

Síntesis conceptual

Asignatura: Fundamentos de <i>Hardware</i>
Unidad: 3. Instalación de <i>software</i> de utilidad y propósito general para un sistema informático

Resumen

Podemos clasificar el software y las aplicaciones según su uso:

- Software de sistema: referencia a cualquier programa que este en contacto con el hardware y actúa de intermediario entre el usuario y el hardware.
- Conjunto de software necesario en el diseño, implementación y desarrollo de software de sistema o aplicación.
- Software de aplicación: tipo de software orientado a realizar tareas concretas y uso cotidiano por parte del usuario.

Firmware hace referencia al software que contiene un hardware específico. Confundido muchas veces con el sistema operativo, el propósito general del *firmware* es la realización de ciertas tareas específicas al mismo tiempo que la optimización completa del *hardware*. El sistema operativo en cambio es de propósito general y muchísimo más complejo.

El termino *software* se usa tanto para el sistema operativo como para las aplicaciones que se desarrollan para la interacción con el sistema. En este último grupo tenemos diversas opciones:

- Aplicaciones web.
- Apps móviles.
- Widgets.
- Plugins.

Software de propósito general, son aplicaciones que tienen unas funciones más generales y de uso muy común: aplicaciones de oficina u ofimática, productividad y negocios, juegos, navegadores, educación, multimedia, antimalware, etc.

El objetivo de la compresión es que el tamaño de un fichero se reduzca de manera considerable para facilitar su gestión y almacenamiento, se realiza mediante algoritmos. Existen dos tipos:

- Algoritmos de compresión con pérdida.
- Algoritmos de compresión sin pérdida.

Hoy en día el termino de malware no solo hace referencia a los virus informáticos como pasaba antes, sino que se ha ampliado mucho el espectro de posibilidades de un programa malicioso, como son: virus, troyanos, botnets, keyloggers, spyware, adware, cookies, backdoors, ransomware, web bug, exploit, rootkits, Leapfrogs, jokes, scumware y spam.

La instalación de un antivirus nos protegerá de estos programas, ya que su función es la de detectar y eliminar o aislar cualquier tipo de programa malicioso.

En el caso de que empleemos Linux podemos realizar ciertas acciones mediante comandos que nos facilitaran el trabajo.

- Podemos monitorizar el sistema con:
 - uptime.
 - time programa.
 - top.
 - ps.
 - iostat.
 - mpstat.
 - pidstat.
 - sar.
- Podemos gestionar los recursos con:
 - df.
 - du.
 - free.
- Una segunda opción es acceder al monitor del sistema, al igual que con Windows nos dará toda la información con una interfaz gráfica.

Conceptos fundamentales

- **Backdoors:** llamadas puertas traseras, son agujeros de seguridad en el sistema que sirven para que un atacante entre sin la necesidad de una identificación previa y sin la detección del acceso por parte del sistema.
- **Ransomware:** el ransomware es posiblemente el más dañino de todos los tipos de malware. Se usa para cifrar todo el sistema y quitarles el acceso a los usuarios ya que no poseen la correspondiente clave.
- **Cookies:** las cookies de los navegadores de internet son archivos que contienen información sobre el usuario y que han ido evolucionando a lo largo de los años.
- **AppStore:** es la tienda de Apple en la cual se pueden descargar aplicaciones para todos los dispositivos Apple y son aplicaciones en su mayoría específicas.
- **Google Play:** se trata de la tienda de aplicaciones creada por Google para dispositivos Android.