Herramientas del sistema operativo

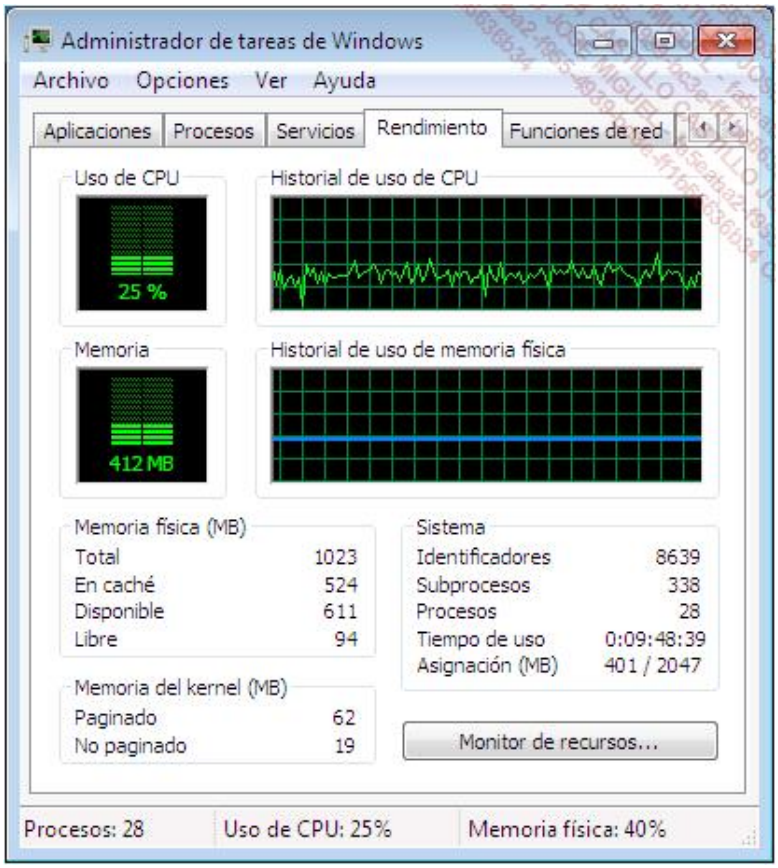
Windows dispone de diversas herramientas para reparar y monitorizar la actividad del sistema operativo. En este apartado veremos tres de las herramientas del sistema útiles para operaciones de reparación.

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*).

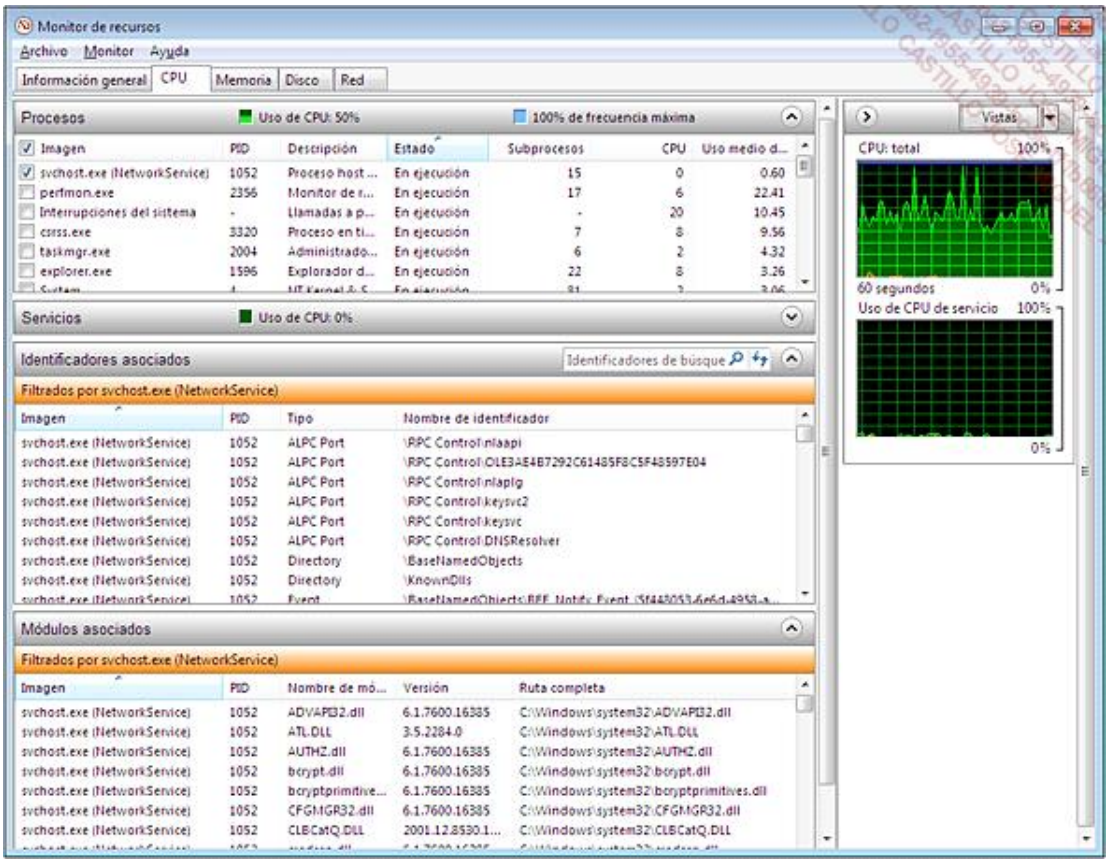
El monitor de recursos completa la información del Administrador de tareas y permite ir más allá en el análisis de los recursos consumidos en el sistema.

- Para lanzar el monitor de recursos, escriba **resmon.exe** en la zona de búsqueda del menú **Iniciar** 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.

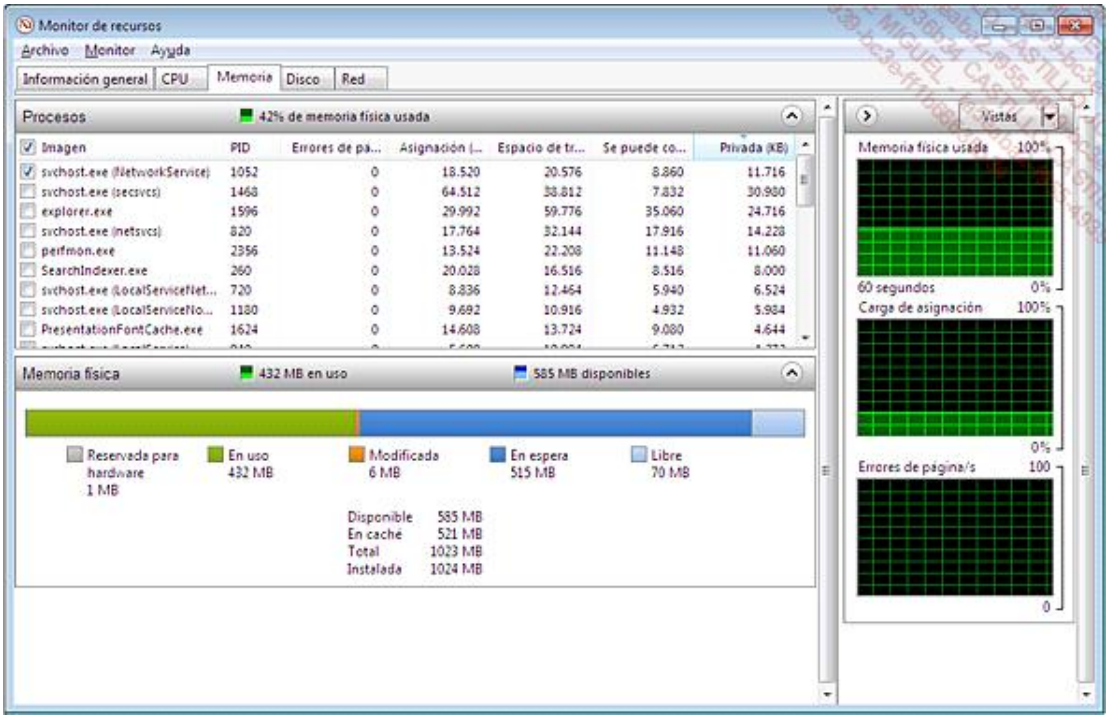


- Para profundizar en el conocimiento del monitor de recursos puede visualizar los servicios que se están ejecutando en su sistema.
- En el **Monitor de recursos**, seleccione la pestaña **CPU** y a continuación haga clic en la sección **Servicios**. Puede hacer más grande la sección con el ratón para 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 (*Dynamic Link Library*) 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.



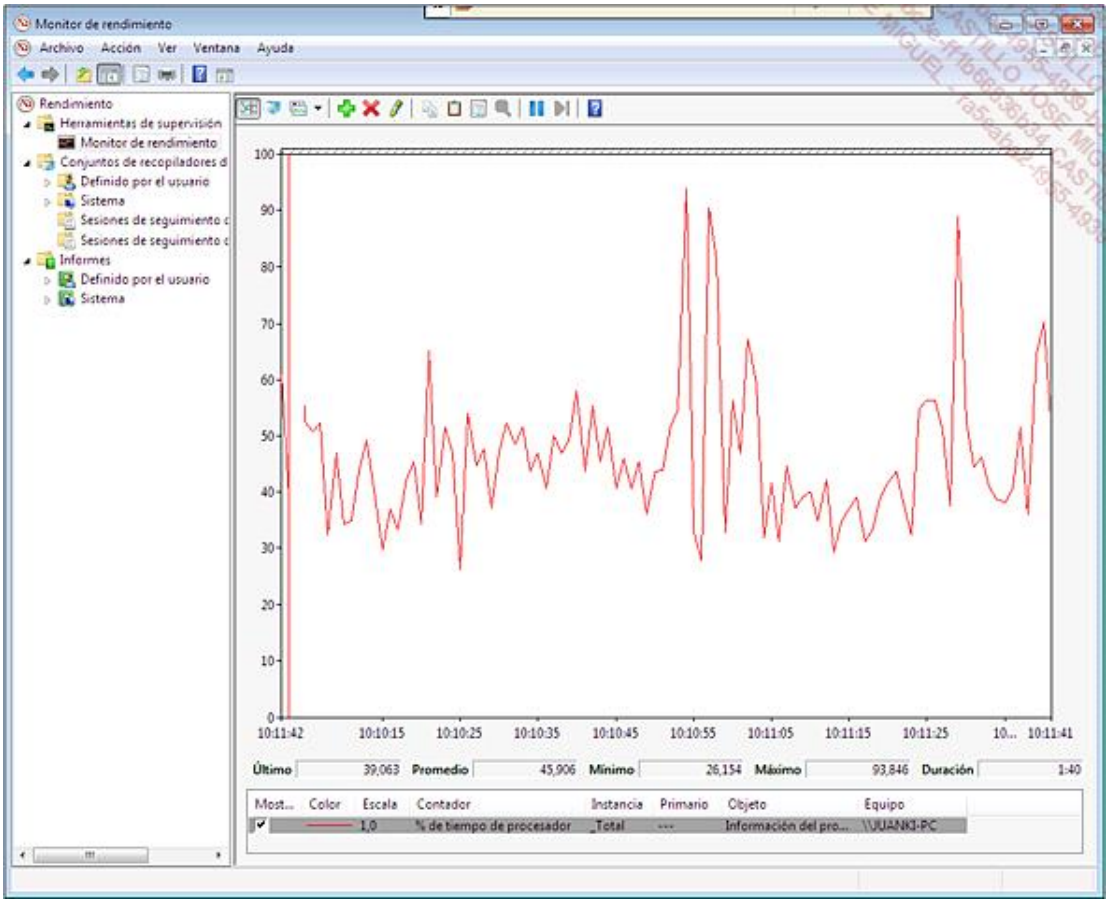
- Finalmente la pestaña **Red** permite visualizar los puertos de red en escucha en su sistema. Esto equivale al comando **netstat -a** ejecutable en el símbolo del sistema.

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 del menú **Iniciar** 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 8 y Windows 7 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

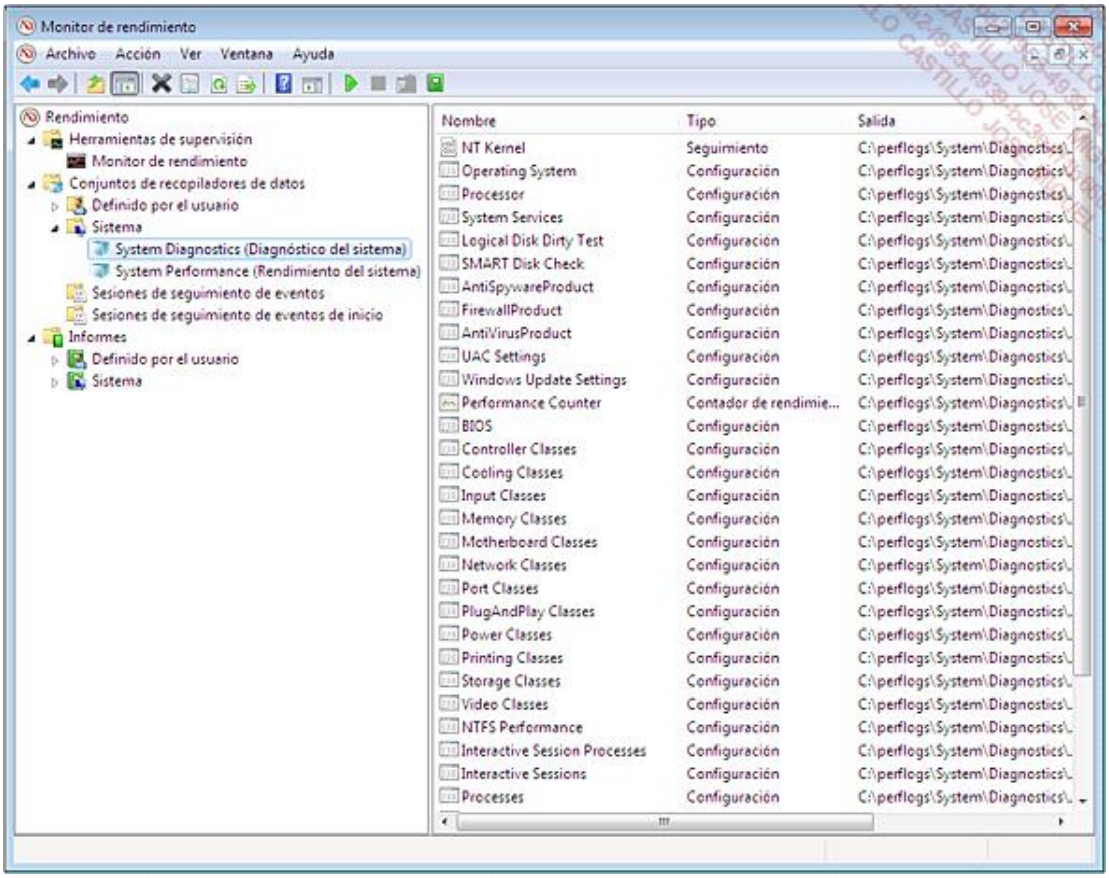
seleccionados, asegúrese del color y la escala definida para cada contador. Utilice preferentemente un color diferente. Se puede acceder a estos elementos desde las propiedades de los contadores de rendimiento.

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\%Nombre del informe%**.

Puede crear sus propios recopiladores de datos a partir de la plantilla de recopiladores de datos del sistema.

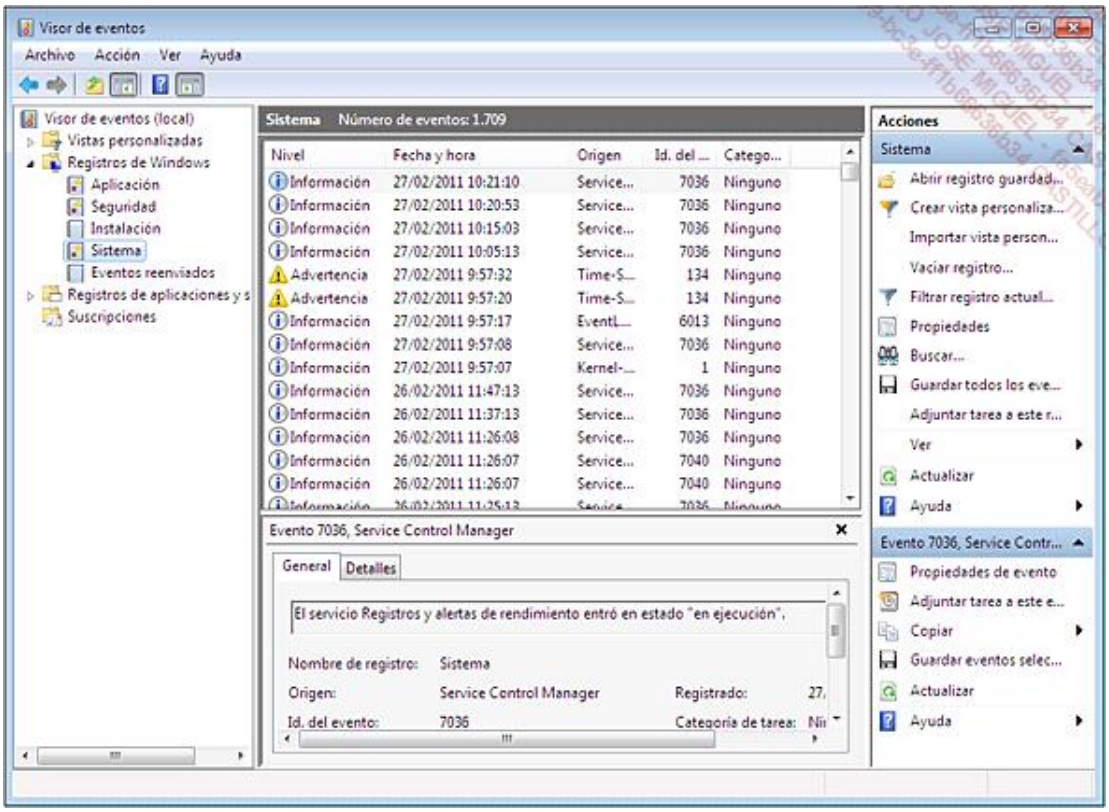
3. Visor de eventos

El visor de eventos es una de las herramientas más utilizadas por los administradores de sistemas para analizar la actividad cotidiana de un equipo Windows. El visor de eventos recopila información del sistema, así como de los

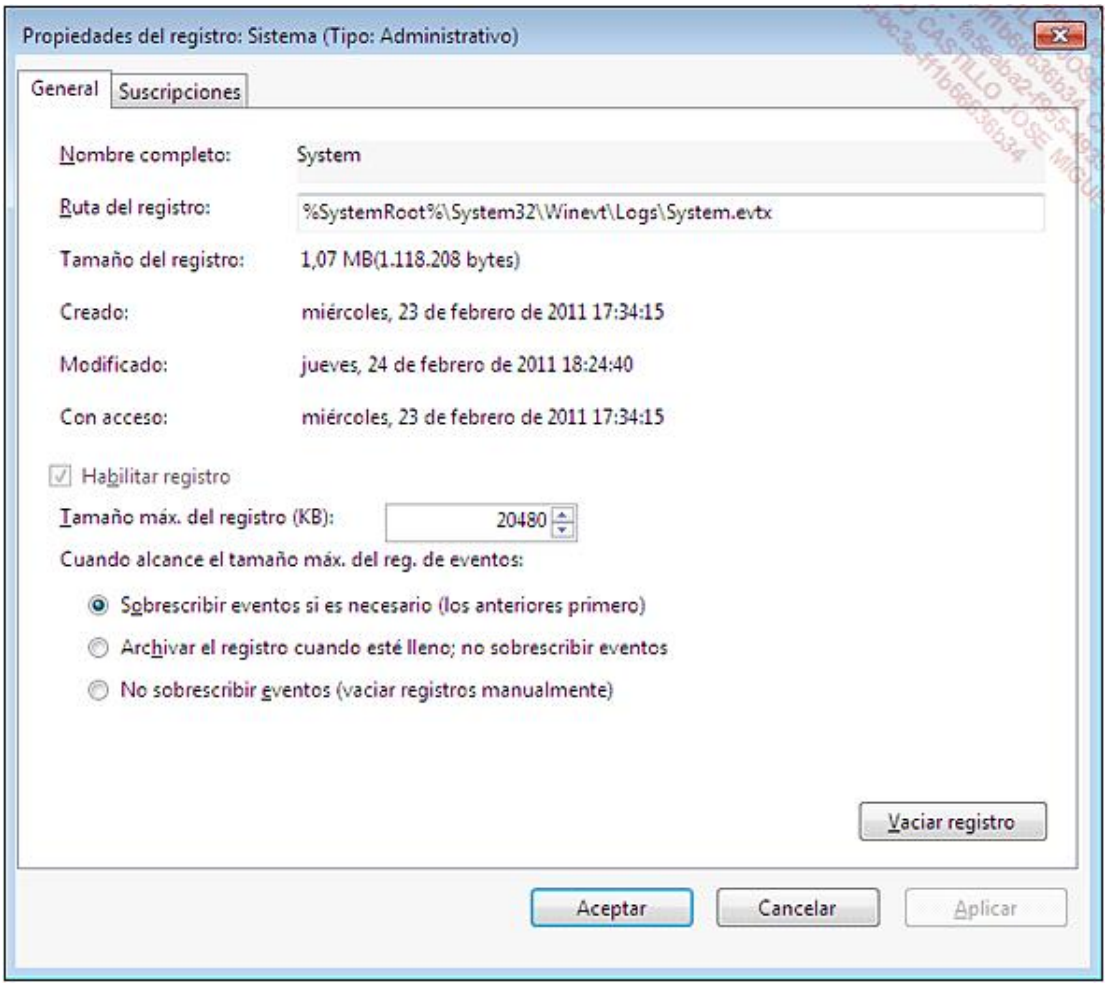
servicios y aplicaciones.

En Windows 8 o Windows 7, la utilización del visor de eventos no se limita a la recopilación de eventos. Puede, por ejemplo, utilizar los registros de eventos Windows para activar una tarea planificada en un evento de tipo error.

- Para lanzar el visor de eventos, teclee **eventvwr.exe** en la zona de búsqueda del menú **Iniciar**, o en la pantalla de inicio en Windows 8, y pulse la tecla [Intro]. Igualmente, puede visualizar el visor de eventos desde el **Panel de control**, sección **Sistema y Seguridad - Herramientas de administración**, opción **Visor de eventos**.
- Para visualizar los eventos generados por los componentes del sistema Windows, en el nodo **Registros de Windows**, seleccione el registro **Sistema**.



Puede acceder al tamaño del registro en las propiedades del registro Sistema. La pestaña **Suscripciones** permite recopilar eventos de otros ordenadores de la red.



Puede archivar los registros en forma de archivos *.evtx gracias a la opción **Grabar todos los eventos como...** disponible en el menú contextual del registro.

En los registros Windows, se visualizan los registros vinculados al sistema, a las aplicaciones y a la seguridad. En los registros de las aplicaciones y servicios, se visualizan los registros vinculados a los diferentes servicios Windows, como por ejemplo el servicio **Windows Defender**.