UF0864: Resolución de averías lógicas en equipos microinformáticos

Elaborado por: Óscar Anaya Martín

Edición: 5.0

EDITORIAL ELEARNING S.L.

ISBN: 978-84-16424-05-4 • Depósito legal: MA 373-2015

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa:

Bienvenido a la Unidad Formativa UF0864: Resolución de averías lógicas en equipos microinformáticos. Esta Unidad Formativa pertenece al Módulo Formativo MF0954_2: reparación de equipamiento microinformático, que forma parte del Certificados de Profesionalidad IFCT0309: Montaje y reparación de sistemas microinformáticos, de la familia de Informática y comunicaciones.

Presentación de los contenidos:

La finalidad de esta Unidad Formativa es enseñar al alumno a diagnosticar y reparar fallos lógicos en equipos microinformáticos, utilizando herramientas software específicas y siguiendo los procedimientos establecidos. Para ello, se profundizará en el funcionamiento del administrador de tareas y en las herramientas de recuperación de datos y se estudiará la resolución de averías lógicas y la instalación y configuración del software antivirus.

Objetivos de la Unidad Formativa:

Al finalizar esta unidad formativa aprenderás a:

– Recuperar la funcionalidad del equipo informático identificando y aplicando los procedimientos de reparación de averías lógicas de acuerdo a las especificaciones recibidas.

Índice

UD1. El administrador de tareas y herramientas de recuperación de datos 9

1.1. El administrador de tareas 11
1.1.1. El administrador de tareas 17
1.1.2. Programas 20
1.1.3. Procesos 23
1.1.4. Medidas de rendimiento 25

1.2. Instalación y utilización de herramientas de recuperación de datos 29
1.2.1. La recuperación de datos. Concepto y funcionamiento 32
1.2.2. Herramientas comerciales de recuperación de datos ... 33
1.2.3. Instalación de herramientas 37
1.2.4. Procedimiento de búsqueda y recuperación de datos . 40

UD2. Resolución de averías lógicas 49

2.1. El Master Boot Record (MBR), particiones y partición activa ... 51

2.2. Archivos de inicio del sistema 55

2.3. Archivos de configuración del sistema 57

2.4. Optimización del sistema 62

2.5. Copia de seguridad 68
2.5.1. Transferencia de archivos 71
2.5.2. Herramientas de back-up 73
2.5.3. Clonación 76

2.6. Restablecimiento por clonación 78
2.7. Reinstalación, configuración y actualización de componentes software 79

UD3. Instalación y configuración del software antivirus 87

3.1. Virus informáticos 91
3.1.1. Software malicioso: Conceptos y definiciones 92
3.1.1.1.Evolución 97
3.1.1.2. Virus, gusanos, troyanos, otros 103
3.1.1.3. Vulnerabilidades en programas y parches 105
3.1.1.4. Tipos de ficheros que pueden infectarse 106
3.1.1.5. Medios de propagación 108
3.1.1.6. Virus en correos, en programas y en documentos 112
3.1.1.7. Ocultación del software malicioso 113
3.1.1.8. Páginas web 114
3.1.1.9. Correo electrónico 116
3.1.1.10. Memoria principal del ordenador 118
3.1.1.11. Sector de arranque 119
3.1.1.12. Ficheros con macros 121
3.1.2. Efectos y síntomas de la infección 123
3.1.3. Virus informáticos y sistemas operativos 124
3.1.4. Actualizaciones críticas de sistemas operativos 128
3.1.5. Precauciones para evitar infección 131

3.2. Definición de software antivirus 133

3.3. Componentes activos de los antivirus 135
3.3.1. Vacuna 136
3.3.2. Detector 139
3.3.3. Eliminador 140

3.4. Características generales de los paquetes de software antivirus 141
3.4.1. Protección anti-spyware 142
3.4.2. Protección contra el software malicioso 143
3.4.3. Protección firewall 144
3.4.4. Protección contra vulnerabilidades 145
3.4.5. Protección contra estafas 146
3.4.6. Actualizaciones automáticas 148
3.4.7. Copias de seguridad y optimización del rendimiento del ordenador 149

3.5. Instalación de software antivirus 151
3.5.1. Requisitos del sistema 152
3.5.2. Instalación, configuración y activación del software 154

3.5.3. Creación de discos de rescate 155
3.5.4. Desinstalación..... 156

3.6. La ventana principal 157
3.6.1. Estado de las protecciones. Activación y desactivación..... 159
3.6.2. Tipos de análisis e informes..... 162
3.6.3. Actualización automática y manual..... 162
3.6.3.1. Actualización de patrones de virus y/o ficheros identificadores de malware..... 164
3.6.4. Configuración de las protecciones. Activación y desactivación 164
3.6.5. Análisis, eliminación de virus y recuperación de los datos..... 166
3.6.6. Actualizaciones 167
3.6.7. Acceso a servicios..... 167
3.6.7.1. Soporte 169
3.6.7.2. Obtención de información 170
3.6.8. Otras opciones 172

Glosario..... 181

Soluciones..... 185

Anexo..... 187

Área: Informática y Comunicaciones

UD1

El administrador de tareas y herramientas de recuperación de datos

1.1. El administrador de tareas
- 1.1.1. El administrador de tareas
- 1.1.2. Programas
- 1.1.3. Procesos
- 1.1.4. Medidas de rendimiento

1.2. Instalación y utilización de herramientas de recuperación de datos
- 1.2.1. La recuperación de datos. Concepto y funcionamiento
- 1.2.2. Herramientas comerciales de recuperación de datos
- 1.2.3. Instalación de herramientas
- 1.2.4. Procedimiento de búsqueda y recuperación de datos

1.1. El administrador de tareas

Introducción

El administrador de tareas es un software que disponen los sistemas operativos para que el usuario pueda conocer los programas, servicios, uso del sistema y usuarios que están siendo usados en el sistema en un momento determinado.

El administrador de tareas en Sistemas Operativos Windows

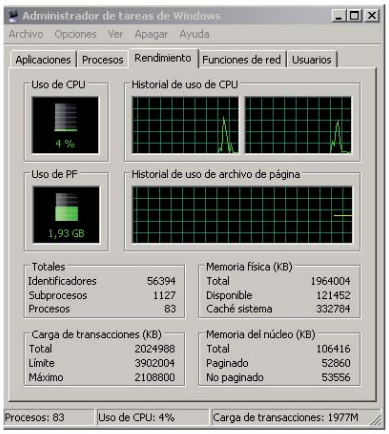
La forma popular de acceso al programa es mediante la famosa combinación de tres teclas Ctrl. + Alt. + Supr. , aunque dispone de otras formas de acceso que son:

– Botón derecho en la barra de tareas y pulsamos en administrar tareas.

– Inicio -> ejecutar ->taskmgr.

Es una aplicación que se suele usar mucho para “matar” aplicaciones que se han quedado “colgadas” y para localizar y “matar” procesos sospechosos de ser un virus, procesos que están ralentizando el sistema, servicios innecesarios, etc. Para finalizar una tarea, se realiza desde el administrador de tareas, seleccionamos la tarea o proceso desea y le damos a finalizar.

Aunque también permite la ejecución de una tarea nueva, disponible desde el botón “Nueva tarea” y también permite el cambio de tarea activa que corresponde con el cambio de ventana activa, el cambio de ventana activa dispone de una combinación de teclas de acceso rápido que es: Alt. + Tab., este modo de cambiar de tarea permite una previsualización de la ventana activa a colocar.



Administrador de tareas

El administrador de tareas, dispone de una serie de funcionalidades organizada en pestañas, que son:

– Aplicaciones, pestaña que nos permite conocer las tareas que están siendo ejecutadas, dispone de un listado donde visualizamos aquellas aplicaciones que se visualizan en una ventana.

  El listado de aplicaciones podemos visualizar la información de las tareas en un formato tabla, compuesto por dos columnas, que son:

  · Columna tarea. En ella se nos muestra el nombre de la tarea, el cual está formado por nombre de archivo y nombre de documento.

    Con el botón derecho sobre el nombre de la tarea, tenemos al menú contextual de la tarea, desde la cuál podemos acceder a las siguientes opciones:

    › Pasar a – esta opción nos permite cambiar la ventana activa a la correspondiente de la tarea elegida.

    › Traer al frente – Permite visualizar la ventana correspondiente a la tarea seleccionada.

    › Minimizar – Ocultar o minimizar la ventana correspondiente a la tarea seleccionada.

- › Maximizar – Visualizar en tamaño completo o maximizar la ventana correspondiente a la tarea elegida.

- › Finalizar tarea – Terminar la tarea, el proceso relacionado con ella y cerramos la ventana de la misma.

- › Ir al proceso – Nos muestra el proceso relacionada con la tarea elegida.

· Columna estado. En ella nos muestra información sobre el estado de la tarea, que puede ser activo cuando el proceso funciona correctamente y No responde cuando está bloqueado.

En la parte inferior de la pestaña, están accesibles tres botones, que son:

· Botón Pasar a nos permite cambiar la ventana activa a la correspondiente de la tarea elegida.

· Botón Nueva tarea. Nos permite ejecutar un comando de la consola de Windows o ejecutar una aplicación introduciendo su nombre.

· Botón finalizar tarea. Terminar la tarea, el proceso relacionado con ella y cerramos la ventana de la misma, este procedimiento se suele usar mucho para forzar el cierre de aplicaciones.

– Procesos. Pestaña que nos muestra todas las aplicaciones en ejecución denominadas procesos o servicios, cada tarea de la pestaña Programas, tiene un proceso asociado.

Dispone de un listado de procesos con la siguiente información:

· Nombre de imagen – Se corresponde con el nombre del ejecutable.

· Nombre de usuario – Usuario que ha ejecutado la aplicación.

· CPU – Cantidad porcentual de recursos del procesador que está usando.

· Memoria principal – Número de bytes que está usando en memoria principal.

· Descripción – Descripción de la aplicación.

Dispone además en esta pestaña de un botón desde el cuál Terminar proceso, con el cuál podemos forzar el cierre del proceso seleccionado.

– Rendimiento, pestaña que nos permite visualizar el rendimiento del equipo, mostrando información sobre el uso del procesador, la memoria, además dispone de una pestaña especifica para mostrar el rendimiento en el uso de la red de área local (normalmente se traduce el rendimiento de la actividad en Internet).

– Usuarios. Pestaña que nos permite conocer los usuarios que han iniciado sesión en el sistema operativo, que normalmente es sólo un usuario, a no ser que se trate de un Windows Server donde suelen iniciar multitud de usuarios.

Las tareas programadas son aquellas que se ejecutan con una cierta periodicidad, podemos gestionar las tareas programadas a través del Administrador de Tareas programas, disponemos de acceso a través Panel de Control, Sistema y Mantenimiento, Herramientas Administrativas, Programador de tareas.

Desde el programador de tareas, visualizamos el listado de tareas programadas. Desde aquí además tenemos la posibilidad de gestionarlas:

– Crear tarea programada. Para comenzar el proceso de creación de una tarea programada, podemos proceder de tres formas:

  · Archivo, Nueva tarea programada.

  · Botón derecho, Nueva tarea programada.

  · Desde el botón Agregar tarea programada.

  El primer paso del asistente es seleccionar la aplicación a ejecutar.

  El segundo paso del asistente es seleccionar la periodicidad de la tarea, que puede ser diaria, semanal, mensual, cuando se arranque el ordenador, etc.

– Para editar una tarea programada, pulsamos el botón derecho del ratón sobre la misma y le damos a propiedades, desde aquí podemos modificar la tarea en la ventana de edición de tarea programada, que dispone de la información dispuesta en tres pestañas, que son:

  · Pestaña tarea, en ella podemos seleccionar la tarea a ejecutar, modificar el nombre, habilitar y deshabilitarla.

  · Pestaña programa, en ella configuramos la periodicidad de la tarea, disponemos de un botón de configuración avanzada para la programación de la periodicidad, donde se puede programar además una fecha hasta la cual tiene vigencia la configuración.

  · Pestaña configuración, en ella podemos configurar los valores avanzados de la programación de tareas.

– Para eliminar una tarea programa, pulsamos el botón derecho sobre la misma y hacemos clic en eliminar.

Un programa es un algoritmo que tiene como objetivo la resolución de problemas por parte del usuario. Los programas usan datos y documentos para realizar sus operaciones.

Un programa puede estar en diferentes posibles estados:

– En ejecución, en ese momento se convierte en un proceso.

– Preparado para la ejecución, instalado en el sistema operativo o ser un programa portable.

– Preparado para la instalación, disponemos del archivo instalador, pero no está todavía instalado en el sistema operativo. Sobre todo cuando hablamos de sistemas Windows, suele ser necesario realizar la instalación de un programa para poder realizar su ejecución.

Un **proceso** es un programa que está siendo ejecutado por el procesador, es decir, cuando las instrucciones del programa están en el disco duro (o sea el programa está cerrado) todavía no es un proceso. Al realizar doble clic en un sistema Windows sobre la aplicación por parte del usuario, el programa y sus datos son cargados en memoria siendo entonces un proceso.

El concepto de proceso es fundamental para comprender el funcionamiento de un procesador y de la gestión que realiza el sistema operativo para priorizar y agilizar la ejecución de tareas por parte del procesador de la forma más eficiente posible.

Un **servicio** es un proceso, es decir, es un programa en ejecución, normalmente de sistema, que se ejecuta sin intervención por parte del usuario.

El sistema operativo suele disponer de muchos servicios en ejecución, muchos de ellos no son necesarios para el uso de un usuario doméstico, por lo que se pueden desactivar sin perjuicio alguno por parte del usuario. Aunque otros servicios son vitales para el correcto funcionamiento del sistema operativo, aportando diversas funcionalidades que permiten mantener el sistema actualizado o debidamente protegido.

Existen servicios de otro tipo de software:

- Protección residente del sistema por parte del antivirus.
- Los servicios de actualizaciones automáticas de diferentes tipos de software.
- Software usado para funcionar como servidor.
- Herramientas de optimización suelen contener servicios de control de la carga del equipo.

Los servicios se pueden configurar con el archivo de configuración services.msc accediendo a esta configuración, podemos visualizar el listado de servicios disponibles, iniciar, parlar, y configurar el arranque del servicio.

El sistema operativo Windows nos ofrece la posibilidad de iniciar o detener servicios accediendo del siguiente modo:

– En Windows XP. Inicio –> Configuración –> Panel de control –> Herramientas administrativas –> Servicios.

– En Windows 7. Inicio –> Panel de control –> Sistema y seguridad –> Herramientas administrativas –> Servicios.

Al acceder al panel de servicios, podemos visualizar el estado en que se encuentra cada uno, tanto los que se encuentran en ejecución (iniciados) como aquellos que estén detenidos.

Para cambiar el estado de un servicio deberemos pulsar sobre él, clic con botón derecho del ratón y clic en "Propiedades", pudiendo desde aquí iniciar o detener cada uno de los servicios listados.

Cada servicio puede pertenecer a un grupo diferente, dependiendo del modo en que se ejecuta durante el sistema de arranque de un sistema operativo:

– Automáticos. Son aquellos servicios que se inicia de forma automática al arrancar el sistema operativo.

– Manuales.Son aquellos que se pueden iniciar y detener manualmente, o "semiautomáticamente", a través de otro servicio o programa.

– Deshabilitados. Son servicios que no se inician bajo ningún concepto.

1.1.1. El administrador de tareas

El administrador de tareas en Sistemas Operativos Linux

El administrador de tareas no es un software exclusivo de los sistemas operativos Windows. Los sistemas operativos Linux disponen de su propio administrador de tareas, algunas distribuciones Linux como Ubuntu dispone de herramientas gráficas para su uso, en todas las distribuciones Linux existen comandos para su ejecución.

Monitor de sistema en distribuciones Ubuntu

El monitor de sistema en sistemas Linux es equivalente al Administrador de Tareas de Windows, para acceder al monitor de sistema, lo realizamos desde el menú Aplicaciones, Herramientas del Sistema, Monitor del Sistema.

Este programa está organizado también en pestañas, siendo estas pestañas:

– Sistema. Nos informa sobre las características del sistema operativo como el nombre y versión de la distribución, características del hardware como microprocesador, memoria, etc.

– Procesos. Es similar a la pestaña de procesos del administrador de tareas de Windows. Con él podemos ver los servicios y programas que se están ejecutando en el ordenador.

– Recursos. Es el equivalente a la pestañas Rendimiento y Funciones de Red del administrador de tareas de Windows, nos muestra información del uso y rendimiento del procesador, la memoria y las conexiones a Internet.

– Sistema de archivos. Nos muestra un resumen de las particiones, espacio ocupado y libre de cada una, su sistema de archivos donde está ubicada y montada.

Si disponemos de un sistema Linux, sin entorno gráfico, esto es muy común en servidores, debemos conocer la forma de administrar las tareas, pero en este caso en modo consola o por comandos, existe un comando en todas las distribuciones Linux que permite la visualización y administración de procesos en ejecución:

– ps"process status" o estado de los procesos, como muchos de los comandos Linux dispone de modificadores y condicionales para facilitar la tarea, la recomendación es ejecutarlo con las variantes ps –ef, que muestra un listado completo de procesos con todos los datos que nos puede facilitar el sistema.

  El resultado se muestra dispuesto en las siguientes columnas:

UID PID PPID C STIME TTY TIME CMD

– La primera columna del resultado es UID es representa el identificador del usuario que ha iniciado el proceso.

– La segunda columna del resultado se denomina como PID (Process ID) que es el código que identifica el proceso, este número se puede usar para matar un proceso que no responde o que está molestando, esto se realiza con el comando kill.

– La tercera columna del resultado se denomina PPID (ParentProcess ID), es el código del proceso padre.

– La cuarta columna, se denomina C representa el porcentaje de uso de CPU.

– La quinta columna, se denomina STIME (Start Time), hora de inicio del proceso.

– La sexta columna, se denomina TTY, representa terminal asociada al proceso.

– La última columna CMD, es el comando que ha iniciado el proceso.

Ejemplo: Queremos matar una aplicación bloqueada que es la calculadora de Ubuntu, el programa se llama calc, tras ejecutar ps –ef optemos el siguiente resultado:

```
UID        PID  PPID  C STIME TTY          TIME CMD

user12130  23210 10:21 pts/1    00:00:00 calc
```

En el resultado visualizamos que el PID es 2130, entonces para matar el proceso debemos ejecutar lo siguiente: kill -9 2130(-9 es para forzar el cierre del programa en cualquier caso).

El comando kill, cuya traducción literal es matar, su se utiliza normalmente para terminar o matar procesos, pero también se puede usar para enviar señales a los procesos, si usamos kill PID estamos enviando una señal de stop al proceso quedando en memoria a espera de continuar.

Para facilitar la tarea de administración podemos contar con otros comandos que nos facilita la administración de tareas y procesos.

El comando grep usado para buscar contenido dentro de archivos, también se puede usar para realizar filtrado en comandos, por ejemplo para buscar el PID del proceso calc en el listado ps –ef, lo realizaremos:

```
ps –ef | grep calc
```

El carácter |, denominado tubería, permite pasar el resultado del comando ps –ef a ser filtrado por el comando grep, obteniendo como resultado un listado filtrado en pantalla con los procesos relacionados con el comando calc.

El comando killall, es similar a kill, pero usado para matar un programa y todos los procesos relacionados con él, se usa introduciendo el nombre del programa, en vez del PID, en el ejemplo anterior se usará de la siguiente forma: killallcalc

El comando nice, es un comando que permite establecer prioridades de ejecución en los procesos, por defecto todos tienen la misma prioridad.

Los sistemas operativos Linux (y los basados en Unix), son sistemas con muy alta seguridad, en la que necesitamos tener los permisos suficientes para la

administración, ejecución, lectura y/o escritura de muchos los archivos y programas que conforma el sistema operativo.

En los sistemas operativos Linux, existe un súper usuario, cuyo nombre de usuario es root (raíz) que tiene todos los permisos sobre el sistema. Si un usuario se identifica como root puede realizar todas las operaciones que desee con el sistema operativo. Para garantizar la seguridad del sistema, el uso del usuario root se recomienda entrar con una cuenta de usuario normal y realizar operaciones que necesiten más privilegios realizando su o sudo.

Para saber si tenemos permiso de lectura, escritura y/o ejecución, puede realizar sobre los archivos y directorios, puede mostrar un listado del directorio actual con el comando ls –l, el comando ls nos muestra el contenido del directorio actual, la variante –l, incluye más información sobre cada uno de los archivos, como por ejemplo los permisos sobre el archivo.

Es muy recomendable que un técnico informático sepa usar sistemas operativos Linux, para lo cual se le recomienda preparar su ordenador para instalar varios sistemas operativos. Para ello será necesario dividir el disco duro en particiones. Cada partición debe ser formateada en un sistema de archivos determinado. Para más información visualice la siguiente descarga.

Para más información, consulta Creación de particiones para instalar varios Sistemas Operativos en el anexo al final de este libro.

1.1.2. Programas

Un **programa** es una secuencia de instrucciones que tienen como objetivo la ejecución de tareas, los programas también disponen de datos. Un programa que no está en ejecución, está almacenado en el disco duro (u otro dispositivo de almacenamiento) e instalado en el sistema operativo (o se trata de un programa portable, que no requiere instalación). El usuario al realizar doble clic sobre su icono (o ejecutar su comando), en este momento el sistema opera-