**ADMINISTRANDO EL EQUIPO**

Operaciones:

Monitorizar sucesos del sistema como la hora de inicio de sesión y los errores de programa (Visor de sucesos o Visor de eventos).

Crear y administrar los recursos compartidos (Carpetas compartidas).

Ver una lista de los usuarios conectados a un equipo local o remoto (Carpetas compartidas).

Administrar usuarios y grupos del equipo (Usuarios locales y grupos o Usuarios y grupos locales).

Configurar los contadores de rendimiento y las alarmas (Registros y alertas de rendimiento o Rendimiento).

Ver la configuración de los dispositivos y agregar controladores de dispositivo nuevos (Administrador de dispositivos).

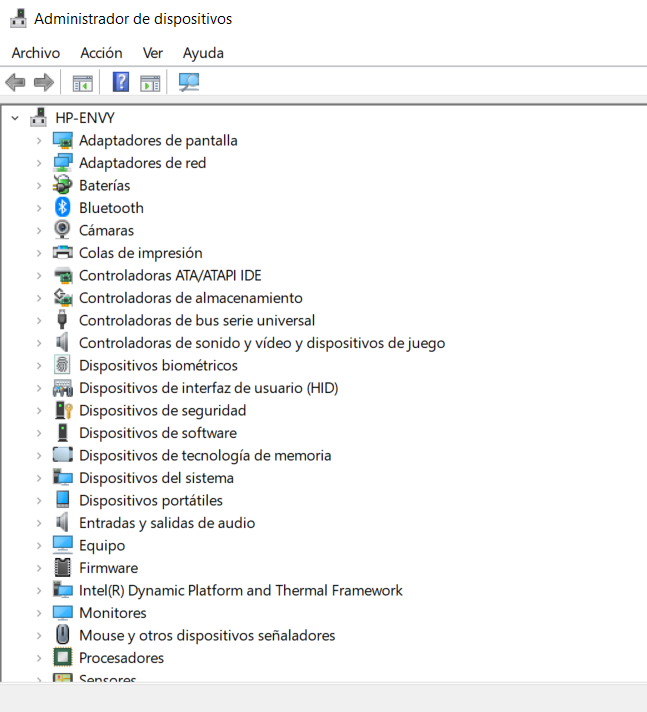
Administrar los discos del equipo (Administración de discos).

Iniciar y detener los servicios del sistema (Servicios y aplicaciones).

**EL ADMINISTRADOR DE DISPOSITIVOS**

Windows dispone de una utilidad que permite ver la configuración de los dispositivos instalados en el equipo y añadir o actualizar sus controladores.

**Equipo 🡪 Propiedades 🡪 Administrador de dispositivos**

****

**ADMINISTRADOR DE TAREAS**

Es una herramienta que sirve para controlar la actividad del sistema y su rendimiento en tiempo real. Visualiza información del estado del procesador, de la memoria, de los procesos, de la red y de los usuarios conectados. Está compuesto por:

1. **El administrador de aplicaciones.**
2. **El administrador de procesos.**
3. **El administrador de servicios.**
4. **El rendimiento del sistema.**
5. **El Administrados de las funciones de red.**
6. **El Administrador de Usuarios.**

*El Administrador de aplicaciones 🡪* Nos muestra el estado de los programas o aplicaciones que se están ejecutando en este momento en el sistema. Posee una columna que nos muestra el “estado” (activo, no responde) 🡪 Posee unos botones que nos va a permitir “finalizar”, terminar la aplicación; “cambiar a”, cambiar de la aplicación actual a la seleccionada; “Nueva tarea”, lanzar nueva aplicación.

*El administrador de procesos* 🡪 Nos va a dar información detallada de todos los procesos que están ejecutándose en ese momento en el sistema, incluidos los de sistema (servicios), los procesos locales, los procesos del usuario que ha iniciado sesión y los procesos de los usuarios remotos. 🡪 Aparecen varias columnas: Nombre de imagen, nombre del usuario, % de CPU, cantidad de memoria, descripción del proceso (por defecto). En el menú ver podemos ampliar esas columnas. (Prioridad: a mayor prioridad mayor cantidad de memoria de CPU).

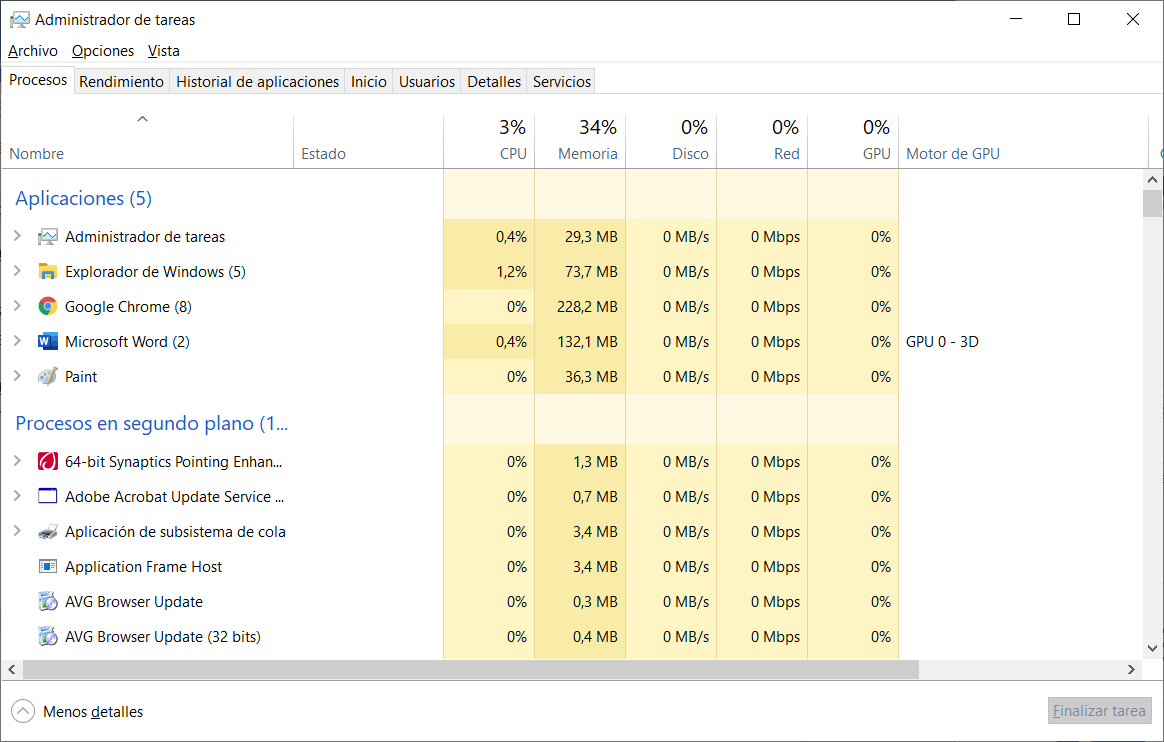
*El administrador de servicios* 🡪Los servicios van a proporcionar características del SO como registro de eventos, informe de errores, etc. De cada servicio vamos a tener la siguiente información: nombre, PID (Identificador del proceso), descripción, estado.

*El rendimiento del sistema* 🡪 Esta pestaña nos ofrece un resumen del uso de memoria y CPU mostrándonos una serie de gráficos (uso de la CPU, historial de uso, el uso de la memoria, historial del uso de la memoria en tiempo); y estadísticas (**Totales sistema** 🡪 nº de identificadores, subprocesos, procesos en ejecución, el tempo en uso desde que se arrancó el sistema y los archivos de paginación. **Memoria del núcleo** (Kernel) 🡪 Cantidad de memoria utilizada por el núcleo y cuanta esta paginada y cuanta no. **Memoria física** 🡪 Información sobre la RAM. **Carga de transacciones**).

*El Administrador de las funciones de red* 🡪 No muestra información sobre el funcionamiento y rendimiento de la red, mostrando el estado de las redes que están funcionando en el sistema, mediante una tabla descriptiva del dispositivo (Adaptador de red): velocidad, estado, bytes enviados/recibidos, etc.

*El Administrador de Usuarios* 🡪 No va a mostrar los usuarios que están conectados al equipo: su identificador, nombre, etc.

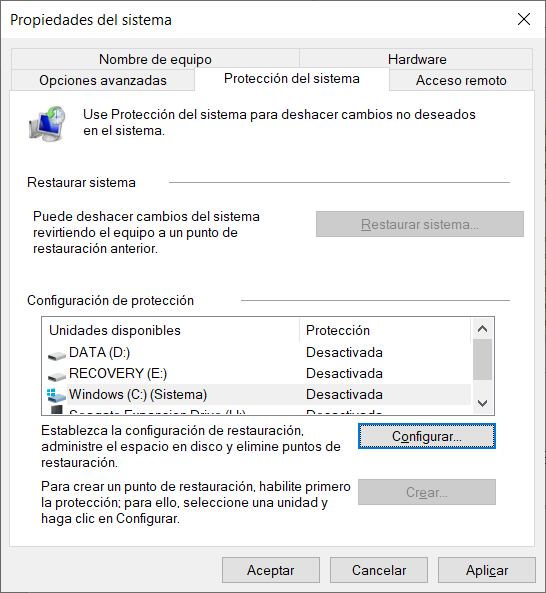
**Ctrl + Alt + Supr 🡪 Administrador de tareas**



**CONFIGURACIÓN AVANZADA DEL SISTEMA**

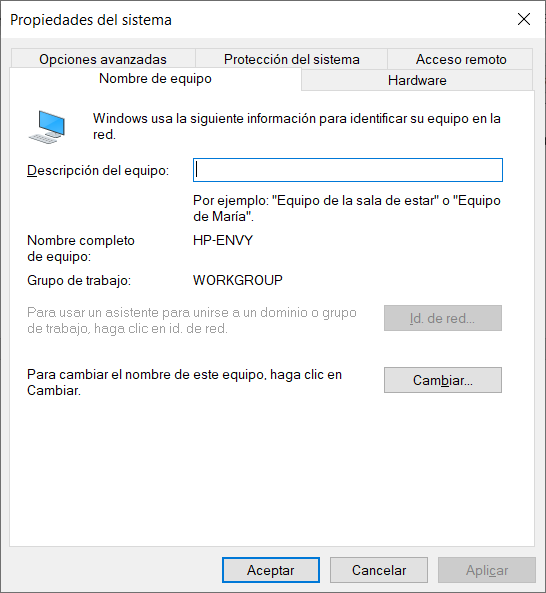
**Equipo 🡪 Propiedades 🡪 Configuración Avanzada del sistema**

PROTECCIÓN DEL SISTEMA



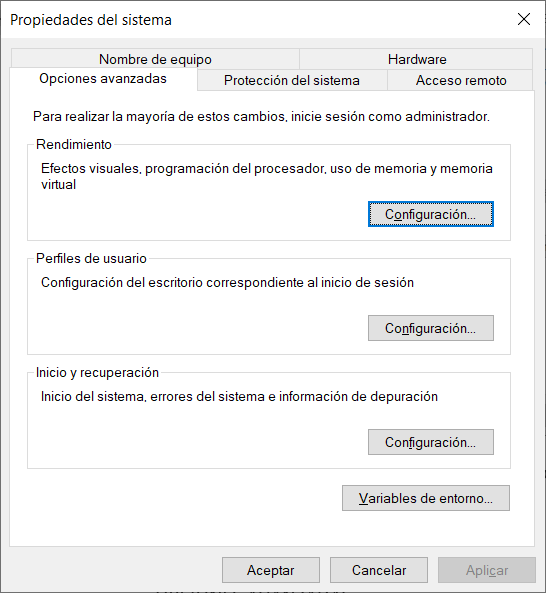
Podemos crear/restaurar puntos de restauración del sistema

NOMBRE DE EQUIPO

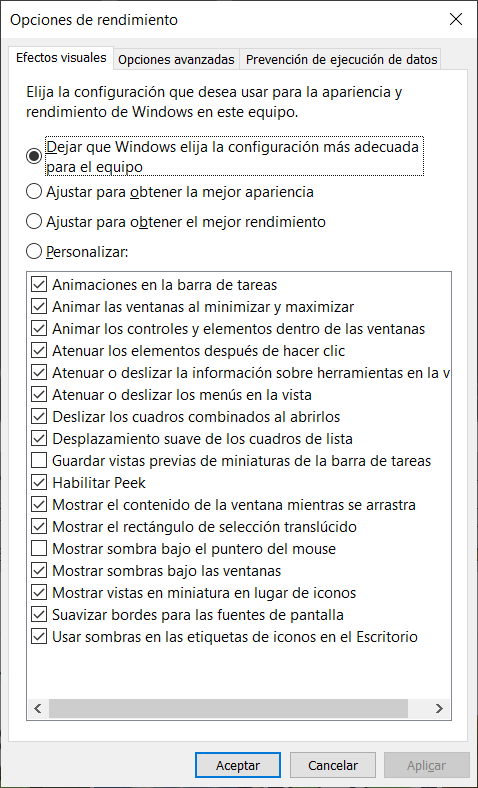
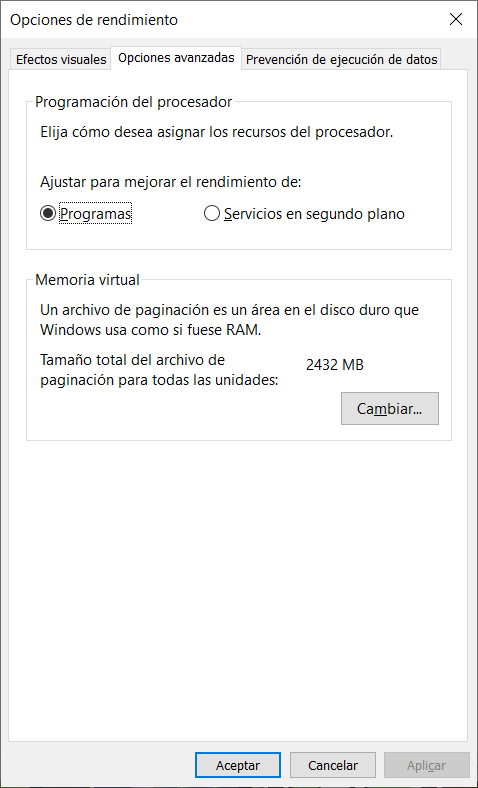
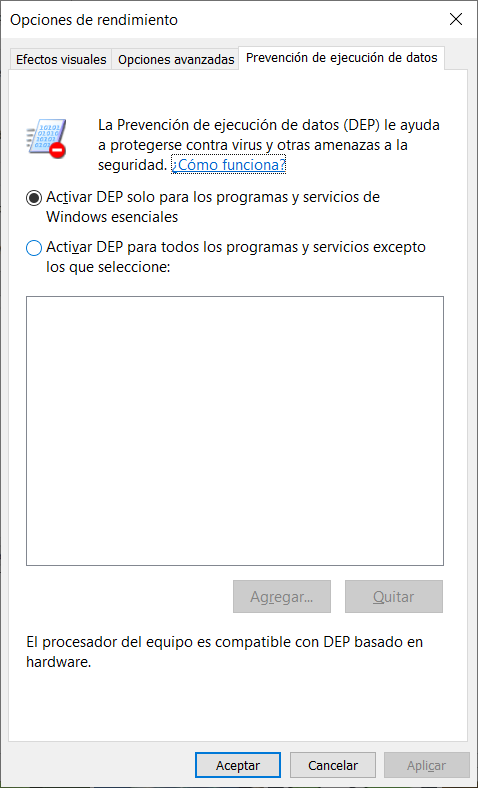


Permite modificar el nombre del equipo, así como el grupo de trabajo o dominio al que pertenece.

OPCIONES AVANZADAS



* OPCIONES DE RENDIMIENTO

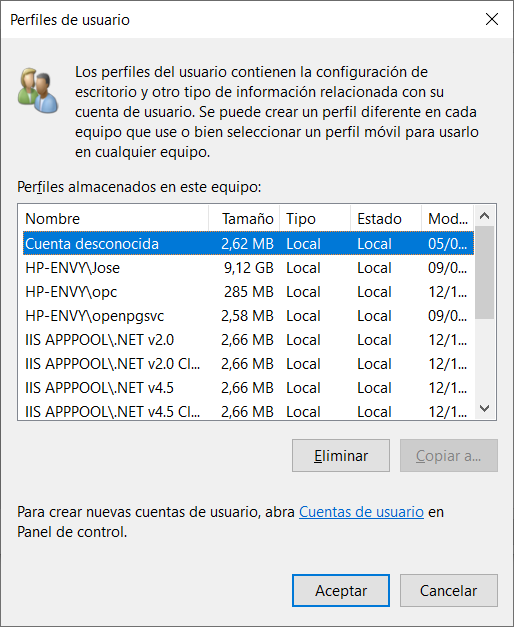
  

Permite configurar algunos parámetros del sistema que pueden optimizar su rendimiento.

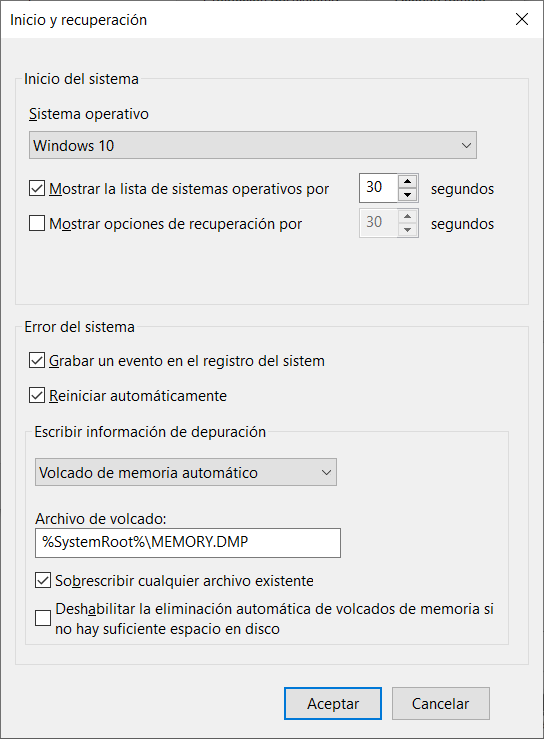
Podemos configurar el espacio en disco que destianmos a memoria virtual

Podemos configurar DEP (Data Execution Prevent)

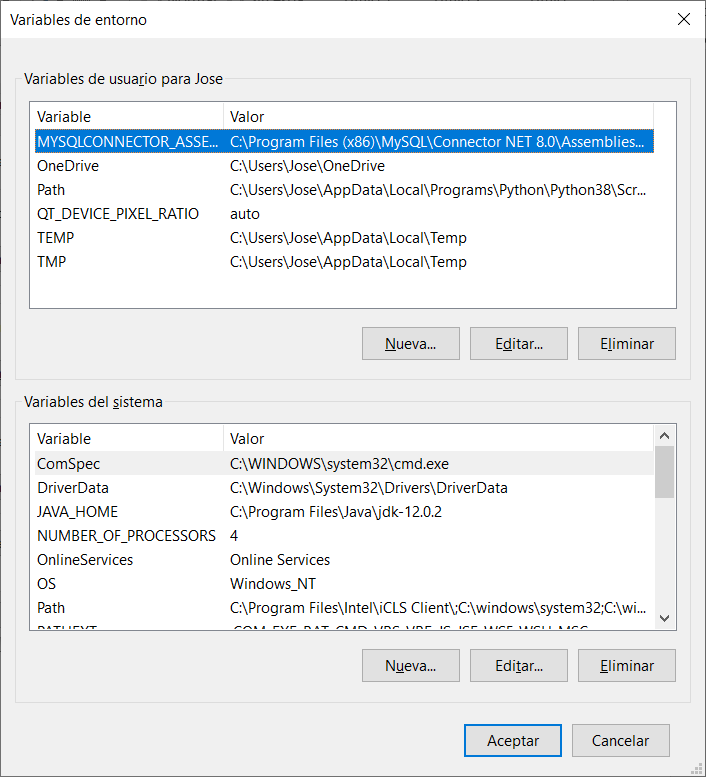
* PERFILES DE USUARIO



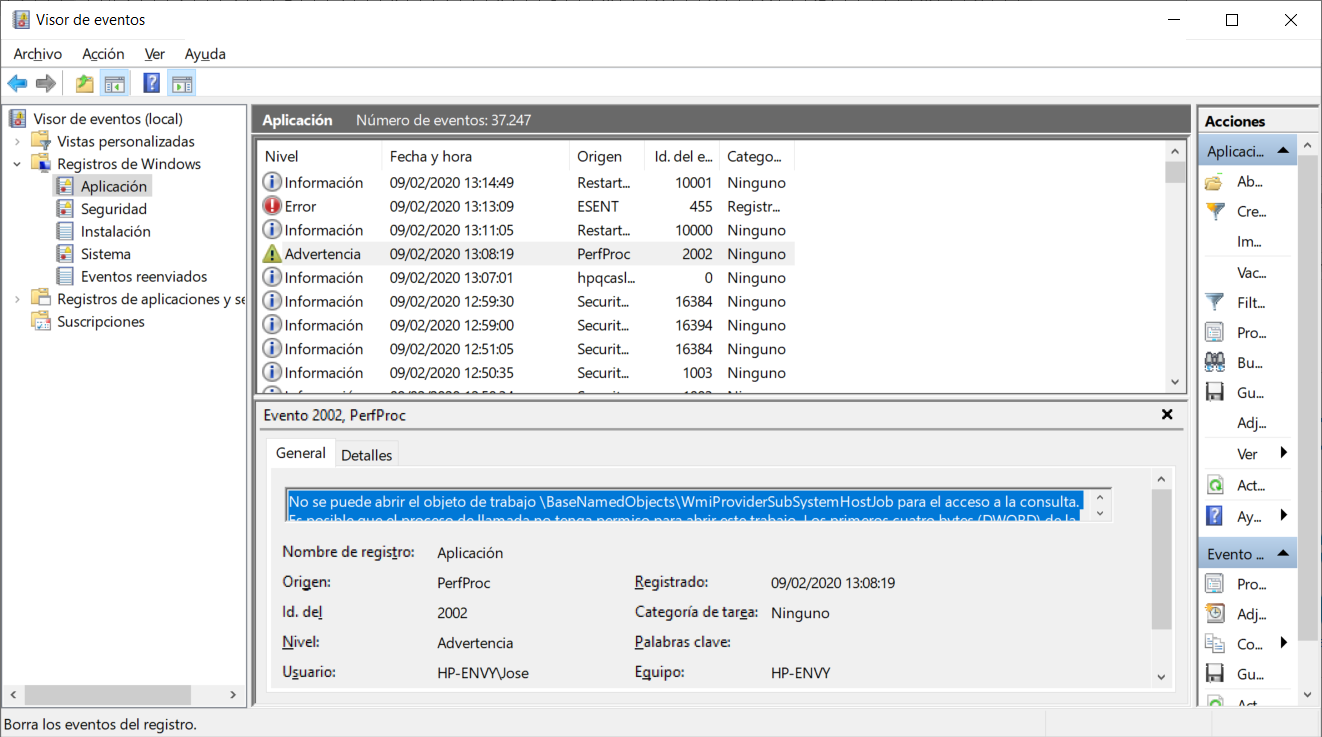
* INICIO Y RECUPERACIÓN



* VARIABLES DE ENTORNO



**VISOR DE EVENTOS**



Es una herramienta de supervisión que nos va a permitir visualizar un conjunto de archivos de registro. Con esta herramienta vamos a poder visualizar y analizar los eventos (sucesos) que han ocurrido en el sistema. Para que esto suceda ha de estar inicializado un servicio concreto que es: “Registro de eventos”🡪 evenlog.

**Eventos supervisables:**

* *Los sucesos de uso de los recursos del sistema, o registros de windows.*
  + - Registros de aplicación 🡪 Sucesos o eventos provenientes de las aplicaciones o programas.
    - Registros de seguridad 🡪 Eventos asociados a las directivas de auditoria establecidas en las directivas de grupo.
    - Registro del sistema 🡪 Contiene los sucesos o eventos que genera el SSOO y sus componentes.
    - Registro de instalación 🡪 Sucesos registrados en el proceso de instalación y configuración de las aplicaciones.
    - Registro de eventos reenviados 🡪 Siempre que este activo, nos va a permitir controlar los eventos reenviados a otros servidores.
* Las acciones de los usuarios, o registros de aplicaciones y servicios.
  + - Eventos de una única aplicación.

**Tipos de sucesos/eventos**:

*Información:* Nos describe el funcionamiento correcto de una aplicación o controlador

*Auditoria correcta/aciertos*: intentos de acceso de seguridad auditada correcta. (inicio de sesión correcta)

*Auditoria de errores*: intento de acceso de seguridad auditada erróneo.

*Advertencia*: Muestra un suceso que inicialmente no es importante pero que hay que tenerlo en cuenta en un futuro. (poco espacio en c:)

*Error*: indica un problema importante, perdida de datos o funcionalidad.

**Información por defecto del sistema:**

Es la información que nos aparece por defecto en la pantalla (en las columnas). Esta es:

* Tipo de suceso.
* Fecha hora.
* El origen. (Si lo ha generado una aplicación, un componente, un servicio.
* El suceso. (Asignado con un número).
* El usuario. El que estaba conectado cuando ocurrió.
* La categoría. (Si es de seguridad, de aplicación, …)
* Y todas las columnas que nosotros queramos ver y seleccionar.

**Configuración de las opciones del registro de sucesos:**

Cada uno de estos registros se van a almacenar en un fichero de extensión \*.evtx, almacenado en System32\Winevt\logs. Estos ficheros por defecto tienen un tamaño definido de 20480 kb, cuando el registro llega a este límite los eventos se sobrescriben empezando por el más antiguo. Esto se puede configurar.

**LAS COPIAS DE SEGURIDAD**

Varios métodos:

Copia de seguridad **diaria**: se realiza con los archivos seleccionados que se hayan modificado en el día en que se realiza la copia de seguridad. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.

Copia de seguridad **diferencial**: se realiza con los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.

Copia de seguridad **incremental**: se realiza con los archivos creados o modificados desde la última copia de seguridad normal o incremental. Los archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.

Copia de seguridad **intermedia**: se realiza con todos los archivos seleccionados. Dichos archivos no se marcan como copiados para que puedan volver a respaldarse cuando se desee.

Copia de seguridad **normal**: se realiza con todos los archivos seleccionados. Dichos archivos se marcan como copiados y ya no podrán volver a respaldarse hasta que se modifiquen.

Además de las copias de seguridad indicadas anteriormente, se puede realizar:

Una **imagen del sistema que es una copia exacta de una unidad**. Cuando se restaura el equipo a partir de una imagen del sistema, se realiza una restauración completa; no se pueden elegir elementos individuales para restaurar, así que todo el contenido se reemplazará por el contenido de la imagen del sistema.

1. **Panel de control** > **Sistema y mantenimiento** > **Copia de seguridad y restauración**.
2. **Crear una imagen del sistema** y, sigue los pasos del asistente.

 Si se te pide una contraseña de administrador o una confirmación, escribe la contraseña o proporciona la confirmación.

Nota

Tanto la unidad original (de la que se va a hacer la copia) como la unidad en la que se guarde deben estar formateadas en NTFS.

Un **disco de reparación del sistema** que arranque el sistema operativo en caso de un error grave del sistema que no permita acceder al sistema.

**Panel de control 🡪 Recuperación 🡪 Crear unidad de recuperación**

Un **punto de restauración del sistema** que permite devolver el equipo a un punto que se creó anteriormente.

1. **Panel de control** > **Sistema y mantenimiento** >**Sistema**.
2. **Protección del sistema** 🡪 pestaña **Protección del sistema** 🡪 **Crear**.
3. Escribe una descripción 🡪 **Crear**.

**Restaurar**

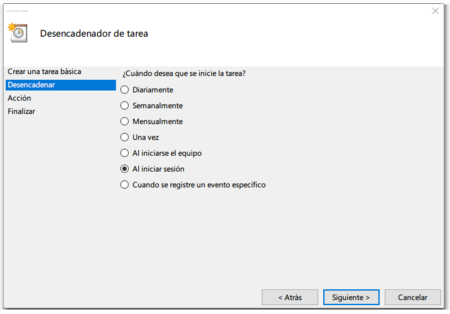
1. **Panel de control > Sistema y mantenimiento** > **Copia de seguridad y restauración**.
2. Realiza una de las siguientes operaciones:
   * **Restaurar mis archivos**.
   * **Restaurar los archivos de todos los usuarios.**
3. Realiza una de las siguientes operaciones:
   * **Buscar archivos** o **Buscar carpetas**. Cuando buscas carpetas, no puedes ver los archivos individuales de una carpeta. Para ver los archivos individuales: **Buscar archivos**.
   * Para buscar en el contenido de la copia de seguridad: **Buscar**, escribe todo o parte del nombre del archivo 🡪 **Buscar**.

**TAREAS PROGRAMADAS**

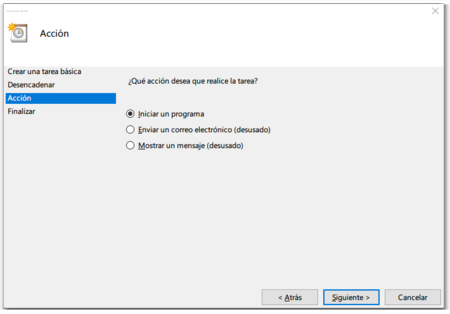
Programador de tareas

Acción 🡪 Crear tarea básica. O Acción 🡪 Crear tarea

Asigna un nombre y una descripción 🡪 siguiente.



Elegir cuando se inicia la tarea. Esto es el desencadenante o "trigger".

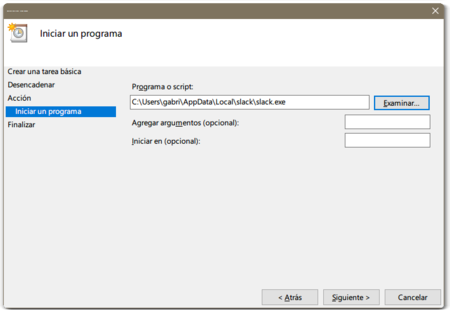


Elegir la acción:

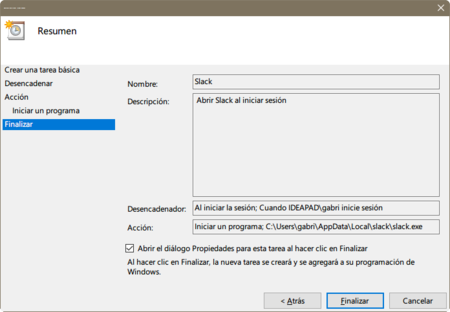
Iniciar un programa.

Enviar un correo. (en desuso en Windows 10)

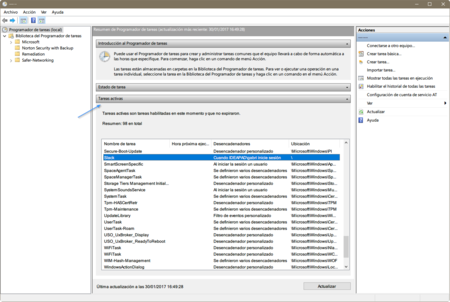
Mostrar un mensaje (en desuso en Windows 10)



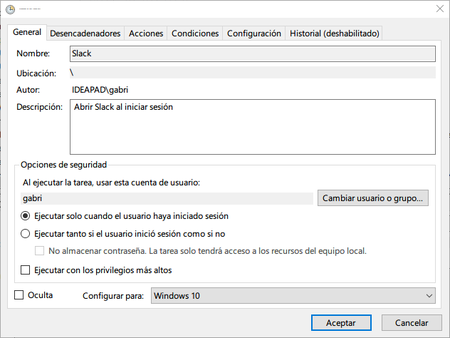
Indicar ruta al programa que se quiere ejecutar.



Para finalizar verás un mensaje de resumen sobre tu tarea, si marcas la casilla "Abrir el diálogo de Propiedades para esta tarea al hacer click en Finalizar" tendrás acceso a muchas más opciones. Es el mismo panel que aparecería si creas una tarea sin usar el asistente.



Tu tarea aparecerá ahora en la lista de Tareas activas. Si haces doble click sobre ella podrás acceder a sus propiedades pero no podrás cambiar nada. Para editar las propiedades de una tarea ya programada debes seleccionarla y luego en el panel de acciones a la derecha, hacer click en esa misma opción.



Desde propiedades se puede:

* añadir más desencadenadores y acciones a una misma tarea
* cambiar el grupo o usuario que ejecutará la tarea
* dar privilegios de administrador a una tarea
* cambiar condiciones referentes a la inactividad del equipo, el nivel de corriente, o la conexión de red
* activar un historial

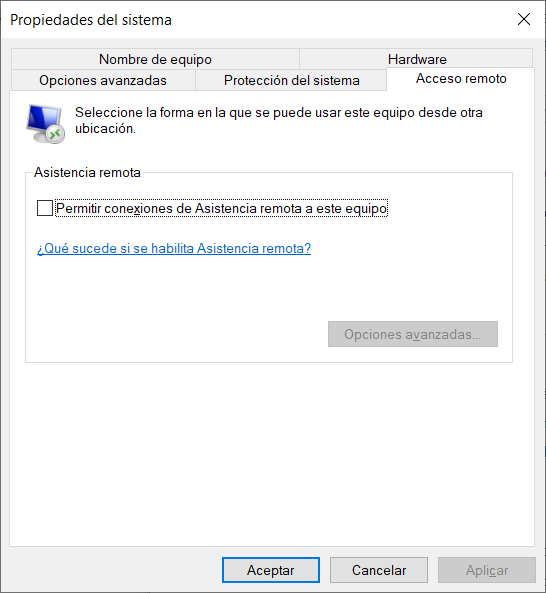
**ADMINISTRACIÓN REMOTA**

La administración remota consiste en realizar determinadas acciones desde un equipo local y que las mismas se ejecuten en otro equipo remoto. Entre las herramientas que se pueden utilizar se encuentran:

Los servicios de terminal: permiten a los usuarios acceder a los programas que están instalados en un servidor de terminales u obtener acceso a todo el Escritorio de Windows de forma remota, desde una red corporativa o desde Internet (está disponible en Windows Server2003/2008).

Los Escritorios remotos: esta utilidad, conocida anteriormente como el cliente de los Servicios de Terminal Server, permite administrar las Conexiones a Escritorio remoto de los servidores de terminales y los equipos que ejecuten una versión de WindowsServer2008R2, o superior.

**Equipo 🡪 Propiedades 🡪 Configuración Avanzada 🡪Acceso remoto**



**CIFRADO DE ARCHIVOS O DIRECTORIOS**

Solo se pueden cifrar archivos y directorios en volúmenes de unidades formateadas para ser utilizadas por el sistema NTFS.

Los archivos cifrados se pueden descifrar si se copian o mueven a una unidad que no esté formateada para ser utilizada por el sistema NTFS.

No se pueden cifrar las carpetas ni los archivos que estén comprimidos ni los archivos del sistema.

Al mover archivos descifrados a una carpeta cifrada, automáticamente se cifrarán en la nueva carpeta; sin embargo, la operación inversa no se hará automáticamente y se deberá realizar explícitamente el descifrado.

1. Clic derecho sobre la carpeta/archivo a **cifrar** 🡪 Propiedades –> Opciones avanzadas.
2. Marcar **Cifrar** contenido para proteger datos.