Estado del servicio** indica si el servicio está iniciado en ese momento. Un servicio está detenido si no aparece ningún mensaje en esta columna, al lado del nombre del mismo. La lista **Tipo de inicio** muestra en Windows Vista una de estas cuatro posibilidades:

- **Automático**: el servicio se activa de manera automática al iniciar el sistema. Si este servicio no es necesario, se detendrá.
- **Automático (inicio diferido)**: esta opción es similar a la anterior con la diferencia de que no se iniciará al mismo tiempo que el sistema, sino después de la aparición del

Escritorio de Windows. Esto permite que no se utilice toda la memoria disponible al iniciar el sistema.

- **Manual**: el servicio se iniciará o detendrá a petición del usuario.

El estado del servicio se puede determinar de dos modos: **Iniciado** o **Detenido**. Por supuesto, es posible iniciar un servicio haciendo clic en el botón **Iniciar**.

Ahora haga clic en la pestaña **Iniciar sesión**.

Se indicará si el servicio está habilitado o deshabilitado en el perfil de hardware en el que usted ha iniciado. Un perfil de hardware muestra la lista de componentes que usted ha elegido activar para una configuración determinada.

Por último, haga clic en la pestaña **Dependencias**.

Podrá ver la serie de dependencias que existen entre los diferentes servicios. Por ejemplo, no le será posible iniciar un servicio si los servicios de los que depende no se ejecutan. Una equivalencia estricta existe en el Registro:

## 1. Los servicios de Windows 8

Hemos realizado una lista con los principales servicios existentes en Windows 8 y en ellos siempre aparece:

- El nombre completo del servicio.
- El nombre abreviado del servicio.
- El proceso que permite su ejecución.
- Una descripción rápida de su función en el sistema.
- Las consecuencias posibles si decide desactivarlo.

Existen diferentes razones para querer desactivar un servicio de Windows:

- Cuantos menos servicios se ejecuten al arrancar el equipo, menor será el tiempo de reacción de este.
- Por cuestiones de seguridad.
- Algunos administradores no dudan en desactivar algunos servicios para impedir que los usuarios puedan acceder a las funciones correspondientes.

Así pues, podrá optar por:

- Configurar en modo Manual un servicio establecido en modo de Inicio automático o Automático (inicio retrasado).
- Desactivar un servicio configurado como Manual, Automático o Automático (inicio retrasado).

¡Actúe siempre con prudencia!

**Adquisición de imágenes de Windows (WIA) - stisvc - svchost.exe**

Ofrece servicios de adquisición de imágenes para escáneres y cámaras. Muchos dispositivos y aplicaciones no funcionarán si desactiva este servicio (por ejemplo, Windows Movie Maker).

**Agente de Protección de acceso a redes - napagent - svchost.exe**

Habilita la funcionalidad de Protección de acceso a redes NAP (*Network Access Protection*) en equipos cliente. La desactivación de este servicio supondría un problema en términos de seguridad.

**Agente de directiva IPsec - PolicyAgent - svchost.exe**

Se encarga de la integridad del protocolo de seguridad IPsec. Si lo desactiva no será posible conectarse si la red ha sido configurada para solicitar un certificado IPsec. Además, no será posible la administración remota del firewall de conexión a Internet integrado en Windows. Si utiliza un módem o router, puede desactivar este servicio.

**Energía - Power - svchost.exe**

Este servicio administra la directiva de energía y la entrega de notificaciones de dicha directiva. La desactivación de este servicio impide el funcionamiento del sistema.

**Llamada a procedimiento remoto (RPC) - RpcSs - svchost.exe**

Sirve como asignador de extremos y administrador de control de servicios COM. Si deshabilita este servicio ya no podrá iniciar Windows. ¡No lo haga bajo ninguna circunstancia!

**Aplicación del sistema COM+ - COMSysApp - dllhost.exe**

Administra la configuración y el seguimiento de los componentes del Modelo de objetos componentes (COM+). ¡Este servicio no se debe desactivar! De lo contrario, un número importante de servicios, como el RPC, no funcionarán.

**Aplicación auxiliar IP - iphlpsvc - svchost.exe**

Proporciona conectividad IPv6 automática en una red IPv4. Lo importante que debe tener en cuenta es que la mayoría de las redes no utiliza una dirección en IPv6 y, por lo tanto, este servicio se puede desactivar sin temer posibles "efectos secundarios".

**Aplicación auxiliar de NetBIOS sobre TCP/IP - lmhosts - svchost.exe**

Se ocupa del servicio NetBIOS sobre TCP/IP y la resolución de los nombres NetBIOS. Este servicio es indispensable en redes pequeñas donde se necesitan configuraciones NetBIOS sobre TCP/IP. Si ha instalado uno o varios servidores que aseguren esta función, puede desactivar este servicio.

**Asistente de Conectividad de red - NcaSvc - svchost.exe**

Notifica el estado de la funcionalidad DirectAccess. Este servicio se puede desactivar si no utiliza esta funcionalidad.

**Asistente de Conexión con una cuenta Microsoft - wlidsvc - svchost.exe**

Servicio utilizado por la conexión al puesto de trabajo a partir de los servicios de cuenta Microsoft. Puede desactivar este servicio si utiliza cuentas de usuario locales.

**Audio de Windows - AudioSrv - svchost.exe**

Administra los dispositivos de audio. Si desactiva este servicio, los dispositivos multimedia dejarán de funcionar.

**Branchcache - PeerDistSvc - svchost.exe**

Administra la funcionalidad de almacenamiento en caché de contenido de la red cuando está activa. Este servicio se puede desactivar si no utiliza esta funcionalidad.

**Tarjeta inteligente - ScardSvr - svchost.exe**

Administra el acceso a tarjetas inteligentes leídas por el equipo. En principio, puede desactivar este servicio excepto si utiliza este tipo de dispositivos.

**Adaptador de rendimiento de WMI - wmiApSrv - WmiApSrv.exe**

Proporciona información sobre la biblioteca de rendimiento de proveedores Hperf y WMI. Si lo desactiva dejarán de compilarse las estadísticas de rendimiento de su ordenador.

**Centro de seguridad - wscsvc - svchost.exe**

Analiza las configuraciones de seguridad y del sistema. Si desactiva este servicio, los mensajes del Centro de seguridad dejarán de ser visibles, pero esto no afectará al funcionamiento de los servicios correspondientes.

**Instantáneas de volumen - VSS - vssvc.exe**

Administra e implementa Instantáneas de volumen usadas para copias de seguridad y otros propósitos. Si lo desactiva ya no podrá utilizar esta serie de funciones.

**Cliente de directiva de grupo - gpsvc - svchost.exe**

Este servicio es responsable de aplicar en el equipo y los usuarios la configuración establecida por los administradores, a través del componente Directiva de grupo. No es posible desactivar este servicio, independientemente de la versión de Windows instalada.

**Cliente de seguimiento de vínculos distribuidos - TrkWks - svchost.exe**

Mantiene los vínculos entre archivos NTFS dentro de un equipo o entre equipos de una red. Los usuarios no podrán seguir los enlaces desde el ordenador en el que este servicio esté desactivado. Pongamos un ejemplo: hemos creado un archivo en el ordenador A con un acceso directo a este en el ordenador B. Si movemos el archivo en el ordenador A, seguirá estando accesible desde el ordenador B. Sin embargo, este tipo de servicio no se utiliza en una red pequeña.

**Cliente DNS - Dnscache - svchost.exe**

Almacena en caché los nombres de Sistema de nombres de dominio (DNS) y registra el nombre completo del equipo. Si este servicio se detiene, el equipo no podrá resolver los nombres DNS en direcciones IP. En un principio, resulta impensable desactivar este servicio.

**Cliente DHCP - Dhcp - svchost.exe**

Registra y actualiza las direcciones IP y los registros DNS en este equipo. Si se detiene este servicio, el equipo no recibirá direcciones IP dinámicas; por lo tanto, puede desactivar este servicio si utiliza una dirección IP fija.

**Recopilador de eventos de Windows - Wecsvc - svchost.exe**

Este servicio administra las suscripciones persistentes a eventos desde orígenes remotos que admiten el protocolo WS-Management. No hemos encontrado una utilidad directa para este servicio y, por lo tanto, puede desactivarse.

**Configuración automática de redes cableadas - dot3svc - svchost.exe**

Este servicio realiza la autenticación IEEE 802.1X en interfaces Ethernet. Si lo desactiva, el proceso de autenticación dejará de funcionar. En pocas palabras, este servicio es necesario si se conecta a una red inalámbrica.

**Configuración automática de dispositivos conectados a la red - NedAutoSetup - svchost.exe**

Instala automáticamente los dispositivos de red calificados. Desactive este servicio si desea suspender la instalación automática de dispositivos de red. De todos modos puede instalar manualmente estos dispositivos.

**Configuración de Escritorio remoto - SessionEnv - svchost.exe**

Este servicio se encarga del buen funcionamiento del Escritorio Remoto y de los servicios Terminal Server. Si no utiliza estas herramientas, puede desactivarlo.

**Reconocimiento de ubicación de red - NlaSvc - svchost.exe**

Recopila y almacena la información de configuración de red. Si deshabilita este servicio, la conexión compartida a Internet o el firewall de Windows no funcionarán.

**Conexiones de red - Netman - svchost.exe**

Administra los objetos presentes en la carpeta *Conexiones de red y acceso telefónico*. Si lo desactiva, será imposible configurar una red. Del mismo modo, no se mostrarán las notificaciones de red presentes en la barra de tareas.

**Control parental - WPCSVC - svchost.exe**

Este servicio habilita el control parental de Windows en el sistema. Si no utiliza esta funcionalidad, puede desactivar el servicio.

**Coordinador de transacciones distribuidas - MSDTC - msdtc.exe**

Coordina las transacciones que se extienden a varios administradores de recursos, como bases de datos, colas de mensajes y sistemas de archivos. La desactivación de este servicio afectaría a los servidores web y SQL. Dado que este tipo de funciones no se utilizan a menudo, puede desactivarlo con total tranquilidad. Tenga en cuenta también que este servicio se requerirá en un futuro próximo para algunas aplicaciones .NET.

**Detección SDDP - SSDPSRV - svchost.exe**

Detecta dispositivos que usan el protocolo de detección SSDP. Si desactiva el servicio, su equipo será incapaz de detectar los dispositivos UPnP presentes en la red.

**Detección de servicios interactivos - UI0Detect - UI0Detect.exe**

Habilita la notificación de entradas de usuario sobre los servicios interactivos. Si desactiva este servicio, no tendrá acceso a los cuadros de diálogo iniciados por los servicios interactivos. No hemos constatado ningún problema aparente al desactivar este servicio y la documentación de Microsoft respecto a este tema tampoco aporta nada.

**Detección de hardware shell - ShellHwDetection - svchost.exe**

Proporciona notificaciones sobre eventos de hardware AutoPlay. Es una manera cualquiera de desactivar todas las notificaciones automáticas. Sin embargo, puede causar molestias: en la ventana de Equipo no verá las unidades y cuando acceda a estas, utilizando el Explorador de Windows, en las propiedades de cualquiera de las unidades, la pestaña de Ejecución automática no aparecerá.

**Diagnostics Tracking Service - DiagTrack - svchost.exe**

Servicio de recopilación de datos cuando el sistema encuentra errores funcionales. Este servicio no es crítico y se puede desactivar.

**Disco virtual - vds - vds.exe**

Proporciona servicios de administración para discos, volúmenes, sistemas de archivos y objetos. Si desactiva este servicio, el componente de software "Administración de discos" dejará de ser accesible.

**Carpetas de trabajo - workfolderssvc - svchost.exe**

Servicio de sincronización de archivos para la funcionalidad Carpetas de trabajo. Esta funcionalidad requiere la implementación del servicio Carpetas de trabajo en el lado servidor. Este servicio se puede desactivar si no se utiliza esta funcionalidad.

**Escuchador Grupo en el hogar - HomeGroupListener - svchost.exe**

Administra la configuración del equipo añadido a un grupo de hogar. Este servicio se puede desactivar excepto si utiliza la funcionalidad de grupo en el hogar.

**Eventos de adquisición de imágenes fijas - WiaRpc - svchost.exe**

Asegura la comunicación entre las aplicaciones y los dispositivos de captura de imagen para edición y uso. Si desactiva este servicio, no podrá utilizar las funciones de captura de imágenes desde un dispositivo externo.

**Experiencia de calidad de audio y video de Windows (aWave) - QWAVE - svchost.exe**

qWave es una plataforma de red para aplicaciones multimedia. Si la desactiva, algunas aplicaciones de trasmisión por secuencias dejarán de funcionar.

**Experiencia con aplicaciones - AeLookupSvc - svchost.exe**

Procesa las solicitudes de la caché de compatibilidad de aplicación para aplicaciones en el momento en que estas se inician. Este servicio es necesario para el inicio de algunas aplicaciones no diseñadas para Windows 8.

**Examinador de equipos - browser - svchost.exe**

Mantiene una lista actualizada de equipos en la red. Este servicio debe estar habilitado si comparte recursos con otros equipos en la red.

**Extensiones y notificaciones de impresoras - PrintNotify - svchost.exe**

Gestiona las notificaciones relacionadas con las impresoras y servidores de impresión. No desactive este servicio si utiliza funciones de impresión de su sistema operativo.

**Archivos sin conexión - CscService - svchost.exe**

Realiza actividades de mantenimiento en la caché de Archivos sin conexión, de modo que si lo desactiva los archivos sin conexión no estarán accesibles.

**Proveedor de instantáneas de software de Microsoft - swprv - svchost.exe**

Administra instantáneas de software de volúmenes. En principio, este servicio se puede dejar en modo Manual si utiliza las funciones de copia de seguridad integradas en Windows 8. Tenga en cuenta que este servicio es necesario para la ejecución de terceras aplicaciones que permiten crear imágenes de copia del disco.

**Proveedor de Grupo Hogar - HomeGroupProvider - svchost.exe**

Este servicio realiza las tareas de red asociadas a la configuración y al mantenimiento de grupos en el hogar. Si lo desactiva, el ordenador no podrá detectar otros grupos de hogar. Microsoft recomienda dejar este servicio en funcionamiento.

**Generador de puntos de terminación del servicio Audio Windows - AudioEndpointBuilder - svchost.exe**

Este servicio es responsable de la administración del hardware de audio por el servicio Audio Windows. Este servicio debe permanecer activo si utiliza las funcionalidades de audio del sistema operativo.

**Administrador remoto de Windows (WS-Management) - WinRM - svchost.exe**

Implementa el protocolo WS-Management para la administración remota. En caso de desactivación, algunas funciones para la conexión remota no funcionarán.

**Administración de aplicaciones - AppMgmt - svchost.exe**

Procesa las solicitudes de instalación, eliminación y enumeración para el software implementado mediante la directiva de grupo. Si no despliega aplicaciones por medio de directivas de grupo, puede desactivar este servicio.

**Administración de certificados y claves de mantenimiento - hkmsvc - svchost.exe**

Proporciona servicios de administración de claves y de certificados X.509 para el Agente de Protección de acceso a redes (NAPAgent). Si deshabilita este servicio, las aplicaciones que utilizan este estándar de cifrado no podrán funcionar. En principio, este tipo de programas no son en absoluto comunes.

**Administrador de identidad de red homologada - p2pimsvc - svchost.exe**

Este servicio es utilizado sobre todo por el protocolo PNRP. Si lo desactiva, puede que la funcionalidad de grupo del hogar no funcione.

**Administrador de credenciales - VaultSvc - lsass.exe**

El administrador de credenciales utiliza este servicio. Ofrece un servicio de almacenamiento y recuperación segura de credenciales para los usuarios, aplicaciones y paquetes de servicios de seguridad. Su desactivación impide el funcionamiento del administrador de credenciales.

**Administrador de instalación de dispositivos - DsmSvc - svchost.exe**

Gestiona la detección, la descarga y la instalación del software asociado al dispositivo conectado al ordenador. No debe desactivar este servicio si desea beneficiarse de las actualizaciones de software para los dispositivos externos.

**Administrador de cuentas de seguridad - SamSs - lsass.exe**

Indica a otros servicios que el Administrador de cuentas de seguridad (SAM) está listo para aceptar solicitudes. Si deshabilita este servicio, no se podrá efectuar ninguna solicitud a la base de seguridad de SAM. Además las directivas de grupo no serán accesibles.

**Administrador de sesión local - LSM - svchost.exe**

Gestiona las sesiones locales de los usuarios de la plataforma. ¡No desactivar!

**Administrador de conexión automática de acceso remoto - RasAuto - svchost.exe**

Crea una conexión a una red remota siempre que un programa hace referencia a un nombre o dirección DNS o NetBIOS remoto. Si lo desactiva, los usuarios deberán conectarse de manera manual a otros sistemas. Si utiliza un router o una puerta de enlace, no necesita este servicio.

**Administrador de conexión de acceso remoto - RasMan - svchost.exe**

Administra conexiones de acceso remoto. Puede desactivar este servicio si no utiliza este tipo de conexiones.

**Administrador de conexiones Windows - Wcmsvc - svchost.exe**

Permite gestionar las conexiones de red del ordenador en función de la política configurada por el usuario. No desactivar este servicio si es necesaria la conectividad de red del equipo.

**Agrupación de red del mismo nivel - p2psvc - svchost.exe**

Proporciona servicios de agrupación de red del mismo nivel. Este servicio solo se utiliza con programas peer-to-peer. A priori se puede desactivar.

**Host de DLL de contador de rendimiento - PerfHost - perfhost.exe**

Permite a los procesos y usuarios remotos de 64 bits solicitar los contadores de rendimiento basados en librerías de 32 bits. Este servicio se puede desactivar.

**Dispositivo host de UPnP - upnphost - svchost.exe**

Permite que los dispositivos UPnP se hospeden en el equipo. Si se detiene el servicio, el ordenador será incapaz de detectar todos los dispositivos UPnP presentes en la red.

**Host de proveedor de detección de función - fdPHost - svchost.exe**

Sirve como proceso host para proveedores de detección de función. Si lo desactiva, su equipo dejará de detectar impresoras compartidas, así como los recursos de red.

**Host de sistema de diagnóstico - WdiSystemHost - svchost.exe**

Activa la detección de problemas y las funciones de reparación de los problemas de los componentes de Windows. Este servicio se puede desactivar con total tranquilidad.

**Identidad de aplicación - AppIDSvc - svchost.exe**

Este servicio se utiliza para determinar y comprobar la identidad de una aplicación. La desactivación de este servicio impide la utilización de la funcionalidad AppLocker.

**Información de la aplicación - Appinfo - svchost.exe**

Facilita la ejecución de algunas aplicaciones que requieren privilegios administrativos. Si este servicio se detiene, los usuarios no podrán responder a ninguna solicitud de elevación de privilegios.

**Instrumental de administración de Windows - Winmgmt - svchost.exe**

Proporciona una interfaz común y un modelo de objeto para tener acceso a la información de administración acerca del sistema operativo. No puede desactivar este servicio, ya que es esencial para el funcionamiento normal de los sistemas Windows NT.

**Captura SNMP - SNMPTrap - snmptrap.exe**

Recibe mensajes de captura generados por los agentes SNMP. Si no utiliza la aplicación con este protocolo, puede desactivar este servicio.

**Aislamientos de claves CNG - KeyIso - lsass.exe**

Este servicio se hospeda en el proceso LSA. Si lo desactiva, los servicios que dependen de él, como el cifrado de archivos, el protocolo EAP (*Extensible Authentication Protocol*, que permite autenticar una conexión de acceso remoto) y la configuración automática de redes cableadas no funcionarán. Si su ordenador no dispone de tarjeta de red inalámbrica, puede desactivar este servicio.

**Registro de eventos de Windows - Eventlog - svchost.exe**

Este servicio administra eventos y registros de eventos. Si se detiene, no podrá acceder a esta característica que le podría ser útil para establecer el diagnóstico de un problema que el usuario pueda tener.

**Registros y alertas de rendimiento - pla - svchost.exe**

Recopila información de rendimiento de equipos locales o remotos. Si se detiene este servicio, la información correspondiente no se recopilará ni será accesible.

**Iniciador de procesos de servidor DCOM - DcomLaunch - svchost.exe**

Ofrece el inicio de funcionalidad para los servicios DCOM. Muchos componentes del sistema dependen de este servicio, por lo que no debe desactivarlo.

**Llamada a procedimiento remoto (RPC) - RpcLocator - locator.exe**

Administra la base de datos de nombres RPC. Los componentes de sistema no utilizan este servicio, sin embargo, las aplicaciones como Microsoft Exchange dejarán de funcionar si lo desactiva.

**Asignador de detección de topologías de nivel de vínculo - lltdsvc - svchost.exe**

Permite crear un mapa de red. Si se deshabilita este servicio, el mapa de red no funcionará correctamente.

**Asignador de extremos RPC - RpcEptMapper - svchost.exe**

Este servicio resuelve identificadores de interfaces RPC en extremos de transporte. Si lo desactiva, los programas que utilizan servicios de llamada de procedimientos remotos (RPC) no funcionarán correctamente.

**Módulos de creación de claves para IKE y AuthIP - IKEEXT - svchost.exe**

Hospeda los módulos de claves IKE (*Internet Key Exchange*) y el protocolo de Internet autenticado AuthIP (*Authentication Internet Protocol*) que se utilizan para asegurar las conexiones basadas en el protocolo de seguridad de Internet IPsec (*Internet Protocol Security*) como las VPN. Si desactiva estos servicios, ocasionará un fallo en la seguridad.

**Motor de filtro de base - BFE - svchost.exe**

Es un servicio que administra las directivas de firewall y del protocolo de seguridad de Internet (IPsec). Si se deshabilita el servicio, se reducirá de manera significativa la seguridad del sistema. Además tendrá problemas con muchos otros servicios que dependen de él. Sin embargo, resulta lógico que lo desactive si utiliza un dispositivo externo como un router y no utiliza las funciones IPsec. También podrá desactivar los siguientes servicios: Agente de directiva IPsec, Módulos de creación de claves de IPsec para IKE y AuthIP, Conexión compartida a Internet y Enrutamiento y acceso remoto.

**Net Logon - Netlogon - lsass.exe**

Mantiene un canal seguro entre el equipo y el controlador de dominio para autenticar usuarios y servicios. Si se detiene el servicio, los usuarios de una estación de Windows no podrán conectarse a un dominio. Este servicio no debe desactivarse excepto si la máquina de destino forma parte de una red organizada en un grupo de trabajo.

**Optimizar los lectores - defragsvc - svchost.exe**

Utilizado para la defragmentación de los lectores del equipo. Deje este servicio activo para garantizar el buen rendimiento del sistema.

**Inicio de sesión secundario - seclogon - svchost.exe**

Habilita procesos de inicio bajo credenciales alternadas. Si se detiene, los usuarios no podrán realizar una elevación de privilegios mediante la opción **Ejecutar como**.

**Firewall de Windows - MpsSvc - svchost.exe**

Ayuda a proteger su equipo. Si ha optado por otra solución o tiene un módem/router, puede y debe desactivar este servicio.

**Conexión compartida a Internet(ICS) - SharedAccess - svchost.exe**

Proporciona servicios de traducción de direcciones de red, direccionamiento y resolución de nombres para una red. En resumen, si desactiva esta opción no podrá compartir su conexión de internet, a no ser que utilice un dispositivo externo, como un router.

**Programador de aplicaciones multimedia- MMCSS - svchost.exe**

Activa la definición relativa de prioridades en el trabajo de acuerdo con unas prioridades en las tareas realizadas en todo el sistema. Si este servicio se detiene, todas las aplicaciones multimedia dejarán de funcionar (así como el servicio Audio de Windows).

**Programador de tareas - Schedule - svchost.exe**

Habilita un usuario para que configure y programe tareas automáticas en este equipo. Este servicio no se puede desactivar utilizando el Administrador de servicios.

**Plug and Play - PlugPlay - svchost.exe**

Habilita un equipo para que reconozca y adapte los cambios de hardware. Si se detiene este servicio, no se reconocerá ningún hardware y el Administrador de dispositivos se quedará completamente vacío de cualquier indicación. Tenga en cuenta que en Windows 8 no podrá desactivar este servicio.

**Preparación de las aplicaciones - AppReadiness - svchost.exe**

Prepara las aplicaciones relacionadas con el perfil de usuario en la primera conexión de este usuario en un equipo Windows 8 y al instalar nuevas aplicaciones desde la tienda de aplicaciones Windows. Este servicio, inactivo por defecto, no se debe desactivar si quiere utilizar los servicios de Windows Store.

**Ayuda del Panel de control de Informes de problemas y soluciones - wercplsupport - svchost.exe**

Este servicio proporciona ayuda para ver, enviar y borrar los informes a nivel del sistema para el panel de control de la aplicación Informes de problemas y soluciones. Si desactiva este servicio, la función de enviar informes de error a Windows dejará de funcionar. En otras palabras, no se registrará ningún evento en el módulo correspondiente.

**Programa de instalación ActiveX (AxInstSV) - AxInstSV - svchost.exe**

Este servicio valida el control de cuenta de usuario para la instalación de los controles ActiveX desde Internet y a partir de los parámetros de la directiva de grupo. Este servicio se inicia previa solicitud y, si se deshabilita, la instalación de los controles ActiveX se comporta de acuerdo con la configuración predeterminada del navegador.

**Instalador de módulos de Windows - TrustedInstaller - TrustedInstaller.exe**

Habilita la instalación, modificación y eliminación de actualizaciones y componentes opcionales de Windows. Si este servicio está deshabilitado, habrá muchos programas, como Windows Update, que no funcionarán.

**Propagación de certificados - CertPropSvc - svchost.exe**

Propaga los certificados de tarjetas inteligentes. Si lo desactiva, los servicios y aplicaciones que utilizan tarjetas inteligentes dejarán de funcionar.

**Protección del software - slsvc - SLsvc.exe**

Permite la descarga, instalación y aplicación de licencias digitales para Windows. Si se deshabilita el servicio por error, el equipo funcionará en modo de funcionalidad reducida.

**Protocolo de autenticación extensible EAP - EapHost - svchost.exe**

Proporciona autenticación de red en escenarios como 802.1x con cable e inalámbrica, VPN y Protección de acceso a redes (NAP). Si no utiliza conexiones inalámbricas o esta norma de seguridad, puede desactivar este servicio.

**Protocolo de resolución de nombres de mismo nivel - PNRPsvc - svchost.exe**

Habilita la resolución de nombres de mismo nivel sin servidor a través de Internet. Si se deshabilitan algunas aplicaciones de colaboración y de punto a punto como, por ejemplo, Windows Meetings, pueden dejar de funcionar.

**Publicación de recursos de detección de función - FDResPub - svchost.exe**

Permite publicar el equipo en la red. La deshabilitación de este servicio no autorizará al resto de equipos de la red a detectar automáticamente los recursos del equipo.

**Redirector de puerto en modo usuario de Servicios de Escritorio - UmRdpService - svchost.exe**

Redirección de los recursos tipo impresoras y puertos para las conexiones RDP. Los recursos dirigidos no estarán disponibles si se desactiva el servicio.

**Registro remoto - RemoteRegistry - svchost.exe**

Habilita usuarios remotos para que modifiquen el Registro. Este servicio debe desactivarse por razones de seguridad.

**Enrutamiento y acceso remoto - RemoteAccess - svchost.exe**

Ofrece servicios de enrutamiento a empresas en entornos de red de área local o extensa. Si lo desactiva, estas funciones dejarán de ser accesibles. Por razones de seguridad, recomendamos desactivarlo.

**Servidor - LanmanServer - svchost.exe**

Ofrece compatibilidad con uso compartido de archivos, impresoras y canalizaciones a través de la red. Si se detiene el servicio, los recursos de red dejarán de compartirse.

**Servidor de prioridad de hilos - THREADORDER - svchost.exe**

Permite la ejecución ordenada de un grupo de hilos en un intervalo específico. Este servicio de optimización no debe estar desactivado.

**Servicio Agente de eventos de sistema - SystemEventsBroker - svchost.exe**

Coordina la ejecución de la carga de trabajo de la aplicación WinRT en segundo plano. Este servicio de optimización no se debe desactivar.

**Servicio Agente para las conexiones de red - NcbService - svchost.exe**

Coordina las conexiones de red de las aplicaciones Windows Store para recibir notificaciones de Internet. Puede desactivar este servicio si no utiliza los servicios de Windows Store

**Servicio Agente para los eventos temporales - TimeBroker - svchost.exe**

Coordina la ejecución de la carga de trabajo de la aplicación WinRT en segundo plano. Este servicio de optimización no se debe desactivar.

**Servicio Recopilador ETW de eventos para Internet Explorer - IEECollectorService - IEEtxCollector.exe**

Recopila y gestiona los eventos que Internet Explorer genera en tiempo real. No desactive este servicio si utiliza Internet Explorer.

**Servicio de asociación de dispositivos - DeviceAssociationService - svchost.exe**

Permite asociar dispositivos con cable o inalámbricos a Windows. Si este servicio está desactivado no se podrá conectar ningún dispositivo de este tipo.

**Servicio de enumeración de dispositivos de tarjeta inteligente - ScDeviceEnum - svchost.exe**

Crea nodos de dispositivos de software para todos los lectores de tarjetas inteligentes accesibles por la sesión de un usuario. Si este servicio está desactivado, las API WinRT no pueden enumerar las lecturas de tarjetas inteligentes. Puede desactivar este servicio si no utiliza dispositivos de este tipo.

**Servicio de historial de ficheros - fhsvc - svchost.exe**

Utilizado por la funcionalidad de historial de ficheros de Windows. Si se detiene, esta característica no funciona.

**Servicio de geolocalización - lfsvc - svchost.exe**

Controla la ubicación actual del sistema y asocia la ubicación geográfica con eventos asociados. Si desactiva este servicio, las aplicaciones no podrán utilizar ni recibir notificaciones relativas a localizaciones geográficas. Numerosos servicios de Internet utilizan esta funcionalidad de geolocalización. Si desactiva este servicio, no podrá utilizar esta funcionalidad.

**Servicio de infraestructura de tareas en segundo plano - BrokerInfrastructure - svchost.exe**

Controla la ejecución de tareas en segundo plano por el sistema operativo. Deje este servicio activo para garantizar el rendimiento del sistema.

**Servicio de instalación de dispositivos - DeviceInstall - svchost.exe**

Configura automáticamente el sistema operativo en caso de modificación del perfil de hardware del equipo. Si este servicio está inactivo provoca la inestabilidad del sistema.

**Servicio biométrico de Windows - WbioSrvc - svchost.exe**

Permite a las aplicaciones clientes capturar, comparar, manipular y almacenar datos biométricos sin tener directamente acceso al hardware o a las muestras. La desactivación de este servicio impide que las aplicaciones utilicen los datos biométricos.

**Servicio de caché de fuentes de Windows - FontCache - svchost.exe**

Este servicio optimiza el rendimiento de las aplicaciones copiando en la memoria caché los datos de fuentes más usados. Se inicia a petición de las aplicaciones. En caso de desactivación del servicio, el rendimiento de las aplicaciones puede disminuir.

**Servicio Cifrado de la unidad BitLocker - BDESVC - svchost.exe**

Este servicio se utiliza para la funcionalidad de cifrado de unidad BitLocker. Este servicio permite que BitLocker solicite a los usuarios que realicen diversas acciones vinculadas a los volúmenes montados y desbloquea los volúmenes automáticamente sin intervención del usuario. Además, si está disponible, almacena la información de recuperación en Active Directory y, si es necesario garantiza que se utilizan los certificados de recuperación más recientes. La parada o desactivación del servicio impide el funcionamiento de BitLocker.

**Configuración automática WLAN - Wlansvc - svchost.exe**

Este servicio enumera las redes locales inalámbricas (WLAN). Actívelo si utiliza una red inalámbrica.

**Servicio de configuración automática WWAN - WwanSvc - svchost.exe**

Administra las conexiones y adaptadores de módulo integrado/tarjeta de datos de alta velocidad móvil (GSM & CDMA) configurando las redes automáticamente. La desactivación de este servicio le impedirá beneficiarse de una experiencia de uso mejorada para la alta velocidad móvil.

**Servicio de detección automática de proxy Web WinHTTP - WinHttpAutoProxySvc - svchost.exe**

Proporciona los componentes de software necesarios para el envío de solicitudes HTTP y la recepción de respuestas. Si lo desactiva, los servidores Proxy no se detectarán de forma automática.

**Servicio de implementación de AppX (AppXSVC) - AppXSvc - svchost.exe**

Permite la implementación de la infrestructura para el despliegue de aplicaciones desde Windows Store. La desactivación de este servicio, que arranca a petición, impide el despliegue de nuevas aplicaciones de Windows Store en el sistema.

**Servicio de compatibilidad de programas - PcaSvc - svchost.exe**

Proporciona soporte técnico para el Asistente para la compatibilidad de programas. En principio, no debe desactivarse salvo que usted utilice aplicaciones completamente compatibles con Windows 7.

**Servicio de la puerta de enlace de nivel de aplicación - ALG - alg.exe**

Proporciona compatibilidad entre los complementos de protocolo de terceros y la conexión compartida a Internet. Si lo desactiva, no funcionarán los programas que lo utilizan, como

MSN y Windows Live Messenger. Puede desactivar este servicio si no utiliza la conexión compartida a Internet.

**Servicio del módulo de copia de seguridad a nivel de bloque - wbengine - wbengine.exe**

El módulo permite recuperar datos y copias de seguridad a nivel de bloque. Si lo desactiva, la copia de seguridad de ficheros a nivel de bloque no funcionará, pero esto no afectará a la copia clásica de seguridad de archivos.

**Servicio de notificación de eventos de sistema - SENS - svchost.exe**

Supervisa los eventos de sistema y notifica a los suscriptores del sistema de estos eventos. Si lo deshabilita, las notificaciones de red dejarán de funcionar.

**Servicio de uso compartido de puertos Net. Tcp - NetTcpPortSharing - SMSSvcHost.exe**

Ofrece la posibilidad de compartir puertos TCP a través del protocolo net.tcp. Si lo desactiva, las aplicaciones diseñadas en VB.net y que utilizan este protocolo no funcionarán.

**Servicio de planificación Windows Media Center - ehSched - ehsched.exe**

Este servicio administra los registros planificados de programas de TV en Windows Media Center. Si deshabilita este servicio la funcionalidad no estará disponible.

**Servicio de compatibilidad con Bluetooth - bthserv - svchost.exe**

Este servicio implementa la detección y asociación de periféricos Bluetooth. Su parada o desactivación impide el funcionamiento de los periféricos Bluetooth ya instalados y la detección y asociación de nuevos periféricos.

**Servicio de perfil de usuario - ProfSvc - svchost.exe**

Este servicio es responsable de cargar y descargar los perfiles de usuario. Si se detiene o deshabilita, los usuarios no podrán iniciar o cerrar la sesión. No lo desactive.

**Servicio de publicación de nombres de equipos PNRP - PNRPAutoReg - svchost.exe**

Este servicio publica un nombre de equipo con la ayuda del Protocolo de resolución de nombres de mismo nivel (PNRP). Si desactiva este servicio, no funcionarán algunas aplicaciones peer-to-peer que utilizan este protocolo de colaboración creado por Microsoft y aplicaciones de colaboración como NetMeeting.

**Servicio de informes de errores Windows - WerSvc - svchost.exe**

Este servicio se utiliza para la gestión de errores de los servicios de diagnóstico y reparación. Si lo deshabilita, estos servicios no indicarán correctamente los errores.

**Servicio receptor de Windows Media Center - ehRecvr - ehRecvr.exe**

Servicio de Windows Media Center para la recepción de TV y FM. Al igual que con los demás servicios de Windows Media Center (Servicio programador de Windows Media Center, Servicio de Windows Media Center Extender, Iniciador del servicio de Windows Media Center), es posible desactivarlo si no usa la aplicación o el servicio correspondientes.

**Servicio de almacenamiento - StorSvc - svchost.exe**

Fuerza la aplicación de la directiva de grupo a los dispositivos de almacenamiento. Si desactiva este servicio, la directiva de grupo no podrá aplicarse correctamente.

**Servicio de directivas de diagnóstico - DPS - svchost.exe**

Permite detectar, reparar y resolver problemas de componentes de Windows. No hemos encontrado problemas en los componentes de Windows después de haber desactivado este servicio. Pruébelo.

**Servicio de supervisión de sensores - SensrSvc - svchost.exe**

Adapta el sistema operativo en función de retornos de valores de capturas. Si se desactiva, provoca la inestabilidad del sistema.

**Servicio de transferencia inteligente en segundo plano - BITS - svchost.exe**

Transfiere archivos en segundo plano mediante el uso de ancho de banda de red inactiva. Si el servicio está deshabilitado, las aplicaciones como Windows Update, MSN Explorer, Reproductor Windows Media y algunas aplicaciones .NET, no podrán funcionar.

**Servicio de Panel de escritura a mano y teclado táctil - TabletInputService - svchost.exe**

Gestiona las funcionalidades de teclado táctil del sistema operativo. Si el servicio está desactivado esta característica no estará operativa.

**Servicio de dispositivo de interfaz humana - hidserv - svchost.exe**

Activa y mantiene la utilización de botones activos en el teclado y controles remotos en otros dispositivos multimedia. No desactive este servicio.

**Servicio enumerador de dispositivos portátiles - WPDBusEnum - svchost.exe**

Exige el cumplimiento de directivas de grupo para dispositivos extraíbles de almacenamiento. Si deshabilita este servicio, no podrá utilizar las directivas de grupo para restringir el acceso a algunos dispositivos extraíbles.

**Servicio host de proveedor de cifrado de Windows - WEPHOSTSVC - svchost.exe**

Negocia las funcionalidades vinculadas al cifrado con los proveedores de cifrado de terceros para los procesos que necesitan evaluar y aplicar directivas EAS. La parada de este servicio comprometerá las comprobaciones EAS que se han establecido para las cuentas de correo conectadas.

**Servicio host WDIServiceHost - WdiServiceHost - svchost.exe**

El servicio de directivas de diagnósticos utiliza este servicio para guardar los diagnósticos que se deben ejecutar en un contexto de servicio local. No desactive este servicio.

**Servicio del iniciador iSCSI de Microsoft - MSiSCSI - svchost.exe**

Administra las sesiones SCSI de Internet. No active este servicio si utiliza el protocolo de la capa de aplicación que permite el transporte de comandos SCSI en una red TCP/IP.

**Servicio Interfaz de almacenamiento en red - nsi - svchost.exe**

Este servicio entrega notificaciones de red a los clientes en modo de usuario. Si se detiene, le será imposible conectarse a cualquier red.

**Servicio KtmRm para Distributed Transaction Coordinator - KtmRm - svchost.exe**

Coordina las transacciones entre el componente Distributed Transaction Coordinator (MSDTC) y el administrador de transacciones del núcleo (KTM). Puede parar este servicio.

**Servicio de lista de redes - Netprofm - svchost.exe**

Identifica las redes a las que se conectó el equipo. Si deshabilita este servicio, las notificaciones de conexión red dejarán de ser visibles en el área de notificación del sistema de la barra de tareas.

**Servicio manos libres Bluetooth - BthHFSrv - svchost.exe**

Implementa la utilización de auriculares Bluetooth inalámbricos. Puede desactivar este servicio si no utiliza esta funcionalidad.

**Servicio Media Center Extender - Mcx2Svc - svchost.exe**

Este servicio se utiliza para la conexión de las unidades Media Center Extender. Si lo deshabilita la funcionalidad no estará disponible.

**Servicio de uso compartido de red del Reproductor de Windows Media - WMPNetworkSvc - wmpnetwk.exe**

Comparte las bibliotecas del Reproductor de Windows Media con otras unidades de red. La desactivación de este servicio le impedirá compartir los recursos registrados en el Reproductor de Windows Media.

**Servicio Windows Defender - WinDefend - MsMpEng.exe**

Servicio básico de la solución antivirus de Microsoft que protege a los usuarios contra el software malicioso y otros programas potencialmente peligrosos. Puede desactivar este servicio si no utiliza esta funcionalidad.

**Servicio Windows Store (WSService) - WSService - svchost.exe**

Gestiona la funcionalidad Windows Store para las aplicaciones Windows 8. Si se desactiva puede provocar la inestabilidad de estas aplicaciones.

**Servicio SSTP (Secure Socket Tunneling Protocol) - svchost.exe**

Este servicio permite utilizar el protocolo SSTP para conexiones VPN. Si lo deshabilita, no podrá utilizar el protocolo SSTP.

**Servicios de Escritorio Remoto - TermService - svchost.exe**

Permite a los usuarios conectarse interactivamente a un equipo remoto. A no ser que utilice conexiones Terminal Server, este servicio debe desactivarse por razones de seguridad.

**Servicios de cifrado - CryptSvc - svchost.exe**

Proceso utilizado por los servicios de administración para, por ejemplo, proporcionar funcionalidades de administración de certificados al sistema operativo. No desactive este servicio.

**SMP del epacio de almacenamiento Microsoft - smphost - svchost.exe**

Servicio del proveedor de administración del espacio de almacenamiento Microsoft (Windows Storage Spaces). No desactive este servicio.

**Cola de impresión - Spooler - spoolsv.exe**

Carga archivos en la memoria para imprimirlos más tarde. Este servicio se puede desactivar si no dispone de impresora.

**Estación de trabajo - LanmanWorkstation - svchost.exe**

Soporta los servicios del protocolo SMB. La interrupción del servicio inutiliza el protocolo. No es aconsejable interrumpirlo.

**Directiva de extracción de tarjetas inteligentes - SCPPolicySvc - svchost.exe**

Autoriza el cierre del escritorio del usuario en el momento de retirar la tarjeta inteligente. Puede desactivar este servicio si no utiliza esta funcionalidad.

**Superfetch - SysMain - svchost.exe**

Mantiene y mejora el rendimiento del sistema a lo largo del tiempo. Si desactiva este servicio, las aplicaciones se lanzarán con las mismas prioridades.

**Sistema de eventos COM+ - EventSystem - svchost.exe**

Se ocupa del Servicio de notificación de eventos del sistema (SENS). Si se interrumpe, dejará de funcionar la notificación de eventos del sistema. Por otra parte, las demás aplicaciones, como la transferencia inteligente en segundo plano y la replicación DFS, no funcionarán correctamente. Este servicio no se debe desactivar.

**Sistema de colores de Windows - WcsPluginServices - svchost.exe**

El servicio WcsPlugInService hospeda módulos de complemento de terceros para el modelo de dispositivo de colores (los perfiles ICS). La desactivación de este servicio hará que los periféricos de captura de imagen utilicen los perfiles predeterminados en lugar de los instalados por los editores o fabricantes. En principio, no debe desactivar este servicio.

**Sistema de cifrado de archivos EFS (Encripting File System) - EFS - lsass.exe**

Implementa la tecnología EFS de cifrado y almacenamiento de ficheros de base en los volúmenes NTFS. Si lo desactiva, las aplicaciones no tendrán acceso a los archivos ya cifrados.

**Fax - FAX - fxssvc.exe**

Permite enviar y recibir faxes. Si lo desactiva no podrá utilizar esta utilidad.

**Telefonía - TapiSrv - svchost.exe**

Admite la interfaz TAPI (*Telephony Application Programming Interface*) para programas que controlan los dispositivos de telefonía. En principio, si no dispone de un módem de acceso telefónico o de fax puede desactivar este servicio.

**Servicio horario Windows - W32Time - svchost.exe**

Este servicio se utiliza para la sincronización de la fecha y la hora en redes Windows. Atención a las dependencias del servicio si desactiva esta función.

**Temas - Themes - svchost.exe**

Proporciona un sistema de administración de temas de experiencia de usuario. Se puede desactivar este servicio.

**Comprobador puntual - svsvc - svchost.exe**

Comprueba el estado del sistema de archivos. Deje activo este servicio para garantizar la coherencia del sistema.

**Cliente web - WebClient - svchost.exe**

Habilita los programas basados en Windows para que creen, tengan acceso y modifiquen archivos basados en Internet. Por razones de seguridad, debe desactivar este servicio, pero tiene dos inconvenientes: los desarrolladores lo necesitan si trabajan en WebDAV y los enlaces de hipertexto no se abrirán en una nueva ventana cuando haga clic en ellos desde una aplicación de correo.

**Registrador de configuración de Windows Connect Now - wcncsvc - svchost.exe**

Actúa como registrador y emite credenciales de red al candidato inscrito. Esta utilidad permite a un equipo que funciona en Windows 7 integrarse de manera fácil en una red mediante la creación de un enlace entre el ordenador y otro elemento de la red, después de haber introducido el código PIN. Por ejemplo, esto le permite conectar una Xbox 360 a una Wi-Fi.

**Windows Driver Foundation - User-mode Driver Framework - wudfsvc - svchost.exe**

Administra procesos host de controlador en modo usuario. En principio, debe dejarlo activado.

**Windows Installer - msiserver - msiexec**

Agrega, modifica y elimina aplicaciones proporcionadas como paquetes de Windows Installer (*.msi). Si se deshabilita, no se podrá modificar o instalar aplicaciones que utilicen esta plataforma de instalación.

**Windows Search - Wsearch - SearchIndexer.exe**

Proporciona servicios de indización de contenido y caché de propiedades para archivos. Si el servicio se detiene o deshabilita, el Explorador de Windows no podrá mostrar las ubicaciones de carpeta virtual y las búsquedas se realizarán con mayor lentitud.

**Windows Update - wuaserv - svchost.exe**

Habilita la detección, descarga e instalación de actualizaciones de Windows. Si se deshabilita, las actualizaciones automáticas dejarán de funcionar por lo que, por razones de seguridad, no se aconseja desactivarlo.

## 2. Los servicios de Windows 10

La siguiente lista completa la lista anterior con los nuevos servicios de Windows 10. Observe que a medida que se añaden nuevas funcionalidades, Microsoft completa esta lista de servicios.

**Servicio de enrutador AllJoyn - AJRouter - svchost.exe**

Dirige los mensajes del servicio cliente AllJoyn para facilitar la interoperabilidad de los objetos conectados. Si este servicio está desactivado, las tareas en segundo plano de este servicio no se activarán.

**Connected Device Platform Service - CDPSvc - svchost.exe**

Servicio de conexión de dispositivos externos. No desactive este servicio.

**Servicios de licencias de cliente (ClipSVC) - ClipSVC - svchost.exe**

Gestiona las licencias para las aplicaciones de pago de la tienda de aplicaciones Microsoft (Windows Store). Si se desactiva este servicio, no podrá comprar aplicaciones en la tienda de aplicaciones Microsoft.

**CoreMessaging - CoreUIRegistar - svchost.exe**

Gestiona la comunicación entre los componentes del sistema. No debe desactivar este servicio.

**Servicio Agente de descubrimiento en segundo plano DevQuery - DevQueryBroker - svchost.exe**

Permite a las aplicaciones descubrir dispositivos en segundo plano.

**Microsoft (R) Diagnostics Hub Standard Collector Service - diagnosticshub.standardcollector.service - diagnosticshub.standardcollector.service.exe**

Recopila en tiempo real eventos y procesos Windows. No desactive este servicio.

**Servicio de inscripción de administración de dispositivos - DmEnrollmentSvc - svchost.exe**

Asegura la inscripción de dispositivos en la entidad de administración correspondiente. No desactive este servicio.

**Dmwappushsvc - Dmwappushservice - svchost.exe**

Gestiona el enrutamiento de las peticiones WAP. Es servicio está relacionado con el envío de SMS y, a priori, se puede desactivar si no utililiza esta funcionalidad.

**Optimización de entrega - DoSvc - svchost.exe**

Optimiza la distribución de contenido. No desactive este servicio.

**Servicio de intercambio de datos - DsSvc - svchost.exe**

Servicio de intercambio de datos entre las aplicaciones. No desactive este servicio.

**EntAppSvc - EntAppSvc - svchost.exe**

Servicio de gestión del almacén de aplicaciones de empresa. Este servicio se puede parar si no utiliza este tipo de funcionalidad.

**Servicio Punto de acceso inalámbrico móvil Windows - icssvc - svchost.exe**

Servicio para compartir la conexión por dispositivo móvil. Se puede parar si no utiliza esta funcionalidad.

**Administrador de mapas descargados - MapsBroker - svchost.exe**

Servicio de acceso para las aplicaciones de mapas descargados. Este servicio se inicia a petición de la aplicación. No desactive este servicio si sus aplicaciones utilizan mapas de carreteras.

**Servicio de Configuración de red - NetSetup - svchost.exe**

Gestiona la instalación de los controladores de red y permite la configuración de parámetros de red de bajo nivel. No desactive este servicio.

**Contenedor Microsoft Passport - NgcCtnrSvc - svchost.exe**

Gestiona las claves de identidad con proveedores de identidad, así como las tarjetas inteligentes virtuales del módulo de plataforma segura (TPM). Puede desactivar este servicio si no utiliza esta funcionalidad.

**Microsoft Passport - NgcSvc - lsass.exe**

Proporciona el aislamiento de la autentificación con los proveedores de identidad asociados a un usuario. Si este servicio está desactivado, las funciones de utilización y la gestión de estas claves, como la apertura de sesión y la autentificación única para las aplicaciones y los sitios web, no estarán disponibles. No desactive este servicio.

**PhoneSvc - PhoneSvc - svchost.exe**

Gestiona el estado de las funciones teléfonicas del dispositivo. Puede desactivar este servicio si no utiliza las funcionalidades de telefonía de Windows.

**Servicio demo de almacén - RetailDemo - svchost.exe**

Controla la actividad del dispositivo mientras que esté en modo demostración. Puede desactivar este servicio si no utiliza esta nueva funcionalidad de Windows 10.

**Servicio de datos del sensor - SensorDataService - svchost.exe**

Proporciona los datos de los sensores integrados en su dispositivo. No desactive este servicio.

**Servicio de sensor - SensorService - svchost.exe**

Administra las diferentes funcionalidades vinculadas a los sensores integrados a su dispositivo sobre todo el sensor de orientación del mismo. No desactive este servicio si quiere utilizar la rotación automática de la pantalla como, por ejemplo, en una tableta.

**Servicio enrutador SMS Microsoft Windows - SmsRouter - svchost.exe**

Enruta los mensajes SMS. Puede desactivar este servicio si no utiliza las funcionalidades de telefonía de Windows.

**Servicio State Repository (StateRepository) - StateRepository - svchost.exe**

Proporciona la infraestructura necesaria al modelo de aplicación. No desactive este servicio.

**Administrador de usuarios - UserManager - svchost.exe**

Proporciona los componentes de ejecución requeridos para una interacción multiusuario. No desactive este servicio.

**Actualizar el servicio Orchestrator - UsoSvc - svchost.exe**

Actualiza el servicio Orchestrator para la instalación de programas o para la actualización a nivel de configuración del sistema. Puede desactivar este servicio si no forma parte de una organización con dominio.

**Xbox Live Auth Manager - XblAuthManager - svchost.exe**

Proveedor de autentificación para interactuar con los servicios Xbox Live. No desactive este servicio si va a utilizar los juegos y servicios Xbox Live.

**Xbox Live Game Save - XblGameSave - svchost.exe**

Sincroniza las copias de seguridad de datos para los juegos Xbox. No desactive este servicio si va a utilizar los juegos y servicios Xbox Live.

**Xbox Live Networking Service - XboxNetApiSvc - svchost.exe**

Servicio de soporte de la API Xbox Live Networking Service. No desactive este servicio si va a utilizar los juegos y servicios Xbox Live

## Encontrar las versiones anteriores de un archivo o carpeta

Esta utilidad se basa en las instantáneas de volúmenes (*Volume Shadow Copy* o VSC). Permite encontrar diferentes versiones de un archivo después de haberlo modificado y eliminado. En efecto, Windows guardará copias sucesivas del conjunto de archivos y carpetas en los que usted trabajó. Por otra parte, se crea de manera automática una versión anterior de un objeto que aparece en el Explorador de Windows cuando:

- Se realiza una copia de seguridad automática de archivos.
- Se crea un punto de restauración del sistema.

Compruebe que ha activado la protección del sistema:

Desde el Panel de control, abra la sección **Sistema y seguridad**.
Haga doble clic en el icono **Sistema**.
Haga clic en el enlace **Protección del sistema**.
Haga clic en **Crear**.
Si el botón **Crear** está atenuado, la razón más probable es que la protección del sistema esté desactivada. En ese caso, haga clic en el botón **Configurar** y seleccione la opción **Activar protección del sistema**. Puede limitar el espacio de disco utilizado para esta funcionalidad si lo desea. Haga clic en el botón **Aceptar** para validar la activación de esta funcionalidad.

Introduzca un nombre para el punto de restauración y haga clic en el botón **Crear**.

Un cuadro de diálogo le avisará de que el punto de restauración se ha creado.

A continuación, haga clic en el botón **Restaurar sistema...** y en **Siguiente**.
Seleccione el punto de restauración del sistema y haga clic en **Siguiente**.

Desde ese momento, podrá volver cuando desee al punto de restauración que acaba de crear.

Esta utilidad permite crear instantáneas del sistema en periodos de tiempo regulares y encontrar las diferentes versiones de un documento.

Esta utilidad no funciona con los archivos de sistema ni con los archivos del directorio \Windows. Por defecto, el almacenamiento de archivos ocupa un 15% del espacio total del disco.

Para volver a una versión anterior de un archivo, haga clic con el botón secundario del ratón sobre el archivo en cuestión y seleccione la opción **Restaurar versiones anteriores**.

También puede activar esta utilidad para discos externos siguiendo las siguientes instrucciones:

Desde el módulo **Sistema**, haga clic en el enlace **Protección del sistema**.
En la columna **Discos disponibles**, seleccione las casillas correspondientes a los discos que desea añadir.

Desde algunas de las aplicaciones de Windows, cuando desee ver directamente las versiones anteriores, haga clic en la flecha pequeña situada a la derecha de **Abrir** y seleccione la opción **Mostrar versiones anteriores**.

## 1. Recuperación de un archivo borrado de manera accidental

Debe conocer el nombre de la carpeta en la que el archivo estaba guardado y haber creado un punto de restauración entre el momento en que creó el archivo y el momento en que lo eliminó.

En Windows 8 y Windows 10, puede utilizar la restauración de archivos a través de la configuración y activación de la funcionalidad Historial de archivos. Puede acceder a esta funcionalidad desde el Panel de control y necesita del uso compartido de red. Es necesario que esté activada previamente para que pueda restaurar un fichero.

Una vez activada, para visualizar el historial de un archivo, haga clic en el botón **Historial** que puede encontrar en el menú **Inicio** de la cinta del Explorador de Windows.
Haga clic con el botón derecho del ratón en el nombre de la carpeta y elija **Restaurar versiones anteriores**.

Seleccione uno de los puntos de restauración de la lista y haga clic en el botón **Abrir**.

La barra de dirección del Explorador de Windows mostrará la fecha de algunos archivos de la lista.

Haga clic con el botón secundario del ratón en el archivo que desea recuperar y seleccione la opción **Copiar** o **Enviar a**.
Pegue el archivo en la ubicación deseada.

También puede recuperar un directorio completo haciendo clic en el botón correspondiente.

Siempre dispondrá de esa posibilidad, incluso si durante ese tiempo vació la Papelera de reciclaje.

## 2. La herramienta de la instantánea de volumen

Vssadmin permite administrar fácilmente el espacio asignado para la herramienta de instantánea de volumen. Esta utilidad está disponible en Windows desde la línea de comandos.

Ejecute el Símbolo del sistema en modo administrador.
Introduzca este comando: **`vssadmin list shadowstorage`**.

Mostramos aquí algunos comandos posibles:

```
vssadmin resize shadowstorage/ on=[Letra de la unidad]:/ For=[ Letra
de la unidad]: /Maxsize=[Tamaño máximo] :
```

Reduce o aumenta el tamaño máximo autorizado.

Si no se especifica el tamaño máximo, el espacio utilizable no tendrá ningún límite. Si se eliminan algunas instantáneas, el espacio de almacenamiento de instantáneas se reducirá. El tamaño máximo debe ser superior o igual a 300 MB. Puede especificar los sufijos siguientes: KB, MB, GB, TB, PB y EB. También puede utilizar los sufijos: B, K, M, G, T, P y E. Si no especifica ningún sufijo, el tamaño máximo se expresará en bytes.

```
vssadmin resize shadowstorage/ on=c: /For=c: /Maxsize=3g :
```

Por ejemplo, este comando limita a 3 GB el tamaño máximo asociado al almacenamiento de instantáneas en el volumen que contiene Windows 8.

También puede comprobar los resultados obtenidos con estos comandos:

- **`vssadmin list providers`**: muestra el nombre, tipo, ID del proveedor y la versión de todos los proveedores de las instantáneas instaladas. La palabra clave "providers" hace referencia a un componente de sistema que crea y administra las instantáneas.
- **`vssadmin list shadows`**: lista todas las instantáneas de volumen existentes.
- **`vssadmin list volumes`**: lista todos los volúmenes que pueden ser objeto de instantáneas.
- **`vssadmin list writers`**: lista todos los redactores suscritos a las instantáneas de volumen. La palabra clave "writers" hace referencia a una aplicación que almacena una parte de la información necesaria para la sincronización de instantáneas de volumen.

# Protección de datos con el historial de archivos

Esta funcionalidad le permite guardar automáticamente sus ficheros en un espacio de almacenamiento remoto, por ejemplo una llave USB o un disco de almacenamiento de red. Esta aplicación sustituye a la herramienta de copia de seguridad de Windows 7. La copia es automática, lo que quiere decir que los ficheros se pueden restaurar a una fecha y hora definidas. Están almacenados en las bibliotecas, los contactos, los favoritos, el Escritorio, así como en el espacio de almacenamiento Microsoft OneDrive.

A continuación, vamos a ver cómo realizarlo. Para comenzar, hay que conectar una unidad de copia externa en su ordenador o seleccionar una ubicación de red. Si dispone de un NAS, esta solución tiene las mejores garantías de disponibilidad. Pero también puede utilizar un disco duro externo conectado a través del puerto USB.

## 1. Copia de seguridad de datos

Desde el **Panel de control**, en la sección **Sistema y seguridad** - **Historial de archivos**, haga clic en el botón **Activar**.

Una vez la funcionalidad está activa, se ejecuta una copia de seguridad de los archivos en el soporte de almacenamiento portátil.

Para modificar la frecuencia y la duración de los ficheros de copia de seguridad, desde la sección **Historial de archivos** del Panel de control, haga clic en el enlace **Configuración avanzada**. Modifique la frecuencia de las copias de los archivos para guardar copias nuevas, por ejemplo, cada doce horas.

También puede modificar la duración de la conservación de las versiones guardadas para limitar esta duración, por ejemplo, a tres meses.

Haga clic en el botón **Guardar cambios** si es necesario.

También puede excluir una carpeta de las carpetas guardadas por defecto. En este caso, desde la sección **Historial de archivos** del Panel de control, haga clic en el enlace **Excuir carpetas**. Haga clic en el botón **Agregar**.

Seleccione la carpeta que quiere excluir y haga clic en en el botón **Guardar cambios**.

## 2. Restauración de los datos

Para restaurar los archivos y carpetas guardados, siempre en la sección **Historial de archivos**, haga clic en el enlace **Restaurar archivos personales**.

A continuación seleccione la hora y la fecha en las que quiere restaurar si archivo o carpeta desplazándose por los diferentes puntos de restauración.

Seleccione el elemento a restaurar y haga clic con el botón derecho sobre este elemento. Puede restaurarlo en su ubicación inicial o en otra diferente.

Observe que también puede acceder al historial de archivos desde el Explorador de Windows. Para ello seleccione el archivo o la carpeta a restaurar, y en la cinta del explorador, en la pestaña **Inicio**, haga clic en el botón **Historial**.

## 3. Copia de seguridad completa

El objetivo de esta operación es permitirle realizar una copia de seguridad de una partición completa o incluso de todo el disco duro. La ventaja de esta utilidad creada para Windows es que una vez haya finalizado la creación completa, dispondrá de una imagen real del disco duro o de una partición. Además, en lo sucesivo podrá realizar copias de seguridad

complementarias que solo registrarán los últimos cambios realizados en el equipo. El ahorro de tiempo y espacio es considerable.

Abra un Símbolo del sistema en modo Administrador y ejecute el siguiente comando: **sdclt.exe**.
Puede acceder a esta herramienta desde el **Panel de control** en la sección **Sistema y seguridad** - **Copias de seguridad y restauración** (**Windows 7**).

Para hacer la copia puede seleccionar una partición existente en el disco duro, una unidad externa, una ubicación de red o una grabadora de DVD.

Haga clic en **Siguiente**.

Por defecto, se seleccionan de manera automática la partición en la que está instalado el sistema operativo y la que tiene el sector de inicio del equipo.

Haga clic en los botones **Siguiente** e **Iniciar la copia de seguridad**.

Si va a utilizar una serie de DVD-ROM, prevea un número de discos suficiente, ya que la relación de compresión es, más o menos, de 1 de 3.

## 4. Restauración completa de una partición

Inserte el disco de instalación.
Si es necesario, modifique en la BIOS la secuencia de arranque.
Arranque desde el disco de Windows en modo WinRE.
Haga clic en **Reparar** y a continuación en **Opciones avanzadas**.
Haga clic en el enlace **Recuperación de la imagen del sistema**.
Quite el disco de Windows y, si es necesario, inserte el disco en el que ha realizado una copia de seguridad completa.

Sin esta modificación, no encontrará ningún soporte válido de copia de seguridad.

Seleccione, preferentemente, la opción **Utilizar la última imagen del sistema (recomendado)**. Observe que también puede seleccionar otra imagen del sistema. Haga clic en **Siguiente**.
Si lo desea, puede instalar controladores para restaurar la imagen del sistema en un perfil de hardware diferente. Haga clic en el botón **Siguiente**.
Haga clic en **Finalizar**.
Active la casilla **Confirmo que deseo borrar todos los datos existentes y restaurar el respaldo** y haga clic en **Aceptar**.

Una vez que la operación de copia de seguridad integral haya terminado, el equipo se reiniciará.

# Windows Update

Windows Update permite mantener el sistema actualizado y ser informado automáticamente si se publica una revisión en el sitio de Microsoft. A continuación, le mostraremos soluciones para los problemas más habituales que pueden aparecer con Windows Update.

## 1. Error 800706BA

Al iniciar le aparecerá este tipo de error: "No se instalaron las siguientes actualizaciones - Error: x actualizaciones - Se encontraron errores: Código 800706BA". Este error ocurre cuando uno o más paquetes de instalación están dañados.

En primer lugar, reinicie en modo seguro.
Active la visualización de archivos y carpetas ocultos en el Explorador de Windows.
Abra en el Explorador el siguiente árbol: \Programdata\Microsoft\network\downloader.
Elimine este tipo de archivos: *qmgr0.dat*, *qmgr1.dat*, etc.

A continuación, reinicie en modo normal y vuelva a iniciar el proceso de actualización de Windows Update.

## 2. Error 0xC004C4A5

Este error parece deberse a un problema aleatorio de los servidores de Windows.

Diríjase a la siguiente dirección: http://windows.microsoft.com/es-ES/windows/genuine/what-to-look-for
Consulte la información que permite comprobar que su versión de Windows es original.

## 3. Error 0x80070424

Si encuentra este mensaje de error, en primer lugar ejecute la utilidad de reparación Windows Update situada en la sección **Sistema y seguridad** del **Panel de control** - **Todos los Paneles de configuración** - **Buscar y corregir problemas**.
Si esta utilidad no le resuelve el problema, puede arrancar el servicio **Programa de instalación para los módulos Windows**.
Si este servicio no arranca o si el fichero TrustedInstaller.exe no está en la carpeta C:\Windows\Servicing, desde un ordenador en que funcione Windows Update, copie este fichero y exporte la siguiente clave de registro: HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\ TrustedInstaller.
Copie estos elementos en el ordenador a reparar y reinicie Windows.

## 4. Error 8024402F

Si encuentra este mensaje de error, en primer lugar ejecute la utilidad de reparación Windows Update situada en la sección **Sistema y seguridad** del **Panel de control** - **Todos los Paneles de configuración** - **Buscar y corregir problemas**.
Si esta utilidad no le resuelve el problema, puede reiniciar el servicio BITS, el servicio Windows Update, el servicio identidad de la aplicación y los servicios de cifrado.

Puede utilizar los siguientes comandos para parar estos servicios:

```
net stop bits
net stop wuauserv
net stop appidsvc
net stop cryptsvc
```

A continuación elimine los archivos qmgr*.dat.

Puede utilizar el siguiente comando para eliminar estos ficheros:

```
Del "%ALLUSERSPROFILE%\Application
Data\Microsoft\Network\Downloader\qmgr*.dat"
```

Reinicie los servicios que paró anteriormente.

Puede utilizar los siguientes comandos para reiniciar los servicios:

```
net start bits
net start wuauserv
net start appidsvc
net start cryptsvc
```

CAPÍTULO 6

# Reparación del S.O.

# Nociones de reparación

Este capítulo del libro se esfuerza en recordar algunas de las reglas esenciales que le permitirán evitar muchos desastres.

## 1. Diez cosas que no debe hacer con el ordenador

Le presentamos una pequeña lista de cosas que no se deben a hacer que le servirá como recordatorio.

- No limpie un ordenador portátil o una pantalla con cualquier tipo de producto. Para limpiar material informático utilice un producto apropiado o un trapo que no sea afelpado y que esté ligeramente húmedo.
- No aspire el interior del ordenador. Utilice más bien un limpiador de aire comprimido, con cuidado de no tocar los componentes eléctricos. El único uso que le podemos dar al aspirador es colocarlo cerca del ventilador de la fuente de alimentación para extraer el polvo ahí depositado.
- Nunca extraiga un disco bloqueado en la unidad de CD/DVD con ayuda de un destornillador. En todas las cubiertas delanteras de las unidades de CD/DVD o grabadoras existe un minúsculo agujero en el que puede insertar la punta de un alfiler o de un clip para provocar la apertura manual de la unidad.
- No coloque un disco dañado en la unidad de CD/DVD. Por increíble que parezca, un disco estropeado puede ser expulsado bruscamente de la unidad con una fuerza y rapidez insospechadas y, con esta acción, hacerle daño.
- No continúe utilizando el ordenador cuando sospeche que existe un problema en el disco duro. En el peor de los casos, se arriesga a perder los datos de manera definitiva. En un primer momento, proceda a realizar una copia de seguridad de los datos y, con la cabeza fría, intente analizar si el problema al que se enfrenta se debe a una avería del disco duro o de alguno de los demás componentes del equipo.
- No instale ningún programa de detección de errores o de reparación del sistema. Siempre hay gente con buenas intenciones que le dirá que con el programa X ha podido solucionar un problema bastante raro y que todo acabó bien; sin embargo, en la mayoría de los casos, esto no hará otra cosa que agravar un problema que puede acabar provocando que el equipo quede definitivamente inutilizable.
- No descargue programas que prometen las mil maravillas en términos de rendimiento. En el mejor de los casos, ganará algunos nanosegundos, pero lo más normal es que

degraden el rendimiento del equipo e incluso le impidan usar las aplicaciones más utilizadas.

- No almacene todo en el disco duro. Hay una regla absoluta en este campo: cuanta menos información contenga el disco duro, más posibilidades tendrá de funcionar de manera eficaz. Compre un paquete de CD grabables o regrabables y, en la medida de lo posible, transfiera las imágenes, vídeos, archivos MP3 a los soportes extraíbles. Por otra parte, existen muchos sitios en línea que le permiten guardar datos. La mayoría de estos servicios disponen de ofertas gratuitas.
- No utilice un ordenador con datos y aplicaciones profesionales para fines personales. Es increíble el número de veces que escuchamos: "Mi hijo ha instalado tal juego y ya no puedo acceder a la contabilidad". Existe una línea clara de separación que debemos tener en cuenta: un equipo que contiene datos importantes debe estar bajo su única responsabilidad y debe evitar a toda costa exponerlo a este tipo de prácticas que suponen un riesgo (juegos, sitios de adultos, redes peer-to-peer, descargas de sitios "Warez", etc.).
- Realice copias de seguridad. Otro comentario común es: "Mi disco duro me ha dejado tirado y he perdido la lista de todos mis clientes". El principal problema es que realmente no sabemos cuándo va a surgir una avería. Puede pasar que un disco duro u otro componente esté defectuoso cuando compra el equipo o años más tarde. Recuerde que si carece de copias de seguridad, siempre ocurrirá en el peor momento. Por consiguiente, tome la costumbre de realizar copias de seguridad regulares en memorias USB, en línea o en discos externos.

Añadimos también un desmentido irrefutable a la creencia de que una pieza nueva no puede estar dañada. Es más bien al contrario, en ese momento es cuando más posibilidades tiene de recibir un componente que no ha sido comprobado y descubrir que es inservible.

El overclocking, que consiste en aumentar la capacidad del hardware, sobretodo la velocidad del procesador, no está recomendado para un uso profesional. Hágalo en ordenadores personales que se utilicen sobretodo para videojuegos. Si de todos modos debe hacer overclocking en su ordenador, no aumente la velocidad más del 10% del procesador, a riesgo de volver inestable el sistema operativo y de acortar el tiempo de vida de su equipo.

Último punto: si debe usar su equipo para asuntos profesionales, infórmese bien sobre las condiciones de garantía. Los plazos de reparación pueden ser de hasta tres meses. Debe desconfiar de mensajes del tipo: "Se reserva el derecho de disponibilidad de piezas por parte del fabricante". Incluso si las condiciones de garantía indican un plazo de cambio de pieza de 24 horas, podría tener que esperar más tiempo si el fabricante no envía al taller la pieza o piezas necesarias.

## 2. ¿Qué actitud debemos adoptar cuando llamamos al soporte técnico?

En primer lugar, debe saber que a menudo estos técnicos son principiantes y es raro que estén suficientemente formados. Por una parte, es una profesión especialmente difícil y que requiere de conocimientos avanzados en campos muy variados (y a menudo incluso psicología). Se puede encontrar con tres situaciones:

- Con frecuencia, el interlocutor está interesado en atender su llamada lo más rápidamente posible y utiliza una solución fácil: "Bueno, señor X, no tiene que hacer gran cosa, tan solo restaure completamente el sistema".
- Casi nunca tiene la solución a su problema, pero intentará llevarle por caminos completamente inútiles (para ganar tiempo).

- Intentará acusarle de causar el problema: "¿Últimamente ha habido tormentas en su área?" o "¿Ha instalado recientemente algún juego o programa descargado de Internet?

Así pues, hay tres precauciones que debe tomar:

- Tómese tiempo de documentarse en la Web y comprobar las diferentes soluciones que puede encontrar. Anote cuidadosamente las soluciones que ha intentado realizar y descríbaselo claramente al experto con el que hable. Debe tener un as bajo la manga antes de hablar con el técnico "Lo sé todo".
- Asegúrese de que ya ha realizado un formateo y una reinstalación completa del sistema, siguiendo las reglas del gremio. El mensaje subyacente es hacerle comprender al interlocutor que el ordenador se encuentra con configuración "de fábrica".
- Invoque su buena fe y jure que siempre que se va de casa, desconecta el equipo de la toma eléctrica, al igual que el módem ADSL. Además, añada que no ha instalado recientemente ningún programa y que jamás de los jamases ha añadido un componente.

## 3. Encontrar la solución de un problema en Internet

Aunque no sea el único motor de búsqueda, Google es el líder indiscutible en este campo. Evite realizar búsquedas generales como: "Problema con Outlook Express" o se encontrará con una tira de resultados sin que ninguno de ellos haga referencia a su problema en particular. Acostumbre a lanzar búsquedas utilizando el mensaje de error que le aparece entre comillas, como en el siguiente ejemplo: "MSIMN provocó un error de página no válida en el módulo MSOE.DLL". Tenga en cuenta que si la expresión buscada no va seguida de otros términos, las comillas de cierre no son obligatorias.

El segundo problema con el que se encontrará es que en el montón de resultados procedentes de foros informáticos de ayuda mutua, pocos le ofrecerán la solución exacta que busca. En ese caso, habrá que echarle una mano a Google y precisar que solo desea que le muestre los resultados de las páginas con la palabra clave: "solucionado": "Problema con Outlook Express" intext:solucionado. Este truco se basa en el hecho de que muchos Webmaster de estos foros piden a la gente que añada este mensaje en el título de la página cuando la pregunta ha recibido una respuesta satisfactoria. Realice algunas pruebas y verá que funciona mejor que un toque de varita mágica.

Tenga en cuenta que los motores de búsqueda Google y Bing disponen de términos que permiten personalizar las consultas de búsqueda. Si quiere más información sobre estos elementos sintácticos, puede consultar en las siguientes páginas:

- Para el motor Google: http://www.google.com/support/enterprise/static/gsa/docs/admin/72/gsa_doc_set/xml_reference/request_format.html#1077029
- Para el motor Bing: https://msdn.microsoft.com/en-us/library/ff795620.aspx

Si no encuentra ninguna solución en las webs españolas, puede intentar, aunque sus conocimientos lingüísticos sean reducidos, lanzar una búsqueda en los sitios anglófonos. El problema principal es traducir de manera exacta el mensaje de error. Pongamos el ejemplo de un internauta que busca una solución para el siguiente error: "Explorer has stopped working".

Acceda a la Knowledge Base de Microsoft en español: http://support.microsoft.com/search/?
En el cuadro de texto **Búsqueda**, introduzca esta frase: *ha dejado de funcionar*.
Haga clic en la lupa a la derecha del cuadro de texto **Buscar**.

Una de las primeras páginas que encontrará es esta: "Qué hacer cuando Internet Explorer no funciona".

Haga clic en el enlace para acceder a esta página.
Haga clic con el botón derecho en esta página y seleccione el enlace **Traducir con Bing**.

El título de la página será: "What to do when Internet Explorer does not work".

Solo tendrá que lanzar esta búsqueda en Google: "What to do when Internet Explorer does not work". Si no encuentra ningún resultado, bastará con que elimine una o varias palabras. En nuestro ejemplo, la búsqueda adecuada es: "Internet Explorer does not work". Si retomamos la técnica vista anteriormente, podemos mejorar la búsqueda de esta manera: "Internet Explorer does not work inurl:(fix|solved)".

Si no encuentra una traducción exacta, traduzca las palabras clave presentes en el mensaje de error (sin intentar reconstruir la frase de manera coherente) y lance una búsqueda en Google, que retomará cada uno de estos términos. Si, por ejemplo, debe aceptar el acuerdo de licencia cada vez que inicia el programa Microsoft Office, tendrá que realizar una búsqueda en Google con las palabras clave: "Microsoft Office license every time". La primera página que aparece es un artículo de la Knowledge Base de Microsoft. Podrá traducir esta página al español pero, a menudo, no resulta comprensible.

Las webs anglófonas son mucho más numerosas que las páginas estrictamente en español por lo que, evidentemente, tendrá más posibilidades de encontrar una respuesta si recorre los sitios ingleses o estadounidenses. Un sitio que dispone de una multitud de soluciones sobre prácticamente todos los campos de la informática es el conocido como "Experts Exchange": http://www.experts-exchange.com

El único problema es que su acceso está condicionado a una participación en dinero contante y sonante (¡pero solo aparentemente!). El truco está en buscar en la página Web el tema y el mensaje que le interese. El sitio no le dejará ver las respuestas, sin embargo, puede copiar el título del asunto que desee leer y realizar una búsqueda en Google añadiendo al final: site:www.experts-exchange.com. De los resultados mostrados elija el que desee, pero pulse en el enlace **En caché**. Solo tendrá que utilizar la barra de desplazamiento para poder leer las soluciones del problema, justo debajo de los mensajes bloqueados.

# Configuración de su equipo

En esta parte del libro vamos a examinar todas las reglas básicas que necesitamos conocer antes de convertirnos en expertos informáticos.

## 1. Evitar los mensajes de error

A fin de limitar los avisos y mensajes de error enviados a Microsoft en caso de fallo del sistema, debe configurar las opciones de arranque y recuperación.

Desde el **Panel de control - Sistema y seguridad**, seleccione la sección **Sistema** y a continuación la opción **Configuración avanzada del sistema**.
En el apartado **Inicio y recuperación**, haga clic en el botón **Configuración**.
En el apartado **Error del sistema**, desactive las casillas **Grabar un evento en el registro del sistema** y **Reiniciar automáticamente**.

Haga clic dos veces en **Aceptar**.

Este último punto es especialmente importante: permite hacer que el sistema operativo muestre un mensaje de error (el más común es un error STOP) y evitar que se reinicie y no avise del problema de que se trata.

Limite igualmente los mensajes relativos a la seguridad y el mantenimiento del sistema.

La activación y desactivación de los mensajes relativos a la seguridad y al mantenimiento del sistema son gestionados por el centro Seguridad y mantenimiento. Puede acceder a este componente desde el **Panel de control** - **Sistema y seguridad** - **Seguridad y mantenimiento** y a continuación seleccione el enlace **Cambiar la configuración de seguridad y mantenimiento**.

## 2. Inicio de una comprobación de archivos

La herramienta del Comprobador de archivos de sistema SFC (*System File Checker*) es un componente del Sistema de protección de archivos WFP (*Windows File Protection*) que permite comprobar la integridad de las versiones de archivos presentes en el sistema. Vea a continuación la sintaxis del comando SFC:

**SFC [/SCANNOW] [/VERIFYONLY] [/SCANFILE=<archivo>] [/VERIFYFILE=<archivo>] [/OFFWINDIR=<directorio de Windows sin conexión> /OFFBOOTDIR=<directorio de inicio sin conexión>]**

- **/scannow**: examina la integridad de todos los archivos del sistema protegidos y repara los archivos dañados.
- **/verifyonly**: analiza la integridad de todos los archivos del sistema protegidos sin efectuar ningún tipo de reparación.
- **/scanfile**: analiza la integridad del archivo de referencia y repara los problemas identificados.
- **/verifyfile**: comprueba la integridad del archivo sin efectuar ningún tipo de reparación.

En los dos últimos casos, necesita especificar la ruta completa de acceso al archivo de destino. Por ejemplo:

**sfc /verifyfile=c:\windows\system32\kernel32.dll**.

Si no se detecta ningún problema, se le mostrará este tipo de mensaje: "Protección de recursos de Windows no encontró ninguna infracción de integridad".

- **/offbootdir**: cuando se realiza una reparación sin conexión, este modificador permite especificar el directorio de inicio.
- **/offwindir**: cuando se realiza una reparación sin conexión, este modificador permite definir la ubicación del directorio de Windows.

Le mostramos un ejemplo de comando: **sfc /scannow /offbootdir=c:\ /offwindir=h:\windows**

Tenga en cuenta que si inicia una comprobación completa del sistema, el proceso puede ser bastante largo.

Si no especifica la ruta de acceso del archivo, se encontrará con este tipo de error: "La protección de recursos de Windows no ha reconocido este archivo como archivo del sistema que pueda comprobarse y repararse. Compruebe la ruta de acceso al archivo y vuelva a comenzar".

## 3. La restauración del sistema

La restauración del sistema crea una imagen del mismo en un momento determinado. Si, después de un error, desea volver a un estado anterior, tan solo deberá acceder a esta herramienta y elegir un punto de restauración.

En Windows, la herramienta de restauración le permite proteger los datos mediante una función llamada "Shadow Copy" o "Instantáneas del sistema".

Ya hemos visto que con este método puede recuperar una versión de los archivos tal y como estaban guardados en el momento de la instantánea. Existen diferentes maneras de abrir la herramienta.

En el cuadro de texto **Iniciar búsqueda**, situado a la derecha del menú **Inicio** introduzca: **msconfig**.
Haga clic en la pestaña **Herramientas** y seleccione **Restaurar sistema**.
Haga clic en el botón **Iniciar**.

Otro modo: ejecutar directamente este comando: **`rstrui`**.

Seleccione el punto de restauración más adecuado.

Generalmente, se trata del más reciente y se creó automáticamente antes de la instalación de una revisión o de la desinstalación de un programa determinado.

Por supuesto, puede utilizar un punto de restauración más antiguo, pero deberá seleccionar uno anterior a la aparición del problema y, preferentemente, lo más reciente posible para evitar eliminar demasiados eventos ocurridos desde su creación. El resto del procedimiento no supone ningún problema. El sistema se reiniciará y el ordenador volverá al mismo estado que tenía en la fecha y hora del punto de restauración seleccionado. Es importante señalar que:

- Los documentos que ha creado después no serán ni destruidos ni modificados.
- Solo se restaurará la configuración del Registro de Windows.

Esta es la razón por la que este método puede ser eficaz para los problemas de Registro dañado o modificado (por un virus, por ejemplo).

Si después de efectuar una restauración del sistema el problema no se resuelve, puede intentar anular este punto de restauración o elegir otro punto diferente. Por defecto, se crea un punto de restauración antes de empezar el proceso de restauración del sistema.

Para crear de manera manual un punto de restauración, siga los siguientes pasos:

Haga clic en las teclas [Windows] + Pausa.
Haga clic en la pestaña **Protección del sistema** y el botón **Crear**.

Tenga en cuenta que, por defecto, esta funcionalidad está desactivada. Para activarla, para cada disco debe seleccionar el disco que desea proteger y a continuación hacer clic en el botón **Configurar**. De esta manera, las características de instantáneas de volumen se aplicarán también a los volúmenes en los que almacene los documentos. Esta es una precaución que debemos tomar antes de cualquier operación delicada o de la instalación de un programa un tanto exótico (¡pero no solo entonces!).

Para suprimir los puntos de restauración que se han creado:

Seleccione el disco del sistema y haga clic en el botón **Configurar**. Seleccione la opción **Desactivar la protección del sistema**.
Finalmente, haga clic en **Aplicar**.
Para volver a activarlo, marque de nuevo la casilla y haga clic en el botón **Aplicar**.
A continuación, haga clic en **Crear** y escriba un nombre descriptivo para este punto de restauración.

De manera predeterminada, el espacio utilizado de la unidad corresponde al 15% del espacio libre de cada partición seleccionada. Cuando sobrepasa el límite, se eliminará el punto de restauración más antiguo (según el método FIFO: el primero que entra es el primero que sale).

Es posible programar la creación automática de un punto de restauración de la siguiente manera:

Desde el Panel de control, en la sección **Sistema y seguridad** - **Herramientas administrativas**abra el **Programador de tareas**.
Localice y abra una tarea llamada "SR" (*System Restore*). Si abre el árbol **Biblioteca del programador de tareas/Microsoft/Windows/SystemRestore**. Para ello, abra el árbol Biblioteca del programador de tareas.

Verá que se han definido varios desencadenadores.

Para ello abra la pestaña **Desencadenadores**.

Puede modificar o crear un nuevo evento que desencadene la creación de un punto de restauración. También es posible cambiar el comportamiento de esta tarea programada y definir otras condiciones de inicio, parada o reanudación diferentes de las que aparecen por defecto.

Observe que la pestaña **Historial** le permite examinar todos los eventos ocurridos en las diferentes tareas iniciadas o los intentos de inicio. Para visualizar este historial, debe activar esta funcionalidad haciendo clic en el enlace **Habilitar el historial de todas la tareas** en el panel **Acciones** de la consola.

Puede ejecutar las tareas de manera manual haciendo clic en el enlace **Ejecutar**, y también puede exportar la información en formato XML, desactivarla o incluso eliminarla.

## 4. Utilidad de la herramienta de restauración del sistema

Los puntos de restauración se crean automáticamente en función de los desencadenadores siguientes:

- Instalación de un controlador no firmado.

- Instalación de una aplicación compatible con la herramienta de restauración del sistema y que ordenará al sistema que genere previamente la creación de un punto de restauración.
- Utilización de las actualizaciones de Windows Update.
- Cuando un usuario restaura el equipo a una fecha anterior.
- Cuando se realiza una restauración de datos que guardados mediante las herramientas integradas en Windows Vista.
- En función de un periodo definido en el Programador de tareas para la tarea llamada SR.

En principio, las áreas siguientes se restaurarán al estado en que se encontraban en el momento de crear el punto de restauración seleccionado:

- el Registro.
- los perfiles locales.
- las bases de datos COM+, IIS y WMI.
- los archivos protegidos del sistema operativo.

En la siguiente dirección, podemos encontrar una lista de los archivos examinados y eventualmente restaurados a su estado inicial: http://msdn.microsoft.com/es-es/library/aa378870(en-us).aspx

Estos elementos no se restauran:

- la configuración DRM.
- las contraseñas almacenadas en la base SAM o ActiveDirectory.
- los documentos personales.
- el contenido de carpetas redirigidas.

Finalmente, señalaremos que no se restauran los datos o entradas del Registro que aparecen en el siguiente árbol: HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Control\BackupRestore ni las claves siguientes:

- FilesNotToBackup
- FilesNotToSnapshot
- KeysNotToRestore

## 5. Cambio de la frecuencia de creación de puntos de restauración

Por defecto, Windows realiza un punto de restauración una vez al día (si no se expresa de otra manera en los desencadenadores). Usted puede cambiar esta frecuencia tanto desde el Editor de objetos de directiva de grupo como desde el Registro de Windows:

Abra HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\ CurrentVersion\SystemRestore.
Edite un valor DWORD llamado RPGlobalInterval.

El valor hexadecimal predeterminado es: 15180.

Seleccione el botón **Decimal**.

El siguiente valor que aparecerá será: **86400**. Se trata del número de segundos que hay en un periodo de 24 horas. Utilice la Calculadora de Windows para calcular un valor más corto o más largo.

## 6. Resolución de un problema en la restauración del sistema

Presentamos algunos errores comunes.

### Error 0x8007007B

**"Error inesperado: El nombre del archivo, directorio o etiqueta del volumen no es válido (0x8007007B) - Restaurar sistema se cerrará ahora":**

Es un problema que parece producirse en los equipos OEM (*Original Equipment Manufacturer*, es un término que designa a un fabricante de componentes de ordenadores) y que se debe a que la etiqueta del volumen no es válida.

Desde la sección **Sistema y seguridad - Sistema**, haga clic en **Protección del sistema**.
En la zona de unidades disponibles, si una unidad está marcada desactive la protección del sistema para esta unidad.

Otra causa posible de este error es que el lector que debe utilizar para la restauración del sistema esté inactivo. En ese caso, active el lector.

### Error 0x8007000E o 0xC00000EA

Este tipo de error se produce generalmente por la presencia de un programa residente de tipo antivirus o antispyware. Tan solo tendrá que desactivarlo durante el tiempo necesario para realizar una copia de seguridad. Compruebe si existe una versión actualizada de la aplicación problemática.

### Error 0x80071A91 o 8007000B

Este problema se debe a la presencia de un controlador RAID no compatible con Windows.

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando: **fsutil resource setautoreset true d:**

En este ejemplo, presuponemos que Windows está instalado en el disco D:\. Ese comando indica que los metadatos transaccionales se limpiarán la próxima vez que se monte.

Reinicie el ordenador.

### Error 0x80070005 - Acceso denegado

Este error se debe a que la partición de recuperación seleccionada no dispone de suficiente espacio. Tendrá que desmarcarla:

Pulse las teclas [Windows] + Pausa.
Haga clic en el enlace **Protección del sistema**.
Identifique la unidad que contiene la partición seleccionada y desactive la protección del sistema para esa unidad.

### No es posible restaurar por completo Windows mediante las herramientas WinRE

Esto supone que utiliza la herramienta BitLocker Drive Encryption y que WinRE está instalado en un volumen de inicio marcado como partición activa.

La única solución consiste en crear una nueva partición y proceder a realizar una copia de seguridad completa de la misma.

### Los componentes .NET Framework no se han restaurado correctamente después de una restauración completa

Cuando configure la restauración completa, asegúrese de realizar una copia de seguridad de los archivos y subcarpetas presentes en los directorios:

- %windir%\assembly
- %windir%\Microsoft.Net

### Error 0x80070057 en la creación de un disco de reparación del sistema

Este error generalmente se provoca por una corrupción del fichero de copia de seguridad cuando se ha cancelado o interrumpido.

La solución consiste en hacer una copia de seguridad de la partición del sistema en un disco externo.

### La función de restauración del sistema no funciona (0x800423F3 o 0x80070570)

Si encuentra este error, en primer lugar compruebe que está activada la opción de protección del sistema. A continuación puede desactivar su antivirus o intentar realizar esta operación de restauración en modo seguro.

También puede comprobar la integridad de su disco y reparar el sistema de ficheros a través de los comandos **sfc /scannow** y **chkdsk /f /r**.

Finalmente, compruebe que dispone de suficiente espacio en disco para esta operación.

Si con todas estas comprobaciones no puede resolver el problema, el error puede venir de una posible corrupción del servicio Windows Management Instrumentation.

En este caso, en un Símbolo del sistema en modo administrador, teclee el comando **net stop winmgmt**.
En el directorio **C:\Windows\System32\wbem**, renombre el directorio de referencia, por ejemplo, "oldrepository".
Reinicie el servicio.
Abra de nuevo un Símbolo del sistema en modo administrador, teclee el comando **net stop winmgmt** y a continuación **winmgmt /resetRepository**.
Reinicie el servicio.

## 7. Añadir un componente al Registro

Durante la instalación del sistema operativo, muchos archivos DLL o ejecutables se colocan en los directorios del sistema (principalmente en \Windows\System32). Para que estos archivos DLL puedan funcionar, registran la información en el Registro de Windows. A veces

ocurre que, aunque un archivo DLL no esté dañado, la información necesaria en el Registro está ausente o corrupta. En esos casos, deberá volver a registrarla. Regsvr32 permite registrar o eliminar el registro de un componente OLE como un archivo DLL o un control ActiveX.

La sintaxis del comando Regsvr32.exe es la siguiente:

**Regsvr32 [/u] [/n] [/i[:Línea_de_comando]] Nombre_del_archivo.dll**

- **/u**: llama al sistema API DllUnRegisterServer para eliminar el registro del archivo especificado.
- **/s**: se ejecuta en modo silencioso y, por lo tanto, no muestra ningún mensaje de confirmación.
- **/i**: llama a DllInstall y transfiere una línea de comandos opcional.
- **/n**: no llama al sistema API DllRegisterServer. Esta opción se debe utilizar con el parámetro /i.

Para algunos componentes COM, debe utilizar los sistemas API DllRegister y DllUnregister (/i o /i /u), mientras que para el resto de componentes COM y para los componentes WIN32, debe llamar a Dllinstall o DllUnistall (sin el modificador o mediante el indicador /u).

Un archivo DLL (*Dynamic Link Library* o biblioteca de vínculo dinámico) es un subprograma que contiene rutinas, instrucciones y funciones que permiten a las aplicaciones y al sistema operativo funcionar. Algunas desempeñan muchas tareas diferentes, mientras que otras son más especializadas.

Una API (*Application Programming Interface*) es una interfaz de programación que ofrece una serie de funciones, por así decirlo, "listas para ser usadas". Un componente COM (*Component Object Model*) es un modelo de objeto de los sistemas de Microsoft, sobre el que se apoya OLE. La tecnología OLE (*Object Linking and Embedding*) permite la vinculación e incrustación de objetos entre las diferentes aplicaciones y componentes del sistema operativo. Esto permite, por ejemplo, llamar a un dispositivo de digitalización desde una aplicación de Office.

En el caso de tratarse de archivos ejecutables, puede probar uno de estos comandos: **Nombre_del_ejecutable /unregister** o **/register**

Por ejemplo, para desactivar y volver a activar la función del reloj de Windows, introduzca, uno a uno, los siguientes comandos: **W32tm /unregister** y **W32tm /register**. Este último comando se ejecuta como servicio y añade la configuración de las entradas necesarias en el Registro.

Veamos un ejemplo de utilización que permite resolver un problema de Windows Update después de realizar la instalación o reparación de Windows XP. El problema surge porque algunos archivos ejecutables que se necesitan para la ejecución de Windows Update no están guardados correctamente en el Registro. Una solución consiste en registrarlos manualmente:

Abra una ventana de Símbolo del sistema.
Introduzca los siguientes comandos aceptando con la tecla [Intro] después de cada uno:

- **regsvr32 /s wuapi.dll**
- **regsvr32 /s wuaueng1.dll**
- **regsvr32 /s wuaueng.dll**
- **regsvr32 /s wucltui.dll**
- **regsvr32 /s wups2.dll**

- **regsvr32 /s wups.dll**
- **regsvr32 /s wuweb.dll**

Veamos otro ejemplo que nos muestra una manera rápida de reparar una aplicación Office:

Haga clic con el botón derecho en el menú **Inicio**, seleccione el comando **Ejecutar** e introduzca: **[Aplicación_ejecutable] /unregserver**
Pulse el botón **Aceptar** e introduzca: **[Aplicación_ejecutable] /regserver**

En el caso de Word, por ejemplo, el comando podrá ser: **winword /unregserver**. De este modo, eliminaremos la inscripción de Word en el registro. En general, nos parece más seguro desactivar una utilidad o componente de Windows antes de reactivarlos.

# Herramientas del sistema operativo

Windows dispone de diversas herramientas para reparar y monitorizar la actividad del sistema operativo. En este apartado veremos tres de las herramientas del sistema útiles para operaciones de reparación.

## 1. El Monitor de recursos

Con ayuda de esta herramienta, puede visualizar el funcionamiento en tiempo real de los recursos del sistema de su equipo, como por ejemplo, los procesos, la actividad del disco o la memoria utilizada, los módulos y descriptores vinculados a los procesos, así como las claves de registro o las bibliotecas dinámicas y ficheros DLL (*Dynamic Link Library*).

El Monitor de recursos completa la información del Administrador de tareas y permite ir más allá en el análisis de los recursos consumidos en el sistema.

Para lanzar el Monitor de recursos, escriba **resmon.exe** en la zona de búsqueda a la derecha del menú **Inicio** y pulse la tecla [Intro]. Puede visualizar igualmente el Monitor de recursos haciendo clic en el botón **Monitor de recursos...** del **Administrador de tareas** de Windows en la pestaña **Rendimiento**.

Para profundizar en el conocimiento del Monitor de recursos puede visualizar los servicios que se están ejecutando en su sistema.
En el **Monitor de recursos**, seleccione la pestaña **CPU** y a continuación haga clic en la sección **Servicios**. Puede hacer más grande la sección con el ratón para poder visualizar el máximo de servicios activos.
Seleccionando el proceso **svchost.exe (RPCSS)**, verá qué servicios se están ejecutando así como los descriptores asociados a este proceso crítico del sistema operativo. Este proceso es iniciado por el servicio RPC (llamada a procedimiento remoto) y utiliza numerosos descriptores, claves de registro y elementos del sistema.
En la sección **Módulos asociados** puede ver las bibliotecas dinámicas y ficheros DLL utilizados por los procesos svchost.exe (RPCSS).

En la pestaña **Memoria**, observe en modo gráfico la información de memoria física de su equipo. Se puede ver la memoria utilizada y la memoria disponible. El sistema pone en modo de espera una parte de la memoria disponible con el fin de asignar más rápidamente nuevos recursos a los programas que la necesiten.

Finalmente la pestaña **Red** permite visualizar los puertos de red en escucha en su sistema. Esto equivale al comando **netstat -a** ejecutable en el símbolo del sistema.

## 2. Monitor de rendimiento

Esta herramienta permite visualizar en tiempo real el rendimiento de su sistema, a nivel de hardware y de software, y grabar estos datos para un análisis posterior. El Monitor de rendimiento dispone por defecto de dos recopiladores de datos System Diagnostics (diagnóstico del sistema) y System Performance (rendimiento del sistema). A partir de esta herramienta, puede igualmente crear sus propios recopiladores de datos.

El Monitor de rendimiento utiliza los contadores de rendimiento de Windows y le permite definir sus propios recopiladores de datos, para poder personalizar su análisis.

Para lanzar el Monitor de rendimiento, teclee **perfmon.exe** en la zona de búsqueda a la derecha del menú **Inicio** y a continuación pulse la tecla [Intro].

Seleccione la herramienta **Monitor de rendimiento** en el nodo **Herramientas de supervisión**. El contador **% de tiempo de procesador** es el contador de rendimiento seleccionado por defecto.

Puede añadir contadores de rendimiento suplementarios haciendo clic derecho en la zona de visualización del Monitor de rendimiento y a continuación seleccionando la opción **Agregar contadores**.

Windows 10 y Windows 8 disponen de numerosos contadores de rendimiento para el análisis y la recopilación de datos de su sistema. Seleccione la opción **Mostrar descripción** para obtener una descripción detallada del contador de rendimiento seleccionado. También puede conectarse a un sistema remoto haciendo clic en el botón **Examinar**. En este caso seleccione en la red el ordenador remoto del que quiere visualizar los contadores de rendimiento.

Para visualizar y distinguir correctamente los datos de los dos contadores de rendimiento seleccionados, asegúrese del color y la escala definida para cada contador. Utilice preferentemente un color diferente. Se puede acceder a estos elementos desde las propiedades de los contadores de rendimiento.

El Monitor de rendimiento dispone por defecto de dos recopiladores de datos:

- **System Diagnostics (Diagnóstico del sistema)**
- **System Performance (Rendimiento del sistema)**

Utilice el recopilador de datos **System Diagnostics** para establecer un diagnóstico del sistema y obtener información detallada de su entorno.

En el nodo **Conjunto de recopiladores de datos - Sistema**, seleccione el recopilador de datos **System Diagnostics**.

En el menú **Acción**, seleccione la opción **Iniciar**. El proceso de recopilación de datos dura 60 segundos. Al final del proceso, puede acceder al informe de la recopilación de datos.

Se puede acceder a los datos del informe en forma de ficheros XML, almacenados en la carpeta **c:\PerfLogs\System\Diagnostics\<host-name>_<%fecha%>\%Nombre del informe%**.

Puede crear sus propios recopiladores de datos a partir de la plantilla de recopiladores de datos del sistema.

# Las opciones del menú de arranque

El menú de arranque de Windows aparece pulsando la tecla [F8] del teclado antes de la aparición de la pantalla de bienvenida. A menudo es indispensable apagar el ordenador completamente y volverlo a arrancar. Las diferentes opciones disponibles le permitirán acceder a la información y al Escritorio de Windows si el modo normal no está accesible. Por otra parte, en estos distintos modos, existe un número mínimo de servicios y no se inicia ninguna aplicación residente. En resumen, muchos controladores instalados se desactivan y ceden su lugar a los controladores de dispositivos genéricos de Windows. Se trata de un medio rápido de comprobar que su problema no sea producido por:

- Un servicio de Microsoft.
- Un servicio que no es de Microsoft.
- Un controlador de dispositivo dañado o incompatible.
- Una aplicación que se ejecuta como tarea en segundo plano cada vez que se abre el Escritorio de Windows (en modo normal).
- La presencia de un virus o spyware.

Observe que en Windows 10 o Windows 8 la tecla [F8] no está operativa si arranca desde un ordenador con un disco SSD. En este caso deberá iniciar desde el disco de instalación de Windows y seleccionar las opciones de reparación.

En los apartados siguientes solo expondremos las opciones indispensables o más interesantes para un posible procedimiento de reparación.

## 1. El modo seguro

Al iniciar el sistema operativo, se utilizan solo los servicios y controladores indispensables (ratón, monitor, teclado, dispositivos de almacenamiento, tarjeta gráfica estándar, servicios del sistema predeterminados y ninguna conexión de red). Cabe señalar que puede iniciar un proceso de grabación pero, en un principio, no será posible instalar o desinstalar una aplicación utilizando el paquete de instalación Windows Installer. Además, las conexiones de red y el acceso a Internet estarán desactivados.

Para forzar que el ordenador se inicie en modo seguro la siguiente vez:

En la zona de búsqueda a la derecha del menú **Inicio**, introduzca **msconfig**.
Haga clic en la pestaña **Arranque** y a continuación active la opción **Arranque a prueba de errores**. Haga clic en el botón **Aceptar**.

## 2. El modo seguro con funciones de red

Esta opción resulta interesante incluso si el equipo no está conectado a una red local. Por ejemplo, los usuarios de un "Livebox" o "Freebox" pueden utilizar este modo si desean acceder a Internet para actualizar el antivirus o el controlador de un dispositivo, ya que no es posible el inicio en modo normal. También es un buen método para realizar una comprobación del sistema mediante el antivirus o antispyware. De hecho, hay menos posibilidades de que un virus se haya cargado en la memoria y juegue al escondite con el programa antivirus (para así permanecer invisible para la aplicación).

Sin embargo, recuerde que el firewall de la conexión a Internet no estará activado y que los paquetes de instalación "Windows Installer" no funcionarán en este modo, por lo que será imposible eliminar o instalar las aplicaciones que utilicen este instalador.

## 3. El modo seguro con Símbolo del sistema

Vd. está en una pantalla de Símbolo del sistema. En otras palabras el shell explorer.exe se remplazará por el cmd.exe, pero puede abrir el Explorador de Windows de la siguiente manera:

Acceda al Administrador de tareas y haga clic **Archivo - Nueva tarea (Ejecutar...)**.
En el cuadro de texto **Abrir**, introduzca **explorer**, y haga clic en **Aceptar**.
Se encontrará en el modo seguro "normal".

## 4. Añadir los eventos de inicio al registro

En este modo, Windows guarda en un archivo llamado ntblog.txt una serie de controladores y servicios que se han cargado o no. Si no puede acceder a Windows, puede iniciarlo desde la consola de recuperación introduciendo el siguiente comando: **Type ntbtlog.txt**. Sin embargo, debemos señalar que la información que aparece es muy difícil de descifrar.

## 5. Última configuración válida conocida

Esta opción es útil en las circunstancias siguientes: después de la instalación de un nuevo dispositivo, de la actualización de un controlador, de la instalación de un programa que necesita crear uno o más servicios para poder funcionar, el sistema no se inicia con normalidad. Esto puede deberse a un antivirus, un software de geometría de discos o una aplicación de grabación capaz de emular una o más unidades virtuales.

En otras palabras, esto significa que, después de una modificación en la rama HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet, el sistema no puede arrancar con normalidad. La solución consistirá en arrancar Windows utilizando la configuración utilizada la última vez que arrancó con éxito. Esta es la operación que se realizará: el sistema de explotación restaurará la información contenida en uno de los conjuntos de copias de seguridad existentes en el árbol de Registro HKEY_LOCAL_MACHINE\SYSTEM (CurrentControlSet002, CurrentControlSet003, etc.).

Todos los cambios realizados en las demás claves de Registro se conservarán. Este es el límite de las herramientas, ya que, lógicamente, será posible iniciar en modo seguro y realizar una restauración del sistema; por tanto, utilice esta solución si ni siquiera es posible iniciar en modo seguro.

# Las herramientas de WinRE

Este modo de inicio desde un disco de Windows Vista le permitirá acceder a numerosas funciones de configuración y reparación. Veamos cómo abrir la Consola de recuperación en Windows Vista. Observe que este conjunto de herramientas ha sido rebautizado como Windows Recovery Environment o WinRE o Entorno de recuperación de Windows. Cada tecnología se basa en Windows PE (Entorno de Preinstalación de Windows es una versión básica del sistema operativo utilizada principalmente para fines de diagnóstico y reparación) y ofrece dos tipos de utilidades:

- Un diagnóstico automático que le permitirá reparar los problemas de arranque más corrientes.
- Una plataforma avanzada que le ofrece herramientas avanzadas de reparación.

Introduzca el disco de instalación de Windows 10 o Windows 8.

Si es necesario, acceda a la BIOS del equipo para configurar la secuencia de arranque.

Pulse cualquier tecla para iniciar desde el disco de Windows Vista.

- También puede pulsar la tecla [F8] para activar el modo de inicio avanzado que le permitirá iniciar desde el disco duro.
- Si pulsa la tecla [Esc], podrá iniciar una nueva instalación de Windows.

Tenga en cuenta que si no puede inicializar esta secuencia de arranque, es, sin duda, porque tiene un PC con disco duro SSD. En ese caso antes de cerrar su sesión, teclee en un Símbolo del sistema el siguiente comando: **shutdown /r /o**. El ordenador se reinicia en modo WinRE.

Windows cargará los archivos necesarios para la instalación y la ventana mostrará las opciones.

Haga clic en el botón **Reparar**.

WinRE le mostrará las cinco opciones posibles:

Seleccione la opción **Solucionar problemas** y se mostrará la siguiente pantalla:

Si selecciona la opción **Restablecer este equipo**, podrá restaurar los valores por defecto del sistema operativo para la configuración del ordenador y del usuario. Las aplicaciones también se eliminan, pero puede elegir si conserva sus archivos personales o no.

Si selecciona **Opciones avanzadas**, acederá a las herramientas de reparación de su instalacion Windows.

## 1. Reparación de inicio

Windows buscará los posibles problemas de inicio. Por ejemplo, puede encontrarse con un mensaje de error que indique que no es posible cargar la entrada seleccionada porque la aplicación está ausente o dañada.

En ese caso, haga clic en el enlace **Solucionar problemas**, a continuación en **Opciones avanzadas** y finalmente en **Reparación de inicio**.

La herramienta de reinicio del sistema buscará posibles problemas en el equipo.

Haga clic en el enlace que aparece para ver los detalles de diagnóstico y reparación.
Finalmente, haga clic en **Cerrar** y **Finalizar** para reiniciar el equipo.

La experiencia nos dice que esta operación puede ser útil en las circunstancias siguientes:

- Una entrada de Registro está dañada.
- Un archivo del sistema está dañado o no se encuentra.
- Un controlador de dispositivo está ausente o defectuoso.

## 2. Restaurar el sistema

Si selecciona esta opción, le aparecerá la ventana **Restaurar archivos y configuración del sistema**.

Haga clic en el botón **Siguiente** y seleccione un punto de restauración.

Haga clic dos veces en **Siguiente** y luego en **Finalizar**.

Se iniciará el proceso de restauración del sistema.

## 3. Restauración de la imagen de sistema

Retire el disco de Windows e inserte, si es necesario, el disco en el que ha efectuado una copia de seguridad completa. Haga clic en el botón correspondiente (**Copia de seguridad Complete PC**), en el asistente Estado y en la configuración de copia de seguridad.

Haga clic en la opción **Recuperación de la imagen de sistema**.

El sistema analizará los dispositivos de copia de seguridad. Puede elegir restaurar el sistema a partir de la última copia de seguridad del sistema o seleccionar una imagen del sistema a partir de un disco o de un soporte de copias de seguridad externo.

Seleccione la opción **Utilizar la última imagen de sistema (recomendado)**. Haga clic en el botón **Siguiente**.
Puede elegir formatear el disco antes de proceder a la restauración de la imagen del sistema. Haga clic en el botón **Siguiente**.
Haga clic en el botón **Finalizar**.
Seleccione la casilla **Confirmo que deseo borrar todos los datos existentes y restaurar el respaldo** y haga clic en **Aceptar**.

El proceso de "Restauración integral del equipo Windows" se lanzará. Una vez que la operación de copia de seguridad haya terminado, el equipo se reiniciará.

## 4. Símbolo del sistema

Cuando haga clic en esta opción, se abrirá una ventana de Símbolo del sistema. El prompt le mostrará lo siguiente: **X:\windows\system32>** y se creará una unidad virtual.

Desde ese momento, podrá utilizar los diferentes comandos y acceder a los datos existentes en el disco duro o memoria USB. Una de las herramientas que podemos lanzar es el Regedit. Aquí le mostramos un ejemplo:

Abra el Editor de Registro mediante el comando **regedit** y seleccione la clave HKEY_USERS.
Haga clic en **Archivo - Cargar subárbol**.

También se puede hacer mediante los comandos: **File - Load Hive**.

Abra \Windows\System32\Config y seleccione el archivo *Security*.

En el cuadro de texto **Nombre**: introduzca el título que va a darle al archivo de subárbol temporal: "Prueba".

Una rama llamada *Prueba* se creará debajo de la clave HKEY_USERS.

Abra este nuevo árbol y edite la entrada que quiera modificar.

Por ejemplo, puede ser un valor binario presente en la clave Policy\ Accounts\ S-1-5-32-544\Privilgs para modificar los permisos adquiridos del grupo de administradores.

Una vez que se han validado los cambios, seleccione otra vez la clave "Prueba".

Haga clic en **Archivo - Descargar subárbol** (o **File - Unload hive**).

Pulse el botón **Sí** para aceptar la pregunta sobre si quiere descargar la clave con todas sus subclaves.

También es posible utilizar estos tres comandos para realizar una reparación:

- **Bootrec**: permite recuperar las estructuras de una unidad que tiene dañado el sector de inicio.
- **Bcdedit**: permite modificar el almacén de datos de configuración de inicio.
- **Diskpart**: permite redimensionar las particiones existentes.

Los demás ejecutables que se pueden lanzar (incluido el Bloc de notas de Windows), se encuentran en una lista en X:\Windows\System32. En caso de que no sea así, aparecerá un mensaje de error indicándole, por ejemplo, que la clase COM+ no está registrada.

## 5. Acceso a los datos utilizando las herramientas de WinRE

Una vez haya reiniciado desde el DVD-ROM de instalación de Windows, haga clic en las opciones **Solucionar problemas** - **Opciones avanzadas** y acceda en el modo Símbolo del sistema.

Utilice el comando cd, para ir a este directorio: C:\Windows\System32.

Para iniciar el Explorador de Windows deberemos usar este truco:

Introduzca este comando: **notepad.exe**.
A continuación, haga clic en **Archivo - Abrir** (o **File - Open**).

En la lista desplegable **Tipo**, seleccione la opción **Todos los archivos**.

Se encontrará en una pequeña ventana del Explorador de Windows.

Utilice ahora los menús contextuales disponibles para guardar los documentos más importantes, por ejemplo, en una memoria USB. ¡No es demasiado práctico, pero permite evitar estragos!

## 6. La herramienta de reparación del sistema

Esta herramienta, a la que se puede acceder en las opciones avanzadas de las herramientas de reparación de WinRE, se debe utilizar si su ordenador no arranca. Haga clic en esta opción y reinicie el ordenador. WinRE ejecuta ahora una herramienta de diagnóstico y de reparación automática del sistema operativo. Deje que la herramienta trabaje para que se reparen los errores que impiden el correcto arranque de Windows.

## 7. Configuración de inicio

Si hace clic en esta opción, accederá a una primera pantalla de descripción de las opciones de arranque. Haga clic en el botón **Reiniciar**.

A continuación accederá al menú de selección del modo de arranque del sistema operativo. Seleccione la opción que desee con la teclas [F1] a [F10].

# Las soluciones especializadas

En esta parte del libro, agruparemos diferentes tipos de soluciones que le permitirán resolver problemas en apariencia complicados. Todos ellos tienen un punto en común: los cambios que describimos requieren de atención y mucha metodología. Estas soluciones se han comprobado cientos de veces y todas ellas son eficaces.

## 1. Procedimiento de reparación genérico

Si después de la instalación de un nuevo dispositivo o un nuevo programa no puede acceder a Windows, reinicie en modo WinRE y a continuación utilice la herramienta de retauración del sistema.

Si puede iniciar o trabajar en modo seguro, en un principio, el problema se debe al software: un controlador de dispositivo que debemos actualizar, un programa que debemos desinstalar o actualizar, o incluso desactivar mediante el Editor de configuración del sistema.

En los demás casos, generalmente se debe a un problema físico: la actualización de la BIOS, su configuración con las opciones predeterminadas o la comprobación de cada componente presente en el equipo (módulos de memoria, procesador, placa base, tarjetas PCI o AGP, dispositivos de almacenamiento y lectura, etc.).

Los errores STOP pueden ir seguidos del nombre de un archivo. Inicie una búsqueda de ese archivo y acceda a sus propiedades. La información que figura ahí le permitirá ver si el archivo causante del problema forma parte del sistema operativo de Windows o si está ligado a un programa o a un controlador de dispositivo. En este último caso, desactive el dispositivo, desinstale el programa, o mejor aún, actualícelo.

En el administrador de dispositivos, desactive uno por uno los dispositivos que considere sospechosos.

Respete el siguiente orden: puertos, módem y categorías añadidas (módem PCI, por ejemplo), adaptadores de red, dispositivos de sonido, vídeo y juegos, dispositivos USB, infrarrojos. Una vez que haya identificado el dispositivo defectuoso, solo tendrá que realizar una actualización del mismo (y eliminar el perfil de hardware que ha creado).

Si su problema ocurrió por la actualización de uno de los dispositivos, deberá volver a la versión anterior del controlador.

## 2. Crear un disco de reparación del sistema

Esta opción de Windows permite crear un disco de reparación del sistema con las funcionalidades WinRe si no conserva el disco de instalación de Windows. Con este disco podrá reparar su instalación a partir de los puntos de restauración del sistema.

Desde un Símbolo del sistema en modo Administrador, utilice el comando **sdclt.exe**. Seleccione el disco de destino, en este caso el lector **E:**. Haga clic en el botón **Siguiente**.

Al final de la creación del disco, haga clic en **Cerrar** y en el botón **OK**. El disco de reparación del sistema está preparado.

En caso de tener algún problema, arranque su equipo con el disco de reparación para poder acceder a las herramientas WinRE.

Observe que puede hacer una copia de seguridad completa de su disco en forma de fichero .vhd a través del comando **wbadmin** o a través del asistente del **Panel de control**.

## 3. Restablecer la configuración de seguridad a los valores predeterminados

Esta operación puede, por ejemplo, ayudarle a resolver un error de Windows Update 0x8007f004 (Derechos insuficientes) o un problema de acceso a un recurso compartido en una red local. Antes de realizar cualquier tipo de modificación, tenga cuidado de crear un punto de restauración del sistema. Los modificadores para el comando **Secedit** son los siguientes:

- **/configure**: el archivo *Secedit.exe* deberá definir la configuración de seguridad del sistema.
- **/DB Nombre_de_archivo**: indica la ruta de una base de datos que contiene la plantilla de seguridad que debe aplicar. Aunque es obligatorio especificar el nombre de archivo, el archivo de base de datos puede no existir.
- **/CFG Nombre_de_archivo**: la ruta de la plantilla de seguridad se importará a la base de datos y posteriormente se aplicará al sistema. Si no especifica el nombre del archivo, la plantilla que ya está almacenada en la base de datos será la que se aplique. Este comando solo es posible si utiliza el modificador **/DB**.
- **/overwrite**: indica si la plantilla de seguridad establecida después del modificador **/CFG**reemplaza la plantilla almacenada en la base de datos, en vez de añadir los resultados en la misma plantilla (es la opción predeterminada). Este comando solo es posible si utiliza el modificador **/DB**.
- **/areas Áreas_de_seguridad**: define las áreas de seguridad que se deben aplicar.

Los valores permitidos son los siguientes:

- **SECURITYPOLICY**: directivas de cuentas y asignación de permisos de usuarios.
- **GROUP_MGMT**: configuración de restricciones para grupos específicos de la plantilla de seguridad.
- **USER_RIGHTS**: autorización de inicio de sesión del usuario y concesión de permisos.
- **REGKEYS**: plantillas de seguridad para las claves locales del Registro.
- **FILESTORE**: seguridad para el almacenamiento local de archivos.
- **SERVICES**: seguridad de todos los servicios establecidos.

Estos son los otros modificadores:

- **/log Ruta_del_archivo_de_Registro**: permite determinar la ubicación del archivo de Registro que muestra la lista de modificaciones.
- **/verbose**: permite mostrar información más detallada.
- **/quiet**: reduce el volumen de información que se muestra así como la información añadida en el archivo de registro.

Debe ejecutar **Secedit** desde el Símbolo del sistema.

Por ejemplo, para configurar los parámetros originales de las directivas de cuentas de usuario, introduzca el siguiente comando:

```
Secedit /configure /cfg %windir%\repair\secsetup.inf
/db secsetup.sdb /areas securitypolicy /verbose
```

La lista de entradas del Registro que se hayan modificado se mostrará si editamos el archivo *Scesrv.log*ubicado en \WINDOWS\security\logs.

La configuración de los permisos de usuario se ejecuta si introducimos el siguiente comando:

```
Secedit /configure /cfg %windir%\repair\secsetup.inf /db
secsetup.sdb /areas user_rights /verbose
```

Puede restablecer los permisos establecidos en el registro mediante este comando:

```
Secedit /configure /cfg %windir%\repair\secsetup.inf /db
secsetup.sdb /areas regkeys /verbose
```

La configuración de permisos relacionados con los archivos y carpetas se puede efectuar mediante el comando:

```
Secedit /configure /cfg %windir%\repair\secsetup.inf /db
secsetup.sdb /areas filestore /verbose
```

A continuación le mostramos un ejemplo práctico: no es posible iniciar una sesión interactiva en un equipo servidor. Este problema se debe a que una directiva local de seguridad está dañada. Tiene dos soluciones:

Cree un script de inicio utilizando **Secedit** para que pueda reiniciar la configuración de seguridad predeterminada.

Utilice la herramienta **Psexec** (que se puede descargar de esta dirección: http://technet.microsoft.com/es-es/sysinternals/bb897553.aspx) y **Secedit** para ejecutar este tipo de comandos:

```
psExec \\Nombre_servidor -u Nombre_Administrador -p Contraseña
secedit /configure /cfg %windir%\repair\secsetup.inf /db
secsetup.sdb /areas user_rights /verbose
```

## 4. Reparar los permisos NTFS en el Registro de Windows

Esta solución le permitirá, por ejemplo, resolver los siguientes problemas:

- Varios cuadros de diálogo están vacíos.
- Existen fallos únicamente en una de las cuentas de usuario.
- El Reproductor Windows Media no puede abrirse.
- Es imposible definir un reproductor como el programa predeterminado.
- Los archivos EXE no se reconocen.
- Los programas que utilizan Windows Installer no se pueden instalar correctamente (Código de error n°10 o mensaje del tipo "Acceso denegado").

- Tiene errores del tipo "código 5" o "0x5" o 0x80070005".
- Algunos parámetros de la Barra de tareas no se memorizan.
- Las asociaciones de archivos no funcionan.

Puede resolver este problema fácilmente utilizando una herramienta llamada SubInAcl que se puede descargar directamente desde: http://www.microsoft.com/en-us/download/details.aspx?id=23510

A continuación, realice la instalación del archivo MSI. SubInACL.exe es una herramienta del Símbolo del sistema que le permite modificar el conjunto de permisos NTFS de los archivos, carpetas, claves de Registro y servicios.

Cree un nuevo documento llamado *registro.cmd* (el nombre no es importante).

El único punto indispensable es que este archivo debe tener una extensión *.cmd* (o *.bat*). Para facilitarle la tarea, guárdelo en el mismo directorio que donde se encuentra "SubInACL".

Copie el contenido siguiente:

```
subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=administrators=f

subinacl /subkeyreg HKEY_CURRENT_USER /grant=administrators=f

subinacl /subkeyreg HKEY_CLASSES_ROOT /grant=administrators=f

subinacl /subdirectories %SystemDrive% /grant=administrators=f

subinacl /subkeyreg HKEY_LOCAL_MACHINE /grant=system=f

subinacl /subkeyreg HKEY_CURRENT_USER /grant=system=f

subinacl /subkeyreg HKEY_CLASSES_ROOT /grant=system=f

subinacl /subdirectories %SystemDrive% /grant=system=f
```

Abra una ventana de Símbolo del sistema.
Mediante el comando **cd**, desplácese en el directorio que contiene el archivo del comando.
Introduzca: **registro.cmd**.

Espere algunos minutos antes de iniciar el equipo.

CAPÍTULO 7. Los dispositivos

# El Administrador de dispositivos

Todos los componentes de hardware que están instalados en el equipo aparecen en el Administrador de dispositivos.

Acceda a las propiedades del sistema seleccionando el vínculo **Sistema** desde la sección **Sistema y seguridad** del **Panel de control**.

En Windows 10 y Windows 8, puede acceder al Panel de control desde el escritorio Windows.

En la ventana de **Propiedades del sistema**, haga clic en **Hardware** y luego en el botón **Administrador de dispositivos**.

También puede ejecutar el comando **devmgmt.msc** o utilizar un método abreviado de teclado [Windows] + [Pausa]. Los dispositivos se agrupan en familias. Por ejemplo, la rama **Adaptadores de red** contiene el conjunto de componentes de red que están instalados en la máquina.

Para hacer que se muestren todos los componentes, haga clic en **Ver - Mostrar dispositivos ocultos**.

Si hace doble clic sobre ellos, accederá a la ventana de propiedades. Después haga clic en la pestaña **Controlador** y en el botón **Detalles del controlador**. De esta manera, podrá ver los archivos del sistema que están instalados con ese componente.

## 1. Los controladores de dispositivos

Un controlador de dispositivos es un programa que permite instalar un componente de hardware o dispositivo para que el sistema operativo pueda comunicarse con él. Un controlador es específico de un tipo de hardware y varía en función del sistema operativo en el que se utiliza. Hablaremos, por ejemplo, de un controlador para un adaptador de red vendido por tal fabricante y de un modelo determinado compatible o no con Windows. Un controlador no tiene nada que ver con el posible abanico de aplicaciones que acompaña a uno u otro dispositivo.

Una impresora 3 en 1 necesita un controlador para funcionar, pero el programa que le permite lanzar la impresión formará parte de otro programa distinto. La instalación del controlador se inicia desde la información contenida en un archivo INF. Todos estos archivos están almacenados en esta ubicación del Explorador de Windows C:\WINDOWS\inf. Este tipo de archivo tiene una extensión *.inf* (de "Setup Information file") y normalmente se pueden instalar de dos maneras:

- Existe un archivo INF en el equipo y, en el momento de la instalación, el sistema lo detecta automáticamente. A veces ocurre que debemos indicarle la ubicación de forma manual.
- El controlador contiene un "Instalador": solo tendrá que hacer doble clic en un archivo llamado *Setup.exe* o *Install.exe* para iniciar su instalación.

## 2. Cómo identificar un dispositivo

Existen dos conceptos importantes: el ID del dispositivo y el GUID de clase de dispositivo.

Cada fabricante de componentes y cada dispositivo poseen identificadores únicos (ID). Podemos encontrar estos dos valores de la siguiente manera:

Acceda al Administrador de dispositivos.
Haga clic con el botón secundario del ratón en uno de los dispositivos existentes en una de las ramas de dispositivos y haga clic en el submenú **Propiedades**.
Haga clic en la pestaña **Detalles**.
En la lista desplegable **Propiedad**, seleccione la opción **Id. de hardware**.

La información que aparece le indicará el ID del proveedor y del hardware.

El segundo concepto:

El GUID (*Globally Unique IDentifier*) de clase de dispositivo es un identificador en forma de clave única de CLSID que define una clase de dispositivo. Abra en el Registro el siguiente árbol: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum.

Cada subclave lista una clase de dispositivos. En el interior, puede encontrar la correspondencia entre el nombre de la clase de dispositivos y el GUID abriendo el contenido de estos dos valores de cadena: Class y ClassGUID. Por ejemplo, la clave Display contiene una subclave que representa la marca de la pantalla del equipo (SAM00C8 para una pantalla de la marca Samsung).

Si abre la subclave que representa la instancia del dispositivo (4&39fc21a&0&UID0), verá dos datos del valor: Monitor y {4d36e96e-e325-11ce-bfc1-08002be10318}. Se trata del nombre corto de la clase de dispositivos y del GUID de la clase de dispositivo, respectivamente.

Podemos encontrar esta misma información siguiendo estos pasos:

En el Administrador de dispositivos, abra la rama **Monitores** y haga doble clic en el nombre de la pantalla.
Haga clic en la pestaña **Detalles**.

En la lista desplegable, seleccione las opciones **GUID de clase de dispositivos**, **Nombre corto de clase**, **Id. de hardware**, **Ruta de acceso a la instancia del dispositivo**, etc. Tenga en cuenta que se mezclan muchos fabricantes y que hay algo de confusión en los valores que aparecen.

## 3. Dispositivo desconocido en el Administrador de dispositivos

Esta es una manera simple de identificar un dispositivo desconocido:

Como se ha explicado anteriormente, active la pestaña **Detalles** en el Administrador de dispositivos.
Acceda a las propiedades del dispositivo que señala el error (en nuestro ejemplo, la tarjeta de sonido).
Seleccione la opción **Id. del dispositivo coincidente**.

Se mostrará la siguiente información: pci\ven_10&dev_0059.

- El número de identificación del fabricante es: 10.
- El número de identificación del modelo es: 59.

Lance una búsqueda con estos números de identificación en el sitio PCIDatabase en la siguiente dirección http://www.pcidatabase.com

En el cuadro de texto **Vendor Search:**, introduzca el "Vendor ID": 10.
En el cuadro de texto **Device Search:**, teclee el "Device ID": 0059.

El modelo de la tarjeta es este: nForce Audio Controller (Nvidia).

Encontrar un controlador adecuado en Internet es difícil, porque deberá conocer exactamente el modelo y las características del chipset de la placa base para dar con el controlador correcto para la tarjeta de sonido. Una vez descargado el controlador, solo tendrá que lanzar su instalación.

Otra forma de obtener información detallada sobre uno o varios dispositivos desconocidos consiste en instalar un software de análisis e identificación de los componentes como, por ejemplo, la solución SiSoft Sandra 2015 que dispone de una versión de evaluación. Esta solución está disponible en la web del fabricante: http://www.sisoftware.net

## 4. Actualización del chipset de la placa base

Un controlador de chipset siempre actualizado le ayudará a resolver muchos problemas relacionados con el funcionamiento de los dispositivos. Existen diferentes fabricantes de chipsets y cada uno de ellos ofrece su propio programa de actualización. Le mostramos los más extendidos, así como la dirección web de los diferentes fabricantes:

- Para los chipset Nvidia: http://www.nvidia.es/page/home.html

En la sección de **Búsqueda manual**, seleccione la opción **Tipo de producto "GeForce"**, la serie correspondiente a su placa y finalmente el sistema operativo.

- Para los chipsets SIS: http://download.sis.com
- Para los chipsets AMD: http://support.amd.com/es-xl/download
- Para los chipsets Intel: http://downloadcenter.intel.com/default.aspx?lang=spa&iid=gg_work-ES+downloads

  Seleccione la familia, la línea y finalmente el producto correspondiente a su placa base.
- Para los chipsets VIA: http://www.via.com.tw/en/resources/download-center/chipsets/

En caso de tener un problema con los puertos USB, elija el submenú correspondiente.

Para identificar el modelo de chipset antes de actualizarlo, siga las siguientes instrucciones:

En el Administrador de dispositivos, abra la rama **Controladores ATA/ATAPI IDE**.
Haga doble clic en **Controlador IDE Bus Master** o en el chipset SATA de su ordenador.
En la pestaña **General**, frente a la mención **Fabricante**, se indicará el nombre del autor del chipset de la placa base.

En nuestro ejemplo, veremos que se trata de: **Via Technologies, Inc**.

## 5. Instalar un dispositivo

En Windows, la detección de dispositivos se realiza mediante Plug and Play. En otras palabras, cuando conecta el dispositivo el sistema le indica inmediatamente que ha detectado un nuevo hardware. Se pueden dar dos casos: que el sistema tenga el controlador en la base de datos interna o que usted deba introducir el disquete o disco en el que se encuentra el controlador del dispositivo. Además pueden ocurrir dos situaciones: el sistema puede encontrar de manera automática el controlador apropiado y la instalación se realizará sin

ninguna molestia, o deberá indicar manualmente la ubicación del controlador (el archivo INF).

Casi siempre, un mensaje de error le indicará que el controlador no tiene firma digital. Con toda tranquilidad, acepte este mensaje e inicie la instalación del controlador "no certificado".

Observe que desde el menú contextual de cada uno de los componentes de hardware que aparecen en la lista del Administrador de dispositivos, puede:

- Desinstalar el controlador.
- Actualizar el controlador.
- Volver a la versión anterior de un controlador.

# Problemas con los dispositivos

Le mostramos algunos ejemplos concretos relacionados con problemas de dispositivos en Windows 8 y Windows 10.

## 1. Error 2738

Este problema puede surgir, por ejemplo, cuando instala un escáner HP. El archivo de ayuda del fabricante le aconsejará instalar los componentes de Windows Script 5.6. Estos ya están incluidos en Windows 8, por lo que no podrá descargar otra versión compatible con Windows 8. El problema proviene de que un archivo DLL no está registrado correctamente en el Registro de Windows. Bastará con que siga las siguientes instrucciones:

Ejecute el Símbolo del sistema como administrador.
Introduzca el siguiente comando: **regsvr32 vbscript.dll**.

## 2. Código de error 0x80070643

Este código de error aparece en Windows 8 cuando intenta agregar un dispositivo de red Wi-Fi a través del asistente Agregar dispositivo.

Se pueden identificar diferentes razones como origen del problema:

- Problema de conexión entre el dispositivo y la red Wi-Fi.
- Configuración errónea del periférico.
- El periférico está conectado a la red Wi-Fi, pero no recupera la dirección IP apropiada desde el servidor DHCP (*Dynamic Host Configuration Protocol*).
- El cortafuegos se ha configurado para bloquear los protocolos SSDP (UDP 1900) o WS-Discovery (TCP/UDP 3702).

Siga este procedimiento para arreglar el problema:

- Compruebe que el router Wi-Fi o el punto de acceso está operativo y funciona, abra el Explorador de Windows y visualice los elementos del nodo **Red**.
- Si aparece el periférico, está conectado a la red, puede volver a ejecutar el proceso de conexión del periférico a través del asistente **Agregar dispositivo**.
- Si el periférico no aparece, no está conectado a la red. Compruebe entonces los siguiente puntos:
    - En caso de configuración errónea, vuelva a poner el dispositivo en modo de asociación Wi-Fi (también llamado modo WPS (*Wireless Protected Setup*)). Si

después de esta operación, el dispositivo aparece en el Explorador de Windows, ejecute de nuevo el asistente **Agregar dispositivo**. No olvide especificar el perfil de red correcto en el asistente.

- Compruebe los parámetros del cortafuegos en el ordenador y router Wi-Fi o punto de acceso. Compruebe que los protocolos SSD (UDP 1900) y WS-Discovery (TCP/UDP 3702) no están bloqueados.
- Configure manualmente los parámetros Wi-Fi del dispositivo. Para más información sobre el procedimiento de configuración de los parámetros, consulte la documentación proporcionada con el dispositivo. Reinicie el dispositivo después del cambio de configuración.
- Si el dispositivo sigue sin detectarse, conéctelo a la red con un cable de red. En caso necesario, desactive el soporte Wi-Fi del periférico. Si este aparece en el Explorador de Windows, entonces el problema corresponde a la configuración Wi-Fi del periférico. Cambie la configuración de los parámetros Wi-Fi del periférico y reinicie el dispositivo.

# Los dispositivos USB

La instalación de un dispositivo USB (*Universal Serial Bus*) puede convertirse fácilmente en una carrera de obstáculos si no tiene algunas nociones básicas.

## 1. Instalación de un controlador USB

Existen dos métodos completamente incompatibles:

- No conecte el dispositivo USB antes de instalar el controlador. Introduzca el CD-ROM de instalación del software y los controladores y, una vez que haya terminado, reinicie el ordenador. La instalación continuará y, en un momento determinado, se le pedirá que conecte el dispositivo USB.
- Conecte el dispositivo USB antes de instalar el controlador. El sistema le indicará que se ha detectado un nuevo hardware. En ese momento, introduzca el CD-ROM o disquete con el controlador del dispositivo y siga las instrucciones.

Antes de instalar un dispositivo USB, deberá asegurarse de que tiene actualizado el controlador de chipset de la placa base.

## 2. Los puertos USB

En el Administrador de dispositivos, haga doble clic en el menú **Controladoras de bus serie universal** y en uno de los concentradores raíz USB.
Haga clic en la pestaña **Energía**.

El apartado **Información del controlador** indicará la batería total disponible por puerto (normalmente 500 mA). El apartado **Dispositivos conectados** indica el número de puertos disponibles.

Haga doble clic en uno de los controladores de host.
Abra la pestaña **Controlador** y pulse el botón **Detalles del controlador**.

Puede que aparezca este tipo de indicación de archivos del sistema: **usbuhci.sys** (para el USB1.1), **usbehci.sys** (para el USB2) y usbxhci (para USB 3).

Recuerde que esto también lo puede configurar en la BIOS.

## 3. Desconectar un dispositivo con seguridad

En Windows 7, las llaves USB utilizan una caché de escritura en el dispositivo o en Windows para tener mejor rendimiento de lectura/escritura. En Windows 8 y Windows 10, esta caché está desactivada por defecto. Esta funcionalidad permite retirar el dispositivo sin expulsarlo previamente. Esta directiva se puede desactivar en el Adminitrador de dispositivos, en la pestaña del dispositivo en cuestión.

El comando **%SystemRoot%\System32\RUNDLL32.EXE shell32.dll, Control_RunDLL hotplug.dll** (en **Iniciar - Ejecutar** o desde la línea de comandos) muestra la ventana **Quitar hardware de forma segura** al desconectar un dispositivo de almacenamiento extraíble.

Útil si alguna vez pierde el icono de notificación en la barra de tareas...

## 4. Utilización de ReadyBoost

Esta tecnología permite acelerar Windows 10 o Windows 8 utilizando la memoria flash disponible en una memoria USB o en una tarjeta de memoria. Necesita un mínimo de 256 MB de espacio libre, una velocidad de lectura de 2,5 MB/s en bloques de 4 KB y de 1,75 MB/s para la escritura en bloques de 512 KB. A pesar de las afirmaciones de algunos fabricantes, no existen muchas memorias USB de gama baja o media que estén diseñadas para utilizar la función "ReadyBoost". Deberá orientarse hacia productos etiquetados claramente como "Compatible con ReadyBoost".

Por último, señalemos que es mucho más interesante utilizar tarjetas de memoria con una tasa de transferencia superior a 20 MB/s.

Para activar ReadyBoost, abra el Explorador de Windows y seleccione la letra del lector de su llave.
Haga clic con el botón derecho en este lector y seleccione la opción **Propiedades**. En la pestaña **ReadyBoost**, active la opción **Usar este dispositivo**. Desplace el cursor para asignar **1 Gb** a la función ReadyBoost.

Haga clic en **Aceptar**.

# Problemas con los dispositivos USB

En los apartados siguientes, intentaremos realizar una vista general de los principales problemas que podemos encontrar a la hora de instalar un dispositivo USB en cualquier versión de Windows.

## 1. Un dispositivo USB de alta velocidad está conectado dentro de un concentrador USB que no es de alta velocidad

Esto puede indicar simplemente que su ordenador no posee puertos USB 2.0. Una solución consistiría en adquirir una tarjeta PCI USB 2.0. Por otra parte, la disponibilidad del USB 2.0 solo es posible desde Windows XP SP1 y posteriores. La versión de estos cuatro archivos: *Usbport.sys*, *Usbhub.sys*, *Hccoin.dll*, *Usbehci.sys* debe ser por lo menos: 5.1.2600.1106.

Los síntomas pueden ser muy variados: los dispositivos USB no funcionan después de haber suspendido el equipo; no es posible activar o salir de una hibernación; el ordenador se reinicia cuando salimos de una hibernación; aparece el error STOP 0x000000A anunciando como causa del mismo el archivo *Usbport.sys*, o el error STOP 0x0000007E con el archivo *Usbhub.sys* como causante; los dispositivos USB aparecen como desconocidos, etc.

Si está seguro de que su equipo está equipado con puertos USB 2.0, actualice el controlador del chipset.

Debemos señalar que todos los puertos USB de la placa base pueden no aceptar esta norma y que, por ejemplo, dos puertos USB frontales funcionarán con USB 2.0, mientras que los traseros solo serán compatibles con la norma más antigua. Otra solución consistiría en desactivar de manera selectiva dos de los cuatro puertos USB para reservarles todos los recursos disponibles de la placa base.

Esto también puede deberse a un problema de recursos en la placa base. En otras palabras, los dispositivos USB pueden admitir un máximo de 500 miliamperios por conexión. Si un dispositivo intenta utilizar una cantidad mayor, el equipo desactivará el puerto hasta que la alimentación del equipo vuelva a la normalidad. Si la placa base no administra suficiente energía para hacer funcionar varios dispositivos al mismo tiempo, deberá optar por comprar un concentrador USB autoalimentado en el que poder conectar los dispositivos USB.

Si tiene este problema después de la instalación de una tarjeta USB 2.0 PCI, intente cambiarla de ranura. Si aun así no funciona, cámbiela en su punto de venta.

## 2. Los dispositivos USB han dejado de reconocerse

También le puede aparecer un error relacionado con la energía de los puertos USB o puede que el equipo detecte el nuevo dispositivo como desconocido.

Acceda a la BIOS del equipo y desactive el conjunto de funciones de USB.

Esta opción estará disponible en un menú como **Integrated Peripherals** o **Advanced Chipset Features** y se llamará **Onboard USB Function** o **On Chip USB**.

Reinicie con normalidad y desinstale todos los programas relacionados con dispositivos USB mediante el módulo **Agregar o quitar programas** del Panel de control.
A continuación, acceda al Administrador de dispositivos.
Haga doble clic en la rama **Controladoras de bus serie universal USB**.
Haga clic con el botón secundario del ratón en el primer dispositivo de la lista y elija **Desinstalar**.
Realice la misma operación para cada uno de los dispositivos presentes en esta rama.

Es mejor empezar por los concentradores raíz.

Si es necesario, compruebe que no hay presencia de dispositivos USB en otras ramas. En caso contrario, deberá desinstalarlos.

Las ramas posibles son: **Dispositivos de imagen**, **Unidades de disco**, **Dispositivos de sonidos, vídeos y juegos**. Acuérdese de activar la vista de dispositivos ocultos mediante el menú **Ver - Mostrar dispositivos ocultos**.

Abra el Explorador de Windows y active la opción de mostrar archivos y carpetas ocultos.
A continuación, abra el siguiente árbol: C:\Windows\System32/config

Reemplace el archivo Drivers con el fichero equivalente del disco de instalación de Windows en modo WinRE.

Este archivo contiene una base de datos de los controladores ya instalados en el equipo. Por este motivo, si desinstala un controlador, se reinstalará automáticamente con la misma configuración. Esta operación impedirá la reinstalación automática de un mismo controlador que puede haberse quedado obsoleto o es incompatible con el sistema operativo.

Reinicie el equipo.
Reinicie de nuevo el ordenador para poder acceder a la BIOS.
Vuelva a activar el conjunto de funciones USB.
Reinicie con normalidad y reinstale los dispositivos.

## 3. Error al desinstalar el dispositivo. Puede que sea necesario para iniciar el equipo

También puede encontrarse con el siguiente mensaje: "No se puede desinstalar este dispositivo porque sus secundarios han rechazado la solicitud. Esto puede suceder si los dispositivos secundarios de dicho dispositivo son necesarios para iniciar el equipo". Le mostramos una manera sencilla de resolver el problema:

Acceda a las propiedades del dispositivo y haga clic en la pestaña **Detalles**.

Verá este tipo de indicación: USBSTOR\DISK&VEN_APPLE&PROD_IPOD &REV_1.62\000A27001AB3A192&0.

En el Registro de Windows, abra HKEY_LOCAL_MACHINE\SYSTEM\ CurrentControlSet\Enum\USBSTOR.
Abra la clave correspondiente a la primera indicación: Disk&Ven_Apple&Prod_Ipod&Rev_1.62.

En el interior aparecerá una subclave cuyo nombre puede parecerse al siguiente: 000A27001AB3A192&0.

Ábrala y compruebe el contenido del valor de cadena FriendlyName para asegurarse de que se encuentra en el árbol correcto del dispositivo.

Una vez realizado este último punto, elimine la clave principal: Disk&Ven_Apple&Prod_Ipod&Rev_1.62.

Si aparece un mensaje de este tipo: "Error al eliminar la clave - No es posible eliminar Disk&Ven_Apple&Prod_Ipod&Rev_1.62: error al intentar eliminar la clave", haga lo siguiente:

Con el botón secundario del ratón haga clic en el nombre de la clave y seleccione **Permisos...**.
Seleccione el grupo **Todos**, marque la casilla **Control total** en la columna **Permitir** y acepte los cambios.
Ahora elimine la clave resistente y reinicie el ordenador.

A pesar de lo que pudiera parecer, este tipo de operación es totalmente inofensiva. Puede utilizar las soluciones descritas en el apartado anterior y también las de este.

## 4. Diferentes dispositivos desconocidos en el Administrador de dispositivos

Intente detectar e instalar los controladores de este dispositivo a través del asistente de actualización de controladores si el problema es relativo a los controladores del dispositivo.

El problema puede estar vinculado a los permisos de las claves de registro que almacenan la información de configuración de los dispositivos.

Haga clic en **Inicio - Ejecutar** e introduzca: **regedit**.
Abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Enum.
Haga clic con el botón secundario del ratón en la clave **Enum** y seleccione **Permisos**.

Los permisos para el grupo **SYSTEM** deben ser los siguientes: **Leer** y **Control total**.

Los permisos para el grupo **Todos** deben ser los siguientes: **Leer**.

Si es preciso, realice las modificaciones necesarias.

En caso de ser necesario, y si no basta con reiniciar el equipo, los permisos para el grupo Administrador deben ser los mismos que los del grupo SYSTEM.

Haga clic en el botón **Opciones avanzadas**.
Marque la casilla **Reemplazar las entradas de permisos en todos los objetos secundarios...**.
Acepte el resto.

## 5. Reinstalar un dispositivo USB declarado como "Unknown Device"

Abra el Administrador de dispositivos, haga clic derecho en el dispositivo identificado como "**Unknown Device**" y seleccione la opción **Actualizar controlador**.
Seleccione la opción **Busque software de controlador en el equipo**.
En la zona de búsqueda de controladores, introduzca la carpeta **C:\WINDOWS\system32** y active la opción **Incluir subcarpetas**. Haga clic en el botón **Siguiente**.

Haga clic en **Cerrar** cuando acabe el proceso de actualización.

## 6. Problema en la detección de los dispositivos USB

Antes que nada, deberá realizar una actualización del controlador del chipset de la placa base y, si es preciso, ejecutar los parches disponibles para permitir una mejor administración de los puertos USB.

Si su problema está relacionado con una memoria USB o un soporte de almacenamiento extraíble, intente lo siguiente:

Con el botón secundario del ratón haga clic en el icono **Mi PC** y en el submenú **Administrar**.

Igualmente puede introducir el comando **diskmgmt.msc** en el cuadro de búsqueda a la derecha del menú **Inicio**.

Haga doble clic en la rama **Administración de discos**.

Con el botón secundario del ratón haga clic en la letra del soporte que aparece y luego en el submenú **Cambiar la letra y rutas de acceso de unidad...**.
Otórguele al lector una letra específica, siguiendo un orden alfabético.

Esta solución funciona si hay una letra de unidad que no aparece en la secuencia de todas las unidades. Por ejemplo, si tiene diferentes particiones que ocupan las letras C, D y E y una unidad de DVD o grabadora tiene asignada la letra G.

## 7. Dos pistas más para solucionar un problema de puertos USB

Existen dos tipos de cables USB: el de alta velocidad y el de baja velocidad. Los cables de baja velocidad se distinguen de los de alta velocidad, en primer lugar, por su blindaje. Si conecta un dispositivo de alta velocidad en un cable de baja velocidad, puede provocar una distorsión de las señales.

Antes de concluir demasiado pronto que se trata de un problema de hardware, no dude en comprobar los puertos USB de la placa base.

## 8. Un dispositivo USB impide el cierre de Windows

Compruebe siempre si existe alguna actualización disponible del controlador en la página web del fabricante. Si no es el caso, siga los siguientes pasos:

En el Administrador de dispositivos, haga doble clic en la rama **Controladoras de bus serie universal USB**.
En la lista de dispositivos que aparecen debajo, haga doble clic en uno de los controladores.
Haga clic en la pestaña **Administración de energía** y desmarque la casilla **Permitir que el equipo apague este dispositivo para ahorrar energía**.

Este truco hará que el sistema no tenga en cuenta el estado del dispositivo USB antes de entrar en modo hibernación. También funciona si tiene problemas al apagar el equipo cuando un dispositivo USB está conectado.

## 9. Desde la instalación de un Box es imposible instalar un dispositivo USB

Desinstale la conexión USB e instale el módem ADSL mediante una conexión Ethernet.
Desactive los controladores USB en la BIOS y vuelva a activarlos después de iniciar en modo seguro y desinstalar todo lo relacionado con los controladores y dispositivos USB en el Administrador de dispositivos.

También puede ser necesario desinstalar los programas relacionados con el dispositivo problemático mediante el módulo **Agregar o quitar programas** del Panel de control. La mayoría de las veces solo es posible si se inicia en modo "normal".

Instale los últimos controladores para el chipset de la placa base.
Si se le pregunta, instale también los controladores de filtro USB 1.0 o USB 2.0.

En resumen, realice una actualización completa de los controladores del chipset de la placa base.

Reinstale el dispositivo. En caso de una impresora multifunción Epson, por ejemplo, esta se reconocerá de manera inmediata.

### 10. Un dispositivo USB 2.0 aparece como un dispositivo USB 1.1

Esto se debe a un problema de hardware en la placa base. Deberá cambiarla.

### 11. Es imposible iniciar Windows si un disco duro externo está conectado vía USB

Esto puede ocurrir, por ejemplo, cuando se carga un servicio relacionado con un programa de grabación (Alcohol 120% y scsiaccess.exe). Utilice la herramienta de configuración del sistema para localizar la aplicación o el servicio culpables.

### 12. La capacidad de la llave USB no es correcta

Este problema se puede producir cuando la llave se ha conectado a un sistema operativo diferente de Windows.

Ejecute un Símbolo del sistema en modo administrador.
Ejecute el comando **diskpart**.
Muestre la lista de los discos introduciendo el comando **list disk**.
Una vez haya identificado su disco, introduzca el comando **select disk #**, remplazando # por el número de disco correspondiente a la llave.
Finalmente, introduzca el comando **clean**.

Formatee ahora la llave para que esté operativa.

## Los dispositivos Bluetooth

Como en el caso de los dispositivos USB, los dispositivos Bluetooth son particularmente sensibles a los problemas de conexión. La integración de este tipo de dispositivos necesita un mínimo de conocimientos.

### 1. Instalar un dispositivo Bluetooth

Antes de poder conectar un dispositivo Bluetooth a su ordenador hay dos puntos que hay que comprobar.

En primer lugar debe disponer de un adaptador Bluetooth. Si tiene un ordenador portátil, ya debe disponer de él. En caso contrario, puede utilizar un adaptador Bluetooth externo. En general, este tipo de adaptador se conecta a través de un puerto USB.

Una vez tiene conectado el adaptador, el sistema tiene que detectarlo, es decir, tiene que estar en modo visible. Este modo permitirá la detección de su dispositivo inalámbrico para sincronizarlo a su ordenador.

Tenga en cuenta que algunos dispositivos siempre están en modo visible. Por el contrario, otros dispositivos como, por ejemplo, los teléfonos móviles, el adaptador Bluetooth no están siempre en este modo de funcionamiento por razones de seguridad y para economizar la energía de la batería. En este tipo de dispositivos, debe activar el modo visible a través de la opción correspondiente en el menú del aparato o a través de una tecla de acceso directo rápido. La activación de este modo permite al adaptador emitir una señal que hace que sea detactable por otros dispositivos u ordenadores. Cuando se pueden detectar los dispositivos a sincronizar, puede iniciar la sincronización.

Para agregar un nuevo dispositivo, desde el **Panel de control**, en la sección **Hardware y sonido** -**Dispositivos e impresoras**, haga clic en la opción **Agregar un dispositivo**.

El ordenador detecta los dispositivos que están en modo visible. Si no detecta el dispositivo que desea agregar, asegúrese que tiene corriente y que está en modo visible. Una vez encontrado, haga clic en el dispositivo a instalar y a continuación haga clic en el botón **Siguiente**.

Algunos dispositivos, al hacer la primera conexión, piden que se introduzca un código de sincronización o contraseña. También puede acceder a los dispositivos a sincronizar desde la pantalla de configuración de Windows. Puede acceder a esta pantalla desde el menú **Inicio** de Windows 10.

## 2. Problemas con los dispositivos Bluetooth

### No se puede reconocer un dispositivo Bluetooth

Antes de todo, compruebe que el dispositivo que quiere conectar tiene corriente y que no es necesario sustituir las baterías. Compruebe también que el adaptador Bluetooth de su ordendor está conectado y que puede detectar el dispositivo.

Puede ocurrir que el ordenador no reconozca un dispositivo ya sincronizado anteriormente. En ese caso, elimine el dispositivo desde la sección **Hardware y sonido** - **Dispositivos e impresoras** del **Panel de control**. Reinstale el dispositivo.

### La conexión es lenta o el dispositivo se desconecta

Si encuentra este tipo de problema, en primer lugar asegúrese que su dispositivo no tenga interferencias con otro aparato. A continuación compruebe las pilas o el indicador de carga de baterías de su dispositivo.

Algunas veces hay que alejar el aparato del ordenador; es el caso, por ejemplo, de algunos ratones.

Desconecte otros dispositivos Bluetooth para comprobar que no hay problemas de compatibilidad con el receptor.

Si el problema aparece después de un periodo de funcionamiento correcto de la conexión con su dispositivo, pruebe a desconectar y volver a conectar su adaptador o receptor Bluetooth. Si es un adaptador interno, pruebe a desactivarlo y volver a activarlo.

# Resolver un problema de códecs

Es un tema cuestionado en todos los sistemas operativos Windows. Hacemos una primera recomendación: evite los "Packs de códecs". A menudo puede resultar una solución milagrosa pero, en la práctica, demuestra estar mal construida, ser pesada y provocar bastantes daños al sistema. Pero, en primer lugar, ¿qué es un códec? Un códec ("COmpresión" y "DEsCompresión") es un algoritmo de compresión de sonido o vídeo digital que permite de este modo codificar y descodificar una señal en un formato en concreto.

Desde Windows Vista, Microsoft ha introducido la tecnología Windows Media Foundation sustituyendo la tecnología DirectShow. De todos modos, esta tecnología sigue estando disponible en Windows por razones de compatibilidad ascendente.

Antes que nada, vamos a conocer qué son los formatos contenedores. De hecho, existe una diferencia entre códec y formato contenedor:

Un códec es un algoritmo de compresión que reduce el tamaño del flujo de audio y vídeo. Los formatos MPEG-1, MPEG-2, MPEG-4, Vorbis, DivX... son códecs.

Un formato contenedor tiene varios flujos de audio y/o vídeo ya codificados (AVI, Ogg, MOV, ASF, etc.). Así pues, los flujos contenedores pueden utilizar diferentes códecs. En un mundo ideal, se podría utilizar cualquier códec en todo tipo de formato contenedor, pero existen muchas incompatibilidades, descritas en esta página web: http://www.videolan.org/streaming-features.html

El proceso de lectura se desarrolla de la siguiente manera: el reproductor "desmultiplexará" el flujo impuesto. Esto consiste en desencriptar y en separar el flujo de audio y vídeo. Cada flujo se envía separado a los descodificadores que podrán entonces descomprimirlo.

Como ya hemos visto, los contenedores multimedia más comunes son AVI (*Audio Video Interleave*), MKV (Matroska), MP4 (MPEG-4) y OGM (Ogg Media).

Windows tiene por defecto muchos códecs. Para visualizarlos, tiene dos posibilidades.

La primera consiste en teclear el comando **msinfo32** desde un Símbolo del sistema. A continuación navegue hasta la sección **Componentes** - **Multimedia** - **Códecs de vídeo**.

El segundo método consiste en ejecutar el reproductor Windows Media y seguir los siguientes pasos:

Pulse la tecla [Alt] para que aparezca el menú.

En la sección **Ayuda**, haga clic en la opción **Acerca de Reproductor de Windows Media**.

A continuación haga clic en el enlace **Información de soporte técnico**.

Puede ver toda la información técnica del Reproductor Windows Media y sobre todo los códecs instalados por defecto.

La segunda etapa es sencilla de entender: si el Reproductor de Windows Media ahora pueden abrir el archivo multimedia y ver lo que hay dentro del mismo, tienen que ser capaces de descodificar y reproducir el contenido de vídeo y audio. Solo tendremos que buscar una solución de software que agrupe todos estos códecs y presente unas sólidas garantías de estabilidad. Descargue e instale ffdshow desde esta dirección: http://ffdshow-tryout.sourceforge.net. En el momento en que escribimos este libro, la última versión era la 1.3.4531 y funcionaba perfectamente con el Reproductor de Windows Media.

Durante el proceso de instalación, marque las casillas necesarias situadas frente a los formatos de vídeo que desea descodificar con ffdshow. A continuación, y en caso de duda, desde la pantalla de inicio de Windows 8 haga clic en el programa **Configuración del decodificador de vídeo**.

Un truco que le enseñamos: si la instalación de ffdshow no resuelve el problema, en la ventana de configuración del descodificador de vídeo, seleccione el enlace **DirectShow control**. Desplace el indicador en forma de regla de la opción **Merit: ffdshow default** hasta situarlo completamente a la derecha.

De esta manera, ffdshow tendrá prioridad sobre el resto de códecs que pueda haber en el equipo.

Finalmente, puede enfrentarse a la imposibilidad de leer un archivo multimedia porque uno de sus códecs esté defectuoso. En esos casos, es posible instalar una herramienta llamada Codec Tweak Tool que puede descargar desde esta dirección: http://www.freecodecs.com/download/codec_tweak_tool.htm

Haga clic en el enlace correspondiente a la última versión disponible que sea compatible con Windows 8.
Haga doble clic en el archivo ejecutable CodecTweakTool_602.exe

Haga clic en el botón **Fixes**. Deje las opciones seleccionadas por defecto y haga clic en el botón **Apply & Close**.

Si por el contrario, no conoce el códec que utiliza un fichero multimedia, puede utilizar la herramienta MediaInfo que puede descargar de la web: http://mediaarea.net/es/MediaInfo

Esta herramienta no tiene ninguna dificultad de instalación.

Le aparecerá a la vez la información sobre el contenedor, los códecs de audio y vídeo necesarios, los metadatos incluidos, así como una multitud de características técnicas sobre el archivo.

Un metadato es, en este contexto, un conjunto de propiedades genéricas que permiten describir un documento (autor, fecha, tamaño del archivo, copyright, vista preliminar, etc.).

Para finalizar, añadiremos que es muy normal que los archivos multimedia descargados desde sitios peer-to-peer estén simplemente dañados. En este caso, no se trata de un problema misterioso de códecs, sino más bien de un problema de datos corruptos.

CAPÍTULO 8. INTERNET Y MOVILIDAD

# Introducción a Internet Explorer

En este capítulo vamos a explicar algunas características esenciales de Internet Explorer. Por otra parte, mostraremos cómo utilizar Edge, el nuevo navegador de Microsoft, así como la tienda de aplicaciones Windows Store. A continuación, nos interesaremos por el funcionamiento del Firewall de Windows y aprenderemos algunas de las estrategias más adecuadas para deshacernos de un virus o spyware.

# El modo protegido en Internet Explorer

Debemos señalar que esta característica solo existe desde Windows Vista y es fuente de muchos problemas. Examinemos cada una de sus particularidades.

## 1. Los niveles de integridad

Existen cuatro niveles:

- **Sistema**: se aplica a los componentes del sistema y no a las aplicaciones.
- **Alto**: se aplica a los procesos que se ejecutan con privilegios de administrador.
- **Medio**: se aplica a los procesos que se ejecutan en el entorno predeterminado.
- **Bajo**: lo utiliza Internet Explorer y Windows Mail cuando se ejecutan en modo protegido.

El nivel de privilegios se puede modificar una vez iniciado el proceso. El aislamiento de privilegios en la interfaz de usuario provoca tres consecuencias:

- Cualquier objeto "asegurable" que se haya creado mediante un proceso heredará el mismo nivel de integridad que el del proceso principal.
- Un proceso no podrá acceder a un recurso cuyo nivel de integridad sea más elevado que el suyo propio.
- Un proceso no puede enviar una ventana de mensaje a un proceso de nivel de integridad más elevado.

## 2. Funcionamiento del modo protegido

El aislamiento de privilegios en la interfaz de usuarios (*User Interface Privilege Isolation* o UIPI) impide a los procesos utilizar las API de usuario en modo de integridad elevada. De este modo, no será posible la instalación silenciosa de programas o la modificación de datos confidenciales. Cuando se ejecuta Internet Explorer en modo protegido se le asigna un nivel de integridad bajo. Por este motivo, no puede pasar de las operaciones de escritura en objetos que poseen un nivel de integridad más elevado.

En modo protegido, Internet Explorer solo puede modificar los objetos ubicados en los siguientes directorios:

- \Usuarios\%USER PROFILE%
- \AppData\Local \Temporary Internet Files
- \AppData \Local \Temp
- \AppData \Local \History
- \%USER PROFILE%\Favorites
- \%USER PROFILE%\Cookies

El esquema de funcionamiento obedece este principio:

- Internet Explorer se abre en modo protegido.
- El mecanismo de integridad (UIPI) se activa de forma automática.
- Finalmente, la capa de compatibilidad de aplicaciones ("Compatibility Layer") proporcionará unos privilegios de usuario bajos que permiten el funcionamiento del navegador.

Esta capa de compatibilidad le permite interceptar los intentos de escritura en objetos con un nivel de integridad medio y los redirige hacia las ubicaciones de nivel de integridad bajo:

- \%userprofile%\APPData\Local\Microsoft\Windows\TemporaryInternet Files\Virtualized
- HKEY_CURRENT_USER\Software\Microsoft\InternetExplorer\Internet Registry

Mostramos un ejemplo de utilización de este mecanismo:

Abra una página de Internet.
Guarde la página en C:\Program Files.

Puede ver el siguiente mensaje que le indica que no tiene autorización para guardar el archivo en esa ubicación.

Se le indica que puede grabar el archivo en otra ubicación de nivel de integridad más débil.

Si desactiva el modo protegido y realiza la misma operación, la misma página se guardará, esta vez, en esta ubicación: C:\Usuarios\Nombre_de_usuario\ AppData\Local\VirtualStore\Program Files.

Esta última acción está relacionada con la capa de compatibilidad de las aplicaciones.

El modo protegido se activa en las siguientes zonas de seguridad: *Internet*, *Intranet Local* y *Sitios Restringidos*, pero se desactiva en las zonas *Sitios de confianza* y *Equipo local*.

## 3. Otras consecuencias del modo protegido

Internet Explorer incluye un mecanismo que impide que ningún código malicioso consiga comunicar o lanzar otro proceso. Por ejemplo, si una extensión del navegador intenta hacerlo, Internet Explorer le pedirá permiso antes de iniciar el proceso.

Si esta extensión posee su propio archivo ejecutable, podrá añadir una clave en el Registro que indique que el proceso es digno de confianza. El árbol de Registro que se modificará será el siguiente: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Low Rights\ ElevationPolicy.

En esta última clave, cree un nuevo GUID en el que añadirá estos tres valores:

- **AppName** (valor de cadena): nombre del archivo ejecutable.
- **AppPath** (valor de cadena): ubicación del archivo ejecutable.
- **Policy** (valor DWORD): la cifra 3 como información del valor.

Le aparecerá el mismo cuadro de diálogo cuando intente mover el contenido de una página web a otra aplicación. El mecanismo es idéntico al descrito anteriormente, con la única diferencia de que en este caso el árbol de registro correspondiente es: HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Low Rights\DragDrop.

## 4. Desactivación del modo protegido

Para desactivar el modo protegido, siga el siguiente procedimiento:

Haga clic en **Herramientas - Opciones de Internet**.

Seleccione la casilla **Seguridad**.
Desmarque la casilla **Activar Modo protegido (requiere reiniciar Internet Explorer)**.

Observe que puede realizar esto para cada una de las zonas con esta característica.

La barra de estado de Internet Explorer, debajo de la ventana del navegador, indica el estado de la protección. Existen otras circunstancias que provocarán la desactivación del modo protegido:

- La desactivación del control de cuentas de usuario comporta la desactivación del modo protegido.
- La ejecución de Internet Explorer en modo Administrador desactiva el modo protegido.
- Cuando se ejecuta Internet Explorer desde un archivo situado localmente en el disco. Esto no se aplicará si la página HTML se ha guardado en el disco pero proviene de la zona Internet.

Mostramos un resumen de casos particulares en los que el modo protegido no está activado:

- El control de cuentas de usuario ("UAC") está desactivado.
- Internet Explorer se ejecuta como Administrador.
- La página se ha guardado desde una zona de seguridad que ya se considera como protegida.
- El modo protegido no está activado para la zona de seguridad en cuestión.

## 5. Modo protegido mejorado

Esta nueva funcionalidad de Windows 8 permite añadir una capa de seguridad complementaria al modo protegido existente desde Internet Explorer 7. Esta capa de protección ofrece seguridad contra los programas y scripts maliciosos que se ejecutan desde Internet Explorer, limitando la exposición de recursos del sistema operativo y sus datos personales. Uno de los efectos visibles de esta capa de protección es el bloqueo de la ejecución de plug-ins no compatibles con el modo protegido mejorado, por ejemplo el plug-in Adobe Flash en el momento de la redacción de esta obra.

En Windows 8, el navegador por defecto es Internet Explorer 11. Este navegador dispone de dos modos de funcionamiento. Si se ejecuta desde la pantalla de inicio, es decir en modo Interfaz de Usuario, el modo protegido mejorado está activo por defecto. En este modo de funcionamiento, Internet Explorer 11 no permite la ejecución de plug-ins, de este forma el modo protegido mejorado influye un poco en la experiencia de usuario. Desafortunadamente, todavía hay numerosos sitios web que necesitan utilizar plug-ins. Para permitir la visualización de este tipo de sitios, ejecute su navegador en el Escritorio de Windows. En este modo de funcionamiento, se permite utilizar plug-ins o módulos complementarios. Si el plug-in es compatible con el modo protegido no habrá mensajes de error. Por el contrario, en caso en que el plug-in sea incompatible con el modo protegido, un mensaje de notificación le pedirá que desactive el modo protegido solo para el sitio que quiere visitar.

Para desactivar el modo protegido mejorado para un sitio web:

Desde el Escritorio Windows, navegue a un sitio que ejecute un módulo complementario no compatible con el modo protegido mejorado.
Un mensaje de notificación indica que se ha bloqueado la ejecución del módulo complementario identificado y no compatible con el modo protegido mejorado.
Haga clic en el botón **Desactivar** en la zona de notificación.

Para desactivar el modo protegido para el equipo:

Desde el Escritorio Windows, abra las opciones de Internet Explorer 11.
En la pestaña **Opciones avanzadas**, sección **Seguridad**, desactive la opción **Habilitar el modo protegido mejorado**.

# Resolución de un problema en Internet Explorer 11

En esta parte, explicaremos cómo aplicar las soluciones genéricas que permiten reparar Internet Explorer 11.

## 1. Problemas de conectividad de red en Internet Explorer 11

Lo primero que debe hacer es comprobar la configuración del firewall o del router. A modo de prueba, puede desactivarlos por un momento.

Compruebe que tiene acceso a los sitios conocidos de estas dos maneras:

En la barra de direcciones, introduzca: http://www.microsoft.com

También puede utilizar la IP del sitio: **23.205.103.238**.

Puede comprobarlo de la siguiente manera:

Abra una ventana de Símbolo del sistema.
Introduzca este comando: **ping www.microsoft.com**.

A la derecha del nombre del sitio le aparecerá esto entre corchetes: 23.205.103.238.

En la barra de direcciones de Internet Explorer, introduzca esta dirección: **23.205.103.238**.

Esta es una manera rápida de comprobar que no existe ningún problema con el funcionamiento de DHCP porque, en caso contrario, no se realizaría la traducción de una dirección IP. Sepa que esto puede deberse a un problema con los servidores de su proveedor de acceso: la señal ADSL puede ser excelente, pero si no se realiza la traducción de las direcciones DNS solo podrá acceder a un sitio introduciendo la dirección IP en la barra de direcciones del navegador.

También puede ocurrir que después de desinstalar un proveedor de acceso a Internet o un programa de protección, la pila de Winsock esté dañada.

Winsock (*WINdows SOCKet*) es una biblioteca dinámica de funciones DLL que permite la implantación del protocolo TCP/IP (*Transmission Control Protocol/Internet Protocol*). Todas las aplicaciones de correo y los navegadores utilizan Winsock. Un LSP (*Layered Service Provider*) es un controlador que sirve de interfaz entre los sockets de Windows y la capa de red. Muchos programas (así como muchos malware) instalan este tipo de controlador para poder comunicar con los servicios de red. Recordemos que un malware es un programa no deseado como puede ser un virus, un Troyano, etc.

Puede restablecer la pila de una manera muy simple:

Ejecute el Símbolo de sistema.
Introduzca estos comandos:

- **netsh winsock show catalog | more** (muestra la lista de LSP).

- **netsh winsock reset catalog** (elimina todos los LSP ajenos).
- **netsh winsock reset** (restablece la pila de Winsock).

Es posible también que no pueda acceder a ciertos sitios. Esto puede deberse a que el archivo **Hosts**está dañado. Se encuentra en: C:\Windows\System32\drivers\etc.

Solo tendrá que abrirlo utilizando un programa como el Bloc de notas de Windows y realizar los cambios deseados. Después de los comentarios que se señalan con el símbolo de almohadilla, este archivo solo contiene dos líneas que reenvían a la dirección de bucle local:

```
127.0.0.1 localhost

::1 localhost
```

**Importante**: tenga en cuenta que tendrá que ejecutar el Bloc de notas como administrador.

## 2. Restablecer la pila TCP / IP

¡Se trata de un tratamiento de choque!

Ejecute el Símbolo del sistema como administrador.
Introduzca los siguientes comandos:

- **ipconfig /flushdns**
- **nbtstat -R**
- **nbtstat -RR**
- **netsh int**
- **ip reset**
- **netsh winsock reset**

Reinicie el equipo.

## 3. Restablecer Internet Explorer 11

Existen diferentes operaciones que le permitirán ver si finalmente el problema no es benigno:

Pulse la tecla [Alt] para que aparezca la barra de menús.
Haga clic en **Herramientas - Opciones de Internet**.
En el apartado **Historial de Exploración**, haga clic en el botón **Eliminar...**.
Seleccione todos los elementos y haga clic en **Eliminar**.

Con esto se procederá a la eliminación de los siguientes datos:

- Archivos temporales de Internet.
- Cookies.
- Historial de los sitios web visitados.

- Historial de ficheros descargados.
- Datos de formularios guardados.
- Contraseñas.
- Información temporal almacenada por los complementos instalados en el equipo.
- Datos de filtrado InPrivate.

Por el contrario, los datos temporales de sus sitios web favoritos se conservan si marca la opción **Conservar datos de sitios web favoritos**.

También puede restablecer los parámetros predeterminados de seguridad:

Haga clic en **Herramientas - Opciones de Internet**.
Vaya a la pestaña **Seguridad**.
Seleccione cada una de las zonas de Internet y haga clic en el botón **Nivel predeterminado**.

Sepa que también puede hacer clic en **Restablecer todas las zonas al nivel predeterminado**.

A veces es necesario restablecer los parámetros de configuración de Internet Explorer:

Haga clic en **Herramientas - Opciones de Internet**.
Vaya a la pestaña **Opciones avanzadas**.
Haga clic en el botón **Restaurar configuración avanzada**.

Es posible restaurar completamente el conjunto de opciones predeterminadas haciendo clic en el botón **Restablecer**. ¡Es la última solución!

Estas son las operaciones que se realizarán:

- Eliminación de:
  - Historial de navegación, archivos temporales de Internet, datos de formularios, contraseñas guardadas, datos de filtrado InPrivate, datos de sitios web favoritos, historial de descargas.
  - Lista de direcciones URL introducidas, páginas sin conexión, extensiones de los menús.
  - Los sitios que figuran en las zonas Sitios restringidos o Sitios de confianza.
  - Todos los sitios que figuran en la configuración de administración de cookies.
  - Todos los sitios que figuran en la configuración del bloqueador de elementos emergentes.
  - Todas las listas MRU relacionadas con Internet Explorer.

    Las listas MRU (*Most Recently Used*) son todas las sugerencias que hace el sistema basándose en datos ya introducidos al ejecutar un comando, guardar un archivo, etc.
- Restaurar los parámetros predeterminados de:
  - la página de inicio.
  - la configuración de navegación de las pestañas.
  - las preferencias de diseño de página.

- el conjunto de configuraciones que aparecen en la pestaña **Opciones avanzadas**.
- la configuración del bloqueador de elementos emergentes y de sitios suplantadores de identidad.
- los controles ActiveX adicionales.
- las barras de herramientas adicionales y otros BHO.

  Un BHO (*Browser Help Object*) es un programa que permite aportar funciones adicionales a Internet Explorer.

De hecho, solo quedan sin modificar estos elementos principales: favoritos, flujo RRS, controles ActiveX instalados por defecto, configuración de la conexión a Internet, configuración del Proxy y comunicaciones VPN, configuración de los programas predeterminados, configuración del control de acceso e información de certificados.

Finalmente, es posible ejecutar Internet Explorer sin que se active ningún complemento. Si, en este modo, no encuentra el problema de navegación, debe pensar que existe un complemento defectuoso.

Para ejecutar Internet Explorer sin módulos complementarios desde el Símbolo del sistema, introduzca el comando **"C:\Program Files\Internet Explorer\iexplorer.exe" -extoff**.

Haga clic en **Herramientas - Administrar complementos**.
Seleccione el primer complemento y haga clic en el botón **Deshabilitar**.

Puede intentar deshabilitar cinco o diez complementos a la vez para localizar más fácilmente el complemento culpable. A continuación, bastará con eliminarlo directamente desde el administrador de complementos o bien con desinstalar la aplicación correspondiente que, normalmente, debería aparecer en la lista de **Programas y características** del **Panel de control**.

Existen otras dos fuentes posibles de problemas.

## 4. Problemas de compatibilidad

Puede ocurrir que un problema de Internet Explorer se deba a una incompatibilidad con uno de los programas instalados, la presencia de un virus o que la cuenta de usuario esté dañada. En este último caso, compruebe que el problema aparece de la misma manera desde otra cuenta de administrador.

## 5. Problemas en los archivos

Introduzca el disco de instalación en la unidad que ha utilizado también para la instalación del sistema operativo.

Abra el Símbolo del sistema.
Teclee el comando: **sfc /scannow**.

También puede restaurar el equipo si elige un punto de restauración anterior a la aparición del problema.

## 6. La conexión a Internet es muy lenta

Además, algunas páginas no se pueden mostrar en Internet Explorer.

Al cabo de un rato largo, aparecerá este mensaje: "Internet Explorer no puede mostrar la página Web".

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando: **netsh int tcp set global autotuninglevel=disabled**

Reinicie el equipo.

## 7. Restablecer una contraseña perdida

Nirsoft ofrece un gran número de herramientas. Mostramos las más importantes (pero hay para dar y tomar).

- PCAnywhere PassView v1.12: contraseña PCAnywhere.
- IPNetInfo v1.62: permite recuperar la información que acompaña a algunas direcciones IP.
- ProduKey v1.70: permite recuperar las claves de los productos perdidos de Windows, MS-Office y SQL Server.
- Dialupass v3.21: permite recuperar las contraseñas de conexiones de acceso remoto y VPN (*Virtual Private Network* o red privada virtual).
- Network Password Recovery v1.334: permite recuperar las contraseñas de red.
- Mail PassView v1.83: le permite recuperar las contraseñas de las cuentas de correo electrónico.

La página de descarga es accesible desde esta dirección: http://www.nirsoft.net/utils/index.html. Solo tendrá que descargar el archivo ZIP y descomprimirlo, después abra el archivo ejecutable correspondiente. Debemos destacar que algunos de estos programas no son compatibles con Windows 8.

## 8. Resolución de un problema en un dispositivo ADSL

Las ofertas de los proveedores de Internet se expresan en kilobits por segundo. Tomemos un ejemplo: la velocidad de descarga de una conexión de 1024 kbit/s corresponde a 128 kB/s. Por esto mismo un byte es igual a 8 bits. Si dividimos 1024 kilobits por 8 bits, obtenemos dicho resultado: 128 kB. Por otra parte, debemos hacer una distinción entre la velocidad de subida (Upload) y la de bajada (Download). Por ejemplo, cuando ve una página web o descarga un archivo, se utiliza la velocidad de bajada.

Vamos a interesarnos ahora por el funcionamiento de los Box, que a menudo se comercializan con una oferta de Internet. Este tipo de módem funciona como una puerta de enlace entre el equipo y la Web, lo que tiene dos consecuencias:

- No es necesario conectarla a un ordenador ya que funciona de manera autónoma.
- Desde el momento en que lo conectamos a la toma de teléfono, el Box ya se conecta a Internet.

Es otra manera de decir que estará conectado a Internet sin ni siquiera haber abierto el navegador.

Por último, debemos señalar que no puede comprobar un Box en otra línea telefónica que aquella que se le ha asignado.

El problema principal que nos podemos encontrar es la ausencia de sincronización ADSL. Este mal funcionamiento se muestra mediante uno de los indicadores luminosos del Box. Existen diferentes causas:

- La línea no está todavía operativa y deberá esperar algún tiempo.
- No ha instalado un filtro ADSL en la toma telefónica o este está defectuoso.
- La instalación telefónica tiene puntos de interrupción (el cable utilizado no es compatible).
- Hay un problema en las instalaciones del proveedor.

Consulte siempre el manual que acompaña el dispositivo ADSL para comprender el significado de los códigos de parpadeo de los LED.

Hay diferentes puntos que debemos comprobar:

- Un sistema de alarma conectado a la instalación telefónica podría causar problemas en una línea ADSL.
- Desconecte todas las tomas telefónicas excepto la del Box para ver si, en este caso, se realiza la sincronización ADSL.
- Compruebe que no existe ningún tipo de alargo desde el dispositivo ADSL que se conecte directamente a la toma telefónica.
- Si es necesario, retire las láminas metálicas que se encuentran en la toma ADSL para conseguir un mejor contacto con la toma mural.
- Compruebe el funcionamiento correcto de la línea con el operador.
- Resetee el "Box" desconectándolo de la toma eléctrica o presionando el botón pequeño que actúa como "reset".

Consulte de nuevo el manual proporcionado con el dispositivo ADSL porque existen diferentes maneras de realizar un reseteo según el modelo del Box. A menudo esta es la solución que ofrece los mejores resultados.

La experiencia nos dice que cuando se trata de una primera instalación, el problema de sincronización es sintomático de un mal funcionamiento de la línea o de que el Box está defectuoso. Siempre puede comprobar si funciona correctamente en casa de un amigo o vecino con conexión ADSL. No podrá conectarse a Internet, pero de todos modos deberá indicar si recibe correctamente la señal ADSL.

Lo segundo más probable es que se trate de un problema de la red del proveedor. En ese caso, exija que le comprueben la línea: se procederá entonces a una "limpieza" de la línea.

Si se enfrenta a un problema de conectividad baja o muy lenta y está conectado al dispositivo ADSL mediante un USB, a menudo tendrá la posibilidad de comprobar el dispositivo conectándose vía Ethernet. Por otra parte, esta es la mejor solución si el equipo no dispone de puertos USB 2.0.

Si tiene problemas de conectividad entre el dispositivo ADSL y el equipo, aparecerá en el área de notificación un pequeño icono que representa dos ordenadores: habrá un aspa roja entre ambos. En ese caso:

- Si es posible, cambie el modo de conexión.

- Invierta el sentido del cable Ethernet.
- Compruebe con otro cable (USB o Ethernet).
- Compruebe en el Administrador de dispositivos que el adaptador de red se reconoce correctamente.
- Si es preciso, compruébelo con otro adaptador de red (u otro puerto USB).

El mensaje de error "Conectividad limitada o nula" se debe a menudo al simple hecho de que la asignación automática de direcciones IP está activada en las propiedades TCP/IP de la conexión de red y que está conectado mediante USB. Por lo tanto, no es revelador de un verdadero problema de conectividad.

## Windows 10 y Edge

Edge es el nuevo navegador Web de Microsoft presente en Windows 10. Es un producto destinado a sustituir a Internet Explorer, cuyas limitaciones para garantizar la compatibilidad ascendente del producto con las versiones anteriores han frenado el desarrollo.

Con Edge, Microsoft ha partido de una arquitectura innovadora y compatible con las últimas tecnologías del mercado, sobretodo con HTML 5, y orientada al rendimiento. El objetivo es competir con los navegadores más populares del mercado como Google Chrome o Firefox.

Edge asegura y garantiza la misma experiencia de usuario sea cual sea el dispositivo utilizado, tableta, PC o smartphone. Este navegador utiliza el nuevo motor de renderizado EdgeHTML derivado del motor Trident, que utiliza Internet Explorer. Tenga en cuenta que este nuevo motor solo está presente en Edge.

A nivel de seguridad, Edge corre en un entorno particionado ya que es una aplicación Windows, lo que limita los riesgos de penetración en el núcleo del sistema.

Por otra parte, desde un símbolo de sistema PowerShell, puede consultar los datos del almacén de aplicaciones local para visualizar las propiedades del paquete asociado.

Teclee desde un Símbolo del sistema PowerShell el siguiente comando: **Get-AppxPackage -Name *spartan***. Verá las propiedades del paquete asociado.

Para ejecutar este nuevo navegador, en su equipo Windows 10, desde el área de búsqueda a la derecha del menú **Inicio**, escriba **Edge** y ejecute el programa.

Se ejecuta el navegador. La interfaz gráfica es ordenada y fácil de manejar. Igual que en Internet Explorer, dispone de gestión multi-pestañas para la visualización de páginas web.

Para acceder a la configuración del navegador, haga clic en el enlace **Más acciones**, simbolizado por tres puntos en la esquina superior derecha del navegador.

En la lista de opciones, hay un enlace que le permite abrir la página con Internet Explorer para asegurar la compatibilidad de páginas y sitios web que puedan presentar problemas de visualización.

Uno de los aspectos interesantes de este nuevo navegador es que puede agregar notas a una página web y guardar o compartir estas notas con otros usuarios.

Para ello, haga clic en el enlace **Crear una nota web**, simbolizado por el lápiz delante de una hoja de papel en la parte superior derecha del navegador

Otro aspecto práctico del navegador es el modo Vista de lectura que le ofrece una experiencia próxima a un libro electrónico para favorecer su confort visual.

Para ello, haga clic en el enlace **Vista de lectura**, simbolizado por un libro.

Finalmente, teclee el comando **about:flags** en la barra de tareas del navegador para poder activar comandos experimentales para probar.

# Virus y otras amenazas en Internet

Le mostramos una lista de los principales programas que pueden resultar nefastos para la salud de su equipo:

- Adware: un Adware rastrea sus costumbres en Internet y puede, por ejemplo, mostrar ventanas publicitarias en función del perfil establecido. Multitud de sitios web pueden instalar este tipo de programa, a sus espaldas.
- Drive-by download: se trata de un programa que se descarga sin su consentimiento. Esto puede ocurrir cuando intenta cerrar un cuadro de diálogo.
- Redirección de páginas: es un programa que redirigirá una parte o todas las páginas predefinidas (página de inicio, de búsqueda, etc.) hacia un sitio malintencionado.
- Spam: e-mail comercial que no se solicita.
- Spyware o Programa espía: programa que espía y después transfiere a una tercera persona su información confidencial.
- BHOs o *Browser Helper Objects*: son programas que permiten personalizar y controlar algunas configuraciones de un navegador como Internet Explorer. Puede ser creado con fines "pacíficos" (la barra de herramientas que propone Google) o malintencionados.
- Dialer: es un programa que creará, además de su conexión predeterminada, una conexión de acceso telefónico con una tarifa extra en la factura.
- Troyano o Caballo de Troya: programa que tiene funciones escondidas que se pueden ejecutar en un segundo plano a espaldas del usuario. Permiten acceder al equipo en el que se están ejecutando, ya que abren una puerta secreta (Backdoor).
- Virus: es un programa capaz de infectar archivos y propagarse utilizando soportes extraíbles o redes.

Debemos señalar que la frontera entre los diferentes tipos de amenaza no es demasiado precisa y muchos programas maliciosos pueden utilizar diferentes técnicas para extenderse.

## 1. Eliminación de un virus

Primero debemos recordar algunas reglas esenciales:

- Su antivirus debe mantenerse actualizado constantemente.
- No debe instalar varios antivirus a la vez, ya que podría provocar conflictos en el sistema.

- Que un antivirus sea gratuito no quiere decir que sea menos eficaz que otros productos más costosos.
- A pesar de las afirmaciones de los especialistas y los test que aparecen en las revistas especializadas, todos los antivirus son válidos.
- Existen comportamientos de riesgo y otros que no lo son.

Es una manera de decir que a menudo se trata de una cuestión de sentido común y que con frecuencia aquellos que se quejan de una falta de eficacia de los antivirus, a menudo son los mayores consumidores de sitios para "adultos" y redes peer-to-peer.

Le mostramos un ejemplo clásico para la erradicación de un virus.

Actualice las definiciones de virus de su antivirus.

Si no puede acceder a Internet, descargue desde otro equipo la lista de definiciones para poder realizar la actualización de manera manual. De hecho, la mayoría de los antivirus poseen un archivo de definiciones que es posible descargar si su antivirus no puede actualizar de manera automática la base de definiciones de virus.

Desactive el proceso de restauración del sistema de todas las unidades.

En los sistemas NT, este directorio forma parte de las carpetas protegidas. Un antivirus no tiene acceso a ellas, pero un virus es capaz de alojarse en los archivos guardados en este directorio. Dicho de otro modo, no podrá eliminar un virus mientras tenga esta función activada.

Desconecte la conexión de Internet físicamente, quitando el cable USB o Ethernet.

Esta es una manera de asegurarse de que el virus no pueda comunicarse con el exterior y utilizar otra información para esconderse de los ojos del antivirus.

Reinicie en modo seguro.
Realice una comprobación completa de todas las unidades.

No siempre es posible iniciar un antivirus en el modo seguro, ya que puede que sean necesarios algunos servicios que no se inician en este modo.

Inicie en modo normal.
En un motor de búsqueda como Google, lance una búsqueda introduciendo el nombre del virus.

Si busca bien, encontrará páginas y sitios de los fabricantes de antivirus que explican la manera manual de eliminar un virus o Troyano. La mayoría de las veces, consiste en eliminar las entradas que aparecen en el Registro y archivos del Explorador de Windows.

Una vez esté seguro de que el equipo está "sano" puede reactivar la función de restauración del sistema.

La experiencia nos dice que muchos antivirus no detectan correctamente todas las amenazas y sobre todo las que crean los spywares y algunos Troyanos. No dude en utilizar varios programas de desinfección. Sí, a veces se trata de un verdadero combate.

## 2. Los antivirus gratuitos

La siguientes direcciones le permiten descargar o utilizar en línea antivirus gratuitos ofrecidos por grandes fabricantes especializados en seguridad. Estas herramientas no sustituyen a los productos de pago más completos pero ofrecen una seguridad básica para proteger eficazmente su ordenador contra las principales amenazas.

- https://security.symantec.com/nss/getnss.aspx
- http://housecall.trendmicro.com/
- http://home.mcafee.com/downloads/free-virus-scan
- http://www.kaspersky.com/free-virus-scan?ICID=KSS_Global_Site_Free_Tools_Win
- https://www.infospyware.com/antivirus-gratis/

## 3. Las herramientas especializadas

Se trata de simples archivos ejecutables que le permitirán eliminar un virus específico. La ventaja es que esto le permite reparar una situación comprometida si su antivirus no está actualizado.

- http://www.symantec.com/es/es/business/security_response/removaltools.jsp
- http://www.avg.com/es.52
- http://www.pandasecurity.com/spain/homeusers/downloads/repair-utilities/
- http://esp.sophos.com/support/disinfection/
- http://www.bitdefender.es/site/Downloads/browseFreeRemovalTool/

## 4. Desinstalación completa de un antivirus

Si no puede eliminar su antivirus a través de la funcionalidad de eliminación de programas de Windows en el Panel de control, tendrá que suprimirlo manualmente.

En la mayoría de casos, necesitará hacerse con un programa especial que puede descargar del sitio del fabricante. Tomemos el ejemplo de los productos Sysmantec: Norton Removal Tool es una herramienta que le permitirá desinstalar todos los productos Norton presentes en el sistema. Antes de continuar, compruebe que dispone de los CD de instalación o de los archivos de instalación descargados de los productos Norton que desea reinstalar. Es compatible con todas las versiones NT de Windows. Puede descargarlo directamente del sitio de la compañía Symantec desde esta dirección: ftp://ftp.symantec.com/public/english_us_canada/removal_tools/Norton_Removal_Tool.exe

## 5. Herramienta de desinfección de software malintencionado

La herramienta de eliminación de software malintencionado se instala y mejora con regularidad cada vez que realiza una actualización con Windows Update. Puede ejecutarla en línea haciendo clic en el enlace que aparece en la página web. También es posible comprobar el disco mediante las herramientas de WinRE. Esto puede ser útil si no puede acceder al equipo en modo normal y si el antivirus no puede ejecutarse en modo seguro. Veamos cómo podemos hacerlo:

Una vez que ha arrancado desde el DVD-ROM de instalación de Windows 10, haga clic en el enlace **Reparar el equipo** y acceda a la opción de Símbolo del sistema.

Le aparecerá el prompt **x:\sources>**.

Mediante el comando **cd**, vaya a este directorio: C:\Windows\System32. A continuación, introduzca el siguiente comando: **mrt.exe**.
Marque el botón de acción correspondiente al tipo de análisis que desea realizar y déjese guiar por el asistente.

Los modificadores autorizados son los siguientes:

- **/Q** o **/quiet**: modo silencioso, no se muestra ninguna interfaz.
- **/?** o **/help**: muestra la sintaxis y la versión del motor de detección.
- **/N**: modo de detección solo.
- **/F**: realiza un análisis completo.
- **/F:Y**: realiza un análisis completo y limpia los archivos infectados.

# El firewall de conexión a Internet

Un firewall de conexión a Internet es un dispositivo lógico o físico que comprueba los datos entrantes o salientes que van o vienen de redes externas como Internet. Así pues, un firewall le permite prevenir los ataques de hackers o programas malintencionados que intenten tomar el control del equipo de una manera u otra. Veamos cómo funciona el firewall de conexión a Internet integrado en Windows Vista. Pero antes, deberemos conocer qué es un puerto y un protocolo.

## 1. Puertos y protocolos de red

Un protocolo de red es un conjunto de reglas para un tipo de comunicación determinado. Los protocolos más conocidos son:

- FTP (*File Transfer Protocol*): se utiliza para el intercambio de archivos en Internet.
- HTTP (*Hypertext Transfer Protocol*): lo utilizan los navegadores web para conectarse a Internet.
- SMTP (*Simple Mail Transfer Protocol*): sirve para transferir el correo electrónico a los servidores de correo.
- UDP (*User Datagram Protocol*): se trata de un protocolo que Internet utiliza y que forma parte de la capa de transporte de la pila de protocolo TCP/IP.
- TCP (*Transmission Control Protocol*): es un protocolo de control de transmisión de datos al igual que el de UDP.

Cuando una aplicación inicia una conexión entrante o saliente, esta utiliza un protocolo al que se asocian uno o más puertos. Vamos a explicar este segundo concepto... En programación, un puerto es el nombre que se le atribuye a una conexión de tipo lógica y que un protocolo utiliza. Lo podríamos considerar como una puerta que se queda abierta o cerrada en el sistema operativo. En otras palabras, una aplicación como el navegador de Internet utilizará uno o varios protocolos y uno o varios puertos para comunicarse con el exterior. En orden inverso, una aplicación que se ejecute desde una máquina remota puede necesitar que uno o varios puertos estén abiertos en su equipo para conseguir realizar ciertas tareas como, por ejemplo, la instalación de una actualización.

Para obtener una lista de los puertos que están definidos en su equipo, solo tendrá que ejecutar el siguiente comando: **%SystemRoot%\system32\drivers\etc\services**, después abra el archivo con un editor de texto como el Bloc de notas de Windows.

En conclusión, un firewall de conexión a Internet es un programa encargado de limitar las entradas que están abiertas en el sistema para ofrecerle la mayor seguridad posible. De manera predeterminada, un firewall impide cualquier conexión entrante o saliente a menos que se establezcan algunas excepciones. Esto consiste simplemente en crear una regla que, por ejemplo, autorice a una aplicación a abrir un puerto determinado y utilizar tal protocolo. Veamos un ejemplo: usted utiliza el programa Peer-To-Peer eMule y se da cuenta de que la tasa de transferencia es extremadamente lenta. Además, el icono del programa le indica que se le ha asignado una ID baja. Esto ocurre simplemente porque eMule utiliza el puerto 4662 por defecto y, por lo tanto, deberá abrirlo en el firewall de conexión a Internet mediante la creación de una regla para esta aplicación.

## 2. Configurar el Firewall de Windows

En Windows, el firewall está vinculado al tipo de ubicación de red. El firewall está activado por defecto, para las redes domésticas o de empresas y para las redes públicas.

A partir del **Panel de control** en la sección **Sistema y seguridad - Firewall de Windows**, haga clic en la opción **Activar o Desactivar el Firewall de Windows**.

Para cada tipo de ubicación de red, puede elegir entre tres opciones:

- **Activar**: esta configuración impide que una conexión exterior se conecte con el equipo, con la excepción de los programas que ha especificado en la pestaña **Excepciones**.
- **Bloquear todas las conexiones entrantes**: se ignorarán todas las excepciones que se hayan definido y ningún mensaje le avisará cuando el Firewall de Windows bloquee los programas.
- **Desactivar**: seleccione esta opción si ha instalado un firewall de otro fabricante o si dispone de un router o módem.

## 3. Administrar las excepciones

Por defecto, solo se comprueban las conexiones entrantes. Si, por el contrario, uno de sus programas intenta comunicarse con el exterior puede hacerlo sin que se realice ninguna comprobación de los datos transferidos. La razón subyacente consiste en que si el sistema está protegido correctamente a nivel de conexiones entrantes, no hay necesidad de comprobar las conexiones salientes.

Cuando instale un programa que necesita una conexión entrante, se le añadirá automáticamente a la lista de excepciones. Para autorizar o eliminar una de las excepciones que ya están configuradas, solo tendrá que marcar o desmarcar la casilla correspondiente.

En Windows, el concepto de excepción no es explícito. Se puede acceder a esta función a través del asistente **Permitir un programa o una característica a través de Firewall de Windows**.

Desde la sección **Firewall de Windows** del Panel de control, haga clic en el enlace **Permitir un programa o una característica a través de Firewall de Windows**.

## 4. Utilización avanzada del Firewall de conexión a Internet

Para acceder a la configuración avanzada de esta herramienta, siga las siguientes instrucciones:

Haga clic en **Iniciar - Panel de control** y abra el módulo de **Herramientas administrativas**.
Abra la rama **Firewall de Windows con seguridad avanzada**.

También puede ejecutar directamente este comando: **wf.msc**.

Este complemento le permite filtrar las conexiones entrantes y salientes, así como la configuración de IPsec que haya establecido. Debemos recordar que IPsec (*Internet Protocol Security*) es un conjunto de protocolos que le permite realizar intercambios de datos de manera segura en una red. Existen tres perfiles definidos:

- Un perfil de dominio, si el ordenador se conecta a un servidor de dominio de Windows.
- Un perfil privado si se conecta a una red privada.
- Un perfil público si, por ejemplo, se conecta a una red inalámbrica en un aeropuerto u hotel.

Existen tres posibles reglas:

- **Reglas de entrada**: estas reglas se encargan del tráfico entrante al equipo.
- **Reglas de salida**: estas reglas determinan cómo está configurado el tráfico saliente del equipo.
- **Reglas de seguridad de conexión**: se utilizan reglas de autenticación cuando dos equipos se comunican entre sí. Las tecnologías IPsec permiten configurar los intercambios de claves, métodos de autenticación y la comprobación y cifrado de datos.

## 5. Funcionamiento de las reglas de seguridad avanzadas

Las reglas permiten:

- Autorizar la conexión.
- Autorizar únicamente la conexión mediante la utilización de un protocolo de Internet seguro IPsec.
- Bloquear una conexión.

Puede configurarlas para que solo afecten a un usuario, equipo, programa, servicio, puerto o protocolo concreto. También puede determinar a qué interfaz de red quiere que se aplique: red local (LAN), conexión inalámbrica, acceso telefónico, etc. Se aplicarán en este orden:

- Reglas de seguridad de conexión.
- Reglas llamadas "de bloqueo".
- Reglas "de permiso".

Un gran número de reglas ya están preestablecidas:

- un pequeño botón gris le señala que la regla no está activa;
- un pequeño botón verde indica que la regla está activa.

Las columnas colocadas en el panel central muestran:

- **Nombre**: el nombre de la regla.
- **Grupo**: el nombre del grupo al que pertenece la regla.
- **Habilitado**: indica si la regla está habilitada o no.

- **Acción**: indica si la regla es una regla de bloqueo o no.
- **Programa**: indica la ubicación y el nombre del archivo ejecutable correspondiente a la regla.
- **Dirección local**: indica la dirección IP en la que se aplica la regla.
- **Dirección remota**: indica la dirección IP o direcciones IP de los equipos remotos relacionadas con esta regla.
- **Protocolo**: indica el protocolo determinado por la regla (TCP o UDP).
- **Puerto local**: indica el número de puerto utilizado localmente por la aplicación de destino.
- **Puerto remoto**: indica los puertos utilizados por los equipos remotos cuando solicitan la aplicación que está establecida.
- **Usuarios y Equipos permitidos**: indica a qué usuarios o equipos les afecta la regla seleccionada.
- **Entidades de seguridad locales permitidas**: indica si la regla se aplica a todos o a parte de las entidades de seguridad locales, como por ejemplo los usuarios locales.
- **Propietario de usuarios locales**: indica el propietario de la regla de seguridad. Se aplica en particular a las aplicaciones de Windows Store.
- **Paquete de aplicación**: indica la aplicación Windows Store para la que se aplica la regla.

Haga doble clic en cada uno de los encabezados de columna si desea filtrar las diferentes listas en función de los valores presentes.

Vamos a observar un ejemplo sencillo: veamos cómo permitir las solicitudes de ping al equipo. Este comando le permitirá enviar una solicitud de eco a otro equipo. Si este no responde, es posible que los dos equipos no puedan comunicarse entre sí.

Haga clic con el botón secundario del ratón en la rama **Reglas de entrada** y en el submenú **Nueva regla...**.
Seleccione el botón de opción **Personalizada** y haga clic en **Siguiente**.
Seleccione el botón de opción **Todos los programas** y haga clic en **Siguiente**.
En la lista desplegable **Tipo de protocolo**, seleccione la opción **ICMPv4** y haga clic en el botón **Personalizar...**.
Seleccione el botón de opción **Tipos de ICMP específicos** y seleccione la casilla **Petición eco**.

Haga clic en los botones **Aceptar** y **Siguiente**.
Si es necesario, determine cuáles son las direcciones IP locales y las direcciones IP de los equipos remotos.
Haga clic dos veces en **Siguiente**.
Indique en qué entorno se debe aplicar la regla y haga clic en **Siguiente**.
Introduzca un nombre y una descripción para la regla y haga clic en **Finalizar**.

## 6. Configuración avanzada del firewall en el símbolo del sistema

La utilización de comandos avanzados para la gestión del firewall permite automatizar las tareas de configuración o intervenir remotamente así como listar rápidamente la información útil para saber la configuración del firewall.

Desde un Símbolo del sistema en modo administrador, teclee el siguiente comando para determinar los perfiles activos

```
netsh advfirewall show allprofiles
```

Para consultar el conjunto de reglas configuradas para el perfil público, teclee el siguiente comando:

```
netsh advfirewall firewall show rule name=all profile=public
```

El siguiente comando permite autorizar el comando ping para todos los perfiles:

```
netsh advfirewall firewall add rule name="ICMP V4" dir=in
action=allow protocol=icmpv4
```

El siguiente comando permite autorizar la funcionalidad Escritorio remoto para todos los perfiles:

```
netsh advfirewall firewall set rule group="Escritorio remoto"
new enable=Yes
```

Hay disponibles muchos otros comandos que están documentados en el sitio TechNet de Microsoft para ayudarle en la administración y configuración de esta funcionalidad.

## 7. Problemas avanzados con el firewall

Si no puede arrancar el firewall de Windows, compruebe los siguientes puntos en orden:

- ¿Dispone de un firewall de otro fabricante? En ese caso, el firewall de Windoes se desactiva. Compruebe la compatibilidad de Windows con su solución de seguridad y busque en el sitio de soporte de la solución o en foros si alguien ha tenido ya el mismo problema y lo ha resuelto.
- El firewall de Windows no arranca y devuelve el código de error Ox5. En ese caso, compruebe que el servicio Motor de filtrado de base (BFE) está iniciado.
- El firewall de Windows no arranca y devuelve el código de error 80070424. En ese caso, compruebe que el servicio Instalador de módulos de Windows (TrustedInstaller) está iniciado.

El firewall bloquea algunos programas. En ese caso, abra los puertos necesarios para el buen funcionamiento de estos programas. Para comprobar la apertura de los puertos, utilice la herramienta en línea de comando telnet.

En caso de que no pueda resolver un problema, puede restaurar la configuración por defecto del firewall. Desde un símbolo del sistema en modo administrador, teclee el siguiente comando:

```
netsh advfirewall reset
```

CAPITULO 9 . LA RED

# Introducción a las redes

En este capítulo vamos a explicar los conceptos más importantes que nos permitirán entender el funcionamiento de una red.

Una red es un conjunto de equipos o de personas conectadas. Por metonimia, se incluye también el conjunto de enlaces que se establecen. Por lo tanto, se trata de un medio que permite a los usuarios o grupos de usuarios compartir datos, información y servicios.

Podemos clasificar las redes en función de su tamaño, extensión y estructura. Existen tres categorías de red:

- Una red local o LAN (*Local Area Network*) o RLE (red local de empresa) es la red que podemos encontrar en un edificio o empresa.
- Una red de área metropolitana o MAN (*Metropolitan Area Network*) se define a nivel de zonas y puede cubrir la extensión de una ciudad.
- Una red de área amplia o WAN (*Wide Area Network*) está formada a menudo por varias LAN interconectadas. Podemos pensar en una red de empresa que permite conectar las diferentes sucursales o bien en una red global que agrupa diferentes sitios repartidos en varios países. Sin embargo, el mejor ejemplo de una WAN es Internet.

# Topologías

Las redes pueden tener estructuras diferentes.

## 1. Componentes de red

Ya hemos visto que un protocolo de comunicación permite a diferentes equipos intercambiar datos entre sí. TCP/IP, NetBEUI, DLC o AppleTalk son protocolos de comunicación.

Un protocolo define un conjunto de reglas que permitirán el intercambio de información en una red.

El cliente de red es un componente de software capaz de comunicar con el servidor de red al que está asociado.

Por ejemplo, el cliente para redes Microsoft establece una comunicación para compartir archivos e impresoras en redes Microsoft y así poder acceder tanto a recursos específicos como a directorios de archivos.

## 2. Bus

La topología de bus se basa en una tecnología en multipuntos (punto a punto). Los ordenadores están conectados a la cadena por medio de un cable que forma la red. Esta configuración no tiene ningún interés a menos que quiera conectar dos equipos con el menor coste posible.

## 3. Estrella

La topología en estrella se basa en el principio de componentes activos. Un componente activo transmite señales y las regenera. Estos puntos centrales pueden ser concentradores (hubs) o conmutadores (switchs). En la práctica, se trata de la configuración más frecuente.

## 4. Anillo

Esta topología se basa en un bucle cerrado en forma de anillo que crea enlaces punto a punto. Todas las tramas transitan por cada nodo, que funciona como un repetidor. Una topología en anillo se aconseja en los casos siguientes:

- El tiempo de respuesta no debe ralentizarse.
- Se requiere una red de alta velocidad.

El inconveniente que tiene es que no puede ampliarse demasiado.

## 5. Topologías derivadas

Estos son algunos ejemplos:

- **Malla**: un ejemplo simple es Internet, ya que esta red está formada por topologías mixtas.
- **Bus en estrella**: en esta configuración, los hubs están conectados entre sí mediante una cadena de cables coaxiales.
- **Anillo en estrella**: se trata de anillos que se conectan entre sí.

# El protocolo TCP/IP

TCP/IP (*Transmission Control Protocol/Internet Protocol*) es el protocolo de comunicación estándar en la red de Internet. Tiene la particularidad de ser enrutable al introducir identificadores de red adicionales (direcciones IP) y requiere de un plan de direccionamiento explícito.

## 1. Direcciones de Internet

Una dirección IP (*Internet Protocol*) identifica de una manera única al equipo, así como a la red en la que este se encuentra. Se puede expresar en un formato binario o decimal. Por ejemplo, la dirección 192.168.0.1 se puede escribir en binario de la siguiente manera: 1100 000.1010 1000.000 000.0000 0001. La Calculadora de Windows permite realizar de manera sencilla este tipo de conversión.

Esta dirección se utiliza para todas las comunicaciones entre los nodos de red.

Está codificada en 32 bits (es decir, 4 enteros decimales separados por puntos) y las cifras comprenden entre 0 y 255. Por ejemplo, 234.65.140.154.

Cada dirección está formada por dos partes:

- Una serie de bits colocados a la izquierda correspondientes al ID o identificador de red (en inglés, Net ID).
- La parte de la derecha de la dirección corresponde al ID del host (o Host Id).

Por ejemplo, en una red con la dirección 42.0.0.0, los equipos que la componen pueden tener direcciones que van de 42.0.0.1 a 42.255.255.254.

Se determinó que el primero, los dos primeros o los tres primeros bytes se utilizarán como identificadores de la red. De hecho, cuanto más pequeño sea el número de bits reservados para la red, más equipos podrá contener. Por ejemplo, una red definida como 192.168.0.0 permite tener 65.534 combinaciones (256*256-2) mientras que una definida como 104.0.0.0 podrá contener 16.777.214 equipos (256*256*256*-2). Veremos más adelante por qué estamos obligados a restarle dos al resultado. Está claro que el objetivo de esta organización jerárquica es facilitar la búsqueda de un equipo en la red.

Esta distinción hecha entre la capacidad de cada tipo de red reside en el concepto de clases de direcciones IP. Veamos una tabla que resume las principales clases.

| Clase de dirección IP | Net Id | Host Id | Número de nodos |
|---|---|---|---|
| A | 1 byte | 3 bytes | 16.777.214 |
| B | 2 bytes | 2 bytes | 65.534 |
| C | 3 bytes | 1 byte | 254 |

Para cada clase, se reservan dos direcciones que no se pueden utilizar:

- La dirección de red.
- La dirección de difusión (broadcast).

Una dirección donde el número de equipo está completamente a cero sirve para hacer referencia a la propia red. En consecuencia, un equipo no puede tener un número en el que todos los bits correspondientes al equipo están puestos a cero.

Una dirección en la que todos los bits correspondientes al número del equipo están a 1 es una dirección de difusión y hace referencia a todos los equipos que forman esa red.

Estas dos direcciones son llamadas "reservadas". Existen otras dos de un tipo un tanto particular:

La dirección 127.0.01, llamada "Dirección de bucle local" ("Loopback" en inglés). Representa al equipo local y permite el funcionamiento de multitud de programas. Una manera de comprobar si el adaptador de red está bien configurado consiste en enviar una solicitud de ping a esta dirección.

La dirección 0.0.0.0 la utiliza el equipo host cuando intenta determinar su propia dirección IP.

## 2. El NIC (Network Information Center)

Dentro de una empresa, los equipos conectado a internet, solo necesitan una dirección IP única. Este tipo de dirección pública lo administra un organismo llamado IANA (*Internet Assigned Numbers Authority*) que se encarga de que no se asignen a dos organizaciones diferentes una misma dirección. Más adelante, la organización a la que se asigna un número de red podrá elegir sus propios números de host. Por convención, este rango de direcciones está reservado a uso privado:

- Clase A: de 10.0.0.1 a 10.255.255.254
- Clase B: de 172.16.0.1 a 172.31.255.254
- Clase C: de 192.168.0.1 a 192.168.255.254

## 3. Máscara de subred

Una máscara de subred se presenta de la misma forma que una dirección IP. Estará formada por 0 en la parte de la dirección IP que queremos anular y por 1 en la parte que queremos conservar. Si tomamos el ejemplo de un equipo cuya dirección IP es 192.168.23.45, debemos asociarle una máscara para saber qué parte de esta dirección representa la red y qué parte el equipo. Si hemos establecido la máscara de subred como 255.255.255.0, esto significa que los tres primeros bytes son 1. La parte de red equivale a 192.168.23. En cuanto al equipo host se identifica con el número 45.

Recuerde que:

- La dirección 192.168.23.0 se utilizará para identificar la red.
- La dirección 192.168.23.255 está reservada (al broadcast).

Por lo tanto, hay 254 direcciones disponibles para los equipos de la red.

Observará que es la máscara elegida la que determina el número de ordenadores que se podrá direccionar.

La otra utilidad de una máscara de subred es que permite detectar si una dirección IP forma parte de una red local o si se debe enrutar este mismo paquete IP al exterior (Internet, por ejemplo). Esto funciona como un tipo de panel indicador.

Puede utilizar una herramienta en línea para hacer todo tipo de cálculos: http://www.subnetmask.info.

## 4. Dirección IPv6

IPv6 (*Internet Protocol version 6*) es el sucesor del protocolo IPv4. Se ha desarrollado para anticipar una posible escasez de direcciones debido al gran desarrollo de Internet en todas las regiones del mundo. Además, presenta otras ventajas con respecto a su antecesor, como una mejor seguridad y una mayor flexibilidad de uso sin dejar de ser compatible con las direcciones IPv4.

IPv6 permite expandir el espacio de dirección a 16 bytes o 128 bits (en contraste con los 4 bytes de la IPv4). Este tipo de dirección se expresa gracias al formato hexadecimal en el que los 8 grupos de 16 bits están separados por dos puntos: 3ffe:0000:0a88:85a3:0200:ac1f:8001. Normalmente, los 8 primeros bytes sirven para identificar la dirección de subred mientras que los 8 bytes siguientes permiten identificar el equipo host. Es el tipo de formato que se utiliza desde Windows Vista.

## 5. Funcionamiento de la pila TCP/IP

La pila TCP/IP está formada por un conjunto de protocolos de transporte que permiten el intercambio de información entre equipos pertenecientes a medios heterogéneos. TCP/IP incluye protocolos de aplicación como el correo electrónico (SMTP), la transferencia de archivos (FTP), la administración de componentes de red (*Simple Network Management Protocol* o SNMP), las conexiones remotas, o el HTTP en el que se basa el World Wide Web... A los paquetes IP también se les llama datagramas.

Un datagrama está compuesto por un encabezado que agrupa el conjunto de información necesaria para el enrutamiento del paquete (versión, tipo de servicio, longitud del paquete, etc.), y un área que contiene los datos que va a transferir. Los protocolos de transporte TCP

(HTTP, FTP, mail, Telnet, etc.) o UDP (TFTP, etc.) se utilizan en este caso. UDP (*User Datagram Protocol*) es un protocolo que permite la transferencia de paquetes entre dos entidades de una red. Al contrario que el protocolo TCP, no existe un control de errores.

### 6. Dirección de bucle local

Esta dirección (*Local Loopback*) equivale a 127.0.0.1 y está destinada a las comunicaciones entre procesos en el equipo local.

### 7. Funcionamiento de los servicios DNS

El objetivo de un servidor DNS (*Domain Name Server*) es el de asegurar que un nombre de dominio corresponde con una dirección IP. Dado que es más difícil memorizar la IP 90.83.78.130 que el nombre del sitio Ediciones ENI, un servidor DNS se encargará de realizar esta transcripción.

Sepa también que dispone en su equipo de una libreta de direcciones DNS bajo la forma de un archivo en formato de texto. Se trata del archivo Hosts y lo puede encontrar si abre en el Explorador de Windows C:\WINDOWS\system32\drivers\ etc. Cuando abre la dirección URL de una página, se consulta este archivo para comprobar si contiene la dirección IP correspondiente al nombre del sitio. Si desea prohibir la consulta de un sitio, solo tendrá que añadir su nombre seguido de la dirección IP 127.0.01 que es, como hemos visto, la dirección local del equipo (localhost).

### 8. Función de un servidor DHCP, un servidor WINS y los nombres NetBIOS

Hemos visto que cada equipo que forma parte de una red debe poseer una dirección IP diferente. La asignación de direcciones puede suponer un quebradero de cabeza en redes de tamaño importante. Por otra parte, sabemos que un equipo puede funcionar como servidor para facilitar la administración de la red. Por esta razón, los equipos llamados servidores DHCP se encargarán de asignar de manera dinámica direcciones IP únicas a todos los equipos que forman parte o se unan a una red local. Esto funcionará del mismo modo cuando se conecte a Internet. Un servidor DHCP le asignará a su equipo una dirección IP única en el momento en que realice la conexión.

Un nombre NetBIOS es el nombre que se le da a un equipo para poder identificarlo dentro de una red local. Los cambios se guardan en un archivo llamado *Lmhosts* cuya estructura recuerda exactamente a la de su hermano gemelo, el archivo *Hosts*. Será, por tanto, el enlace entre una dirección IP y el nombre NetBIOS del equipo.

Desde Windows 2000, el nombre NetBIOS de un equipo (nombre de equipo para la capa de red Microsoft) se deduce a partir del nombre de host (nombre del equipo para el protocolo de Internet).

Un servidor Wins (WINS de *Windows Internet Naming Service*) es un equipo-servidor que contiene una tabla de correspondencias entre el nombre NetBIOS del ordenador y la dirección IP.

## Creación de una conexión de red

Antes de nada, deberemos conocer dos conceptos importantes.

## 1. Grupo de trabajo o dominio

Podemos distinguir entre una red organizada en forma de grupo de trabajo u organizada por dominio. Son formas diferentes de llamar a una red de software, independientemente de su organización física.

En el primer caso, todos los equipos pueden funcionar como servidor (compartir recursos) y como cliente (acceder a los recursos). En el segundo caso, solo algunos equipos actúan como servidores. Esto supone la instalación de sistemas operativos especialmente diseñados para este tipo de tareas.

Por defecto, el nombre del equipo de trabajo asignado al equipo de Windows 10 es WORKGROUP. Puede modificarlo de la siguiente manera:

Pulse las teclas [Windows] + [Pausa].
Haga clic en el enlace **Configuración avanzada del sistema**.
Seleccione la pestaña **Nombre de equipo** y haga clic en el botón **Cambiar...**.

El nombre del equipo no puede sobrepasar los quince caracteres y no puede incluir los siguientes símbolos: ` ~ @ # $ % ^ & ( ) = + [ ] { } | ; : , ’ ” . < > / ?.

Una vez que haya modificado el nombre del grupo de trabajo, haga clic en **Aceptar** y reinicie el equipo.

## 2. Velocidad de transferencia de datos

La tecnología de cableado más común es LAN (*Local Area Network*) debido a su bajo coste y facilidad de instalación.

La velocidad de transferencia de datos permitidos por un cable Ethernet es la siguiente:

- 10 Mbit/s (Ethernet): 10 Megabits por segundo.
- 100 Mbit/s (Fast Ethernet): 100 Megabits por segundo.
- 1.000 Mbit/s (Gigabit Ethernet): 1.000 Megabits por segundo.
- 10.000 Mbit/s (10 Gigabit Ethernet): 10.000 Megabits por segundo.

El prefijo multiplicador "mega" no representa en este caso a un millón de unidades, sino a 1.048.576 unidades (1024 x 1024), es decir, $2^{20}$.

La primera regla consiste en comprobar que todos los componentes de red soportan la misma velocidad de transferencia (router, adaptador de red, concentrador y cable de conexión).

## 3. Material necesario

Si está pensando en crear una red cableada, necesitará cables Ethernet para conectar los diferentes componentes. Los cables utilizados se llaman pares trenzados porque están formados por cuatro pares de filamentos trenzados.

Un cable recto se utiliza para conectar un ordenador con un dispositivo como un router, o un router con un módem.

Un cable cruzado se utiliza para conectar dispositivos idénticos y solamente dispositivos.

Las categorías de cables son las siguientes:

- Cat 5: 10/100 Mbps.
- Cat 5e y Cat 6 UTP: 10/100/1000 Mbps.
- Cat 6a y Cat7a: 1.000/10.000 Mbps

Estas cinco normas de cables pueden utilizarse para fabricar cables rectos o cruzados.

Los cables rectos se utilizan para:

- Conectar un ordenador a un switch o a un hub.
- Conectar un ordenador a un módem ADSL en el puerto LAN.
- Conectar un router del puerto WAN al puerto LAN de un módem ADSL.
- Conectar el puerto LAN de un router al puerto "Uplink" de un switch o un hub.
- Conectar dos switches o hubs cuando uno utiliza el puerto normal y el otro el puerto "Uplink".

¿Cómo saber si un cable de red es recto? Muy simple: cuando compara los dos conectores de un cable recto, el orden de colores es el mismo.

Un cable cruzado puede servir para:

- Conectar directamente dos ordenadores.
- Conectar el puerto LAN de un router al puerto normal de un switch o de un hub.
- Conectar dos switches o hubs utilizando en ambos el puerto normal.

A diferencia del cable recto, cuando compara los dos conectores del cable cruzado, el orden de colores no es el mismo.

En la práctica, muchas tarjetas de red o Box (Freebox, Livebox, etc.) disponen de una función llamada MDI/MDIX o Auto-MDIX que hace que acepten estos dos tipos de conexión. En caso de duda, consulte el manual del fabricante.

¿Qué hay de los conectores USB? Si puede elegir, opte por una conexión Ethernet en lugar de una conexión USB. En otras palabras, compruebe que el LiveBox u otro Box disponen de una conexión Ethernet. En la práctica, la calidad y la estabilidad de la conexión serán mucho mejores. Si no tiene otra elección, utilice conexiones USB 2.0 o USB 3.0 y evite a toda costa soluciones de conexión USB 1.0 o 1.1. Por supuesto, la placa base de su equipo debe poder soportarlo.

## 4. Las tarjetas de red

Las tarjetas de red pueden ser integradas, conectarse a las ranuras PCI de la placa base o ser del tipo PCMCIA. En todos los casos, disponen de un puerto RJ45 en el que introducir el cable Ethernet. También puede utilizar un adaptador de red USB pero no es la mejor solución que puede tomar.

## 5. Router

Un router es un dispositivo de comunicación que asegura una conexión física entre dos redes. La función que desempeña se denomina enrutamiento y permite determinar el próximo nodo de la red al que se va a enviar un paquete de datos. Este proceso se produce a nivel de la

capa 3 (capa de red) del modelo OSI. OSI (*Open Systems Interconnection*) establece un conjunto de normas que permiten asegurar el intercambio de datos en una red y entre sistemas heterogéneos. Este modelo dispone de siete niveles de compatibilidad: aplicación, presentación, sesión, transporte, red, enlace y físico. En la práctica, un router permite compartir la conexión a Internet entre varios equipos. Sepa que también se puede beneficiar de las funciones de enrutamiento utilizando un Livebox.

Un router doméstico dispone, por lo general, de cuatro puertos Ethernet, así como de un puerto WAN que permite conectarse a un módem ADSL. También tiene integrado un firewall de conexión a Internet.

## 6. Concentrador o hub

Un concentrador (o hub en inglés) permite la conexión de varios ordenadores a una misma red Ethernet. Un concentrador funciona simplemente como repetidor de datos sin asegurar ninguna protección especial.

Dispone de dos tipos de puertos:

- Los puertos (llamados normales) que permiten conectar los diferentes equipos.
- Los puertos que sirven para extender la red y a los que se conectará otro concentrador.

Un hub repetirá los datos emitidos por uno de los equipos a los demás, haciendo que formen un único nodo. Esto hace que cualquier elemento conectado a un concentrador pueda acceder a todos los demás elementos conectados al mismo concentrador. Por otra parte, una red de 100 Mbits compuesta de cinco ordenadores solo podrá proporcionar simultáneamente 20 Mbits por equipo.

## 7. Conmutador o Switch

Podemos definir un switch como un tipo de concentrador inteligente. Mientras que un concentrador transfiere los datos por todos los equipos conectados al Hub, un conmutador permite elegir por qué equipos se van a enrutar los datos. De hecho, cada intercambio puede realizarse sin desperdiciar el ancho de banda.

## 8. Organización física de la red

Conecte el puerto WAN del router al puerto LAN del módem ADSL utilizando un cable recto. A continuación, conecte los equipos que forman la red a los puertos LAN del router. Utilice el rango de direcciones que va de 192.168.1.1 a 192.168.1.254 con la máscara de subred: 255.255.255.0.

## 9. Instalación del adaptador de red

La mayoría de equipos actuales dispone de un componente de red directamente integrado en la placa base. Si añade una tarjeta Ethernet, Windows detectará un cambio en la configuración y deberá instalar de nuevo el componente. Solo tendrá que introducir el disco de instalación que venía junto con el adaptador de red (si el sistema operativo no dispone de un controlador integrado). Nada le impide instalar, a continuación, un controlador más reciente que puede encontrar en un sitio especializado o en la página del fabricante del adaptador.

## 10. Elección del tipo de ubicación

Desde el **Panel de control**, haga clic en el vínculo **Ver el estado y las tareas de red**, en la sección **Redes e Internet**.
En la red activa puede ver el tipo de ubicación de su red.

A continuación puede ver una breve descripción de los tres tipos distintos de ubicaciones a los que su red puede corresponder:

- **Red pública**: el equipo formará parte de una red conectada directamente a Internet. Las funciones de descubrimiento de red, archivos compartidos y otras opciones disponibles de uso compartido están desactivadas. De esta manera, se disminuye el riesgo de ser víctima de un programa malintencionado. El firewall de conexión a Internet (si está activado) bloqueará todo intento de acceso desde otros equipos.
- **Red privada**: en esta configuración, el ordenador está conectado a una red de confianza (ya sea profesional o personal). Las funciones de descubrimiento de red y uso compartido de archivos estarán activadas.
- **Red de trabajo**: el equipo forma parte de un dominio que contiene un controlador de dominio Active Directory.

En Windows 10, para pasar de una red pública a una red privada, en la configuración del PC del menú **Inicio**, haga clic en la sección **Red e Internet**.
A continuación haga clic en el enlace **Ethernet** y en la conexión Ethernet activa.
Cambie la opción **Buscar dispositivos y contenido** a la posición **Activado**.

## 11. Configuración TCP/IP

Desde el **Panel de control**, haga clic en el vínculo **Ver el estado y las tareas de red** de la sección **Redes e Internet**. A continuación seleccione el vínculo **Cambiar configuración del adaptador**.
Haga clic con el botón secundario del ratón en la conexión de red que desea configurar y después en **Propiedades**.

Se deben instalar los siguientes elementos:

- Cliente para redes Microsoft.
- Compartir impresoras y archivos para redes Microsoft.
- Protocolo de Internet versión 4 (TCP/IPv4).
- Controlador de E/S del asignador de detección de topologías de nivel de vínculo.
- Respondedor de detección de topologías de nivel de vínculo.
- Protocolo de Internet versión 6 (TCP/IPv6).
- Planificador de paquetes Qos.

Si uno de los elementos no aparece, haga clic en el botón **Instalar**.
Haga clic en la versión del protocolo de Internet que utiliza y en **Propiedades**.
Puede especificar de forma manual una dirección IP, una máscara de subred y una puerta de enlace, así como direcciones DNS concretas.

Si tiene un ordenador portátil, es interesante seleccionar la pestaña **Configuración alternativa**que aparece al lado de la pestaña **General**. Podemos suponer que en el ámbito profesional el equipo obtendrá de manera automática una dirección IP, mientras que cuando se conecte desde su casa, el equipo utilizará una dirección IP fija. En este último caso, haga clic en el botón de opción **Configurada por el usuario** e introduzca la configuración necesaria.

## 12. Impresora compartida

Primero compruebe que el elemento de Uso compartido de impresoras y archivos está activado en las propiedades de su conexión de red.

Abra el **Centro de redes y recursos compartidos**.
Haga clic en el vínculo **Cambiar configuración de uso compartido avanzado**.
Despliegue el perfil activo.
Seleccione el botón de opción **Activar el uso compartido de archivos e impresoras** y haga clic en **Guardar cambios**.
Acceda a continuación al Panel de control y haga clic en el vínculo **Dispositivos e impresoras**.
Seleccione la impresora a compartir, haga clic con el botón derecho del ratón y seleccione el comando **Propiedades**.
Haga clic en la pestaña **Compartir** y marque la casilla **Compartir impresora**.

Es posible cambiar el nombre del recurso compartido.

## 13. Uso compartido simple de archivos en Windows

Compruebe que ha activado correctamente el uso compartido de archivos e impresoras para su conexión de red.

Acceda al **Centro de redes y recursos compartidos**.
Haga clic en el vínculo **Cambiar configuración de uso compartido avanzado**.
Marque el botón de opción **Activar el uso compartido de archivos** para el perfil de su conexión de red y pulse **Guardar cambios**.
Haga clic en el botón en forma de flecha a la derecha de **Todas las redes**.
Marque el botón de opción **Desactivar el uso compartido con protección por contraseña**.

Haga clic en el botón **Guardar cambios**.
Abra el Explorador de Windows, haga clic con el botón secundario del ratón en la carpeta que desea compartir y haga clic en el submenú correspondiente. Para ello, haga clic en el menú **Compartir con** y a continuación en el submenú **Usuarios específicos**.
Haga clic en la pequeña flecha situada a la derecha de la lista desplegable, que está vacía por el momento, y seleccione el grupo **Todos** o la entidad de usuario "Invitado".

Haga clic en **Agregar**.
Seleccione este usuario y defina el tipo de permisos que tendrá sobre la carpeta compartida:

- **Lectura**: el usuario solo podrá ver y leer los archivos y carpetas contenidos en la carpeta compartida.
- **Lectura/escritura**: el usuario podrá ver, modificar, añadir y eliminar archivos y carpetas de la carpeta compartida.

Como se indica en la parte superior de la ventana, las personas que no disponen de cuenta de usuario y contraseña no podrán obtener acceso a los archivos que comparte con el grupo **Todos**.

Haga clic en los botones **Compartir** y **Listo**.

Se indica el nombre y la ubicación del recurso compartido. Puede hacer clic con el botón secundario del ratón y seleccionar **Copiar enlace** para comunicárselo a los demás usuarios con los que ha compartido el recurso.

A veces, a pesar de todo, aparece una ventana de identificación. Si ocurre esto, solo tendrá que introducir el usuario: **invitado**.

Para mostrar de una manera rápida las opciones de uso compartido de una carpeta, haga clic sobre ella con el botón secundario del ratón y en el submenú **Propiedades**.
Haga clic en la pestaña **Compartir**.
A continuación, seleccione la pestaña **Seguridad** para mostrar el conjunto de permisos NTFS de la carpeta.

Esto le da la posibilidad de realizar ajustes si, por casualidad, un grupo de usuarios no tuviera acceso a una carpeta ("no tiene permisos para acceder a este recurso de red").

## 14. Utilización de la carpeta Acceso público en Windows 8

La carpeta *Acceso público* es una manera aún más sencilla de compartir rápidamente un recurso en la red.

Desde el Panel de control, en el **Centro de redes y recursos compartidos**, haga clic en **Cambiar configuración de uso compartido avanzado**.
En el perfil de red **Todas las redes**, marque el botón de opción **Activar el uso compartido** para que cualquiera que acceda a la red pueda leer y escribir ficheros en las carpetas Públicas.
Haga clic en **Guardar cambios**.

Compartir la carpeta Acceso público agrega el grupo de usuarios **Todos** a la lista de permisos de la carpeta Acceso público en C:\Usuarios.

## 15. Recursos compartidos con contraseña

Desde el Panel de control, en el **Centro de red y recursos compartidos**, haga clic en **Cambiar configuración de uso compartido avanzado**.
En el perfil de red **Todas las redes**, marque el botón de opción **Activar el uso compartido con protección por contraseña** para que el acceso a las carpetas compartidas de su equipo sea seguro.
Haga clic en **Guardar cambios**.
En el Explorador de Windows, abra la carpeta que desea compartir y agregue, como se ha explicado anteriormente, los usuarios con acceso al recurso.

A partir de entonces, los usuarios deberán identificarse e indicar una contraseña antes de poder acceder a los recursos que usted comparte.

## 16. Establecer el uso compartido avanzado

Requiere que estas dos funciones estén activadas:

- Uso compartido de archivos.
- Uso compartido con protección por contraseña.

Localice la carpeta que desea compartir.
Haga clic en ella con el botón secundario del ratón y acceda a sus **Propiedades**.
Seleccione la pestaña **Compartir** y pulse el botón **Uso compartido avanzado...**.
Marque la casilla **Compartir esta carpeta**.
Defina el nombre del recurso compartido.
Si lo desea, limite el número de usuarios autorizados a conectarse simultáneamente a esta carpeta compartida.
Si quiere puede añadir comentarios.

Haga clic en el botón **Permisos**.

Por defecto, el grupo **Todos** tiene permiso de lectura sobre sus recursos.

Puede añadir otros usuarios y definir permisos NTFS para cada uno de los usuarios o grupos de usuarios.

Pulse el botón **Aplicar**.
Haga clic en **Caché**.

Defina el tipo de disponibilidad del contenido del recurso compartido para los usuarios no conectados.

Retomamos simplemente el funcionamiento de los archivos sin conexión.

Acepte el resto del procedimiento.

Si vuelve a la ventana **Uso compartido avanzado**, tendrá la posibilidad de añadir otros perfiles de uso compartido haciendo clic en el botón correspondiente.

# Grupo hogar

El concepto grupo hogar apareció con Windows 7. El grupo Hogar facilita compartir recursos entre los equipos Windows 8 y Windows 10 de una red doméstica.

## 1. Creación de un grupo hogar

Debe configurar el primer equipo miembro de su grupo de hogar para utilizar una ubicación de red de tipo **Red doméstica**. Este tipo de configuración lanza automáticamente la creación y configuración del grupo hogar. También puede lanzar manualmente la creación del grupo hogar.

Para ello, desde el **Panel de control**, en la sección **Redes e Internet - Grupo hogar**, haga clic en **Crear grupo hogar**.
A continuación, seleccione los elementos que va a compartir con los miembros del grupo hogar.

Seleccione todos los elementos y a continuación haga clic en el botón **Siguiente**.
Anote la contraseña aleatoria que se pedirá a los miembros del grupo hogar para acceder a los recursos del equipo.

Haga clic en **Finalizar**. Se visualiza la ventana de configuración de los parámetros del grupo hogar. Desde esta ventana, puede visualizar o cambiar la contraseña de su grupo hogar, salir del grupo hogar o modificar las bibliotecas compartidas.

## 2. Añadir un segundo equipo al grupo hogar

Para agregar un segundo equipo al grupo hogar, configure el equipo para utilizar una ubicación de red tipo **Red doméstica**. Seleccione los elementos que va a compartir en el segundo equipo con los miembros del grupo hogar. Haga clic en el botón **Siguiente**.

Introduzca la contraseña del grupo hogar y haga clic en **Siguiente**.
Haga clic en el botón **Finalizar**; el equipo se acaba de unir al grupo hogar.

Abra una ventana del Explorador de Windows y expanda el nodo **Grupo hogar** para visualizar los recursos compartidos del grupo hogar.

## Introducción a Direct Access

Únicamente disponible en la edición Entreprise de Windows 8, Direct Access es una de las principales novedades de Windows 8. Gracias a esta funcionalidad, podrá conectar con la red corporativa de su empresa desde cualquier red o punto de acceso sin tener que configurar e implementar una conexión de tipo VPN (*Virtual Private Network*) del lado cliente.

Direct-Access utiliza el protocolo de comunicación IPv6 para establecer una conexión segura entre el cliente y el servidor Direct Access. La compatibilidad con los equipos IPv4 actuales está asegurada por los protocolos TEREDO, 6TO4, NAT-PT (*Network Address Translation Protocol*) e ISATAP (*Intra-Site Automatic Tunnel Addressing Protocol*). Direct Access necesita Windows Server 2012 R2 para la implementación de la infraestructura en el lado servidor.

Para implementar Direct-Access debe disponer previamente de una infraestructura operativa. Esto implica la instalación y configuración de un dominio Active Directory, la implementación de una infraestructura de clave pública (PKI) y la configuración de Direct-Access en un servidor que disponga de acceso externo y dos direcciones públicas consecutivas.

El servidor Direct Access debe disponer igualmente de un servidor web para determinar la ubicación de los equipos clientes.

La implementación de esta funcionalidad sobrepasa el marco de este libro, pero puede ser útil saber que cuando el equipo está conectado a través de Direct-Access a su infraestructura, la ejecución del comando **ipconfig** permite comprobar la presencia del túnel 6TO4 y la utilización de direcciones del tipo IPv6.

La ejecución del comando **gpresult /R /scope COMPUTER** permite comprobar la aplicación de los parámetros de directivas necesarios para el funcionamiento de Direct-Access.

## Las conexiones inalámbricas

El estándar IEEE 802.11 define dos modos de conexión:

- **Modo infraestructura**: los clientes inalámbricos se conectan a un punto de acceso.
- **ad-hoc**: los clientes se conectan entre sí sin ningún punto de acceso.

Existen cinco estándares principales de conexión inalámbrica: 802.11a, 802.11b, 802.11g, 802.11n y 802.11ac. La norma 802.11n es la que se utiliza normalmente, dado que dispone de una mejor banda ancha y tiene mayor seguridad.

Para comunicar con la red inalámbrica, el equipo debe disponer de un adaptador.

Esto puede ser una tarjeta PCI que disponga de antena, una tarjeta PCMCIA si tiene un ordenador portátil o un adaptador USB (recomendado si el equipo dispone de puertos USB 2.0).

Si no se instala automáticamente, debe instalar el controlador del adaptador Wi-Fi. Si observa que no funciona correctamente, siempre tiene la posibilidad de descargar el último controlador disponible desde el sitio del fabricante. Para comprobar si el controlador está bien instalado, acceda al Controlador de dispositivos y abra la rama **Adaptadores de red**.

## 1. Configuración de una red inalámbrica

Una manera simple de configurar una red inalámbrica es utilizar un servicio llamado **Configuración automática WLAN**.

Compruebe que el **Administrador de servicios**, esté iniciado.

Si el adaptador está correctamente instalado, la conexión inalámbrica se detectará automáticamente. A continuación, debe proceder del siguiente modo:

Desde el **Panel de control**, en la sección **Redes e Internet - Centro de redes y recursos compartidos**, haga clic en la opción **Configurar una nueva conexión o red**. Seleccione la opción **Conectarse a Internet** y haga clic en el botón **Siguiente**. Seleccione la conexión de tipo **Inalámbrica**.
Seleccione la conexión Wi-Fi y haga clic en el botón **Conectar**.

En el Livebox hay un botón pulsador que se encuentra al lado de la antena Wi-Fi; púlselo.

En el cuadro de texto **Clave o frase de contraseña de seguridad:**, indique la clave de seguridad de su red Wi-Fi. Hay diferentes formatos de claves dependiendo del nivel de seguridad de su instalación. Los dos principales tipos de claves de seguridad son los siguientes: WEP (*Wired Equivalent Privacy*) y WPA/WPA2 (*Wi-Fi Protected Access*). Indique la clave de conexión y pulse el botón **Conectar**.
Deje las dos casillas marcadas (**Guardar esta red** y **Conectarse automáticamente a esta red**) y haga clic en **Cerrar**.
Compruebe que delante de **Intensidad de la señal** aparece la siguiente valoración: **Excelente**.

## 2. Creación manual de un perfil de conexión Wi-Fi

Esto se utiliza sobre todo para preconfigurar una conexión inalámbrica no disponible en ese momento pero cuya configuración básica conoce.

En el **Centro de redes y recursos compartidos**, haga clic en el enlace **Configurar una nueva conexión o red**.
Seleccione el botón **Conectarse manualmente a una red inalámbrica** y haga clic en **Siguiente**.
Introduzca un nombre para esta conexión.
En las listas desplegables visibles debajo, seleccione el tipo de autenticación y el tipo de cifrado que se utilizará.
Introduzca la clave de seguridad o la contraseña y haga clic en **Siguiente**.
Pulse el botón **Conectar** o **Cerrar**.

## 3. Configuración de su conexión inalámbrica

De la misma manera que una conexión de red clásica, puede cambiar la dirección IP o configurarla utilizando el DHCP en automático:

Acceda al **Centro de red y recursos compartidos**.
Haga clic en el enlace **Cambiar configuración del adaptador**.
Haga doble clic en la conexión inalámbrica. A continuación haga clic en el botón **Propiedades inalámbricas**.

En la pestaña **Seguridad**, puede seleccionar el tipo de autentificación y de cifrado, y también introducir una nueva clave de seguridad para su conexión.

## 4. Configuración de una conexión ad hoc

Este tipo de red puede utilizarse para compartir recursos con otros ordenadores, iniciar un juego en modo multijugador o compartir una conexión a Internet con amigos.

Imaginémonos que debe administrar una red con tres ordenadores. Este es el procedimiento que debería seguir en un equipo host:

Debe utilizar la herramienta **netsh** para crear e implementar una red ad hoc inalámbrica.

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando: **netsh wlan show drivers**.

Este comando permite comprobar si su interfaz de red soporta este tipo de configuración de red. Compruebe que la respuesta al comando anterior es sí en la línea **Red hospedada admitida**.

A continuación introduzca este comando: **netsh wlan set hostednetwork mode=allow ssid=nombrered key=newpass1**

Reemplace la SSID y la clave (key) por valores personalizados.

Inicie la red con el comando: **netsh wlan start hostednetwork**

Una vez iniciada la red ad hoc, si quiere navegar por Internet desde esa red, debe compartir su conexión Wi-Fi estándar.

Si quiere detener la red ad hoc, introduzca el comando: **netsh wlan stop hostednetwork**

## 5. Exportación de un perfil de red inalámbrico

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando para ver los perfiles de conexión inalámbrica: **netsh wlan show profiles**

Imaginemos ahora que quiere exportar este perfil a una llave USB cuya letra de unidad es H:, bastará con introducir este comando: **netsh wlan export profile name="vínculo en modo infrastructura" folder="h:\guardar"**. El archivo generado estará en formato XML en la carpeta (que debería haber creado antes) llamada "Guardar".

A la inversa y para poder importar un perfil inalámbrico, utilice este comando: **netsh wlan add profile filename="h:\Guardar\conexión de red inalámbrica - Vínculo en modo infraestructura.xml"**

## 6. Impedir que Windows se conecte a una red ad hoc

El riesgo subyacente es que el ordenador pueda conectarse de forma accidental a una red inalámbrica. Esto supone un peligro, ya que podría ser víctima de un ataque con la intención de entrar en su sistema. Le explicamos una manera simple de impedir conexiones indeseadas:

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando que permite mostrar una lista de los filtros eventualmente aplicados: **netsh wlan show filters**

Para bloquear cualquier conexión en modo ad hoc, introduzca el siguiente comando: **netsh wlan add filter permission=denyall networktype=adhoc**
Introduzca de nuevo el primer comando para comprobar que el filtro se ha guardado correctamente: **netsh wlan show filters**

Para eliminar este filtro, debe utilizar el siguiente comando: **netsh wlan delete filter permission=denyall networktype=adhoc**

# Las herramientas útiles para la red

Existe un gran número de herramientas que se pueden lanzar desde el Símbolo del sistema. Deberá utilizar el Símbolo del sistema como administrador.

## 1. Ping

Es el acrónimo de *Packet InterNet Groper*. Esta utilidad funciona como un sonar y envía una solicitud de eco ICMP (*Internet Control Message Protocol*) a una estación de la red. El comando permite determinar el tiempo necesario para que el paquete alcance la red, lo que sirve para comprobar si una estación está conectada a la red o la disponibilidad de un servidor. Una estación puede designarse con su nombre o con su dirección IP. Los modificadores principales son:

- **-t**: las señales se transfieren hasta que el usuario interrumpe el proceso pulsando la combinación de teclas [Ctrl] + C.
- **-a**: si la resolución del nombre se efectúa de manera correcta, el comando mostrará el nombre del host correspondiente.
- **-n <número>**: esta opción permite establecer el número de señales emitidas. El valor predeterminado es 4.
- **-l <longitud>**: esta opción permite establecer la longitud del paquete de datos (de 0 a 65.000 bytes). El valor predeterminado es 32 bytes.
- **-f**: este parámetro impide la fragmentación de los paquetes.
- **-s <valor>**: se utiliza un valor para definir una evaluación del tiempo de respuesta de un ordenador remoto.
- **-k <Lista Host>**: permite definir una ruta de origen libre para la transferencia de paquetes (los valores posibles van del 1 al 4).
- **-j <Lista Host>**: permite definir una ruta "de origen estricto".
- **-w <tiempo de espera>**: permite definir el tiempo de espera hasta que la estación correspondiente se declara como inaccesible. El valor se expresa en milisegundos y por defecto es 4000.
- **-4**: permite forzar la utilización de IPv4.
- **-6**: permite forzar la utilización de IPv6.

## 2. Tracert

El comando **tracert** determina el tiempo necesario para que los paquetes se transfieran a un router. Los modificadores son los siguientes:

- **-d**: si no desea que el comando resuelva y muestre los nombres de todos los routers de la ruta de acceso.
- **-h**: permite limitar el número de saltos para alcanzar el destino. El valor predeterminado es 30 saltos.

- **-j**: permite definir una ruta de origen libre para identificar el tiempo de reacción de los routers.
- **-w <tiempo>**: permite definir un valor en milisegundos más allá del cual se declara el router como inaccesible.
- **-4**: permite forzar la utilización de IPv4.
- **-6**: permite forzar la utilización de IPv6.

Introduzca, por ejemplo: **tracert microsoft.com**. El comando realiza un seguimiento de la ruta tomada por la solicitud para alcanzar el sitio del editor.

## 3. Ipconfig

Este comando muestra todos los valores actuales de la configuración de la red TCP/IP y actualiza los parámetros de DHCP (*Dynamic Host Configuration Protocol*) y DNS (*Domain Name System*). También resulta muy útil en los equipos configurados para obtener de manera automática una dirección IP. Si se utiliza sin modificadores, **ipconfig** muestra la dirección IP, la máscara de subred y la puerta de enlace predeterminada de todos los adaptadores de red. Los principales modificadores son:

- **/all**: permite mostrar toda la información disponible relacionada con los adaptadores de red activos. Este comando muestra todas las configuraciones de sus conexiones de red.

- **/renew <adaptador>**: renueva la configuración DHCP de todos los adaptadores (si no se especifica ninguno) o del adaptador determinado si se incluye el valor del **adaptador**.
- **/renew6 <adaptador>**: renueva la configuración DHCP para el protocolo IPv6.
- **/release <adaptador>**: permite liberar la configuración DHCP actual y anular la configuración de dirección IP de todos los adaptadores (si no se especifica ninguno) o de un adaptador determinado si se incluye el valor del **adaptador**.
- **/release6 <adaptador>**: libera la configuración DHCP para el protocolo IPv6.
- **/flushdns**: restaura el contenido de la caché de resolución del cliente DNS. Le aparecerá el siguiente mensaje: "Se vació correctamente la caché de resolución DNS".
- **/displaydns**: muestra el contenido de la caché de resolución del cliente DNS.
- **/registerdns**: comienza un registro dinámico manual de los nombres DNS y las direcciones IP configuradas en un equipo. Puede utilizar este parámetro para resolver problemas de error de registro de nombres DNS o problemas de actualización dinámica entre un cliente y el servidor DNS sin reinicio del cliente. En Windows, le aparecerá el siguiente mensaje: "Se ha iniciado el registro de los recursos DNS para todos los adaptadores de este equipo. Se reportará cualquier error en el visor de sucesos en 15 minutos".

## 4. Netstat

El comando **netstat** muestra las conexiones TCP activas, los puertos en los que el equipo realiza la escucha, la tabla de enrutamiento IP, así como las estadísticas Ethernet, IPv4 e IPv6. Sin configuración, el comando mostrará las conexiones activas. Los principales modificadores son:

- **-a**: muestra todas las conexiones TCP activas, así como los puertos TCP y UDP que el equipo utiliza para la escucha.

- **-e**: muestra las estadísticas Ethernet y el número de bytes de los paquetes enviados y recibidos.
- **-n**: muestra las conexiones TCP activas seleccionadas en orden numérico.
- **-o**: muestra las conexiones TCP activas e incluye el ID del proceso (PID) de cada conexión.
- **-p <protocolo>**: muestra las conexiones que utilizan el protocolo indicado (TCP, UDP, TCPv6, etc.).
- **-s**: muestra las estadísticas de las conexiones de red por protocolo.
- **-r**: muestra el contenido de la tabla de enrutamiento IP. También puede utilizar el comando **route print**.

En el Símbolo del sistema, introduzca: **netstat -an |find /i "listening"**

Obtendrá una lista de los puertos de escucha de su equipo.

Si desea realizar un redireccionamiento a un archivo de salida en formato de texto, introduzca: **netstat -an |find /i "listening" > c:\ports.txt**

Para ver los puertos utilizados en ese momento, teclee: **netstat -an |find /i "established"**

A la izquierda se enumerarán las direcciones locales y a la derecha, las remotas.

En este ejemplo, podemos ver que la dirección IP del equipo es: 192.168.0.202. Se crea una conexión hacia un equipo con la dirección IP 216.58.210.134. Esta corresponde al sitio español de Google. Por otra parte, el puerto de escucha es el 443 (que se utiliza para ver páginas web).

El comando **netstat -o** muestra el ID del proceso utilizado para cada conexión.

El comando **netstat -a** ofrece una vista completa de los puertos abiertos, cerrados y utilizados.

Para mostrar las aplicaciones que comunican con el exterior, introduzca este comando: **netstat -b 5 > log.txt**.

Al cabo de algunos minutos, pulse las teclas [Ctrl]+C para interrumpir la ejecución del comando. A continuación, teclee lo siguiente: **notepad log.txt**. Puede ver el archivo de registro generado con el Bloc de notas de Windows.

## 5. Nbtstat

Es el equivalente al comando **netstat**, pero para conexiones NetBIOS sobre TCP/IP. Mediante este comando también puede volver a cargar el archivo *Lmhosts* en la caché NetBIOS.

- **-a <nombre remoto>**: muestra la tabla de nombres de una estación remota utilizando su nombre NetBIOS.
- **-A <dirección IP>**: lo mismo que en el caso anterior pero, utiliza la dirección IP.
- **-c**: muestra el contenido de la caché de nombres NetBIOS, la tabla de nombres NetBIOS y las direcciones IP correspondientes.

- **-n**: muestra la tabla de nombres NetBIOS del equipo local.
- **-r**: muestra las estadísticas de resolución de los nombres NetBIOS.
- **-R**: depura y vuelve a cargar el archivo LmHosts sin tener que reiniciar el equipo.
- **-RR**: libera y actualiza los nombres NetBIOS para el equipo local registrado por servidores WINS.
- **-s**: muestra las sesiones NetBIOS sobre TCP/IP para intentar convertir la dirección IP de destino en un nombre.
- **-S**: lo mismo que en el caso anterior salvo que las direcciones IP no se resuelven en nombres.
- **<intervalo>**: vuelve a mostrar las estadísticas seleccionadas, indicando una pausa igual a "intervalo" en segundos entre cada muestra. La combinación de teclas [Ctrl]+C interrumpe el ciclo de estadísticas.

### 6. Limpiar la caché ARP

El protocolo de resolución de direcciones (*Address Resolution Protocol* o ARP) es un protocolo que permite traducir una dirección de protocolo de la capa de red (una dirección IPv4) en una dirección MAC. En IPv6, ARP se ha reemplazado por "ICMP para IPv6" (*Internet Control Message Protocol Version 6*).

Este procedimiento funciona en todas las versiones de Windows. El hecho de no poder navegar por internet puede venir de un problema de corrupción de la caché ARP. Para saber a qué atenerse, intente probar con el comando ping seguido de la dirección del bucle local (127.0.0.1) o la dirección local del equipo. A continuación, realice la misma comprobación, pero elija una dirección IP de un sitio remoto (microsoft.com o google.com). Si puede "pingear" una dirección local pero no una remota, la caché ARP es claramente la causa. En ese caso, le indicamos la solución:

Abra una ventana de Símbolo del sistema en modo administrador.
Introduzca el siguiente comando: **netsh interface ip delete arpcache**

Reinicie el equipo.

CAPITULO 10. REPARACION DE REDES

## Introducción

En este capítulo, vamos a revisar los principales problemas que podrá encontrar en la instalación de una red.

## Nociones de reparación de redes

Le presentamos a continuación los principales elementos de configuración que deberá comprobar.

### 1. Nombre del grupo de trabajo

En el Panel de control, en la sección **Sistema y seguridad - Sistema**, seleccione la opción **Configuración avanzada del sistema**.
Haga clic en la pestaña **Nombre de equipo** y en el botón **Cambiar...**.

Puede cambiar el nombre del equipo, así como el del grupo de trabajo. A continuación, deberá reiniciar.

En un equipo con Windows 8, puede acceder a esta opción desde el Escritorio.

En Windows 10, también puede modificar esta opción desde la nueva pantalla de gestión de la configuración del ordenador.

## 2. Activación NetBIOS sobre TCP/IP

Acceda a las propiedades de la conexión de red.
Seleccione el protocolo TCP/IPv4 y haga clic en **Propiedades**.
Haga clic en el botón **Configuración avanzada...** y en la casilla **WINS**.
Seleccione el botón de opción **Predeterminada** o la opción **Habilitar NetBIOS a través de TCP/IP**.

## 3. Configuración correcta del Firewall

Los puertos siguientes deben estar abiertos si desea beneficiarse del uso compartido de archivos y comunicaciones SMB (*Server Message Block*):

- Puerto TCP 139, puerto UDP 137 y 138 (”SMB de uso compartido de archivos de Microsoft”).
- Puerto TCP 445 (”Tráfico de SMB de host directo sin protocolo NetBIOS”).

Si utiliza firewalls de conexión a Internet, su interfaz de red debe ser parte de las interfaces de confianza.

Para configurar el firewall de Windows 10, siga el procedimiento siguiente:

Desde el **Panel de control**, en la sección **Sistema y seguridad - Firewall de Windows**, haga clic en la opción **Permitir una aplicación o una característica a través de Firewall de Windows**.
Haga clic en el botón **Cambiar la configuración**. Seleccione la funcionalidad **Compartir archivos e impresoras**, permita la ejecución de este programa a través del firewall para la ubicación de red de tipo Privada como debería ser para su entorno. Haga clic en **Aceptar**.

Compruebe que estos tres servicios estén arrancados correctamente: Cliente DHCP, Servidor y Estación de trabajo.

## 4. El tipo de nodo de red

El tipo de nodo determina el método de resolución de los nombres NetBIOS en direcciones IP. Utilizamos el término de difusión (en inglés, Broadcast) para designar el mecanismo que permite a un equipo direccionar los paquetes de datos a varios equipos presentes en la red. Existen cinco tipos diferentes de nodos:

- Nodo B (o B-node, B por Broadcast): hace que un equipo solo utilice la difusión para resolver nombres NetBIOS en direcciones IP.
- Nodo P (o P-node, P por "Point to Point" o "Vínculo punto a punto"): en este caso, un equipo se dirigirá directamente a su servidor WINS para la resolución de nombres.
- Nodo M (M-node, Mixto): obliga al equipo a utilizar el nodo B y en caso de error, utilizará el nodo P.
- Nodo H (H-node, nodo Híbrido): el equipo utiliza los nodos P y si el servidor WINS no puede resolver el nombre, utilizará el nodo B.
- Nodo B avanzado (B+ -node): obliga a utilizar la difusión y el archivo Lmhosts.

En el Símbolo del sistema, introduzca: **ipconfig /all**.

Frente a **Tipo de nodo** aparece el mensaje **Desconocido** o **Híbrido**.

En caso de que no sea así:

Desde el Editor del Registro, abra: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters.
Elimine una entrada que lleva uno de estos dos nombres: NodeType o DhcpNodeType.
Reinicie el equipo.

### 5. Acceso a un equipo en el que el uso compartido simple está desactivado y sin contraseña

Si desea acceder a los recursos compartidos sin tener que identificarse cada vez, asegúrese de que las directivas siguientes estén configuradas de este modo en el equipo remoto:

En el Editor de directivas de grupo, abra el siguiente árbol: Configuración del equipo/Configuración de Windows/Configuración de seguridad/Directivas locales/Opciones de seguridad.
Desactive esta directiva: **Cuentas: limitar el uso de cuentas locales con contraseña en blanco solo para iniciar sesión en la consola**.
Active esta directiva: **Acceso a redes: permitir la aplicación de los permisos Todos a los usuarios anónimos**.

## El explorador de red: WS-Discovery

Antes de Windows 7 y Windows Vista, el servicio ”Explorador de Windows” determinaba todos los equipos de la red local por medio del protocolo NetBIOS. En el arranque, cada equipo se anuncia con una difusión en la red local. Este modo de funcionamiento todavía es operativo para las versiones anteriores a Windows Vista. Windows 8 y Windows 10 soportan este modo de funcionamiento para ser compatibles con sistemas operativos anteriores. De todos modos, las últimas generaciones de sistemas operativos Windows utilizan la función **Host de proveedor de detección de función** y el **Web service-Dynamic Discovery (WS-Discovery)** para encontrar otros ordenadores de la red del mismo tipo. Utilizando este protocolo, el equipo que busca visualizar los recursos de la red envía una petición de tipo multicast y no una difusión a todo el segmento de red.

Cuando explore la red en un equipo Windows 8 puede observar, por ejemplo, la presencia de dispositivos multimedia. En este caso, Windows 8 utiliza el servicio Dispositivo host de UPnP y el protocolo SSDP (*Simple Service Discovery Protocol*, o Servicio de descubrimientos SSDP).

Cuando active la detección de redes, el firewall se configura automáticamente para permitir la comunicación de los dispositivos en la red. WS-Discovery utiliza el protocolo SOAP (*Simple Object Access Protocol*) a través del puerto UDP 3702. La dirección Multicast de difusión es la dirección 239.255.255.250 para IPv4 y FF2::C para IPv6.

En caso de problemas con la detección de dispositivos de red, compruebe que estén iniciados los siguientes servicios:

- Host de proveedor de detección de función.
- Publicación de recurso de detección de función.

- Detección SSDP.
- Dispositivo host de UPnP.

Compruebe igualmente la configuración del firewall. Para permitir la búsqueda de redes a través del firewall, desde el Panel de control, en la sección **Sistema y seguridad - Firewall de Windows**, haga clic en la opción **Permitir un programa o una característica a través de Firewall de Windows**.
Haga clic en el botón **Cambiar la configuración**. Seleccione el programa **Detección de redes** y permita la ejecución de este programa a través del firewall para la ubicación de red de tipo Privada. Haga clic en el botón **Aceptar**.

# Problemas de conectividad

Compruebe que el Firewall no bloquee los puertos utilizados para el uso compartido de archivos e impresoras.

Compruebe que puede pingear los demás equipos.

Si puede pingear una dirección IP, pero no un nombre de equipo, a menudo se debe a un problema de permisos NTFS.

Si puede pingear una dirección IP o un nombre de equipo pero no puede asignar una letra de unidad, utilice el comando: **net view \\Equipo_remoto**

Si obtiene un error número 5, se trata de un problema de permisos:

En el Editor del Registro, abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
Edite un valor DWORD llamado RestrictAnonymous.
Introduzca como información del valor la cifra 0.
Reinicie el equipo.

Si le aparece un error 51, debe activar el uso compartido de archivos e impresoras.

## 1. "Medios desconectados"

También le puede aparecer el error: "Compruebe que el interruptor de red está encendido en el equipo". La siguiente solución provisional funciona: cambie su adaptador de red inalámbrica y, al cabo de un rato, vuelva a colocar su adaptador antiguo.

## 2. La dirección IP es de tipo 169.254.X.X

Se trata de una dirección APIPA y se le asigna cuando el equipo no puede obtener una IP válida del servidor DHCP (y si tiene activado el direccionamiento automático). APIPA (*Automatic Private Internet Protocol Addressing*) es un servicio de Windows que le permite asignar de manera automática una dirección IP a un equipo. El rango de direcciones IP utilizado es el siguiente: 169-254-0-0/16.

Por lo general, esto se debe a un problema de conectividad (lógica o física) o al hecho de que el servicio DHCP no ha sido iniciado.

Si un equipo se desconecta de un segmento de red para conectarse a otro segmento sin llegar a conseguirlo, se trata de un problema de error de registro de nombres DNS. En ese caso, compruebe las direcciones IP que ha configurado de manera manual para los demás equipos que forman la red. Por otra parte, intente desactivar el firewall de conexión a Internet y compruebe que el adaptador de red está instalado correctamente. Utilice este comando: **ipconfig /registerdns**.

## 3. Su dirección IP es de tipo 0.0.0.0

Otro equipo está utilizando la misma dirección IP.

## 4. No se asigna ninguna dirección IP

Además se indica que la conexión es limitada o nula. En muchos casos basta con reparar la pila Winsock utilizando, por ejemplo, desde un Símbolo del sistema en modo administrador el comando **netsh winsock reset** y reiniciando el ordenador.

También puede ser que la dirección IP esté reservada para otra interfaz de red:

En el Administrador de dispositivos active la opción de mostrar los dispositivos ocultos.
Desinstale los elementos que aparezcan en la rama **Adaptadores de red**.

## 5. "Se intentó realizar una operación en un elemento que no es un socket"

Por lo general, el equipo es capaz de recibir paquetes IP pero no de enviarlos. La pila Winsock está dañada y debe restaurarla como se explicó anteriormente.

## 6. No es posible renovar la dirección IP de una conexión de red

En el Símbolo del sistema introduzca:

- **ipconfig /release**
- **ipconfig /renew**

Si este último comando no funciona, puede ser que la clave Winsock2 esté dañada. El procedimiento para comprobarlo es el siguiente:

Haga clic en **Inicio - Ejecutar** e introduzca : **msinfo32.exe**.
Abra las ramas **Componentes - Red - Protocolo**.

Deben aparecer dos tipos de componentes:

- Tcpip MSAFD (cuatro ramas)
- Proveedor de servicio RSVP (cuatro ramas)

Si aparecen otros mensajes, es posible que otro programa haya dañado la pila Winsock. En ese caso deberá repararla como se explicó anteriormente.

## 7. Problemas de conexión con los juegos en red

También puede aparecer este tipo de error: "NET_SedPacket ERROR: NO ERROR". Por otra parte, las transferencias de datos desde un dispositivo IP son muy lentas.

Acceda a las propiedades de la conexión de red.
Seleccione la casilla **Planificador de Paquetes QoS** y haga clic en **Desinstalar**.

# Problemas de acceso a la red

Estos problemas son rara vez físicos, pero son síntomas de un problema de configuración. Debe comprobar dos cosas:

- La configuración del firewall. Asegúrese de que el uso compartido de archivos e impresoras está permitido.
- La conexión de su tarjeta de red y la dirección IP asignada a su equipo, que no debe ser una dirección APIPA, es decir, diferente del rango de direcciones IP 169.254.0.0/16

## 1. "No se encontró la ruta de red"

Active el NetBIOS sobre TCP/IP como se ha explicado anteriormente.

## 2. No es posible ver los demás equipos de un grupo de trabajo

"La lista de servidores de este grupo de trabajo no está disponible actualmente" o "Puede que no tenga los permisos necesarios". El comando **net view** da un error de sistema 6118. Puede pingear los equipos entre sí pero no puede acceder a las redes favoritas.

En el Símbolo del sistema, introduzca: **ipconfig /all**.
Compruebe la mención que aparece situada frente al tipo de nodo.

Si la indicación dice: "Peer-Peer", el equipo está configurado en el modo p-node. En este modo, las solicitudes de resolución de nombres de equipo se enviarán directamente al servidor WINS en modo punto a punto. Como no existe un servidor WINS que asegure la resolución de nombres NetBIOS, los equipos no se pueden identificar.

En el Editor de Registro, abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters.
Elimine los valores: NodeType y DhcpNodeType.

También puede ser que el protocolo NetBIOS no esté activado:

Acceda a las propiedades de la conexión de red.
Seleccione la opción **Protocolo de Internet versión 4 (TCP/IPv4)** y haga clic en los botones **Propiedades** y **Opciones avanzadas**.
En la pestaña **WINS**, active la opción **Habilitar NetBios a través de TCP/IP** y haga clic en el botón **Aceptar**.

## 3. "Red inaccesible o no dispone de permisos..."

Sin embargo, no hay problemas de uso compartido si asigna una unidad de red mediante el Símbolo del sistema. Utilice este tipo de sintaxis: **net use x:\\nombre_de_equipo\nombre_de_recurso_compartido**, en la que x: es la letra de la unidad que desea asignar al recurso compartido.

En el equipo que inicie primero, abra el Registro de Windows.
Abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ Browser\Parameters.
Edite un valor de cadena llamado MaintainServerList e introduzca como información el valor "Yes".
Realice lo contrario en los demás equipos de la red (pase de "Yes" a "Auto").

## 4. Puede pingear una dirección IP pero no un nombre de equipo

En resumen, en uno de los equipos no puede acceder al entorno de red.

En el Símbolo del sistema introduzca el comando: **net view Nombre_de_equipo**

Si le aparece el error nº53, tiene un problema de resolución de nombres.

Debe comprobar que NetBIOS sobre TCP/IP está activado y que el servicio Examinador de equipos está iniciado.

Introduzca el comando: **net use Z: \\Dirección_IP\Nombre_de_recurso_compartido**

Si aparece el error n°5 "Acceso denegado", tiene un problema de permisos. Compruebe que el uso compartido de archivos e impresoras está activado, que el nombre del grupo de trabajo sea el mismo y que esté conectado con el mismo nombre de usuario y contraseña en todos los equipos de la red.

Si, por el contrario, debe acceder a un ordenador que no forma parte del grupo de trabajo, deberá activar el uso compartido simple de archivos: en el Explorador de Windows, haga clic en el menú **Vista**. En la cinta del explorador, haga clic en el botón **Opciones**. En la pestaña **Ver**, marque la casilla **Utilizar uso compartido simple de archivos (recomendado)**.

## 5. No es posible renovar una dirección IP

Tampoco puede reparar las conexiones de red haciendo clic con el botón secundario del ratón y seleccionando la opción correspondiente. Resetee el router.

## 6. Error 67: "No se pudo encontrar el nombre de red"

Realice una comprobación en el Símbolo del sistema introduciendo los comandos: net use Nombre_de_unidad: \\Nombre_de_equipo\Nombre_de_recurso _compartido. Por ejemplo: net use N: \\Equipo1\Carpetas. No se le pedirá ningún nombre de usuario ni contraseña. Le aparecerá solo un mensaje: "La operación se completó correctamente".

Si, desde Mi PC, intenta acceder al lector de red le aparecerá este error: "Nombre_de_unidad:\ no está accesible - Acceso denegado", se trata de un problema de permisos NTFS de las carpetas compartidas. Compruebe que los usuarios con los que comparte los recursos disponen de los permisos necesarios.

## 7. No es posible examinar la red

Sin embargo, puede utilizar una ruta UNC para asignar un recurso de red. Debe tener activado NetBIOS sobre TCP/IP en las propiedades de conexión o configurar el modo de inicio "Automático" de este servicio: Estación de trabajo.

## 8. Su red va demasiado lenta

- Compruebe los mapas de red.
- Compruebe el buen funcionamiento del Hub o de su Box.
- Compruebe que no tiene ningún virus ni spyware.

## 9. Inicio de sesión muy lento

Este problema ocurre cuando, una vez que vuelve a casa, abre una sesión en una cuenta perteneciente a un dominio. En este caso, el Explorador de Windows es muy lento. Solo tiene que desactivar las conexiones problemáticas mediante el siguiente comando: **net use /delete**.

## 10. El equipo no puede acceder a Internet

Compruebe que el filtro de direcciones MAC configurado en el router no bloquea la de su ordenador.

## 11. No es posible acceder al entorno de red aunque el acceso a Internet funciona

Se trata de un problema de configuración del Firewall.

## 12. Puede pingear un sitio pero no navegar por Internet

En Símbolo del sistema introduzca: **telnet www.google.es 80**.

Si le aparece el error "No se puede abrir la conexión al host, en puerto 80: Error en la conexión", puede suponer que existe una mala configuración del firewall.

Si lo ha desactivado y todavía tiene problemas de conexión, compruebe que el problema no está relacionado con una desinstalación incompleta de Norton Antivirus. Si fuera el caso, realice una desinstalación completa del programa con ayuda de las herramientas proporcionadas por el fabricante. Solo tiene que lanzar una búsqueda en Google: **desinstalar norton site:symantec.com**. Otra solución posible consiste en reinstalar el adaptador de red.

## 13. No hay conexión de Internet

Sin embargo, puede pingear una dirección IP o un nombre de dominio. El comando Ipconfig reenviará la información correcta. Esta es una solución posible:

Desconecte el router.
Espere unos minutos y vuelva a conectarlo.
En Símbolo del sistema, introduzca estos dos comandos:

- **ipconfig /release**
- **ipconfig /renew**

Los dos comandos van a permitirle renovar la configuración DHCP de todas las interfaces de red.

# Problemas con el comando ping

El comando Ping es fuente de numerosos problemas que son síntomas de una mala configuración de la red.

## 1. No es posible pingear su propia dirección IP

Se debe a un problema de configuración del firewall que bloquea el funcionamiento del comando **ping** o a un problema físico.

## 2. El comando ping devuelve el código de error n° 5

Señalemos, además, que no le es posible navegar por Internet.

Esto se debe, por ejemplo, a una desinstalación incompleta del firewall de conexión a Internet o de otro programa antivirus.

Abra el Administrador de dispositivos.
Haga clic en **Ver - Mostrar dispositivos ocultos**.
Abra la rama Dispositivos que no son Plug and Play.
Desinstale los elementos relacionados con el programa que no se ha desinstalado completamente.

Si el problema viene de una desinstalación incompleta de un firewall como Kerio, deberá eliminar este tipo de controladores: **Kerio HIPS Driver**. Puede que necesite desactivar los dispositivos fantasma si no puede desinstalarlos.

## 3. No es posible acceder al controlador NetBT - "NetBT no se puede cargar"

En el Editor del Registro, abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\netbt.
Edite un valor de cadena llamado Start.
Introduzca como información del valor la cifra 2.
Abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\ netbt\Parameters.
Edite un valor de cadena llamado TransportBindName.
Introduzca como información del valor lo siguiente: **\Device**.

# Problemas de acceso a los recursos

A menudo estos errores son signo de problemas aleatorios de conectividad. Compruebe que no hay fallos de cableado o malos contactos.

## 1. No es posible ver los recursos compartidos

Configure el router de manera que la asignación de direcciones IP se realice manualmente y no en modo automático.

## 2. "Nombre_de_equipo no es accesible - No tiene permiso de acceso al recurso"

Sin embargo, puede acceder a cualquier directorio compartido mediante una ruta UNC (\\Nombre_de_equipo\Nombre_de_recurso compartido). Por otra parte, la lista de recursos compartidos sí que aparece. Se trata de un problema corriente en redes mixtas.

En el equipo host, abra el Editor del Registro.
Abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\ Lsa.
Edite un valor DWORD llamado RestrictAnonymous.
Introduzca como información del valor la cifra 0.
Reinicie el equipo.

## 3. "Nombre_de_recurso_compartido no es accesible"

El mensaje continúa así: "Puede que no tenga permiso para utilizar este recurso de red. Póngase en contacto con el administrador de este servidor para comprobar si tiene permisos de acceso" - "Espacio de almacenamiento insuficiente en el servidor para procesar este comando".

En el Editor de Registro, abra HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\LanmanServer\Parameters.
Edite un valor DWORD llamado IRPStackSize.

En algunos casos, deberá crearlo.

Introduzca como información del valor el número hexadecimal F (15 en base decimal).

Como regla general, tendrá que aumentar con 3 unidades el valor inicial.

## 4. No se puede acceder a una carpeta compartida

Compruebe que el nombre de la carpeta compartida tiene menos de 15 caracteres.

## 5. "Error 71"

El mensaje de error completo es el siguiente: "No se pueden realizar más conexiones a este equipo remoto en este momento ya que hay más de las que puede aceptar". Este problema ocurre cuando un ordenador ha alcanzado el límite de conexiones activas permitidas y no puede responder a ninguna solicitud adicional. Puede ver el número de sesiones abiertas introduciendo en el Símbolo del sistema el siguiente comando: **net session**.

En el editor del Registro, abra HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\LSA.
Edite un valor DWORD llamado RestrictAnonymous.
Introduzca como datos del valor la cifra 2.

Este valor permite restringir el número de conexiones de sesión anónima. Se configurará la directiva correspondiente con la opción "No obtener acceso sin permisos anónimos explícitos".

No olvide que una sesión también puede ser una conexión anónima procedente del uso compartido de archivos, impresoras, intercambios mediante una conexión de canalización con nombre, etc.

### 6. No es posible ejecutar un archivo script desde una ubicación de red

En Internet Explorer, haga clic en **Herramientas - Opciones Internet...**.
Seleccione la pestaña **Seguridad** y pulse sobre el icono **Sitios de confianza**.
Haga clic en el botón **Sitios...**.
En el cuadro de texto **Agregar este sitio web a la zona de:**, introduzca la IP del equipo. Por ejemplo, **192.168.0.100**.
Confirme pulsando **Aceptar** y reinicie el equipo.

### 7. "No es posible copiar el archivo - Ruta de acceso demasiado larga..."

A pesar de lo que parece, se trata de un problema físico (normalmente el cable o el Box están defectuosos).

## Problemas con las funciones DHCP

Si ha elegido un modo de direccionamiento automático, puede encontrarse con algunos problemas, pero casi siempre bastante inofensivos...

### 1. No es posible obtener una dirección IP de un servidor DHCP

No puede renovar la concesión DHCP que determina el principio y fin de validez de una dirección IP. Asigne una dirección IP fija a la interfaz de red. Si aun así no puede pingear el servidor DHCP, se trata de un problema material. Si puede pingear el servidor DHCP, se trata de un problema de configuración del servidor.

Compruebe la configuración del firewall.
Restablezca el protocolo TCP/IP mediante el comando Netsh.
Reinstale el protocolo TCP/IP.

Estas dos últimas operaciones se explican en el capítulo Internet y movilidad, apartado Problemas de conectividad de red en Internet Explorer 11.

Si utiliza un router y ha activado las funciones DHCP, actualice el firmware del mismo.

Nos gustaría añadir que si se encuentra con este tipo de error: "No es posible realizar la conexión. Error al renovar la dirección IP actual", normalmente se debe a un problema de conexión USB o Ethernet. Solo tendrá que cambiar el cable.

### 2. Las funciones DHCP no funcionan

Sin embargo, no hay problemas de conectividad cuando asigna una dirección IP fija al equipo causante. En muchas ocasiones, bastará con reparar la pila Winsock desde un Símbolo del sistema en modo administrador con el comando **netsh winsock reset** y reiniciando el ordenador.

El problema puede ocurrir con un router, por ejemplo. El indicador de conexión verde indica que la conexión Ethernet se realiza correctamente, pero el icono de conexión de red señala

que no se encuentra la dirección de red. Recordemos que se trata de un problema muy común.

### 3. Conflicto de direcciones con las funciones DHCP

Si dos equipos tienen la misma dirección IP.

Introduzca en el Símbolo del sistema:

- **ipconfig /release**
- **ipconfig /renew**

### 4. No se puede obtener una concesión de DHCP

Cuando introducimos el comando "ipconfig /renew", nos aparece el error: "Se produjo un error al renovar la interfaz de la conexión: Acceso denegado". Normalmente, se debe a que la dirección IP ya está siendo utilizada o está reservada. Solo tendrá que eliminar la reserva otorgada a un equipo en función de su dirección MAC. Puede hacerlo desde el módulo DHCP, en **Herramientas administrativas**.

## Problemas en el módulo de conexiones de red

En este apartado, vamos a explicar únicamente el módulo **Conexiones de red** del Panel de control.

### 1. Existe un tiempo de latencia para poder abrir una aplicación

Este problema se plantea solo al inicio y, a veces, durante la construcción del Escritorio de Windows. Si aparece después de instalar una conexión ADSL, se debe a que la dirección IP ha cambiado al modo automático y esto provoca lentitud al iniciar.

Acceda a las propiedades de la conexión de red y a continuación a las propiedades del protocolo Internet version 4 (TCP/IPv4).
En la pestaña **General** active el botón de opción **Utilizar la siguiente IP**.
Frente a la **Dirección IP**, introduzca una dirección IP fija como la siguiente: 192.168.0.1.
En el cuadro de texto **Máscara de subred**, introduzca la máscara **255.255.255.0** y haga clic en **Aceptar**.

En teoría, no es preciso cumplimentar las demás opciones. La próxima vez que inicie, notará la diferencia.

### 2. "No es posible desconectar en este momento"

El mensaje de error continúa de esta manera: "Esta conexión puede estar usando uno o más protocolos que no admitan Plug and Play o quizá ha sido iniciada por otro usuario o cuenta del sistema".

No podrá desactivar la conexión de red y la única solución es desactivar la interfaz de red mediante el Administrador de dispositivos. Esto puede deberse a que el servicio **Servicios de cifrado** está desactivado:

Haga clic en **Inicio - Ejecutar** e introduzca: **services.msc**.
Abra el servicio "Servicios de cifrado".

En la lista desplegable **Tipo de inicio**, seleccione la opción **Manual** y haga clic en el botón **Iniciar**.

También puede que el servicio esté dañado. En ese caso realice una reparación de los servicios de cifrado:

Reinicie en modo seguro.
En Símbolo del sistema, introduzca los siguientes comandos:

- **net stop cryptsvc**
- **ren %systemroot%\System32\Catroot2 oldcatroot2**
- **net start cryptsvc**

También puede pasar que un tercer programa monopolice el adaptador de red. Por ejemplo, una herramienta Intel que controla la velocidad, el modo de transferencia, etc. del adaptador de red. Esta herramienta no firmada impide liberar el dispositivo correspondiente a la conexión de red. En este caso, solo tendrá que desinstalarlo o actualizarlo.

## 3. No es posible crear un puente de red

El problema puede aparecer si posee una tarjeta Wi-Fi. Cabe recordar que un puente de red permite unir dos interfaces de red como si formaran parte de la misma red local. En este caso, se crea un puente de red, pero no hay tráfico, por lo que no puede hacer un ping al adaptador inalámbrico.

El problema se debe a que muchos adaptadores Wi-Fi no soportan de manera nativa la "promiscuidad" con una red de tipo "clásico".

En el Símbolo del sistema, introduzca: **netsh bridge show adapter**.
Observe que el número de identificación de la interfaz de red no responde.
Introduzca: **netsh bridge set adapter X forcecompatmode=enable**
Reemplace X por el número de interfaz de red que va a crear en modo compatibilidad.
Introduzca de nuevo: **netsh bridge show adapter**.

**ForceCompatibilityMode** debe aparecer, esta vez, como activado.

Ahora desactive el puente de red y vuelva a reactivarlo.

## 4. Pérdida de conectividad inalámbrica

Este problema se produce principalmente por la desactivación accidental de la interfaz de red inalámbrica, especialmente en los equipos portátiles. La reactivación de esta función difiere en función del tipo de máquina. La combinación de las teclas [Fn] y [F3] o [F8] permite reactivar la interfaz de red inalámbrica.

## 5. "Error en el intento de conectar a WMI"

"Asegúrese de que la conexión de red funciona correctamente". Los otros mensajes de error posibles son: "No se pueden mostrar las propiedades de la red. Windows no puede mostrar las propiedades de esta conexión. Es posible que la información de Instrumental de administración de Windows (WMI) se encuentre dañada" o "No es posible mostrar la información del sistema (MSinfo32). Error de conexión al equipo_local debido a un fallo general de WMI".

Haga clic en **Inicio - Ejecutar** e introduzca: **services.msc**.

Haga doble clic en el nombre del servicio: **Instrumental de administración de Windows**.
Haga clic en **Detener**.
En el Explorador de Windows, abra C:\windows\system32\Wbem\repository.
Elimine todos los archivos de la lista y reinicie el equipo.

### 6. Problema de conectividad durante la conexión de un ordenador portátil Windows 8 o Windows 10 a un punto de acceso inalámbrico

Los problemas de conectividad aparecen de manera aleatoria cuando conecta un ordenador portátil con Windows 8 o Windows 10 a un punto de acceso inalámbrico. Estos problemas pueden surgir si el ordenador funciona con batería y pueden ser:

- Conexión inalámbrica interrumpida.
- La conexión muestra bajo rendimiento.

A menudo el origen de este tipo de problema se debe a los puntos de acceso inalámbricos que no soportan el protocolo de ahorro de energía 802.11.

Para resolver este problema, conecte el ordenador portátil a una fuente de alimentación. En este caso Windows sustituye el parámetro de energía **Ahorro de energía** por **Rendimiento máximo** para la tarjeta de red inalámbrica. Esto tiene como efecto desactivar el modo de ahorro de energía 802.11.

Igualmente puede modificar el ahorro de energía utilizado por defecto.

En la zona **Búsqueda** a la derecha del menú **Inicio**, introduzca **Opciones de energía**. Abra esta ventana y a continuación seleccione el vínculo **Cambiar la configuración del plan** del modo de gestión de energía utilizado por defecto.
Seleccione el vínculo **Cambiar la configuración avanzada de energía**.
Expanda el árbol **Configuración de adaptador inalámbrico - Modo de ahorro de energía - Con corriente alterna** y a continuación seleccione la opción **Rendimiento máximo**.

## Problemas específicos en Windows 8 y Windows 10

Sin pretender detallar uno a uno todos los problemas que nos podemos encontrar en estos sistemas operativos, vamos a examinar los puntos más importantes.

### 1. Pérdida de la conexión a Internet al cabo de un rato

Si ejecuta el comando **ipconfig /all**, se indicará claramente al lado del adaptador de red que el dispositivo está deshabilitado. La solución es bastante simple: solo tendrá que acceder al Administrador de dispositivos, activar la visualización de dispositivos ocultos y desactivar una interfaz de software llamada "6to4 adapter" o "Teredo Tunneling Pseudo-Interface".

6to4 es un sistema que permite que los paquetes IPv6 se transfieran en una red IPv4. 6to4 es útil cuando dos hosts desean intercambiar información en IPv6, pero una porción de la red que les separa solo soporta IPv4.

El protocolo TEREDO (*Tunneling IPv6 over UDP through NAT*) consiste en encapsular los paquetes IPv6 sobre IPv4.

## 2. Problema de copia de archivos

Puede que tenga un tiempo de transferencia extremadamente lento o que le aparezca este tipo de mensaje de error: "No hay memoria suficiente para completar esta operación". Es muy evidente que se debe a las unidades de red, pero el problema también puede acarrear interrupciones en la conexión de redes inalámbricas.

Ejecute el Símbolo del sistema como administrador.
Introduzca este comando: **netsh int tcp set global autotuninglevel=disabled**

Reinicie el equipo.

Hay otro truco que puede probar:

Como regla general, compruebe que NetBIOS y el nombre NetBIOS (tanto de entrada como de salida) tienen permisos. A continuación, reinicie el equipo.

## 3. Problema de red mixta con Windows XP y Windows Vista o Windows 7

El nombre del grupo de trabajo en Windows Vista o Windows 7 es "WORKGROUP" y en las versiones anteriores "MSHOME", por lo que no es el mismo. Sin embargo, si realiza una actualización de Windows XP a Windows Vista, este último sistema conservará el nombre del grupo de trabajo antiguo. Esto explica que a veces, equipos que trabajan en Windows Vista o Windows 7 posean nombres de grupo de trabajos diferentes.

Windows Vista o Windows 7 utiliza como carpeta compartida un directorio llamado *Carpeta pública*, mientras que en Windows XP se llama *Documentos compartidos*. Todas las subcarpetas de la *Carpeta pública* se comparten de manera automática. Para compartir otros recursos, bastará simplemente con copiarlos en el mismo directorio.

De manera predeterminada, Windows Vista o Windows 7 no aceptan el uso compartido simple de archivos. Cualquier tipo de acceso a los recursos compartidos (incluido el directorio *Carpeta pública*) necesita un nombre de usuario y contraseña. Hay otros puntos que debemos comprobar:

- La interfaz de red debe declararse como interfaz de confianza en el firewall de conexión a Internet.
- El uso compartido de archivos e impresoras debe activarse en todos los equipos.
- Debe abrir los puertos necesarios en el firewall. Para más detalles, diríjase a la sección Nociones de reparación de redes - Configuración correcta del Firewall de este capítulo.

## 4. "Acceso denegado"

Ese mensaje puede aparecerle cuando intenta instalar una impresora compartida en un equipo que trabaja con Windows 8 (aunque no haya problema para acceder a los demás recursos).

Compruebe que la configuración de Uso compartido de archivos e impresoras es la correcta en el equipo origen.
Compruebe el nombre de este equipo ("Equipo 1", por ejemplo).
Compruebe el nombre de la impresora compartida ("Impresora 1", por ejemplo).
Desde el equipo destino con Windows 8, inicie el asistente Agregar una impresora.
Elija instalar una impresora local.

Seleccione la opción que le permite crear un nuevo puerto.
Cree un puerto local.
Introduzca como nombre este tipo de ruta: **\\Equipo1\Impresora1**.
Solo le quedará indicar la ubicación del controlador de la impresora.

No olvide asignar un nombre diferente a la impresora y establecerla como impresora predeterminada.

## 5. La conexión inalámbrica es muy lenta

Mostramos una solución que funciona si tiene un ordenador portátil:

Desde el **Panel de control** abra la sección **Hardware y sonido** - **Opciones de energía**.
Haga clic en el enlace **Cambiar la configuración del plan** que aparece debajo del plan que ya está configurado.
A continuación, pulse sobre el enlace **Cambiar la configuración avanzada de energía**.
En la lista desplegable seleccione la opción **Alto rendimiento**.

En el ordenador portátil, debe configurar este plan tanto para la opción con batería como con corriente alterna.

Reinicie el equipo.

## 6. Acceso a los archivos compartidos de un equipo Macintosh desde Windows 8

Este problema ocurre porque, por defecto, los protocolos de autenticación LM y NTLM están desactivados en Windows 8. También puede suceder que el equipo Windows vea los equipos que forman parte del grupo de trabajo pero no pueda acceder a los recursos compartidos. De forma más general, es posible que no pueda acceder a un recurso Unix o agregar un dominio Samba.

Desde el **Panel de control** abra la sección **Sistema y seguridad** - **Herramientas Administrativas**.
Abra el acceso directo **Directiva de seguridad local**.
Abra las ramas **Directivas locales y opciones de seguridad**.
Abra la siguiente directiva: **Seguridad de red: nivel de autenticación LAN Manager**.
En la lista desplegable, seleccione la opción: **Enviar LM y NTLM - Usar la seguridad de sesión NTLM2 si se negocia**.

Observe que la opción predeterminada es la siguiente: Enviar solo respuesta NTLM v2.

Si no tiene acceso a la directiva de seguridad local, siga estos pasos:

En el Editor del Registro, abra la rama: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa.
Edite un valor DWORD llamado LmCompatibilityLevel.
Introduzca como información del valor la cifra 1 (en lugar de 3).

## 7. "Nombre de usuario desconocido o contraseña incorrecta"

El problema ocurre cuando se accede con un equipo Windows a recursos de un dominio Active Directory.

En ese caso compruebe su nombre de usuario. Introduzca el nombre de usuario seguido del nombre del dominio de pertenencia como, por ejemplo, juan@miempresa.com

Compruebe que utiliza la contraseña correcta asociada a la cuenta de usuario y respete las mayúsculas.

## 8. No es posible sincronizar los archivos entre un equipo y una carpeta de red

Normalmente se debe a un programa como Panda Antivirus. Bastará con configurar el programa de manera que se excluyan estos archivos del análisis. Consulte el archivo de ayuda que acompaña a su versión del antivirus para saber cómo proceder.

## 9. No se puede acceder a algunas ubicaciones de red

Este problema ocurre cuando el control de cuentas de usuario está activado. En ese caso, los usuarios que pertenecen al grupo de administradores reciben un token de acceso de usuario estándar. Las redes compartidas creadas mediante los scripts de conexión se comparten con un token de acceso estándar y no de administrador. Cuando un administrador que ha recibido un token de acceso de usuario estándar (puesto que el control de cuentas de usuario está activado) realiza una operación que necesita un token de acceso de administrador, le aparecerá una ventana de elevación de privilegios. De este modo, un programa que utilice el token de acceso de usuario estándar puede estar activo a la vez que otro que utilice un token de acceso de administrador (después de confirmar la solicitud de elevación de privilegios). Cuando se asignan las redes compartidas, se las vincula al inicio de sesión en curso utilizando el token de acceso atribuido al proceso. Esto quiere decir que, aunque un usuario abra una ventana de Símbolo de sistema con un token de acceso estándar para asignar una unidad de red, la red compartida no se asignará a los procesos que se ejecuten con permisos de administrador.

La solución consiste simplemente en configurar un valor del Registro llamado EnableLinkedConnections. Este valor autoriza a Windows a compartir las conexiones de red entre un token de acceso filtrado y el token concedido a un miembro del grupo de administradores. El Administrador de seguridad local comprobará si existe otro token de acceso concedido al usuario que ha abierto la sesión actual.

En el Editor del Registro, abra el siguiente árbol: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current Version\Policies\System.
Cree un nuevo valor DWORD llamado EnableLinkedConnections.
Edite este valor e introduzca como información del valor la cifra 1.

## 10. Reparar los errores de red del Escritorio remoto en Windows 8

Puede darse cuenta, por ejemplo, de que al intentar utilizar las funciones de un equipo Windows 8 en un servidor Windows Server 2008, el rendimiento no es satisfactorio. Ya hemos tratado este problema. El componente culpable es la pila de red de Windows. Esta nueva generación de pila TCP/IP incluye una tecnología llamada "Receive Window Auto-Tuning". En resumen, la ventana de recepción TCP define la suma de datos que un equipo remoto puede recibir antes de enviar un acuse de recibo. Una técnica clásica de optimización de la conexión a Internet trata de disminuir este retraso para que los datos se envíen más rápidamente. La técnica que utiliza Windows consiste en supervisar en tiempo real el ancho de banda consumido y el tiempo de latencia, de manera que modifiquen sobre la marcha el tamaño de la ventana TCP. El único problema que puede encontrar es que muchos programas de firewall de conexión a Internet o dispositivos no soportan esta función. Si no existe una actualización en el sitio del editor o fabricante, la única opción consiste en desactivar por completo esta característica. Siga el siguiente procedimiento:

Ejecute una ventana de Símbolo del sistema como administrador.
Ejecute estos dos comandos:

- **netsh interface tcp set global autotuninglevel=disabled**
- **netsh interface tcp set global rss=disabled**

No es necesario reiniciar el equipo.

## 11. El estado de los iconos de la zona de notificación de red y altavoces no corresponde a la configuración de su equipo

Este problema aparece tras salir del estado de suspensión o de hibernación.

En este caso, puede optar por una de las siguientes acciones:

Reinicie su equipo.
Pare y vuelva a lanzar el proceso **explorer.exe** desde el **Administrador de tareas de Windows**.
Desde el **Panel de control**, haga clic en el vínculo **Ver el estado y las tareas de red**.

## 12. Desactivar el protocolo SMB v3 en Windows 8

Si tiene problemas con el protocolo SMB v3 presente en Windows 8, puede ser útil desactivarlo. Este protocolo utiliza la misma pila que el protocolo SMB v2, por lo que la desactivación de SMB v3 conlleva la desactivación de SMB v2.

Para desactivar el protocolo SMB v3 en un equipo con Windows 8:

Ejecute la consola **PowerShell** en modo administrador desde las herramientas de administración del Panel de control.
Introduzca el comando: **SetSmbServerConfiguration -EnableSMB2Protocol $false**.
Compruebe entonces que el protocolo se ha desactivado correctamente ejecutando el comando: **Get-SmbServerConfiguration | SelectEnableSMB1Protocol, EnableSMB2Protocol**.