

TAREA ISO08

Actividad 1

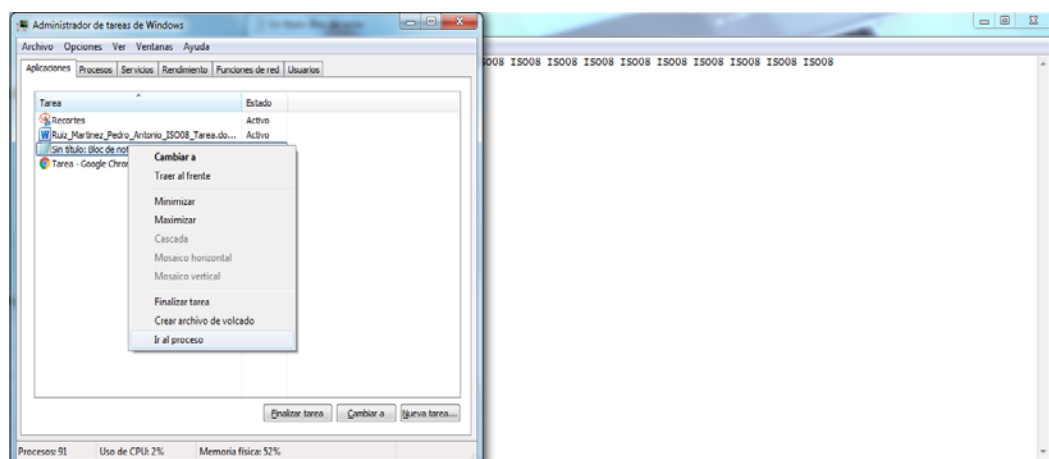
1.- Abrir bloc de notas. Localizar proceso asociado y finalizar su árbol.

Para abrir el bloc de notas nos dirigimos a "Inicio>Todos los programas>Accesorios>Bloc de notas".

Para comenzar iniciamos el "Administrador de tareas de Windows" pulsando la combinación de teclas "Alt+Ctrl+Supr", nos aparecerá una pantalla en la que entre otras opciones nos aparece "Administrador de tareas" y la seleccionamos. También podemos iniciarlo haciendo click con el botón derecho de ratón en una zona libre de la barra de tareas y seleccionando la opción "Iniciar el Administrador de tareas" y también ejecutando la combinación de teclas "Ctrl+Mayúsculas+Esc".

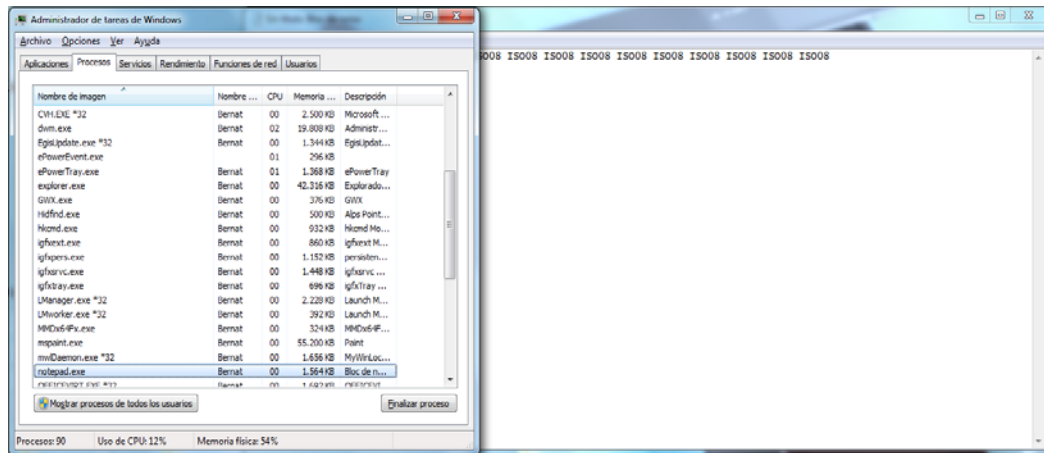
Ahora procedemos a abrir el bloc de notas. Para ello nos dirigimos a "Inicio>Todos los programas>Accesorios>Bloc de notas".

Ya iniciado el bloc de notas podemos observar en el "Administrador de tareas" que en la pestaña "Aplicaciones" se encuentra el "Bloc de notas" con estado activo.



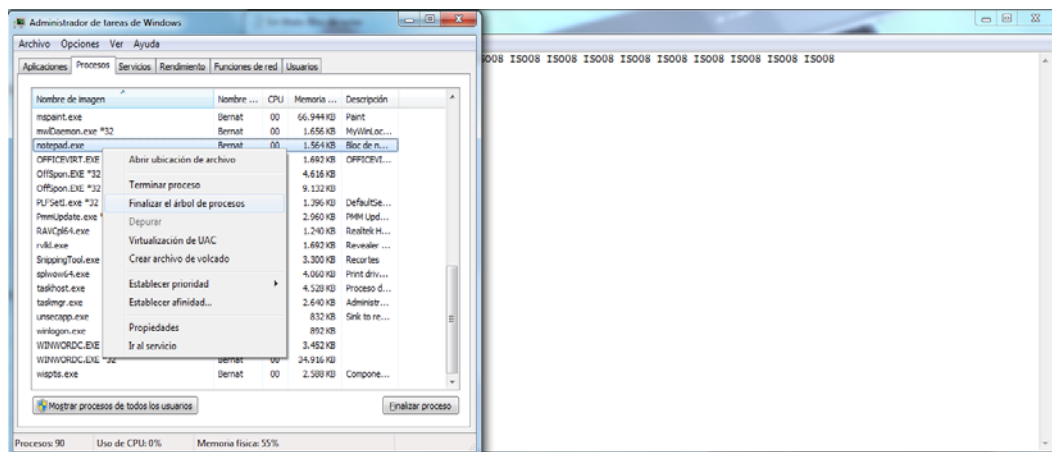
Ahora situándonos en la aplicación activa y pulsando el botón derecho del ratón nos aparecen una serie de opciones, entre

ellas la opción “Ir al proceso” que si la seleccionamos nos llevara directamente al proceso relacionado con el “Bloc de notas”.

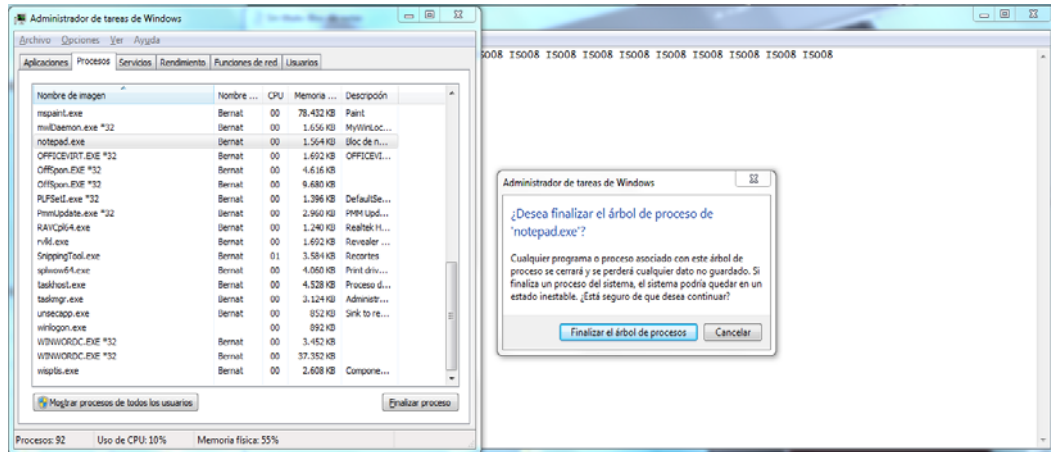


En la imagen anterior podemos observar que una vez elegida la opción “Ir al proceso” el “Administrador de tareas” nos ha cambiado a la pestaña proceso y aparece sombreado el proceso asociado al “Bloc de notas” que es el proceso denominado “notepad.exe”.

Para finalizar el árbol del proceso volvemos a pulsar el botón derecho del ratón y seleccionamos la opción “Finalizar el árbol de procesos”.



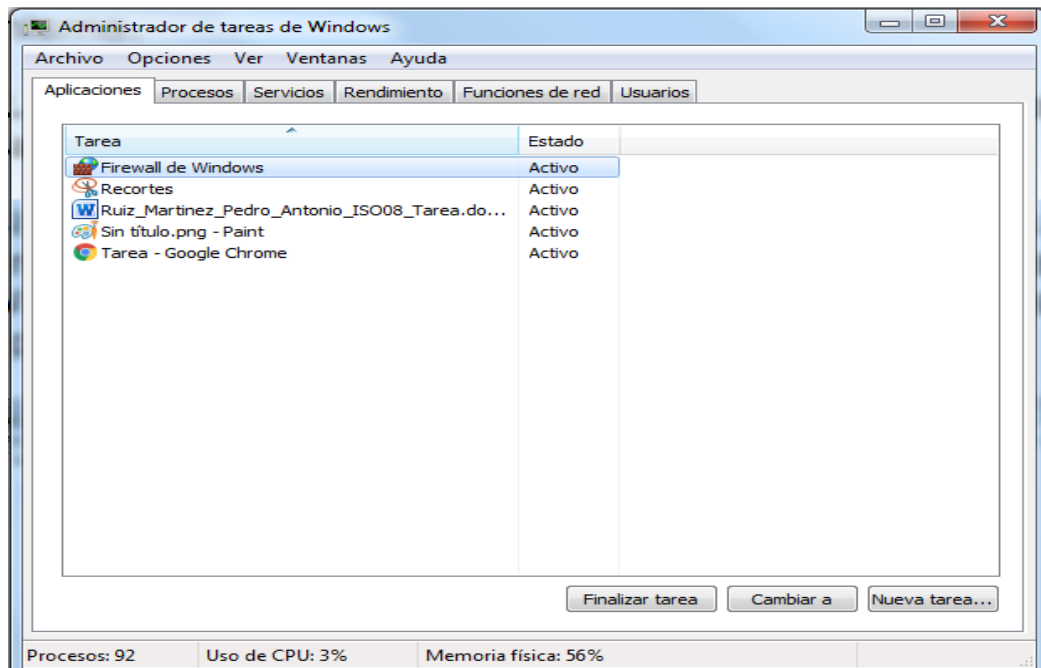
Una vez seleccionada la opción nos aparece un mensaje de advertencia y confirmación de finalización del árbol de procesos.



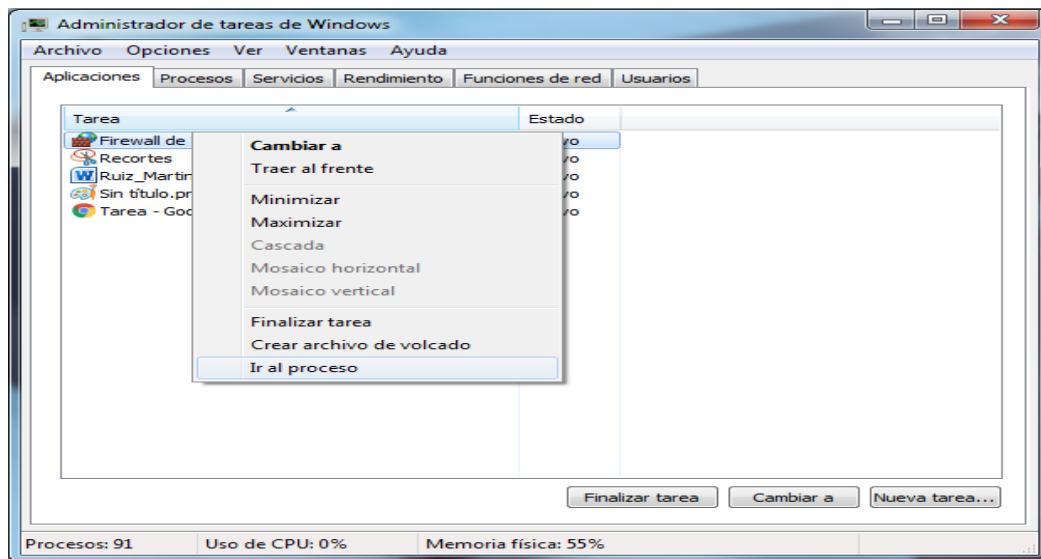
Al confirmar el cierre del árbol de procesos se cierran todos los procesos relacionados con la aplicación y la aplicación en sí misma.

2. Localizar el servicio de Firewall de Windows, comentar campos y detenerlo.

Si no tenemos activado el Firewall de Windows lo ejecutamos en "Inicio>Panel de Control>Sistema y Seguridad> Firewall de Windows". Una vez ejecutado lo encontraremos en la pestaña aplicaciones del "Administrador de Tareas".

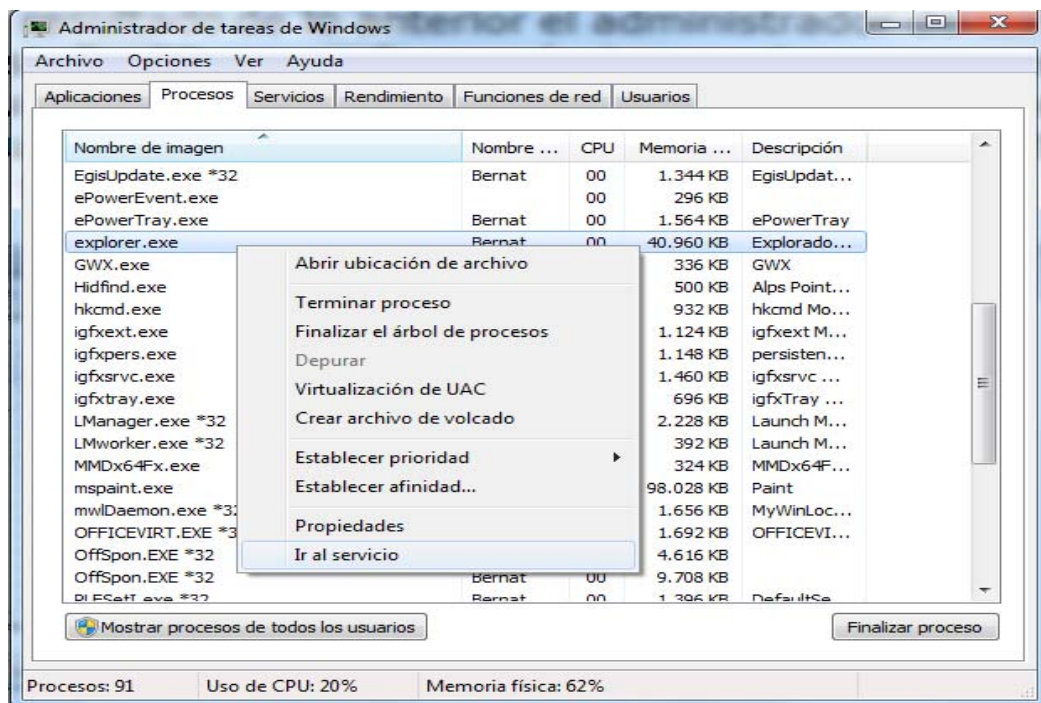


Ahora pulsamos el botón derecho del ratón y en el menú que aparece seleccionamos la opción "Ir al proceso".

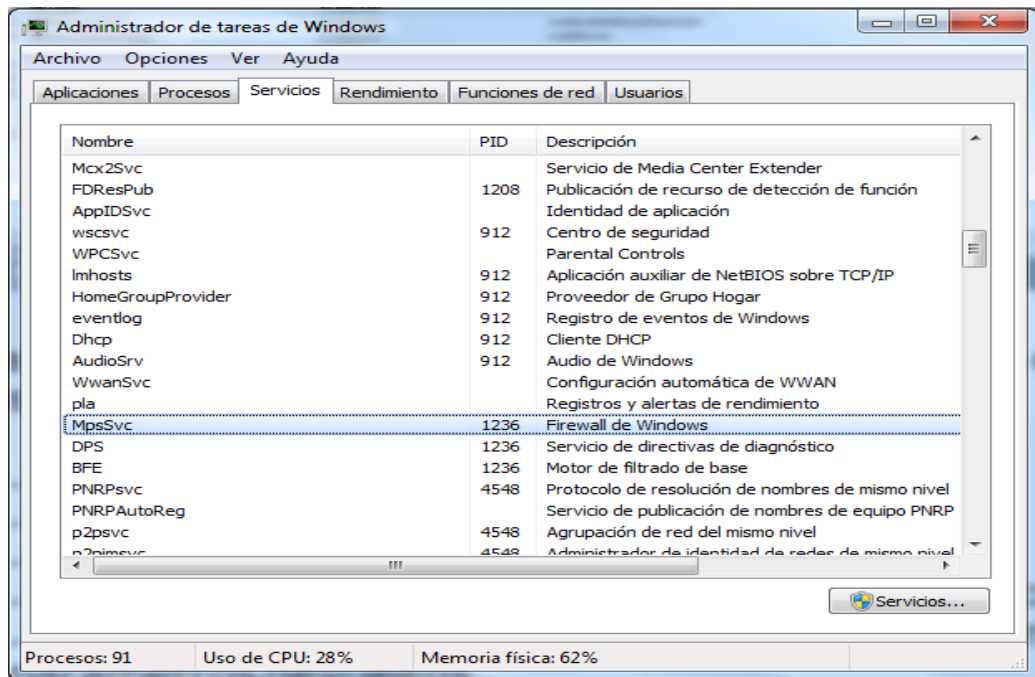


Como resultado de lo anterior el administrador de tareas pasa a la pestaña "Procesos" marcándonos el proceso asociado al "Firewall de Windows" que es en este caso "explorer.exe".

El siguiente paso es pulsar el botón derecho del ratón y en el menú seleccionar la opción "Ir al servicio".



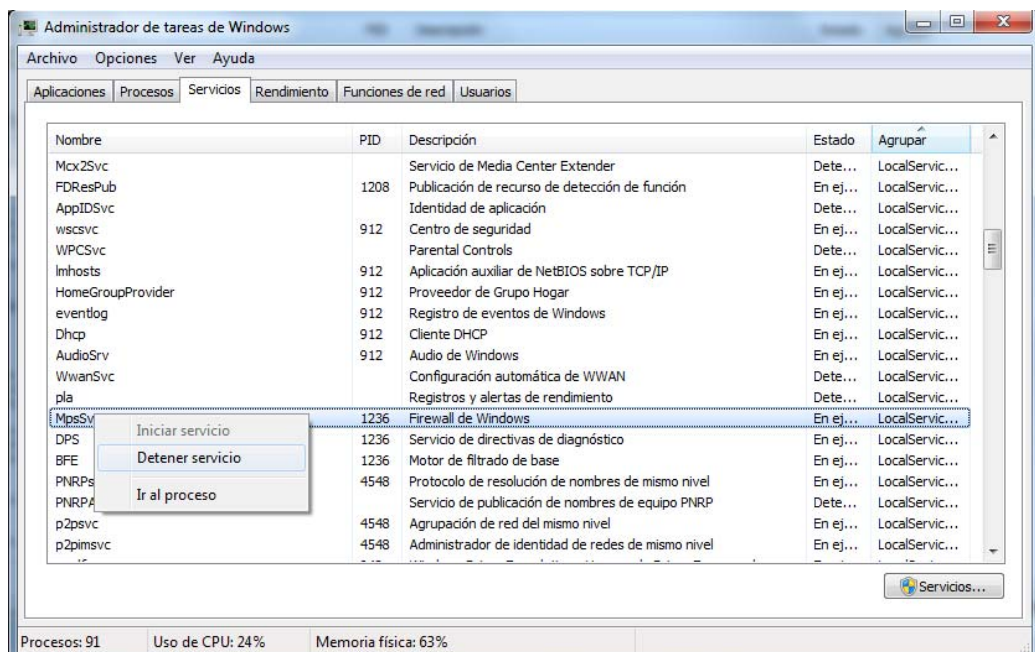
Cuando lo hemos realizado el "Administrador de tareas" nos cambia a la pestaña "Servicios" marcándonos el servicio correspondiente al "Firewall de Windows", en este caso es el servicio "MpsSvc".



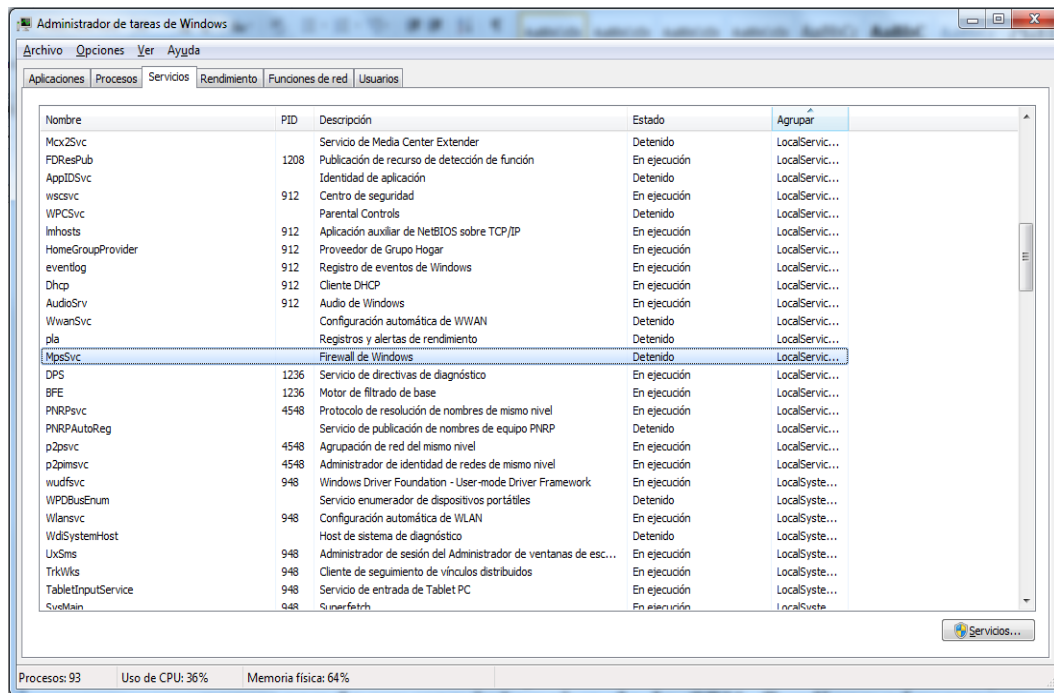
Los campos que se nos muestran en pantalla sobre el servicio son los siguientes:

- Nombre del servicio.
- PID: Identificador del Proceso
- Descripción: Descripción del servicio
- Estado: Estado del servicio (Detenido, en ejecución)
- Agrupar: proporciona información sobre restricciones o parámetros devueltos.

Para detener el proceso pulsamos el botón derecho del ratón y seleccionamos en el menú la opción "Detener servicio"

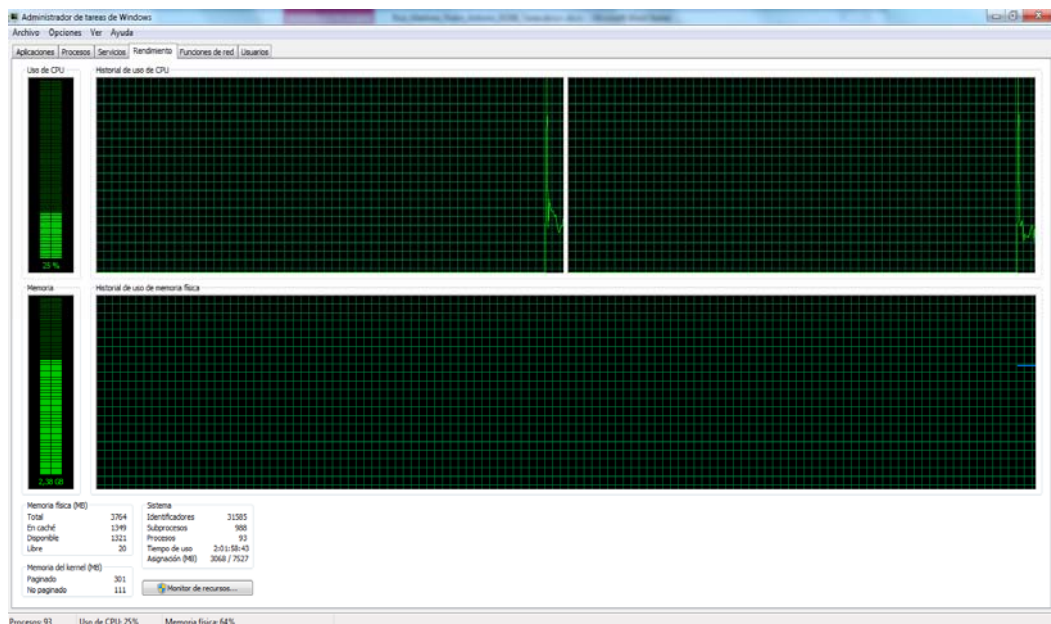


Una vez realizado esto el servicio se detiene.



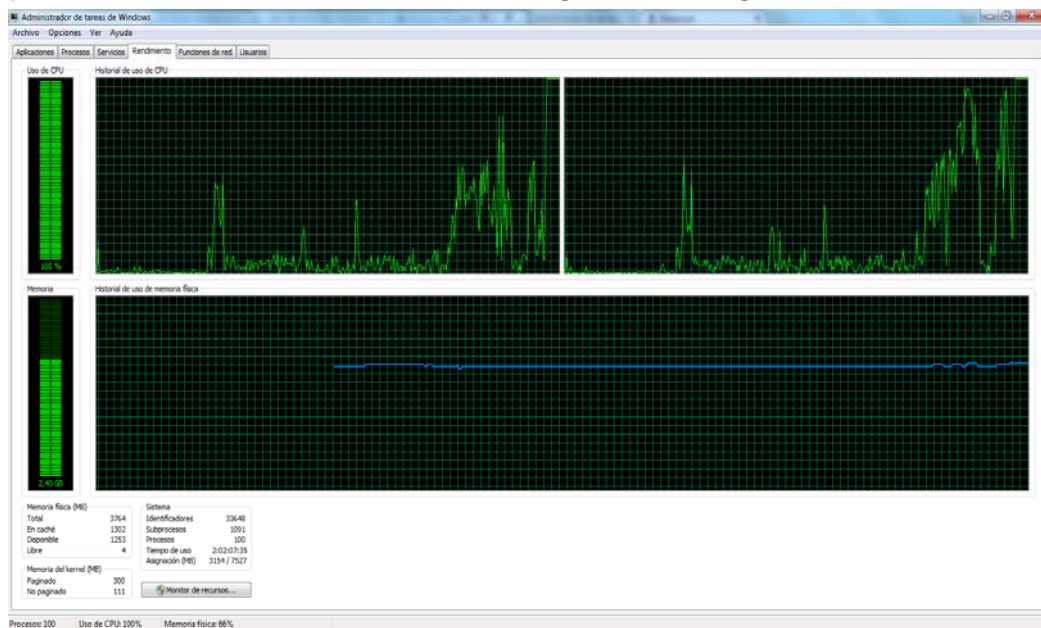
3.- Realizar captura de pantalla de graficas de rendimiento de CPU y memoria en estado normal y provocando un uso intensivo de la CPU. Explicar cómo se consigue.

En la imagen siguiente se puede observar el grafico del uso de la CPU y de la memoria en estado normal. Estos gráficos se presentan cuando nos situamos en la pestaña rendimiento del "Administrador de Tareas".



En la siguiente imagen podemos observar el grafico anterior con un uso intensivo de la CPU. Se puede comprobar que en este caso el uso de la CPU llega al

100% según se nos muestra en el gráfico de la izquierda de la pantalla cuando en la anterior imagen solo llegaba al 25%.

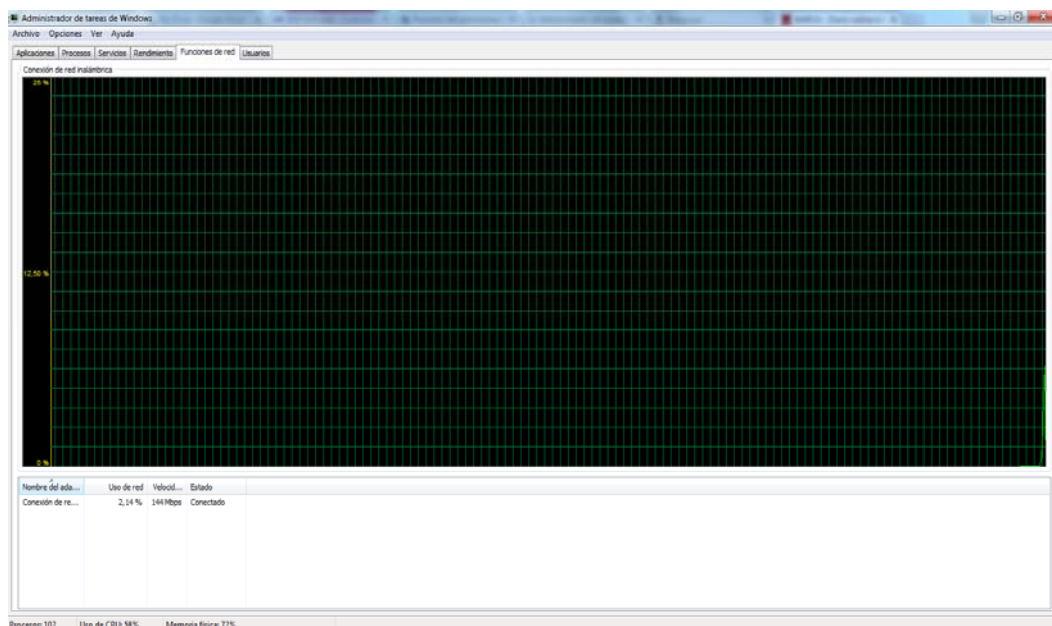


Este incremento en el uso de la CPU se ha conseguido ejecutando test de stress de cpu "HeavyLoad".

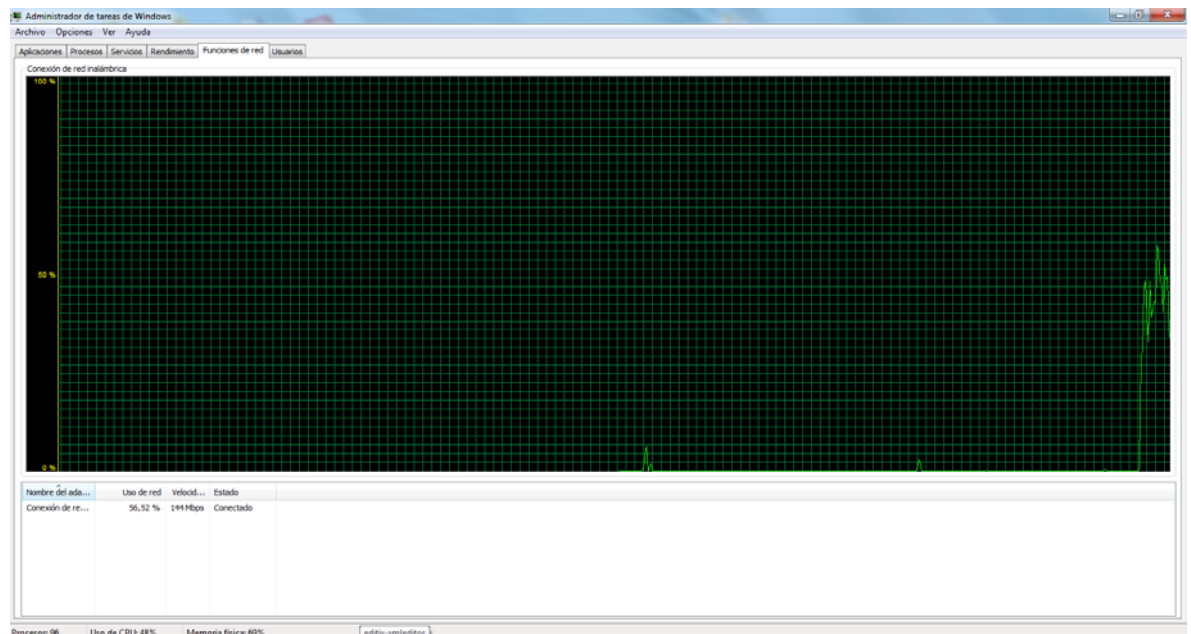
4.- Realizar captura de graficas de funciones de red en estado normal y provocando un uso intensivo de la conexión.

Situándonos en la pestaña "Uso de red" del "Administrador de Tareas" se nos mostraran los gráficos del uso de la red.

Esta imagen corresponde a un uso en estado normal cuando el ordenador está navegando por páginas de internet, se puede apreciar que el uso de la red solo llega a un 2,14%.



En la siguiente imagen podemos comprobar un uso mayor de la red que llega hasta un 56,52% aproximadamente según el pico mostrado en el gráfico. Esto se ha conseguido copiando y pegando en nuestro ordenador un archivo compartido en otro equipo que se encuentra en la misma red que nuestro ordenador.

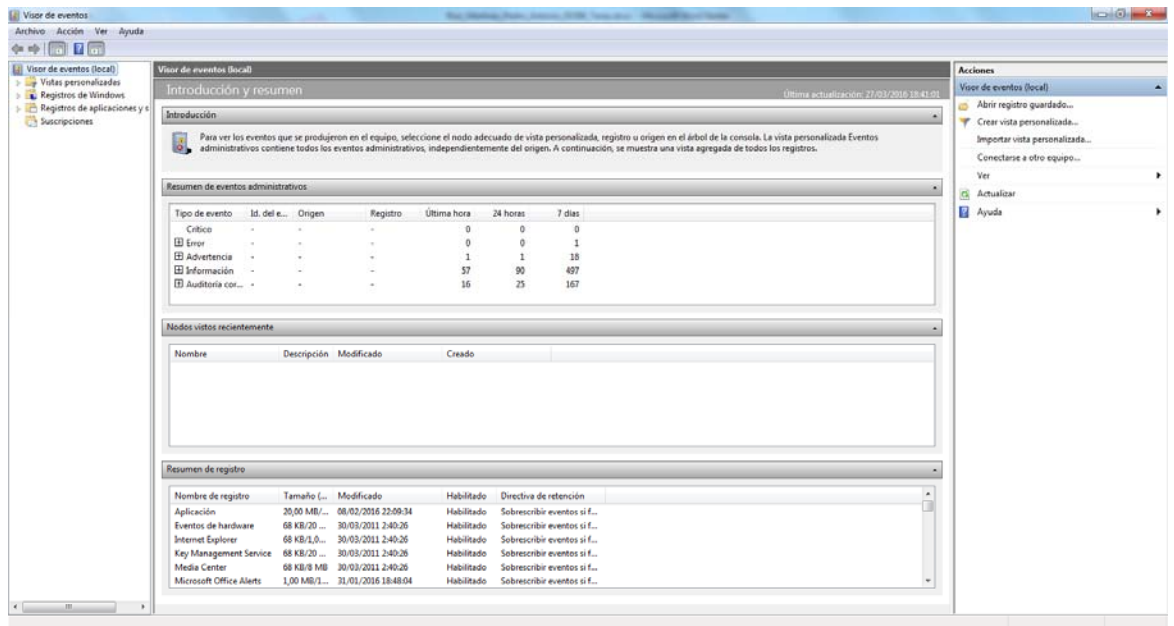


Así como en el caso del uso de la CPU se ha podido llegar a un uso del 100% en el caso del uso de la red no se ha podido pasar de este nivel de uso, pero con esto se demuestra el incremento en el uso de la red.

Actividad 2.

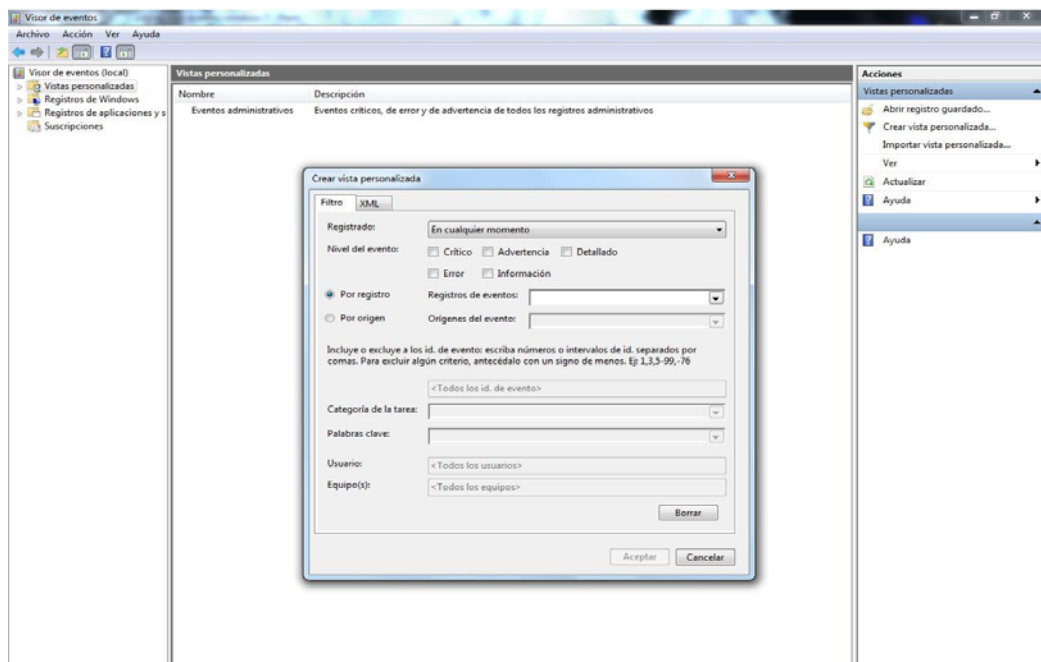
Para crear una vista personalizada en el "Visor de eventos de Windows" primero accederemos a dicho visor, para ello nos dirigimos a "Inicio> Tecleamos en la barra de búsqueda visor de eventos" y nos aparece el icono para ejecutar dicho visor o también podemos acceder desde "Inicio>Panel de control> Sistema y seguridad>Herramientas administrativas".

El aspecto del visor de eventos es el siguiente

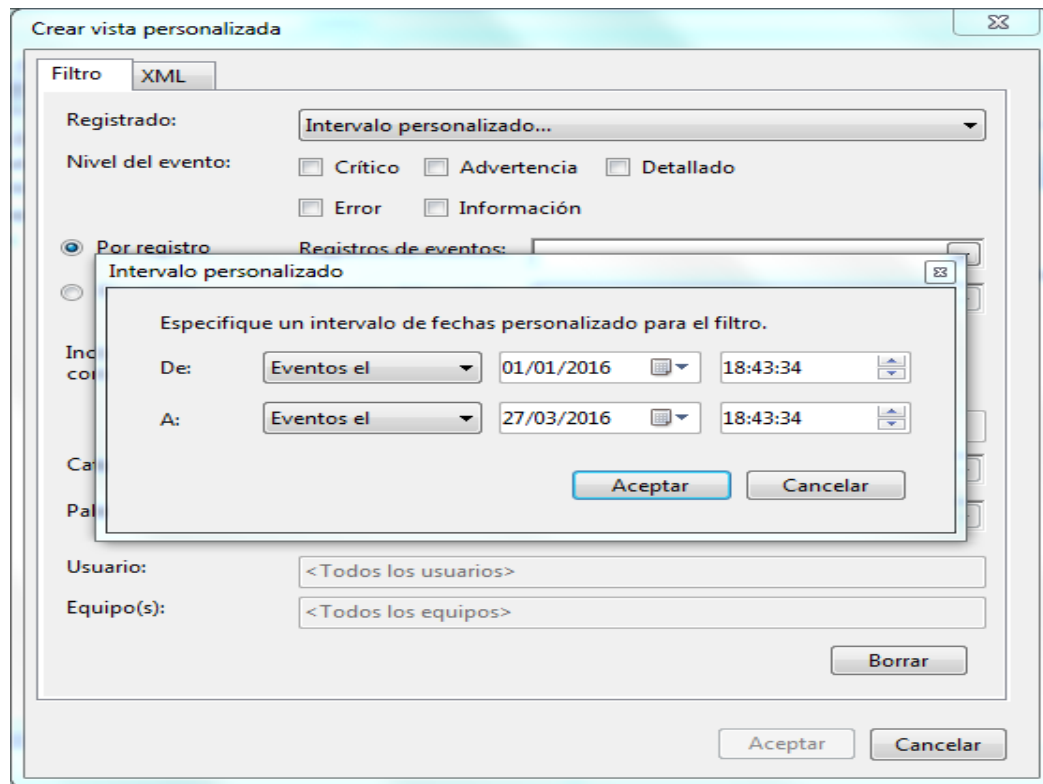


Una vez dentro del visor nos dirigimos a la parte derecha de la pantalla a la opción "Crear vista personalizada".

Al seleccionarla no aparece una ventana en la que debemos de determinar el intervalo de tiempo que queremos visualizar, el nivel de evento (Crítico, detallado, advertencia, error e información)

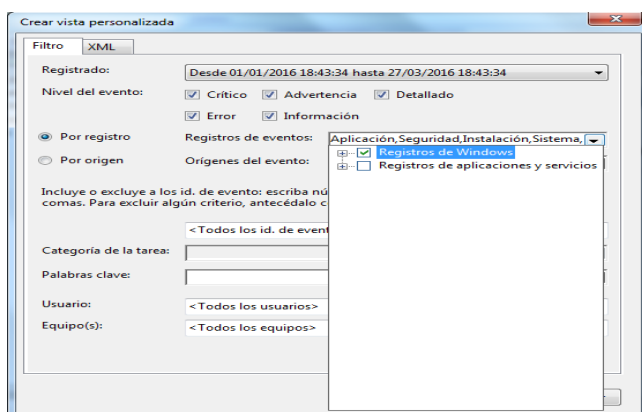


En nuestro caso seleccionaremos la opción del menú desplegable "Intervalo personalizado" y en la nueva ventana que aparece fijaremos un intervalo de tiempo desde el día 01/01 al 27/03 que fue el día en el que se realizó este ejercicio.

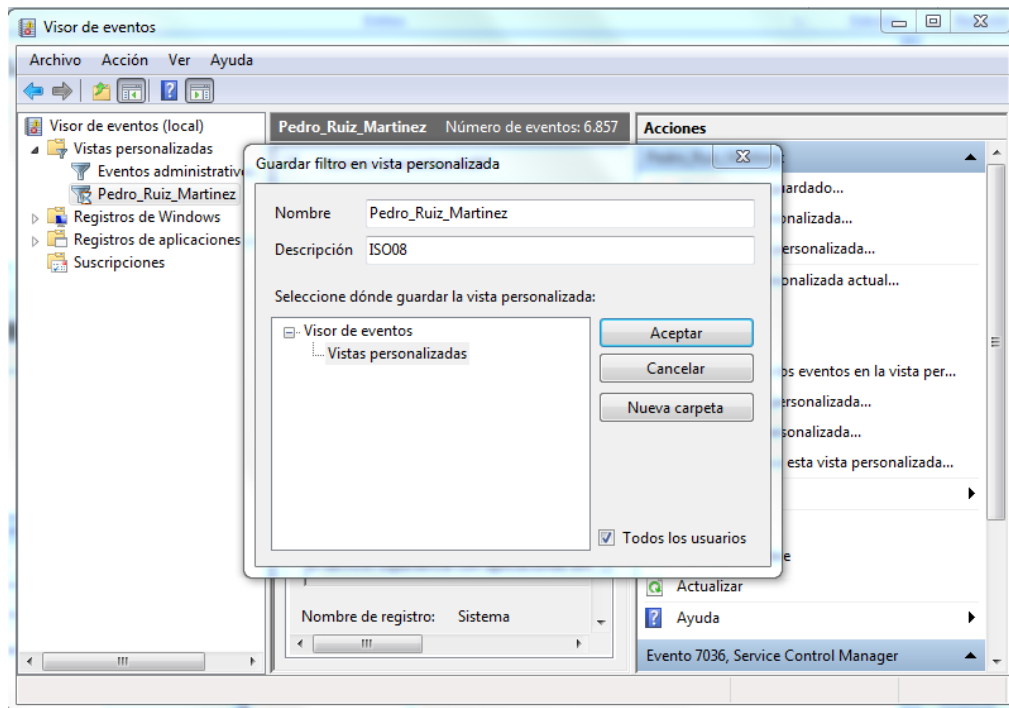


Tal y como se puede observar en la siguiente imagen también marcaremos las casillas de todos los niveles de eventos que queremos que se nos muestre, en nuestro caso marcamos todos.

Además tenemos que definir los registros a mostrar, seleccionamos "Por registro" y en el menú desplegable "Registros de windows".

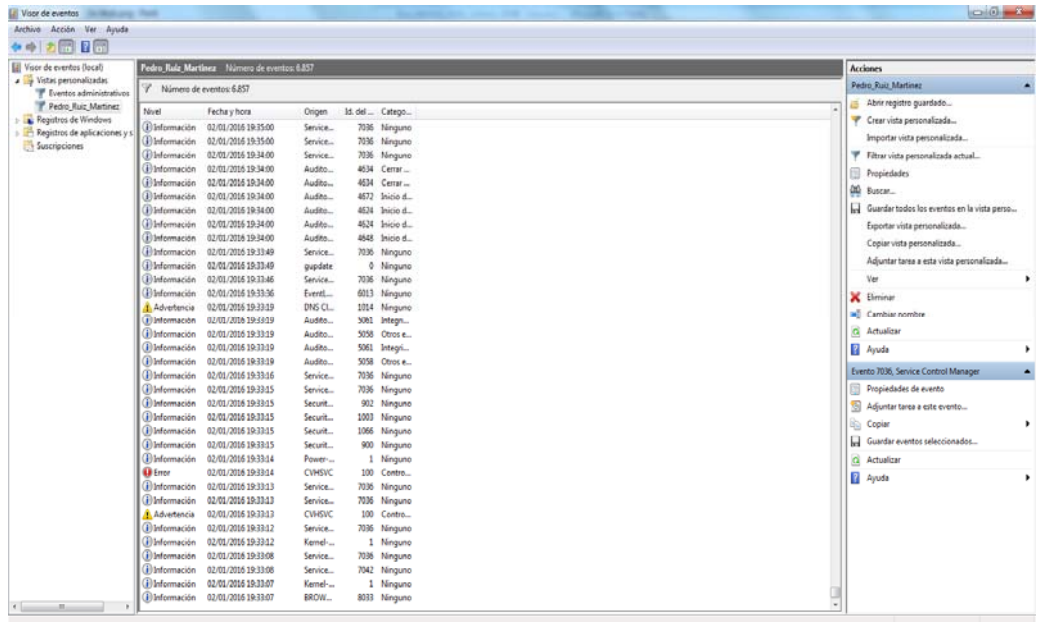
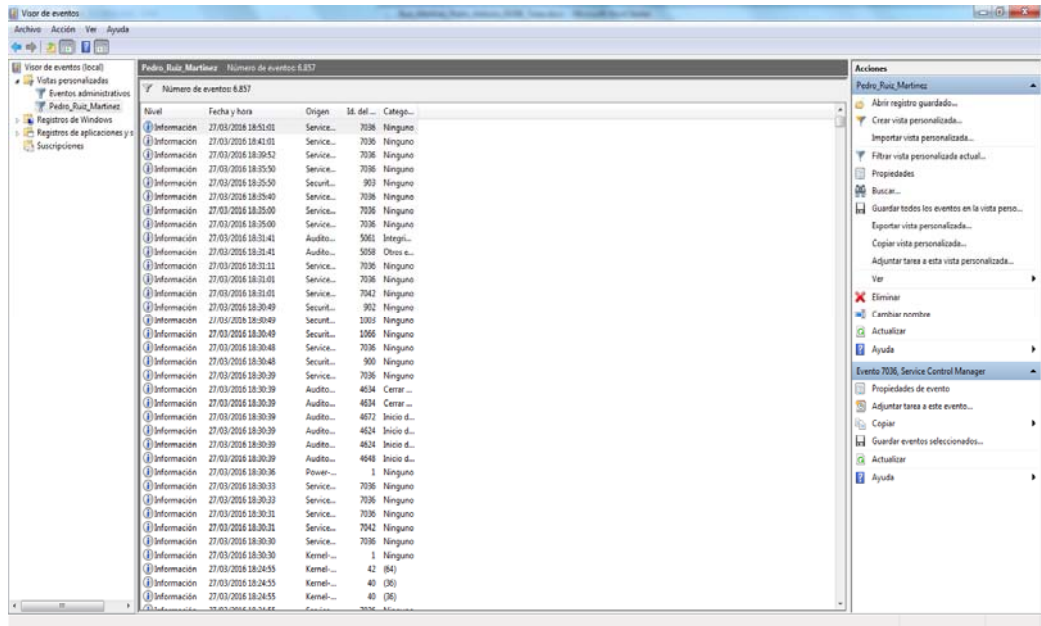


Una vez determinados los parámetros que queremos visualizar damos nombre a nuestra vista personalizada y pulsamos aceptar.

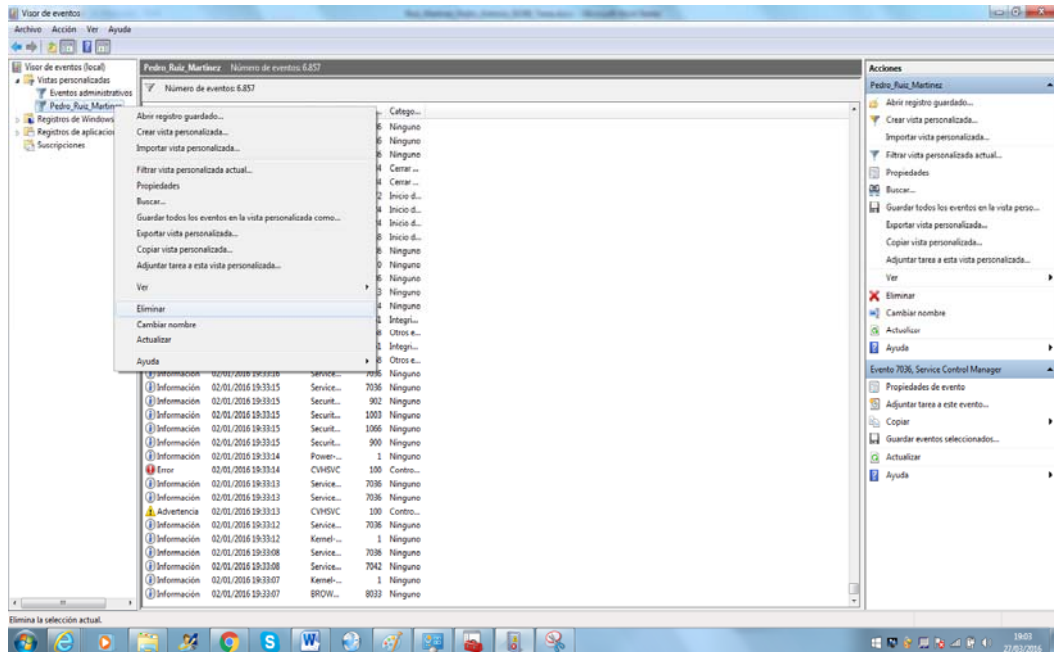


Después de realizar lo anterior tenemos nuestra vista personalizada mostrando los eventos ocurridos según hemos configurado anteriormente.

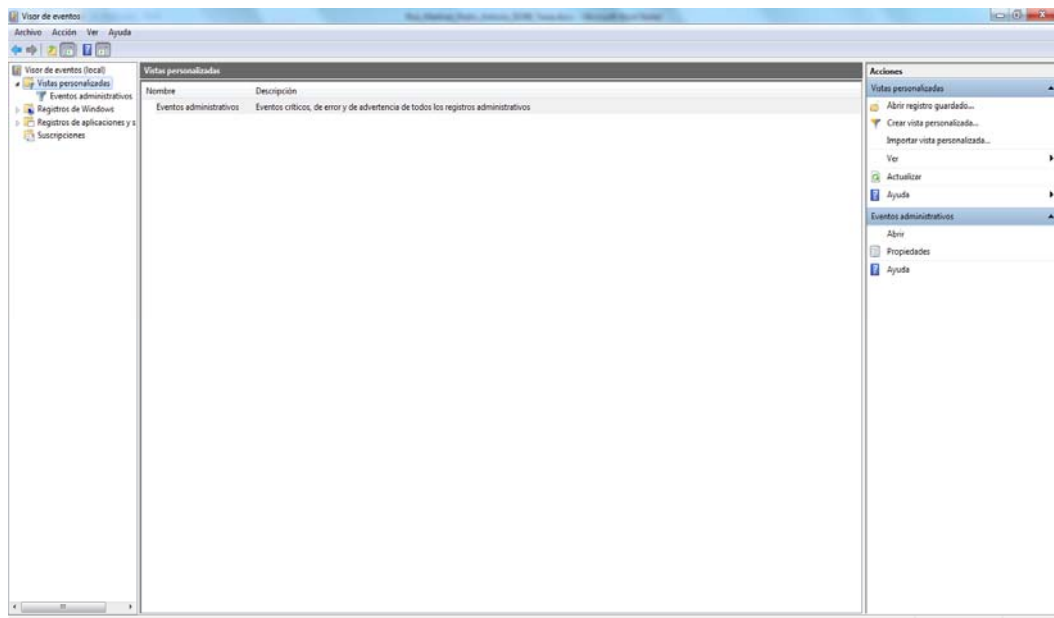
En las imágenes se puede apreciar los mensajes recibidos entre la fecha inicial y la final determinadas.



Para eliminar la vista que hemos creado nos situamos en la parte izquierda de la pantalla. Seleccionamos la vista creada "Pedro_Ruiz_Martinez" y pulsamos el botón derecho del ratón. En el menú que aparece seleccionamos la opción eliminar.

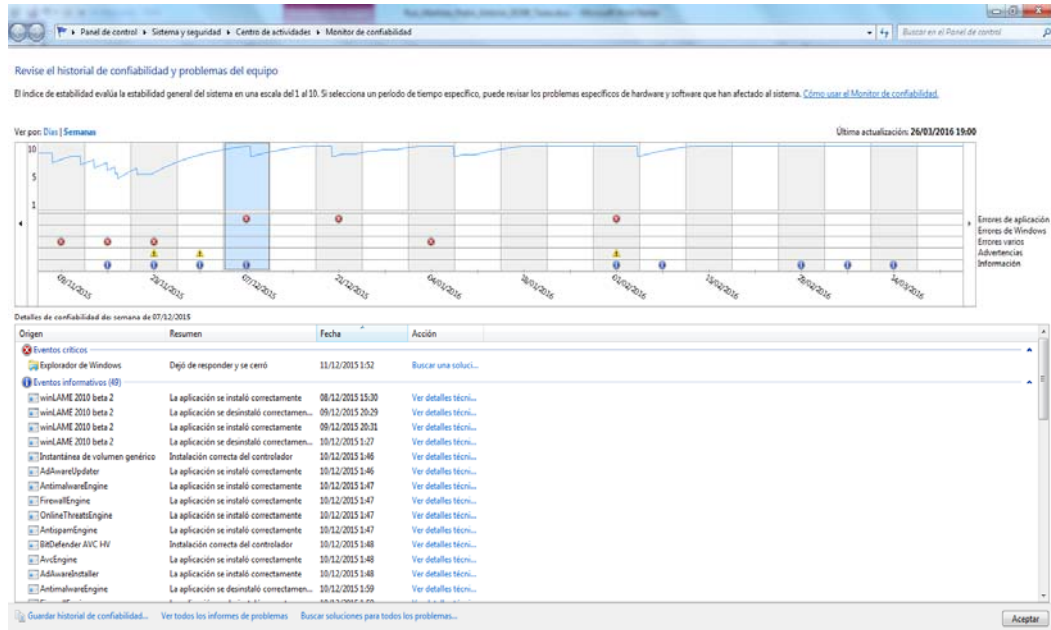


Al realizar lo anterior ya hemos eliminado la vista personalizada.



Actividad 3.

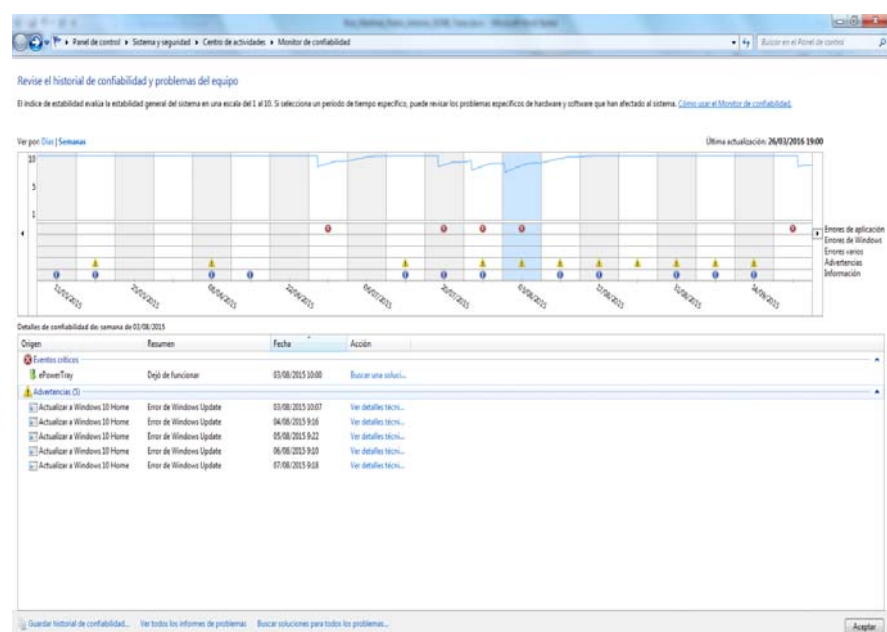
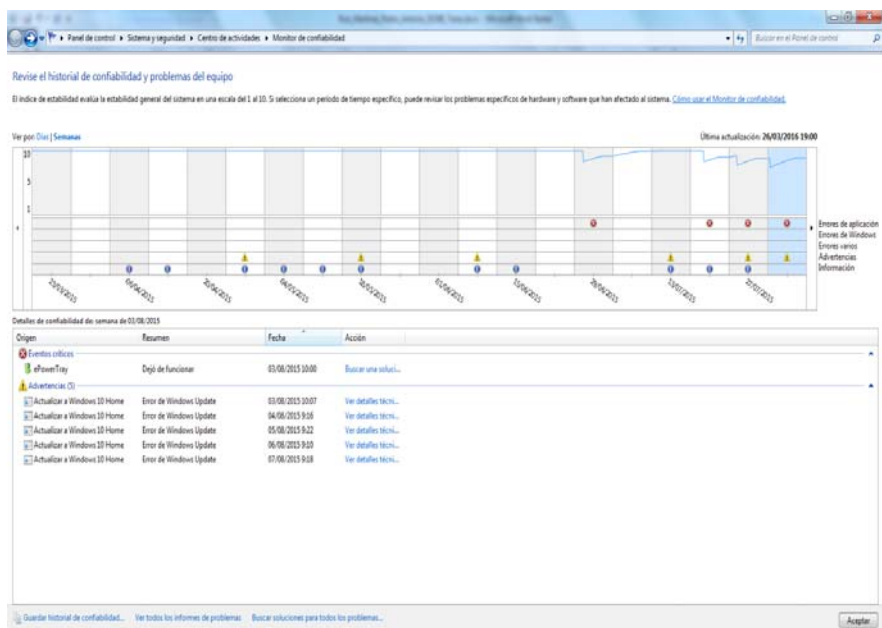
Para conocer los valores del índice de confiabilidad. Debemos de ejecutar el "Monitor de confiabilidad", se accede a él desde "Inicio>Panel de control>Sistema y seguridad>Centro de actividades". El aspecto que presenta es el siguiente:



Aproximadamente el nivel de confiabilidad máximo del equipo ha sido de 9 y el mínimo de 1 en el periodo visualizado.

La mayoría de errores encontrados en el último trimestre son por el mal cierre de aplicaciones y algún cierre inesperado del sistema, pero en líneas generales el nivel de confiabilidad es óptimo.

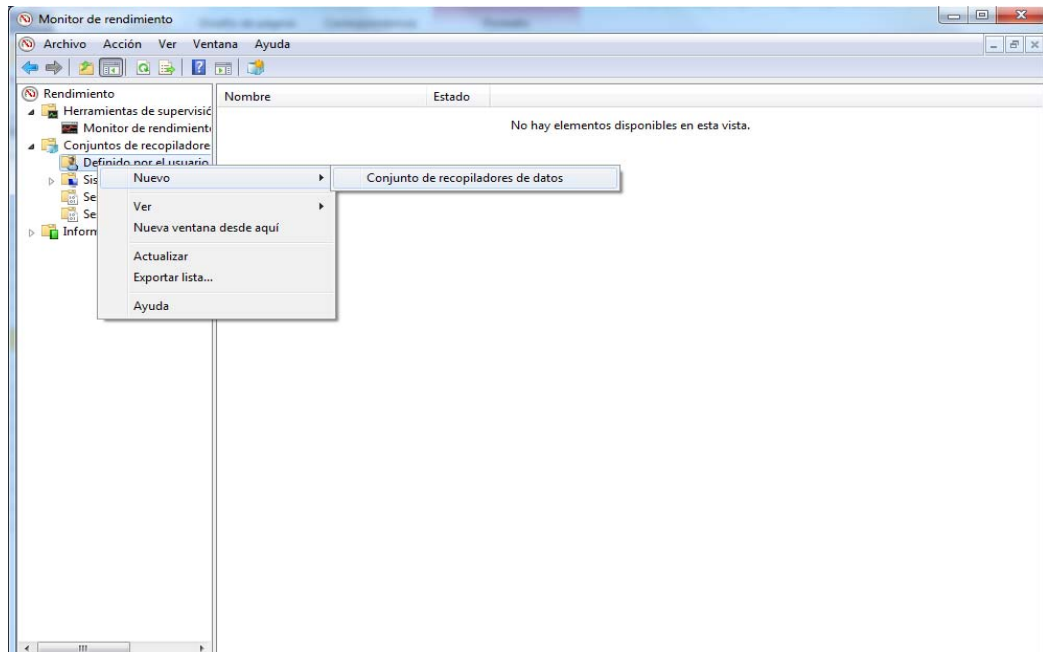
A continuación se presentan las capturas de pantalla semana por semana en la que se aprecian los fallos más importantes.



Actividad 4

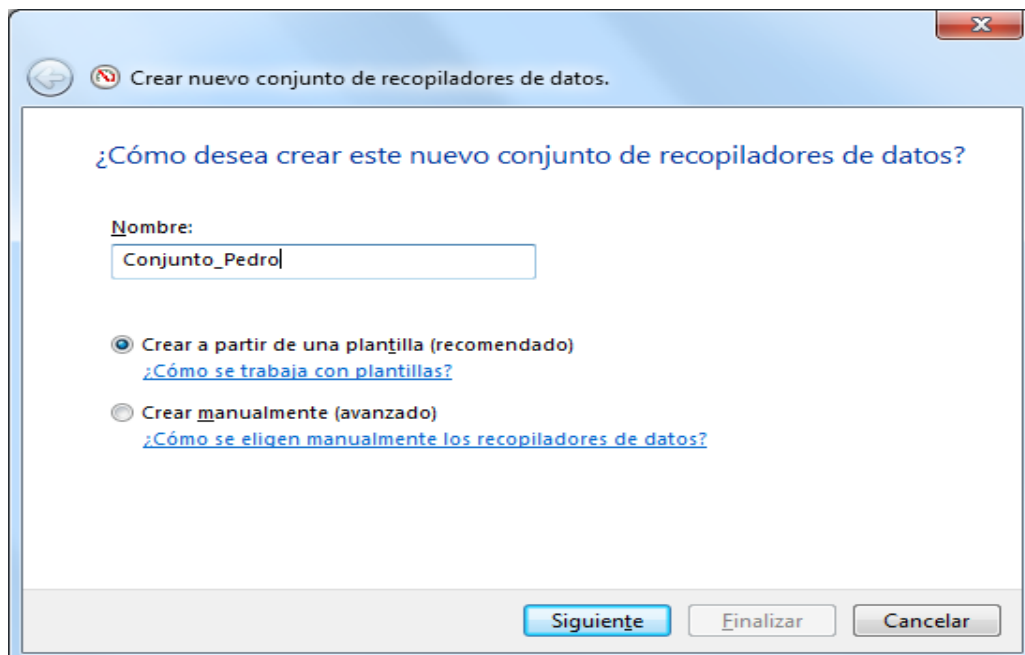
Para crear un conjunto recopilador de datos abrimos el "Monitor de rendimiento" para ello nos dirigimos a "Inicio>Panel de Control>Sistema y seguridad>Herramientas administrativas" y ejecutamos el acceso directo al monitor de rendimiento o directamente escribiendo en el terminal la orden "perfmon".

Una vez abierto nos dirigimos a la parte izquierda de la pantalla y desplegamos la opción "Conjunto de recopiladores" nos situamos en la opción "Definido por el usuario" pulsamos el botón derecho del ratón y en el menú seleccionamos la opción "nuevo" y en el nuevo menú que aparece "Conjunto de recopiladores de datos"

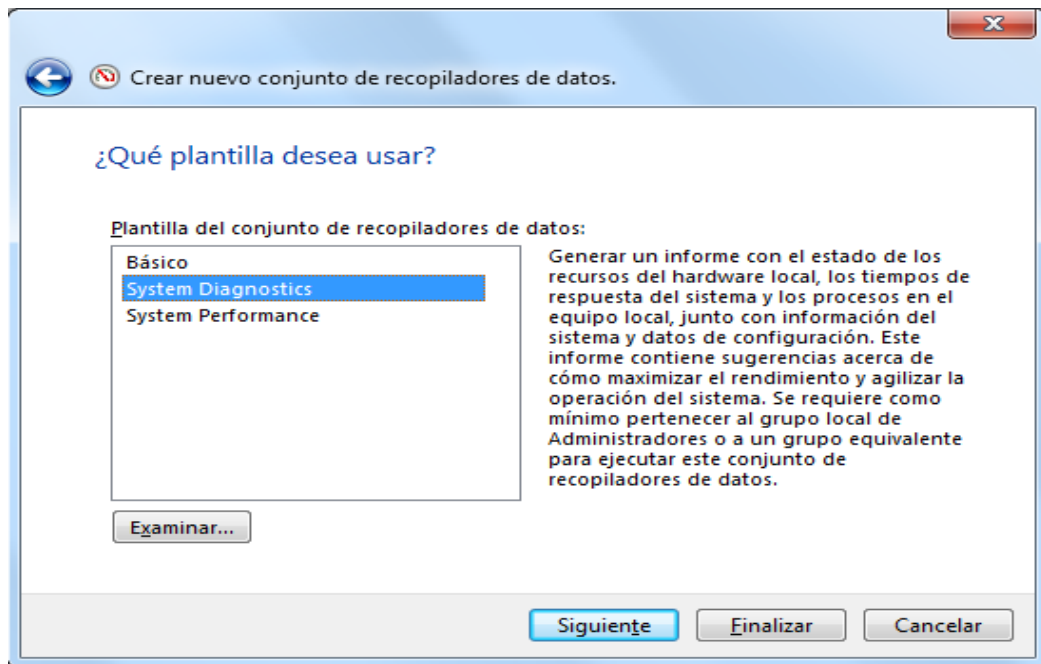


Realizado lo anterior nos aparece una nueva ventana en la que debemos de poner el nombre que le queremos dar al conjunto recopilador y la forma de crearlo, que puede ser mediante una plantilla (opción recomendada por el sistema) o de forma manual.

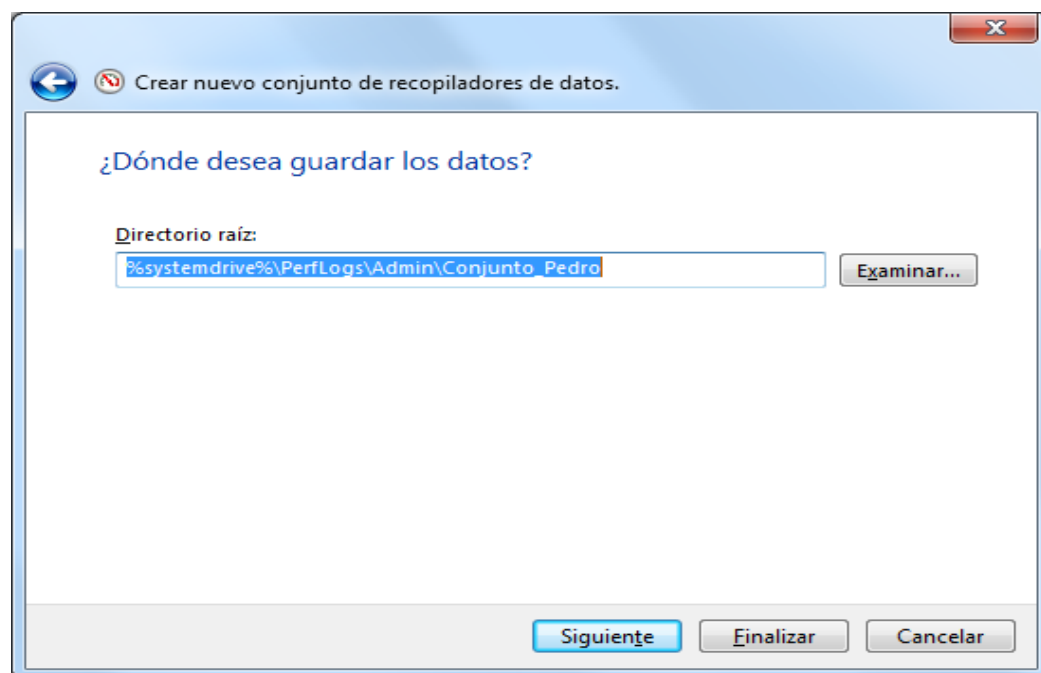
Damos el nombre "Conjunto_Pedro" y elegimos la opción crear mediante plantilla. A continuación pulsamos en siguiente.



El siguiente paso es seleccionar el tipo de plantilla que vamos a utilizar. Seleccionamos la opción "System Diagnostics", que es la que solicita el enunciado.

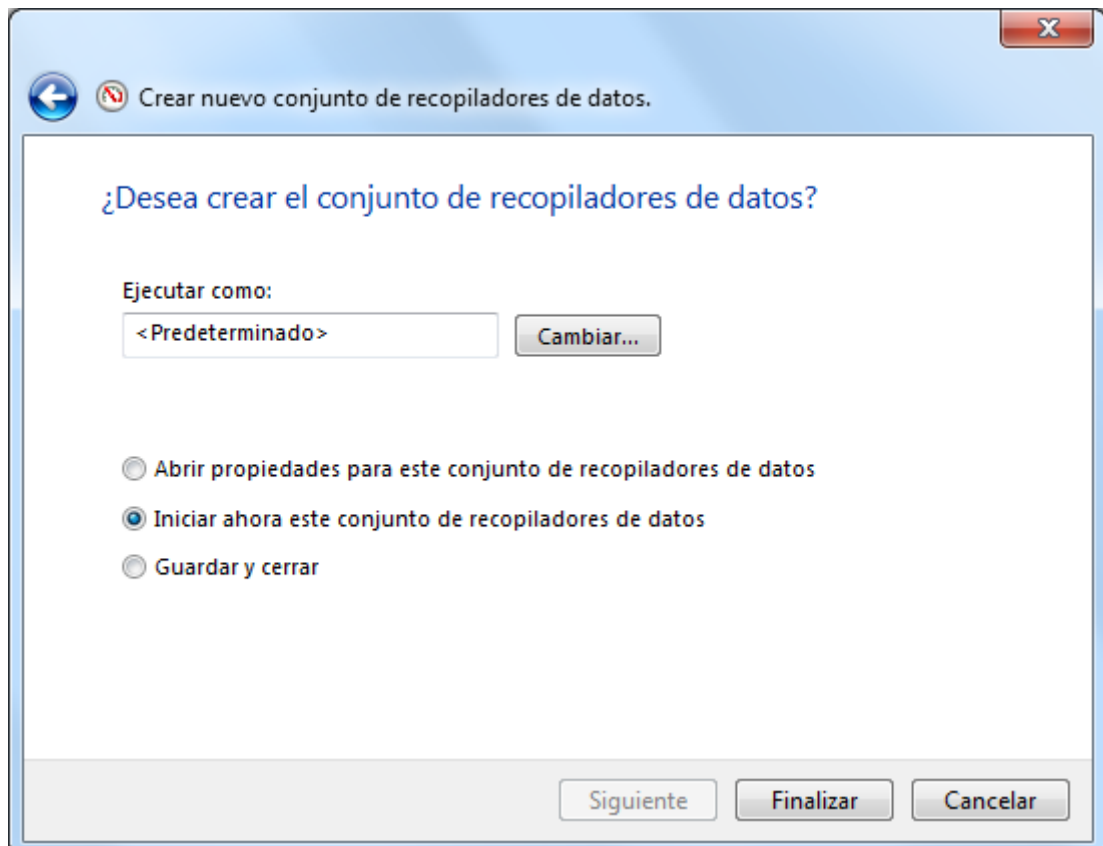


Lo siguiente es determinar la ruta donde queremos guardar los datos del recopilador.



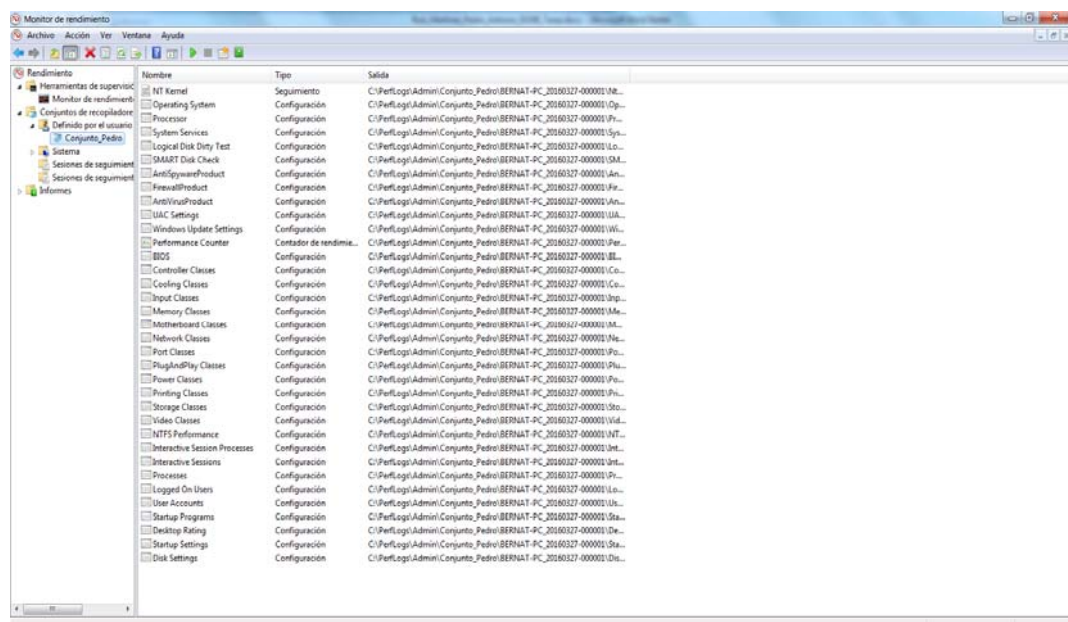
A continuación se nos solicita confirmación para crear el conjunto recopilador de datos, como se desea ejecutar y si queremos abrir las propiedades del conjunto recopilador de datos, iniciar ahora el conjunto recopilador o guardarlo y cerrarlo.

Seleccionamos las opciones "Ejecutar como: predeterminado" e "Iniciar ahora este conjunto de recopiladores de datos" y pulsamos en *finalizar*.

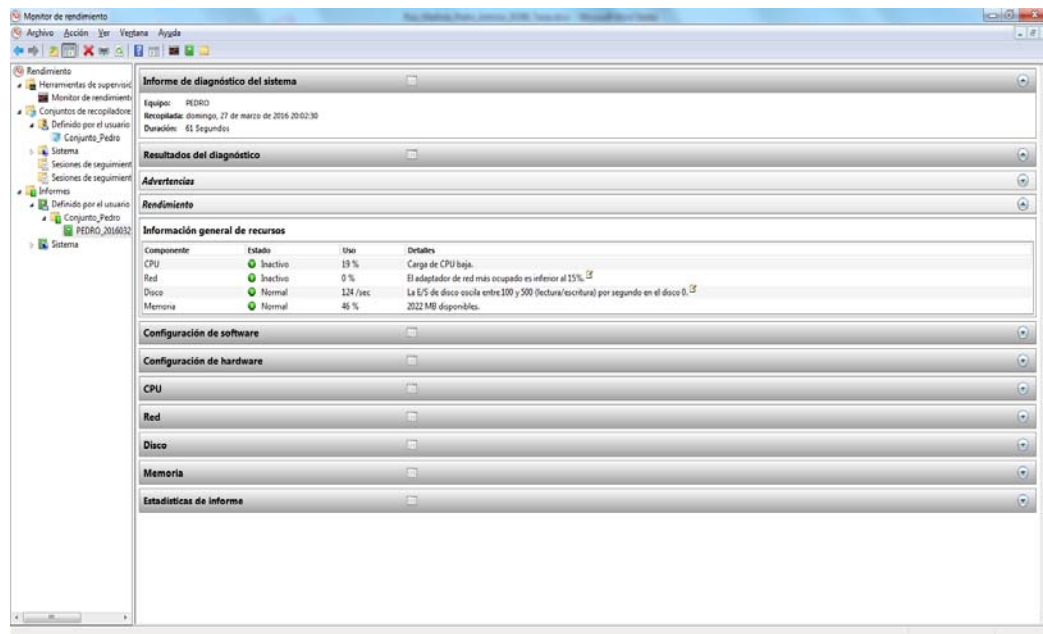


Una vez realizado lo anterior el recopilador de datos ya aparece en la parte derecha de la pantalla del Monitor de Rendimiento y pasa estar con estado "Activo", es decir comienza a recoger los datos del sistema.

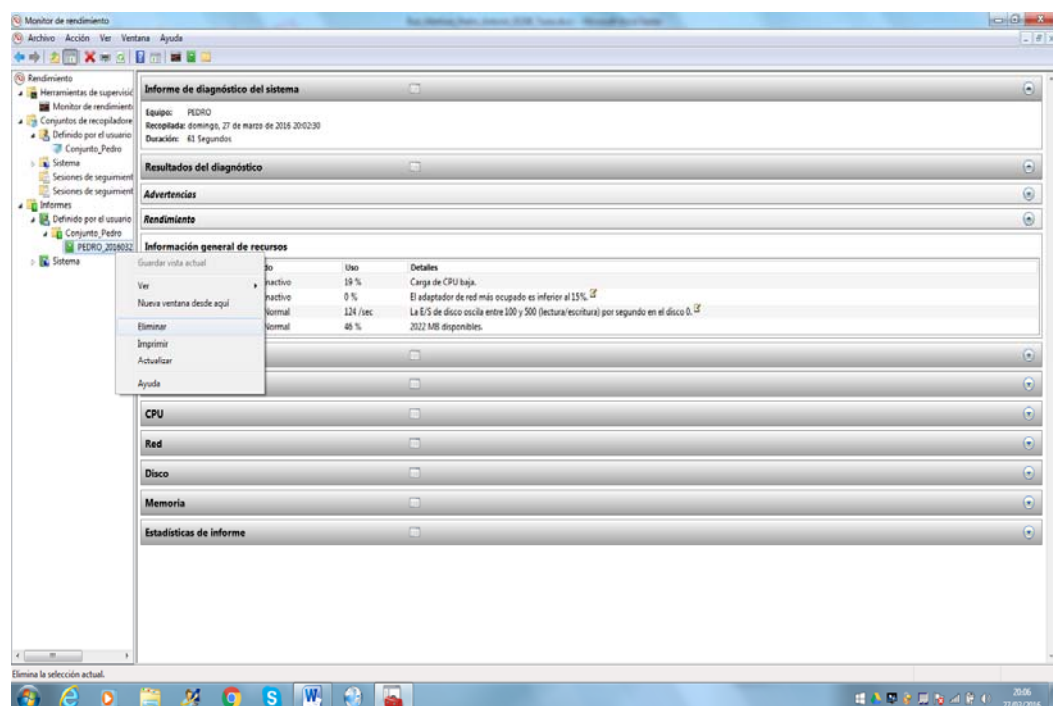
Pasados unos segundos comienza a verse en la pantalla la recogida de los datos.



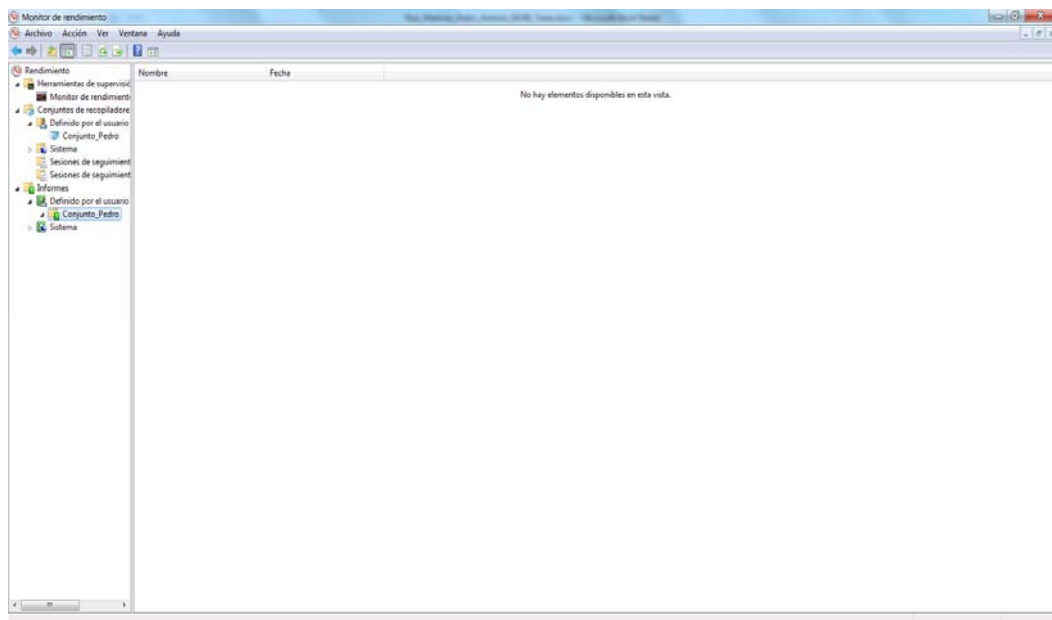
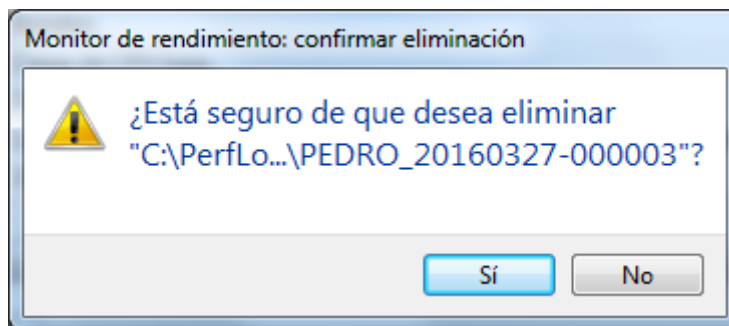
Una vez finalizada la recogida de datos se nos presenta en pantalla un informe sobre el diagnóstico del sistema. En este informe hemos desplegado el apartado rendimiento que es el solicitado en el enunciado de la actividad. En el podemos observar los componentes CPU, Red, Disco y Memoria y en cada uno de ellos su estado, uso y detalles.



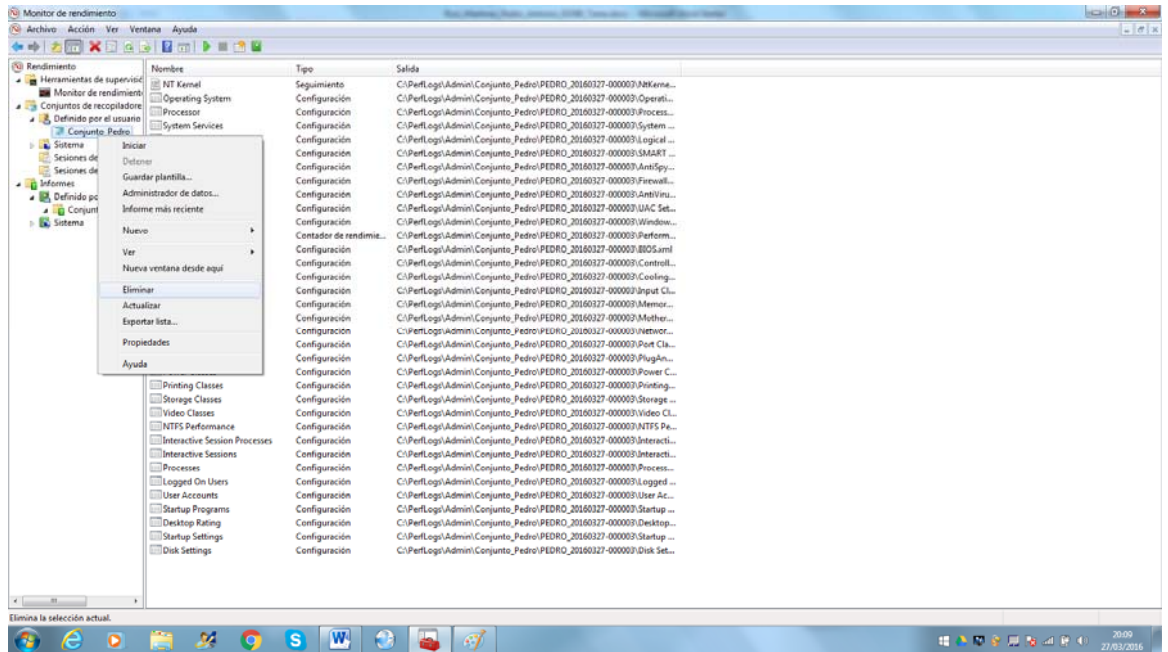
Ahora procedemos a eliminar el informe que acabamos de crear. Para ello nos situamos en la parte izquierda y en desplegamos la carpeta "Informes" desplegamos la carpeta "Definido por el usuario" desplegamos la carpeta "Conjunto_Pedro" y dentro de esta nos situamos sobre el informe que acabamos de crear. Pulsamos el botón derecho del ratón y seleccionamos la opción eliminar en el menú que nos aparece.



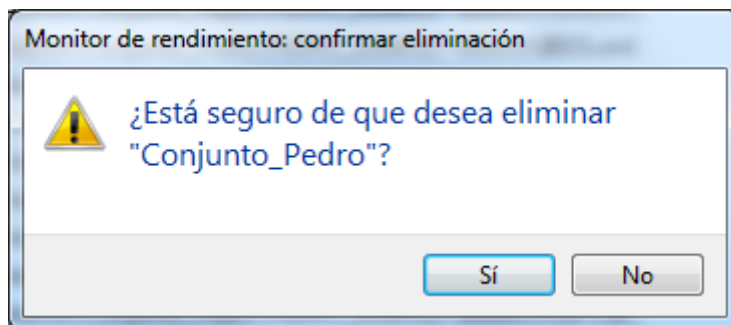
Realizado lo anterior se nos solicita confirmación de la eliminación del informe. Pulsamos en "sí" y el informe quedará eliminado.



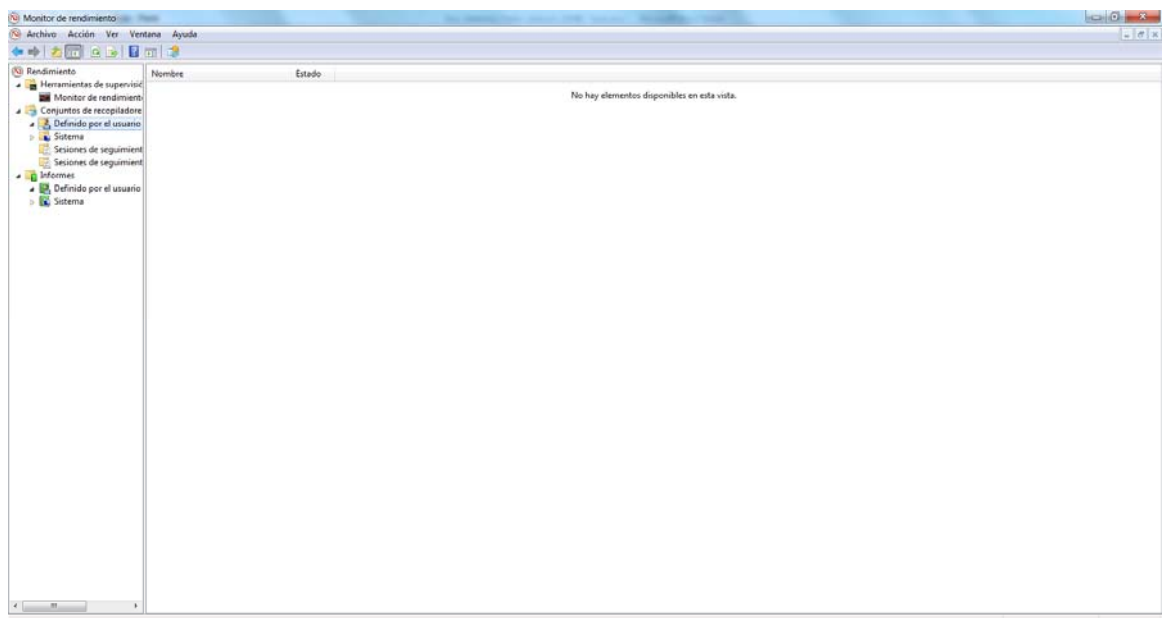
Para eliminar el conjunto recopilador de datos, seguimos en la parte izquierda de la pantalla y nos dirigimos al apartado "Conjuntos de recopiladores" desplegamos la carpeta "Definido por el usuario". Nos situamos en el conjunto recopilador "Conjunto_Pedro" y pulsamos el botón derecho de ratón seleccionando posteriormente la opción eliminar.



Se nos vuelve a solicitar confirmación para eliminar el conjunto recopilador.



Pulsando en "Si" habremos eliminado el conjunto recopilador de datos"

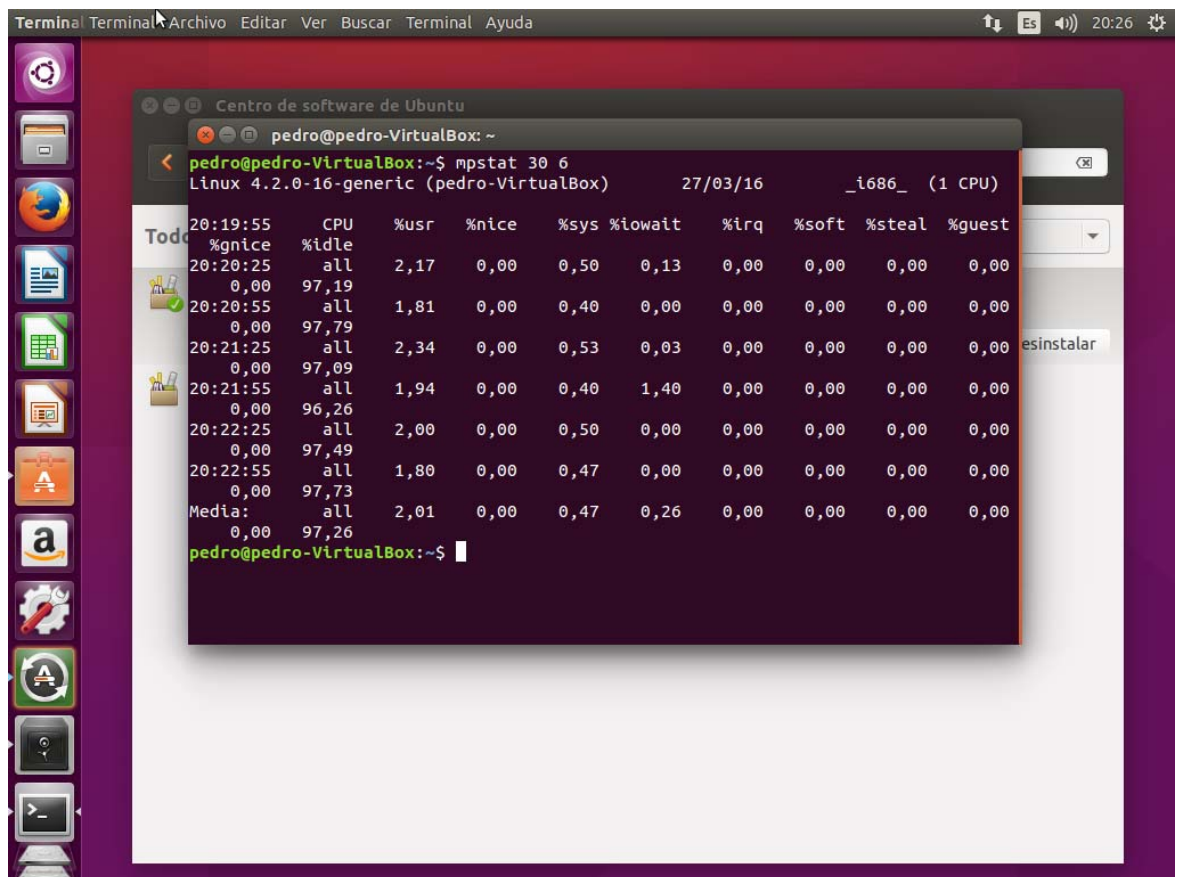


Actividad 5.

Previamente a la realización de los apartados de esta actividad hemos descargado e instalado la aplicación SYSSTAT en nuestra máquina virtual de Linux Ubuntu.

1.-Monitorización del procesador durante los últimos 3 minutos en intervalos de 3 segundos.

Desde una línea de comandos de Ubuntu ejecutamos la orden "mpstat 30 6", "30" ya que queremos una línea de informe cada 30 segundos. Además como queremos que este sea durante 3 minutos añadimos "6", ya que necesitaremos seis informes para llegar a los tres minutos de duración.



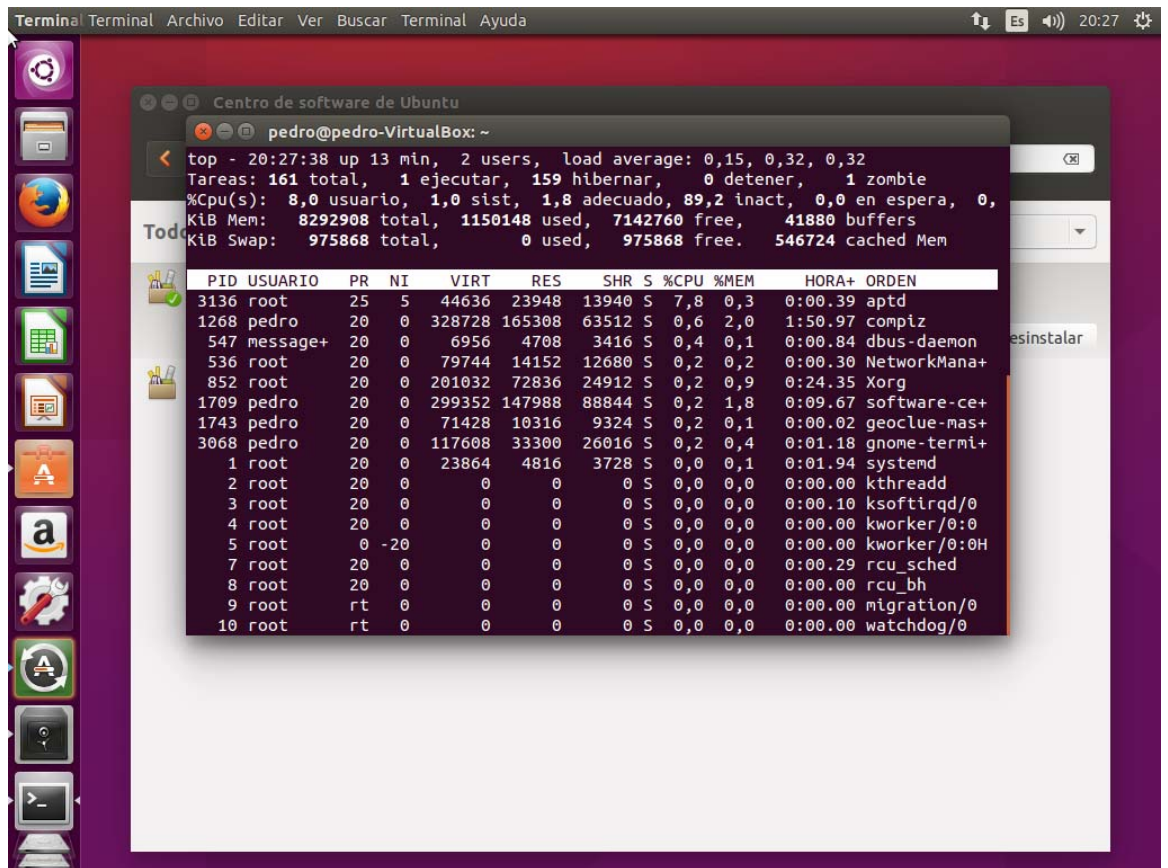
```
Terminal Terminal Archivo Editar Ver Buscar Terminal Ayuda
Centro de software de Ubuntu
pedro@pedro-VirtualBox: ~
pedro@pedro-VirtualBox:~$ mpstat 30 6
Linux 4.2.0-16-generic (pedro-VirtualBox)      27/03/16      _i686_ (1 CPU)

20:19:55   CPU   %usr   %nice    %sys %iowait    %irq   %soft  %steal  %guest
 %gnice   %idle
20:20:25   all    2,17    0,00    0,50    0,13    0,00    0,00    0,00    0,00
          0,00   97,19
20:20:55   all    1,81    0,00    0,40    0,00    0,00    0,00    0,00    0,00
          0,00   97,79
20:21:25   all    2,34    0,00    0,53    0,03    0,00    0,00    0,00    0,00
          0,00   97,09
20:21:55   all    1,94    0,00    0,40    1,40    0,00    0,00    0,00    0,00
          0,00   96,26
20:22:25   all    2,00    0,00    0,50    0,00    0,00    0,00    0,00    0,00
          0,00   97,49
20:22:55   all    1,80    0,00    0,47    0,00    0,00    0,00    0,00    0,00
          0,00   97,73
Media:     all    2,01    0,00    0,47    0,26    0,00    0,00    0,00    0,00
          0,00   97,26

pedro@pedro-VirtualBox:~$
```

2.- Monitorización de los procesos durante el último minuto en intervalos de 5 segundos.

Ejecutamos en la línea de comandos la orden "top -d5 -n12". Con el modificadores "-d5" conseguimos que la lista de proceso se actualice cada 5 segundos y con "-n12" conseguimos que top se actualice 12 veces y después se cierre así conseguiremos la duración de 1 minuto con actualización de los procesos cada 5 segundos.



Este comando también nos da información acerca del sistema. En la primera línea actual, tiempo que lleva funcionando el sistema, usuarios conectados en este momento y carga de la CPU. En la segunda línea nos muestra un resumen de los procesos que están corriendo divididos por estados (totales, ejecutándose, hibernadas, detenidas y zombie).

En la tercera línea nos da información sobre el uso de la CPU en este momento.

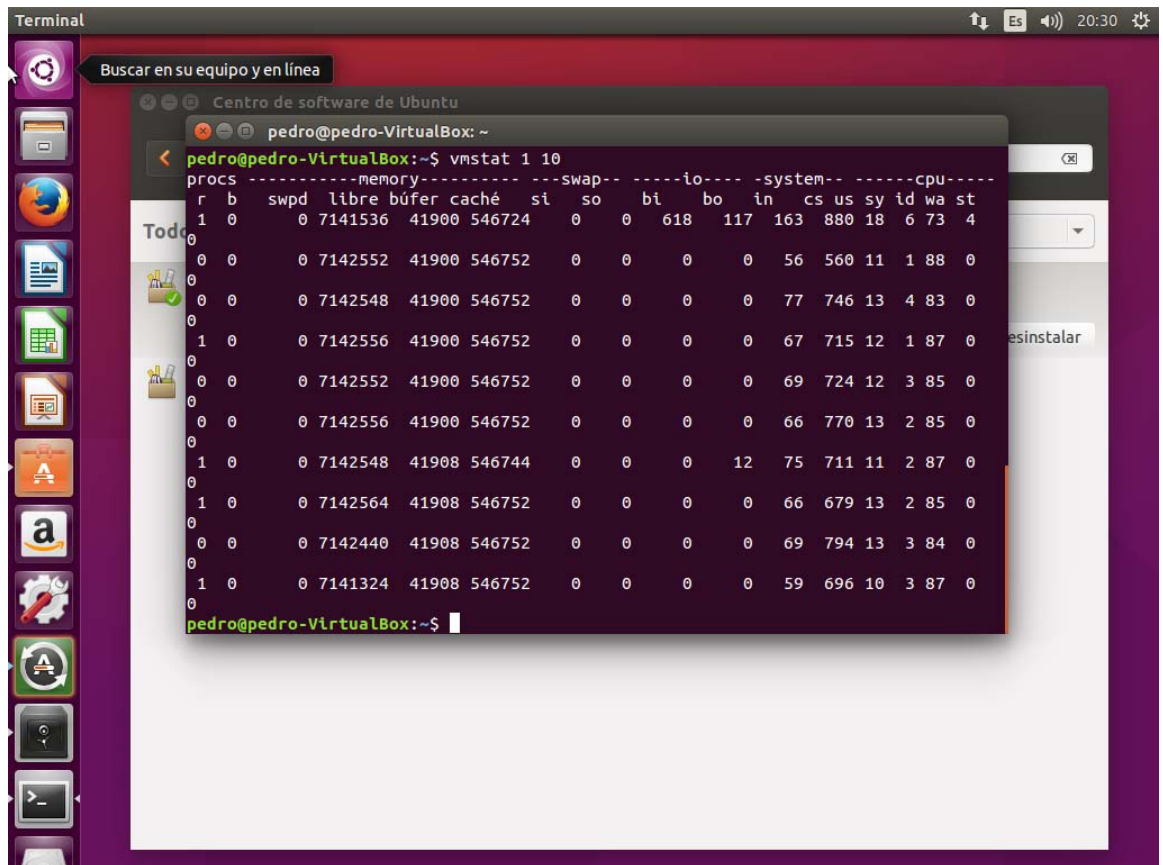
La cuarta línea nos da información sobre memoria física.

La quinta línea no muestra valores de uso de la memoria de SWAP.

A partir de allí ya se nos muestra la información sobre los procesos.

3.- Monitorización de la memoria durante los últimos 10 segundos en intervalos de 1 segundo.

Ejecutamos desde la línea de comandos la orden "vmstat 1 10". Con el "1" indicamos el intervalo de tiempo en segundos que debe transcurrir entre los informes y con el "10" determinamos el número de informes que queremos que se nos muestren. Como se nos solicita que el análisis se realice sobre diez segundos con intervalos de un segundo debemos de determinar diez informes.



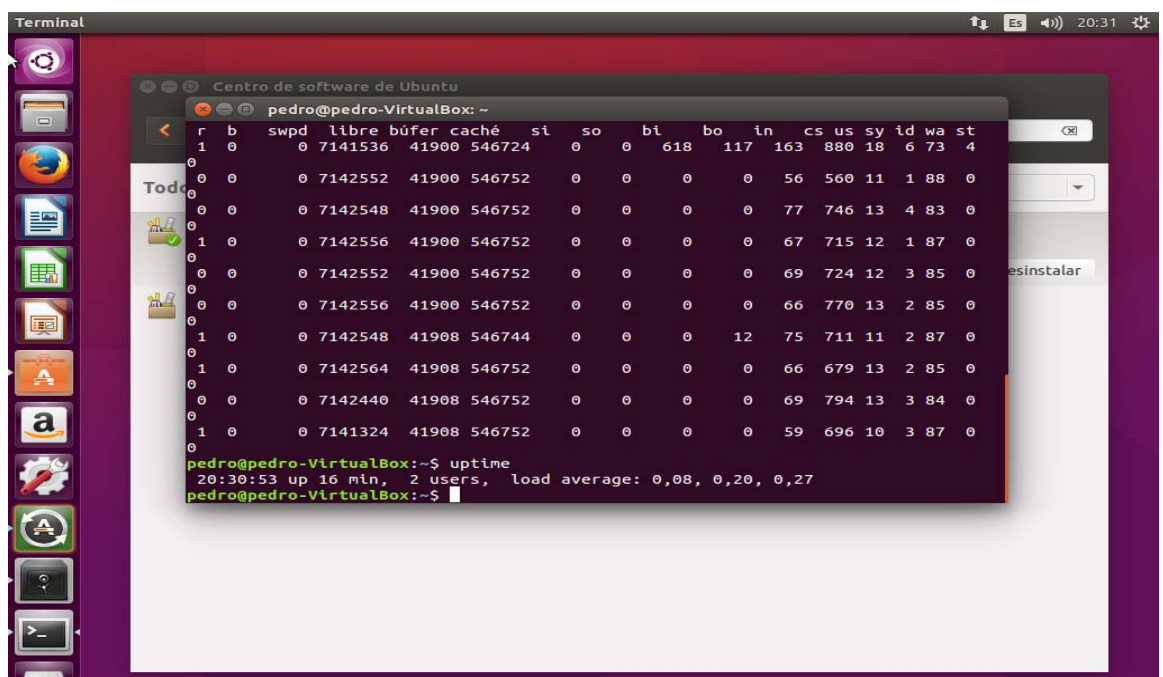
```
Terminal
Buscar en su equipo y en línea

Centro de software de Ubuntu

pedro@pedro-VirtualBox: ~
pedro@pedro-VirtualBox:~$ vmstat 1 10
procs-----memory-----swap-----io-----system-----cpu-----
r b swpd libre búfer caché si so bi bo in cs us sy id wa st
1 0 0 7141536 41900 546724 0 0 618 117 163 880 18 6 73 4
0 0 0 7142552 41900 546752 0 0 0 0 56 560 11 1 88 0
0 0 0 7142548 41900 546752 0 0 0 0 77 746 13 4 83 0
0 0 0 7142556 41900 546752 0 0 0 0 67 715 12 1 87 0
0 0 0 7142552 41900 546752 0 0 0 0 69 724 12 3 85 0
0 0 0 7142556 41900 546752 0 0 0 0 66 770 13 2 85 0
1 0 0 7142548 41908 546744 0 0 0 12 75 711 11 2 87 0
1 0 0 7142564 41908 546752 0 0 0 0 66 679 13 2 85 0
0 0 0 7142440 41908 546752 0 0 0 0 69 794 13 3 84 0
1 0 0 7141324 41908 546752 0 0 0 0 59 696 10 3 87 0
pedro@pedro-VirtualBox:~$
```

4.- Monitorización de la carga del sistema.

Ejecutamos en línea de comandos la orden "uptime" y como resultado se nos muestra la carga del sistema en el último minuto, en los últimos cinco minutos y en los últimos 10 minutos.



```
Terminal
Buscar en su equipo y en línea

Centro de software de Ubuntu

pedro@pedro-VirtualBox: ~
pedro@pedro-VirtualBox:~$ uptime
20:30:53 up 16 min, 2 users, load average: 0,08, 0,20, 0,27
pedro@pedro-VirtualBox:~$
```