

ÍNDICE

[1. Introducción 2](#_Toc156158656)

[2. Servicios y procesos 3](#_Toc156158657)

[3. Gestión de recursos desde *Recopilador de Eventos* 5](#_Toc156158658)

[3.1. Gestión vía GUI: Aplicación del sistema *Servicios* 5](#_Toc156158659)

[3.2. Gestión vía CLI 7](#_Toc156158660)

[4. Informe de los recursos de hardware y del sistema 11](#_Toc156158661)

[4.1. Hardware 11](#_Toc156158662)

[4.2. Sistema 16](#_Toc156158663)

[5. Logs 19](#_Toc156158664)

[6. Conclusión 22](#_Toc156158665)

[7. Bibliografía 23](#_Toc156158666)

[7.1. Servicios y procesos 23](#_Toc156158667)

[7.2. Gestión de recursos desde *Recopilador de Eventos* 23](#_Toc156158668)

[7.3. Informe de los recursos de hardware y del sistema 23](#_Toc156158669)

[7.4. Logs 23](#_Toc156158670)

# 1. Introducción

Para entender el porqué de cada ejercicio, si se presta atención a los resultados de aprendizaje de la unidad, se puede identificar claramente aquello que pretende tratar,  coincidiendo un RA por cada ejercicio. Asimismo, comentaré brevemente ejercicio por ejercicio:

En el ejercicio 1, se pretende  *“conocer e identificar los tipos de procesos y servicios de un sistema operativo”*. No creo que necesite recursos teóricos adicionales más allá de la teoría del tema ya que trata de explicar con capturas propias puntos del tema. Realizaré el ejercicio entre las aplicaciones *Servicios,* *Administrador de tareas* y *Genial.ly*.

En el ejercicio 2, se pretende *“utilizar herramientas de monitorización del sistema”*. Para ello, se pide un caso práctico en el que hay que usar el Recopilador de eventos y modificar el tipo de inicio a través de comandos. También se hace una pregunta teórica. En caso de no hallar el modo de realizar el ejercicio entre los apuntes, acudiré a Google y buscaré resultados de Microsoft.

En el ejercicio 3, se pretende *“Visualizar los sucesos del sistema”*. Se pide realizar un informe de los recursos del hardware y del sistema, y para ello buscaré la información en el punto 5 del tema.

En el ejercicio 4, se pretende *“Entender un log del sistema”*. El ejercicio pide la definición de log, así como un pequeño caso práctico. Todo está dentro del punto 5 del tema.

# 2. Servicios y procesos

<https://view.genial.ly/659e48c4d348840013613d6b/presentation-servicios-y-procesos>

1ª Diapositiva:

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

2 º Diapositiva:

Interfaz de usuario gráfica, Diagrama

Descripción generada automáticamente

3ª Diapositiva:

Interfaz de usuario gráfica

Descripción generada automáticamente

4ª Diapositiva:

Diagrama

Descripción generada automáticamente

# 3. Gestión de recursos desde *Recopilador de Eventos*

## 3.1. Gestión vía GUI: Aplicación del sistema *Servicios*

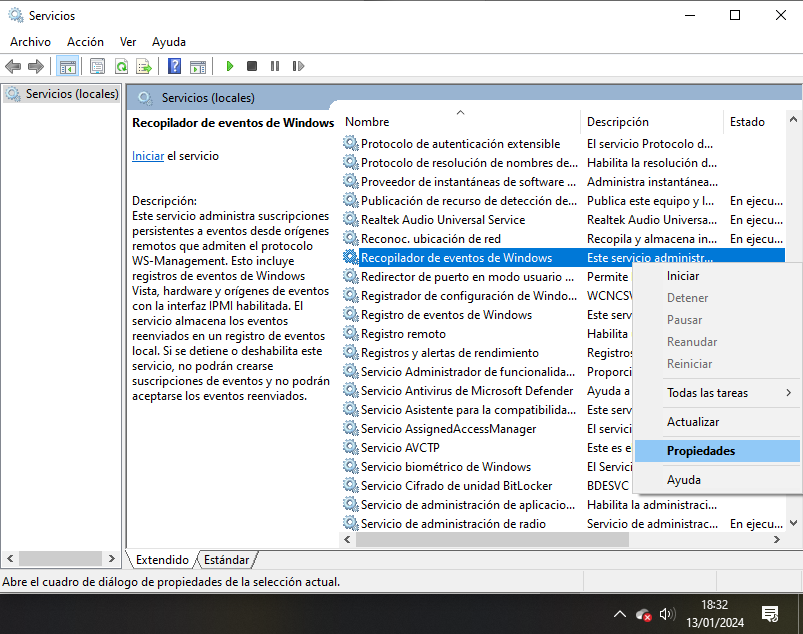
El recopilador de eventos es un Servicio de Windows. Por ello, hay que buscarlo en la aplicación *Servicios*.

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza media

Para ello, abrimos dicha aplicación buscándola en el buscador de la barra de herramientas.

Se busca dentro de la aplicación, clic derecho y *Propiedades*.



**Modo Manual** **Modo Deshabilitado**

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamenteInterfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

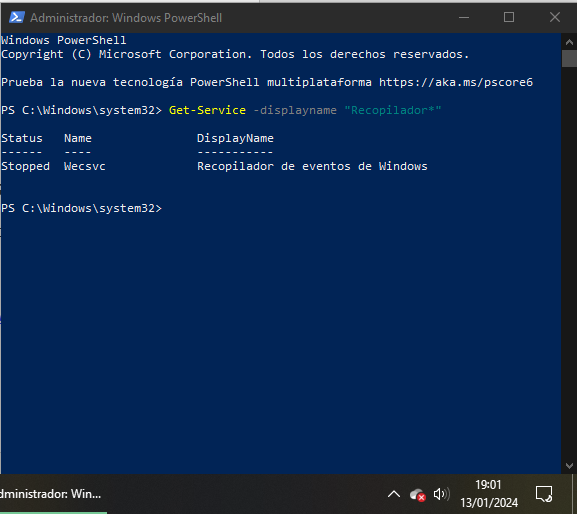
Descripción generada automáticamenteEn *Tipo de inicio*, seleccionar Manual. En *Tipo de inicio*, seleccionar Deshabilitado

## 3.2. Gestión vía CLI

Para la gestión del tipo de inicio del servicio *Recopilador de eventos*, se usará Powershell, una de las dos consolas que tiene Windows.

Captura de pantalla de un celular

Descripción generada automáticamente

Se busca mediante el buscador de la barra de tareas y se ejecuta como administrador.

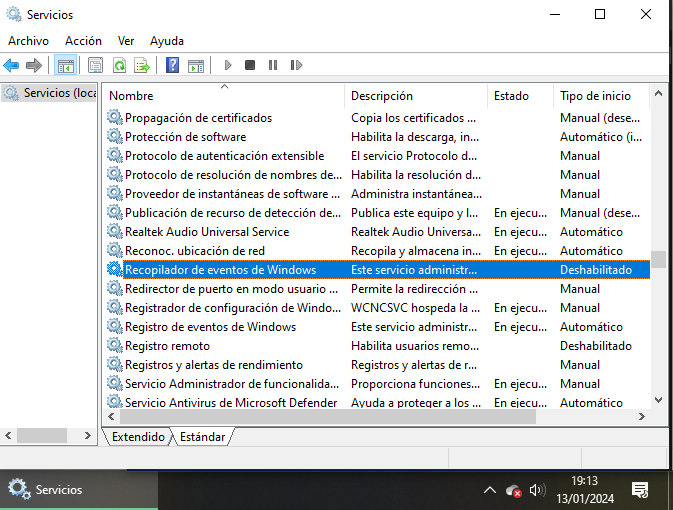
Se busca el nombre del servicio mediante el comando

Get-Service -displayname "Recopilador\*"

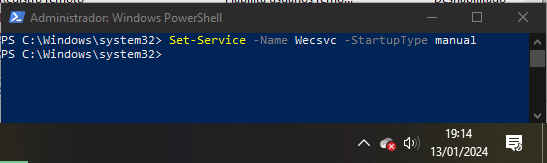
Ahora que ya se sabe como se llama el servicio, se puede gestionar el servicio.

Captura de pantalla de computadora

Descripción generada automáticamente

Para el tipo de inicio Manual, introducir el comando (en este ejemplo se empieza con el servicio deshabilitado, comprueba las horas).

Se introduce el comando Set-service -Name Wecsvc -StartupType manual.



Listo, ya está el servicio con el tipo de inicio configurado a manual.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

Ahora, para deshabilitar el servicio, se introduce el comando Set-service -Name Wecsvc -StartupType disabled.

Texto

Descripción generada automáticamente con confianza media

Listo, ya se ha deshabilitado el servicio.

Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamente

# 4. Informe de los recursos de hardware y del sistema

## 4.1. Hardware

Para poder comprobar el estado del hardware, se empleará la herramienta *Monitor de recursos*, la cual es fácilmente accesible a través del buscador de la barra de herramientas de Windows.

Imagen de la pantalla de un celular de un mensaje en letras blancas

Descripción generada automáticamente con confianza media

Dentro del monitor de recursos, se encuentra una interfaz con cinco pestañas distintas.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

- En la pestaña *CPU*, se puede ver el porcentaje dedicado tanto a los procesos como a los servicios del sistema. La frecuencia máxima hace referencia al máximo al que puede llegar la CPU, que no necesariamente al uso que se le está dando en ese momento. En el caso de mi procesador, al permitir *overclock* y funcionar por encima de sus capacidades, permite hasta un 160% de su frecuencia máxima. Hay un 12% de la CPU destinada a los procesos y un 0% a los servicios durante la toma de la captura de pantalla.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

En los procesos, llama la atención que casi la mitad de la CPU que consume mi equipo está destinada al proceso llamado MsMpEng.exe. Dicho proceso resulta ser Windows Defender, pero no es extraño que pueda consumir un buen trozo de la CPU debido a que está constantemente escaneando el sistema.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente

Máquina verde con letras blancas

Descripción generada automáticamente con confianza baja

Otra cosa que llama la atención es que los núcleos de la CPU no se usan de manera uniforme; en el caso de mi equipo, el noveno núcleo (se empieza a contar desde el 0) está a pleno rendimiento mientras muchos otros están casi a 0. Tras haber indagado, esto puede ser normal, y se debe a que hay programas que distribuyen sus procesos de manera uniforme entre los núcleos que formen el procesador y otros que centran sus procesos en el mínimo número de núcleos posible.

- En la pestaña *Memoria,* se puede ver el uso que el sistema le da a la memoria RAM. Se divide entre los procesos que están usando a RAM y una barra con los totales de uso. Windows Defender es el que más RAM está usando.

Interfaz de usuario gráfica, Aplicación

Descripción generada automáticamente con confianza media

- En la pestaña *Disco*, pueden verse los parámetros relacionados con la memoria del sistema (el almacenamiento).

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Pueden verse los procesos que están teniendo actividad en el sistema; en el caso de mi equipo, el sistema y Windows Defender son los que más están haciendo uso del disco. Además, puede verse los dispositivos de almacenamiento disponibles en el sistema, en mi caso, tan solo dos.

- En la pestaña Red, pueden verse todos aquellos parámetros relacionados con la red. Esto abarca desde los procesos que usan red hasta los puertos de escucha abiertos.

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

En mi caso, Chrome, Microsoft Word y Windows Defender son los que mas están usando la red.

## 4.2. Sistema

Para realizar el informe del sistema, se necesita la aplicación Monitor de confiabilidad. Para acceder, seguir a ruta Panel de control > Seguridad y mantenimiento > Ver historial de confiabilidad.

Una captura de pantalla de una computadora

Descripción generada automáticamente

Estos son los datos de errores críticos que han ocurrido en el equipo.

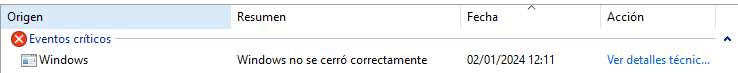
Gráfico, Gráfico de dispersión

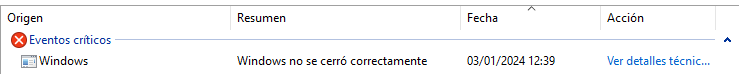
Descripción generada automáticamente

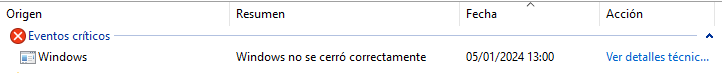
La mayor parte de los errores estuvieron relacionados con que Windows no se cerro correctamente, hubo un error relacionado con *Windows Defender*, otro con a aplicación de escritorio de *WhatsappWeb*, y otro error relacionado con un programa llamado *Zulu Platform*, el cual esta relacionado con un juego que, efectivamente, jugué ese día.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente con confianza media

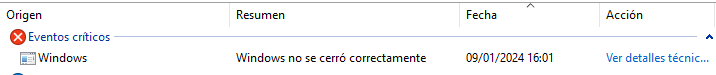






Interfaz de usuario gráfica, Texto, Aplicación

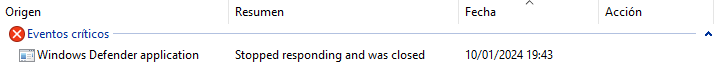
Descripción generada automáticamente

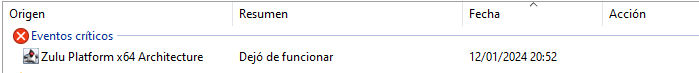


Aquí una extensión de los detalles técnicos del evento crítico anterior.

Texto

Descripción generada automáticamente con confianza media





# 5. Logs

Un log es un archivo que contiene registros de eventos dentro de un determinado espacio de tiempo. Para revisar los eventos guardados en un log, hay que acceder al *Visor de eventos*. Para ello, abrir la aplicación de ejecutar con Win+R y escribir *eventvwr.msc*.

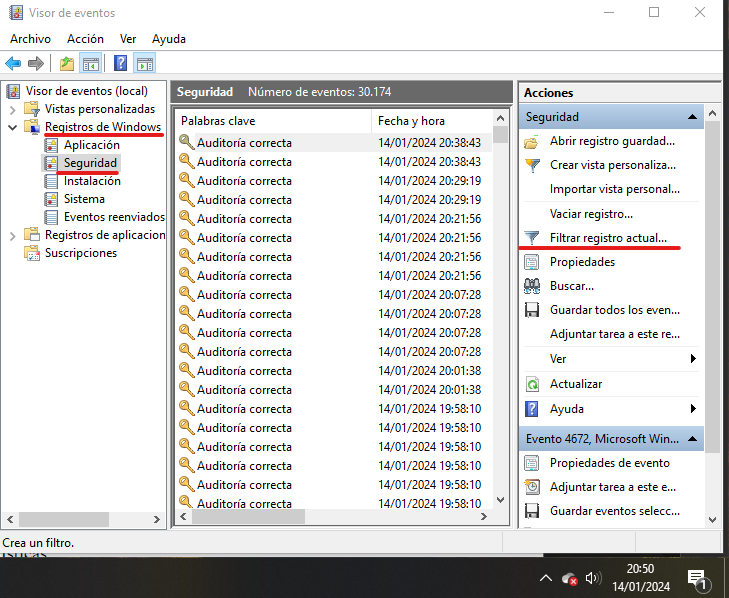
Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Interfaz de usuario gráfica, Texto, Aplicación

Descripción generada automáticamente

Ahora, para acceder a los eventos de nivel crítico de seguridad, hay que ir a los *Registros de Windows>Seguridad*. Luego, en la sección vertical de la derecha *Acciones*, pulsar en *Filtrar registro actual…*



Interfaz de usuario gráfica, Texto, Aplicación, Correo electrónico

Descripción generada automáticamenteEn el apartado Nivel del evento, marcar la casilla de *Crítico* y darle a *Aceptar*.

Interfaz de usuario gráfica, Texto

Descripción generada automáticamente

Ahora no sale ningún log puesto que no ha habido eventos de nivel crítico de seguridad, pero si hubiera alguno, aparecería.

# 6. Conclusión

A lo largo de esta práctica, más allá de comentar lo obvio acerca del aprendizaje que se contempla en los resultados de aprendizaje del temario, puedo afirmar que he aprendido acerca de como funciona el hardware, y de cómo interactúan entre sí de manera más práctica.

En especial, destaco el uso de los núcleos que hacen las aplicaciones. Según he aprendido, depende totalmente no del sistema ni del hardware, sino de las aplicaciones, y aunque sea contraintuitivo, hay aplicaciones que buscan sacar el máximo rendimiento de un solo núcleo, dejando libre los demás.

# 7. Bibliografía

## 7.1. Servicios y procesos

- Apuntes de la asignatura.

## 7.2. Gestión de recursos desde *Recopilador de Eventos*

- Muycomputer.com. Eduardo Medina (2022). *Cómo gestionar de forma básica los servicios de Windows*.

<https://www.muycomputer.com/2022/09/09/gestion-basica-servicios-windows/>

## 7.3. Informe de los recursos de hardware y del sistema

- Apuntes de la asignatura.

- TASK MANAGER How to view CPU usage and cores virtual core usage.

<https://www.youtube.com/watch?v=oilyee1UUyM>

- FreeCodeCamp.org. Kolade Chris (2023). *¿Qué es msmpeng.exe? ¿Por qué consume tanta CPU?*

<https://www.freecodecamp.org/espanol/news/que-es-msmpeng-exe-porque-consume-tanta-cpu/>

## 7.4. Logs

- Apuntes de la asignatura