



Sistemas informáticos

Tarea 1. UT5. Procesos,
servicios y sucesos en
Windows

Francisco José García Cutillas | 1FPGS_DAM



Índice

Ejercicio 1. Administrador de tareas	3
Ejercicio 2. Memoria Virtual	7
Ejercicio 3. Tareas programadas.....	10
Ejercicio 4. Servicios	16
Ejercicio 5. Sucesos.....	24

Ejercicio 1. Administrador de tareas

1.1 Lanza el “Bloc de notas” y a continuación el Administrador de Tareas.

Nombre	Estado	8% CPU	40% Memoria	0% Disco	0% Red	Consumo de ...	Tendencia de ...
Aplicaciones (3)							
Administrador de tareas		2,2%	9,4 MB	0,1 MB/s	0 Mbps	Muy baja	Muy baja
Bloc de notas		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Procesador de comandos de Wi...		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Procesos en segundo plano (44)							
Aislamiento de gráficos de disp...		0%	0,3 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Antimalware Service Executable		0%	9,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Aplicación de subsistema de cola		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Application Frame Host		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Búsqueda		0%	0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
Cargador de CTF		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
CCleaner		0%	1,0 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
CCleaner Performance Optimiz...		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
COM Surrogate		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja
COM Surrogate		0%	0,1 MB	0 MB/s	0 Mbps	Muy baja	Muy baja

1.2 En ocasiones el Explorador de Windows se queda bloqueado y no podemos hacer uso del menú Inicio ni de la barra de tarea. Para solucionarlo, habría que volver a lanzarlo desde el Administrador de tareas. Lánzalo (el nombre del fichero ejecutable es “explorer”).

Crear nueva tarea

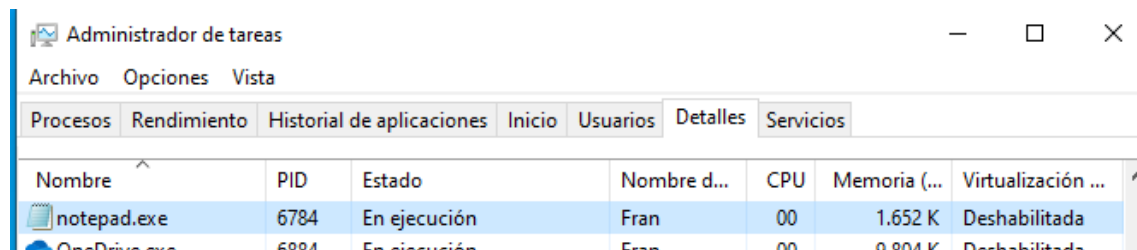
Escriba el nombre del programa, carpeta, documento o recurso de Internet que desea abrir con Windows.

Abrir:

☐ Crear esta tarea con privilegios administrativos

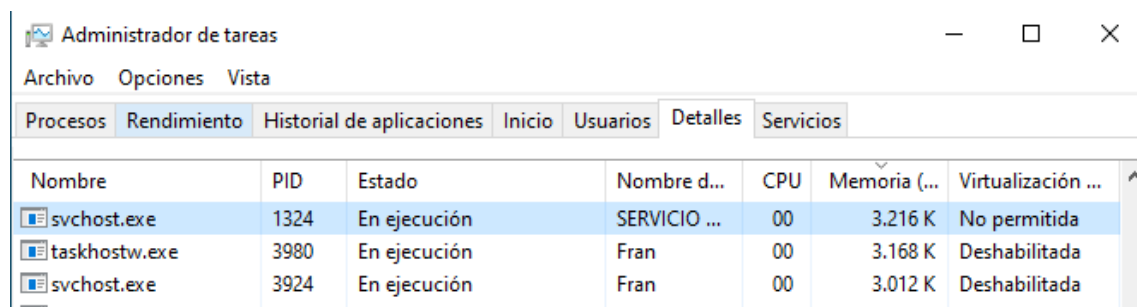
Aceptar Cancelar Examinar...

1.3 ¿Cuál es el proceso que ejecuta el “Bloc de notas”?



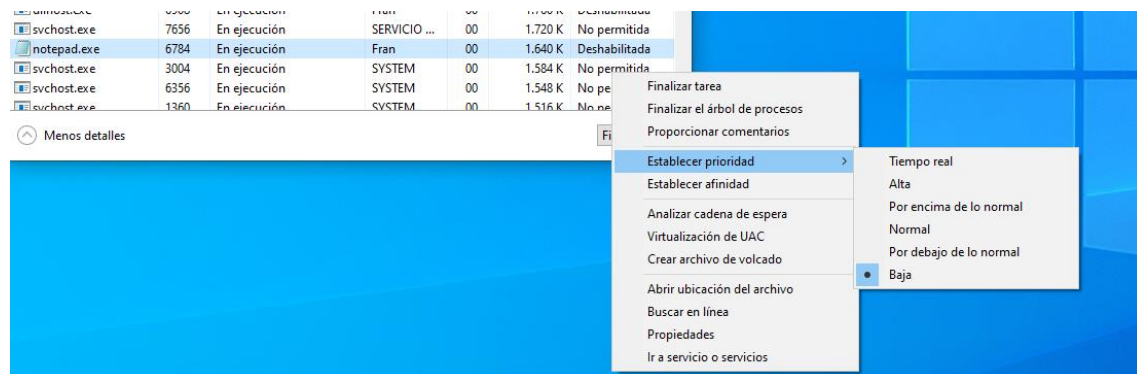
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
notepad.exe	6784	En ejecución	Fran	00	1.652 K	Deshabilitada
OneDrive.exe	6084	En ejecución	Fran	00	0.004 K	Deshabilitada

1.4 Determina cuál es el proceso que consume más memoria.



Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
svchost.exe	1324	En ejecución	SERVICIO ...	00	3.216 K	No permitida
taskhostw.exe	3980	En ejecución	Fran	00	3.168 K	Deshabilitada
svchost.exe	3924	En ejecución	Fran	00	3.012 K	Deshabilitada

1.5 Asigna al proceso del “Bloc de notas” la menor prioridad posible.



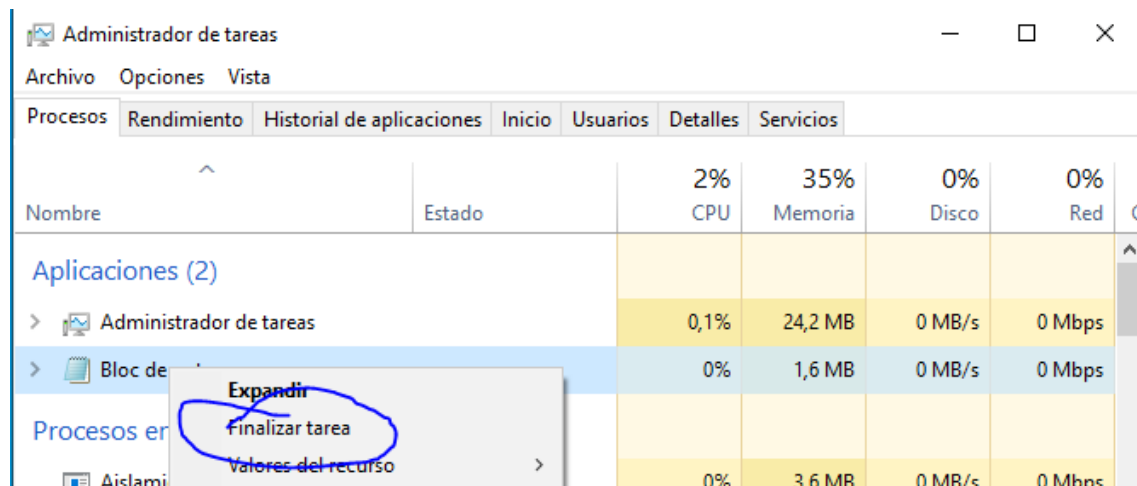
Nombre	PID	Estado	Nombre d...	CPU	Memoria (...)	Virtualización ...
svchost.exe	7656	En ejecución	SERVICIO ...	00	1.720 K	No permitida
notepad.exe	6784	En ejecución	Fran	00	1.640 K	Deshabilitada
svchost.exe	3004	En ejecución	SYSTEM	00	1.584 K	No permitida
svchost.exe	6356	En ejecución	SYSTEM	00	1.548 K	No permitida
svchost.exe	1360	En ejecución	SYSTEM	00	1.516 K	No permitida

Menos detalles

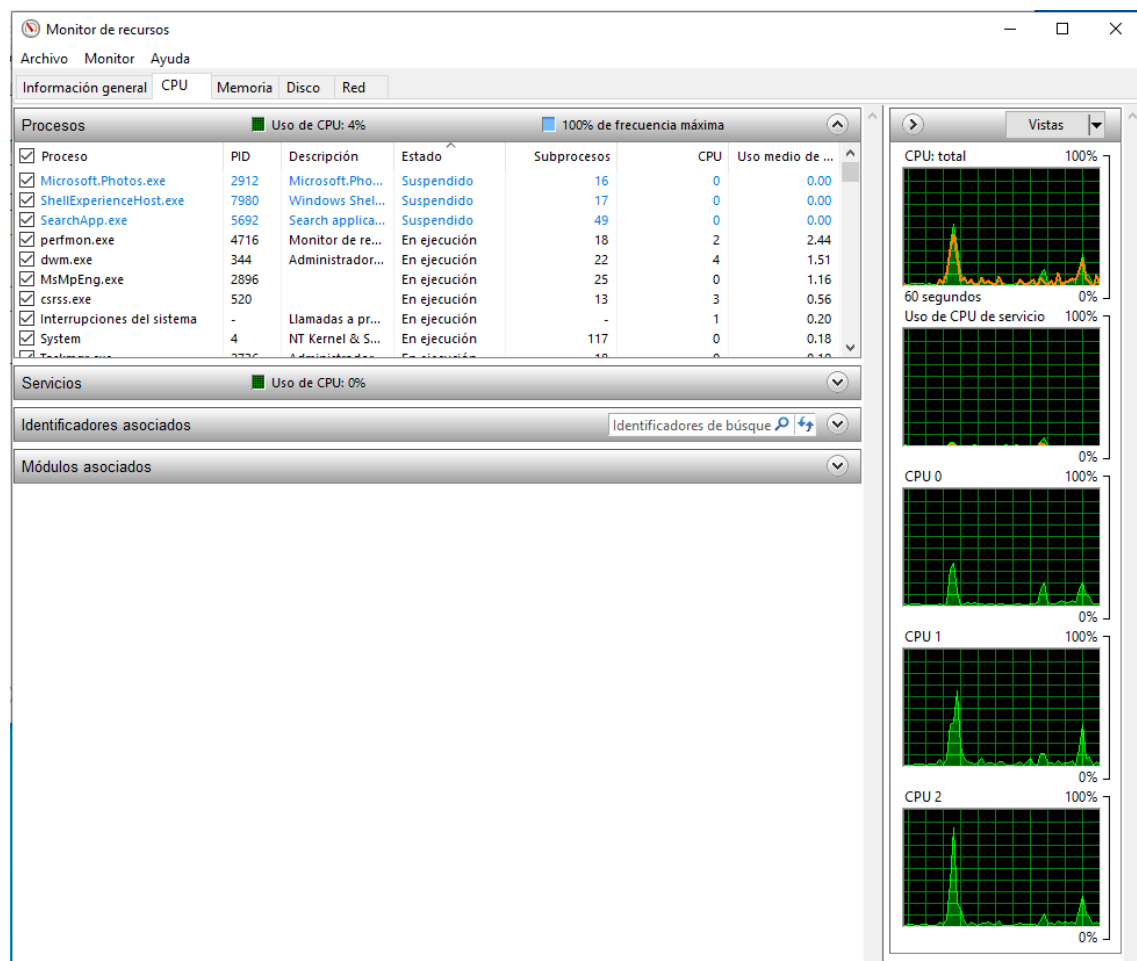
Establecer prioridad

- Tiempo real
- Alta
- Por encima de lo normal
- Normal
- Por debajo de lo normal
- Baja**

1.6 Desde el Administrador de Aplicaciones termina la ejecución del “Bloc de notas”.



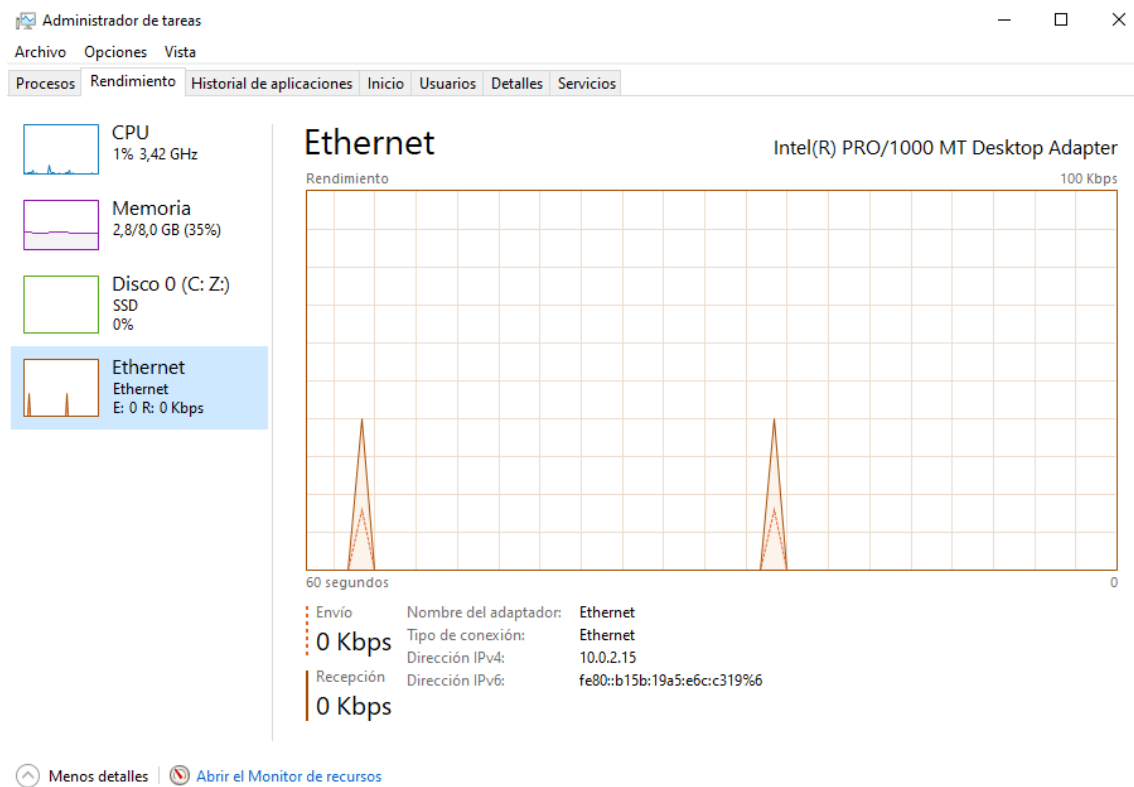
1.7 Haz que en el gráfico de “Uso de la CPU” también se muestre la información referente al núcleo.



1.8 En la tabla de la “Memoria del núcleo”, ¿qué representa la memoria del núcleo No paginada?

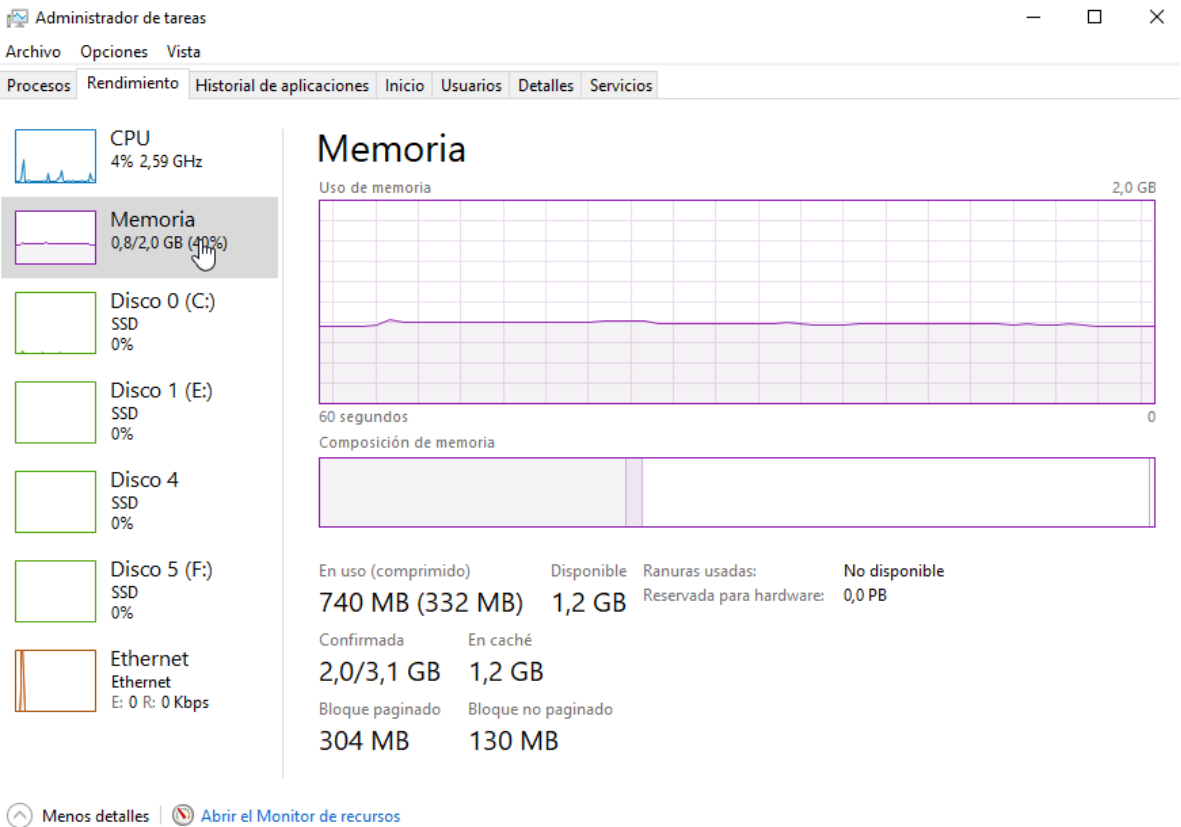
Es aquella memoria que no se puede paginar al disco, es decir, aquella memoria que no se puede transferir desde memoria RAM al disco duro para liberar espacio en la misma

1.9 Muestra la información de Bytes enviados y Bytes recibidos.

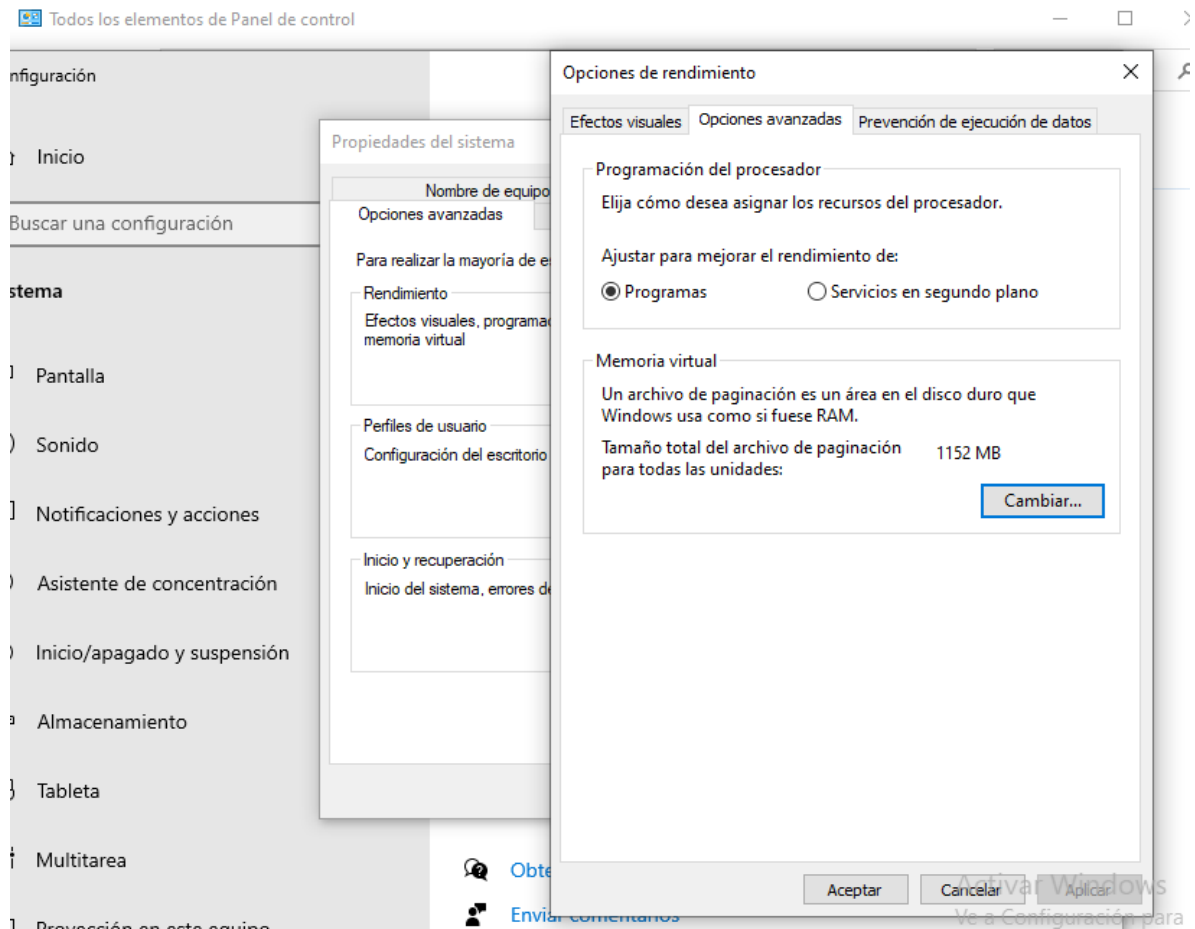


Ejercicio 2. Memoria Virtual

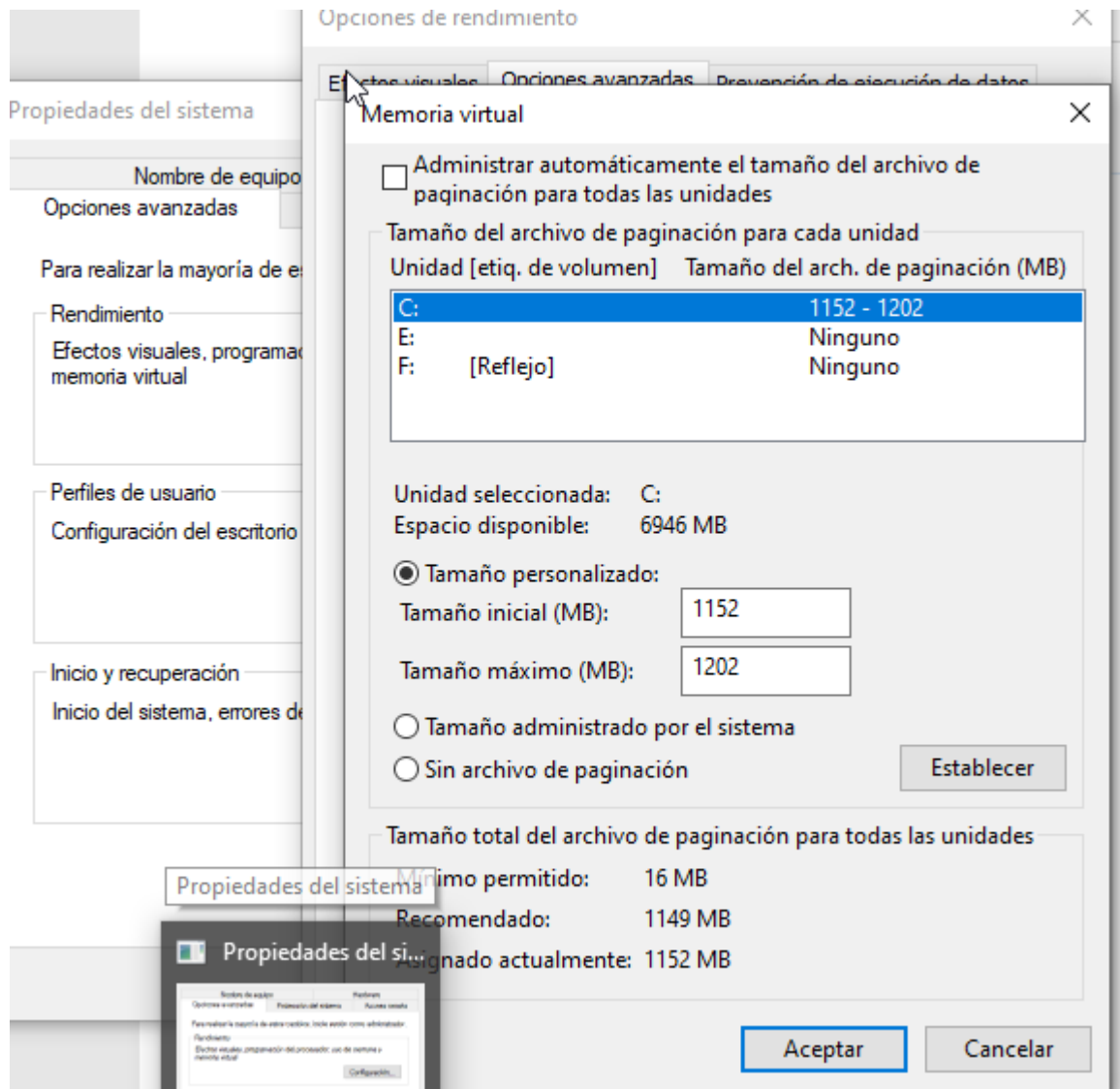
2.1 Desde el Administrador de tareas indica qué cantidad de memoria de paginación está usada en este momento.



2.2 Indica cómo verías el tamaño total del archivo de paginación para todas las unidades de disco.

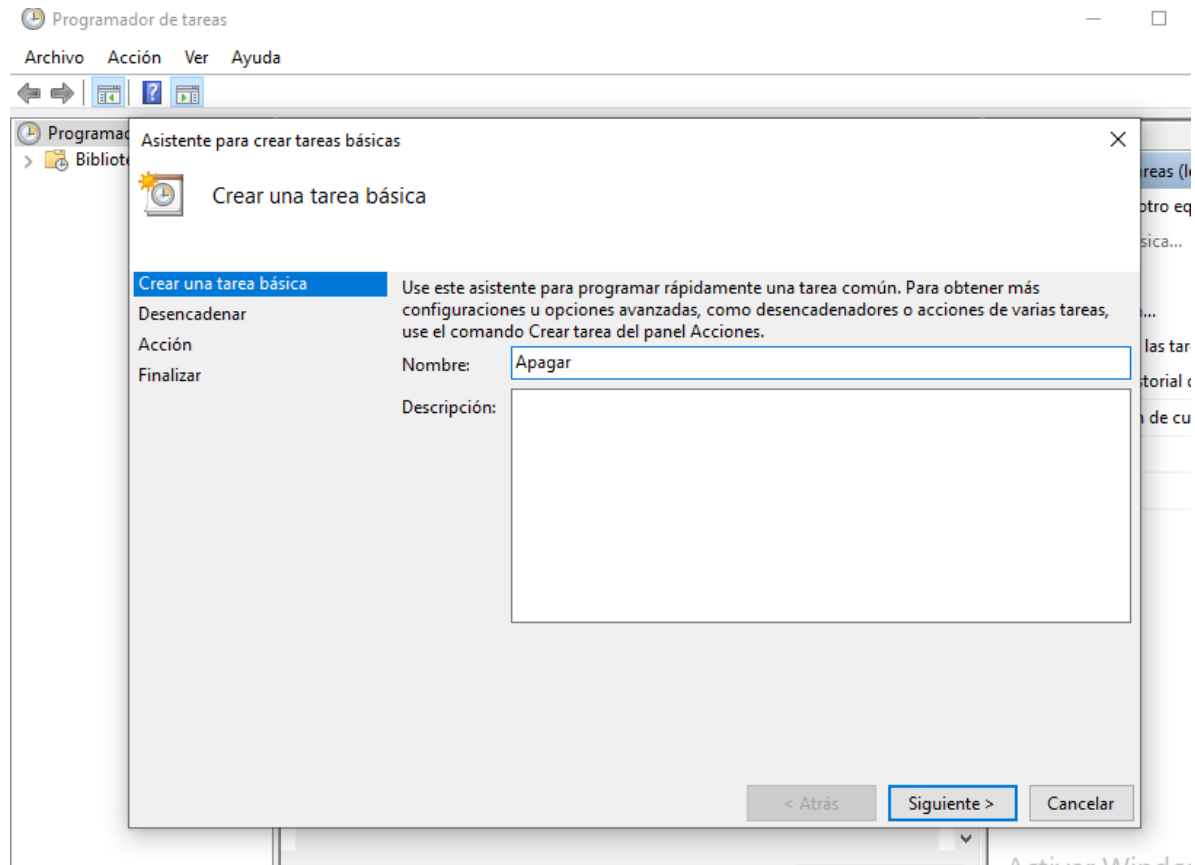


2.3 Cambia el tamaño del archivo de paginación para que ahora tengas 50MB más de límite máximo.




Ejercicio 3. Tareas programadas

3.1 Configura una tarea programada para que todos los días a las 14:30 se apague tu ordenador.



Asistente para crear tareas básicas

 Desencadenador de tarea

Crear una tarea básica

Desencadenar

Acción

Finalizar

¿Cuándo desea que se inicie la tarea?

☒ Diariamente

☐ Semanalmente

☐ Mensualmente

☐ Una vez

☐ Al iniciarse el equipo

☐ Al iniciar sesión


☐ Cuando se registre un evento específico

< Atrás

Siguiente >

Cancelar

Asistente para crear tareas básicas

 Diariamente

Crear una tarea básica

Desencadenar

Diariamente

Acción

Finalizar

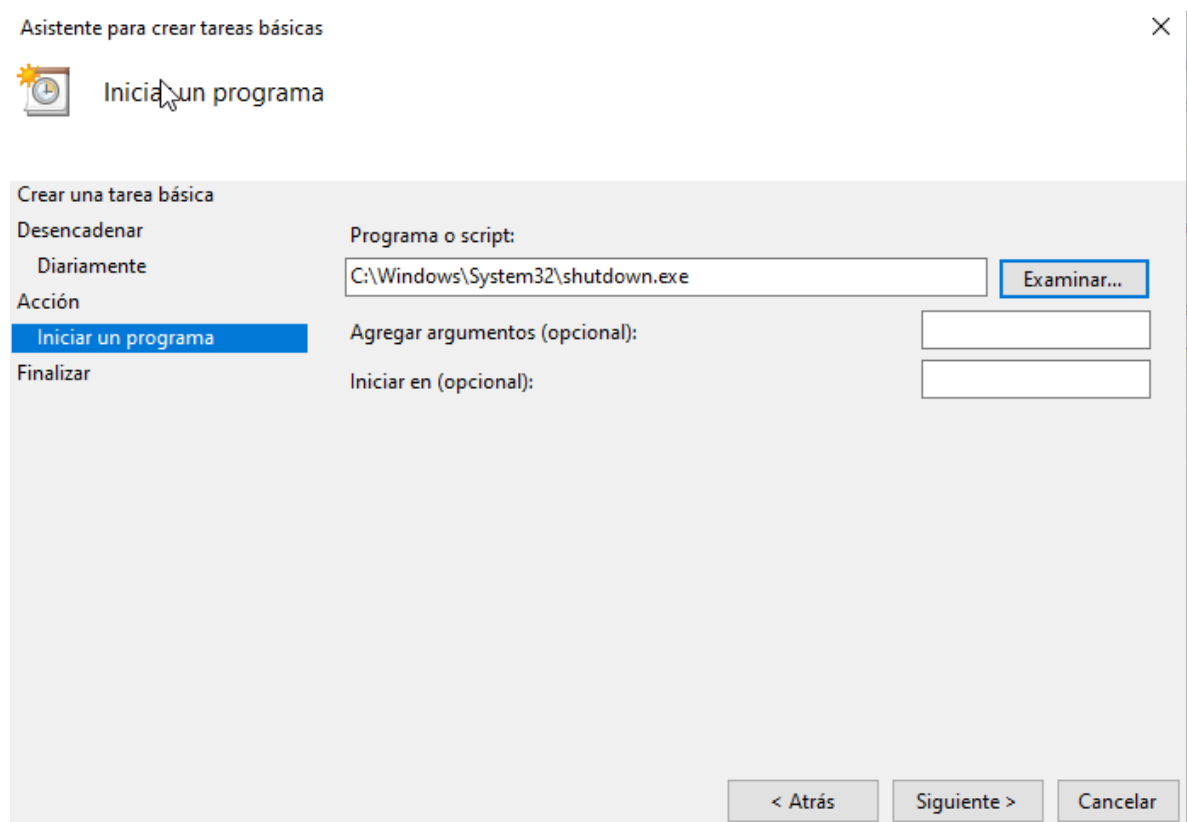
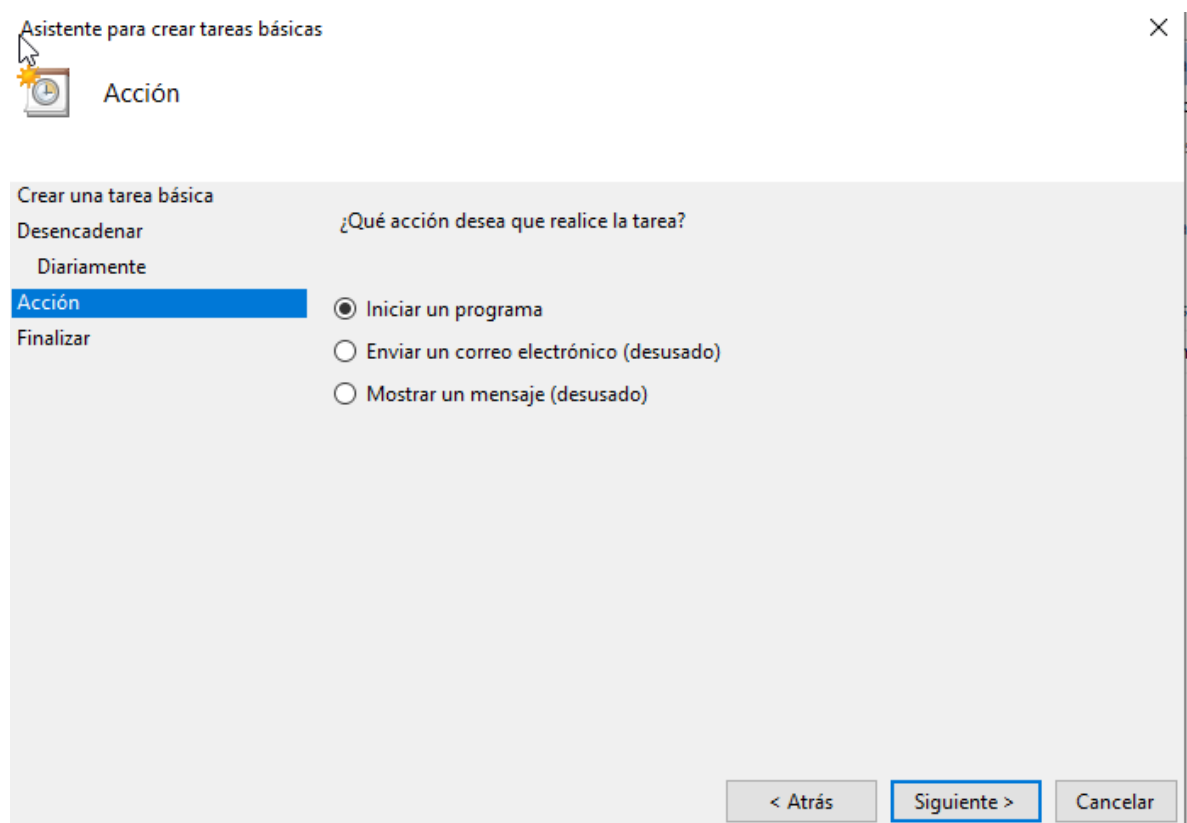
Inicio: 02/03/2023 14:30:00 ☐ Sincronizar zonas horarias

Repetir cada: 1 días

< Atrás

Siguiente >

Cancelar



Asistente para crear tareas básicas



Resumen

Crear una tarea básica

Desencadenar

Semanalmente

Acción

Iniciar un programa

Finalizar

Nombre:

Copia

Descripción:

Desencadenador: Semanalmente; A las 11:00 cada Lunes, Miércoles, Viernes de todas las s

Acción:

Iniciar un programa; C:\bat\Tarea1.bat

☐ Abrir el diálogo Propiedades para esta tarea al hacer clic en Finalizar

Al hacer clic en Finalizar, la nueva tarea se creará y se agregará a su programación de Windows.

< Atrás

Finalizar

Cancelar

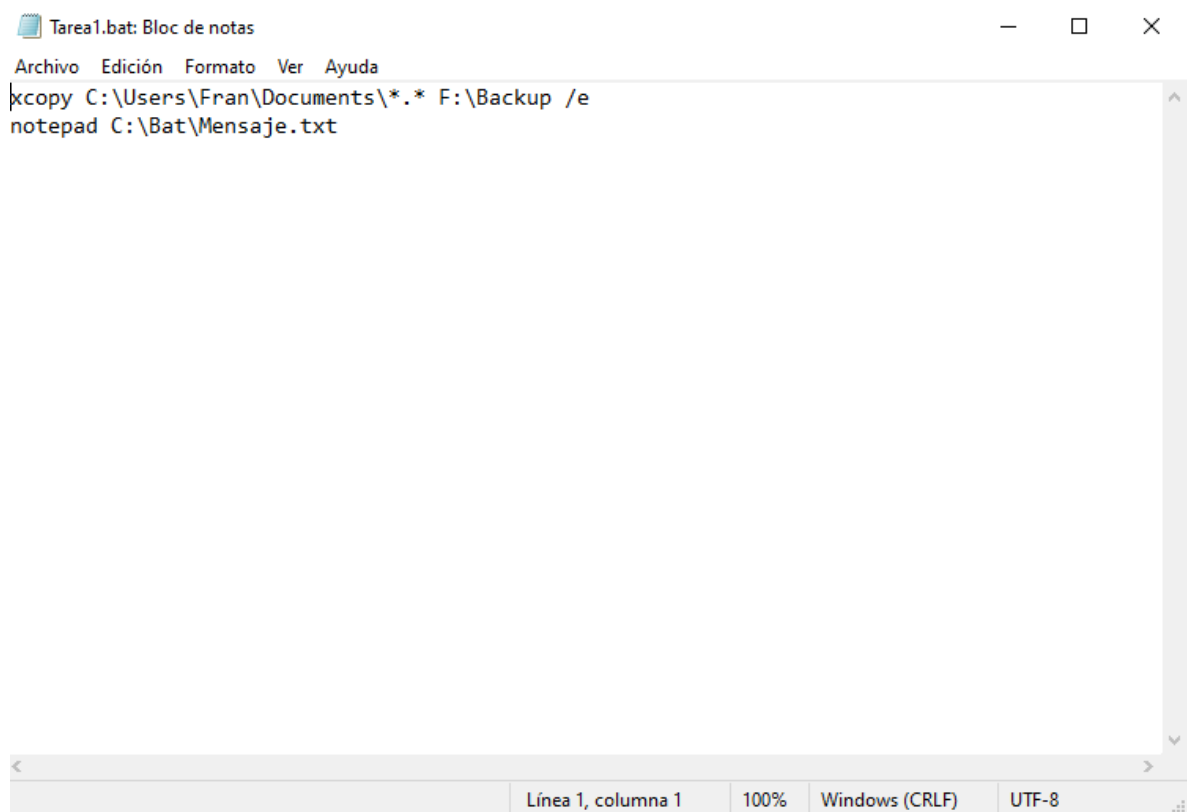
C:\WINDOWS\SYSTEM32\cmd.exe

Mensaje.txt: Bloc de notas

Archivo Edición Formato Ver Ayuda

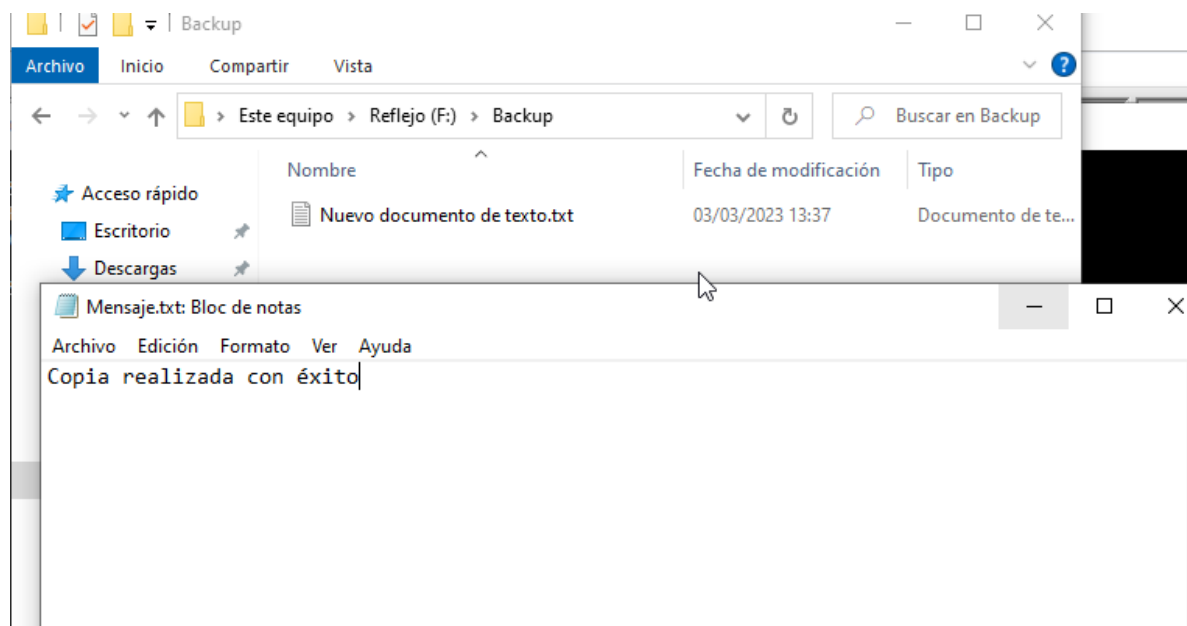
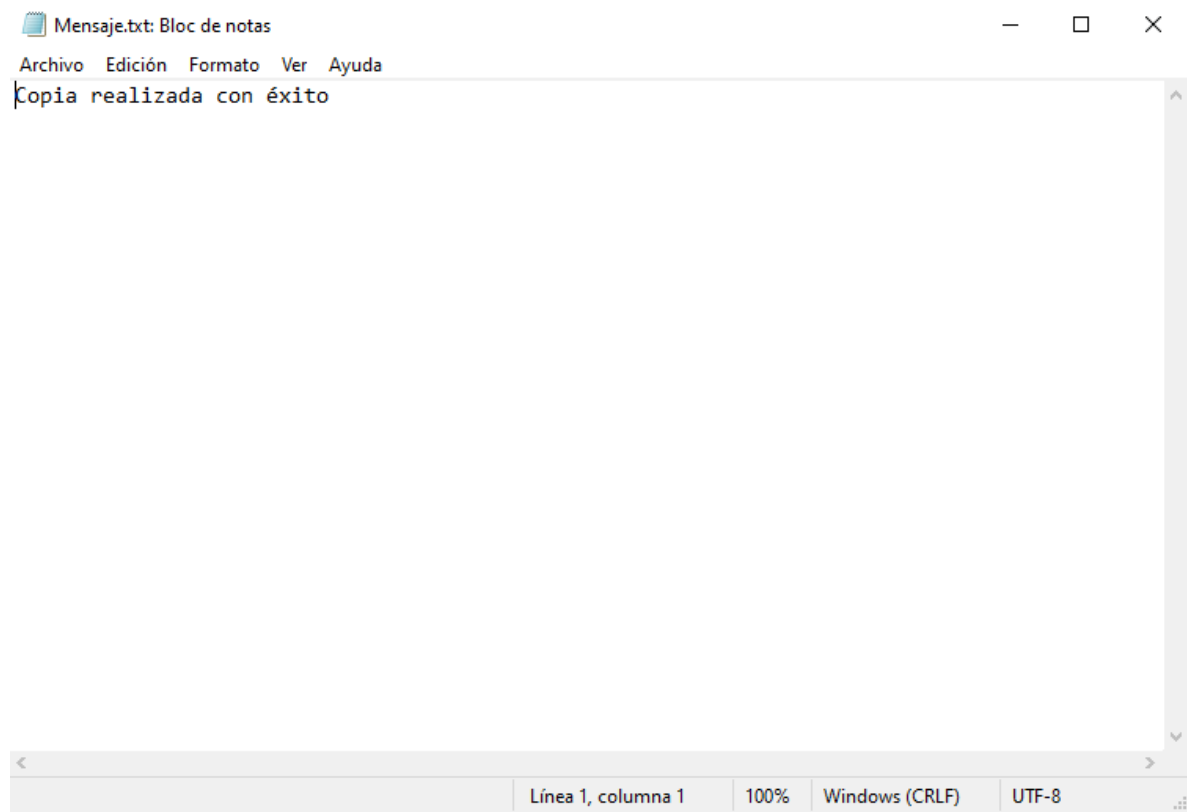
Copia realizada con éxito

3.2 Configura una tarea programada llamada Copias que realice una copia de los archivos de la carpeta “Mis Documentos” a una carpeta llamada Backup que se encuentre en una partición diferente a la C: .La tarea se debe realizar todos los lunes, miércoles y viernes a las 23:00. Al terminar la copia debe abrir el bloc de notas con un archivo que contenga la frase “COPIA REALIZADA”



```
Tarea1.bat: Bloc de notas
Archivo  Edición  Formato  Ver  Ayuda
xcopy C:\Users\Fran\Documents\*. * F:\Backup /e
notepad C:\Bat\Mensaje.txt
```

Línea 1, columna 1 100% Windows (CRLF) UTF-8



Ejercicio 4. Servicios

4.1 Desde la herramienta Servicios: ¿cómo sabemos qué servicios se están ejecutando en un momento dado? ¿Cómo se indica que un servicio está detenido? ¿y que está pausado? ¿Cuáles de ellos se lanzan en el proceso de arranque?

Se ejecutan los que en su estado pone “En ejecución”.

Un servicio está detenido si en su estado no aparece nada.

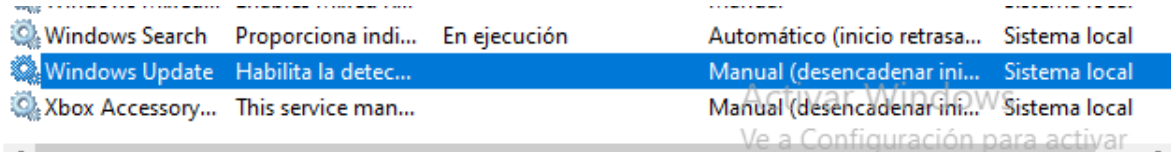
Se lanzan en el proceso de arranque los que tienen el “tipo de inicio” en automático

Seleccione un elemento para ver su descripción.

Nombre	Descripción	Estado	Tipo de inicio	Iniciar sesión co
Acceso a datos de usuarios...	Proporciona a la...	En ejecución	Manual	Sistema local
Actualizador de zona horari...	Establece la zona...		Deshabilitado	Servicio local
Adaptador de rendimiento ...	Proporciona info...		Manual	Sistema local
Administración de aplicacio...	Procesa las solici...		Manual	Sistema local
Administración de autentic...	Proporciona serv...		Manual	Sistema local
Administración de capas de...	Optimiza la colo...		Manual	Sistema local
Administración remota de ...	El servicio Admi...		Manual	Servicio de red
Administrador de conexio...	Crea una conexi...		Manual	Sistema local
Administrador de conexio...	Administra cone...		Manual	Sistema local
Administrador de conexio...	Toma decisiones ...	En ejecución	Automático (...)	Servicio local
Administrador de configura...	Habilita la detec...		Manual (dese...	Sistema local
Administrador de credencia...	Proporciona un ...	En ejecución	Manual	Sistema local
Administrador de cuentas d...	El inicio de este s...	En ejecución	Automático	Sistema local
Administrador de cuentas ...	El Administrador...	En ejecución	Manual	Sistema local
Administrador de identidad...	Proporciona serv...		Manual	Servicio local
Administrador de mapas de...	Servicio de Wind...		Automático (i...	Servicio de red
Administrador de pagos y ...	Administra los p...	En ejecución	Manual (dese...	Servicio local
Administrador de sesión local	Servicio central d...	En ejecución	Automático	Sistema local
Administrador de usuarios	El administrador ...	En ejecución	Automático (...)	Sistema local
Adquisición de imágenes d...	Proporciona serv...		Manual	Servicio local
Agent Activation Runtime...	Runtime for acti...		Manual	Sistema local
Agente de conexión de red	Conexiones de a...	En ejecución	Manual (dese...	Sistema local
Agente de detección en seg...	Permite a las apli...		Manual (dese...	Sistema local
Agente de directiva IPsec	El protocolo de s...		Manual (dese...	Servicio de red
Agente de eventos de tiempo	Coordina la ejec...	En ejecución	Manual (dese...	Servicio local
Agente de eventos del siste...	Coordina la ejec...	En ejecución	Automático (...)	Sistema local
Agente de supervisión en ti...	Supervisa y certif...	En ejecución	Automático (i...	Sistema local
Agrupación de red del mis...	Permite la comu...		Manual	Servicio local

4.2 Con el Servicio de Windows Update (Actualizaciones Automáticas) responde a las preguntas o realiza las tareas que se piden, según sea el caso:

4.2.1 ¿Cuál es el estado actual del servicio?

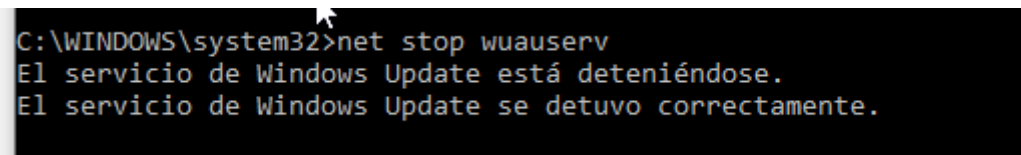


A screenshot of the Windows Services console. The 'Windows Update' service is selected and highlighted in blue. The service status is 'En ejecución' (Running). The startup type is 'Automático (inicio retrasado)' (Automatic (Delayed Start)). The service is installed on the 'Sistema local' (Local system). A watermark 'Activar Windows' is visible in the background.

Nombre	Descripción	Estado	Tipo de inicio	Ubicación
Windows Search	Proporciona indi...	En ejecución	Automático (inicio retrasado)	Sistema local
Windows Update	Habilita la detec...	En ejecución	Automático (inicio retrasado)	Sistema local
Xbox Accessory...	This service man...	En ejecución	Manual (desencadenar ini...)	Sistema local

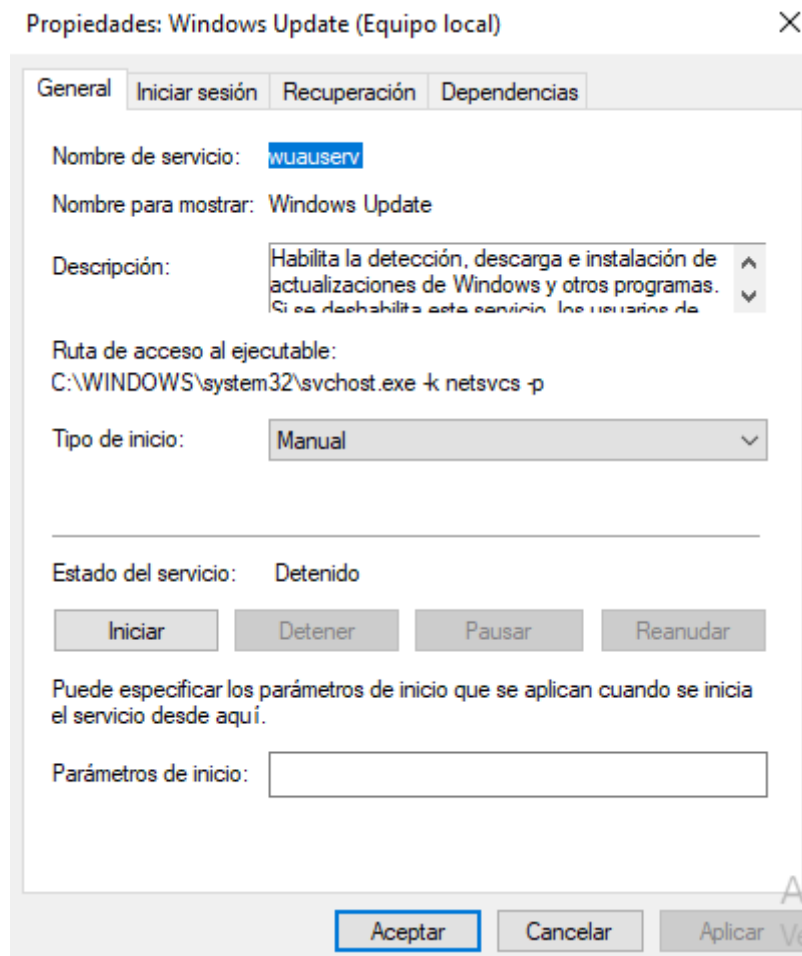
Ahora mismo está parado

4.2.2 Detén el servicio. ¿Qué sucede?



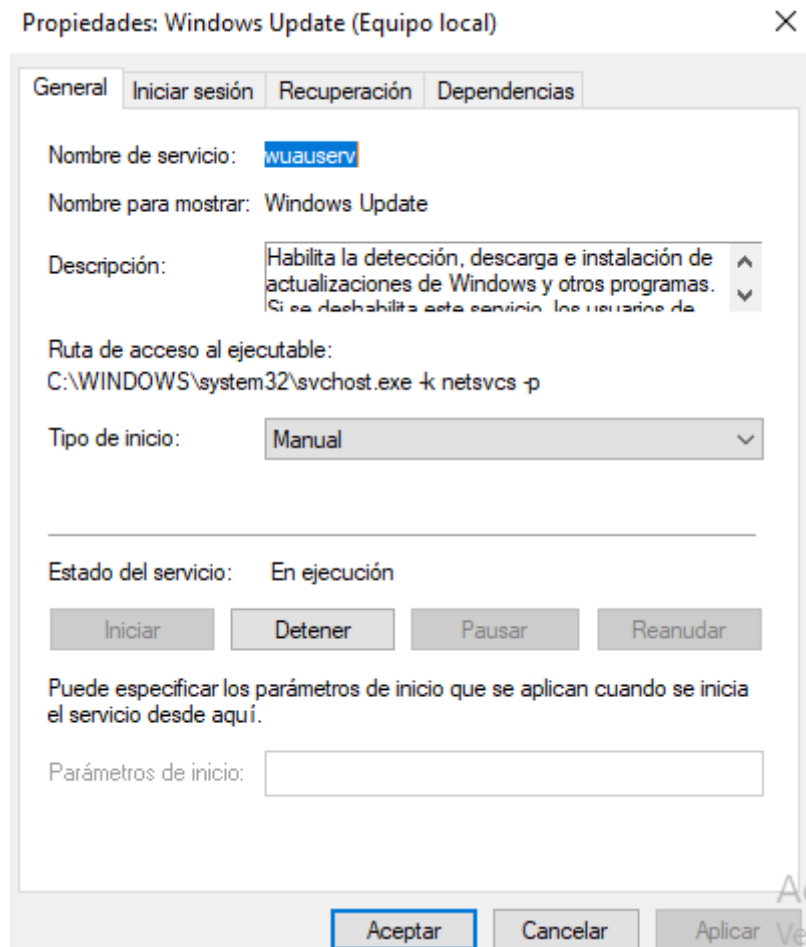
A screenshot of a Windows command prompt window. The command 'net stop wuauserv' has been entered and executed. The output shows that the service is stopping and has stopped successfully. A watermark 'Activar Windows' is visible in the background.

```
C:\WINDOWS\system32>net stop wuauserv
El servicio de Windows Update está deteniéndose.
El servicio de Windows Update se detuvo correctamente.
```



4.2.3 Vuelve a lanzar el servicio. ¿Sucede algo?

```
C:\WINDOWS\system32>net start wuau servicing
El servicio de Windows Update está iniciándose.
El servicio de Windows Update se ha iniciado correctamente.
```



4.2.4 ¿Cuál es el ejecutable que se lanza cuando se invoca el servicio?

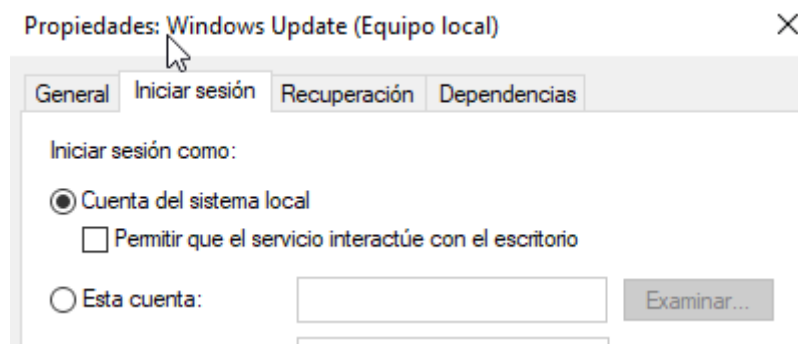
Ruta de acceso al ejecutable:
C:\WINDOWS\system32\svchost.exe -k netsvcs -p

4.2.5 Consulta la información de la descripción del servicio.

Nombre para mostrar: Windows Update

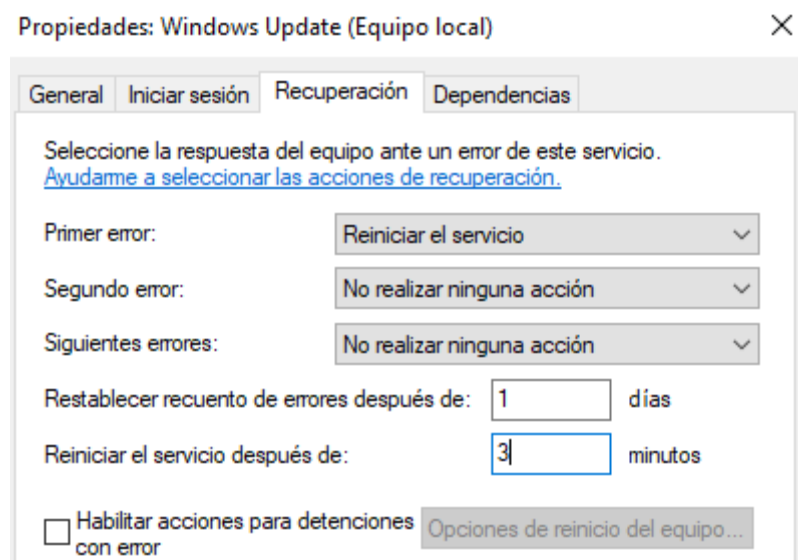
Descripción: Habilita la detección, descarga e instalación de actualizaciones de Windows y otros programas. Si se deshabilita este servicio, los usuarios de...

4.2.6 ¿Cómo y con qué cuenta de usuario se inicia el servicio?

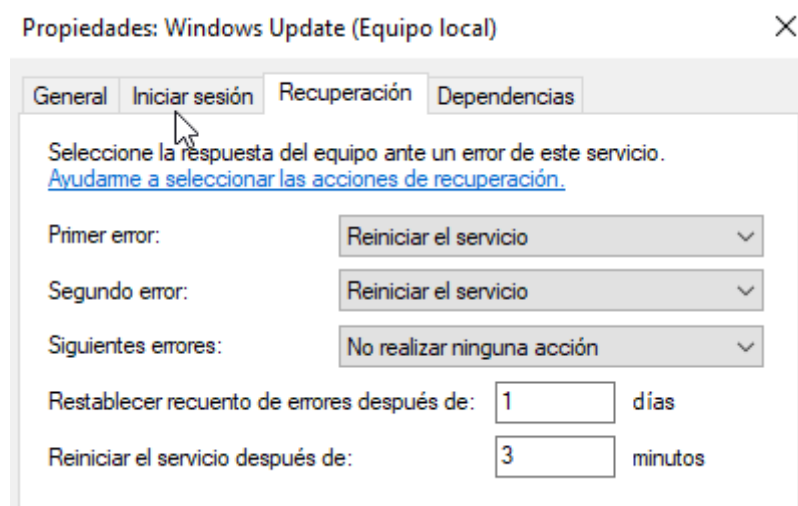


4.2.7 Configúralo para que realice las siguientes tareas en caso de error:

- Primer error: Reiniciar el servicio en 3 minutos.



- Segundo error: Reiniciar el servicio en 3 minutos.



- Siguietes errores: Reiniciar el equipo en 5 minutos.

Propiedades: Windows Update (Equipo local) X

General Iniciar sesión **Recuperación** Dependencias

Seleccione la respuesta del equipo ante un error de este servicio.
[Ayúdame a seleccionar las acciones de recuperación.](#)

Primer error: Reiniciar el servicio v

Segundo error: Reiniciar el servicio v

Siguientes errores: Reiniciar el equipo v

Restablecer recuento de errores después de: 1 días

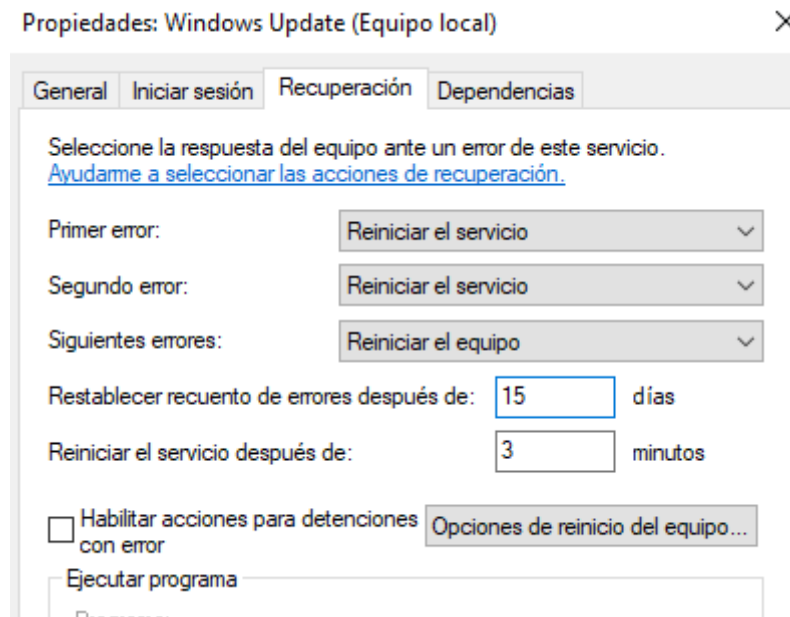
Reiniciar el servicio después de: 3 minutos

Opciones de reinicio del equipo X

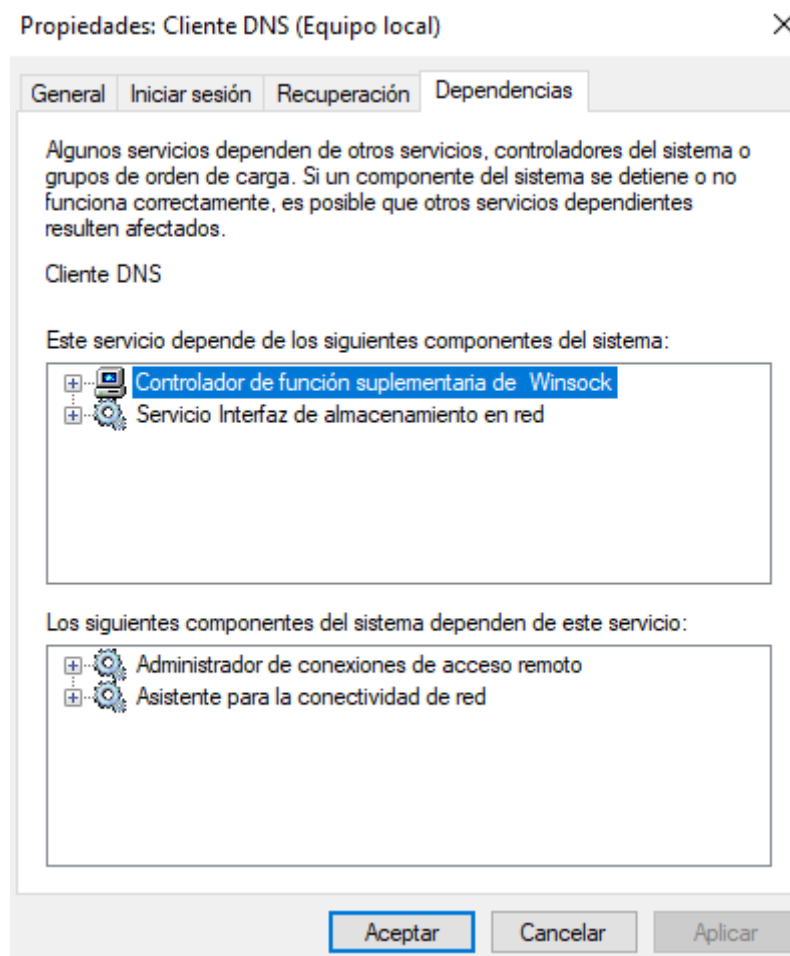
Reiniciar el equipo después de: 5 minutos

☐ Antes de reiniciar el equipo, enviar este mensaje a equipos en la red:

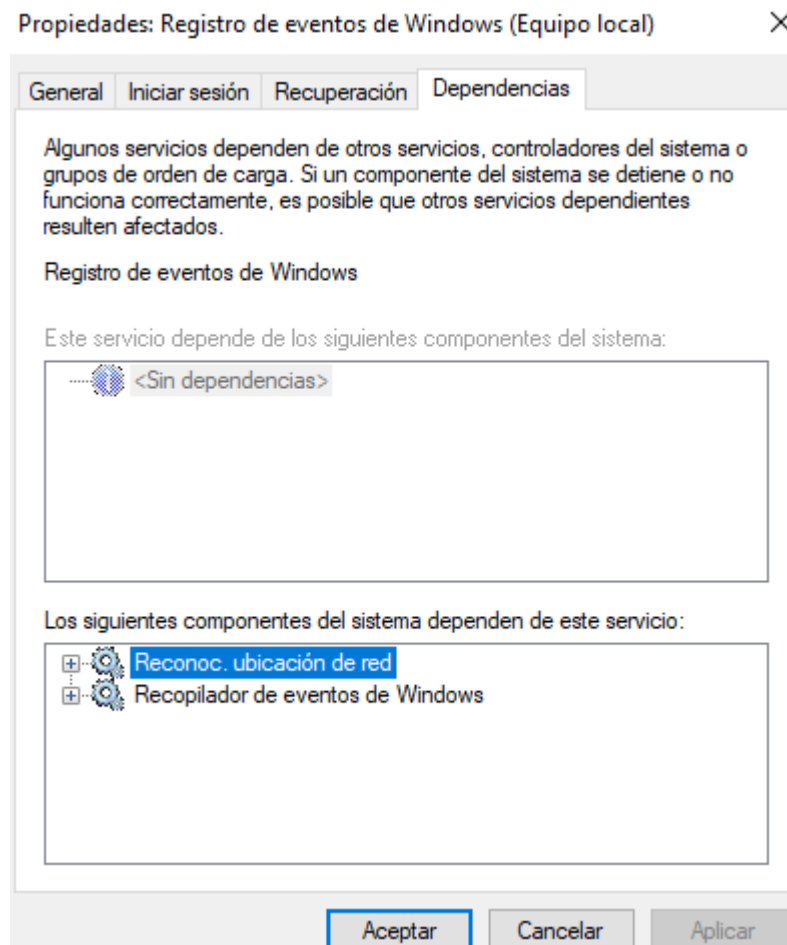
4.2.8 Restablece que el recuento de errores se realice después de 15 días.



4.3 ¿De qué servicios o componentes depende el servicio Cliente DNS?



4.4 ¿Qué componentes o servicios dependen del servicio Registro de eventos?



4.5 Sobre el equipo de clase busca el servicio Virtualbox System e indica los comandos necesarios para parar el servicio y para iniciarlo. Comprueba también si se puede pausar y reiniciar.

```
C:\Windows\system32>net stop VBoxSDS
El servicio de VirtualBox system service está deteniéndose.
El servicio de VirtualBox system service se detuvo correctamente.

C:\Windows\system32>net start VBoxSDS
El servicio de VirtualBox system service está iniciándose.
El servicio de VirtualBox system service se ha iniciado correctamente.

C:\Windows\system32>net pause VBoxSDS
La interrupción, continuación o detención solicitada no es válida para este servicio.

Puede obtener más ayuda con el comando NET HELPMSG 2191.
```

Ejercicio 5. Sucesos

5.1 Desde el Visor de eventos ¿cómo podemos obtener una descripción más detallada de un suceso que ha ocurrido en el sistema y que está registrado en un registro de los mencionados antes?

The screenshot shows the Windows Event Viewer interface. On the left, the 'Visor de eventos (local)' tree is expanded to 'Registros de Windows' > 'Sistema'. The main pane displays a list of system events. The selected event is an error from 'Service Control Manager' with ID 7000, occurring on 21/02/2023 at 20:35:35. The right pane shows the 'Acciones' menu with options like 'Abrir registro guardado...', 'Crear vista personalizada...', and 'Ver'. Below the list, a detailed view of the selected event is shown, including the error message and metadata.

Nivel	Fecha y hora	Origen	Id. del ...	Categoría de la tarea
Error	09/02/2023 16:57:31	Service Control Manager	7000	Ninguno
Error	21/02/2023 20:35:35	Service Control Manager	7000	Ninguno
Error	26/02/2023 19:52:59	Service Control Manager	7000	Ninguno
Error	30/01/2023 19:18:56	Service Control Manager	7000	Ninguno
Error	30/01/2023 19:17:59	Service Control Manager	7023	Ninguno
Error	21/02/2023 20:36:41	WindowsUpdateClient	20	Agente de Windows ...
Error	22/02/2023 20:52:27	WindowsUpdateClient	20	Agente de Windows ...
Error	22/02/2023 20:51:21	WindowsUpdateClient	20	Agente de Windows ...
Advertencia	26/02/2023 19:55:00	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 19:43:42	DNS Client Events	1014	(1014)
Advertencia	26/02/2023 19:53:09	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 19:53:06	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 19:53:04	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 19:55:00	DistributedCOM	10016	Ninguno
Advertencia	30/01/2023 19:19:30	DistributedCOM	10016	Ninguno
Advertencia	21/02/2023 20:36:40	DistributedCOM	10016	Ninguno
Advertencia	09/02/2023 16:57:50	DistributedCOM	10016	Ninguno
Advertencia	21/02/2023 20:37:36	DistributedCOM	10016	Ninguno
Advertencia	21/02/2023 20:37:36	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 5:28:16	Time-Service	52	Ninguno
Advertencia	22/02/2023 20:51:18	Time-Service	52	Ninguno
Advertencia	30/01/2023 19:20:41	Bits-Client	16385	Ninguno
Advertencia	26/02/2023 19:37:45	Time-Service	52	Ninguno
Advertencia	30/01/2023 19:59:56	DistributedCOM	10016	Ninguno
Advertencia	26/02/2023 19:55:00	DistributedCOM	10016	Ninguno

Evento 7000, Service Control Manager

General Detalles

El servicio VBoxService no pudo iniciarse debido al siguiente error:
El archivo o directorio está dañado o es ilegible.

Nombre de registro: Sistema

Origen: Service Control Manager Registrado: 21/02/2023 20:35:35

Id. del: 7000 Categoría de tarea: Ninguno

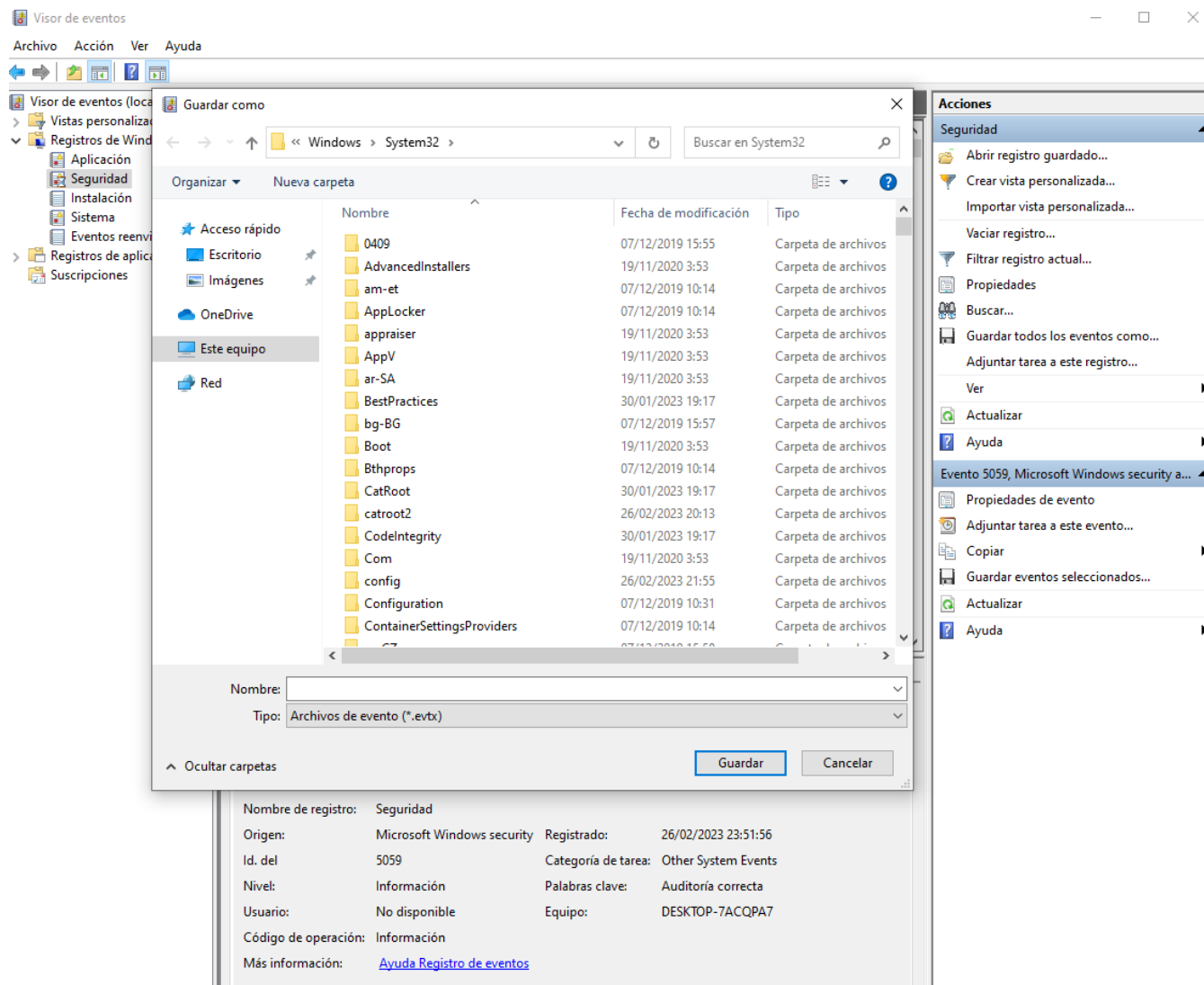
Nivel: Error Palabras clave: Clásico

Usuario: No disponible Equipo: DESKTOP-7ACQPA7

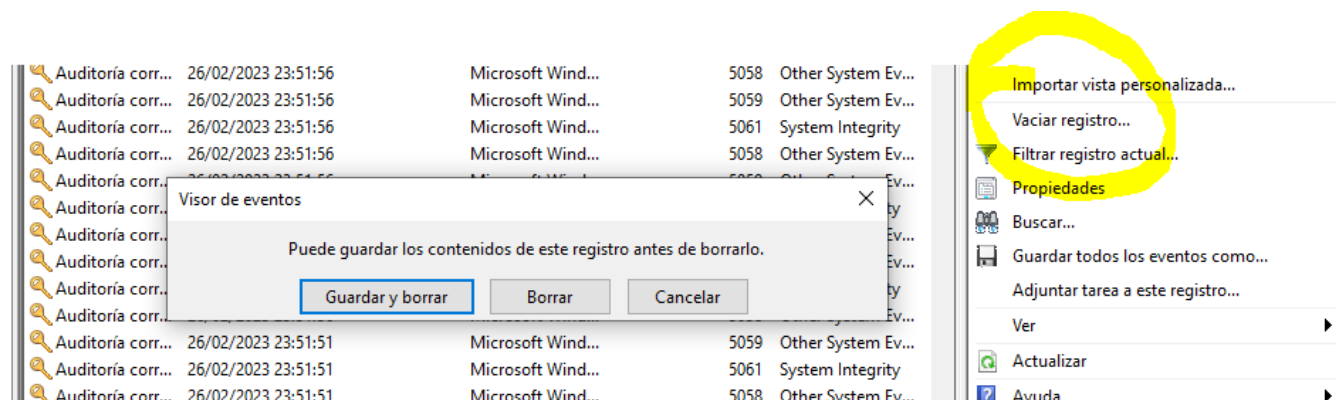
Código de operación: Información

Más información: [Ayuda Registro de eventos](#)

5.2 Guarda los sucesos del registro de seguridad en un archivo de tipo registro de sucesos.



5.3 ¿Cómo borrarías todos los sucesos de un registro? (No lo hagas, para que el siguiente grupo pueda hacer este ejercicio).



5.4 Del registro de sucesos Sistema obtén los siguientes datos:

5.4.1 Fichero donde se almacenan estos sucesos.

Propiedades del registro: Sistema (Tipo: Administrativo) ✕

General **Suscripciones**

Nombre completo: System

Ruta del registro: %SystemRoot%\System32\Winevt\Logs\System.evtx

Tamaño del registro: 1,07 MB(1.118.208 bytes)

5.4.2 Tamaño actual del fichero.

Tamaño del registro: 1,07 MB(1.118.208 bytes)

5.4.3 Tamaño máximo.

Tamaño máx. del registro (KB): 20480

Cuando alcance el tamaño máx. del reg. de eventos:

5.4.4 Fecha de la última modificación.

Modificado: domingo, 26 de febrero de 2023 22:33:11

5.5 De nuevo para ese registro de sucesos:

5.5.1 Amplia el tamaño máximo del fichero a 40 MB.

Tamaño máx. del registro (KB): 40960

Cuando alcance el tamaño máx. del reg. de eventos:

5.5.2 Fija que se sobrescriban los sucesos o eventos cuando sea necesario.

Tamaño máx. del registro (KB): 40960

Cuando alcance el tamaño máx. del reg. de eventos:

- ☒ Sobrescribir eventos si es necesario (los anteriores primero)
- ☐ Archivar el registro cuando esté lleno; no sobrescribir eventos
- ☐ No sobrescribir eventos (vaciar registros manualmente)

5.5.3 Establece que los sucesos de tipo Información no se guarden.

No disponible para W10

5.6 Abre el registro guardado en el ejercicio 5.2, y comprueba la información que se almacenó.

