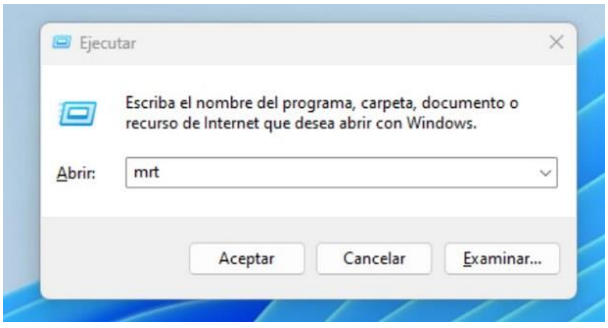
Utilidades Ocultas en Windows

MSRT, la herramienta oculta de Windows para detectar y eliminar malware

Lo más probable es que no hayas oído hablar de ella, pero esta herramienta de 'segunda opinión' acompaña a todas las versiones de Windows desde los tiempos de XP



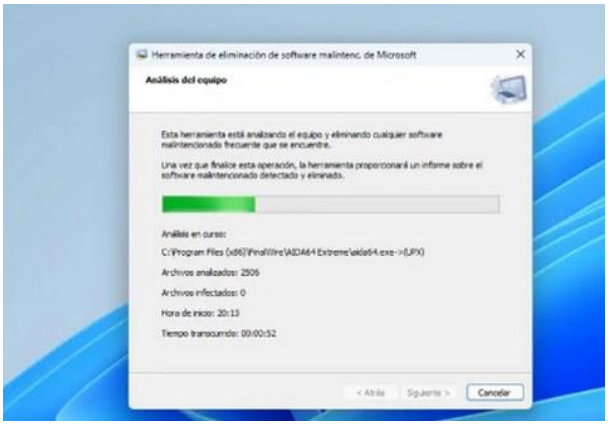
Microsoft Defender es el programa de seguridad antivirus que acompaña a **Windows** desde los tiempos de XP. Antes conocido como **Windows Defender** y más anteriormente como **Microsoft Security Essentials**, es una solución que hace tiempo dejó atrás la terrible reputación de sus primeras encarnaciones y que es suficiente para proteger a la mayoría de los usuarios, pero **no es la única opción contra malware que tiene el sistema operativo**.

Hay otras herramientas, que también acompañan al sistema operativo de Microsoft desde Windows XP y cuya misión es **acabar con los virus y malware que hayan podido infectar un**

equipo. Se trata de **MSRT**, acrónimo de Microsoft Malicious Software Removal Tool o **Herramienta de eliminación de software malicioso de Microsoft**.

Fue lanzada en **2005** y desde entonces ha estado integrada con las diferentes versiones de Windows que Microsoft ha ido lanzando a lo largo de los años. Es posible descargarla de forma independiente, pero está incluida en las actualizaciones de **Windows Update**. Si mantienes tu sistema operativo actualizado, **MSRT también lo está con las nuevas definiciones de virus y malware que Microsoft incorpora cada mes a la herramienta**.

MSRT es útil para determinados casos de uso, pero **no es un sustituto del antivirus**, sea Microsoft Defender o uno de otro proveedor. Primero, porque no monitorea el sistema de forma constante, como sí hacen los antivirus, por lo que **no previene infecciones**. **Las elimina una vez identificadas**, cuando el usuario realiza un escaneo manual del sistema. Y para eliminarlas, **deben estar activas**. Un malware que no esté en ejecución no será detectado, algo que sí hace un antivirus.



Tiene otras limitaciones. Es capaz de **eliminar el software malintencionado más extendido, pero no todo**. En realidad, ningún antivirus es capaz de detectar todo lo que hay, pero en Microsoft resaltan este aspecto para diferenciarlo. **Y aunque puede eliminar virus, gusanos y troyanos, no quita spyware**.

Dado que Windows la actualiza todos los meses, es un buen recurso para eliminar amenazas una vez han entrado en el sistema y puede usarse sin necesidad de tener que desactivar otras soluciones antivirus instaladas. MSRT es un complemento a Microsoft Defender u otro antivirus con el que se refuerza la seguridad del equipo. **Un software de 'segunda opinión', por decirlo así. Además, su uso es extraordinariamente sencillo**.

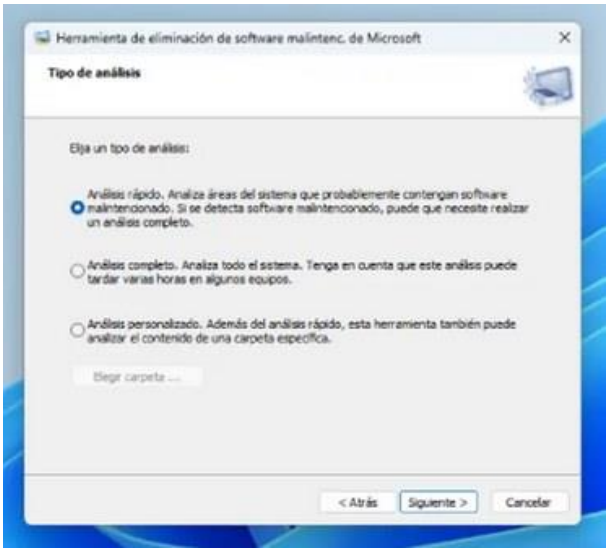
Cómo eliminar malware en Windows con la Herramienta de eliminación de software malicioso de Microsoft

Para utilizar MSRT, debes seguir estos pasos:

- MSRT no se encuentra en la lista de programas de Windows. Para acceder a la herramienta, debes pulsar las teclas **Windows + R** para abrir la **consola de comandos**.

Esta aparecerá sobre el botón de inicio de Windows, en una ventana con el nombre de **Ejecutar**.

- En el campo de texto de **Ejecutar**, escribe **mrt** —no es una errata, el comando es sin la s— y haz clic en **Aceptar**. Cuando Windows te pregunte si quieres dejar que el programa haga cambios en el equipo, **responde afirmativamente**.
- Esto abrirá una nueva ventana, ya de MSRT. Haz clic en **Siguiente**.
- Selecciona el tipo de análisis que quieres realizar. Puedes elegir entre **Análisis rápido** —examina las partes del sistema que más probablemente contengan malware—, **Análisis completo** —que puede llegar a durar varias horas— o **Análisis personalizado** -si solo quieres revisar una determinada carpeta o unidad de disco duro-. Si encuentra malware, te dará la opción de **eliminarlo**.

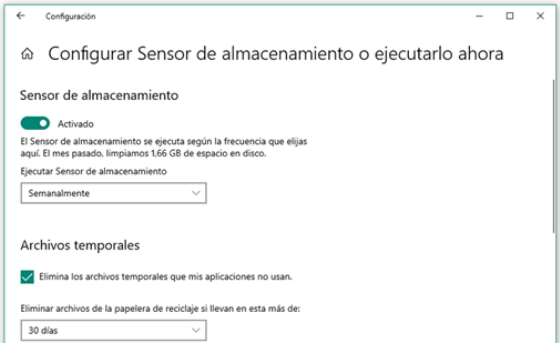


Si quieres tener la herramienta más a mano y simplemente lanzarla desde un acceso directo, puedes **anclarla en la barra de tareas cuando esté activa**.

SENSOR DE ALMACENAMIENTO

El sensor de almacenamiento fue lanzado en la versión 1809 de Windows 10 y desde entonces se ha vuelto una herramienta imprescindible para mantener tu ordenador limpio de archivos basura. El sensor se ejecuta cada cierto tiempo con el objetivo de buscar y eliminar archivos temporales del equipo que ocupan espacio innecesariamente.

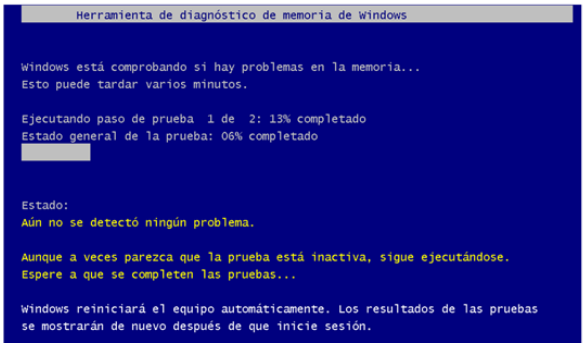
Para activarlo **ve a Configuración, Sistema, Almacenamiento y activa el sensor de almacenamiento**. Para configurar la ejecución del mismo haz clic en Configurar Sensor de almacenamiento.



En esta pestaña se puede configurar la frecuencia de ejecución del sensor y la frecuencia para eliminar archivos temporales como los almacenados en la papelera de reciclaje. Si usas OneDrive también se puede configurar para indicar cada cuanto tiempo debe de dejar el contenido en la nube y no guardado en el ordenador.

DIAGNÓSTICO DE LA RAM

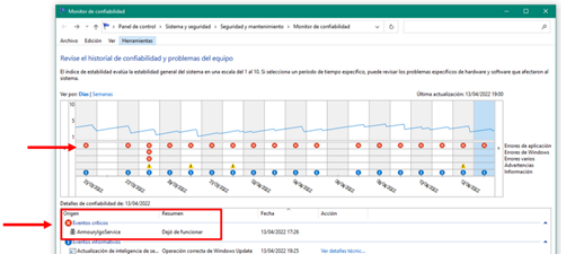
Esta herramienta permite comprobar si tienes dañada alguna celda de tu memoria RAM. Un síntoma común que puede indicar que tu memoria RAM está fallando es la aparición de pantallazos azules o BSOD (Blue Screen of Death).



Para ejecutar la herramienta pulsa en **Win+R** y escribe ***mdsched.exe***. A continuación, se reiniciará el equipo y comenzará la prueba.

MONITOR DE CONFIABILIDAD

Esta herramienta permite generar un informe en el que nos indica la estabilidad general del sistema. Desde este informe se puede comprobar qué aplicaciones están fallando y cuál es el grado de estabilidad de nuestro sistema.



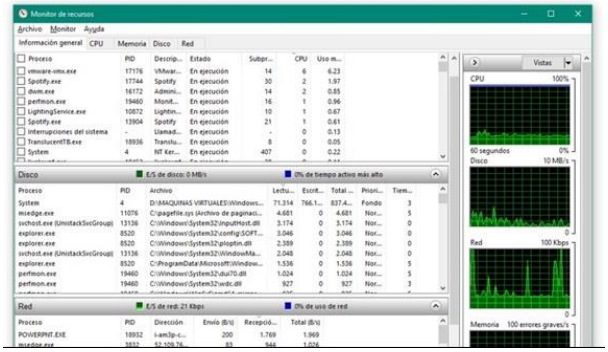
En la anterior imagen te señalo los días en los que aparece un evento crítico y el proceso que ha provocado la excepción.

Para ejecutar la herramienta pulsa **Win+R** y escribe ***perfmon /rel***.

MONITOR DE RECURSOS

El monitor de recursos nos permite ver, con un gran nivel de detalle, dónde está gastando Windows los recursos hardware de nuestro equipo. La herramienta nos ofrece cuatro pestañas: CPU, memoria, disco y red. En cada una de ellas nos desglosa qué procesos están haciendo un uso del recurso y en qué medida.

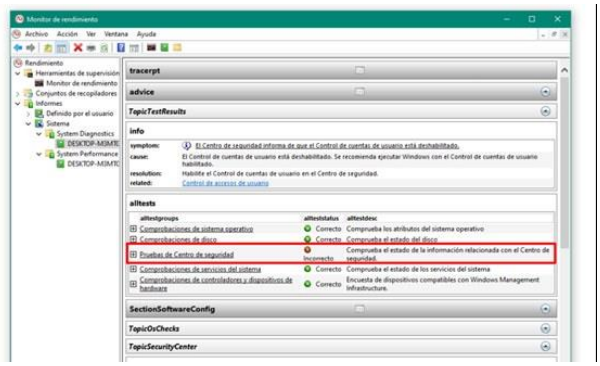
Un ejemplo de las operaciones que podemos ver es qué archivos del sistema están siendo utilizados por procesos.



Para ejecutar la herramienta pulsa **Win+R** y escribe ***perfmon /res***.

MONITOR DE RENDIMIENTO

Es otra herramienta que permite comprobar el estado del rendimiento de nuestro PC. Tiene dos funciones principales: el medidor de valores, que permite escoger una métrica de rendimiento y valorarla, y el generador de informes, que nos informarán de posibles problemas en el equipo como muestra la siguiente imagen:

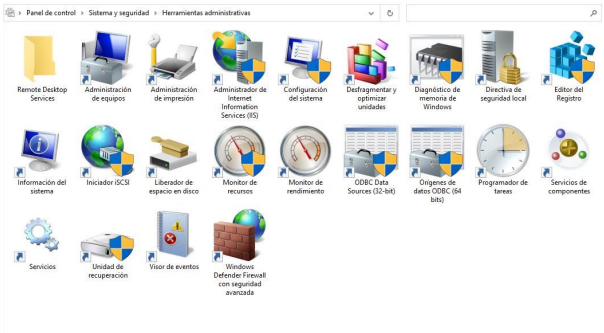


Para ejecutar la herramienta pulsa **Win+R** y escribe ***perfmon***.

Herramientas Administrativas

El panel de control de Windows esconde una subsección donde podrás encontrar la mayoría de herramientas avanzadas que incorpora Windows. De todas las que aparecen que no he mencionado destaco:

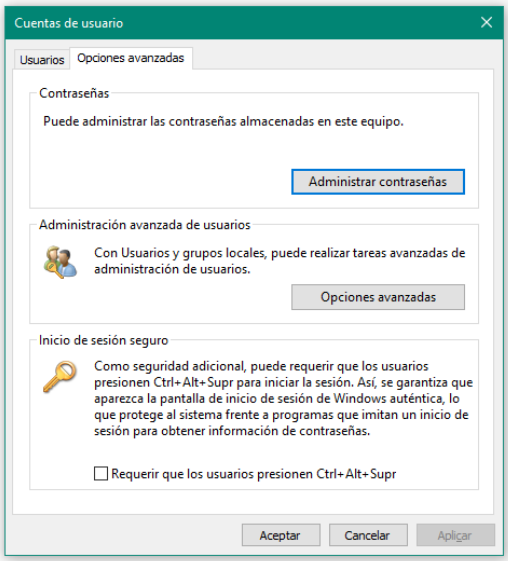
- **Administrador de equipos:** Aglutina las herramientas más usadas para administrar un equipo.
- **Programador de tareas:** Permite programar la ejecución de programas o scripts, pudiendo crear rutinas automáticas.
- **Liberador de espacio en disco:** Permite eliminar archivos temporales del sistema.
- **Firewall de Windows**: Permite establecer reglas para permitir o denegar el acceso a internet de programas o puertos.



Para ver las herramientas administrativas **ve al panel de control, sistema y seguridad y pulsa sobre herramientas administrativas.**

HERRAMIENTA DE CUENTAS DE USUARIO

Esta herramienta, también veterana, permite administrar todo lo referente a configuraciones con cuentas de usuarios: añadir cuentas de usuarios, asignarles privilegios, o cambiarles de grupos.



Para ejecutar la herramienta pulsa **Win+R** y escribe ***n*etplwiz**.

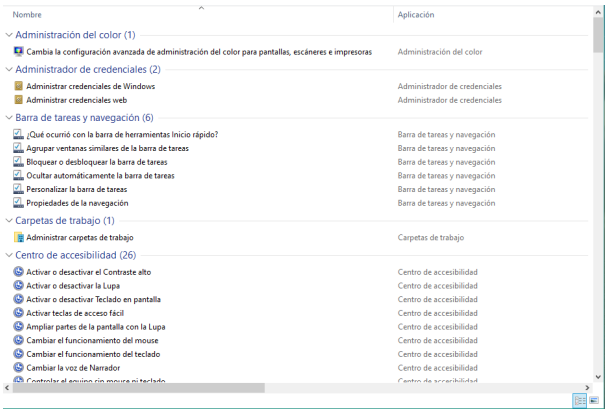
Modo Dios de Windows

El modo Dios nace con Windows 7 y consiste en un panel de control que despliega una gran cantidad de herramientas y opciones para configurar el sistema.

Para activarlo **crea una carpeta** y ponle el siguiente nombre:

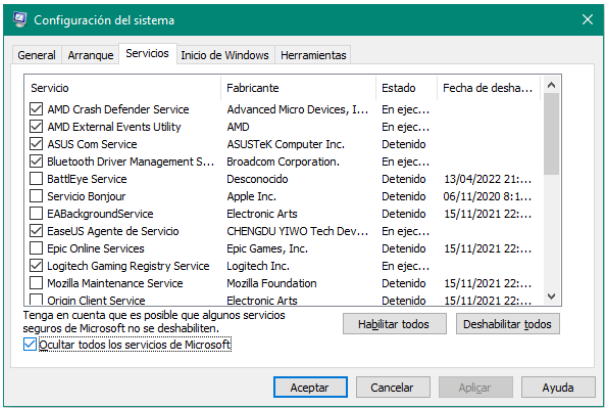
GodMode.{ED7BA470-8E54-465E-825C-99712043E01C}

A continuación, verás que el icono de la carpeta cambia y se convierte en el mismo que el panel de control. Abre el nuevo panel de control y ya solo te queda investigar con él.



Configuración del sistema

Otra herramienta clásica de Windows pero que no muchos conocen es la configuración del sistema. Con herramienta podrás modificar el comportamiento del arranque del sistema, detener servicios que arrancan con Windows o iniciar otras herramientas del sistema.



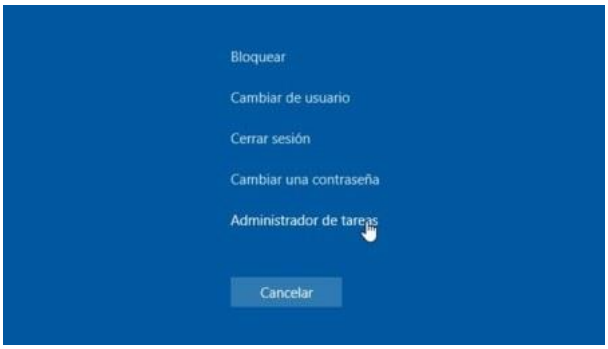
Para ejecutarla pulsa en **Win+R** y escribe **msconfig**.

Funciones ocultas del Administrador de tareas de Windows

El Administrador de tareas es una de esas herramientas de Windows que **usas casi cada día**, generalmente para *parar* algún proceso o programa que se ha quedado colgado, pero en la que **apenas te fijas** una vez ha cumplido con su tarea. Quizás por eso muchas de sus funciones pasan desapercibidas.

Sin embargo, esta pequeña utilidad **sirve para mucho más** que para cerrar aplicaciones colgadas, sobre todo en las versiones más recientes del sistema operativo (Windows 8 y Windows 10), en las que recibió una actualización tanto en diseño como en funciones.

Cómo acceder al Administrador de tareas

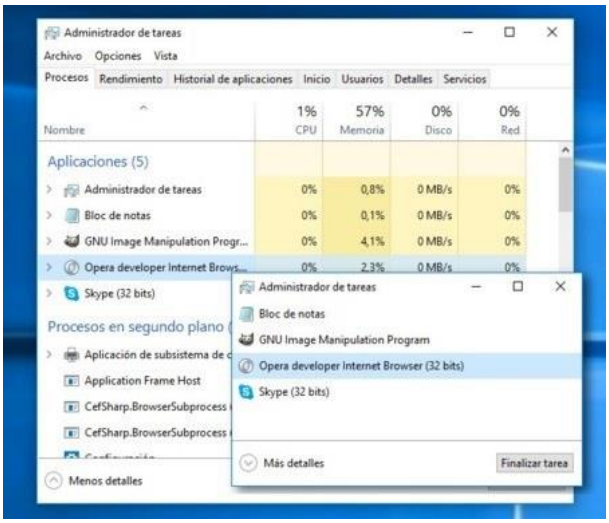


Antes de empezar a descubrir algunas de las funciones que se ocultan en esta herramienta de Windows, lo primero es llegar a ella, ¿verdad? Y para ello, la inmensa mayoría conocemos y usamos el atajo de teclado **Ctrl + Alt + Supr**.

Pero lo cierto es que este atajo sólo nos da acceso a un menú de opciones, dentro del cual tenemos la posibilidad de ejecutar el Administrador de tareas. Si lo que quieres es abrir esta herramienta directamente, el atajo correcto para hacerlo es **Ctrl + Mayús + Esc**.

Por supuesto, no es la única forma de acceder al Administrador de tareas. Otras maneras de conseguirlo es buscándolo directamente en el **buscador integrado** en la barra de herramientas, o usando el acceso directo incluido en el **Power User Menu** (que puedes abrir con el atajo Win + R o haciendo clic derecho en el botón de Inicio).

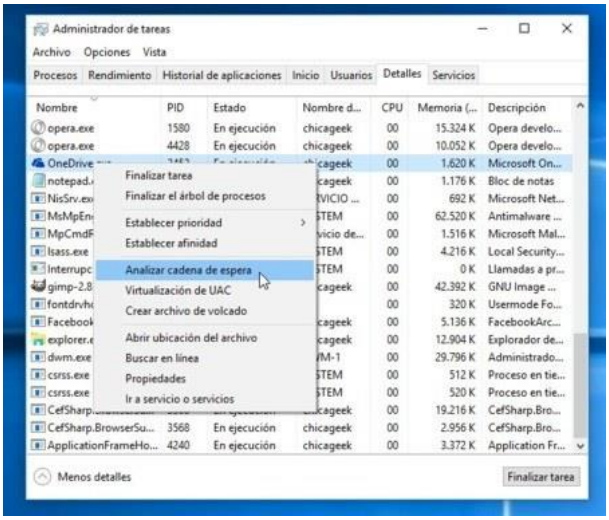
Alterna entre los dos tipos de interfaz



Una de las novedades tras la modernización del Administrador de tareas en Windows fue la creación de **dos interfaces**: una más simplificada y otra con más información. Para alternar entre una y otra, sólo tienes que hacer clic en "Más detalles" o "Menos detalles" en la esquina inferior izquierda.

Dependiendo de lo que quieras hacer con la herramienta, puedes optar por una u otra. La versión simplificada, obviamente, está dedicada a la función "estrella" de esta utilidad: cerrar procesos.

Descubre por qué se ha colgado una aplicación

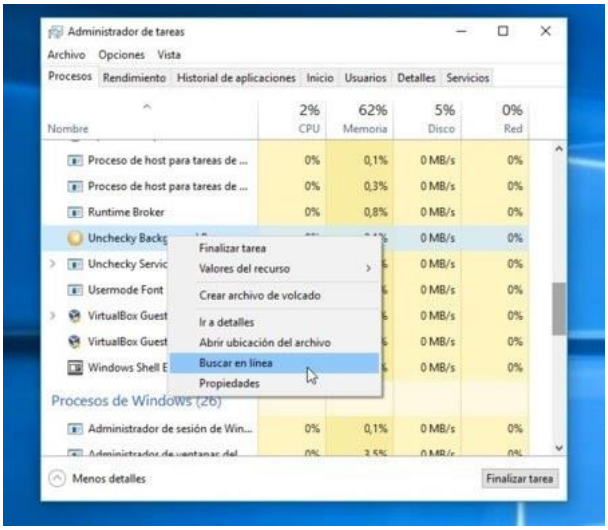


El primer instinto cuando una aplicación deja de responder es abrir el Administrador de tareas (con cualquiera de los métodos explicados en el punto 1) y **finalizar el proceso** inmediatamente. Pero si no hemos guardado antes, esto puede comportar la pérdida de datos: el artículo a medio escribir, la foto a medio editar...

A veces es más recomendable esperar a ver si la aplicación se puede recuperar por sí sola, y esta situación, hay una función del Administrador de tareas que te puede ayudar. Ve a la pestaña **Detalles**, busca el proceso en cuestión, haz clic derecho sobre él y elige la opción **Analizar cadena de espera**.

Esta función te puede dar más pistas sobre las **dependencias entre procesos**, y si, por ejemplo, la culpa de que esa aplicación esté colgada es en realidad "culpa" de otro proceso que no responde.

Busca información sobre procesos sospechosos

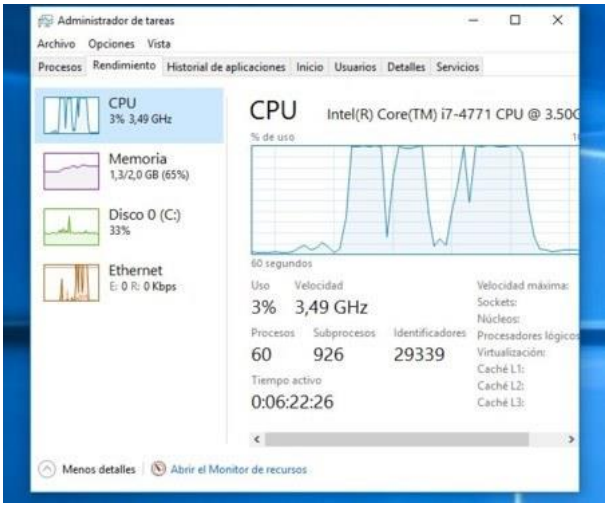


Hablando de procesos, ¿conoces todos los que están en ejecución en tu sistema? Algunos están claros, desde luego, pero otros no tanto... y Administrador de tareas también te puede echar una mano con esto.

Si en la lista de procesos de la ventana del Administrador de tareas ves **algo sospechoso**, que no te suena de nada o simplemente quieres saber a qué programa pertenece o por qué se está ejecutando, haz clic derecho sobre ese proceso y en el menú contextual elige la opción **Buscar en línea**.

Windows lanzará una búsqueda en Internet para que puedas **averiguar más cosas** sobre el mismo, y decidir si deberías seguir manteniéndolo activo o no.

Controla los recursos del sistema



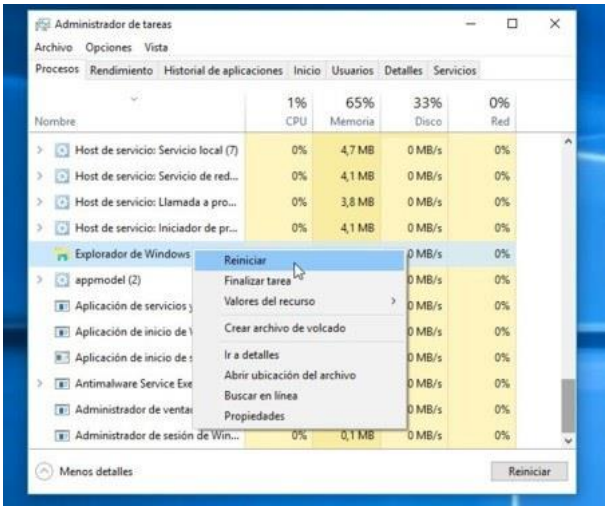
Además de ver los procesos que están actualmente activos, ¿sabías que el Administrador de tareas también incluye herramientas con las que vigilar el rendimiento del sistema? Las puedes encontrar en la pestaña **Rendimiento**, en forma de **gráficas** que hacen seguimiento del procesador, memoria, disco y conexión a Internet en tiempo real.

Dentro de esta sección tienes además varias opciones. En la parte inferior de la ventana, por ejemplo, hay un enlace para abrir el **Monitor de recursos**, una utilidad avanzada de control de recursos.

Además, con un clic derecho en las pequeñas gráficas de la barra lateral izquierda puedes elegir entre **mostrarlas u ocultarlas**. Otra opción útil de este menú contextual es **copiar la información al Portapapeles** (para luego, por ejemplo, pegarla en un foro técnico donde quieras pedir ayuda).

Por último, si seleccionas la gráfica de red para verla en grande, y luego haces clic derecho sobre ella, verás la opción de **Ver detalles de la red**, que te muestra una ventana adicional con todo tipo de datos sobre tu conexión a Internet.

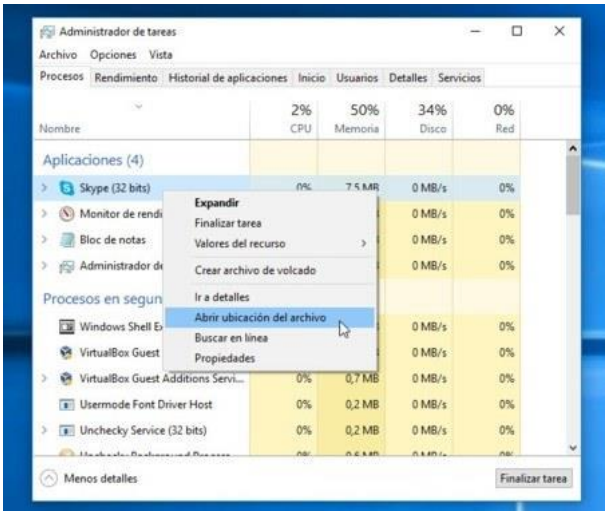
Reinicia el Explorador de ficheros de Windows



Si todos los programas del ordenador te van bien, pero es justo el propio Explorador de Windows (la barra de tareas, el explorador de ficheros, el menú de inicio...) lo que está fallando, **no es necesario reiniciar** para arreglarlo. Una visita rápida al Administrador de tareas puede solucionarlo sin problemas.

De hecho, era algo tan común en el Administrador de tareas que han acabado por integrarlo como una nueva función: sólo tienes que buscar el **Explorador de Windows** en la lista de procesos, hacer clic derecho y verás la opción **Reiniciar**. Con eso se debería arreglar.

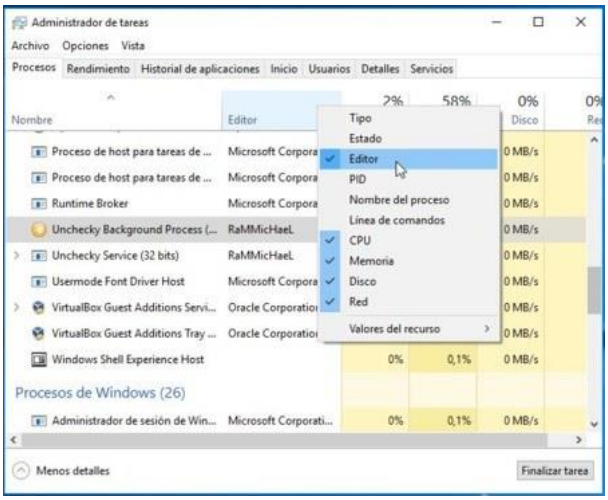
Localiza la ubicación de un fichero



¿Necesitas encontrar la **ubicación exacta** de un programa que tienes en ejecución en ese momento? Tienes dos opciones: la primera es navegar por toda la estructura de carpetas de Windows hasta encontrarlo (lo que puede llevarte unos cuantos clics...) y la segunda es simplemente usar el Administrador de tareas.

Todos lo que tienes que hacer es localizar el proceso en cuestión, hacer clic derecho sobre él y elegir la opción **Abrir ubicación del archivo**. Windows abrirá una ventana del Explorador con el fichero seleccionado en su carpeta correspondiente.

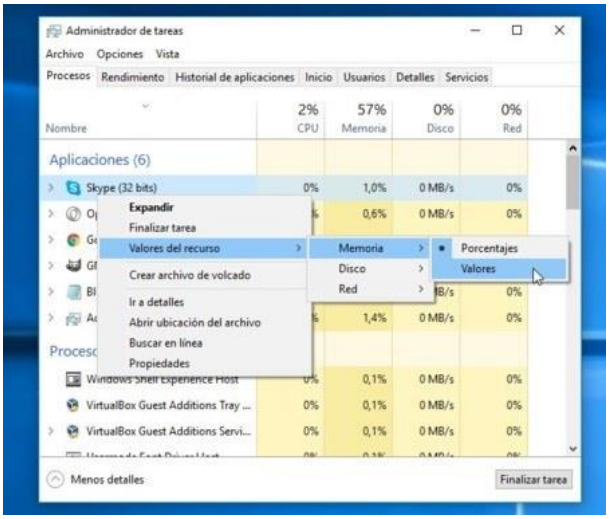
Añade tantos detalles como necesites



En el punto 2 hablaba de la existencia de dos tipos de interfaz en el Administrador de tareas, pero aquí no acaban sus **posibilidades de personalización**. La ventana de esta herramienta muestra cuatro **columnas** por defecto (CPU, Memoria, Disco y Red), pero puedes mostrar hasta seis más si quieres.

Para ello, haz clic derecho sobre la cabecera de cualquiera de las columnas actuales, y **selecciona la nueva columna** que quieres mostrar. También puedes, por supuesto, ocultar cualquiera de las columnas que vienen por defecto.

Cambia números por porcentajes



Otra pequeña opción de personalización, pero que puede ser muy útil, es la posibilidad de alternar entre las posibilidades de **mostrar valores absolutos o mostrar porcentajes** en las columnas de Memoria, Disco y Red.

Puedes hacerlo haciendo clic derecho en cualquier proceso, eligiendo la opción **Valores** del recurso en el menú contextual, y luego seleccionando el elemento en cuestión (Memoria, Disco o Red) y el tipo de medida que prefieres ver. Porque está bien saber que Skype está

usando 40 MB de RAM, pero quizás es más informativo saber que eso es un **5%** del total de RAM de tu sistema.

Herramientas de SysInternals para administración de sistemas Windows

Process Monitor

Similar al administrador de tareas de Windows, pero mucho más potente. Te enseña toda la información disponible para cada uno de los procesos que se encuentran en ejecución en el sistema.

Cosas tan relevantes como los ficheros que lee o escribe, conexiones de red o las claves del registro de Windows a las que accede. Con esta herramienta, podrás ver, exactamente, qué es lo que hace cada uno de los programas que se ejecutan en el sistema.

ADExplorer

Esta herramienta es capaz de enseñarte información abundante sobre un dominio concreto. Para que funcione correctamente y, te aporte mayor información, debes ejecutarla en una estación de trabajo conectada a un dominio de Active Directory. No se requieren permisos de administrador para ejecutarla y, además, te enseña toda la estructura de la base de datos del dominio, incluyendo objetos del tipo Computer, User, OUs, GPOs, etc.

RootkitRevealer

Sirve para detectar Rootkits en el sistema y, para ello, se basa en un análisis de algunas de las claves más criticas del registro de Windows, las invocaciones a funciones sensibles de la API de Windows y comportamientos típicos en software malicioso.

AccessEnum

Muy útil para enumerar los accesos a diferentes recursos por parte de los usuarios del sistema.

Lista todas las operaciones de lectura y escritura que se realizan por parte del usuario y enseña, en formato de lista, aquellos accesos que han sido garantizados y denegados.

AccessChk

Te permite especificar un usuario o grupo y, en base a eso, te enseña los accesos a ficheros, claves del registro o servicios del sistema operativo a los que ha tenido acceso.

TCPView

Te permite monitorizar las conexiones que se están realizando en el sistema, de esta forma, puedes tener una imagen de qué está pasando en el entorno de red de dicha máquina. Entre

otras cosas, te enseña conexiones las TCP/UDP y su estado, es similar netstat, pero con una interfaz gráfica.

Autorun

Consulta las claves del registro que permiten la ejecución de programas al inicio del sistema y el software instalado, para después con esta información, enseñarte los programas que se ejecutan automáticamente en tu sistema Windows. Algo que te vendrá bien, por ejemplo, para detectar puertas traseras.

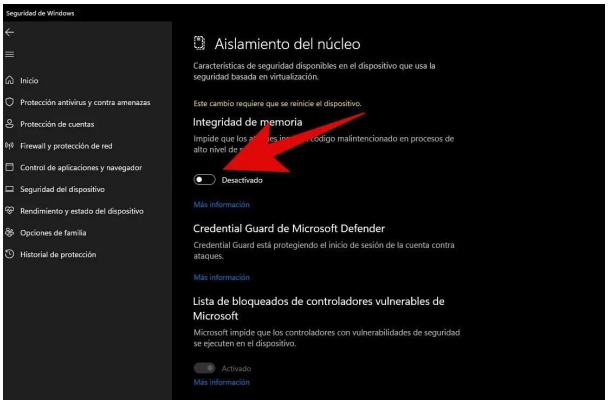
Descargar herramientas de Sysinternals

Tres ajustes recomendados por Microsoft para mejorar el rendimiento de tu PC.

Realizar un correcto mantenimiento de nuestro equipo es importante si queremos alargar su vida útil

Para mejorar el rendimiento en sistemas con Windows 10 y 11, Microsoft ofrece una serie de soluciones a las que todo el mundo puede acceder. De esta manera, si cuentas con un equipo pobre en especificaciones, siempre puedes echar mano de algunos trucos para mejorar el rendimiento general en el sistema, **optimizar tu equipo para ejecutar juegos** o para edición multimedia. Bajo estas líneas te hemos dejado con **tres ajustes recomendados por Microsoft para mejorar el rendimiento de tu PC**.

Desactivar la integridad de memoria



Windows 11 cuenta con una función que mejora la seguridad del equipo. Esta función se encuentra activa por defecto, y se llama '**Aislamiento del núcleo**'. Se trata de un conjunto de herramientas destinadas a proteger el sistema por medio de técnicas basadas en sistemas de virtualización. Una de sus herramientas es la 'Integridad de memoria', la cual previene el sistema de determinados ciberataques basados en la inserción de código malicioso en procesos de alta seguridad.

Microsoft reconoce que esta opción puede disminuir el rendimiento del equipo, sobre todo a la hora de jugar a juegos, por lo que **conviene desactivarla si quieres hacer que tu PC rinda mejor**. Para ello escribe 'aislamiento del núcleo' en el cuadro de búsqueda de la barra de tareas y desactiva el interruptor de la integridad de memoria.

Desactivar la plataforma de máquina virtual (VMP)

La plataforma de máquina virtual (VMP) de Windows nos permite **acceder a máquinas virtuales** para ejecutar distintos sistemas operativos en nuestro equipo o comandos propios de éstos. Si la desactivas, no podrás acceder al **subsistema de Linux**, aunque podrás seguir recurriendo a máquinas virtuales mediante la tecnología Hyper-V.

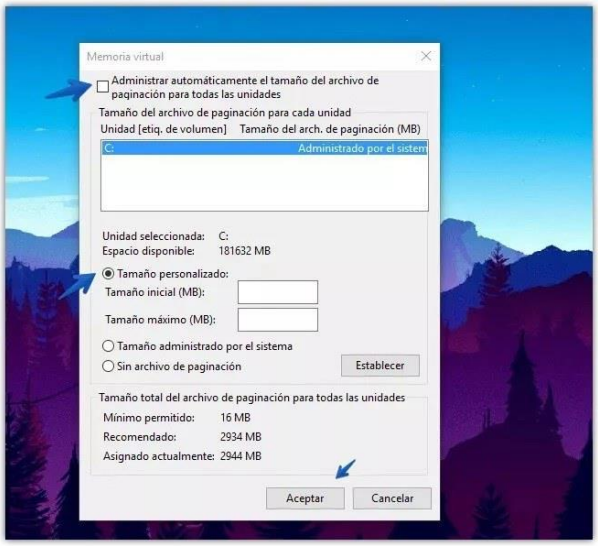
VMP es también un ajuste que **puede disminuir el rendimiento del equipo** según Microsoft, por lo que para desactivarla puedes hacerlo escribiendo en el cuadro de búsqueda de la barra de tareas lo siguiente: 'Activar o desactivar las características de Windows'. Al presionar Enter, debes desmarcar de la lista la opción de '**Plataforma de máquina virtual**'.

Ajusta el tamaño del archivo de paginación en Windows

El archivo de paginación es un área de nuestro sistema de almacenamiento interno que se usa como memoria para que se ejecuten correctamente los procesos del equipo. En Windows **podemos ajustar el tamaño de este archivo para optimizar el rendimiento del**

equipo dependiendo de la cantidad total de memoria RAM y espacio en nuestro disco de almacenamiento.

Debes asegurarte de que **la administración automática de archivos de paginación está activada**, algo que Microsoft recomienda como sugerencia para mejorar el rendimiento. Para ello escribe 'Sistema avanzado' en el cuadro de búsqueda de la barra de tareas y selecciona la opción de 'Ver configuración avanzada del sistema'. Una vez aquí, en 'Propiedades', selecciona la pestaña 'Avanzado' y después 'Configuración', dentro del área de 'Rendimiento'.



Dentro de 'Opciones de rendimiento' ve a la pestaña de 'Avanzado' y después selecciona 'Cambiar' en el área de 'Memoria Virtual'. Aquí debes asegurarte de que la casilla de 'Administrar automáticamente el tamaño del archivo de paginación para todas las unidades' está seleccionada. Si no lo está, **selecciónala y reinicia el PC**.

Modificar el tamaño del archivo de paginación te puede venir bien si tu PC no dispone de especificaciones técnicas muy avanzadas, ya que utiliza tu sistema de almacenamiento interno como memoria. En caso de que la asignación automática no te sea útil, puedes probar a modificar el tamaño del archivo de paginación mediante **una configuración más agresiva añadiendo más espacio**, siempre teniendo en cuenta nuestras especificaciones.

Restaura tu PC con Windows 10 con un solo comando

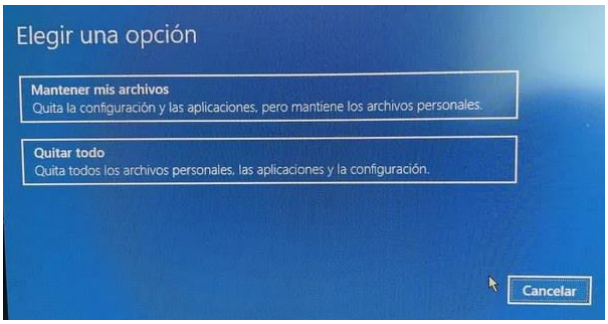
Se trata de un comando poco conocido, pero extremadamente útil que te permite **restaurar Windows 10 a su configuración inicial sin perder tus archivos personales**. Esta técnica aprovecha las herramientas internas de Microsoft para llevar a cabo una restauración segura.

Restablece el sistema a su estado original de fábrica, eliminando todos los archivos basura, aplicaciones no deseadas y configuraciones erróneas que se han acumulado con el tiempo. Al hacerlo, tu PC funcionará como nuevo.

Este comando te da la opción de conservar todos tus documentos, fotos, vídeos y demás archivos importantes. Solo se eliminarán las aplicaciones y configuraciones del sistema, dejando tus datos intactos, por lo que es una muy buena opción.

Es crucial mencionar que antes de ejecutar este comando, es recomendable que hagas una copia de seguridad de tus archivos más importantes, por si acaso. Aunque la opción Mantener mis archivos debería conservar tus datos, siempre es mejor prevenir.

- Para ello, haz clic derecho en el botón de inicio y selecciona Símbolo del sistema como administrador.
- En la nueva ventana, escribe ***systemreset --factoryreset*** y pulsa ***Enter***. Este comando iniciará el proceso de restauración del sistema.



- Aparecerá una ventana con dos opciones donde debes elegir ***Mantener mis archivos***. Esta opción restablecerá Windows 10 a su estado original, pero conservará tus archivos personales.
- Una vez que hayas elegido la opción, sigue las instrucciones en pantalla para completar el proceso.

Debes tener en cuenta que este proceso puede tardar un tiempo, dependiendo de la cantidad de datos que tengas en tu ordenador. Una vez que haya finalizado, Windows 10 estará como nuevo, listo para ofrecer el mejor rendimiento.

Eso sí, tendrás que volver a instalar todas las aplicaciones que hayas descargado, pero **tus archivos personales estarán a salvo**. Así que ya lo sabes, si tu PC tiene fallos y quieres volver a disfrutar de él como el primer día, no dudes en probar este comando.